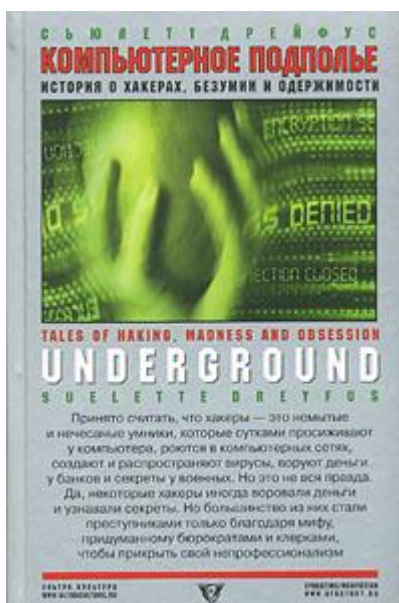


## Сьюлетт Дрейфус

### Компьютерное подполье. Истории о хакинге, безумии и одержимости



Марсель из Казани <http://reced.ru/>

«Дрейфус Сьюлетт «Компьютерный андеграунд: Истории о хакинге, безумии и одержимости»»: У-Фактория; Екатеринбург; 2005

ISBN 5-9709-0040-0

Оригинал: Suelette Dreyfus, “Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier”

Перевод: А. Луцанов

## **Аннотация**

*При техническом содействии австралийского хакера Джулиана Ассанжа талантливой журналистке удалось проникнуть в тесно граничащий с криминалом мир хакерского подполья в США, Австралии и Великобритании. Помимо аккуратно фиксируемых технических подробностей, в фокусе повествования постоянно находятся живые люди, стоящие за всеми этими проникновениями. Порой блестящие до гениальности, порой одержимые, многие из этих хакеров так втянулись в свое «дело», что в конце концов стали социальными изгоями. Кто-то закончил наркотиками и безумием, кого-то подполье привело к аресту и длительному тюремному заключению...*

*По признанию многих, «Underground» стала чуть ли не единственной книгой, в которой автор глубоко и тщательно проанализировал компьютерное подполье.*

*(«Компьютерра»)*

*Это не просто очередная книга об Интернете. В ее фокусе – причудливые судьбы и эксцентричные преступления выдающейся группы молодых хакеров. Захватывающая, в высшей степени читабельная книжка. Дрейфус открыла один из наиболее хорошо охраняемых спецслужбами секретов и создала книгу, читающуюся с удовольствием и напряжением...*

*(«Rolling Stone»)*

**Дрейфус Сьюлетт**  
**(при участии Джулиана Ассанжа)**  
**Компьютерный андеграунд.**  
**Истории о хакинге, безумии и одержимости**

*Посвящаю Питеру и моей семье*  
**С. Д.**

*Посвящаю Д.*  
**Д. А.**

*Авторские примечания имеют цифровые сноски, сноски на примечания переводчика начинаются с «р» – прим. сост. FB2*

**Мои благодарности**

Многие люди дали мне интервью для этой книги. Множество других помогли мне с документами, жизненно необходимыми для проверки описанных в ней фактов. Зачастую эта помощь требовала от них значительных затрат времени, поскольку требовалась в сложных технических и юридических вопросах. Я хотела бы выразить свою благодарность всем этим людям, многие из которых предпочли сохранить анонимность, за их готовность просмотреть файлы в поисках еще одного отчета и их терпение при ответе на еще один вопрос.

Я хочу сказать спасибо членам компьютерного подполья, бывшим и настоящим, которые согласились дать интервью для этой книги. Многие позволили мне получить доступ в их жизни, за что я чрезвычайно признательна.

Я также хочу поблагодарить Джулиана Ассанжа за его неустанные поиски. Его бесценный технический опыт отражен в огромном количестве деталей, включенных в книгу.

Три исключительных женщины – Фиона Инглис, Деб Каллахан и Дженнифер Бирн – поверили в мое видение этой книги и помогли осуществить мой замысел. Великолепная редакторская работа Карла Харрисона-Форда привела в порядок пространную и сложную рукопись, несмотря на крайне ограниченные сроки. Большое спасибо также Джуди Брукс.

Еще я очень признательна следующим людям и организациям за их помощь (оказанную не частным образом): Джону Мак-Магону, Рону Тенкати, Кевину Оберману, Рэю Каплану, сотрудникам библиотеки *New York Daily News*, сотрудникам библиотеки *New York Post*, сотрудникам Городского суда на Боу-стрит, сотрудникам суда Саутворк, Секретной службе США, полиции Блэк-Маунтин, Майклу Розенбергу, Майклу Розену, сотрудникам Городского суда Мельбурна, сотрудникам D. L. Sellers & Co., сотрудникам Окружного суда штата Виктория, Полу Голбалли, Марку Дорсету, Suburbia.net, Freeside Communications, Грегу Хуперу, H&S Support Services, Питеру Эндрюсу, Кевину Томпсону, Эндрю Уиверу, Мухтару Хусейну, Midnight Oil, Хелен Мередит, Ивану Химельхоху, Майклу Холлу, Донну Феррису, сотрудникам Государственной библиотеки штата Виктория, сотрудникам библиотеки News Limited (Сидней), Алану Янгу, Эду Де-Харту, Аннет Сибер, Артуру Аркину, Дугу Барнсу, Джереми Портеру, Джеймсу Мак-Наббу, Кэролин Форд, АТА, Домини Банфилду, Алистер Келман, Энн-Мэри Муди, Джейн Хатчинсон, Кэтрин Мерфи, Норме Хокинс, Н. Ллевеллин, Кристин Ассанж, Расселу Брэнду, Мэтью Бишопу, Мэтью Коксу, Мишель Зелки, Эндрю Джеймсу, Брендану Мак-Грату, Warner Chapell Music Australia, News Limited, Pearson Williams Solicitors, Рами Фридман, The Free Software Foundation (GNU Project) и Консультативной службе по компьютерным инцидентам Министерства энергетики США.

Спасибо также Клер, Лэнсу, Майклу и Либби.

Напоследок я хочу поблагодарить мою семью и Питера. Их неизменная поддержка, советы и ободрение дали мне возможность написать эту книгу.

**Предисловие**

Сестра моей бабушки занималась подводной живописью.

Люси в своем тяжеленном подводном снаряжении образца 1939 года напоминала персонаж

«20 000 лье под водой». Она медленно погружалась под воду с палитрой, специальными красками и холстом в руках, устраивалась на дне океана, раскладывала особый утяжеленный мольберт и полностью отдавалась во власть иного мира. Красно-белые полосатые рыбки сновали в полях сине-зеленых кораллов и голубых раковин моллюсков. Неспешно проплывали скорпены, грациозно покачивая опасными ядовитыми иглами. Полосато-зеленые мурены тарасились на нее из расщелин в скалах.

Люси ныряла и рисовала повсюду. Архипелаг Сулу, Мексика, Большой Барьерный Риф в Австралии, Гавайи, Борнео... Иногда она оказывалась первой белой женщиной, увиденной обитателями тех районов Тихого океана, где она, бывало, жила месяцами.

В детстве я приходила в восторг от ее рассказов о неизведанном мире океанских глубин, о странных и чудесных культурах, с которыми она познакомилась в своих путешествиях. Я выросла в преклонении перед избранным ею путем – стремлением уловить на холсте суть совершенно чуждого ей мира.

Новая технология – революционная для того времени – позволила это осуществить. Используя компрессор, а иногда просто ручной насос, соединенный с воздушными шлангами, выходящими на поверхность воды, люди могли надолго погружаться в другой, ранее недоступный мир. Новая технология позволила Люси бросить вызов этому неисследованному царству и запечатлеть его на своих холстах.

Я столкнулась с дивным новым миром компьютерных коммуникаций и его темной стороной – компьютерным подпольем – почти случайно. И вскоре после начала путешествия по этому миру меня поразила мысль о том, что мой трепет и противоречивое желание исследовать этот чуждый мир очень напоминают чувства моей тетушки, которые она испытывала почти полвека назад. И ее, и мои путешествия стали возможными только благодаря новым технологиям. Подобно ей, я попыталась зафиксировать маленький кусочек этого мира.

Эта книга рассказывает о компьютерном подполье. Ее герои – не законопослушные граждане, но книга написана не со слов полицейских. Говоря литературным языком, я отразила в этих историях взгляды многих компьютерных хакеров. Поступая таким образом, я надеялась представить читателю возможность увидеть таинственный, скрытый, обычно недоступный мир.

Кто такие хакеры? Почему они взламывают компьютерные сети? На эти вопросы нет простых ответов. Ни один хакер не похож на другого. Поэтому я попыталась изобразить галерею индивидуальных, но переплетенных между собой историй, крепко связанных с международным компьютерным подпольем. Это подлинные хроники, повествующие о самых блестящих хакерах и фрикерах. [\[p1\]](#) В этой книге я поведала лишь о некоторых из них, хотя те, что остались в тени, тоже достойны высших рангов в мировом хакерском движении. В общем, я предпочла детально прорисовать портреты нескольких хакеров, вместо того, чтобы дать полную, но поверхностную панораму.

Хотя каждый хакер имеет свою собственную историю, в их судьбах зачастую много общего. Бунт против любых проявлений власти. Неблагополучные семьи. Способные дети, задыхающиеся под гнетом недалеких учителей. Душевная болезнь или неуравновешенность. Одержимость и зависимость.

Я приложила все силы, чтобы проследить за тем, что произошло с каждым из них с течением времени: личные хакерские приключения, полицейские налеты и последовавшие за ними судебные дела. Некоторые из этих дел затянулись на годы. Hawk, Crawler, Toucan Jones, Comhack, Dataking, Spy, Ripmax, Fractal Insanity, Blade. [\[p2\]](#) Это подлинные хэндлы [\[p3\]](#) австралийских хакеров.

В компьютерном подполье ник хакера заменяет ему имя. Именно по этой причине и еще потому, что большинство героев этой книги теперь изменили образ жизни, я решила использовать только их ники. Если у хакера было несколько прозвищ, я использовала то, которое он сам предпочитал.

Каждая глава в этой книге сопровождается цитатой из песни группы Midnight Oil, акценти-

---

p1

Взломщики телефонных сетей.

p2

Ястреб, Ползун, Тукан Джонс (тулканы – самые крупные представители отряда дятлов, отличаются непропорционально большими и ярко окрашенным клювом), Комхак, Король данных, Шпион, Максимальный Раздражитель, фрактальное безумие, Лезвие.

p3

Жаргонное значение английского «handle» – «прозвище, кличка». Другое часто используемое понятие – «nick» или «nick-name».

рующей важный аспект главы. Это уникальная австралийская группа. Ее громкий голос, протестующий против истеблишмента (особенно против военно-промышленного комплекса), созвучен основным настроениям андеграунда, для которого музыка часто жизненно важна.

Мысль использовать отрывки из их песен в качестве эпиграфов пришла ко мне, когда я собирала материалы для первой главы, рассказывающей о кризисе с червем WANK в NASA.<sup>[p4]</sup> После червя RTM, WANK является самым знаменитым в истории существования компьютерных сетей. Это первый червь с политическим посланием. WANK стал примером того, как жизнь следует за искусством – компьютерный термин «червь» заимствован из научно-фантастического романа Джона Брунера «Наездник ударной волны» [John Brunner «The Shockwave Rider»] о черве, оружии против олигархии.

Принято считать, что червь WANK стал первым червем, написанным австралийцем (или австралийцами).

Эта глава рассказывает о нескольких системных администраторах – людях, стоящих по другую сторону баррикады. Она демонстрирует изощренность, с которой совершали свои компьютерные преступления один или несколько членов австралийского компьютерного подполья.

Последующие главы представляют собой сцену драматических событий, которые раскрывают и показывают метаморфозы андеграунда: рождение, потеря невинности, замыкание в изолированных кружках и – неизбежный исход – одиночество хакера. В момент своего возникновения компьютерное подполье было таким же открытым и дружелюбным, как паб на углу. Теперь же хакеры могут лишь случайно столкнуться друг с другом в этом эфемерном пространстве, где безвозвратно утеряна изначальная идея открытого сообщества.

Компьютерный андеграунд с течением времени переменялся. В значительной степени это связано с принятием новых законов против компьютерных преступлений в разных странах мира и с последовавшими полицейскими мерами. Я не только пытаюсь запечатлеть важную часть истории Австралии, но и стремлюсь показать фундаментальные изменения, произошедшие в самом подполье, показать, в сущности, как подполье переросло самое себя.

*Сьюлетт Дрейфус*

*Март 1997 года*

## 1

### 10, 9, 8, 7, 6, 5, 4, 3, 2, 1

*Кто-то там продолжает ждать,  
Кто-то хочет мне что-то сказать.*

Песня «Somebody's Trying to Tell Me Something», альбом «10, 9, 8, 7, 6, 5, 4, 3, 2, 1» группы **Midnight Oil**<sup>1</sup>

**Понедельник, 16 октября 1989 года**

*Космический центр имени Кеннеди, Флорида .*

NASA лихорадило от возбуждения по мере приближения времени запуска. «Галилей» наконец-то отправлялся к Юпитеру.

Руководители и научные сотрудники самого престижного в мире космического агентства потратили годы, чтобы подготовить к старту этот беспилотный исследовательский аппарат. И вот теперь, если все пойдет по плану, 17 октября пятеро астронавтов на космическом челноке «Атлантис» стартуют с космодрома на мысе Канаверал с «Галилеем» на борту. На пятом витке челнока, когда он будет находиться на высоте 295 километров над Мексиканским заливом, астронавты должны будут отпустить трехтонный космический аппарат в свободный полет.

Через час после расстыковки двигатель «Галилея» тягой в 32 500 фунтов придет в движение, и персонал NASA сможет увидеть, как это замечательное порождение человеческого гения отправится

---

p4

National Aeronautics and Space Administration – Национальное управление по аэронавтике и космическим исследованиям.

<sup>1</sup> Слова и музыка: Rob Hirst, Martin Rotsey, James Moginie, Peter Garrett, Peter Gifford. © Copyright 1982 Sprint Music. Administered for the World-Warner/Chappell Music Australia Pty Ltd. Used by permission.

с шестилетней миссией к самой большой планете Солнечной системы. «Галилею» по необходимости предстояло отправиться окольным путем, пройдя сначала около Венеры и вновь мимо Земли, чтобы получить гравитационный толчок и набрать достаточную скорость для полета к Юпитеру.<sup>2</sup>

Самые могучие умы NASA годами бились над тем, как поддерживать связь с аппаратом в его пути через Солнечную систему. Одним из способов решения задачи была энергия самого Солнца. Но если Юпитер находится довольно далеко от Земли, то от Солнца он еще дальше (если точнее, то в 778,3 миллиона километрах). «Галилею» потребовались бы чудовищно большие солнечные батареи, чтобы вырабатывать энергию для своих систем на таком расстоянии от Солнца. В конце концов инженеры NASA решили использовать проверенный источник энергии – ядерный.

Ядерная энергия идеальна для космического пространства, гигантского вакуума, свободного от людей, которые едва ли обрадовались соседству с радиоактивным куском двуокиси плутония-238. Плутония было сравнительно немного, зато энергии вырабатывалось более чем достаточно. Этакий пустячок весом менее 24 килограммов в свинцовом корпусе, дайте ему только разогреться как следует благодаря радиоактивному распаду – и он сможет снабдить электричеством аппаратуру спутника. И вот «Галилей» уже на пути к Юпитеру.

Но американские антиядерные организации смотрели на это иначе. Они представили, что может произойти в случае неудачи, и им не слишком понравилась мысль о плутониевом дожде. NASA заверило их, что энергетический отсек «Галилея» абсолютно безопасен. Агентство израсходовало около пятидесяти миллионов долларов на испытания, которые, по общему мнению, доказали, что генератор совершенно безопасен. NASA заявило журналистам, что вероятность радиоактивного заражения по причине «непредусмотренного входа аппарата в плотные слои атмосферы» равна 1:2 000 000. Вероятность утечки радиации в результате неудачного запуска тоже выглядела весьма успокаивающе – 1:2700.

Но активистов это не убедило. В лучших американских традициях решения споров они продолжили свою борьбу в суде. Коалиция антиядерных и других групп посчитала, что NASA недооценивает возможность утечки плутония. Они обратились в окружной суд в Вашингтон с требованием остановить запуск. Был вынесен судебный запрет, так что ставки росли. Беспрецедентное слушание должно было состояться за несколько дней до запуска, предварительно намеченного на 12 октября.

Неделями протестующие демонстрировали свою силу, привлекая внимание СМИ. Ситуация стала крайне напряженной. В субботу 7 октября активисты надели противогазы и с плакатами в руках заняли перекрестки вокруг космодрома на мысе Канаверал. В восемь часов утра в понедельник 9 октября NASA начало отсчет времени до запуска, намеченного на четверг. Но пока часы «Атлантика» тикали, приближая время старта, активисты флоридской «Коалиции за мир и справедливость» устроили демонстрацию в туристическом комплексе космического центра.

Хотя в свете этих протестов сияние дерзкого космического замысла NASA слегка потускнело, они не слишком волновали агентство. Настоящей головной болью стало заявление Коалиции о том, что ее члены могут «пробраться на пусковую площадку для ненасильственного протеста».<sup>3</sup> Глава Коалиции Брюс Гэньон [Bruce Gagnon] изложил свою угрозу на понятном народу языке, противопоставив маленьких людей большому злодею – правительственному агентству. Джереми Ривкин [Jeremy Rivkin], президент «Фонда экономических тенденций» – другой группы, тоже протестовавшей против запуска, – внес свой вклад в попытку вбить клин между «народом» и «людьми из NASA». Он сказал в интервью ЮПИ: «Астронавты добровольно пошли на эту миссию. Но те народы мира, которые могут стать жертвой радиационного заражения, не давали на это своего согласия».<sup>4</sup>

Но не только манифестанты работали в тесном контакте с прессой. В NASA тоже умели с ней обращаться. Они вывели на сцену своих звезд – самих астронавтов. В конечном итоге, именно эти мужчины и женщины были пионерами, отважившимися на опасное предприятие в холодном и темном космическом пространстве в интересах всего человечества. Командир «Атлантика» Дональд Уильямс [Donald Williams] не стал резко высказываться о демонстрантах, но сказал с холодным презрением: «Всегда находятся люди, у которых есть что сказать по любому поводу, о чем бы ни шла речь. Но ведь носить плакат не так уж сложно. Гораздо труднее идти вперед и делать что-то стоя-

<sup>2</sup> При описании «Галилея» и обстоятельств старта в основном использованы сообщения информационных агентств, особенно репортажи журналиста ЮПИ Уильяма Харвуда.

<sup>3</sup> William Harwood, «NASA Awaits Court Ruling on Shuttle Launch Plans», UPI, 10 October 1989.

<sup>4</sup> William Harwood, «Atlantis 'Go' for Tuesday Launch», UPI, 16 October 1989.

щее».<sup>5</sup>

У NASA был еще один козырь в колоде героев. Второй пилот «Атлантика» Майкл Мак-Калли [Michael McCully] сказал по поводу использования окруженных свинцовой броней плутониевых радиоизотопных термоэлектрических генераторов: «Тут нечего обсуждать». Он был до такой степени уверен в их безопасности, что собирался пригласить близких на запуск челнока.

Возможно, астронавты были рискованными парнями и сумасшедшими, как утверждали протестующие, но не до такой же степени, чтобы подвергать собственные семьи опасности. Кроме того, сам вице-президент США Дэн Куэйл также намеревался наблюдать за стартом из центра управления примерно в семи километрах от стартовой площадки.

Хотя сотрудники NASA выглядели спокойными и владели ситуацией, меры безопасности были усилены. Около двухсот охранников наблюдали за местом запуска. NASA не хотело испытывать судьбу. Ученые слишком долго ждали этого момента. Старт «Галилея» не будет отменен из-за кучки пацифистов.

Запуск и так задержался почти на семь лет. Конгресс утвердил проект «Галилей» в 1977 году, по плану аппарат стоимостью 400 миллионов долларов должен был стартовать в 1982 году. Но с самого начала все пошло наперекосяк.

В 1979 году NASA перенесло запуск на 1984-й из-за проблем с конструкцией челноков. Новые планы предполагали «раздельный запуск» «Галилея», то есть вывод в космос носителя и собственно научной станции с помощью двух различных запусков челноков. К 1981 году из-за постоянного удорожания проекта NASA внесло в него серьезные изменения. Работы над трехступенчатым двигателем «Галилея» были свернуты в пользу другой системы, так что запуск снова был отложен, на этот раз до 1985 года. После того, как в 1981 году федеральный бюджет урезал ассигнования, NASA снова пришлось перенести дату старта на май 1986 года, чтобы спасти программу разработки ракеты-носителя «Галилея».

Самым предпочтительным вариантом казалась двухступенчатая твердотопливная система. Такой двигатель мог бы доставить «Галилей» на Марс или Венеру, но топливо закончилось бы задолго до того, как аппарат достиг бы Юпитера. Но тут Роджеру Дилу [Roger Diehl] из Лаборатории реактивного движения [p5] NASA пришла в голову блестящая идея: «Галилею» нужно сделать несколько витков вокруг двух соседних планет, что сообщит ему гравитационное ускорение, после чего он сможет отправиться к Юпитеру. Такая траектория откладывала прибытие космического аппарата к Юпитеру еще на три года, но все же он должен был попасть туда.

Активисты антиядерной кампании доказывали, что каждый виток «Галилея» вокруг Земли увеличивает риск ядерной катастрофы. Но, по мнению NASA, такова была цена успеха.

Незадолго до запуска проект «Галилей» столкнулся и с другими проблемами. В понедельник 9 октября NASA объявило, что неисправен компьютер, управляющий вторым основным двигателем челнока. Правда, неприятность касалась «Атлантика», а не «Галилея», но технические неполадки, а тем более проблемы с компьютерами, управляющими двигателями выглядели не слишком красиво на фоне судебной тяжбы с активистами антиядерного движения.

Инженеры NASA обсудили в телеконференции возникшую проблему. Ее устранение могло отложить запуск не на часы, а на дни. Поскольку требовалось определенное расположение планет, аппарат должен был стартовать не позднее 21 ноября. Если «Атлантика» не поднимется в космос к этому сроку, «Галилею» придется ждать следующей возможности девятнадцать месяцев. Первоначальный бюджет проекта в 400 миллионов долларов и так уже был превышен на целый миллиард. Еще полтора года задержки обошлись бы в 130 миллионов долларов и могли поставить под угрозу дальнейшее финансирование. Этот момент был для «Галилея» решающим – сейчас или никогда.

Несмотря на проливные дожди (на стартовой площадке выпало сто миллиметров осадков, а в соседнем городке Мельбурн и все сто пятьдесят), отсчет времени шел своим чередом, пока NASA не приняло очередное решение. Было решено перенести старт на пять дней (17 октября), чтобы получить возможность спокойно устранить компьютерную проблему.

Тем ученым и инженерам, которые участвовали в проекте с самого начала, в этот момент казалось, что судьба действительно настроена против запуска «Галилея». Словно по какой-то непости-

<sup>5</sup> Ibid.

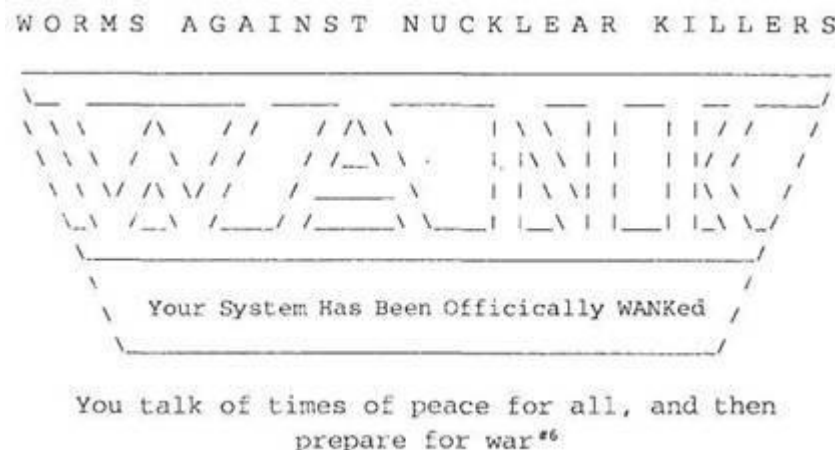
жимой причине все силы небесные и земные восстали против человечества, замахнувшегося на Юпитер. Как только NASA устраняло одну преграду, некая невидимая рука сию же минуту воздвигала другую.

## Понедельник, 16 октября 1989 года

*НАСА, Годдардовский центр космических полетов, Гринбелт, штат Мэриленд .*

В этот день сотрудники огромной империи NASA, простершейся от Мэриленда до Калифорнии и от Японии до Европы, как обычно, здоровались друг с другом, просматривали почту, наливали кофе и садились к компьютерам, чтобы решать очередные сложные научные проблемы. Но многие компьютерные системы повели себя чрезвычайно странно.

В тот момент, когда персонал вошел в систему, стало ясно, что кто-то (или что-то) их опередил. Вместо привычной официальной заставки системы они с ужасом обнаружили следующее сообщение, глядевшее на них с мониторов:



[p6]

Wanked? Большинство американских администраторов компьютерных систем, прочитавших этот баннер, никогда не слышали слова wank. [p7]

Кто мог решиться на вторжение в компьютерную систему NASA? Кто такие эти «черви», выступающие против «ядерных убийц»? Какая-то группировка полоумных маргиналов? Или NASA угрожают атакой террористы? И почему «черви»? Странный талисман для революционной группы, ведь черви находятся в самом низу биологической пирамиды. И говорится: «Аки червь во прахе». [p8] Кто мог выбрать червя символом власти?

С ядерными убийцами было еще непонятнее. «Твердишь о мире ты для всех, а сам готовишься к войне» – совершенно неподходящая NASA надпись. Агентство не занималось производством ядерных ракет, оно посылало людей на Луну. В некоторых проектах NASA присутствовала «военная составляющая», но все же агентство не занимало место в первых строчках списка «ядерных убийц», уступая другим правительственным институтам США, например, Министерству обороны. Так что вопрос оставался неясным – почему NASA?

А бессмысленное слово «WANKирована»? Что значит «ваша система WANKирована»?

Это значит, что NASA больше не контролирует свою компьютерную систему.

p6

«Черви против ядерных убийц.  
Ваша система официально WANKирована.  
Твердишь о мире ты для всех, а сам готовишься к войне»

(англ.).

Слово *officially* в оригинальном баннере написано с ошибкой.

p7

Wank (сленг, груб.) – заниматься мастурбацией (англ.).

p8

Автор, по всей видимости, имеет в виду библейскую фразу: «И они вместе будут лежать во прахе, и червь покрывает их» (Иов. 21:26).



Когда в этот понедельник один из ученых NASA вошел в зараженную систему, то получил следующее сообщение:

```
deleted file &lt;filename1>gt;  
deleted file &lt;filename2>gt;  
deleted file &lt;filename3>gt;  
deleted file &lt;filename4>gt;  
deleted file &lt;filename5>gt;  
deleted file &lt;filename6>gt;
```

Тем самым компьютер сказал: «Я уничтожаю все твои файлы». Командная строка выглядела так, словно пользователь сам ввел команду

```
delete/log *.*
```

и дал команду компьютеру уничтожить все файлы.

Научная сотрудница, сидевшая за терминалом, должно быть, просто остолбенела, наблюдая, как все ее файлы один за другим проходили по монитору дорогой смерти. Наверное, она попыталась остановить процесс, нажав «Ctrl+C». Эта операция должна была разорвать последовательность команд и приказать компьютеру прервать процесс, который он осуществлял в данный момент.

Но компьютером управлял чужак, а не сотрудник NASA. Он сказал компьютеру: «Эта команда ничего не значит. Не обращай внимания».

Сотрудница нажимала клавиши еще и еще раз. Она была совершенно сбита с толку и одновременно крайне расстроена непостижимым поведением компьютера. Она неделями, месяцами корпела над секретами мироздания. И вот результаты работы гибнут у нее на глазах в ненасытной утробе компьютера. Все выходит из-под ее контроля. Уходит. Уходит. Ушло.

Обычно люди не склонны спокойно относиться к потере контроля над своими компьютерами. Как правило, это будит в них худшие чувства: некоторые шепотом ругаются и сжимают кулаки, другие взывают о помощи, начальство властно ревет и стучит кулаком по столу.

Представьте, если сможете, что вы управляете одной из локальных компьютерных сетей NASA. В понедельник утром вы приходите в офис, и вам начинают беспрерывно звонить обезумевшие и растерянные работники NASA. Все они уверяют вас, что их файлы, учетные записи и исследовательские проекты – *все, что пропало из компьютерной системы*, – являются жизненно важными.

В данном конкретном случае проблема усугублялась тем, что научно-исследовательские центры NASA часто состязались друг с другом за получение заданий. Всякий раз, когда на горизонте появлялся какой-нибудь особенно важный космический проект, в борьбу за него вступали два-три центра, в каждом из которых работала не одна сотня служащих. Потеря контроля над компьютерами, потеря всех данных, планов и расчетов могла запросто привести к тому, что центр мог потерять проект и, соответственно, весьма значительное финансирование.

Этот день не предвещал ничего хорошего для парней в офисе компьютерной сети SPAN.

Этот день не сулил ничего хорошего и Джону Мак-Магону [John McMahon].

;)

Джон Мак-Магон работал консультантом по протоколу DECNET. В его обязанности входило управление всей компьютерной сетью SPAN, которая связывала между собой полтора-два десятка зданий Годдарда.

Мак-Магон работал на Проект 630.4, иначе известный под названием Goddard's Advanced Data Flow Technology Office, [\[p9\]](#) в строении № 28. Сотрудники Центра вызывали его, когда им требовалась помощь с компьютерами. Чаще всего ему приходилось слышать две жалобы: «Кажется, он не работает» и «Я не могу попасть отсюда в тот сектор сети».

SPAN – это Space Physics Analysis Network, [\[p10\]](#) соединявшая 100 000 компьютерных терминалов по всему миру. В отличие от Интернета, в настоящее время доступного любому, SPAN связы-

---

p9

Годдардовский центр передовых технологий обработки данных.

p10

Международная сеть исследователей физики космоса.

вала только ученых NASA, Министерства энергетики и исследовательских институтов, например университетских центров. Компьютеры SPAN также отличались от большинства компьютеров в сети Интернет важнейшей технической особенностью – они использовали другую операционную систему. Большие компьютеры в Интернете в основном работают в операционной системе Unix, тогда как SPAN состояла из компьютеров VAX, где применялась операционная система VMS. Эта сеть работала почти аналогично Интернету, но компьютеры говорили на другом языке. Интернет «общается» на языке протокола TCP/IP, SPAN же использует DECNET.

Сеть SPAN и была более широко известна как международная сеть DECNET. Большинство ее компьютеров производились Digital Equipment Corporation (DEC) в Массачусетсе – отсюда и название DECNET. Это были мощные компьютеры. К любому компьютеру DEC в сети SPAN можно было подключить сорок терминалов, а к некоторым из них даже больше. Для компьютера DEC не было ничего особенного в том, чтобы обслуживать четыре сотни человек. В общем, компьютерами этой сети пользовалось свыше четверти миллиона ученых, инженеров и других исследователей.

Инженер-электрик по образованию, Мак-Магон ранее работал в проекте NASA под названием Cosmic Background Explorer project (COBE),<sup>[p11]</sup> где он осуществлял управление компьютерами пятисот исследователей. В здании № 7 Годдардовского центра, где он работал на проект COBE, проводилась очень интересная работа. Исследователи пытались картографировать Вселенную, надеясь сделать это с помощью волн, невидимых человеческому глазу. NASA запустило спутник COBE в ноябре 1989 года. Его задача заключалась в том, чтобы «измерять рассеянное инфракрасное и микроволновое излучение, возникшее на заре вселенной, насколько позволяет наше астрономическое оборудование».<sup>6</sup> Для дилетанта проект выглядел произведением современного искусства, которое могло быть названо «Карта вселенной в инфракрасном свете».

Но 16 октября, едва Мак-Магон вошел в офис и приступил к работе, раздался странный телефонный звонок из офиса SPAN. Тодд Батлер [Todd Butler] и Рон Тенкати [Ron Tencati] из National Space Science Data Center,<sup>[p12]</sup> который управлял половиной сети SPAN, принадлежащей NASA, обнаружили в компьютерной сети нечто странное и явно несанкционированное. Это напоминало компьютерного червя.

Компьютерный червь отчасти напоминает компьютерный вирус. Он вторгается в компьютерные системы, создавая помехи их нормальной работе. Он путешествует по любой доступной и совместимой компьютерной сети и стучится в двери систем, связанных с этой сетью. Если в системе безопасности компьютера есть щель, червь обнаружит ее и вползет в систему. Сделав это, он может получить самые различные инструкции – от передачи сообщений всем пользователям компьютеров до овладения всей системой. Главное отличие червя от других компьютерных программ-вирусов заключается в том, что он способен воспроизводить сам себя. Он продвигается вперед, вторгается в новую систему и копирует себя на новом сайте. Другое отличие червя от вируса состоит в том, что он не замкнут рамками файла данных или программы. Он автономен.<sup>7</sup>

Термин «червь» в применении к компьютерам пришел из классического научно-фантастического романа Джона Бруннера «Всадник ударной волны», написанного в 1975 году. В нем идет речь о том, как программист-мятежник создал программу под названием «ленточный червь». Он запустил ее во всемогущую компьютерную сеть, при помощи которой олигархическое правительство управляло своим народом. Чтобы уничтожить червя, правительству пришлось отключить компьютерную сеть, что привело к потере контроля.

Книга Бруннера была так же далека от реального червя-разбойника, как и большинство администраторов компьютерных сетей VMS. До конца 80-х годов о червях были довольно смутные представления, и они преимущественно ассоциировались с исследованиями в компьютерных лабораториях. Например, несколько червей-помощников было разработано исследователями компании Хегох,

---

p11

Исследование космического фона.

<sup>6</sup> Цитируется сайт NASA.

p12

Национальный центр информации по космическим наукам.

<sup>7</sup> Thomas A. Longstaff and E. Eugene Schulz, «Analysis of the WANK and OILZ Worms», *Computer and Security*, vol. 12, no. 1, February 1993, p. 64.

которые хотели более эффективно использовать возможности компьютеров.<sup>8</sup> Они разработали «червя-глашатая», который передвигался по сети, рассылая важные сообщения. Их «червь-диагност» также постоянно находился в сети, выявляя возникающие неполадки.

Для некоторых компьютерных программистов создание червя равносильно созданию жизни. Сотворить нечто «разумное», способное выжить в мире и воспроизводить себе подобных, – это высшая степень созидания. Породить червя-разбойника, овладевшего компьютерной системой NASA, означало увенчать себя лаврами творческого бессмертия. Еще бы – наследить в компьютерах, которые отправили человека на Луну!

К тому моменту, когда баннер WANK появился на компьютерных экранах NASA, было известно всего два незаконных червя, сколько-нибудь достойных внимания. Один из них, червь RTM, поразил базирующийся на Unix Интернет менее чем за год до описываемых событий. Другой, известный как Father Christmas,<sup>[p13]</sup> стал первым червем в VMS.

Father Christmas был маленьким, простеньким червем, не особенно вредившим компьютерным сетям, по которым путешествовал. Он был запущен перед самым Рождеством 1988 года, незаметно пробрался в сотни машин VMS и затаился в них до праздника. Рождественским утром он встал пораньше и с большим усердием принялся за работу. Из зараженных червем компьютерных систем неукротимым потоком, подобно тому, как конфетти сыплются на голову с балкона, устремились рождественские поздравления, адресованные всем их пользователям. Ни один из тех, кто был подключен к сети в этот момент, не ушел без рождественской открытки. Сделав свое дело, червь испарился. Джон Мак-Магон входил в состав команды, сражавшейся с Father Christmas.

Спустя считанные дни после Рождества 1988 года около четырех пополудни мониторинговые программы Мак-Магона подали сигнал тревоги. Мак-Магон попытался проследить десятки входящих соединений, которые и вызывали тревожные сигналы. Он быстро обнаружил, что на другом конце линии не было человека. После дальнейших поисков он нашел в своей системе программу-чужака под названием HI.COM. По мере того, как из принтера выползали распечатки с кодом HI.COM, его глаза все больше расширялись. Мак-Магон понял, что это *червь*, а червя он никогда раньше не видел.

Ринувшись к пульту, Мак-Магон со всей возможной быстротой принялся выключать системы из сети. Может быть, он действовал не по инструкции, но решил, что люди скажут ему спасибо, когда осознают, от какой опасности он их уберег. Отключив свою часть сети, он сообщил об этом в местный офис сети, затем взял распечатку кода червя и отправился в головной офис, где в компании с несколькими другими программистами нашел способ к концу дня покончить с червем. Впоследствии они проследили Father Christmas до того места, где, по-видимому, он был создан и запущен – до Швейцарии. Никто так и не узнал, кто его написал.

Father Christmas был не только простым, но также и неопасным, потому что не старался удержаться в системе навсегда. Это был червь-однодневка.

О возможностях захватчика WANK проектный офис SPAN не знал ничего, в том числе, конечно, и того, кто его создал или запустил. Но имелась копия программы. Не мог бы Мак-Магон взглянуть на нее?

Джон Мак-Магон всегда готов был оказать любезность. Будучи любителем решать сложные загадки, он попросил, чтобы ему прислали копию червя из проектного офиса SPAN, которое очень быстро становилось кризисным центром по отражению нападения. Он принялся просматривать семистраничную распечатку исходного кода захватчика, пытаясь представить себе, на что он способен.

Два предыдущих червя-разбойника работали только в определенных компьютерных системах и сетях. В этом случае червь WANK также атаковал только компьютерные системы VMS. Но исходный код был совершенно не похож на то, что Мак-Магон когда-либо видел. По его словам, анализ напоминал исследование блюда спагетти: «Ты вытаскиваешь одну макаронину и думаешь: „Ага, вот что он делает“. Но потом видишь остальное месиво в тарелке».

Программа, написанная на цифровом командном языке, или DCL, не была аккуратно исполненной и логичной. В ней все было вверх ногами. Джон с трудом пробивался сквозь 10–15 строк компьютерного кода лишь для того, чтобы затем вернуться к началу и попытаться представить, что намерена предпринять следующая часть программы. Он постоянно делал записи, и вот уже медлен-

<sup>8</sup> Katie Heffner and John Markoff, *Cyberpunk*, Corgi, London 1994, p. 363.

но, но верно в его голове начало складываться представление о том, что способен сделать этот червь с компьютерной системой NASA.

:)

Это был важный день для активистов антиядерных групп, собравшихся у Космического центра имени Кеннеди. Хотя они и проиграли дело в окружном суде, но не собирались складывать оружие и обратились с жалобой в Апелляционный суд США.

Новость пришла 16 октября. Апелляционный суд встал на сторону NASA.

Манифестанты вновь были силой отогнаны от главных ворот Космического центра. Восемь, по меньшей мере, из них были арестованы. Газета *St Louis Post-Dispatch* распространила фотографию агентства Франс-Пресс, запечатлевшую, как полиция арестовывает восьмидесятилетнюю женщину за проникновение в запретную зону. Джейн Браун [Jane Brown] из флоридской «Коалиции за мир и справедливость» заявила: «Это только начало... правительственного плана по использованию ядерной энергии и оружия в космосе, в который входит и программа „звездных войн“».

В самом Центре имени Кеннеди дела тоже шли не так уж гладко. В последний понедельник перед стартом технические эксперты NASA обнаружили еще одну проблему. Черный ящик, записывающий данные о скорости и другие важные параметры работы навигационной системы космического челнока, оказался поврежден. Но техники заменили прибор, пресс-секретарь агентства успокоил журналистов, и в NASA решили не отменять запуск, назначенный на вторник. Обратный отсчет не был прерван. NASA все держало под контролем.

Кроме погоды.

Памятуя о катастрофе с «Челленджером», инструкции NASA о подготовке к запуску проявляли особенную строгость. Плохая погода могла все испортить, но прогнозы метеорологов были благоприятными. Шаттл должен был обязательно стартовать вовремя, потому что на следующий день обещали сильную облачность.

Во вторник утром охрана «Галилея» затаила дыхание. Отсчет времени запуска неумолимо приближался к 12 часам 57 минутам пополудни. Демонстранты, казалось, утихомирились. Все выглядело обнадеживающе. «Галилей» мог, наконец, стартовать.

За десять минут до старта сработали sireны систем безопасности. Кто-то прорвался на территорию стартовой площадки. Служба охраны мгновенно пришла в движение и быстро обнаружила нарушителя – дикую свинью.

Свинью благополучно удалили, и отсчет времени продолжил свой бег. Продолжили движение и дождевые облака, плавно двигаясь к запасной взлетно-посадочной полосе космического челнока, расположенной примерно в шести километрах от места старта. У «Атлантика» было в запасе 26 минут. После этого время запуска истечет, и его придется отложить, скорее всего, до среды. Похоже, погода не собиралась меняться.

В 13 часов 18 минут, когда до старта «Атлантика» оставалось пять минут, руководитель запуска Роберт Сик [Robert Sieck] перенес запуск на среду.

:)

В центре SPAN царил настоящая лихорадка. Червь внедрялся во все новые и новые системы, и телефоны теперь звонили каждые пять минут. Компьютеры NASA подвергались массовой атаке.

Людям, работавшим в проекте SPAN, не хватало рук. Им нужно было успокаивать звонивших и сосредоточиться на анализе программы-пришельца. Что это такое – розыгрыш или бомба замедленного действия, готовая взорваться? Кто стоит за всем этим?

NASA работало в информационном вакууме, когда червь пошел на приступ. Некоторые сотрудники знали об акции протеста, но никто не был готов к такому повороту событий. Официальные лица NASA были вполне уверены в том, что демонстрации против запуска «Галилея» и нападение на компьютеры агентства связаны между собой. Они были готовы заявить об этом публично. Это казалось достаточно вероятным, но множество вопросов требовали ответа.

Те, кто звонил в офис SPAN, были взволнованы и даже напуганы. Многие звонки поступали от системных администраторов SPAN в отдельных центрах NASA, таких как Маршалловский центр космических полетов. Некоторые из них были в панике, голос других звучал подавленно. Из-за таких вещей управляющий может запросто потерять работу.

Большинство тех, кто звонил в головной офис SPAN, хотели информации. Как этот червь пролез в их компьютеры? Было ли это сделано злонамеренно? Что будет с научными данными? Что нужно делать, чтобы уничтожить червя?

NASA хранило большое количество ценной информации в компьютерах SPAN. Эти сведения не предполагалось засекречивать, но они были чрезвычайно важны. На их сбор и анализ ушли миллионы человеко-часов. Поэтому кризисная команда, сформированная в офисе SPAN в NASA, была крайне встревожена, когда начали поступать сообщения о невероятной по размаху гибели баз данных. Люди звонили, чтобы сказать, что червь стирает файлы.

Для любого компьютерного администратора это было самое ужасное, и все выглядело так, будто наихудшие опасения кризисной команды оказались реальностью.

Кроме всего прочего, червь вел себя непоследовательно. Некоторые компьютеры всего лишь получали анонимные послания, иногда забавные, иногда причудливые, иногда грубые и непристойные. Как только пользователь входил в систему, на мониторе могла появиться надпись:

Помни, даже выиграв крысиные бега, ты все равно остаешься крысой.

Некоторые послания отличались плоским юмором:

Нет ничего быстрее скорости света...

Чтобы убедиться в этом, попробуй открыть дверцу холодильника, прежде чем включится свет.

Другие пользователи столкнулись с протестом параноика против властей:

ФБР следит за ТОБОЙ.

Или:

Голосуйте за анархистов.

Но червь не собирался стирать файлы в этих компьютерах. Возможно, этот трюк с якобы случайным выбором стираемых файлов был лишь предвестником грядущих действий – этаким легким намеком на то, что может произойти, например, в полночь. Возможно, случайный удар по клавише ни о чем не подозревающего пользователя только что зараженной системы мог запустить что-то в самом черве и спровоцировать необратимую цепь команд, которые сотрут все, что только есть в этой системе.

Компьютерная группа SPAN соревновалась с червем в скорости. Каждую минуту, пока они пытались понять, что он сделал, захватчик продвигался все глубже в компьютерную сеть NASA. Каждый час, потраченный NASA в поисках противоядия, червь искал слабые места, взламывал и захватывал компьютерные системы, вытворяя в них бог знает что. Команде SPAN нужно было полностью проанализировать эту штуку и сделать это очень быстро.

Некоторые администраторы компьютерных сетей испытали страшное потрясение. В офис SPAN поступил звонок из Лаборатории реактивного движения (ЛРД) в Калифорнии. Это важный центр NASA, в котором работает 6500 служащих, тесно связанный с Калифорнийским технологическим институтом (Калтех).

Лаборатория реактивного движения отключилась от сети.

Этот червь был слишком опасен. Единственным возможным решением была изоляция компьютеров. К тому времени как кризис окажется под контролем, от коммуникаций, связывающих SPAN (и базирующихся на DEC) и остальные части NASA, не останется ничего. Ситуация становилась все сложнее: «достать» программу-терминатор, не имея доступа к сайту ЛРД и другим сайтам, отключившимся от SPAN, было гораздо более сложной задачей. Все приходилось делать по телефону.

К несчастью, ЛРД была одним из пяти распределительных центров сети SPAN. Лаборатория походила на центр колеса, от которого отходила дюжина спиц, каждая из которых вела к другим сайтам SPAN. Все эти периферийные сайты нуждались в сайте лаборатории для соединения со SPAN. Когда ЛРД отключилась от сети, зависимые сайты сделали то же самое.

Это стало серьезной проблемой для людей из офиса SPAN в Виргинии. Для Рона Тенкати, главы службы безопасности SPAN, отключение распределительного центра было наилучшим выходом.

Но его руки были связаны. Офис SPAN выполнял функции центральной власти в обширной зоне сети, но он не мог диктовать свою волю периферийным центрам, каждому из которых приходилось самостоятельно принимать решение. Команда SPAN могла только помочь советом и постараться поскорей найти способ покончить с червем.

Джону Мак-Магону снова позвонили из офиса SPAN, на этот раз с более серьезной просьбой. Не мог бы он прийти и помочь им справиться с кризисом?

Центр SPAN был всего в восьмистах метрах от офиса Мак-Магона. Его босс, Джером Беннетт [Jerome Bennett], менеджер протокола DECNET, согласился одолжить им Мак-Магона до тех пор, пока кризис не будет разрешен.

Когда Мак-Магон прибыл в строение № 26, где размещался офис, управлявший относящимся к NASA сектором SPAN, то вошел в штаб кризисной команды NASA наравне с Тоддом Батлером, Ронном Тенкати и Пэтом Сиссоном [Pat Sisson]. Другие ведущие программисты NASA, такие как Дэйв Питерс [Dave Peters] и Дэйв Стерн [Dave Stern], подключались к работе кризисной группы по мере надобности. Джим Грин [Jim Green], глава National Space Science Data Center и главный босс SPAN, требовал ежечасных докладов о развитии ситуации. Сначала в команду входили только сотрудники NASA, в основном из Годдарда, однако с течением времени к команде присоединялись новые люди из других государственных агентств.

Червь распространился и за пределы сети NASA.

Он напал на всемирную сеть HEPNET (High Energy Physics Network[[p14](#)]) Министерства энергетики США. Эта сеть наряду с Euro-HEPNET и Euro-SPAN входила в состав всемирной сети SPAN. Компьютерные сети NASA и Министерства энергетики пересекались во многих местах. Например, исследовательские лаборатории могли иметь доступ и в компьютеры HEPNET, и в компьютеры NASA. Для своего удобства лаборатория могла просто соединить обе сети. Все это способствовало размножению червя, поскольку SPAN NASA и HEPNET Министерства энергетики фактически представляли собой единую гигантскую компьютерную сеть, которую червь мог полностью захватить.

Министерство энергетики хранит в своих компьютерах секретную информацию. Там работают в двух направлениях: над проектами использования энергии в гражданских целях и над атомным оружием. Поэтому Министерство энергетики очень серьезно относится к вопросам безопасности, поскольку это – «национальная безопасность». Хотя секретная информация не должна была передаваться по сети HEPNET, Министерство энергетики по-военному четко отреагировало, когда его компьютерщики обнаружили чужака. Они тут же связались с парнем по имени Кевин Оберман [Kevin Oberman], который знал все о компьютерной безопасности систем VMS, и поставили перед ним задачу.

Как и Мак-Магон, Оберман официально занимался отнюдь не проблемой компьютерной безопасности, просто он интересовался ей и был известен своей компетентностью в вопросах защиты систем VMS. Вообще же он работал сетевым администратором в техническом отделе финансируемой Министерством энергетики Ливерморской национальной лаборатории,[\[p15\]](#) расположенной неподалеку от Сан-Франциско.

Ливерморская лаборатория занималась в основном военными исследованиями, в значительной степени связанными с проектом Стратегической оборонной инициативы. Многие ученые лаборатории разрабатывали ядерное и лазерное оружие для программы «звездных войн».<sup>9</sup> У Министерства энергетики была своя команда безопасности, известная как Computer Incident Advisory Capability (CIAC).[\[p16\]](#) Но ее эксперты больше разбирались в Unix, нежели в компьютерных системах и сетях, базирующихся на VMS. «В течение многих лет они почти не сталкивались с проблемами в VMS, – сделал вывод Кевин Оберман, – и этот вопрос их совершенно не заботил. Поэтому у них и не оказалось спецов по VMS».

Червь подорвал безмятежное доверие к компьютерам VMS. Еще когда WANK путешествовал

p14

Сеть по физике высоких энергий.

p15

Lawrence Livermore National Laboratory (LLNL).

<sup>9</sup> *The Age*, 22 april 1996, reprinted from *The New York Times*,

p16

Консультативная служба по компьютерным инцидентам.

по сетям NASA, он энергично атаковал Национальную лабораторию ускорителей имени Ферми в окрестностях Чикаго, объявившись во множестве компьютерных систем, что очень встревожило сотрудников этой лаборатории. Они позвонили в Ливерморскую лабораторию, и оттуда рано утром 16 октября связались по телефону с Оберманом, попросив его проанализировать код червя. Они хотели знать, насколько опасен незванный гость. Но еще больше их интересовало, что можно ему противопоставить.

Сотрудники Министерства энергетики установили, что первый контакт с червем состоялся 14 октября. Более того, они предположили, что червь был запущен днем раньше – в пятницу 13 октября. Эта зловещая дата, по мнению Обермана, как нельзя более соответствовала черному юмору создателя или создателей червя.

Оберман начал собственный анализ червя, не подозревая о том, что на расстоянии 3200 километров от него, на противоположном побережье материка, его коллега и знакомый Джон Мак-Магон делает то же самое.

;) )

Всякий раз, как Мак-Магон отвечал на телефонный звонок сердитого системного или сетевого администратора NASA, он старался получить копию червя из зараженной машины. Он также просил предоставить ему логи [\[p17\]](#) их компьютерных систем. Из какого компьютера явился червь? В какую систему он готовит вторжение из зараженного сайта? Теоретически лог-файлы позволяли команде NASA проследить маршрут червя. Если команда сможет связаться с администраторами на предполагаемом пути червя, те будут предупреждены о грозящей опасности. Можно также обнаружить тех, чьи системы были недавно заражены, и оповестить их о том, что они стали стартовой площадкой для нападений червя.

Но это не всегда было возможно. Если червь захватил компьютер и все еще находился в нем, администратор мог проследить, откуда он пришел, но оставалось тайной, куда он направится. Кроме того, многие менеджеры не сохраняли полные лог-файлы в своих компьютерах.

Мак-Магон всегда знал, что очень важно собирать как можно больше информации о том, кто подключался к компьютеру. На предыдущей работе он модифицировал машины таким образом, что они сохраняли максимум информации, представляющей полезность с точки зрения безопасности соединения с другими компьютерами.

Компьютеры VMS имели стандартные наборы сигнальных программ, но Мак-Магон не считал, что их достаточно. Эти системы лишь отправляли администратору сообщение следующего содержания: «Привет! К вам только что подключились отсюда-то». Модифицированная система оповещения говорила: «Привет! К вам только что подключились из такого-то пункта. Вызванный абонент перекачивает файл». Также она сообщала и другие фрагменты информации, которую Мак-Магон мог выжать из другого компьютера. К сожалению, многие компьютерные и сетевые администраторы NASA не разделяли его энтузиазма по поводу проверок логов. Они просто не сохраняли подробные записи о том, кто и когда имел доступ к их машинам, и это очень затруднило преследование червя.

Но офис SPAN постарался тщательно фиксировать данные о компьютерах NASA, ставших жертвой червя. Каждый раз, когда сотрудник NASA докладывал об очередном вторжении, один из членов команды записывал все детали *ручкой на бумаге*. Список, включающий адреса пострадавших компьютеров и детальные описания особенностей их заражения, был и в компьютере, но записи, сделанные вручную, казались более надежными. Червь наверняка не ест бумагу.

Когда Мак-Магон узнал, что Министерство энергетики тоже подверглось нападению, он стал связываться с ними приблизительно каждые три часа. Обе группы обменялись списками зараженных компьютеров по телефону, потому что голос, как и слово, написанное от руки, был застрахован от посягательств червя. «Это, конечно, архаичный способ, но, с другой стороны, мы не хотели зависеть от системы и того, что в ней творилось, – рассказывал Мак-Магон. – Нам был необходим способ общения помимо связи через зараженную систему».

Некоторые члены команды компьютерщиков NASA устанавливали контакты с различными подразделениями DEC с помощью общества пользователей продуктами компании (DECUS). Эти

контакты оказались очень полезными. Любой запрос мог запросто потеряться в бюрократической системе DEC. В компании работало 125 000 человек, ее обороты исчислялись миллиардами долларов, а прибыль в 1989 году составила двенадцать миллиардов долларов.<sup>10</sup> Такой крупной и солидной корпорации вовсе не улыбалось иметь дело с проблемами вроде червя WANK, особенно в такой находящейся на виду организации, как NASA. Так или иначе, вопрос о степени вины программного обеспечения DEC в победном шествии червя наверняка бы встал. Кризис был, мягко говоря, нежелателен для компании и не украсил бы ее репутацию. Если бы DEC полезла в эту кашу, это могло обернуться для нее большим ущербом.

Ситуация менялась, если у кого-нибудь были приятельские отношения с техническим экспертом DEC. Они могли поговорить по-дружески, не так, как обычно разговаривали менеджеры NASA с сотрудниками DEC, которые полгода назад продали агентству компьютеров на миллион долларов, а как парень из NASA с парнем из DEC, сидевшие рядом на конференции в прошлом месяце. Как коллеги, общавшиеся не один раз.

Анализ Джона Мак-Магона показал, что существуют три версии червя WANK. Эти версии, выделенные из собранных в сети образчиков, были очень схожи, но небольшие отличия все-таки были. По мнению Мак-Магона, эти различия не объяснялись особенностями самовоспроизведения червя на новых сайтах по мере распространения. Но зачем создателю червя понадобилось запускать разные версии? Почему он не написал одну, но чище? Червь не был одиночной ракетой, наносилс массивированный удар со всех направлений, по всей компьютерной сети NASA.

Мак-Магон предположил, что автор червя запустил три разные версии своего произведения с небольшими временными интервалами. Возможно, создатель запустил червя, а потом обнаружил ошибку. Он немного поработал с червем, чтобы устранить проблему, и запустил его снова. Может быть, ему не понравилось, как он исправил ошибку, и он еще раз изменил его и запустил теперь уже в третий раз.

В Северной Калифорнии Кевин Оберман пришел к другому заключению. Он считал, что существует лишь одна настоящая версия червя, который вгрызлся в HEPNET и SPAN. Небольшие вариации в разных копиях, которые он проанализировал, казалось, обуславливались способностями червя к обучению и видоизменению по мере того, как он продвигался от компьютера к компьютеру.

Мак-Магон и Оберман были не единственными сыщиками, пытавшимися разобраться с разными вариантами червя. DEC тоже занялась изучением червя, имея на это веские причины. Выяснилось, что червь WANK пробрался в самую корпорацию и ползает по ее собственной компьютерной сети Easynet, соединяющей заводы, торговые и другие подразделения DEC по всему миру. Компания проявляла осторожность при обсуждении проблемы вне собственных стен, но версия червя в Easynet имела явные отличия. В ее коде присутствовала странная строка, которой не было в других версиях. Ни при каких обстоятельствах червь не должен был вторгаться в компьютеры в зоне 48 сети DEC. Команда NASA задумалась над этим обстоятельством, кто-то проверил, что такое зона 48. Это оказалась Новая Зеландия. Новая Зеландия?

Команда NASA принялась ломать головы. Нападение становилось все более странным. Когда уже казалось, что члены группы SPAN вышли на верный путь к центру лабиринта, они вновь оказывались перед новой загадкой. Вдруг кто-то вспомнил, что заявкой Новой Зеландии на всемирную славу было объявление ее безъядерной зоной.

В 1986 году Новая Зеландия заявила, что отказывается допускать в свои гавани американские суда с ядерным оружием на борту или имеющие ядерные силовые установки. США ответили формальной приостановкой своих обязательств по обеспечению безопасности южно-тихоокеанских государств. Если бы какая-нибудь враждебная страна решила напасть на Новую Зеландию, Штаты со спокойной душой закрыли бы на это глаза. Кроме того, американцы отказались от практики обмена разведывательной информацией и от проведения совместных военных маневров.

Многие в Австралии и Новой Зеландии считали, что Америка отреагировала слишком остро. Новая Зеландия не изгоняла американцев, она просто отказалась подвергать свое население опасностям, связанным с ядерным оружием. И в самом деле, новозеландцы по-прежнему не возражали против существования американской разведывательной базы в Вайхопаи даже после введения США санкций. В стране царили не антиамериканские, а антиядерные настроения.

И у Новой Зеландии были очень серьезные причины для таких настроений. В течение многих лет эта страна боролась с Францией, проводившей испытания ядерного оружия в Тихом океане. В

<sup>10</sup> DEC, Annual Report, 1989, listed in «SEC Online».



июле 1985 года французские агенты в гавани Окленда взорвали корабль Rainbow Warrior [p18] организации «Гринпис», который с протестующими защитниками природы должен был отправиться к полигону на атолле Муруроа. При этом погиб активист «Гринписа» Фернандо Перейра.

Несколько недель Франция все отрицала. Когда же правда вышла наружу (оказалось, что сам президент Миттеран был в курсе планов спецслужб), французы не знали, куда деваться от стыда. Полетели головы. Министр обороны Франции Шарль Эрню [Charles Hernu] был вынужден подать в отставку, адмирал Пьер Лакост [Pierre Lacoste], глава французского бюро разведки и тайных операций, был уволен. Франция принесла свои извинения и заплатила тринадцать миллионов новозеландских долларов компенсации в обмен на выдачу Новой Зеландией двух диверсантов, каждый из которых был приговорен в Окленде к десяти годам тюрьмы.

В сделку входило обещание Франции подвергнуть этих агентов трехлетнему заключению на военной базе Франции на атолле Хао. Оба агента были освобождены в мае 1988 года, отбыв менее двух лет. По возвращении во Францию один из них, капитан Доминик Приёр [Dominique Prieur], был произведен в майоры.

Наконец-то, подумал Мак-Магон, хоть что-то осмысленное. Исключение Новой Зеландии подкрепило политическое послание червя.

;) )

Червь WANK вторгся в компьютерную систему с инструкциями копировать себя и рассылать копии в другие машины. Он проскользнул в компьютерную сеть, найдя лазейку в компьютере, подключенном к сети. В действительности он стремился завладеть привилегированными компьютерными учетными записями, но пока ему пришлось довольствоваться только учетными записями пользователей самого низкого уровня.

В системах VMS есть учетные записи с различными уровнями привилегий. Владелец учетной записи высокого уровня может, к примеру, прочитать электронную почту другого пользователя или стереть файлы из его директории. Он также может самостоятельно создавать новые учетные записи в системе или сделать активными заблокированные учетные записи. Владелец привилегированной учетной записи способен менять пароли других пользователей. Тем, кто управляет компьютерными системами и сетями, нужна учетная запись с самым высоким уровнем допуска, чтобы без помех работать в системе. Червь особенно стремился отыскать такие учетные записи, потому что его создатель знал, что именно там – источник власти.

Червь был толков и обучался в процессе передвижения. По мере перемещения по сети он создавал список обычно используемых названий учетных записей. Сначала он старался скопировать список компьютерных пользователей той системы, до которой еще не добрался. Ему не всегда это удавалось, но зачастую система безопасности оказывалась достаточно слаба и червь добивался успеха. Затем он сравнивал этот список со списком пользователей в нынешнем месте обитания. Когда он находил пару (учетную запись, общую для обоих списков), то добавлял эту запись к основному списку, который переносил с собой из системы в систему, и помечал, что эту учетную запись можно будет применить при вторжении в новую систему.

Это был ловкий метод атаки, так как создатель червя знал, что некоторые учетные записи с высоким уровнем допуска вполне могли иметь стандартные названия, общие для разных машин. Учетные записи с такими названиями, как SYSTEM, DECNET или FIELD, и стандартными паролями, вроде DECNET или SYSTEM, зачастую записывались в компьютеры еще до того, как производитель отгружал их покупателю. Если администратор, получивший компьютер, не менял запрограммированные учетную запись и пароль, его машина имела серьезную дыру в системе безопасности, которая так и ждала, пока ею кто-нибудь не воспользуется.

Автор червя мог угадать некоторые названия учетных записей, использованных производителем, но не всех. Наделив червя способностью к обучению, он дал ему мощнейшее оружие. По мере распространения червь становился все умнее и умнее. Он размножался, и его потомство эволюционировало, все успешнее вторгаясь в новые системы.

Когда Мак-Магон вскрыл одного из потомков червя, он пришел в ужас от того, что он обнаружил. Изучив его внутренности, программист обнаружил обширную коллекцию групповых учетных

записей с высоким допуском, собранную со всей сети SPAN. На деле червь не только собирал стандартные привилегированные учетные записи VMS, но также уделял внимание учетным записям, обычным для NASA, но вовсе не обязательным для других компьютеров VMS. Например, многие сайты NASA работали с почтовой программой по протоколу TCP/IP, который нуждался в учетной записи POSTMASTER или MAILER. Джон обнаружил эти названия в потомке червя.

Даже если червью удавалось захватить только учетную запись непривилегированного уровня, он использовал ее, как инкубатор. Червь копировался, а затем атаковал другие компьютеры в сети. Когда Мак-Магон и остальные члены команды продолжили разбор кода червя, чтобы понять, что может сделать чудовище, если доберется до учетной записи с самым высоким уровнем допуска, они обнаружили новое доказательство черного чувства юмора хакера, скрывающегося за червем. Одна из его подпрограмм называлась *find fucked*.[\[p19\]](#)

Команда SPAN постаралась дать сотрудникам NASA максимум сведений о черве. Это был лучший способ помочь компьютерным администраторам, изолированным в своих офисах по всей стране, обрести чувство, что кризис остается управляемым.

Как и все в команде SPAN, Мак-Магон старался успокоить звонивших, после чего подвергал их опросу, с помощью которого рассчитывал определить степень контроля червя над их системами. Сначала он спрашивал, какие симптомы обнаруживали их системы. В кризисной ситуации, когда молоток занесен, все кажется гвоздем, поэтому Мак-Магон хотел убедиться, что сбой в системе действительно спровоцирован червем и ничем иным.

Если бы проблема заключалась только в странных комментариях, появляющихся на экране, Мак-Магон сделал бы вывод, что червь, возможно, лишь пугает пользователя этого компьютера из соседней системы, которую он уже успешно захватил. Послания наводили на мысль, что учетные записи принимающих их машин еще не захвачены червем. Во всяком случае, пока.

Машины VAX/VMS обладают функцией, называемой Phone, использующейся для онлайн-связи. Например, ученый NASA может «позвонить» одному из своих коллег на другой компьютер и по-дружески побеседовать с ним в режиме реального времени. Это живое общение, но происходит оно посредством клавиатуры и монитора, а не голоса. Функция Phone в VMS позволила червью отправлять послания пользователям. Он просто «звонил» им, используя этот протокол. Но вместо начала сеанса связи он посылал им сообщения из той своей части, которая, как выяснилось впоследствии, носила вполне подходящее название *Fortune Cookie*[\[p20\]](#) и представляла собой собрание приблизительно шестидесяти запрограммированных высказываний.

В некоторых случаях, когда червь сильно досаждал персоналу, Мак-Магон советовал менеджеру на другом конце провода отключить в компьютере функцию Phone. Некоторые менеджеры жаловались, и тогда Мак-Магон ставил перед ними ультиматум: Phone или спокойствие. Почти все предпочли спокойствие.

Когда Мак-Магон закончил предварительный анализ червя, у него появились хорошие и плохие новости. Хорошей новостью был тот факт, что, вопреки тому, что червь сообщал пользователям из NASA, он вовсе не стирал их файлы, а только делал вид, что стирает их. Просто шутка. Во всяком случае, для создателя червя. А для ученых NASA – головная и сердечная боль. А порой и сердечный приступ.

Плохая новость заключалась в том, что когда червь сможет получить контроль над учетной записью пользователя с высоким уровнем доступа, он поможет кому-то – предположительно, своему создателю – совершить гораздо более серьезное вторжение в NASA. Червь нашел учетную запись FIELD, созданную производителем, и если ее отключить, он постарается вновь активировать ее и установить пароль FIELD. Червь был также запрограммирован на изменение пароля стандартной учетной записи DECNET случайным набором из по меньшей мере двенадцати символов. Короче говоря, червь старался вломиться в систему с черного хода.

Информацию о тех учетных записях, которые он успешно взломал, червь посылал назад, в электронный почтовый ящик – учетная запись GEMPAK на узле 6.59 SPAN. Предположительно, хакер, создавший червя, должен был проверять его почтовый ящик, чтобы получить информацию, ко-

---

p19

Найди трахнутого (англ.).

p20

«Печенье-гаданье», в котором запечена записка с предсказанием (подается в китайских ресторанах). В компьютерной среде так называют сообщения, выводимые на экран в процессе загрузки.

торуую он мог бы использовать позже для проникновения в учетную запись NASA. Стоит ли удивляться, что почтовые ящики, к немалому удивлению их законных владельцев, были тайком «позаимствованы» хакером.

Компьютерный хакер создавал массу дополнительных проблем. Хотя червь был способен взламывать новые учетные записи с гораздо большей скоростью и размахом, чем одинокий хакер, он был более предсказуем. Как только команды SPAN и Министерства энергетики разобрали червя на составляющие, они совершенно четко представили, что от него можно ожидать. А вот действия хакера было совершенно невозможно прогнозировать.

Мак-Магон понял, что уничтожение червя не сможет решить проблему. Всем системным администраторам сетей NASA и Министерства энергетики придется поменять пароли учетных записей, захваченных червем. Им придется также проверить каждую систему, подвергшуюся нападению, чтобы убедиться, что червь не оставил в ней лазеек для хакера. Администраторам нужно найти и запереть на замки все черные ходы – адский труд.

Но больше всего команду SPAN напугало то, что червь свирепствовал в системе NASA, используя примитивнейшую стратегию атаки: имя пользователя равняется паролю. Он получил контроль над компьютерами NASA, просто вводя пароль, идентичный названию учетной записи пользователя.

Команда SPAN не могла поверить в это, но факты – упрямая вещь.

Тодд Батлер ответил на звонок с одного из сайтов NASA. Новости были удручающие. Он повесил трубку.

– Этот узел только что подвергся нападению, – сказал он остальным.

– И насколько все плохо? – спросил Мак-Магон.

– Привилегированная.

– Черт!

Мак-Магон бросился к одному из терминалов, набрал SET HOST, получив доступ к удаленному компьютеру сайта NASA. Готово.

«Ваша система официально WANKирована».

Мак-Магон повернулся к Батлеру.

– В какую учетную запись он проник?

– Они думают, что это SYSTEM.

Специалисты ничем не могли помочь. Глупость ситуации напоминала черную комедию.

Сайт NASA имел пароль SYSTEM для учетной записи высшего допуска SYSTEM. Это было просто невероятно. NASA, возможно, самое большое в мире сообщество специалистов, обладало такой расхлябанной системой компьютерной безопасности, что любой мало-мальски разбирающийся в компьютерах тинейджер мог без труда ее вскрыть. Этот колосс был сокрушен компьютерной программой, похожей на тарелку спагетти.

Первое, что может узнать любой системный администратор из инструкции по компьютерной безопасности № 101, – никогда не использовать пароль, идентичный имени пользователя. Достаточно скверно, что наивные пользователи могли угодить в эту западню... но не администраторы же компьютерных систем с учетными записями высокого уровня допуска!

Каковы были намерения хакера? Возможно, не такими уж злодейскими. Если бы он захотел, он мог бы запрограммировать WANK на уничтожение всех файлов NASA. Он мог бы снести их в один момент.

На деле червь оказался гораздо менее заразен, чем хотелось его автору. WANK получил инструкции на выполнение нескольких задач, которым он не повиновался. Важные составляющие червя попросту не работали. Мак-Магон пришел к выводу, что это случайная неудача. Например, его анализ показал, что червь был запрограммирован взламывать учетные записи в тех случаях, когда пользователь оставил место пароля пустым. Когда он разобрался в черве, то обнаружил, что эта часть программы не работала должным образом.

Несмотря ни на что, «неполноценный» червь устроил серьезный переполох в недрах нескольких правительственных агентств США. Мысль о том, что мог бы сделать из такого червя крутой программист на DCL с многолетним опытом работы с компьютерами VMS, всерьез волновала Джона. Такой человек мог бы нанести непоправимый ущерб. А что если червь WANK был только пробным шаром для чего-то более серьезного, что должно прийти по его следу? Такая перспектива пугала.

Невзирая на то обстоятельство, что червь WANK вроде бы не питал особенно злобных намерений, команду SPAN ожидали трудные времена. Анализ Мак-Магона обнаружил намного более тревожные аспекты программы червя. Если ему удалось захватить учетную запись SYSTEM, он может заблокировать все электронные почтовые сообщения для системных администраторов. Офис SPAN не мог посылать электронные предупреждения или инструкции по поводу того, что делать с червем, в те системы, которыми тот уже овладел. Проблема усугублялась недостатком информации о том, какие системы были подключены к SPAN. Помочь в борьбе с этой заразой мог телефонный звонок, но зачастую главный офис SPAN не знал, кому звонить. Команда SPAN могла лишь надеяться, что те администраторы, у которых номер телефона штаб-квартиры сети был приколот рядом с компьютером, догадаются позвонить по нему, когда их машины подвергнутся нападению.

Предварительный доклад Мак-Магона подчеркнул, что червь и сам по себе был способен нанести огромный ущерб. Но масштабы ущерба, причиненного по вине администраторов их собственным системам в борьбе с червем, были несравнимо выше.

Один обезумевший компьютерный администратор, позвонивший в офис SPAN, отказался принять на веру слова Джона о том, что червь лишь делает вид, что стирает данные. Он заявил, что червь не только вторгся в его систему, но и уничтожил ее. «Он просто не поверил, когда мы сказали ему, что червь, в общем, представляет собой сборник острот, – рассказывал Джон Мак-Магон. – Он реинициализировал систему». «Реинициализировал», то есть начал с чистого листа. Все данные персонала NASA исчезли, словно стертые зараженным компьютером. Сотрудник агентства просто сделал то, на что червь лишь претендовал.

Печальная ирония заключалась в том, что команда NASA так и не получила копии данных от системы администратора. Они даже не могли подтвердить, что его машина вообще была заражена.

Весь остаток дня Мак-Магон метался между беспрерывно звонящими телефонами и анализом червя. Он передал по сети зашифрованное электронное послание о нападении червя, и Кевин Оберман прочел его. Послание должно было быть тщательно продуманным, так как никто не был уверен в том, что создатель червя WANK не притаился где-то в сети, наблюдая и выжидая. Через некоторое время Мак-Магон и Оберман связались по телефону, чтобы обменяться идеями и сверить выводы.

Ситуация была обескураживающей. Даже если бы Мак-Магону и Оберману удалось создать работающую программу для уничтожения червя, команда NASA столкнулась бы с другой сложнейшей задачей. Ввести охотника на червя во все сайты NASA на проверку оказалось гораздо более сложным делом, чем можно было предположить, поскольку агентство не имело точной и свежей карты сети SPAN. Мак-Магон вспоминал, что почти сразу после нападения червя один менеджер попытался составить карту системы. Его усилия вызвали такой всплеск сообщений о тревоге, что его отвели в сторонку и попросили больше этого не делать.

В результате, когда кто-то из членов команды звонил администраторам в поисках новых деталей, информация часто оказывалась устаревшей.

– Нет, он раньше работал здесь, но ушел год назад.

– У нас нет списка телефонов людей, которым можно позвонить, если что-то разладится в компьютерах. У нас тут куча народу в разных местах следит за компьютерами.

Такие слова Джону приходилось слышать довольно часто.

Сеть росла беспорядочно, представляя собой своего рода сборную солянку. Почти никакого центрального управления. Гораздо хуже был тот факт, что масса компьютеров по всей Америке подключались к SPAN, не ставя в известность головной офис в Годдарде. В специальный кризисный центр звонили люди из компьютерных узлов, у которых даже не было названия. Они исповедовали философию «безопасность через скрытность» (так это называли в кругах, профессионально занимавшихся компьютерной безопасностью). Им казалось, что если никто не будет знать о существовании их компьютерной системы, у нее не будет названия и она не будет внесена в список или карту сети SPAN, они будут застрахованы от хакеров и других компьютерных врагов.

Мак-Магон получил множество звонков от системных менеджеров, говоривших: «Здесь творится что-то странное в компьютерной системе». Джон прежде всего спрашивал: «Где это „здесь“?» Само собой, если в офисе SPAN не знали о существовании этой системы, было гораздо труднее оказать помощь ее администраторам, дать им совет, как справиться самостоятельно, снабдить противоядием, когда оно будет готово, или помочь им залатать бреши в учетных записях, которые червь передал своему создателю.

Путаница была невероятная. Время от времени Мак-Магон садился и начинал думать о том, кто мог создать этого червя, который выглядел так, словно его запустили раньше, чем закончили. Его автор (или авторы) производил впечатление человека, богатого плодотворными идеями о том, как

решать проблемы, но не доводящего дело до ума. Червь содержал программу совершенствования стратегии штурма, но она не была завершена. Код червя не имел удовлетворительной процедуры отслеживания ошибок, чтобы обеспечить его выживание в течение длительного времени. Кроме того, червь не отправлял адреса успешно взломанных учетных записей в свой почтовый ящик вместе с их паролями и именами. Какой толк в пароле и названии учетной записи, если неизвестно, какая компьютерная система их использует?

С другой стороны, возможно, что создатель червя сделал это умышленно. Например, чтобы показать всему миру, в какое количество компьютеров может успешно проникнуть его червь.

Его программа, отсылавшая собранные данные, сделала это. А если бы она содержала адреса зараженных сайтов, это облегчило бы работу администраторов. Они смогли бы использовать коллекцию GEMPAK как список подлежащих дезинфекции сайтов. Впрочем, предположения можно было строить до бесконечности.

Местами программа червя была просто блестящей, некоторые решения впечатляли, поскольку никогда не приходили в голову Мак-Магону с тех пор, как он стал интересоваться способами взлома компьютеров VMS. Это была серьезная творческая работа, но в ней отсутствовала какая-либо логика. После нападения червя некоторые эксперты по компьютерной безопасности решили, что он написан не одним человеком. Но Мак-Магон отстаивал свою точку зрения, по-прежнему считая, что это работа одного-единственного хакера.

Было похоже на то, что создатель червя начинал развивать какую-то мысль, а затем отвлекался. Внезапно он просто переставал писать код, необходимый для того, чтобы закончить мысль, и направлялся по другой тропинке, снова не дойдя до конца. У его создания была шизофреническая структура. Все было не на своем месте.

Мак-Магон подумал, не было ли это сделано намеренно, чтобы замаскировать то, на что способен червь. Возможно, подумал он, изначально код был упорядочен, последователен и все в нем имело смысл. Затем автор порубил его на куски, переместил середину в начало, начало в конец, перемешал остатки и связал их с набором команд передачи управления. Вполне вероятно, что хакер, написавший червя, был очень элегантным DCL-программистом, который решил сделать червя хаотичным, чтобы защитить его. Безопасность через скрытность.

Оберман придерживался другого мнения. Он считал, что стиль программирования так варьируется в разных частях червя, потому что это продукт деятельности многих людей. Он знал, что когда программисты пишут код, они не делают так много мелких отклонений от стиля без особых на то причин.

Кевин Оберман и Джон Мак-Магон перебрасывались идеями и продолжали собственные исследования червя. Оберман привлек к процессу перекрестной проверки Марка Калетку [Mark Kaletka], который управлял внутренними сетями в Лаборатории имени Ферми, одном из самых больших сайтов NEPNET. У червя было много уязвимых мест, но требовалось как можно скорее найти одно, которое могло быть использовано для его уничтожения с минимальными потерями для осажденных компьютеров. Как только машина VMS начинает процесс, она присваивает ему уникальное имя. Когда червь проползал на компьютерный сайт, он первым делом убеждался, что там нет его собственной копии. Он делал это, сличая названия процессов со своими, которые все именовались NETW\_ плюс случайный набор из четырех цифр. Если червь-пришелец обнаруживал такое имя, он соображал, что другая его копия уже роется в компьютере, и самоуничтожался.

Похоже, оставалось сделать ловушку – написать программу, которая сможет выдавать себя за червя, а затем установить ее на всех уязвимых компьютерах NASA. Первая анти-WANK программа работала именно так. Притаившись в компьютерах SPAN, она притворялась процессом NETW\_ и тем самым уничтожала любую настоящую версию червя WANK, которая могла пробраться внутрь.

Оберман первым закончил анти-WANK программу и поделился ею с Мак-Магоном. Она отлично работала, но Мак-Магон заметил одно серьезное упущение. Программа Обермана делала проверку на предмет наличия процессов с именем NETW\_, но при этом предполагала, что червь действует в группе SYSTEM. В большинстве случаев так и было, но не всегда. Если червь находился в другой группе, программа Обермана становилась бесполезной. Когда Мак-Магон указал на ошибку, Оберман подумал: «Боже, как я мог *такое* пропустить?»

Мак-Магон работал над своей версией анти-WANK программы на базе программы Обермана, готовясь запустить ее в NASA.

В то же время Оберман пересмотрел свой вариант программы для Министерства энергетики. К

вечеру понедельника (по восточному стандартному времени [\[p21\]](#)) Оберман был готов разослать исправленную копию вакцины, созданную для защиты еще не зараженных компьютеров, и приложил к ней электронную инструкцию о том, как действовать против червя. Его первая электронная инструкция, распространенная CIAC, в частности, гласила:

**КОНСУЛЬТАТИВНАЯ СЛУЖБА ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ (CIAC)  
ПРЕДУПРЕЖДЕНИЕ**

Червь W.COM Worm, поражающий системы VAX VMS

16 октября 1989, 18:38 PST [\[p22\]](#) Номер A-2

Этого червя трудно уничтожить, и он может причинить большие разрушения. С того момента, как он уведомляет (по почте) о каждом из успешных захватов и оставляет лазейку (учетная запись FIELD), его недостаточно просто убить. Вам нужно войти в систему и убедиться, что все учетные записи имеют пароли, и эти пароли отличны от названий учетных записей.

Р. Кевин Оберман

**Предупреждение**

Червь атакует принадлежащую NASA сеть SPAN через системы VAX/VMS, подключенные к DECnet. Не совсем понятно, ограничено ли распространение червя. Он может внедриться в другие системы, такие как HEPINET Министерства энергетики, в течение нескольких дней. Системные менеджеры VMS должны быть готовы к этому.

Червь поражает машины VMS и может распространяться только посредством DECnet. Для воспроизведения самого себя червь использует два свойства машин DECnet/VMS. Во-первых, это учетная запись DECnet по умолчанию, которая дает возможность пользователям, не имеющим специальных идентификационных логинов для машин, добиться некоторого уровня анонимного доступа. Червь использует учетную запись DECnet по умолчанию для самокопирования в машине, а затем использует функцию «TASK O» DECnet для запуска удаленной копии. Он имеет несколько других функций, включая жесткую силовую атаку.

Как только червь проникает в вашу систему, он заражает файлы .COM и создает новые уязвимые места в системе безопасности. Есть мнение, что он попытается переслать информацию об этих слабостях. Он может также разрушить файлы, преднамеренно или непреднамеренно.

Анализ червя, представленный ниже, проведен Кевином Оберманом из Национальной лаборатории имени Лоренса Ливермора. К анализу приложена программа DCL, которая блокирует текущую версию червя. В настоящее время существуют не менее двух версий червя, но могут появиться и другие. Эта программа предоставит вам достаточно времени, чтобы залатать очевидные дыры в системе безопасности. Создается более совершенная программа DCL.

Если ваш сайт подвергнется нападению, пожалуйста, обратитесь в CIAC для получения дальнейших инструкций...

**Сообщение о черве W.COM**

Р. Кевин Оберман

Технический отдел

Национальная лаборатория имени Лоренса Ливермора

16 октября 1989 года.

Приводим описание работы червя W.COM, основанное на исследовании двух первых версий. Техника репликации предполагает небольшое изменение кода, на что указывает источник нападения и накапливаемая в результате самообучения червя информация.

---

p21

Минус пять часов от Гринвича.

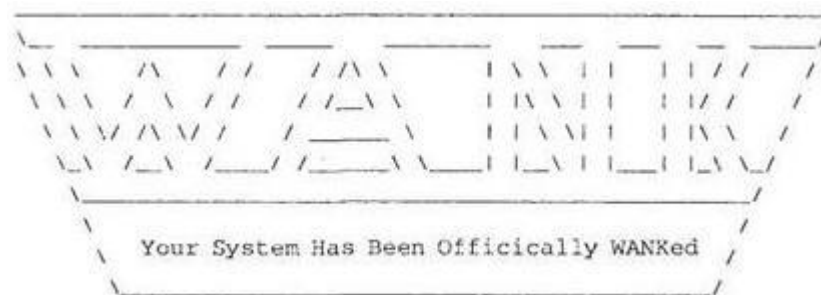
p22

Стандартное тихоокеанское время, минус восемь часов от Гринвича.

Весь анализ был сделан в большой спешке, но я считаю, что все факты достоверны. Для начала – описание программы:

1. Программа удостоверяет, что работает в директории, к которой сам владелец имеет полный доступ (с правами чтения, записи, исполнения и удаления файлов).
2. Программа проверяет, не работает ли уже другая копия червя, для чего она ищет процесс с первыми пятью знаками NETW\_. В случае его обнаружения она самоуничтожается и прекращает работу. (ПРИМЕЧАНИЕ: Быструю проверку на зараженность можно провести, поискав процесс, начинающийся с NETW\_. Это можно сделать с помощью команды SHOW PROCESS.
3. Затем программа изменяет пароль по умолчанию учетной записи DECnet случайной последовательностью двенадцати или более знаков.
4. Информация о пароле, использованном для доступа в систему, отправляется пользователю GEMTOP<sup>11</sup> на узле SPAN 6.59. Некоторые версии могут иметь другие адреса.
5. Процесс меняет свое имя на NETW\_ плюс случайно выбранный набор цифр.
6. Затем программа смотрит, имеет ли SYSNAM привилегию. Если да, то она замещает сообщение системы своим баннером.

### WORMS AGAINST NUCKLEAR KILLERS



You talk of times of peace for all, and then prepare for war

7. Если она имеет SYSPRV, то блокирует почту учетной записи SYSTEM.
8. Если она имеет SYSPRV, то изменяет процедуру выполнения команд при входе в систему так, как если бы стирались все файлы пользователя (но в действительности не делает этого).
9. Затем программа сканирует логическую таблицу учетных записей для командных процедур и стремится изменить учетную запись FIELD на известный пароль с логином из любого источника и всеми привилегиями. Это примитивный вирус, но он очень эффективен, если проникает в высокопривилегированную учетную запись.
10. Программа приступает к попытке проникновения в другую систему путем случайного выбора номеров узлов. Кроме того, она использует функцию PHONE для получения списка активных пользователей удаленных систем. Она начинает беспокоить их, звоня им с помощью PHONE.
11. Затем программа стремится получить доступ к файлу RIGHTLIST и пытается получить доступ к какой-либо удаленной системе с помощью найденных пользователей и списка «стандартных» пользователей, заложенного в червя. Она ищет пароли, идентичные названиям учетных записей или просто пустые, и регистрирует все такие учетные записи.
12. Она ищет учетную запись, которая имеет доступ к SYSUAF.DAT.
13. Если привилегированная учетная запись обнаружена, программа копируется в эту учетную запись и запускается. Если привилегированная учетная запись не найдена, программа копируется в другие учетные записи, выбранные случайным образом.
14. Как только программа завершает работу в системе, она случайным образом выбирает другую, и все повторяется (и так до бесконечности).

<sup>11</sup> GEMTOP был исправлен CIAC на GEMPAK в более позднем предупреждении.

Ответные меры:

1. Прилагаемая программа заблокирует червя. Воспользуйтесь приведенным ниже кодом и запустите ее (это потребует минимальных ресурсов). Она создаст процесс под названием NETW\_BLOCK, который предупредит запуск червя.

ПРИМЕЧАНИЕ: Настоящая версия программы будет работать только с этой версией червя.

Видоизмененные черви потребуют модификации этого кода, тем не менее эта программа будет защищать от вторжения червя достаточно долго, чтобы обезопасить вашу систему от новых нападений червя.<sup>12</sup>

Программа Мак-Магона тоже была готова к запуску в понедельник, но он столкнулся с барьерами, существующими в NASA. Работа в агентстве требовала умения балансировать, представляя своего рода балет, требующий совершенной хореографии, чтобы выполнять свою работу, соблюдать формальные требования и не наступать на мозоль тому или иному начальнику. Поэтому анти-WANK-программа NASA была выпущена только несколько дней спустя.

В Министерстве энергетики тоже не обошлось без проблем с запуском анти-WANK-программы и консультациями в HEPNET. 17 октября в 17 часов 04 минуты по тихоокеанскому времени, когда Оберман был готов закончить последний параграф своего окончательного сообщения о черве, пол у него под ногами вздрогнул. Здание затряслось. Кевин Оберман оказался в центре сан-францисского землетрясения 1989 года.

Землетрясение в Лома-Приета силой в 7,1 балла по шкале Рихтера прокатилось по Сан-Франциско и окрестностям. В своей компьютерной лаборатории Оберман приготовился к худшему. Как только толчки закончились и он убедился, что компьютерный центр все еще стоит, он снова сел к терминалу. Под вопли динамиков внутренней радиосети, призывающих весь персонал немедленно покинуть здание, Оберман в спешке заканчивал последнее предложение доклада. Он на секунду задумался, а затем добавил постскрипtum, в котором шла речь о том, что если абзац не слишком связан, так только потому, что его мысли смешались из-за толчков землетрясения, обрушившегося на Ливерморскую лабораторию. Он нажал клавишу, отправляя окончательный вариант сообщения о черве WANK, и выбежал из здания.

На восточном побережье в офисе SPAN продолжалась работа по оказанию помощи тем, кто звонил с пораженных сайтов NASA. Список сайтов, сообщавших о нападении червя, неуклонно рос всю неделю. Официальные оценки масштабов атаки червя WANK были неопределенными, однако профессиональные издания, такие как *Network World* и *Computer World*, сообщали, что червь успешно проник всего лишь в 60 VMS-компьютеров космического агентства. Менеджер по безопасности SPAN Рон Тенкати насчитал в той части сети, которая относилась к NASA, только 20 успешных вторжений, но другая внутренняя оценка гораздо выше – 250–300 машин. Каждая из этих машин могла обслуживать 100 и более пользователей. Оценки сильно отличаются, в сущности же, от червя пострадали все 270 000 учетных записей в сети: либо из-за отключения части сети, либо из-за постоянных попыток червя войти в систему с уже зараженного сайта. К концу нападения червя офис SPAN составил список пораженных сайтов, который даже в две колонки занял площадь в несколько страниц дисплея. Каждый из них так или иначе пострадал от червя.

---

<sup>12</sup> Это предупреждение опубликовано с разрешения CIAC и Кевина Обермана. CIAC настояла на публикации следующего заявления:

«Этот документ был подготовлен в результате работы агентства Правительства Соединенных Штатов. Ни Правительство США, ни университет Калифорнии, ни один из служащих этих институтов не несет никаких гарантий, специальных или предполагаемых, и не принимает на себя никаких законных обязательств и никакой ответственности за точность, полноту или пригодность любой информации, приборов, продукта или описания процесса, и не гарантирует, что их использование не станет нарушением закона о частной собственности. Имеющиеся ссылки на любые специальные коммерческие продукты, процессы или услуги, обозначенные торговым именем, торговой маркой, названием производителя или как-либо иначе, не обязательно являются или требуют их подтверждения, рекомендации или предпочтения Правительством Соединенных Штатов или университета Калифорнии. Точка зрения и мнение авторов не обязательно являются или выражают точку зрения или мнение Правительства Соединенных Штатов или университета Калифорнии, и не могут быть использованы в целях рекламы или поддержки какой-либо продукции».



Также к концу кризиса группа менеджеров компьютерной сети NASA и Министерства энергетики определилась с тем, какие требуются «вакцины», «противоядия» и «анализы крови». Мак-Магон выпустил свою программу ANTIWANK.COM, которая убивала червя и делала системе «прививку» против возможных атак в будущем, а также распространил WORM-INFO.TEXT, содержащий список признаков заражения червем. Программа Обермана, названная [SECURITY]CHECK\_SYSTEM.COM, латала все прорехи в системах безопасности, которые использовал червь для проникновения в компьютерную систему. У DEC также появилась возможность заделать дыру в системе безопасности учетной записи DECNET.

Каково бы ни было реальное число зараженных машин, несомненно, что червь совершил кругосветное путешествие. Из компьютеров Годдардовского центра в Мэриленде и Лаборатории имени Ферми в Чикаго он добрался до европейских сайтов (например, до сайта ЦЕРНа – Европейского совета по ядерным исследованиям в Швейцарии) и перелетел Тихий океан, оказавшись в Японии (в Riken Accelerator Facility).<sup>13</sup>

Официальные лица NASA заявили прессе, что, по их мнению, червь был запущен около 4.30 утра в понедельник 16 октября.<sup>14</sup> А также то, что червь пришел из Европы, возможно из Франции.

### **Среда, 18 октября 1989 года**

#### *Космический центр имени Кеннеди, Флорида*

Пять членов экипажа «Атлантиса» получили в среду утром не слишком приятные известия. Метеорологи с сорокапроцентной вероятностью предсказывали дождливую и облачную погоду в районе стартовой площадки. А затем произошло землетрясение в Калифорнии.

Космический центр имени Кеннеди был не единственным местом, от чьей безукоризненной работы зависел успех запуска. Таковые были во множестве и за пределами Флориды. Среди них была база ВВС Эдвардс (Калифорния), где челнок должен был совершить посадку в понедельник. Были и другие места, в основном военные базы, необходимые как для слежения за шаттлом, так и для другой технической поддержки экспедиции. Одним из них была станция слежения на базе ВВС Онизука в Саннивэйл, Калифорния. Толчки, встряхнувшие район залива, повредили станцию, и чиновники NASA, ответственные за принятие решений, решили встретиться в среду утром для оценки ситуации в Саннивэйл. Несмотря на все это, агентство сохраняло спокойствие и невозмутимость. Вопреки техническим проблемам, судебному преследованию, демонстрантам, капризам погоды, стихийным бедствиям и червю WANK, NASA по-прежнему контролировало ситуацию.

«Там нанесен некоторый ущерб, но мы не знаем, насколько он серьезен. Тем не менее я считаю, что в целом все неплохо, – заявил пресс-атташе NASA агентству ЮПИ. – Но все же проблемы есть». <sup>15</sup> В Вашингтоне пресс-секретарь Пентагона тоже успокаивал общественность. «Они смогут осуществлять слежение за челноком и поддерживать полет... Они сделают свое дело». <sup>16</sup>

«Атлантис», готовый к старту, томился в ожидании на пусковой площадке 39В. Техники заправили челнок ракетным топливом, поскольку казалось, что погодные условия могут позволить ему стартовать. Была переменная облачность, но по правилам Центра Кеннеди запуск все же мог состояться.

Астронавты проследовали на борт челнока.

Но если во Флориде погода была приемлемой, то на месте аварийной посадки в Африке возникли проблемы. Не одно, так другое. NASA объявило о четырехминутной отсрочке.

Наконец, в 12.54 «Атлантис» оторвался от своей стартовой площадки. Поднявшись над космодромом, он выпустил двойные языки пламени из своих огромных твердотопливных ракетных двигателей, поднялся над атмосферой и вышел в космическое пространство.

В 19.15, ровно через 6 ч 21 мин после старта, «Галилей» начал свое самостоятельное путешествие в космосе. В 20.15 его стартовый двигатель пришел в движение.

---

<sup>13</sup> Michael Alexander and Maryfran Johnson, «Worm Eats Holes in NASA's Decnet», *Computer World*, 23 October 1989, p. 4.

<sup>14</sup> Ibid.

<sup>15</sup> William Harwood, «Shuttle Launch Rained Out», UPI, 17 October 1989.

<sup>16</sup> Vincent Del Guidice, «Atlantis Set for Another Launch Try», UPI, 18 October 1989.

В центре управления полетом пресс-атташе NASA Брайан Уэлч [Brian Welch] объявил: «Космический аппарат „Галилей“... развил вторую космическую скорость».<sup>17</sup>

### Понедельник, 30 октября 1989 года

*НАСА, Годдардовский центр космических полетов, Гринбелт, штат Мэриленд*

Неделя, начавшаяся 16 октября, показалась невероятно долгой членам команды SPAN. Они работали по двенадцать часов в день и постоянно контактировали с людьми, находившимися на грани истерики. Все же им удалось создать анти-WANK-программы, несмотря на устаревшие данные о SPAN и недостаток нормальных лог-файлов, которые позволили бы проследить, откуда пришел червь. «За эту неделю мы поняли, сколь многими данными *не* располагаем», – заметил Мак-Магон.

К пятнице, 20 октября, не поступило ни одного нового сообщения о нападениях червя. Все говорило о том, что кризис миновал. Привести дела в порядок могли и без него, так что Мак-Магон вернулся к своей непосредственной работе.

Прошла неделя. Все это время Мак-Магона не покидало беспокойство. Он подозревал, что тот, кто ввязался во всю эту историю с червем, не позволит так быстро уничтожить свое создание. Стратегия ловушки сохраняла эффективность только до тех пор, пока червь сохранял неизменным имя процесса и был запрограммирован не активироваться в уже зараженных системах. Стоило изменить имя процесса или разучить червя самоуничтожаться, и команда SPAN столкнулась бы с новой, еще более серьезной проблемой. У Джона Мак-Магона было предчувствие, что червь в любой момент может вернуться.

Он как в воду глядел.

В следующий понедельник Мак-Магону позвонили из офиса проекта SPAN. Закончив разговор, он заглянул в кабинет своего начальника. Джером Беннетт вопросительно посмотрел на него из-за своего стола.

«Он вернулся, – сказал ему Мак-Магон, и не было нужды объяснять, о ком идет речь. – Я иду в офис SPAN».

Рон Тенкати и Тодд Батлер уже приготовили для Мак-Магона новую копию червя WANK. Эта версия оказалась гораздо опаснее. Она копировала себя намного эффективнее и, следовательно, продвигалась по сети несравненно быстрее. Скорость проникновения обновленного червя была в четыре с лишним раза выше, чем у первоначальной версии WANK. Снова затрезвонили телефоны. Джон принял звонок одного разъяренного администратора, который обрушил на него целую тираду: «Я запустил вашу анти-WANK-программу, в точности выполнил все инструкции, и посмотрите, что случилось!»

Червь изменил имя процесса. Он также получил новое указание – преследовать программу-приманку и уничтожать ее. Теперь сеть SPAN могла быть втянута в настоящую кровавую битву. Этот червь уничтожал не только приманку, но и любую другую копию червя WANK. Даже если бы Мак-Магон изменил имя процесса для своей программы, эта стратегия все равно бы не сработала.

В новой версии червя были и другие усовершенствования. Ранее было известно, что он меняет пароль любой учетной записи, в которую проникает. Уже это было проблемой, но теперь червь менял лишь те пароли, которые предназначались для учетных записей с высоким уровнем доступа. Новый червь был способен не пускать администраторов в их собственные системы.

Обнаружив, что он не может использовать свою учетную запись, администратор мог попытаться одолжить учетную запись обычного пользователя, назовем его Эдвин. К сожалению, учетная запись Эдвина могла иметь более низкий уровень допуска. Даже в опытных руках возможности учетной записи Эдвина оказывались слишком ограничены для того, чтобы уничтожить червя в его новообретенном высоком статусе администратора. Компьютерщик мог убить бог знает сколько времени, меряясь силами с червем с невыгодной позиции учетной записи обычного пользователя. В какой-то момент ему не оставалось ничего, кроме вынужденного решения отключить всю компьютерную систему.

Администратор был вынужден произвести перезагрузку машины. Освободить ее для новой загрузки (с восстановлением исходного состояния), затем запустить ее вновь в минимальной конфигурации. Снова прервать запуск. Зафиксировать пароль, который изменил червь. Выйти из системы. Восстановить некоторые настройки. Снова перезагрузить машину. Закрыть любую возможную щель

<sup>17</sup> William Harwood, «Astronauts Fire Galileo on Flight to Jupiter», UPI, 18 October 1989.

в системе безопасности, которую червь мог оставить после себя. Изменить все пароли, соответствующие именам пользователей. Холостой запуск большой VMS машины требует времени, в течение которого астрономы, физики и инженеры этого офиса NASA не смогут работать за своими терминалами.

По крайней мере, на этот раз команда SPAN была более подготовлена к встрече с червем. Ее члены были психологически готовы к возможному повторению нападения. Контактная информация по администраторам сети была обновлена. Все сообщество DECNET получило предупреждение о черве с просьбой оказать посильную помощь.

Она пришла из Франции, страны, к которой, кажется, проявлял особенный интерес автор червя. Системный администратор из Института ядерной физики в Орсе Бернар Перро [Bernard Perrot] получил копию червя, внимательно изучил ее и подметил слабую способность червя контролировать ошибки. Это была его настоящая ахиллесова пята.

Червь был натаскан на базу данных RIGHTLIST, представляющую собой список всех, кто имеет учетные записи в этом компьютере. Что если кто-нибудь переименует и переместит базу данных и поставит на ее место фикцию? Теоретически червь должен последовать за куклой, в которую будет встроена скрытая бомба. Когда червь обнаружит приманку и проглотит ее, она взорвется и он издохнет. Если это произойдет, команде SPAN не придется зависеть от самоубийств червя, как это было во время первого вторжения. Они получают удовлетворение от «собственноручного» уничтожения этого создания.

Рон Тенкати получил копию программы-убийцы французского администратора и передал ее Мак-Магону, который устроил нечто вроде лабораторного мини-эксперимента. Он рассек червя на части и извлек из него необходимые биты, что позволило ему испытать французскую программу почти без риска, что червь сбежит и примется бушевать в системе. Программа работала чудесно. Что ж, вперед! Вторая версия червя была гораздо опаснее, и ее удаление из SPAN заняло куда больше времени, чем в первый раз – почти две недели.

По оценке Мак-Магона червь нанес ущерб примерно в полмиллиона долларов. В основном он состоял в том, что людям приходилось тратить время и средства в погоне за червем, вместо выполнения обычной работы. Это, на его взгляд, была кража. «Впустую потрачены человеческие ресурсы и время, – говорил он, – и произошло это не случайно. Кто-то намеренно заварил эту кашу. В общем, я поддерживаю уголовное преследование тех, кто считает, что взламывать машины забавно. Эти люди, по-моему, не понимают, какие последствия могут иметь их забавы. Они думают, что если вломиться в машину и ничего не тронуть, то ничего страшного не произойдет. Это не так. Вы тратите чужое время. Людям приходится тащиться в офис в неурочный час. Они вынуждены писать информационные сообщения. Масса криков и воплей. За это надо отвечать перед законом. Таково побочное действие чьей-то веселой прогулки по чужой системе, даже если он не причинил вреда. Кто-то должен за это платить».

Мак-Магон так никогда и не узнал, кто создал червя WANK. Он также не понял, что автор хотел сказать этой демонстрацией. Мотивы создателя остались неясны, и даже если в них и был политический смысл, он не вызывал уважения.

Сойдя со сцены, червь WANK оставил массу вопросов, массу запутанных концов, которые все еще пытался распутать Джон Мак-Магон. Может быть, хакер, создавший червя, был против запуска NASA космического аппарата «Галилей» на плутониевом топливе? Что означало совершенно неамериканское слово WANK, – что автор не американец? Почему автор возродил червя и запустил его снова? Почему ни одна политическая или какая-либо иная группа не взяла на себя ответственность за червя WANK?

Одна из загадок заключалась во второй версии червя. Его создатель изменил исходное имя процесса NETW\_, по-видимому, для того, чтобы помешать выполнению анти-WANK-программы. Мак-Магон решил, что исходное имя означало NETWANK – логичная догадка, принимая во внимание намерения хакера. Но новое имя процесса поставило в тупик каждого члена в команде SPAN: оно, по-видимому, не означало ничего. Набор букв вряд ли мог составлять инициалы чьего-либо имени. Никто не признал в этом акроним поговорки или аббревиатуру названия организации. И уж, конечно, такого слова не существовало в английском языке. Осталось совершенно непонятно, почему создатель червя WANK, хакер, устроивший вторжение в сотни компьютеров NASA и Министерства энергетики, мог выбрать такое непонятное слово?

Это слово было OILZ.

## Паб на углу

*Твердишь о мире ты для всех,  
А сам готовишься к войне.*

Песня «Blossom of Blood», альбом «Species Deceases»<sup>[p23]</sup> группы Midnight Oil<sup>18</sup>

Неудивительно, что команда безопасности SPAN попала пальцем в небо. Нет также ничего странного в том, что должностные лица тогда произнесли название версии червя WANK как oil zee.<sup>[p24]</sup> Также неудивительно их предположение о том, что создатель червя выбрал слово OILZ, поскольку изменения, внесенные им в последнюю версию, сделали червя скользким, как бы маслянистым.

Видимо, только австралиец мог заметить связь червя с текстами группы Midnight Oil.

Это был первый в мире червь, несший политическое послание, и второй червь, оставивший заметный след в истории мировых компьютерных сетей. Он дал импульс для создания FIRST (Forum of Incident Response and Security Teams)<sup>[p25]</sup>. FIRST стал первым международным союзом безопасности, который позволил правительствам, университетам и коммерческим организациям делиться информацией об инцидентах в компьютерных сетях.<sup>19</sup> Однако NASA и американское Министерство энергетики ни на шаг не приблизились к поимке создателя червя WANK. Пока следователи распутывали электронные следы, ведущие во Францию, выяснилось, что взломщик прятался за своим компьютером и модемом в Австралии.

Австралия далеко. В головах американцев эта страна вызывала скорее образы пушистых сумчатых зверушек, нежели компьютерных хакеров. Перед американскими сотрудниками компьютерной безопасности в NASA и Министерстве энергетики вставляли и другие препятствия. Сами они функционировали в конкретном мире условленных и состоявшихся встреч, подлинных имен, визитных карточек и официальных должностей. Компьютерное подполье – это тайный мир, населенный персонажами, которые появляются из тени и прячутся в ней же. Здесь не используют настоящие имена и не сообщают о себе никаких сведений.

У компьютерного подполья нет никакого места в пространстве. Это эфемерный, нематериальный, запутанный лабиринт извилистых улочек, которых нет ни на одном плане. Здесь лишь случайно можно заметить силуэт такого же, как ты сам, путешественника.

Когда Рон Тенкати, отвечавший в NASA за безопасность SPAN, понял, что компьютеры NASA подверглись нападению, он позвонил в Федеральное бюро расследований. Подразделение по борьбе с компьютерными преступлениями ФБР поставило перед ним массу вопросов. Сколько компьютеров было атаковано? Где они находятся? Кто стоит за нападением? ФБР велело Тенкати «держаться в курсе ситуации». Оказалось, что ФБР (как и команда CIAC в Министерстве энергетики) не очень разбирается в VMS, основной операционной системе, используемой в SPAN.

Но ФБР знало достаточно, чтобы понять, какую потенциальную опасность представляла атака червя. Запутанный электронный след смутно указывал на иностранную компьютерную систему, и вскоре в дело была вовлечена Секретная служба США. Затем в бой вступила французская контрразведка Direction de la Surveillance de Territoire (DST).<sup>[p26]</sup>

p23

«Цветение Крови», «Смерть Видов» (англ.).

<sup>18</sup> Слова и музыка: Rob Hirst, James Moginie. © Copyright 1985 Sprint Music. Administered for the World-Warner/Chappell Music Australia Pty Ltd. Used by permission.

p24

«Масло Z». Zee («зи») – американское название буквы Z.

p25

Форум реагирования на инциденты и групп безопасности.

<sup>19</sup> FIRST первоначально назывался CERT System. Это был международный вариант Команды быстрого компьютерного реагирования (Computer Emergency Response Team), созданной Министерством обороны США на базе университета Карнеги-Меллона.

p26

Управление охраны территории.

DST и ФБР начали сотрудничать в этом расследовании. Сторонний наблюдатель задним числом мог заметить различие мотивов, которыми руководствовались два правительственных агентства. ФБР хотело поймать злоумышленника. DST – доказать, что самое уважаемое космическое агентство подверглось коварному нападению червя WANK не из Франции.

В лучших традициях правительственных служб плаща и кинжала люди из ФБР и DST установили между собой два канала связи: официальный и неофициальный. Первый включал в себя посольства, атташе, официальные коммюнике и нескончаемые проволочки в получении ответов на простейшие вопросы. Неофициальный канал требовал небольшого числа телефонных звонков и нескольких быстрых ответов.

У Рона Тенкати был коллега по имени Крис в сети SPAN во Франции. Французская сеть была самой большой сетью SPAN в Европе. Крис занимался не только научными компьютерными сетями, у него были и некоторые контакты в правительстве Франции и какое-то отношение к правительственным компьютерным сетям. В общем, когда ФБР в ходе расследования потребовалась некая техническая информация – тот сорт информации, который мог быть не пропущен посольскими бюрократами, – один из федеральных агентов позвонил Рону Тенкати: «Рон, спроси у своего приятеля об этом».

И Рон спросил. Крис получил необходимую информацию и перезвонил Тенкати: «Рон, вот ответ. Теперь DST нужно узнать вот *это*». И Рон в свой черед разыскивал сведения, запрашиваемые DST.

Расследование так и продвигалось благодаря взаимопомощи, оказываемой по неофициальным каналам. Но американские сыщики по каким-то причинам все больше склонялись к тому, что плацдарм нападения на NASA следует искать именно во французских компьютерах. Конечно, червь мог лишь пройти через машину во Франции, но, тем не менее, французский компьютер стал источником для заражения NASA.

Французам не нравился такой вывод. Совсем не нравился. Немыслимо, чтобы червь пришел из Франции. *Ce n'est pas vrai.* [p27] В ответ французы уверяли, что червь появился из США. Иначе зачем бы он программировал пересылку информации о взломанных им учетных записях на другой конец мира именно в американскую машину GEMPAK? Конечно, автор червя – американец! Так что это не наша проблема, сказали французы американцам. Это *ваша* проблема.

Все эксперты по компьютерной безопасности знают, что создание максимально запутанного пути между хакером и объектом нападения является обычной практикой в хакерской среде.

Это очень затрудняет таким службам, как ФБР, отслеживание взломщика. Поэтому очень сложно судить о национальности хакера по месту, откуда о нем появилась первая информация. Хакер, конечно же, знает, что после запуска червя власти в первую очередь проверят именно это место.

Тенкати нашел французский след в лог-файлах некоторых компьютеров NASA, подвергшихся нападению ранним утром понедельника 16 октября. Эти логи были очень важны своей относительной ясностью. Поскольку червь размножался весь этот день, он взламывал компьютеры по всей сети, все больше расширяя сферу своих атак. К 11 утра было невозможно определить, где начиналась одна атака и заканчивалась другая.

Некоторое время спустя после первой атаки DST уведомило, что несколько его агентов вылетают в столицу США по другим делам, но хотели бы также встретиться с агентами ФБР. Представитель генерального инспектора NASA присутствовал на этой встрече вместе с одним из членов команды безопасности SPAN.

Тенкати был уверен в своей способности доказать, что нападение червя WANK на NASA началось из Франции. Но он также знал, что ему придется подтвердить все документально, убедительно ответить на любые вопросы и контраргументы, выдвинутые агентами французских спецслужб на встрече с ФБР. Когда он разрабатывал хронологическую шкалу нападений, то обнаружил, что машина GEMPAK зафиксировала сетевое соединение по протоколу X.25 через другую систему из компьютера, находящегося во Франции, примерно в то же время, когда началось вторжение червя WANK. Он пошел по следу и установил контакт с менеджером этой системы. Не сможет ли он помочь? О чем речь! Машина в вашем распоряжении, мсье Тенкати.

Тенкати никогда раньше не пользовался сетью X.25, имевшей собственный набор команд, не

похожий ни на какие другие типы коммуникационных компьютерных сетей. Он хотел проследить маршрут червя, но ему требовалась помощь. Он позвонил в DEC своему другу Бобу Лайонсу [Bob Lyons] с просьбой послужить ему проводником в этом деле.

То, что удалось обнаружить, удивило Тенкати. След, оставленный червем в машине, был очевиден – знакомая схема повреждения логинов, которые червь пытался взломать в разных учетных записях. Но эти свидетельства деятельности червя датировались не 16 октября или другим близким временем. Лог-файлы показывали, что имеющая отношение к червю деятельность велась примерно на две недели раньше нападения на NASA. Этот компьютер был не просто транзитной машиной, использованной червем для начала атаки на NASA. Здесь разрабатывалась программа. Точка отсчета.

Тенкати пришел на встречу DST и ФБР подготовленным. Он знал, на чем построить обвинение французов. Когда он представил результаты своей детективной работы, французская секретная служба не смогла их опровергнуть, но она взорвала свою собственную бомбу. Хорошо, сказали французы, вы можете указать на французскую систему как исходный пункт атаки, но наше расследование установило, что соединения с X.25, совпадающие по времени с развитием червя WANK, исходили из другого места.

Они пришли из Австралии.

Французы были довольны собой, еще бы, ведь не французский хакер создал червя WANK. *Se n'est pas notre probleme.* [p28] По крайней мере, *теперь* это не наша проблема.

Здесь след червя начал остывать. Силы правопорядка и люди из компьютерной безопасности США и Австралии имели мысли насчет того, кто мог создать червя WANK. Персты указывали, обвинения были готовы прозвучать, но никто не был арестован. При ближайшем рассмотрении все догадки оказались лишь совпадениями и намеками, их было недостаточно для того, чтобы открыть дело. Подобно многим австралийским хакерам, создатель червя WANK лишь на мгновение показался из тени компьютерного подполья размытым силуэтом и сразу же исчез.

;) )

В конце 80-х годов компьютерное подполье Австралии стало той средой, которая сформировала автора червя WANK. Недорогие домашние компьютеры, вроде Apple II и Commodore 64, могли себе позволить обычные семьи из пригородов. Хотя эти компьютеры не были широко распространены, цена делала их вполне доступными для преданных компьютерных энтузиастов.

В 1988 году, за год до нападения червя WANK, Австралия была на подъеме. Страна отпраздновала свое двухсотлетие. Экономика переживала бум. Торговые барьеры и устаревшие регулирующие структуры исчезли. По экранам всего мира победоносно прошел «Крокодил Данди» и сделал австралийцев хитом месяца в таких городах, как Нью-Йорк и Лос-Анджелес. Настроение было радужным. У всех было такое чувство, что они обрели почву под ногами. Австралия, мирная страна с семнадцатимиллионным населением и западноевропейской демократией, вышла на уровень азиатских тигров и продолжала двигаться вперед. Возможно, впервые за свою историю австралийцы избавились от своего культурного низкопоклонства, уникального типа неуверенности в себе, совершенно неизвестного мощным культурам, таким как американская. Эксперименты и исследования требуют уверенности в собственных силах, и в 1988 году Австралия обрела эту уверенность.

Но ни эта вновь обретенная уверенность, ни оптимизм не ослабили традиционного циничного отношения австралийцев к истеблишменту. Все эти чувства, вместе взятые, породили странный парадокс. Австралийский юмор, круто замешанный на скепсисе в отношении всех серьезных и священных тем, по-прежнему с глубокой непочтительностью обращался с правительственными институтами, что несказанно удивляло многих иностранцев. Этот цинизм по отношению к большим уважаемым учреждениям насквозь пропитал зарождающийся компьютерный андеграунд Австралии, ничуть не охладив его восхищения и оптимизма перед дивным новым миром компьютеров.

В 1988 году австралийское компьютерное подполье цвело буйным цветом, как шумный азиатский базар. Это было королевство места, а не пространства. Покупатели заходили в лавки, торговались из-за товара с продавцами, по-дружески толкались и перемещались по переполненным улочкам, завязывая знакомства. Рынок был как местом общения, так и совершения покупок. Люди заходили в маленькие кофейни и местные бары, чтобы просто поболтать. Новейшие импортные товары, подобно

штукам блестящего китайского шелка, лежали на столах и служили предлогом к началу разговора. И, как на любом уличном рынке, лучшие товары были припрятаны в надежде, что появится друг или стоящий покупатель, пользующийся расположением продавца.

Валютой подполья были не деньги, а информация. Люди обменивались и делились информацией не для того, чтобы разбогатеть в денежном отношении, — они делали это для того, чтобы заслужить уважение и вызвать восхищение.

Члены австралийского компьютерного андеграунда встречались на досках объявлений — BBS.<sup>[p29]</sup> Очень простые по сегодняшним стандартам, BBS часто были скомпонованы из усиленного компьютера Apple II, модема и единственной телефонной линии. Но они соединяли людей из разных слоев общества. Тинейджеров из рабочих районов и их сверстников из дорогих элитных школ. Студентов университетов и двадцатилетних безработных. Даже работающих людей от 30 до 40 лет, кто просиживал все выходные, зарывшись в компьютерные учебники и собирая примитивные компьютеры в комнате для гостей. Большинство пользователей BBS были мужчинами. Иногда чья-нибудь сестра могла появиться в мире BBS в поисках нового друга. Добившись своего, она исчезала со сцены на недели, а то и месяцы, по всей видимости, до тех пор пока не возникала необходимость в новом посещении.

У пользователей BBS было мало общего. В основном они обладали достаточно высоким интеллектом — обычно с техническим уклоном — и были одержимы своим хобби. Они должны были быть одержимы. Часто приходилось минут по 40–45 тратить на набор единственного телефонного номера BBS лишь для того, чтобы всего на полчаса зайти в компьютерную систему. Большинство фанатов BBS делали это по несколько раз в день.

Как подсказывает название, BBS представляет собой электронную версию обычной доски объявлений. Владелец BBS делил доску на разные части, как школьный учитель разделяет на четыре части поверхность пробковой доски с помощью четырех разноцветных ленточек. Одна BBS могла иметь более тридцати дискуссионных групп.

Будучи пользователем доски, вы могли посетить политическую секцию и высказать там свое мнение по поводу деятельности ALP<sup>[p30]</sup> или либерального политического курса любому, кому оно будет интересно. Если кто-то воображал себя немного поэтом, он мог набраться смелости и поместить свое творение в «Уголке поэта». Там часто можно было встретить мрачные, мизантропические опусы, навеянные невзгодами пубертатного периода. Может быть, вы хотели поговорить о музыке? На многих BBS можно было найти информацию практически о любом музыкальном стиле. Самыми популярными были такие исполнители, как Pink Floyd, Tangerine Dream и Midnight Oil. Восстающие против истеблишмента настроения Midnight Oil задевали особые струны в молодом сообществе BBS.

1988 год был золотым веком BBS-культуры в Австралии. Это было время невинности и общности интересов. Это была тусовка под открытым небом, полная жизни и новых идей. Люди, по большей части, доверяли своим товарищам по сообществу и администраторам BBS, которые зачастую почитались, как полубоги. Это было счастливое место. И в целом надежное. Возможно, этот факт стал одной из причин, по которой люди чувствовали себя в безопасности, высказывая новые идеи. Это было место, где создатель червя WANK мог оттачивать и совершенствовать свое компьютерное мастерство.

Столицей новой духовной электронной цивилизации Австралии стал Мельбурн. Трудно сказать, почему этот южный город стал культурным центром BBS-мира и его темной стороны, австралийского компьютерного подполья. Возможно, история этого интеллектуального центра Австралии создала благоприятную почву для появления множества молодых людей, которые создавали свои системы, руководствуясь чем-то большим, нежели простое любопытство, и давали приют компьютерным битам, отвергнутым другими. Может быть, индивидуальность Мельбурна как города с большими пригородными районами и паяльными мастерскими на задних дворах породила культуру, которая привела к появлению BBS. Или причиной стали тоскливые мельбурнские пляжи и часто скверная погода? Как сказал один мельбурнский хакер: «А чем еще заниматься здесь всю зиму? Только залечь в берлогу с компьютером и модемом».

В 1988 году в Мельбурне было от шестидесяти до ста действующих BBS. Оценки расплывчаты,

---

p29

Bulletin Board System, т. е. система электронных досок объявлений.

p30

Австралийская лейбористская партия.

потому что невозможно сосчитать количество движущихся объектов. Любительская природа систем, часто спутанный в беспорядке клубок проводов и подержанных электронных плат, спаянных в каком-нибудь гараже, означали, что жизнь системы была не длиннее периода времени, в течение которого подросток проявлял к ней интерес. Системы неожиданно возникали и функционировали пару недель, затем снова растворялись в небытие.

Некоторые из них работали только в определенное время суток, скажем, с 10-ти вечера до 6-ти утра. Когда хозяин системы отправлялся спать, он подключал домашнюю телефонную линию к BBS и оставлял ее так до утра. Другие были доступны круглосуточно, но самым популярным временем всегда оставалась ночь.

Конечно, некоторые пользователи были подвижны не только интеллектуальными стимулами. Посетители BBS часто стремились к обретению индивидуальности не меньше, чем к новым идеям. На электронной доске объявлений можно создать личность, придать ей очертания и сделать ее своей собственностью. Возраст и внешний вид не имели значения. В отличие от технической подкованности. Любой прыщавый и застенчивый подросток мог превратиться в элегантного и обходительного джентльмена. Трансформация начиналась с выбора имени. В жизни вас могло угораздить носить имечко Эллиот Дингл, выбранное вашей матерью в честь давно почившего дальнего родственника. Но на BBS вы могли стать Blade Runner,<sup>[p31]</sup> Ned Kelly<sup>[p32]</sup> или Mad Max.<sup>[p33]</sup> Неудивительно, что подростки предпочитали проводить время в BBS.

Как правило, когда пользователь выбирал хэндл, он накрепко прилипал к нему. Вся его электронная почта приходила на учетную запись, подписанную этим именем. Регистрации на доске объявлений осуществлялись под ним же. Другие обитатели мира системы знали его только под этим именем. Хэндл превращался в настоящее имя с врожденным значением, хотя личность, отраженная в нем, могла быть лишь *alter ego*. И вот на сцену выходят такие персонажи, как Wizard, Conan и Iceman.<sup>[p34]</sup> Они проводят время в BBS под названиями Crystal Palace, Megaworks, The Real Connection и Electric Dreams.<sup>[p35]</sup>

Устремления посетителей BBS очень отличались друг от друга. Некоторые из них хотели участвовать в ее социальной жизни. Они хотели встретить себе подобных – блестящих, но странных и замкнутых людей, разделяющих их интерес к тонким техническим компьютерным вопросам. Многие были изгоями в реальной жизни и никогда не имели «нормальных» друзей в школах и в университетах. Хотя некоторые из них уже начали работать, они так и не смогли избавиться от своей досадной неловкости, которая преследовала их с подросткового возраста. В обычном мире им никогда не предлагали зайти в паб, чтобы пропустить пивка после футбольного матча.

Но это и хорошо. Во всяком случае, они никогда особенно не интересовались футболом.

Каждая BBS имела свой собственный стиль. Некоторые из них были абсолютно законны, все их компоненты легальны и совершенно открыты. Другие, подобные Real Connection, приютили было первых австралийских хакеров, но это шло вразрез с их честным образом жизни. Хакерские секции на таких досках объявлений были закрыты еще до того, как правительство Австралии приняло первые антихакерские законы в июне 1989 года. В то время на 10–12 мельбурнских BBS можно было уловить душок компьютерного подполья. Некоторые из них, например Greyhawk и The Realm,<sup>[p36]</sup>

---

p31

«Бегущий по лезвию бритвы» – название фильма режиссера Ридли Скотта (1982), снятого по мотивам романа Филиппа Дика «Снятся ли андроидам электроовцы?».

p32

Нед Келли – австралийский гангстер второй половины XIX века, ставший своего рода национальным героем Австралии.

p33

«Безумный Макс» – название фильма австралийского режиссера Джорджа Миллера (1979), герой которого, бывший полицейский Макс (актер Мел Гибсон), в одиночку борется за справедливость в апокалиптическом мире будущего.

p34

Чародей, Конан и Снежный Человек.

p35

Хрустальный дворец, Мегатруд, Реальное соединение и Электрические сны.

p36

Серый Ястреб и Королевство



допускали пользователей только при наличии приглашения. Вы не могли просто позвонить, создать новую учетную запись и зарегистрироваться. Вас должен был пригласить владелец доски. Обычную публику с модемами просили не беспокоиться.

Два самых главных места в австралийском подполье между 1987 и 1988 годами назывались Pacific Island и Zen.<sup>[p37]</sup> Двадцатитрехлетний деятель, называвший себя Craig Bowen, запустил обе системы из своей спальни.

Известный также как Thunderbird,<sup>[p38]</sup> Craig Bowen запустил Pacific Island в 1987 году, потому что хотел создать штаб хакеров. Не успев опериться, хакерское сообщество рассеялось после того, как ANUBBS, возможно, самая первая хакерская доска в Мельбурне, свернула свою деятельность. Craig Bowen решил создать убежище, нечто вроде темного, похожего на утробу кафе-бара посреди суматохи базара BBS, где хакеры Мельбурна могли бы собираться и делиться информацией.

Его спальня была обычной мальчишеской комнатой. Встроенные стенные шкафы, кровать, на одной стене комнаты – плакаты с изображениями старинных автомобилей. Окно, выходящее на соседский двор, заросший листвой. Стопка компьютерных журналов с названиями вроде *Nibble* или *Byte*. Несколько книг по программированию. Учебники VAX/VMS. Книг немного, среди них неплохая подборка научно-фантастических романов Артура Кларка. «Автостопом по Галактике».<sup>[p39]</sup> Словарь китайского языка, которым он пользовался, когда учился в школе «Мандарин» и после, когда продолжал самостоятельно изучать язык в попытке удержаться на своей первой работе.

Apple II, модем и телефон разместились на большой чертежной доске и столике в ногах его постели. Craig Bowen поставил телевизор сразу за компьютером, так что он мог сидеть на кровати, смотреть телевизор и одновременно наблюдать, что происходит в Pacific Island. Позже, когда появился Zen, он поставил его рядом с PI. Это было отлично устроено.

Pacific Island вряд ли представляет интерес с точки зрения современных стандартов Unix и Интернета, но в 1987 году это была впечатляющая машина. PI (местные юзеры произносили это «pie»<sup>[p40]</sup>) имел жесткий диск на 20 мегабайт – поистине чудовищный объем памяти для тогдашнего домашнего компьютера. На установку одного только PI Craig Bowen истратил около 5000 долларов. Он любил обе системы и проводил много времени, пестуя их. Как и на большинстве BBS, на PI и Zen не вносили никакой платы с пользователей. Этот юноша с мягкими чертами лица, полумальчик-полумужчина, который со временем приютил на своей скромной BBS многих умнейших компьютерных и телефонных хакеров Австралии, мог позволить себе платить за свои компьютеры. Во-первых, он жил с родителями, во-вторых, у него была постоянная работа в Telecom, в то время единственной телефонной компании Австралии.

PI посещало около 800 пользователей, 200 из которых постоянно висели в системе. У PI была собственная телефонная линия, независимая от домашнего телефона, поэтому родители Craig Bowen'a не расстраивались из-за того, что телефон вечно занят. Позже он провел еще четыре телефонных линии для Zen, в которой было около 2000 пользователей. Благодаря опыту, полученному в Telecom, Craig Bowen установил множество нестандартных, но вполне легальных устройств в своем доме. Коммутаторы, телефонные переключатели. В телекоммуникационном плане дом Craig Bowen'a был похож на старый автомобиль с усовершенствованным двигателем.

Craig Bowen сразу решил, что если он хочет сохранить работу, то ему лучше не предпринимать ничего незаконного в отношении Telecom. Однако австралийская национальная телекоммуникационная сеть была подручным источником технической информации. Так, у него был легальный доступ в компьютерную систему Telecom, где он мог очень многое узнать о ее коммутаторах. Но он никогда

---

p37

Тихоокеанский остров и Дзен.

p38

Буревестник.

p39

«The Hitchhiker's Guide to the Galaxy» – радиоспектакль BBC (1978), а затем и книга Дугласа Адамса, образец юмористической фантастики.

Русский перевод книги доступен на <http://lib.rus.ec/b/120291> (прим. сост. FB2)

p40

Пай – пирог (англ.).

не использовал эту учетную запись для хакинга. Большинство серьезных хакеров исповедовали такую же философию. У многих были легальные компьютерные учетные записи в университете, но они свято оберегали их невинность. По выражению одного хакера, основное правило подполья гласило: «Не гадить в своем гнезде».

PI состоял из общедоступного и частного сектора. Общий сектор был похож на старинный кабачок. Любой мог забрести в него, плюхнуться на табурет у стойки и завязать разговор с компанией. Достаточно было просто позвонить в систему через модем и сообщить сведения о себе – настоящее имя, хэндл, номер телефона и другие детали.

Многие пользователи BBS давали ложную информацию, с тем чтобы скрыть свою настоящую личность, и многих операторов это не слишком волновало. Но только не Craig Bowen'a. Посещение хакерского сайта было связано с риском даже до того, как были введены антихакерские законы. Пиратское программное обеспечение было незаконным. Хранение данных, скопированных во время хакерских набегов на иностранные компьютеры, также могло считаться незаконным. Желая избежать контактов с полицией и репортерами, Craig Bowen старался проверять персональную информацию о каждом пользователе PI и звонил ему домой или на работу. Иногда ему это удавалось.

Иногда нет.

Общественная секция PI приютила несколько дискуссионных групп, где собирались любители поболтать о главных производителях ПК – IBM, Commodore, Amiga, Apple и Atari – наравне с фанатами популярной группы Lonely Hearts.<sup>[p41]</sup> В Lonely Hearts было около двадцати постоянных пользователей, большинство из которых изнемогали от гормональных изменений, присущих периоду полового созревания. Мальчуган, жаждущий внимания девчонки, которая его бросила или, хуже того, вообще не подозревала о его существовании. Подростки, обдумывающие самоубийство. Послания были абсолютно анонимны, читатели даже не знали хэндлов авторов, и эта анонимность обеспечивала искренность посланий и подлинность ответов.

Система Zen стала более сложной младшей сестрой PI. Через два года работы PI Craig Bowen открыл Zen, одну из первых австралийских BBS, имевших больше одной телефонной линии. Главная причина открытия Zen заключалась в его желании положить конец тому, что компьютерные пользователи постоянно беспокоили его. Когда кто-то входил в PI, первое, что он делал, был запрос онлайн-чата с системным оператором. Apple II, на котором размещался PI, по современным стандартам был крайне примитивной системой. Craig Bowen не мог сделать его многозадачным. Он не мог работать за своей машиной, не мог даже проверить почту, пока в PI был посетитель.

Zen стал водоразделом в истории BBS Австралии. Многозадачный Zen. В систему могли позвонить и войти до четырех человек одновременно, при этом Craig Bowen продолжал спокойно заниматься своими делами, в то время как пользователи были онлайн. Более того, пользователи могли общаться между собой и не донимать его без конца. Несколько юзеров на многозадачной машине с несколькими телефонными линиями – то же самое, что стайка детей. По большей части, они играют друг с другом.

Внешне респектабельный и законопослушный Craig Bowen был, как и большинство участников андеграунда, недолюбливал официальные власти. Выбор названия Zen подчеркнул этот факт, поскольку оно было заимствовано из научно-фантастического сериала британского телевидения Blake 7, в котором кучка бунтовщиков пыталась свергнуть злое авторитарное правительство. Компьютер на космическом корабле восставших носил имя Zen. Бунтовщики объединились, встретившись на тюремном корабле; их всех перевозили в исправительное поселение на другую планету. Один из главных персонажей, этакий антигерой, угодил в тюрьму за компьютерный хакинг. Он говорил товарищам по борьбе, что его главной ошибкой было то, что он полагался на других людей. Он доверился им, а должен был работать в одиночку.

Craig Bowen понятия не имел, насколько пророческими окажутся эти слова лишь через несколько месяцев.

Тусовка у Craig Bowen'a стала центром настоящих и будущих светочей компьютерного подполья. The Wizard.<sup>[p42]</sup> The Force.<sup>[p43]</sup> Powerspike.<sup>[p44]</sup> Phoenix.<sup>[p45]</sup> Electron.<sup>[p46]</sup> Nom.<sup>[p47]</sup> Prime

p41

Одинокие сердца.

p42

Чародей.

p43

Suspect.<sup>[p48]</sup> Mendax. Train Trax. Некоторые, вроде Prime Suspect, лишь время от времени появлялись в Zen, чтобы глянуть, что там происходит, и поздороваться с друзьями. Другие, например Nom, были частью сплоченной семьи PI. Nom помогал Craig Bowen'у устанавливать PI. Как и многие другие первые участники подполья, они встретились в AUSOM – «Обществе пользователей Apple» в Мельбурне. Craig Bowen хотел установить в Zen программу ASCII Express, которая позволяла пользователям перемещать файлы между своими компьютерами и PI. Но, как обычно, у него и его друзей была лишь пиратская копия программы. Никаких учебников. И Nom с Craig Bowen'ом за один уик-энд самостоятельно проанализировали программу. Каждый сидел у себя дома со своей копией программы. Они часами висели на телефоне, пытаясь разобраться, как она работает, и в конце концов написали собственный учебник для других членов подполья, страдавших от того же недостатка информации. Затем они подготовили программу и запустили ее в PI.

Членство в одной из многих групп такой BBS, как PI, имело и другие преимущества, помимо получения хакерской информации. Если кому-то хотелось сбросить покров анонимности, он мог присоединиться к организованному, сплоченному дружескому кружку. Например, члены одной из групп были фанатами фильма «Братья Блюз».<sup>[p49]</sup> Вечером каждой пятницы они одевались по их подобию – черный костюм, белая рубашка, галстук-шнурок, солнечные очки Rayban и, конечно, шляпа с полями, загнутыми сзади вверх, а спереди – вниз. Одна супружеская пара даже приводила ребенка, одетого а-ля маленький Брат Блюз. Группа пятничных завсегдатаев приходила к 11.30 вечера в Northcote's Valhalla Theatre (теперь Westgarth). Его пышная, слегка кричащая атмосфера вполне соответствовала этой альтернативной культуре, буйно цветущей на еженедельных сборищах в кино-театре. Прыгая на сцену посреди фильма, группа PI принималась откалывать номера, пародируя актеров в ключевых сценах фильма. Это был веселый и, что самое главное, недорогой вечер. Администрация Valhalla бесплатно пропускала завсегдатаев в соответствующих костюмах. Фанатам оставалось только заплатить за напитки в антракте.

Время от времени Craig Bowen'у тоже удавалось собирать вместе других пользователей PI и Zen. Обычно они встречались в центре Мельбурна, иногда на центральной городской площади. Эта группа состояла в основном из парней, но иногда попадались и девушки. Сестра Craig Bowen'а, известная под хэндлом Syn, некоторое время тоже околачивалась там. Она дружила с несколькими хакерами из разных BBS. И она была не одна. В этой группе обмена друзьями и подружками происходили с завидной регулярностью. Они ошивались на городской площади после кино, обычно очередного ужастика («Кошмар на улице Вязов-2», «Дом ужасов-3»...). Иногда, для разнообразия, они ходили в боулинг и действовали на нервы другим игрокам. Если мероприятия заканчивались рано, они шли в Макдональдс и съедали по бургеру, шутили, смеялись и бросались маринованными огурчиками в стену фаст-фуда. Потом они еще немного болтали, сидя на каменных ступенях центральной площади, прежде чем сесть на последний автобус или поезд домой.

Социальные секции Zen и PI были более успешными, чем технические, но частная хакерская секция была успешней всех. Хакерская секция была скрыта от посторонних глаз; те, кто мечтал стать частью мельбурнского андеграунда, знали, что там что-то происходит, но что именно – никто не

---

Сила.

p44

Сильный шип.

p45

Феникс.

p46

Электрон.

p47

Имя.

p48

Главный подозреваемый.

p49

«The Blues Brothers» («Братья Блюз») – музыкальная комедия режиссера Джона Лэндиса (1980), в главных ролях заняты Джон Белуши и Дэн Эйкройд.

знал.

Чтобы получить приглашение в закрытую секцию, кандидат должен был обладать хакерскими навыками или ценной информацией и, как правило, быть рекомендован Craig Bowen'у кем-то, кто уже был внутри. В Inner Sanctum/[p50] (так называлась закрытая хакерская секция) люди могли спокойно обмениваться информацией – своим мнением о новых компьютерных продуктах, о технике хакинга, подробностями о компаниях и новых сайтах для взлома и последними слухами о деятельности карательных органов.

Но Inner Sanctum не была самым неприступным частным владением. Две хакерских группы, Elite и H.A.C.K., ревностно охраняли вход в свои собственные, еще более закрытые тайные комнаты. Даже если вам удалось получить доступ в Inner Sanctum, вы могли и не подозревать о существовании H.A.C.K. и Elite. Вы могли догадываться, что существует еще более эксклюзивное место, чем доступная вам область, но как много слоев отделяет вас от нее, было неизвестно. Почти каждый хакер, давший интервью для этой книги, говорил о смутном чувстве, что есть нечто вне пределов первого внутреннего круга. Они знали, что что-то существует, но не могли сказать, что именно.

Иногда Craig Bowen'у приходилось отвечать на телефонные звонки желающих «стать хакерами», которые пытались нахрапом прорваться в Inner Sanctum.

– Мне нужен доступ в вашу пиратскую систему, – пищал голосок очередного юного претендента.

– Какую пиратскую систему? Кто тебе сказал, что у меня пиратская система?

Craig Bowen вытягивал у звонившего все, что мог, пытаясь узнать, откуда у него такие сведения. Затем все отрицал.

Чтобы оградить себя от таких попыток, Craig Bowen старался держать в секрете свой адрес, настоящее имя и номер телефона от большинства пользователей своей BBS. Но это не всегда оказывалось возможно. Однажды он был несказанно удивлен появлением у своих дверей Masked Avenger.[p51] Как он нашел его адрес, осталось загадкой. Они по-дружески общались в чате, но Craig Bowen не сообщал личных подробностей. Он совершенно не был готов к появлению паренька в огромном шлеме, который остановился на своем велосипеде у дверей его дома. «Привет! – пропищал он. – Я – Masked Avenger!»

Masked Avenger – подросток лет пятнадцати – оказался достаточно сообразительным, чтобы узнать подробности личной жизни Craig Bowen'a. Тот пригласил его войти и показал ему систему. Они стали друзьями. Но после этого случая Craig Bowen решил еще больше усилить меры безопасности вокруг своей личной жизни. Он начал, по его собственным словам, «смещаться к полной анонимности». Он взял себе псевдоним Craig Bowen и в дальнейшем в андеграунде его знали только под этим именем или под псевдонимом Thunderbird. Он даже открыл счет в банке на имя Craig Bowen'a для добровольных пожертвований, которые пользователи иногда отправляли в PI. Это всегда были небольшие суммы – 5–10 долларов, потому что у студентов никогда не бывает много денег. Craig Bowen вкладывал все эти деньги в PI.

У людей было много причин желать проникнуть в Inner Sanctum. Некоторым нужны были копии последнего программного обеспечения (преимущественно речь шла о пиратских копиях американских компьютерных игр). Другие хотели поделиться информацией и идеями по поводу способов взлома компьютеров, часто принадлежавших местным университетам. Третьи желали научиться манипулировать телефонной системой.

Закрытые секции функционировали, как королевский двор, населенный аристократами и придворными с различными степенями старшинства и духом соперничества. В них царил сложный социальный порядок и уважение было правилом игры. Если вы хотели получить допуск, вам нужно было лавировать и демонстрировать вышестоящим тот факт, что вы обладаете достаточно ценной хакерской информацией, чтобы быть избранным, и стараться не показать им слишком много, чтобы они не сочли вас болтуном. Лучшим предметом сделки был старый добрый пароль к функции dial-out компьютера Мельбурнского университета.

Dial-out университета был ценной штукой. Хакер мог позвонить на компьютер университета, зарегистрироваться, как «модем», и машина соединяла его с модемом, который позволял ему осуще-

ствлять дальнейший удаленный набор. Затем он мог звонить куда угодно в мире, а телефонный счет оплачивал университет. В конце 80-х годов, до начала эры дешевого общедоступного Интернета, университетский dial-out позволял хакеру иметь доступ куда угодно – от нелегальных BBS в Германии до военных систем США в Панаме. Такой пароль помещал весь мир на кончики его пальцев.

Хакер, стремившийся проникнуть в Inner Sanctum, не должен был распространять текущий пароль удаленного набора в общедоступных областях PI. Скорее всего, если он находился на низкой ступени официальной иерархии, он попросту не мог иметь такой ценной информации. Даже если ему удавалось каким-то образом заполучить текущий пароль, то отдавать его широкой публике было крайне рискованно. Если это случалось, то все, кому не лень, начинали следить в учетной записи доступа к университетскому компьютеру вместе со всеми своими родственниками и собаками. Системный администратор мог счесть необходимым изменить пароль, так что хакер очень быстро терял свой доступ к университетской системе. Хуже того, он лишал доступа других хакеров – тех, кто вращался в Elite, H.A.C.K. и Inner Sanctum. Им обрезали крылья. Хакеры ненавидят, когда пароли и учетные записи, которые они привыкли считать своими, вдруг меняются без предупреждения. Даже если пароль не был изменен, хакер-претендент выглядел человеком, не умеющим хранить секреты.

Но предоставление старого пароля было совершенно другим делом. Информация была практически бесполезной, так что хакер ничего не приносил общине. Но тот простой факт, что он имел доступ к информации такого рода, подразумевал, что он не был обычным пользователем. Другие хакеры могли подумать, что он получил пароль, когда тот был еще действителен. И главное, показывая уже известный просроченный пароль, кандидат намекал, что он вполне способен раздобыть текущий пароль. Voila! [\[p52\]](#) Мгновенное уважение.

Попытка заслужить приглашение в Inner Sanctum была стратегической игрой: дразнить, но никогда не доходить до конца. В конце концов кто-нибудь из посвященных, возможно, заметит тебя и шепнет словечко Craig Bowen'у. И ты получишь приглашение.

Если у тебя были действительно серьезные амбиции и ты жаждал попасть в первый внутренний круг, тебе нужно было начинать действовать по-настоящему. Ты не мог спрятаться за извинениями, что общедоступный сектор, возможно, контролировался властями и что там было полно идиотов, которые могли злоупотребить ценной хакерской информацией.

Хакеры круга избранных судили о тебе по тому, как много информации о взломе компьютеров ты сможешь им предоставить. Они также обращали внимание на ее точность. Было не слишком сложно раздобыть старые логины и пароли к студенческой учетной записи в компьютерной системе университета Монаш. А вот если предоставить действующую учетную запись в системе VMS Лесного департамента Новой Зеландии, то это могло заинтриговать серьезных людей.

Великим ритуалом перехода от мальчика к мужчине была Minerva. ОТС (тогда еще принадлежавшая австралийскому правительству<sup>20</sup> Overseas Telecommunications Comission [\[p53\]](#)) пользовалась Minerva, системой из трех мейнфреймов Prime в Сиднее. Для хакеров, таких как Mendax, взлом Minerva был настоящим испытанием.

В начале 1988 года Mendax только начал постигать азы хакинга. Ему удалось преодолеть барьер между публичным и частным секторами PI, но этого было недостаточно. Чтобы тебя признали восходящей звездой хакерские аристократы вроде Force и Wizard, ты должен был проникнуть в систему Minerva. Mendax взялся за работу в надежде взломать ее.

Minerva была особенной по многим причинам. Хотя она находилась в Сиднее, телефонный номер ее входного компьютера, называемого PAD X.25, был бесплатным. В то время Mendax жил в Эмеральде, сельском городишке неподалеку от Мельбурна. Звонок на большинство мельбурнских номеров привел бы к неизбежному появлению счета, и это исключало возможность удаленного набора из Мельбурнского университета, который мог бы предоставить возможность для дальнейших действий.

Эмеральд вряд ли можно было назвать Изумрудным городом. [\[p54\]](#) Умному шестнадцатилет-

---

p52

Вот! (фр.)

<sup>20</sup> ОТС впоследствии была объединена с Telecom в одну компанию – Telstra.

p53

Комиссия трансокеанских коммуникаций.

p54

нему пареньку там было смертельно скучно. Mendax жил в Эмеральде со своей матерью. Этот городок был лишь остановкой, одной из многих, так как мать таскала сына по всему континенту, пытаясь сбежать от его бывшего отчима-психопата. Гостиница была аварийным убежищем для семей, находящихся в бегах. Это было безопасное место, и поэтому измученная семья Mendax'a на время остановилась здесь, чтобы отдохнуть перед тем, как сорваться в поисках нового убежища.

Иногда Mendax ходил в школу. Иногда нет. Школьная система не слишком интересовала его. Это не давало такой пищи его мозгам, какую могла дать Minerva. Сиднейская компьютерная система была намного более привлекательным местом для прогулок, чем сельская средняя школа.

Minerva была компьютером Prime, и круче этого не было ничего. Force, один из самых уважаемых хакеров в 1987–1988 годах в австралийском компьютерном подполье, специализировался на Primos, особой системе, используемой в машинах Prime. Он написал свою собственную программу – мощный хакерский инструмент, поставляющий текущие имена пользователей и пароли, – и сделал систему модной в компьютерном андеграунде.

Компьютеры Prime были большими и дорогими, и ни один хакер не мог себе позволить такой, поэтому возможность доступа к скоростным вычислительным мощностям такой системы, как Minerva, была бесценной для запуска собственных программ хакера. Например, сетевой сканер (программа, которая собирала адреса компьютеров в сети X.25, мишеней будущих хакерских приключений) требовал большого количества ресурсов. Но большая машина, подобная Minerva, могла с легкостью это сделать. Minerva также позволяла пользователям подключаться к другим компьютерным системам по всему миру. Вдобавок у Minerva был встроенный интерпретатор BASIC. Это позволяло писать программы на языке программирования BASIC – самом популярном в те времена – и запускать их в Minerva. Не надо было быть фанатом Primos, как Force, чтобы написать и выполнить программу в компьютере ОТС. Minerva отлично подходила для Mendax.

У системы ОТС были и другие преимущества. Многие большие австралийские компании имели учетные записи в этой системе. Взлом учетной записи требует имени пользователя и пароля: найди имя пользователя – и половина уравнения решена. Имена с учетных записей Minerva было легко достать. Каждое имя состояло из трех букв, за которыми следовало три цифры. Такую систему было бы трудно расколоть, если бы не подбор букв и цифр. Три первых буквы почти всегда были акронимами компании. Например, у учетных записей ANZ Bank были имена ANZ001, ANZ002, ANZ003. Цифры были одними и теми же у большинства компаний. BHP001. CRA001. NAB001. И даже OTC007. Любой пользователь с коэффициентом интеллекта настольной лампы мог угадать самое малое пару-тройку имен учетных записей Minerva. Раздобыть пароли было посложнее, но у Mendax'a были мысли на этот счет. Он собирался прибегнуть к социальному программированию. Социальное программирование – это особый метод, который заключается в том, чтобы разговаривать с собеседником очень вежливо и всегда уметь проявлять желание в чем-то ему помочь. Правда, для этого требуется некоторая хитрость.

Mendax решил, что он применит этот маневр, чтобы узнать пароль одного из пользователей Minerva. Он раздобыл список пользователей Minerva, который был щедро предоставлен другим хакером PI в полное распоряжение молодежи, достаточно талантливой, чтобы найти ему применение. Этот список, к тому же неполный, был примерно двухгодичной давности, но он содержал 30 разрозненных страниц имен пользователей учетных записей Minerva, названия компаний, адреса, контактные фамилии и телефоны, номера факсов. Некоторые из них, возможно, еще годились.

У Mendax'a был довольно низкий голос для его лет; без этого нечего было и думать о социальном программировании. Ломающиеся голоса подростков не оставляли и камня на камне от надежд тех, кто мечтал стать социальным инженером. Но даже при наличии такого голоса, у него не было офиса или номера телефона в Сиднее, чтобы предполагаемая жертва могла перезвонить ему. Поиск там и сям, он откопал номер в Сиднее с кодом района 02, который был постоянно занят. Одна проблема долой, идем дальше.

Следующая задача – создать реальный шум работы в офисе. Едва ли он мог позвонить в какую-нибудь компанию и выуживать у них пароль, прикинувшись менеджером ОТС, когда единственным шумовым фоном вокруг него было щебетание птиц в прозрачном деревенском воздухе.

Нет, ему нужен был такой же фоновый гул, как в переполненном офисе в деловом квартале Сиднея. У Mendax'a был кассетный магнитофон, так что он мог предварительно записать звук работающего офиса и проиграть запись, когда будет звонить по номерам компаний из списка Minerva.

Единственной сложностью было найти подходящий офисный шум. Местная почта для этого явно не годилась. Не сумев найти ничего правдоподобного, он решил генерировать свой собственный шум работающего офиса. Это было непросто. С единственной дорожкой на кассетнике он не мог наложить один звук на другой; ему нужно было одновременно создать все шумы.

Первым делом Mendax включил TV, канал новостей, очень тихо, чтобы они жужжали на заднем плане. Затем он установил на печать длинный документ в своем принтере Commodore MPS 801. Он снял крышку с шумной матричной машины, чтобы создать нужную громкость ее стрекотания на заднем плане. Но этого было мало, требовалось что-то еще. Голоса операторов, невнятно что-то говорящих в переполненном офисе. Он мог бы и сам бормотать себе под нос, но, попытавшись, он понял, что его красноречия не хватит, чтобы стоя посреди комнаты разговаривать с самим собой битых четверть часа. Поэтому он взял томик Шекспира и начал читать вслух. Достаточно громко, чтобы слышать голос, но не до такой степени, чтобы будущая жертва могла разобрать строки из «Макбета». У операторов ОТС были клавиатуры, поэтому он вразнобой принялся стучать по клавишам. Иногда, для разнообразия, он подходил к кассетнику, задавал вопрос и быстро отвечал на него – другим голосом. Затем он с топотом отходил от магнитофона через всю комнату, а потом тихонько крался назад к клавиатуре и снова печатал и бормотал «Макбета».

Это был изнурительный труд. Mendax хотел, чтобы запись крутилась без перерыва, как минимум минут пятнадцать. Внезапные трехсекундные остановки в работе офиса, когда Mendax нажимал на паузу, чтобы отдохнуть, выглядели не слишком правдоподобно.

Запись потребовала множества попыток. Он был уже на полпути к успеху, продираясь сквозь строки Шекспира, беспорядочно шлепая по клавишам и начальственным тоном задавая вопросы самому себе, как вдруг его принтер зажевал бумагу. Черт. Ему пришлось начать все заново. Наконец, после очередного часа изнурительной слуховой шизофрении он получил идеальную запись офисного гула.

Mendax вытащил свой разрозненный список пользователей Minerva и принялся перелопачивать его 30 страниц. Это было не менее утомительно.

– Набранный вами номер отключен. Пожалуйста, проверьте номер, прежде чем набрать его еще раз.

Следующий номер.

– Извините, у него сейчас встреча. По какому номеру вам перезвонить?

– Спасибо, не стоит.

Другая попытка.

– Он больше не работает в нашей компании. Кто-то другой может помочь вам?

– Нет, не думаю.

И еще попытка.

И наконец, успех.

Mendax добрался до одной из фамилий в Перте. Действующий номер, действующая компания, действующее имя. Он прочистил голос, чтобы сделать его еще более низким и начал:

– Говорит Джон Келлер, оператор ОТС Minerva из Сиднея. Один из наших жестких дисков D090 полетел. Мы просмотрели данные с резервной ленты, и нам кажется, что мы располагаем верной информацией о вашей компании. Но, возможно, в результате инцидента что-то пострадало, и мы бы хотели подтвердить некоторые детали. К тому же резервная лента позавчерашняя, поэтому мы хотели бы проверить, насколько свежи ваши данные, и убедиться, что ваша работа не будет прервана. Позвольте мне уточнить детали...

Mendax пошелестел бумагой на своем столе.

– О, боже. Да, давайте проверим, – ответил встревоженный менеджер.

Mendax начал читать всю информацию из списка Minerva, полученную на Pacific Island, кроме одной вещи. Он немного изменил номер факса. Это сработало. Менеджер клянуул.

– О, нет. Номер нашего факса у вас точно неправильный, – сказал он и продиктовал верный номер.

Mendax постарался изобразить озабоченность.

– Хм, у нас может быть больше проблем, чем мы ожидали. Хм, – сказал он менеджеру и выдержал еще одну значительную паузу.

Нужно было набраться смелости для главного вопроса.

Трудно было сказать, кто вспотел больше: измученный менеджер из Перта, в ужасе представивший громкие жалобы персонала всей компании из-за того, что их учетная запись в Minerva ошибочна, или нескладный подросток, впервые пробующий свои силы в социальном программировании.

– Ладно, – начал Mendax, стараясь сохранить в голосе властные нотки. – Посмотрим. У нас есть номер вашей учетной записи, но будет лучше, если мы заодно проверим и ваш пароль... Что это было?

Стрела вылетела из лука. И поразила цель.

– Да, конечно, это L-U-R-C-H – все.

Ларч? *[p55]* Ага. Фан «Семейки Адамсов».

– Вы можете убедиться, что все в порядке? Мы не хотим, чтобы наша работа была остановлена, – менеджер из Перта был явно напуган.

Mendax беспорядочно постучал по клавишам и остановился.

– Что ж, кажется, теперь все работает великолепно, – он хотел поскорей успокоить менеджера. Лучше не бывает.

– Слава богу! – воскликнул тот. – Спасибо вам за все. Спасибо. Не знаю, как поблагодарить вас за этот звонок.

И так далее.

Mendax пора было выбираться из этой ситуации.

– О'кей, мне пора. Нужно еще позвонить в кучу мест.

Это сработало. Пертский менеджер попросил, как и ожидалось, номер контактного телефона на тот случай, если что-то будет не так, и Mendax дал ему тот, что был постоянно занят.

– Еще раз спасибо за любезность.

Ага. Сколько угодно.

Mendax повесил трубку и набрал бесплатный телефонный номер Minerva. Пароль сработал. Он не мог поверить, насколько легко он ему достался.

Mendax быстро осмотрелся, следуя примеру большинства хакеров, взламывающих новую машину. Во-первых, нужно было проверить электронную почту «позаимствованной» учетной записи. Какой-нибудь менеджер компании мог отправить информацию о названиях учетных записей, об изменениях паролей и даже о телефонных номерах модемов самой компании. Затем нужно было просмотреть директории, которые мог прочитать каждый в главной системе – еще один отличный источник информации. Конечная остановка – доска объявлений и новостей Minerva. На ней помещалась информация от системных операторов о запланированном простое и других рабочих моментах. Он пробыл там недолго. Первый визит обычно бывал коротким – нечто вроде вознаграждения за работу.

У Minerva было множество применений. Самым важным из них было то, что Minerva давала хакерам возможность для входа в разные сети X.25. X.25 – это вид сети компьютерных коммуникаций, очень похожий на базирующийся на Unix Интернет и использующий VMS DECNET. У них разные команды и протоколы, но принцип всемирной сети передачи данных один и тот же. Хотя есть и одно важное отличие. Цели хакеров в сетях X.25 намного более интересны. Например, в X.25 работают большинство банков. Отсюда следует, что на X.25 опираются многие элементы мировых финансовых рынков. Большое количество стран разместило свои военные компьютерные сайты исключительно в X.25. Многие считали X.25 более надежной и безопасной, чем системы Интернет или DECNET.

Minerva позволяла входящим пользователям получить доступ в сети X.25, в то время как многие университеты в Австралии не предоставляли такой возможности. И она позволяла делать это без всякой платы за телефонные звонки.

В начале деятельности Minerva операторы ОТС не особенно беспокоились по поводу хакеров, видимо, потому, что казалось совершенно невозможным избавиться от них. Операторы ОТС управляли коммутатором ОТС X.25, который был похож на телефонный коммутатор в сети данных X.25. Этот коммутатор был воротами к данным Minerva и других систем, подключенных к этой сети.

Первые австралийские хакеры легко получали к ней доступ, пока не появился Майкл Розенберг [Michael Rosenberg].

Розенберг, известный онлайн просто как MichaelR, решил очистить Minerva. Выпускник инженерного факультета Квинслендского университета, Майкл переехал в Сидней, где устроился на работу в ОТС в возрасте 21 года. Он был примерно одного возраста с хакерами, которых преследовал в своей системе. Розенберг не был оператором ОТС, он управлял программным обеспечением Minerva.



И он превратил жизнь таких, как Force, в ад. Закрывая лазейки в системе безопасности, отмечая учетные записи, используемые хакерами, а затем уничтожая их, Розенберг почти в одиночку подавил большую часть хакерской деятельности в Minerva.

Несмотря на это, хакеры («мои хакеры», как Розенберг называл завсегдатаев), стиснув зубы, уважали его. В отличие от кого бы то ни было в ОТС, он был их ровней в техническом плане, и в мире, где техническая удалость стала валютой, Розенберг котировался очень высоко.

Он хотел поймать хакеров, но не хотел видеть, как их сажают в тюрьму. Они раздражали его, и он просто хотел их убрать из своей системы. Но любой след линии должен был пройти через Telecom, в то время отдельную от ОТС структуру. А Telecom, как сказали Розенбергу, был очень не-сговорчив в таких делах из-за жестких законов о частной собственности. Розенберг не мог полностью обезопасить систему, пока ОТС не стала диктовать пароли своим клиентам. Обычно клиенты больше беспокоились о том, чтобы их служащие могли легче запомнить пароль, нежели о том, чтобы отразить нападение хитрых хакеров. В результате пароли многих учетных записей Minerva были легко доступны.

Хакеры и ОТС воевали с 1988 по 1990 годы. Это была война на множестве фронтов.

Иногда оператор ОТС мог взломать онлайн-сессию хакера, спрашивая, кто же это такой использует учетную запись. Иногда операторы отправляли хакерам оскорбительные послания и вламывались в сессию хакера со словами: «Идиоты, вы опять здесь». Операторы не могли удержать хакеров на расстоянии, но у них были другие способы помешать им.

Electron, мельбурнский хакер и восходящая звезда австралийского андеграунда, пробрался в немецкую систему через канал X.25 ОТС. Используя VMS-машину, вроде сестры системы Minerva, он играл в игрушку «Empire» в системе Altos – популярном месте встречи хакеров. Это был его первый опыт в «Empire», комплексной военной стратегии, которая привлекала геймеров всего мира. У каждого из них было меньше часа в день, чтобы завоевывать новые области, постоянно следя за сохранением производственных возможностей на соответствующем стратегическом уровне. Мельбурнский хакер неделями улучшал свою позицию. Он был на втором месте.

В один прекрасный день он вошел в игру через Minerva и немецкую систему и не мог поверить в то, что увидел на экране своего монитора. Его завоеванные области, его позиция в игре – все это исчезло. Оператор ОТС использовал пакетный сниффер [\[p56\]](#) X.25, чтобы проследить регистрацию хакера и захватить его пароль доступа в «Empire». Вместо обычного обмена оскорблениями оператор подождал, пока хакер выйдет из игры, а затем взломал ее и разрушил его позицию.

Electron был в ярости. Он так гордился достижениями в своей первой игре. Но не было и речи о том, чтобы в отместку учинить безобразия в самой Minerva. Несмотря на то, что они уничтожили его многонедельный труд, Electron не хотел вредить их системе. Он чувствовал признательность за то, что мог так долго пользоваться ей.

;)

Антиправительственные настроения в BBS, типа PI или Zen, тесно переплетались с любовью ко всему новому и неизведанному. В этом не было ожесточенности, просто желание сбросить старые одежды и окунуться в новые воды. Товарищество выросло из приятного чувства возбуждения от того, что юность в этом особенном времени и месте постоянно была на гребне больших открытий. Люди звонили на компьютеры через свои модемы и экспериментировали. Что даст эта последовательность клавиш? Как насчет этого тона? Что произойдет, если... Это были вопросы, интересующие их круглосуточно, заставляющие их все время искать и думать. Эти хакеры в своем большинстве не принимали наркотиков. Учитывая их возраст, они даже особо и не пили. Все это противоречило сжигающему их желанию знать, притупило бы остроту их восприятия. Антиавторитарные взгляды андеграунда были направлены в основном на структуры, которые преграждали им путь к новым горизонтам – такие как, например, Telecom.

Это было сильное слово. Скажи «Telecom» тогдашнему члену компьютерного андеграунда и увидишь самую поразительную реакцию. Мгновенное презрение появляется на его лице. После короткой паузы его губы растягиваются в презрительной ухмылке, и он отвечает с явной насмешкой:

«Telescum».

[p57] Подполье ненавидело австралийскую национальную телефонную сеть так же страстно, как оно любило исследовать все новое. Они чувствовали, что Telecom – отсталая контора и его персонал не имеет никакого представления о том, как использовать свои собственные телекоммуникационные технологии. Хуже всего было то, что Telecom явно активно не нравились BBS.

Помехи на линии перебивали разговор одного модема с другим, и андеграунд полагал, что ответственным за это является Telecom. Хакер читал послание в PI, и вдруг среди самых сочных, лакомых технических подробностей появлялась ложка дегтя – случайный набор символов вроде 2%28v#I;D&gt;nj4 и комментариев: «Помехи на линии. Чертов Telescum! Опять все обгадил!» Иногда помехи были так сильны, что хакеру приходилось отключаться и терять еще минут сорок в попытках дозвониться до BBS. У модемов не было программы коррекции ошибок, и чем выше была скорость модема, тем сильнее было действие помех. Частенько это превращалось в соревнование – нужно было прочитать почту и сообщения до того, как помехи Telecom отключат тебя.

В андеграунде постоянно ходили слухи о том, что Telecom собирается перейти на повременную оплату местных звонков.

Степень оскорбления была чудовищной. Сообщество BBS считало, что национальную сеть, видимо, раздражает, что люди могут провести час на доске объявлений по цене одного местного звонка. Другие, не менее интенсивные слухи были еще ужаснее. Говорили, что Telecom вынудил по меньшей мере одну BBS ограничить каждый входящий звонок 30 минутами. Отсюда появилось новое прозвище Telecom – Teleprofit.

[p58]

Для сообщества BBS служба безопасности Telecom, Protective Services Unit, стала врагом номер один. Это была электронная полиция. Андеграунд видел в службе безопасности «насильников», полновластную правительственную силу, которая могла вломиться в твой дом, прослушать твою телефонную линию и конфисковать твое компьютерное оборудование в любое время. Чем не повод ненавидеть Telecom.

Telecom был так ненавистен, что члены подполья привычно обсуждали способы саботажа в сети. Некоторые говорили о том, чтобы загнать разряд в 240V в телефонную линию – это бы вывернуло наизнанку коммутаторы, а заодно и всех техников, которые могли случайно оказаться у кабеля в этот момент. У Telecom были защитные предохранители, но хакеры BBS разработали соответствующую схему цепи, которая бы позволила высокочастотным разрядам обойти их. Другие члены андеграунда мечтали о том, чтобы восстановить справедливость и спалить все кабели отдельно взятого коммутатора Telecom – до них было очень легко добраться.

На этом фоне андеграунд начал смещаться к фрикингу. В широком смысле фрикинг понимался как взлом телефонных систем. Это очень свободное определение. Некоторые считают, что фрикинг подразумевает кражу номеров кредитных карт и их использование для оплаты телефонных разговоров. Пуристы осторожно относятся к этому определению. По их мнению, кража телефонных карт – это не фрикинг, а кардинг. Они доказывают, что фрикинг требует значительных технических навыков и подразумевает манипуляции с телефонным коммутатором. Эти манипуляции могут осуществляться с использованием компьютеров или электрических цепей для генерации специальных импульсов и изменения напряжения в телефонной линии. Эти манипуляции изменяют восприятие коммутатором отдельной телефонной линии. Результат – бесплатный и абсолютно безнаказанный телефонный разговор. Сторонники чистоты жанра среди хакеров скорее расценивают фрикинг как уничтожение собственных следов в телефонной сети, чем как возможность бесплатно поболтать с друзьями в других странах.

Первые симптомы перехода от хакинга к фрикингу и, возможно, к кардингу появились в период, занявший около полугода в 1988 году. Сначала хакеры из PI и Zen, чтобы пробираться в международные компьютерные сети, полагались на dial-out Мельбурнского университета или офис Telecom в Клейтоне. Они также использовали X.25 dial-out в других странах – США, Швейцарии, Германии – для совершения новых прыжков в своих международных путешествиях.

Постепенно люди, создавшие линии dial-out, прозрели и стали «перекрывать кран». Пароли изменились. Дополнительные возможности были отменены. Но хакеры не хотели терять доступ к заокеанским системам. Они вкусили этого и хотели добавки. Там находился большой электронный

мир, и его нужно было исследовать. Они начали пробовать разные методы, чтобы попасть туда, куда они хотели. Так, подполье Мельбурна докатилось до фрикинга.

Фрикеры слетались на RABX, как пчелы на мед. RABX (private automatic branch exchange<sup>[p59]</sup>) работал как телефонный мини-коммутатор Telecom. При помощи RABX служащий большой компании мог позвонить другому служащему внутри фирмы, не оплачивая стоимость местных телефонных звонков. Если, предположим, служащий остановился в отеле за пределами города, компания могла обязать его совершать все звонки через свой RABX, чтобы не платить по грабительским гостиничным тарифам за междугородные звонки. Если служащий был по делам в Брисбене, он мог набрать брисбенский номер, который соединял его с Сиднеем через RABX компании. Оттуда он мог позвонить хоть в Рим, хоть в Лондон, и счет за переговоры получала непосредственно компания. То, что годилось для клерка, подходило и фрикеру.

Фрикер, набирающий номер RABX, как правило, должен был знать или угадать пароль, который позволил бы ему звонить дальше. Часто фрикера приветствовал автоответчик и спрашивал у него дополнительный личный номер служащего – он также служил паролем. Что ж, это было довольно просто. Фрикер говорил автомату несколько номеров наугад, пока не находил подходящий.

В отдельных случаях система RABX даже не требовала пароля. Менеджеры RABX воображали, что они сделают достаточно для безопасности системы, сохраняя номер телефона в секрете. Иногда фрикерам удавалось звонить из RABX, просто исследовав отдельные модели или марки RABX на предмет лазеек в системе безопасности. Особая последовательность нажатий на клавиши позволяла фрикеру добиться желаемого, не зная ни пароля, ни имени служащего, ни даже названия компании.

Фрикинг начал затмевать хакинг, становясь все более модным способом времяпрепровождения на BBS. На PI появилась специальная фрикерская секция. Называть себя хакером какое-то время считалось старомодным. Фрикинг стремительно вырывался вперед.

Примерно в это время появилась Phreakers Five.<sup>[p60]</sup> Группа из пяти хакеров-ставших-фрикерами собралась вместе на PI. Легенды об их ночных забавах просочились в другие области доски объявлений и заставили других так называемых фрикеров позеленеть от зависти.

Первым делом фриеры находили телефонный щиток – серо-стальной закругленный ящик, помещенный очень высоко почти на каждой улице. В идеале щиток должен был находиться в густонаселенном районе, по возможности, пустынном по ночам. Телефонные коробки напротив пригородных домов были довольно опасными – в доме могла жить любопытная старая леди, склонная звонить в полицию при виде любого подозрительного человека или события. Что уж говорить о ее реакции, если бы она выглянула из-за своих кружевных занавесок и увидела небольшое, но очень активное представление.

Один из пятерки вылезал из микроавтобуса и открывал щиток ключом, выпрошенным, одолженным или украденным у техника Telecom. Достать ключ было плевым делом. Доски объявлений на BBS были переполнены веселыми списками ценного оборудования Telecom, вроде пятисот метров кабеля или ключа от телефонной коробки, добытых во время визита ремонтной бригады Telecom либо законным способом, либо в обмен на упаковку пива.

Фрикер рылся в щитке, пока не находил чью-нибудь телефонную линию. Он оголял кабель и прилаживал пару зажимов-крокодилов. Если ему надо было позвонить, он тут же делал это при помощи портативного телефонного устройства, позаимствованного, купленного или украденного у того же Telecom. Если он хотел позвонить на другой компьютер, а не по телефону, ему нужно было протянуть телефонную линию до своей машины. Длинный кабель протягивался к фургону, в котором сидели еще четверо сгорающих от нетерпения молодых людей в окружении как попало расставленного невообразимого количества аппаратуры. Теперь им уже не надо было часами торчать рядом со щитком, рискуя вызвать подозрительный взгляд местного жителя, выгуливающего свою собаку посреди ночи.

Фрикер протягивал кабель вдоль улицы и, по возможности, за угол. Он проводил его в фургон и подключал к истосковавшемуся модему. По меньшей мере один из пятерки был достаточно опытен в обращении с электронным оборудованием, чтобы запитать компьютер и модем от автомобильного аккумулятора. Phreakers Five теперь могла звонить на любой компьютер, и никому не удалось бы их

---

p59

Частный автоматический вспомогательный коммутатор.

p60

Пятерка фрикеров.

выследить и прислать им счет. Он будет фигурировать только на телефонных квитанциях какого-нибудь местного бедняги. В то время Telecom не детализировал телефонные счета. Конечно, было не слишком интересно мотаться по окраинам посреди ночи в фургоне, битком набитом компьютерами, зажимами-крокодилами и адаптерами к аккумулятору, но это не имело значения. В действительности это была такая же захватывающая шпионская операция, как и сам тогдашний хакинг. В глазах фрикеров это было круто. Кроме того, это было забавно.

Craig Bowen не особенно задумывался о стиле фрикинга Phreakers Five. Успех фрикинга как все более модного времяпрепровождения немного подавлял его. Он считал, что это не требовало технических навыков, необходимых для чистого хакинга. По его мнению, хакинг был исследованием дивного нового мира компьютеров. Фрикинг был вроде как недостойн честного доброго хакера. Иногда это принижало статус предстоящей задачи.

Теперь он видел необходимость сохранения принципов настоящего хакинга. Многие в андеграунде развивали базовые фрикерские навыки, но такие, как Craig Bowen, всегда считали фрикинг не более чем средством – просто еще один способ попасть из компьютера А в компьютер В, не более того. Тем не менее он все-таки позволил существование дискуссионных секций по фрикингу в частном разделе РІ, но наотрез отказывался предоставлять свою систему для дискуссионных групп по кардингу. Это было табу для Craig Bowen'a, и он с тревогой наблюдал, как некоторые участники подполья начали скатываться от фрикинга к мошенничеству с кредитными картами.

Подобно переходу от хакинга к фрикингу, движение к кардингу было вполне логичной последовательностью. Оно произошло примерно в тот же период 1988 года, и бросалось в глаза, как стайка хихикающих школьников.

Многие фриконы рассматривали кардинг как вид фрикинга. На самом же деле это было гораздо проще, чем возиться с коммутаторами. Ты просто звонил оператору, давал ему чужой номер кредитной карты, чтобы оплатить разговор, и дело в шляпе. Конечно, кредитные карты имели куда больший диапазон действия, нежели оплата международных звонков. Пришествие кардинга означало, что ты мог запросто позвонить своим друзьям в Штаты или Англию и подолгу болтать с ними всеми одновременно – устроить такую штуку с RABX было бы намного сложнее. Были и другие преимущества. Ты мог свободно оплачивать этой кредиткой разные товары. Делать покупки по почте.

Рассказывают, что один из подпольщиков, известный под хэндлом Ivan Trotsky, заказал по краденной кредитной карте товаров из США на сумму \$50 000, в том числе и водный мотоцикл, который безнадежно ржавел где-то в австралийских доках. Таможенники не принимали кредитные карты для оплаты пошлины. Но, если верить слухам, в других случаях Trotsky везло больше. Это был упорный хакер, который приклеил на свой монитор портреты Маркса и Ленина и старался распространить семена коммунистической доктрины в среде андеграунда. Парадоксально, но он делил свое свободное время между участием в митингах коммунистической партии Австралии и охотой на уток. По словам одного хакера, личный вклад Trotsky в свержение капиталистического порядка состоял в том, что он оплачивал поставку дорогих модемов из США с помощью краденых кредитных карт. Ходили слухи, что он сделал из этого маленький бизнес, продавая модемы в подполье по \$200 за штуку. Видимо, тот факт, что он был частью мировой революции, предоставил в его распоряжение весь набор готовых приемов. Членство в партии имело свои преимущества.

Craig Bowen считал, что кардинг ненамного лучше карманной кражи. Хакинг тоже был спорным вопросом с моральной точки зрения, но в 1988 году в нем пока еще не было ничего криминального. Кардинг же был сомнителен и с моральной, и с юридической стороны. Craig Bowen признавал, что многие люди склонны рассматривать хакинг как вид воровства – кражу чужих компьютерных ресурсов, но в их аргументах была и обратная сторона. Что если никто не нуждался в этих компьютерных ресурсах в два часа ночи? До тех пор пока хакер не завладевал навсегда чьей-нибудь собственностью, к хакингу следовало относиться, как к невинной детской шалости, хотя и весьма нахальной. С кардингом дело обстояло иначе.

Еще одна причина, по которой кардинг считался недостойным занятием, заключалась в том, что он требовал технических навыков ваньки-встаньки. Это было не только недостойно большинства приличных хакеров, это еще и привлекало ненужных людей в близкие к хакерам круги. Людей, которые почти или совсем не уважали золотые правила раннего австралийского андеграунда: не наносить вреда компьютерным системам, которые ты взламываешь (не говоря уже об их уничтожении); не изменять информацию в этих системах (за исключением изменения регистрации, чтобы замести следы); делиться информацией с другими. Для большинства ранних австралийских хакеров посещение чьей-то системы было сродни экскурсии в национальный парк. Оставь все в том же виде, как оно было до твоего прихода.

Пока сливки поднимались на вершину хакерской иерархии, на поверхности кардерской среды болталась накипь. Мало кто в андеграунде воплощал это более полно, чем Blue Thunder,<sup>[p61]</sup> который отирался на задворках мельбурнского андеграунда, по крайней мере с 1986 года. Старшие хакеры относились к Blue Blunder,<sup>[p62]</sup> как иногда называли этого типа, с большой издевкой.

Его первое появление в подполье было таким же позорным, как выход дебютантки, которая впервые осторожно спускается по большим ступеням в танцевальный зал, но внезапно спотыкается и кувырком летит на танцпол. Он повздорил с великой герцогиней андеграунда Мельбурна.

Real Article<sup>[p63]</sup> занимала особое место в иерархии подполья. Для его членов Real Article была женщиной, возможно единственной, которая играла заметную роль в раннем австралийском андеграунде. Хотя она не взламывала компьютеров, она очень много знала о них. Она запустила Real Connection, популярную среди завсегдатаев РІ электронную доску объявлений. Она не была чьей-то сестрой, то появлявшейся в поисках бой-френда, то снова исчезавшей из виду. Она была старше. Она была хороша собой. Она была замужем, и у нее были дети. Она пользовалась авторитетом в хакерском сообществе, с ее мнением считались все.

Показателем уважения, которым она пользовалась, может служить тот факт, что участники Н.А.С.К. пригласили ее в свой клуб избранных в качестве почетного члена. Может быть, это случилось из-за того, что она запустила популярную доску объявлений. Но скорее всего, это произошло потому, что при всех своих наклонностях к блефу и похвальбе, хакеры оставались молодыми людьми с типичными молодежными проблемами. Будучи мудрее и старше, Real Article знала, как с сочувствием выслушать их. Она была женщиной и не была хакером, поэтому оставалась в стороне от иерархических проблем мужского эго, которые невозможно обсуждать с равным. Она стала кем-то вроде матери для новорожденного хакерского сообщества, но все же она была достаточно молода, чтобы избежать назидательных ловушек, в которые попадали родители, пытаясь образумить детей.

Real Article и Blue Thunder вступили в партнерские отношения, познакомившись на BBS в начале 1986 года. Blue Thunder, тогда еще ученик старших классов, в доске объявлений просто скучал, и Real Article допустила его к участию в управлении системой. Сначала партнерство работало. Blue Thunder обычно приносил ей школьные сочинения, чтобы она прочла их и исправила ошибки. Но немного времени спустя партнерство развалилось. Real Article не понравилось стремление Blue Thunder'а к тому, чтобы использовать ее BBS в качестве источника получения информации от других хакеров. Он просто кидал их самым наглым образом, используя самую примитивную стратегию: убеждал хакера зарегистрироваться и оставить на хранение в BBS важную хакерскую информацию, затем похищал эту информацию и выбрасывал хакера из его собственной учетной записи. Сделав это, Blue Thunder получал всю их славу: он мог преспокойно заявить, что все похищенные хакерские секреты принадлежат только ему. По мнению Real Article, такое поведение было не только недопустимо, оно было аморально. Она разорвала отношения с Blue Thunder и исключила его из своей BBS.

Через некоторое время Real Article стали донимать назойливыми телефонными звонками в четыре часа утра. Они не прекращались. Ровно в четыре каждую ночь. Голос в трубке был синтезирован на компьютере. За этим поступало изображение пулемета, отпечатанное на ее дешевом матричном принтере Commodore ASCII, подключенном к ее почтовому ящику. Дальше следовало угрожающее послание в духе: «Если вы хотите сохранить детям жизнь, выведите их из дома».

Потом был кирпич, влетевший в ее окно. Он вдребезги разнес ее телевизор. Кроме того, однажды утром она проснулась и обнаружила, что ее телефонная линия отключена. Кто-то отыскал кабель Telecom, висящий над дорогой, и вырезал из него метр. Это означало, что вся улица осталась без телефонной связи.

Real Article склонялась к тому, чтобы обвинить в этих проделках трусливых подростков с бунтующим эго, но чаша ее терпения переполнилась. Она позвонила в службу безопасности Telecom, которая установила на ее телефонной линии определитель номера, чтобы проследить назойливые ночные звонки. Она подозревала, что это дело рук Blue Thunder'а, но ей так и не удалось это дока-

---

p61

Голубой гром.

p62

Голубой промах.

p63

Настоящая вещь.

зять. В конце концов звонки прекратились. Она поделилась своими подозрениями с другими членами андеграунда. Жалкие остатки репутации Blue Chunder'a, [\[p64\]](#) как теперь его стали называть, были напроочь уничтожены.

Пока его приятели пользователи BBS придерживались невысокого мнения о его технических способностях, Blue Thunder обычно пребывал в полумраке, вынужденный проводить свое время в андеграунде, путаясь под ногами аристократов хакинга. Но зарождение кардинга стало для него счастливым случаем. Он пустился в кардинг во все тяжкие, настолько тяжкие, что вскоре был арестован.

Все в андеграунде признавали, что ему есть за что ответить – всем были известны его аморальные взгляды и безудержное хвастовство якобы совершенными подвигами. Один уважаемый хакер сказал: «Казалось, ему нравится мысль о том, что его могут арестовать. Он говорил людям, что работает на кредитный союз и украл кучу номеров кредитных карточек. Он продавал информацию вроде учетных записей разных систем, хотел нажиться». Вместе с еще одним кардером он якобы послал букет цветов в отдел полиции по борьбе с мошенниками, заплатив за него по номеру краденной кредитной карты.

31 августа 1988 года Blue Thunder'у было предъявлено 22 обвинения в Городском суде Мельбурна. Но ему удалось отвести или объединить большинство обвинений. Кончилось тем, что он признал себя виновным по пяти пунктам, включая мошенничество и кражу. Real Article сидела на последнем ряду в зале суда и наблюдала за процессом. Blue Thunder явно очень нервничал по поводу возможного приговора. Она рассказывала, что Blue Thunder подошел к ней во время обеденного перерыва и спросил, не могла бы она стать свидетелем защиты. Real Article посмотрела ему в глаза и сказала: «Не думаю, чтобы ты действительно этого хотел». Он получил 200 часов общественных работ и штраф в \$706.

Craig Bowen был не в восторге от того, куда вело направление андеграунда, воплощенное в лице Blue Thunder'a. По его мнению, Chunder и Trotsky были паршивыми овцами в здоровом стаде. Они стали первыми признаками неприятного сползания к продаже информации. А это, возможно, было самым строгим табу. Это было грязно. Это было низко. Это годилось для преступников, а не для исследователей. Компьютерный андеграунд Австралии начал терять свое свежее невинное лицо. Где-то посередине всех этих событий в мельбурнском андеграунде появился новый игрок. Его звали Стюарт Гилл [Stewart Gill], он входил в группу под названием Hackwatch. [\[p65\]](#)

Craig Bowen познакомился со Стюартом через Кевина Фицджеральда [Kevin Fitzgerald], известного местного комментатора хакерства, который основал Chisholm Institute of Technology's Computer Abuse Research Bureau. [\[p66\]](#) Позже оно было преобразовано в Australian Computer Abuse Research Bureau. [\[p67\]](#) Просмотрев газетные статьи, цитирующие Фицджеральда, Craig Bowen решил позвонить этому человеку, хотя многие в андеграунде считали его охотником за хакерами. Почему нет? В Австралии пока не было законов против хакинга, поэтому Craig Bowen не слишком волновался. Кроме того, он хотел лично познакомиться с врагом. Никто в австралийском подполье не делал этого раньше, и Craig Bowen решил, что сейчас самое время. Он решил завязать отношения прямо с Фицджеральдом и показать ему, что представляют собой хакеры. Они начали периодически общаться по телефону.

В это же время Craig Bowen познакомился со Стюартом Гиллом, который сказал, что он работает с Фицджеральдом.<sup>21</sup> Вскоре после этого Гилл начал посещать PI. Иногда Craig Bowen лично бывал у Гилла в Маунт-Марте, где тот жил вместе со своими дядей и тетей. В доме Стюарта было полно компьютерного оборудования плюс штабеля коробок с литературой в гараже.

---

p64

Голубой брюзга.

p65

Хакстража.

p66

Исследовательское бюро компьютерных злоупотреблений Чисхольмского технологического института.

p67

Австралийское исследовательское бюро компьютерных злоупотреблений.

<sup>21</sup> Стюарт Гилл подробно описан в книге «Operation Iceberg: Investigation of Leaked Confidential Police Information and Related Matters», издано по решению Законодательного собрания Виктории в октябре 1993 года.

– О, привет, Пол! – сказал пожилой дядя Гилла, увидев пару приятелей.

Как только старик уковылял прочь, Гилл сказал Craig Bowen'у:

– Не волнуйся насчет старика Эрика. Это у него с войны. Сегодня он думает, что я Пол, завтра это будет кто-то еще.

Craig Bowen понимающе кивнул.

У Стюарта Гилла было много странностей, и у всех вроде бы находилось рациональное объяснение, хотя эти объяснения никогда не давали полного ответа на вопрос.

Ему было далеко за тридцать, он был намного старше и гораздо опытнее хакера. У него была очень-очень бледная кожа, такого нездорового оттенка, будто он никогда в своей жизни не бывал на солнце.

Гилл ввел Craig Bowen'а в свою жизнь. Вскоре он сказал молодому хакеру, что не только руководит Hackwatch, но и занимается настоящей разведывательной деятельностью. На Австралийскую федеральную полицию. На ASIO.<sup>[p68]</sup> На Национальное криминальное управление. На Полицейское бюро криминальной разведки штата Виктория. Он показал Craig Bowen'у секретные компьютерные файлы, но прежде продемонстрировал ему специальный бланк – явно законный документ, требующий неразглашения некоторых видов официальной секретной деятельности.

Craig Bowen был впечатлен. Еще бы! Мир плаща и кинжала Гилла был сродни самому интересному мальчишескому приключению. Он был обширнее и интереснее, чем хакинг. Стюарт был странноватым, но это было частью его игры.

Как в тот раз, когда они вместе ездили в Сэйл перед Рождеством 1988 года. Гилл сказал Craig Bowen'у, что ему нужно уехать из города – какие-то подозрительные личности преследовали его. Он не умел водить, так не мог ли Craig Bowen помочь? Конечно, нет проблем. Они сняли в мотеле одну комнату на двоих, оплаченную Гиллом.

Поскольку это было накануне Рождества, Гилл сказал Craig Bowen'у, что он приготовил для него пару подарков. Первый – руководство по фитнесу Джона Траволты. Когда Craig Bowen развернул второй, он слегка опешил. Это были красные мужские трусики-стринги. В то время у парня не было подружки – возможно, Стюарт хотел помочь ему найти девушку.

– О, спасибо! – сказал Craig Bowen немного смущенно.

– Рад, что тебе понравилось, – сказал Стюарт. – Давай-ка, примерь.

– Примерить? – юноша смутился еще больше.

– Ну да, посмотрим, как сидят. Давай.

– Гм, ну ладно.

Craig Bowen колебался. Он не хотел показаться грубияном. Это была странная просьба, но ему раньше никогда не дарили стринги, и он не знал, как вести себя в таких случаях. В конце концов, если кто-то дарит тебе джемпер, совершенно нормально, если он просит тебя примерить его прямо на месте, чтобы посмотреть, подходит ли тебе подарок.

И он примерил.

– Да, тебе идут, – спокойно сказал Стюарт и отвернулся. Craig Bowen почувствовал облегчение. Он переоделся в свою одежду.

Этой ночью, как и многими другими ночами во время их путешествий или ночных визитов в дом дяди Стюарта, он ложился в постель, удивляясь таинственности своего нового друга.

У Стюарта явно были «не все дома», но ему, похоже, нравились девушки, поэтому Craig Bowen был уверен, что не интересуется Стюарта в этом отношении. Стюарт хвастал, что у него была связь с газетной репортершей, и всегда не прочь был поболтать с девушкой в видеомагазине.

Craig Bowen постарался не преувеличивать странного поведения Стюарта, так как хотел забыть об эксцентричности своего нового друга, чтобы сохранить отношения. Вскоре Стюарт попросил хакера разрешить ему доступ в PI. Неограниченный доступ.

Эта мысль внушала парню беспокойство. Но Стюарт был так убедителен. Как он сможет продолжить свою жизненно важную разведдеятельность без доступа в самый важный хакерский сайт в Виктории? Кроме того, Стюарт Гилл из Hackwatch не собирался преследовать невинных хакеров, таких как Craig Bowen. Фактически он мог защитить хакера, если дело дойдет до полиции. На самом деле Стюарту нужны были мошенники-кардеры. Ведь Craig Bowen не стал бы покрывать таких людей?

Стюарт, казалось, противоречил себе, так нелестно высказываясь против кардинга и в то же время поддерживая близкие отношения с Trotsky. Конечно, полагал Craig Bowen, были секреты, которых Стюарт не мог раскрыть – просто не имел права объяснять некоторые вещи из-за своей разведывательной работы.

Craig Bowen согласился.

Но, думая о Стюарте Гилле в полной безопасности своей мальчишеской комнаты, Craig Bowen, конечно, не мог знать о том, что терял андеграунд в эти минуты. Если бы он мог представить себе следующие несколько лет – полицейские рейды, расследования омбудсмена,<sup>[p69]</sup> потоки газетных статей и судебные дела, – то, вероятно, сейчас же выключил бы навсегда свои любимые PI и Zen.

### 3

#### Американский связной

*Если армия США согласно кивает,  
Это шаг назад для твоей страны.*

**Песня «US Forces», альбом «10, 9, 8, 7, 6, 5, 4, 3, 2, 1» группы Midnight Oil<sup>22</sup>**

У Force был секрет. Parmaster хотел узнать его.

Как большинство хакеров, Parmaster не просто хотел узнать секрет, он нуждался в нем. Он был в том особенном состоянии, знакомом каждому настоящему хакеру, когда ты способен на все, чтобы получить необходимую информацию. Он сходил сума.

Само собой, Parmaster не впервые так жаждал информации. И ему самому, и Force было известно все о такой безрассудной страсти. Это часто бывает с истинными хакерами. Им не по нраву подбирать случайные осколки информации здесь и там. Как только они узнают, что где-то появились сведения о какой-то особенной системе, о том, что в нее имеется замаскированный вход, они незамедлительно пускаются на их поиски. Именно этим занимался Par. Он решил преследовать Force до тех пор, пока не получит желаемое.

Это началось вполне безобидно, как праздная беседа двух гигантов компьютерного андеграунда в первой половине 1988 года. Force, известный австралийский хакер, завсегдатай эксклюзивной BBS Realm в Мельбурне, общался в немецком чате с Par'ом, американским мастером сети X.25. Никто из них в эту минуту не находился в Германии, но там был Altos.

Компьютерные системы Altos в Гамбурге имели на одной из своих машин функцию конференции, известную как Altos Chat. Можно было позвонить откуда угодно в коммуникационную сеть данных X.25, и компьютерная компания позволяла вам подключиться. После подключения и введения определенной последовательности команд немецкая машина давала вам возможность поговорить посредством монитора в режиме реального времени с тем, кто был онлайн. Пока остальная часть компьютерной системы компании корпела над решением повседневных задач, этот уголок машины был отведен для живого онлайн-чатинга. Совершенно бесплатно. Это было похоже на зачатки Internet Relay Chat. Компания наверняка и в мыслях не держала, что ее система может стать местом встречи самых серьезных хакеров планеты, но именно так все и случилось.

Altos был первым значительным международным чат-каналом, и для многих хакеров это была презабавная штука. Умелые хакеры путешествовали по компьютерным сетям всего мира. Иногда они сталкивались друг с другом в онлайн и обменивались последними сплетнями. Изредка они регистрировались в иностранных BBS, помещая там свою информацию. Но Altos был совсем другое дело. Если нелегальные BBS могли исчезнуть раз и навсегда в один прекрасный момент, то Altos всегда был на месте. Он был живой. Он предоставлял мгновенные соединения с десятками хакеров из самых экзотических стран. Италия. Канада. Франция. Англия. Израиль. США. И все эти люди не только разделяли твой интерес к компьютерным сетям, но и испытывали огромное презрение к власти любого уровня. Моментальная переписка с товарищами по духу.

При этом Altos был более труднодоступен, чем обычная подпольная BBS. Хакеры, желающие в него попасть, могли столкнуться с трудностями, связанными с режимом оплаты времени в сетях

---

p69

Омбудсмен – чиновник, рассматривающий жалобы граждан на правительственных служащих.

<sup>22</sup> Слова и музыка: Peter Garrett/James Moginie. © Copyright 1982 Sprint Music. Administered for the World-Warner/Chapell Music Australia Pty Ltd. Used by Permission.



X.25. Некоторые системы в сети осуществляли соединение за счет вызываемого абонента вроде номера 1-800, но в других, например в Altos, это не практиковалось. Чтобы попасть в Altos, был нужен идентификатор пользователя сети, NUI, [p70] который выполнял функцию номера телефонной карты для сети X.25. С помощью NUI и оплачивалось сетевое время. Либо нужно было иметь доступ к системе вроде Minerva, которая автоматически оплачивала счета за все совершенные соединения.

Сети X.25 во многом отличаются от Интернета, получившего распространение гораздо позже. Сети X.25 используют другие коммуникационные протоколы, и в отличие от Интернета на пользовательском уровне они применяют не буквенные, а цифровые адреса. Каждый пакет данных, путешествующий по сети, должен находиться в специальном конверте. «Письмо», следующее по сети X.25, должно иметь на своем конверте «штемпель» X.25, а не Интернета.

Сети X.25 контролировались несколькими сильными игроками, такими как Telenet и Tymnet, тогда как современный Интернет, напротив, представляет собой разрозненный набор множества мелких и средних сайтов.

Altos объединил международный хакерский мир, как никакая другая сила. Делясь информацией о компьютерах и сетях своих стран, хакеры помогали друг другу продвигаться все дальше и дальше. Австралийцы пользовались заслуженным уважением на Altos. Тем более что у них был DEFCON, программа, картографирующая не нанесенные на карту сети и сканирующая учетные записи в этих сетях. Force написал DEFCON, взяв за основу простую автоматическую сканер-программу, представленную ему его другом и учителем Craig Bowen'ом (Thunderbird).

Подобно телефонным системам, сети X.25 имели большое количество «телефонных номеров», которые назывались адресами пользователей сети, NUA. [p71] Большинство из них были недействительны. Они попросту еще не были закреплены за кем бы то ни было. Чтобы взломать компьютеры в сети, нужно было сначала найти эти адреса. Для этого требовалось либо узнать о них от приятеля-хакера, либо сканировать. Сканирование – набор на клавиатуре одного адреса за другим – занятие еще менее вдохновляющее, чем искать иголку в стоге сена. 02624-589004-0004. Нужно было менять последнюю цифру с каждой новой попыткой. 0005. 0006. 0007. Пока машина напротив тебя не сдастся.

В конце 1987 или в начале 1988 года Force появился в Pacific Island, чтобы поговорить с Craig Bowen'ом. Force стал жаловаться приятелю на утомительность ручного сканирования.

– А какого черта ты делаешь это вручную? – спросил Craig Bowen. – Тебе надо использовать мою программу.

И он дал Force код к своей простой автоматической сканинг-программе вместе с инструкциями.

Force просмотрел программу и решил, что она послужит отличным стартом для более серьезных вещей. Правда, у программы было одно значительное ограничение. Она могла сканировать только одно соединение в один временной промежуток, то есть только одну ветвь сети.

Меньше чем через три месяца Force создал на основе программы Craig Bowen'а гораздо более мощный DEFCON, который стал бриллиантом в короне австралийских хакеров. С DEFCON хакер мог сканировать пятнадцать, а то и двадцать сетевых адресов одновременно. Он мог дать компьютеру команду нанести на карту части бельгийской, британской или греческой сети X.25, отыскивая компьютеры, подключенные к сети, как почки на ветвях дерева.

В общих чертах разница была примерно такая же, как между использованием простого компьютера, который может выполнять одну операцию за один отрезок времени, и более сложной машиной, где можно одновременно открыть множество окон с разными программами. Даже если ты сам можешь работать только в одном окне, скажем писать письмо, компьютер способен делать вычисления в таблице в окне на заднем плане. Ты можешь перемещаться между различными функциями, которые одновременно отображаются на экране монитора.

Пока DEFCON был занят сканированием, Force мог делать свои дела, например общаться в Altos. Он продолжал совершенствовать DEFCON, написав еще четыре версии программы. Вскоре DEFCON не только сканировал двадцать разных соединений одновременно, но также пытался автоматически взломать все компьютеры, найденные им во время этих соединений. Хотя программа использовала только откровенно ущербные пароли, степень успеха была поистине чудесной, поскольку

---

p70

Network User Identifier.

p71

Network user address.

массированной атаке подвергалось сразу множество адресов. Кроме того, новые сайты и мини-сети возникали так быстро, что службы безопасности неизбежно забывали о предосторожностях, спеша присоединиться к ним. К тому же, пока их адреса не были официально опубликованы, компании считали, что это обеспечивает достаточную защиту.

DEFCON создавал списки тысяч новых компьютерных сайтов. Force запустил сканирование из взломанного компьютера Prime, и через денек-другой у него на выходе был файл с 6000 адресов в разных сетях. Он внимательно исследовал список и выбрал сайты, которые привлекли его внимание. Если его программа находила интересный адрес, он путешествовал по сети X.25 на этот сайт, чтобы попытаться проникнуть в компьютер по этому адресу. Порой DEFCON самостоятельно проникал в машину, используя легкодоступный пароль. В этом случае адрес, имя учетной записи и пароль ждали Force у входа. Ему нужно было только совершить небольшую прогулку.

Все в Altos хотели заполучить DEFCON, но Force отказывался делиться программой. Он не хотел, чтобы другие хакеры окучивали девственные сети. Даже Eric Bloodaxe, [\[p72\]](#) один из лидеров престижнейшей американской хакерской группы Legion of Doom (LOD), [\[p73\]](#) получил от Force отказ, когда попросил у него DEFCON. Eric позаимствовал свой хэндл у короля викингов, чья ставка была в Англии на месте нынешнего города Йорка. Хотя Eric дружил с австралийскими хакерами, Force предпочел сохранить свое сокровище. Он ни за что не хотел выпускать его из рук.

Но в тот судьбоносный день в 1988 году Par хотел не DEFCON. Ему нужен был секрет, который только что открыл Force, но хранил его пуще зеницы ока. Австралиец не собирался выдавать этот секрет ни Par'у, ни кому бы то ни было в целом свете.

Force был скрупулезным хакером. Его комната для хакерского обиталища была невероятно аккуратна. Порядок в комнате был самого безупречного, спартанского свойства. В ней располагались несколько тщательно расставленных образцов минималистской мебели: черная лакированная металлическая кровать, модный черный прикроватный столик и одинокая картина на стене – постер фотографии молнии – в раме под стеклом. Большую часть комнаты занимал серо-голубой рабочий стол с полкой, на которой покоились компьютер, принтер и аккуратная стопка распечаток. Замыкал список мебели книжный шкаф, где хранилась впечатляющая коллекция фэнтези, включая, кажется, все, что когда-либо было написано Дэвидом Эддингсом. [\[p74\]](#) Нижние полки приютили всевозможные труды по химии и программированию. Награда по химии гордо красовалась на полке, заполненной книгами из серии «Башни и Драконы». [\[p75\]](#)

Он хранил свои хакерские записи в пластиковых папках, сложенных в полном порядке на нижней полке книжного шкафа. Каждая страница записей, распечатанная и снабженная краткими и четкими рукописными пометками, имела собственную пластиковую обложку для защиты от пыли и пятен.

Force считал, что будет непродуктивно выпустить на волю программу DEFCON, в результате чего десять человек в разное время будут сканировать одну и ту же систему. Это будет пустой тратой времени и ресурсов. Более того, это затруднило бы доступ к основным сайтам X.25 в Австралии, таким как Minerva. Сканирование было тем видом деятельности, который наверняка привлек бы внимание системного администратора, который в конце концов уничтожил бы учетную запись. Чем больше народу будет сканировать, тем больше учетных записей погибнет, следовательно, тем меньше возможностей для доступа в сеть останется у австралийских хакеров. Поэтому Force наотрез от-

---

p72

Эрик Кровавый Топор.

p73

Легион Страшного суда.

Doom (англ.) – судьба; роковой конец; приговор; Страшный суд.

Следует иметь в виду, что компьютерная игра Doom появилась только в 1993 г.

p74

Дэвид Эддингс (р. 1931) – автор вполне традиционных и без особых претензий на оригинальность серий романов в жанре фэнтези «Элениа», «Белгариад», «Маллореон» и др.

p75

«Dungeons & Dragons» («Башни и Драконы») – игровая система, на которой основываются настольные и компьютерные игры, книги и т. д. Система поддерживается фирмой Wizards of the Coast, Inc. (дочерняя компания Hasbro, Inc.), которая поддерживает также «Magic: The Gathering» и другие игровые системы.

казывался предоставлять DEFCON хакерам за пределами Realm. Этот факт стал одним из показателей мощи Realm.

Сканирование с помощью DEFCON означало использование Netlink, программы, которую редко применяли легальные пользователи. Охотясь за хакерами, админ мог поискать народ в Netlink либо просто проверить, к какой системе подключился пользователь. Например, если хакер подключался к Altos прямо через Minerva, а не через какой-нибудь серьезный перевалочный пункт вроде другой корпоративной машины за океаном, он должен был готовиться к тому, что админ Minerva уничтожит его учетную запись.

DEFCON был революционной программой для своего времени, которую нелегко было воспроизвести. Он был написан для компьютеров Prime. Немногие хакеры умели писать программы для Prime. Откровенно говоря, изучение способов программирования больших коммерческих машин было непомерно трудным делом для большинства хакеров. Трудно было даже достать учебники по системному программированию. Многие большие компании берегли такую литературу почти как секреты фирмы. Конечно, если ты покупал систему за \$100 000, компания снабжала тебя набором учебников, но такой вариант лежал вне возможностей подростка-хакера. Большинство информации хранилось в секрете производителями компьютеров, большими компаниями-покупателями систем, системными администраторами и даже университетами.

Обучение онлайн шло медленно и почти так же трудно. Большинство хакеров использовало модемы на 300 или на 1200 бод.<sup>[p76]</sup> В принципе любой доступ к таким большим, дорогим машинам являлся незаконным. Каждая минута онлайн была рискованным делом. В школах никогда не водилось таких дорогих устройств. Хотя во многих университетах и стояли такие системы, но, как правило, администраторы были не особенно щедры, распределяя машинное время среди студентов. В большинстве случаев обучающиеся на факультете компьютерных наук получали доступ к большим машинам только на втором курсе. Но даже тогда сто процентов студенческих учетных записей помещались в самых старых и медленных машинах. А если ты не был студентом-компьютерщиком, можно было и вовсе не помышлять об этом. Удовлетворение твоего интеллектуального любопытства к системам VMS так и осталось бы несбыточной мечтой.

Даже если тебе и удавалось обойти все препятствия и получить некоторый опыт программирования в системах VMS, ты мог получить доступ в крайне ограниченное число машин отдельно взятой сети. Сети X.25 имеют дело с огромным количеством машин, использующих самые разные операционные системы. Во многих, таких как Prime, недостаточно было интуиции – их нужно было знать. Если ты хотя бы немного знал VMS и мог разобраться в машине Prime, ты мог считаться героем.

Если же ты принадлежал к клану хакеров вроде Realm, то в этом случае мог позвонить на BBS и оставить послание: «Эй, я нашел реальную систему Primos по такому-то адресу. Проблемы с попыткой определить netlink-параметры команды. Есть идеи?». И кто-нибудь из твоей группы спешил на помощь.

Force постарался собрать в Realm особую группу из лучших хакеров Австралии, каждый из которых был экспертом в своей области. Сам Force был асом в компьютерах Prime.

Хотя Force не хотел давать DEFCON никому за пределами Realm, он не был так уж несговорчив. Если ты не входил в братство, но знал об интересной системе и хотел ее расколоть, он мог сканировать ее для тебя. Обычно Force сканировал адреса пользователей сети, такие как NUA. Он давал тебе копию NUA и обязательно делал еще одну копию для Realm. *Это* было продуктивно. Любимым проектом Force было составление базы данных систем и сетей для Realm, так что он просто добавлял к ней новую информацию.

Force с величайшей страстью отдавался составлению карты новых сетей, которые добавлялись на общий план сети X.25 непрерывно. Большая корпорация вроде BHP<sup>[p77]</sup> могла создать свою собственную мини-сеть, соединяющую ее офисы в Западной Австралии, Квинсленде, Виктории и Великобритании. Эта мини-сеть могла быть подключена к особой сети X.25, например Austrac. Войди в сеть Austrac, и у тебя появится шанс попасть в любой из сайтов компании.

Исследование всех этих не нанесенных на карту территорий отнимало большую часть времени

---

p76

Бод – количество элементов сигнала, переданных модемом за секунду; примерно эквивалентно бит/сек.

p77

BHP – транснациональная корпорация со штаб-квартирой в Австралии, специализирующаяся на добыче полезных ископаемых

Forge. Это было настоящее приключение – на бреющем полете находить новые сети и тщательно воссоздавать картину постоянно растущей паутины. Он вычерчивал детальные рисунки и диаграммы, наглядно показывающие, как новая часть сети подключена ко всей сети. Возможно, это было продиктовано его стремлением к порядку или он просто искатель приключений. Но вне зависимости от внутренней мотивации Forge, его карты обеспечивали Realm очередным ценным преимуществом перед другими хакерами.

Когда Forge не был занят составлением карт, он издавал первый в Австралии журнал хакерского андеграунда под названием *Globetrotter* [p78]. Его читало все международное сообщество хакеров. Журнал еще более укрепил лидерство австралийских хакеров в мировом компьютерном подполье.

Но в этот особенный день Par думал не о том, чтобы получить копию *Globetrotter* или попросить Forge отсканировать для него сеть. Он думал об этом секрете. О новом секрете Forge. О секрете, который он стремился узнать больше всего на свете.

Forge запустил DEFCON, который сканировал полдюжины систем, пока он чатился с Par'ом в Altos. В процессе сканирования он обратил внимание на интересное соединение и решил исследовать его. Когда он вошел в незнакомый компьютер, тот обрушил на его машину бесконечные столбцы цифр. Forge сел за стол и принялся смотреть на цифры, бегущие по экрану.

Это было очень странно. Он ничего не делал, не посылал никаких команд на таинственный компьютер, не предпринимал ни малейших попыток взломать машину. А эта штука вывалила на него потоки цифр. Что это был за компьютер? Должен был присутствовать хоть какой-то заголовок, идентифицирующий компьютер, но он промелькнул так быстро в неожиданном обвале данных, что Forge пропустил его.

Forge вернулся в чат с Par'ом в Altos. Он не совсем доверял Par'у, считая, что дружелюбный американец встал на довольно скользкий путь. Но Par был экспертом в сетях X.25 и, возможно, имел какой-то ключ к этим номерам. Кроме того, если окажется, что они представляют собой что-то важное, Forge вовсе не обязан сообщать Par'у, где он их нашел.

– Я только что обнаружил странный адрес. На очень странной системе. Когда я вошел в нее, она вывалила на меня кучу каких-то номеров. Глянь-ка на них.

Forge не знал, что это за номера, зато Par был с ними хорошо знаком.

– Это похоже на кредитные карты, – напечатал он.

– А, ясно, – спокойно набрал Forge.

Par подумал, что обычно разговорчивый австралийский хакер сейчас явно ошеломлен. После короткого молчания заинтересованный Par подтолкнул разговор вперед.

– У меня есть способ проверить, действительны ли эти карты, – вызвался он. – Это потребует времени, но я смогу их проверить, а потом верну тебе.

– Ладно, – Forge колебался. – ОК.

Отделенный от Par'а Тихим океаном, Forge размышлял о неожиданном повороте событий. Если эти кредитные карты действительны, это круто. Не потому, что он собирался использовать их по методу Trotsky. Но Forge мог использовать их для международных звонков при хакерских вылазках в другие страны. Количество карт было просто невероятным. Там было, может быть, десять тысяч карт. Все, что Forge мог подумать: «Черт! Бесплатные соединения до конца моей жизни».

Хакеры, подобные Forge, считали использование чужих карт для международных звонков в компьютерные системы не вполне чистоплотным, но допустимым делом. Авось владелец карты не перестанет пополнять счет. Хакеры считали, что Telecom, который они презирали, скорее всего, пришлет ему счет без детализации, и это их устраивало. Использование кредитных карт для хакинга в корне отличалось от покупки товаров, что было настоящим мошенничеством. А Forge никогда не марал рук подобными делишками.

Он вернулся к захваченным номерам, которые теперь были в его машине. После более тщательного просмотра он обнаружил, что заголовки периодически появляются в списке. Один из них носил название «CitiSaudi».

Он еще раз проверил первую часть сетевого адреса таинственной машины. Из опыта предыдущих сканирований Forge знал, что он принадлежит одному из самых больших банков мира – Citibank.

Обвал данных продолжался почти три часа. После этого Forge показалось, что машина Citibank устала. Перед Forge был только чистый экран, но он сохранил соединение. Он ни за что не хотел по-

терять его. Он предположил, что это было случайное соединение, что на самом деле оно не могло произойти посредством сканирования сети Citibank его программой DEFCON.

Как еще это могло случиться? Само собой, у Citibank не могло быть компьютера, битком набитого номерами кредитных карт, который выворачивался наизнанку всякий раз, как кто-то оказывался рядом и говорил: «Привет!» На таких машинах стоят километровые слои безопасности. У таких машин даже нет пароля. Им не нужны специальные команды, вроде тайного рукопожатия.

Соединения-ошибки время от времени происходят в сетях X.25. Они похожи на ошибки при телефонных звонках. Ты набираешь номер телефона приятеля – и набираешь его правильно, но иногда звонок сбивается с пути в лабиринте спутанных проводов и коммутаторов и попадает на совершенно другой номер. Когда такое случается с хакером в X.25, он немедленно пытается представить, что, черт возьми, происходит, начинает обследовать каждую частицу данных машины в поисках истинного адреса системы. Из-за того, что соединение произошло случайно, он опасается, что у него больше никогда не будет шанса найти эту машину.

Форсе пожертвовал двумя днями школьных занятий, чтобы сохранить соединение и воссоздать маршрут, по которому он пришел к дверям этого компьютера. В этот промежуток времени компьютер Citibank еще несколько раз просыпался, сбрасывал очередную порцию информации и снова засыпал. Сохранение связи было сопряжено с определенным риском. Администратор мог в любой момент засечь Форсе со своего рабочего места. Но в этом случае награда была несоизмеримо выше любого риска.

Для Форсе было обычным делом прогуливать школу ради хакинга. Родители часто говорили ему: «Тебе лучше поменьше сидеть за компьютером, а то однажды ты ослепнешь». Все же они не слишком волновались, пока их сын преуспевал в школе, не прилагая к этому особых усилий. Начав учиться в старших классах, он попытался убедить учителей, что сможет перескочить через девятый класс. Некоторые возражали. Это оказалось нелегко, но, в конце концов, он выполнил программу девятого класса, пока учился в восьмом.

После того, как Форсе окончательно отключился от компьютера CitiSaudi и хорошенько выспался, он решил проверить, возможно ли снова войти в эту машину. Сначала никто не ответил, но когда он попробовал еще раз, его впустили. Это был тот же болтливый резидент, что открыл ему дверь в первый раз. Несмотря на то, что вся эта система, казалось, работает только в определенные часы, сетевой адрес Citibank был верным. Он снова был там.

Просмотрев свой улов после проникновения в Citibank, он отметил, что последняя порция данных содержит не номера кредитных карт, как предыдущие части. Там были имена людей – восточные имена – и списки оплаченных покупок и услуг. Обед в ресторане. Посещение борделя. Все что угодно. Еще там была цифра, похожая на лимит кредита. У каждого из этих людей были очень-очень большие кредиты. Один шейх и его жена пользовались кредитом в один миллион долларов на каждого. Еще у одного человека был кредит в пять миллионов долларов. Форсе подумал, что с данными что-то не так. Было не похоже, что машина Citibank просто передает данные на другую машину. Это выглядело как текст файла, сброшенного с компьютера на принтер.

Форсе сел к компьютеру и обдумал свое чудесное открытие. Он решил, что такими вещами можно поделиться лишь с несколькими, самыми близкими и проверенными друзьями из Realm. Он скажет Phoenix'у и, может быть, еще одному человеку, но больше никому.

Когда Форсе просмотрел данные еще раз, то почувствовал легкое беспокойство. Citibank был мощным финансовым институтом, который зависел от полной конфиденциальности вкладов своих клиентов. Корпорация потеряет лицо, если новости об открытии Форсе выйдут наружу. И они дорого дадут за то, чтобы достать его. И с внезапной четкостью разряда молнии на фотографии в его комнате мозг Форсе пронзила мысль: «Я играю с огнем».

:)

– Где ты откопал эти номера? – спросил Par у Форсе, когда они снова встретились в Altos.

Форсе промолчал. Par продолжил:

– Я проверил эти карты. Они действительны, – американец был более чем заинтригован. Он хотел этот адрес. Это была страсть. Следующая остановка – таинственная машина. – Ну что, какой у нее адрес?

На этот вопрос Форсе отвечать не собирался. Он был в отличных отношениях с Par'ом, и при случае они легко делились информацией. Но в этой ситуации все могло пойти слишком далеко. Насколько было известно Форсе, Par мог не самым должным образом воспользоваться этой информаци-

ей. Force не знал, занимался ли американец кардингом, но чувствовал, что у того могли быть такие друзья. Поэтому Force отказался сообщить Раг'у, где находится таинственная машина.

Но Раг не собирался так легко сдаваться. Нельзя сказать, что он собирался использовать эти карты, чтобы разжиться халявными деньгами, но эта загадочная машина была суперместом, и это надо было ценить. Force не будет покоя, пока Раг не получит то, что ему нужно. Ничто так не искушает хакера, как легкий аромат информации в вожденной системе, и Раг преследовал Force, пока австралийский хакер на мгновение не расслабился.

В конце концов Force сказал Раг'у очень приблизительно, где сканировал DEFCON, когда на- рвался на машину Citibank. Force указал не улицу, а только название района. DEFCON попал в сеть Citibank через Telenet, большую американскую сеть данных, использующую протоколы X.25. Начальными цифрами адресов для сети Citibank в сети были 223 и 224.

Раг еще какое-то время донимал Force насчет остальной части номера, но австралиец стоял на- смерть. Force был слишком осторожным игроком и слишком разборчивым хакером, чтобы оказаться причастным к возможным выходкам Раг'а. «Ладно, – подумал семнадцатилетний Раг, – обойдусь без тебя». Он прикинул, что в этой сети могло быть тысяч двадцать адресов, за каждым из которых, воз- можно, скрывалась загадочная машина. Но он предположил, что она должна находиться ближе к на- чалу диапазона номеров сети, так как начальные номера обычно использовались в первую очередь, а те, что повыше, как правило, отводились для других, специальных функций сети. Его предположение ограничило вероятное поле поиска до двух тысяч номеров.

Раг приступил к ручному сканированию Global Telecommunications Network (GTN)<sup>[p79]</sup> Citibank в поисках таинственной машины. Используя свое знание сети X.25, он определил, с какого номера начать. Он набрал 22301, 22302, 22303. Один за другим, постепенно двигаясь к 22310000. Час за часом, медленно и упорно, не пропуская ни одного варианта, Раг сканировал ряд внутри сети. Ко- гда ему надоело возиться с 223, он, для разнообразия, продолжал сканирование с 224.

Изнуренный, с помутившимся взглядом после бессонной ночи, Раг чувствовал, что пора завя- зывать. Солнце уже давно залило светом окна его дома в Салинасе, штат Калифорния. Гостиная в доме была настоящей помойкой – пустые смятые пивные банки в беспорядке валялись вокруг его Apple IIe. Раг устроил небольшой перерыв, немного вздремнул. Он прошел по целому списку адре- сов, постучался в каждую дверь, но ничего не произошло. Тем не менее следующие несколько дней он полностью посвятил сканированию сети. Он решил действовать более методично и проверить все заново.

И это произошло. Компьютер Раг'а к чему-то подключился. Он с интересом уставился на экран. Что происходит? Раг проверил адрес. Он был уверен, что уже пробовал его раньше, но не получил ответа. Ситуация выглядела еще более странной. Он напряженно вглядывался в компьютер.

Экран был абсолютно пуст, лишь курсор слабо мерцал в верхнем углу. Что дальше? Что сделал Force, чтобы заставить компьютер спеть свою песню?

Раг попытался нажать кнопку Control и несколько разных букв. Ничего. Может, это все-таки не тот адрес? Он отключил соединение и тщательно записал координаты машины, решив вернуться к нему попозже.

Он подключился к компьютеру в третий раз, но обнаружил тот же раздражающе пустой экран. Теперь он принялся перебирать весь алфавит с клавишей Control.

Control L.

Вот она, магическая команда. Та, что заставила CitiSaudi распахнуть свою таинственную со- кровещницу. Та, что подарила Раг'у всплеск адреналина вместе с тысячами карт. Моментально «живые» деньги затопили экран его монитора. Он оставил компьютер в том же состоянии, чтобы из-влечь из него всю возможную информацию и проанализировать ее. Раг'у пришлось обеспечить свой маленький Apple II достаточным количеством дискет, чтобы собрать всю информацию, которая про-ходила через его 1200-бодовый модем.

Это было великолепно. Раг наслаждался моментом, думая о том, какое счастье будет сказать об этом Force. Эй, австралиец, ты не единственный герой в городе. До встречи в Citibank.

Около часа спустя, когда сброс данных наконец прекратился, Раг остолбенел, осознав, что же такое он нашел. Здесь не было ни единой старой карты. Это были дебетовые карты, принадлежащие очень богатым арабам. Эти люди кинули миллионы долларов на свои банковские счета, с которыми

поддерживали связь с помощью маленького прямоугольного куска пластика. Каждая выплата отражалась в банковском балансе. Один парень купил в Стамбуле Mercedes за \$330 000 – по своей карте. У Раг’а в голове не укладывалось, что для этого можно было использовать кусок пластмассы. Прогулка с таким пластиком по микрорайону придавала совершенно новый смысл выражению «На мой счет!».

Когда кто-то выигрывает в лотерею, он часто хочет разделить удачу с друзьями. Именно это чувство осенило Раг’а. Сначала он показал свою находку соседям по дому. Те подумали, что это круто. Но по-настоящему ее смогли оценить пяток хакеров и фрикеров, которым случилось оказаться на телефонном мосту, когда Раг, мастер сетей X.25, огласил список карт.

С этого дня Раг стал популярным парнем в округе. Он был крут, как Робин Гуд андеграунда. Вскоре все хотели пообщаться с ним. Хакеры из Нью-Йорка. Фрикеры из Вирджинии. И Секретная служба из Сан-Франциско.

:)

Раг не собирался влюбляться в Theorem. [p80] Это вышло случайно, и он не мог найти для своей любви более неудачный объект. Начать с того, что она жила в Швейцарии. Ей было двадцать три, а ему только семнадцать. У нее уже были отношения, да еще с кем – с Electron’ом, одним из лучших австралийских хакеров конца 80-х. Но Раг не мог бороться с самим собой. Она была неотразима, пусть даже они никогда не встречались лично. Theorem не была похожа на других. Она была умной и забавной, но и утонченной, какой может быть только европейская девушка.

Они познакомились в Altos в 1988 году.

Theorem не взламывала компьютеров. Да ей и не нужно было этого делать, пока она могла выходить в Altos через свою учетную запись в старенькой университетской машине. Впервые она попала в Altos 23 декабря 1986 года. Она запомнила дату по двум причинам. Во-первых, она была потрясена мощностью Altos – еще бы, она могла общаться онлайн с десятком людей из разных стран одновременно. Altos стал для нее совершенно новым миром. Во-вторых, в этот день она познакомилась с Electron’ом.

Electron умел насмешить Theorem. Его язвительный бунтарский юмор задел чувствительные струнки ее души. Традиционное швейцарское общество было душным и замкнутым, и Electron стал глотком свежего воздуха. Theorem была швейцаркой, но она совершенно не соответствовала общепринятому штампу. Она ненавидела лыжи, была шести футов ростом, ей нравились компьютеры.

Когда они встретились онлайн, двадцатиднолетняя Theorem находилась на распутье своей жизни. Она провела полтора года в университете, изучая математику. К сожалению, с учебой не ладилось. Она признала очевидное, и второй курс в университете был равносителен первому – все пришлось начинать сначала. Сокурсница привела ее в Altos с университетского компьютера. Вскоре после того, как Theorem познакомилась с Electron’ом, она бросила университет и начала учиться на курсах секретарей. Немного позже она нашла место секретаря в финансовом учреждении.

Theorem и Electron общались в Altos часами. Они говорили обо всем – о жизни, семье, кино и вечеринках и почти не касались самой распространенной в Altos темы хакинга. Однажды Electron набрался смелости и попросил у Theorem номер ее домашнего телефона. Она с удовольствием дала ему номер, и Electron стал звонить ей в Лозанну. Вскоре они все время висели на телефоне.

У семнадцатилетнего Electron’а никогда не было подружки. Ни одна из девушек его школы для среднего класса не обращала на него внимания, когда дело доходило до ухаживаний. А здесь была чудесная, живая девушка (изучавшая математику), доверительно беседующая с ним с мягким французским акцентом. Лучше всего было то, что он действительно ей нравился. Несколько его слов могли заставить ее рассмеяться серебряными колокольчиками.

Когда пришел счет за телефон, в нем стояла цифра в \$1000. Electron тайком изъяс и похоронил его на дне выдвижного ящика стола в своей комнате.

Когда он рассказал об этом Theorem, она предложила свою помощь. Вскоре прибыл чек на \$700. Это очень облегчило объяснения с отцом по поводу повторного счета из Telecom.

Романтические отношения развивались весь 1987 и половину 1988-го. Electron и Theorem об-

менивались любовными письмами и нежными посланиями через 16 000 километров компьютерных сетей, но такой долгий путь не мог быть абсолютно ровным. Как в тот раз, когда Theorem в течение нескольких месяцев тесно общалась с Pengo. Известный немецкий хакер, связанный с немецкой же группой Chaos Computer Club, <sup>[p81]</sup> Pengo также был другом и наставником Electron'a. Но Pengo и Theorem находились на расстоянии короткой поездки на поезде. Она подружилась с Pengo в Altos и в конце концов съездила к нему в гости. Отношения стремительно развивались.

Theorem была честной с Electron'ом, но он чувствовал, что остается что-то недосказанное, что-то скрытое. Даже когда отношения закончились, Theorem с нежностью отзывалась о Pengo, как обычно девушка хранит привязанность своей первой любви, вне зависимости от того, сколько других мужчин побывало в ее постели с тех пор.

Electron был разгневан и уязвлен, но проглотил свою гордость и простил Theorem этот флирт. В конце концов, Pengo сошел со сцены.

Pengo был связан с людьми, которые продавали КГБ американские военные секреты, украденные из компьютеров. Хотя его прямое участие в международном компьютерном шпионаже было ограниченным, он начинал волноваться из-за связанного с ним риска. Его настоящим интересом был хакинг, а не шпионаж. Связь с русскими, к которым он не испытывал никакой симпатии, просто позволяла ему иметь доступ к большим и лучшим компьютерам.

В первой половине 1988 года он добровольно сдался немецким властям. По тогдашним законам Западной Германии гражданин, занимавшийся шпионажем, который явился с повинной, до того как преступление было раскрыто, и тем самым предотвратил нанесение дальнейшего ущерба государству, приобретал иммунитет. Pengo уже арестовывали в декабре 1986-го за использование краденого NUI, и он решил, что если сдастся добровольно, то получит надежду и сможет извлечь выгоду из этой легальной вседозволенности.

К концу года положение Pengo стало ухудшаться, и в марте 1989-го этот двадцатилетний берлинец снова попал под арест, на этот раз вместе с четырьмя другими участниками шпионской игры. История вышла наружу, и в СМИ появилось настоящее имя Pengo. Он не знал, будет ли он осужден и приговорен в связи с этим инцидентом. В общем, Pengo было о чем подумать, кроме высокой швейцарской девушки.

С исчезновением Pengo отношения между Theorem и австралийским хакером стали улучшаться. Пока не появился Раг.

Theorem и Раг начали довольно невинно. Она была одной из немногочисленных девушек в международных хакерских и фрикерских кругах, в частности в Altos, и к ней относились по-разному. У нее было много друзей мужского пола в немецком чате. Парни часто доверяли ей то, в чем никогда бы не признались друг другу. Они искали у нее совета. Иногда ей казалось, что она меняет маски – мать, подруга, психиатр, когда общается с парнями в Altos.

У Раг'a были сложности с его онлайн-подругой Норой. Раг приехал из Калифорнии в Нью-Йорк, чтобы лично познакомиться с ней. Но когда он без предупреждения прибыл в изнурительную духоту нью-йоркского лета, ее родители-китайцы неадекватно восприняли это неожиданное появление. Между Раг и Норой были и другие трения. В Altos и по телефону все шло отлично, но при личной встрече их отношения не имели успеха.

Раг уже знал, что виртуальные взаимоотношения с помощью электронного медиума, который игнорировал телесное в человеке, часто оборачивались крушением надежд.

Обычно Раг зависал на телефонном мосту с другим австралийским членом Realm по прозвищу Phoenix и с веселой девушкой из Южной Калифорнии. Tammi, фрикер по случаю, обладала яркой индивидуальностью и отличным чувством юмора. После бесконечных часов за разговорами они с Phoenix'ом оказались охвачены пылким взаимным чувством. Во фрикерском подполье их считали в некотором роде виртуальным единством. Tammi даже пригласила Phoenix'a как-нибудь приехать к ней в гости. Однажды Tammi решила приехать в гости к Раг'у в Монтеррей. Ее появление стало для него шоком.

Tammi описывала себя Phoenix'у как голубоглазую блондинку из Калифорнии. Раг знал, что Phoenix представлял ее себе как типичную пляжную куклу в бикини из Лос-Анджелеса.

Его восприятие базировалось на представлении иностранца о культуре Южной Калифорнии. Молочные реки, кисельные берега. Родина Beach Boys и телесериалов типа «Ангелы Чарли».



Когда Par увидел Tammi, он понял, что им с Phoenix'ом не суждено быть вместе. У Tammi действительно были голубые глаза и светлые волосы. Но она не сочла нужным упомянуть, что весила около 300 фунтов.<sup>[p82]</sup> у нее было невзрачное лицо и какой-то базарный стиль общения. Par действительно симпатизировал Tammi, но никак не мог выкинуть из головы злую фразу «белая шваль».<sup>[p83]</sup> Он гнал и отталкивал ее прочь, но она словно застряла в его мыслях. Он должен был сказать Electron'у правду о Tammi.

Так что Par прекрасно знал о том, как реальная жизнь может разрушить виртуальные отношения.

Оставив позади Нью-Йорк и Нору, Par переправился через реку в Нью-Джерси, чтобы остановиться у друга по имени Byteman.<sup>[p84]</sup> который входил в хакерскую группу, специализирующуюся на взломе компьютерных систем Bell Communications Research (Bellcore).<sup>[p85]</sup> Бюро начало свою деятельность в начале 1984 года после разделения американской телефонной монополии Bell Systems. До раскола материнская компания Bell Systems, American Telephone & Telegraph (AT&T), взлелеяла все самое лучшее и передовое в Bell Labs. За время их существования из Bell Labs вышло по меньшей мере семь Нобелевских лауреатов и множество научных достижений. Все это делало Bellcore отличной мишенью для хакера, желающего доказать свою доблесть.

Обычно Byteman болтал с Theorem в Altos, но в конце концов он связался с ней по телефону. Par, должно быть, выглядел безутешным, потому что как-то раз, разговаривая с Theorem, Byteman вдруг сказал ей: «Эй, хочешь поговорить с моим другом?». Theorem сказала: «Конечно», и Byteman протянул трубку Par'у. Они разговаривали минут двадцать.

После этого случая они часто общались в Altos и по телефону. Затем, когда Par вернулся в Калифорнию, Theorem попыталась утешить его после невеселого опыта с Норой. К середине 1988 года они окончательно и страстно полюбили друг друга.

Electron, нерегулярный участник Realm, отнесся к этой новости без особого восторга. Не всем в Altos нравился Electron. Он мог быть неприятным и язвительным, когда ему этого хотелось, но он был асом хакинга международного уровня, и все прислушивались к нему. Увлеченный, креативный, невероятно быстрый, Electron внушал уважение, и Par еще и поэтому чувствовал себя неловко.

Когда Theorem сообщила Electron'у ужасную новость в частном разговоре онлайн, он ворвался в общий чат и обругал американского хакера в главной секции чата на Altos на виду у всех.

Par выдержал удар и не стал отвечать. А что еще он мог сделать? Он знал, что такое страдать. Он сочувствовал парню и понимал, что сам повел бы себя так, если бы потерял Theorem. Он знал, что Electron наверняка страдает от ужасного удара по самолюбию. Все считали Theorem и Electron'а половинками единого целого. Они были вместе больше года. Поэтому Par встретил ярость Electron'а спокойно и попытался тактично утешить его.

С тех пор Par почти не общался с Electron'ом. Австралиец продолжал посещать Altos, но стал более замкнутым, во всяком случае, когда Par был рядом. После этого дня Par лишь однажды напикнул на Electron'а на телефонном мосту с группой австралийских хакеров.

Phoenix сказал: «Эй, Electron, Par на связи».

Electron выдержал паузу и спокойно ответил: «В самом деле?» Затем замолчал.

Par не стал пробиваться сквозь молчание Electron'а. В конечном счете Par'у досталось самое главное – девушка.

Par звонил Theorem почти каждый день. Вскоре они принялись строить планы ее приезда в Калифорнию, чтобы наконец увидеться друг с другом лично. Par старался не ждать от этой встречи слишком многого, но вскоре обнаружил, что очень трудно запретить себе с предвкушением думать о предстоящем первом личном свидании. Он дрожал от волнения и нетерпения.

---

p82

Примерно 136 кг.

p83

Презрительное название белых бедняков из южных штатов США.

p84

Человек-Байт.

p85

Исследовательское бюро компании Bell.

«Да, – думал Par, – дела наконец-то пошли в гору».

;)

Прелесть Altos, как и Pacific Island или любой другой BBS, заключалась в том, что хакер мог воспользоваться любой личиной, которая была ему по душе. И он мог делать это в международном масштабе. Сходить в Altos было равносильно посещению бала-маскарада. Любой мог придумать себе новую личность. Социально неадаптивный хакер мог предстать в качестве романтического героя в поисках приключений. А сотрудник службы безопасности мог прикинуться хакером.

Что и сделал 27 октября 1988 года Стив Мэтьюз [Steve Mathews], сотрудник безопасности Telenet. Par как раз был онлайн, болтая со своими друзьями и коллегами-хакерами. В Altos почти никогда не бывало посторонних, тех, кто не принадлежал к завсегдатаям. Само собой, Мэтьюз не стал объявлять, что он из Telenet. Он просто осторожно проскальзывал в Altos и старался выглядеть, как любой другой хакер. Он вступал с хакером в разговор, но предоставлял тому возможность выговориться. Он был здесь, чтобы слушать.

В этот роковой день Par пребывал в самом радужном настроении. У Par'a никогда не водилось много денег, но он всегда был очень щедр с тем, что у него было. Он немного поговорил в Altos с незнакомым хакером, а затем дал ему номер одной из дебитных карт, полученный во время посещения компьютера CitiSaudi. Почему бы и нет? В Altos это было примерно то же самое, что оставить визитку. «The Parmaster – Parameters Par Excellence». [p86]

Par получил это прозвище – Parmaster – в самом начале своей хакерской деятельности. В то время он принадлежал к группе подростков, которые занимались взломом защитных систем копий программного обеспечения Apple IIe, особенно игр. У Par'a был особый дар к решению задач с параметрами систем – это было первым шагом к обходу схем безопасности, установленных производителями. Вожак банды стал звать его «мастер параметров» (Parmaster, сокращенно Par). Когда он перешел к серьезному хакингу и поднабрался опыта в сетях X.25, то сохранил свой хэндл, тем более что тот отлично вписывался в его новое окружение. «Par?» – это обычная команда на контактной площадке X.25, модемном входе в сеть.

– Там, откуда это взято, такого добра полно, – сказал Par незнакомцу. – У меня около четырех тысяч таких карт из системы Citibank.

Стив Мэтьюз снова проверял Altos, когда опять появился Par, раздавая карты направо и налево.

– Я залез внутрь, – признался Par. – Там целая куча новеньких пластиковых карт с действительными номерами. Реально большие счета. Ни одного меньше \$25 000.

Может быть, Par просто болтал языком, желая набить себе цену в Altos? Или он в самом деле пробрался в систему, совершив серьезное преступление? Citibank, Telenet и Секретная служба США так и не узнали этого, потому что службы безопасности начали сжимать кольцо вокруг Par'a до того, как он успел развить по-настоящему бурную деятельность.

Мэтьюз связался с Ларри Уоллесом [Larry Wallace], занимавшимся в отделении Citibank в Сан-Матео (Калифорния) случаями мошенничества. Уоллес проверил карты. Они и правда были действительны. Карты принадлежали Saudi-Arabia Bank в Саудовской Аравии и хранились в базе данных Citibank в Сиу-Фоллз, Южная Дакота. Уоллес выяснил, что Citibank отвечал за полную сохранность этих счетов, будучи напрямую связанным с саудовским банком. Этот факт означал, что он может начать полномасштабное расследование.

7 ноября Уоллес привлек к делу Секретную службу. Четыре дня спустя Уоллес и специальный агент Томас Хольман [Thomas Holman] получили первую конкретную ниточку, побеседовав с Джерри Лайонс [Gerry Lyons] из службы безопасности Pacific Bell в Сан-Франциско.

«Да, – сказала Лайонс следователям, – у меня есть кое-какая информация, может быть, она окажется важной». Она знала все о хакерах и фрикерах. Кроме того, полиция Сан-Хосе недавно арестовала двух парней, которые пытались провести сеанс фрикинга из телефона-автомата. Фрикеры что-то плели о системе Citibank.

Когда агенты появились в Департаменте полиции Сан-Хосе, чтобы встретиться с сержантом Дэйвом Флори [Dave Flory], их ждал еще один приятный сюрприз. У сержанта была записная книжка, набитая именами и телефонами хакеров – он изъял ее во время задержания фрикеров у телефо-

на-автомата. Он также получил запись телефонного разговора фрикеров с Раг'ом – они позвонили ему с тюремного телефона.

Наглые фриеры воспользовались тюремным телефоном, чтобы позвонить на телефонный мост, расположенный в Университете штата Вирджиния. Раг, австралийские хакеры и несколько лучших американских фриеров частенько посещали его. В любой момент на мосту висело 8–10 подпольных деятелей. Фриеры обнаружили, что Раг, как обычно, на месте, и предупредили его. Они сообщили, что его имя и номер телефона есть в записной книжке, захваченной полицией во время ареста.

Казалось, что Раг'а это совершенно не волнует.

– Эй, не суетитесь, – успокоил он их. – Все в норме. Как раз сегодня я отключил телефон и запутал концы.

Но это было не совсем так. Скотт, сосед Раг'а по дому, действительно отключил телефон, который был зарегистрирован на его имя, потому что кто-то постоянно звонил и донимал его дурацкими шутками. Но в этот же день Скотт открыл новый телефонный счет по тому же адресу и на то же имя. Все это очень облегчило работу правоохранительных органов по преследованию таинственного хакера по имени Раг.

Тем временем Ларри Уоллес обзванивал все свои контакты в области безопасности и вытянул еще одну ниточку. Ванда Гэмбл [Wanda Gamble], куратор юго-восточного направления из MCI Investigations в Атланте, оказалась кладезем информации о хакере, называвшем себя Раг. Она умела устанавливать контакты с хакерами и обзавелась целым списком надежных информаторов за время своих расследований хакерских инцидентов. Она сообщила следователям Citibank два номера почтовых ящиков Раг'а и помогла им с предполагаемым номером его телефона.

Номер проверили, и 25 ноября, на следующий день после Дня благодарения, полиция совершила налет на дом Раг'а. Это было ужасно. По меньшей мере четверо полицейских с пистолетами выломали дверь. У одного было даже ружье. Как часто бывает в Штатах, сотрудники частных структур – в этом случае Citibank и Pacific Bell – тоже принимали участие в рейде.

Копы перевернули дом вверх дном в поисках улик. Пытаясь найти спрятанные компьютерные дискеты, они опорожнили коробку с кукурузными хлопьями в раковину на кухне. Они рыскали повсюду, обнаружив даже пустое пространство над потолком в стенном шкафу, о котором никто и не подозревал до их появления.

Они конфисковали компьютер Apple IIe, принтер и модем Раг'а. Для полной уверенности они прихватили справочник Yellow Pages, телефон и новую игру Nintendo, только что купленную Скоттом. Они выгребли огромное количество бумаг, сложенных под журнальным столиком, включая тетрадку Скотта, где он записывал заказы на доставку авиабилетов – Скотт подрабатывал турагентом. Они забрали даже мусор.

Потом они наткнулись на красную коробку из-под обуви, полную компьютерных дискет. Она находилась под аквариумом рядом с компьютером Раг'а.

Они нашли массу улик. Единственное, чего им не хватало – самого Раг'а.

Зато они нашли Скотта и Эда, друзей и соседей Раг'а. Бедняги были совершенно потрясены налетом. Агенты не знали, как выглядит Раг, и не знали его настоящее имя, поэтому, недолго думая, они обвинили Скотта в том, что он и есть Раг. Телефон был зарегистрирован на его имя, и специальный агент Хольман [Holman] даже установил наблюдение за неделю с небольшим до налета, записав номера припаркованного возле дома черного Ford Mustang 1965 года, принадлежавшего Скотту. Спецслужбы были убеждены в том, что это их человек, и Скотт убил уйму времени, пытаясь убедить их в обратном.

И Скотт, и Эд клялись всеми святыми, что они не хакеры, не фриеры и уж, конечно, не Раг. Но они знали, кто такой Раг, и сообщили агентам его настоящее имя. Под мощным прессингом спецслужб Скотт и Эд согласились дать показания в полицейском участке.

В Чикаго, на расстоянии 2700 километров от катастрофы в Южной Калифорнии, Раг с матерью наблюдали, как его тетя в белом подвенечном наряде идет по проходу между скамьями.

Раг лишь однажды позвонил домой Скотту, чтобы передать привет со Среднего Запада – уже после рейда.

– Ну, – спросил Раг у своего соседа, – как дела дома?

– Нормально, – ответил Скотт, – ничего особенного.

Раг смотрел на свой красный рюкзак с мгновенно охватившим его выражением ужаса. Ему казалось, что на автобусной станции Сан-Хосе он выглядит, как павлин в курятнике...

Пребывая в блаженном неведении о налете полиции, случившемся три дня назад, Раг с матерью прилетели в аэропорт Сан-Хосе. Они добрались до автобусной станции, чтобы сесть на Greyhound[*p87*] до Монтеррея. В ожидании автобуса Раг позвонил своей подруге Тамми, чтобы сообщить, что он вернулся.

Любой, кто случайно стоял в очереди к телефону-автомату в этот момент, мог бы заметить удивительную метаморфозу в поведении паренька с каштановыми волосами в одной из кабин. Улыбающееся лицо внезапно сменилось гримасой ужаса. Его кожа стала пепельно-серой. Кровь отхлынула от лица. Глубоко посаженные карие глаза с длинными изящными ресницами, загнутыми кверху, и мягким застенчивым взглядом вдруг невероятно расширились.

Именно в этот момент Тамми рассказывала Раг'у, что в его доме был обыск. Что Скотт и Эд страшно перепугались, когда копы размахивали пистолетами у них перед носом, и дали на него показания в полиции. Что они думают, что их телефон прослушивается. Что Секретная служба охотится за Раг'ом и знает его настоящее имя, что, по ее мнению, на него разосланы ориентировки. Скотт сообщил спецслужбам о красном рюкзаке Раг'а, в котором он всегда носил свои хакерские записи. В нем и хранились распечатки номеров кредитных карт Citibank.

Поэтому Раг стоял и смотрел на свой рюкзак тревожным взглядом. Он сразу же осознал, что спецслужбы будут искать именно этот красный рюкзак. Если они не знают, как он выглядит, они будут просто искать рюкзак.

Рюкзак было не так-то легко спрятать. Распечатки Citibank приближались по размерам к телефонному справочнику. В рюкзаке были еще и дискеты, загруженные номерами карт, и другая важная хакерская информация.

Раг использовал карты для нескольких бесплатных телефонных звонков, но не заказывал по ним никаких водных мотоциклов.

Он доблестно бился с искушением и в конце концов победил, но другие могли не выстоять в этой битве. Раг был уверен, что многие менее щепетильные хакеры могли начать заказывать по картам все подряд. Он был прав. Например, один из таких деятелей попытался послать букет цветов за \$367 своей знакомой в Эль-Пасо, используя номер одной из краденых карт. Так вышло, что кардера угораздило выбрать карту, принадлежавшую старшему администратору саудовского банка, который оказался в офисе, когда был сделан заказ на цветы. Следователь Citibank Ларри Уоллес добавил материал об этом инциденте в свою растущую папку.

Раг подумал о том, что Citibank может попытаться свалить на него любую попытку кардинга. Почему бы нет? Кто поверит семнадцатилетнему хакеру, если он осмелится оспорить такие обвинения? Никто. Раг принял простое решение. Он незаметно отошел к урне в темном углу. «Просканировав» окружающее пространство, Раг залез в красный рюкзак, вытащил оттуда толстую пачку распечаток Citibank и запихал их в урну. Сверху он прикрыл их каким-то мусором.

Он переживал из-за компьютерных дискет с другой ценной хакерской информацией. Они представляли собой тысячи часов работы, и он не мог заставить себя отправить их вслед за распечатками. Добыча объемом в 10 мегабайт. Больше 4000 карт. 130 000 различных транзакций. В итоге он решил сохранить диски, плюнув на риск. Во всяком случае, без распечаток ему удалось кое-как свернуть рюкзак и сделать его менее заметным. Отойдя от урны, он бросил беглый взгляд назад, чтобы проверить, насколько незаметно выглядит место захоронения со стороны. Могила выглядела как куча мусора. Мусор, стоящий миллионы долларов, отправится на свалку.

Сев вместе с матерью в автобус до Салинаса, Раг не переставал представлять себе, как какой-нибудь бездомный выуживает распечатки из урны и начинает спрашивать у всех подряд, что это такое. Он постарался отогнать прочь эту мысль.

Сидя в автобусе, Раг напряженно думал о том, что ему делать. Он ничего не сказал матери. Она так и не смогла разобраться в его мире компьютеров и сетей и вряд ли поняла бы его нынешние затруднения. Кроме того, у Раг'а были несколько натянутые отношения с матерью с тех пор, как он ушел из дома сразу же после своего семнадцатого дня рождения. Его исключили из школы за систематические прогулы, но он нашел работу, натаскивая студентов местного колледжа в компьютерных вопросах. Последний раз до этой поездки в Чикаго он видел мать полгода назад. Нет, у нее не стоит

искать поддержки.

Автобус приближался к Салинасу. По дороге к автобусной станции он проехал по улице, на которой жил Раг. Он увидел бегуна, худого чернокожего мужчину с плеером. «Какого черта он тут делает?» – подумал Раг. Никто не бежит трусцой в полуиндустриальном пригороде. Дом Раг'а был едва ли не единственным жилым зданием среди промышленных построек. Как только бегун миновал дом и его не могли оттуда заметить, он резко свернул с дороги, отошел в сторону и лег на землю. Лежа на газоне на животе и глядя на дом, он, кажется, что-то говорил *в свой плеер*.

Наблюдая за бегуном с сиденья автобуса, Раг аж подпрыгнул. Они поджидали именно его, нет никаких сомнений. Когда автобус наконец прибыл на станцию, мать Раг'а начала выгружать багаж, а он сам схватил рюкзак под мышку и был таков. Он нашел телефон-автомат и позвонил Скотту, чтобы выяснить, как обстоят дела. Скотт передал трубку Крису, еще одному соседу. Крис уезжал к родителям на День благодарения, и его не было в доме во время обыска.

– Сиди тихо и не высовывайся, – сказал Крис Раг'у, – я сейчас приеду за тобой и отвезу тебя к адвокату. Там тебе смогут помочь.

Ричард Розен [Richard Rosen], специалист по уголовному праву, родился в Нью-Йорке, но вырос в Калифорнии. В его личности отразилось непреклонное упрямство жителя Нью-Йорка, смягченное спокойным дружелюбием западного побережья. Розен также обладал сильной антиавторитарной жилкой. Он представлял интересы жоака местной группировки «Ангелы Ада» в графстве Монтеррей, где жил по преимуществу средний класс. Он также вызвал сенсацию, защищая растущее акушерское движение, пропагандирующее домашние роды. У калифорнийских властей не было особых причин любить его.

Соседи Раг'а встретились с Розеном после налета, чтобы подготовить почву для его возвращения. Они поведали Розену о том, какой ужас они пережили во время налета спецслужб, и о том, как их допрашивали полтора часа, вынуждая дать показания. Скотт, в частности, признался, что был вынужден дать показания против Раг'а исключительно под давлением следствия.

Разговаривая с Крисом, Раг заметил мужчину, который стоял в конце ряда телефонных кабин. У этого человека тоже был плеер. Он не смотрел прямо на Раг'а. Напротив, он стоял лицом к стене, бросая быстрые взгляды украдкой туда, где находился Раг. Кто этот парень? Страх охватил Раг'а, и все мыслимые и немыслимые подозрения заполнили его мозг. Кому можно верить?

Скотт не сказал ему о налете. Может быть, все его соседи в сговоре с Секретной службой? Может быть, они просто тянут время, чтобы сдать его? Но Раг'у больше не к кому было обратиться. Мать не поймет. Кроме того, у нее полно своих проблем. Отца у Раг'а не было. Вернее сказать, он был убежден, что его отец все равно что мертв. Он никогда не видел его, но знал, что тот служил тюремным охранником где-то во Флориде. Неподходящий кандидат в помощники в такой ситуации. Раг был в хороших отношениях с бабушкой и дедушкой – это они подарили ему компьютер, – но они жили в маленьком городке на Среднем Западе и тоже, скорее всего, не поняли бы его затруднений.

Раг не знал, что делать, но в тот момент у него не было особого выбора, и он сказал Крису, что будет ждать его на станции. Он шмыгнул за угол и постарался спрятаться.

Через несколько минут Крис приехал на станцию. Раг нырнул в его Toyota Landcruiser, и Крис рванул в направлении офиса Розена. Они заметили белый автомобиль, выехавший со станции вслед за их машиной.

По дороге Раг пытался восстановить картину по рассказу Криса. Никто не предупредил его о налете, потому что все в доме были уверены, что телефон на прослушке. Если бы они позвонили Раг'у в Чикаго и сообщили бы об обыске, то наверняка накликали бы новый налет спецслужб. Все, что они могли сделать, чтобы помочь ему – это связаться с Розеном.

Раг глянул в зеркало заднего вида. Белая машина по-прежнему преследовала их. Крис сделал резкий поворот на следующем перекрестке и, выехав на калифорнийский спидвей, прибавил газу. Белая машина вылетела из-за поворота, не отставая от них.

Что ни делал Крис, ему никак не удавалось оторваться от хвоста. Раг пересел на сиденье рядом с Крисом, совершенно потеряв самообладание.

Всего сутки назад он был в Чикаго и все было в полном порядке. Как получилось, что сейчас в Калифорнии за ним гонится неизвестный водитель в белой машине?

Крис делал все возможное, чтобы уйти от преследования. Он лавировал и гнал все быстрее. Белая машина не отставала. Но у Криса с Раг'ом было существенное преимущество перед белым автомобилем – они ехали в полноприводном внедорожнике. Мгновенно приняв решение, Крис резко повернул руль и свернул с дороги на поле салата-латука. Раг ухватился за ручку с внутренней стороны

двери, когда их вездеход пробивался через грязь по аккуратным рядам зелени. Совсем спелые пучки салата вылетали из-под крыши. Обрывки листьев носились в воздухе. Облако грязи окутало машину. Ее мотало и заносило, но все же она пробила на хайвэй, проходивший с другой стороны поля. Крис продолжил гонку по скоростному шоссе, вывернув на полосу на высокой скорости.

Когда Раг посмотрел назад, он увидел, что белая машина исчезла. Крис жал на газ, и не успел Раг перевести дух, как машина остановилась напротив здания, где находился офис Ричарда Розена.

Раг выскочил из машины, по-прежнему крепко сжимая под мышкой красный рюкзак, и буквально влетел в офис адвоката. Секретарша посмотрела на него с явным испугом, когда он сказал ей свое имя. Видимо, она была в курсе дела.

Розен немедленно принял его в своем кабинете. После короткого знакомства Раг выложил историю с преследованием. Розен внимательно слушал, время от времени задавая ясные, точные вопросы. Затем он начал действовать.

Прежде всего необходимо, сказал он, добиться прекращения слежки спецслужб, чтобы Раг'у больше не надо было тратить время, ныряя за углы и прячась на автостанциях. Розен позвонил в Сан-Франциско и попросил специального агента Томаса Дж. Хольмана [Thomas J. Holman] прекратить слежку в обмен на соглашение о том, что Раг признает официальное обвинение.

Хольман настаивал на том, что он *должен* поговорить с Раг'ом.

– Нет, – сказал Розен. Агенты правоохранительных органов не будут допрашивать Раг'а, пока сделка не состоится.

«Но Секретной службе *необходимо* побеседовать с Раг'ом», – продолжал настаивать Хольман. Они смогут обсудить все остальное после разговора с Раг'ом.

Розен вежливо предостерег Хольмана от попыток связаться с его клиентом. Он заявил, что если у спецслужб есть вопросы к Раг'у, они должны обращаться к нему через его адвоката. Хольману это не понравилось. Когда Секретная служба хочет с кем-то поговорить, она обычно добивается своего. Он продолжал требовать, но ответ был по-прежнему отрицательный. Нет, нет и еще раз нет. Хольман просчитался. Он был уверен, что каждый мечтает помочь Секретной службе США.

Когда Хольман осознал, что Розен не уступит, он сдался. Затем Розен вступил в переговоры с федеральным прокурором – государственным обвинителем Джо Бёртоном [Joe Burton], который в данном случае был фактическим начальником Хольмана. Ему он тоже предложил снять слежку в обмен на признание Раг'а. После этого Раг отдал на хранение Розену свой красный рюкзак. Примерно в это же время следователь Citibank Уоллес и детектив Портер из полиции Салинаса допрашивали мать Раг'а, после того, как она вернулась домой с автобусной станции. Она сообщила им, что сын ушел из дома полгода назад, оставив ей телефонный счет на \$2000, который она с трудом оплатила. Они спросили, нельзя ли им обыскать дом. В душе она волновалась о том, что может произойти, если она откажет. А вдруг они сообщат об этом на работу в ее офис? А вдруг ее уволят?

Мать Раг'а, простая женщина, не привыкла иметь дело с сотрудниками правоохранительных органов. Она согласилась. Следователи забрали дискеты и записи Раг'а.

Раг появился в полиции Салинаса в начале полудня 12 декабря. Там его сфотографировали и сняли отпечатки пальцев, после чего вручили вызов в суд – маленькую желтую полоску бумаги с грифом «502 (с) (1) PC». Судебная повестка была похожа на автобусный билет, но в ней шла речь о двух уголовных преступлениях, каждое из которых грозило ему как минимум тремя годами тюрьмы, да и то с учетом его возраста. Первый пункт обвинения – проникновение в Кредитный отдел Citicorp – мог повлечь за собой штраф в \$10 000. Второе обвинение – «мошенничество с телефонной службой в течение продолжительного времени» – не влекло за собой штрафа.

Федеральные следователи были потрясены юным возрастом Раг'а. Федеральная судебная система США всегда сталкивалась с большими трудностями, имея дело с подростками. Поэтому прокурор решил передать рассмотрение дела властям штата. Раг'у было приказано явиться в суд по делам несовершеннолетних графства Монтеррей 10 июля 1989 года.

В течение нескольких последующих месяцев Раг и Розен работали бок о бок. Хотя Розен и был очень компетентным адвокатом, ситуация выглядела довольно тоскливо. Citibank заявил, что израсходовал \$30 000 на безопасность своих систем, и Раг был уверен, что корпорация может потребовать возмещения убытков на сумму до \$3 миллионов. Хотя они не смогли доказать, что Раг лично получил какие-либо деньги с этих карт, обвинение утверждало, что их щедрая раздача привела к серьезным финансовым потерям. И это были только денежные вопросы.

Гораздо более тревожным было то, что суд мог заняться проникновением Раг'а в компьютеры TRW. У Секретной службы имелась по меньшей мере одна дискета из коллекции Раг'а с материалами TRW.

TRW была большой многопрофильной компанией с активами в \$2,1 миллиарда и объемом продаж почти на \$7 миллиардов в 1989 году. Почти половину ее деятельности занимало выполнение правительственных заказов. В TRW работало больше 73 тысяч человек. Многие из них занимались кредитным направлением бизнеса компании. Обширные базы данных TRW содержали частные детали жизней миллионов людей – адреса, телефоны, финансовое положение.

Но это была лишь одна из граней множества интересов компании. TRW также занималась оборонными вопросами из разряда совершенно секретных. Было широко известно, что ее космическое и оборонное подразделение в Редондо-Бич, Калифорния, являлось главным получателем средств по программе «звездных войн» администрации Рейгана. В этом отделении работало больше 10 % служащих компании. Они создавали космические летательные аппараты, коммуникационные системы, спутники и другое секретное космическое оборудование.

Захваченный диск содержал почту из почтовой системы компании TRWMAIL. Информация была не особенно важной, в основном обычная текучка, рассылаемая служащим, но правительственные агенты полагали, что нет дыма без огня. TRW занималась таким родом деятельности, что, когда кто-то получал несанкционированный доступ в ее системы, правительство начинало серьезно нервничать. А Раг побывал в нескольких машинах TRW; ему было известно, что в компании существует отдел ракетных исследований и даже отдел космических вооружений.

Раг подумал, что если столь многие против него – Citibank, Секретная служба, местная полиция, даже его родная мать на их стороне, – то они обязательно докопаются до действительно секретных вещей, которые он видел, занимаясь хакингом, – это лишь вопрос времени. Раг начал спрашивать себя, правильно ли он поступает, ожидая начала суда.

:)

В начале 1989 года, когда Theorem спускалась по трапу самолета, доставившего ее из Швейцарии в аэропорт Сан-Франциско, она с удовольствием думала о том, что ей все-таки удалось сдержать обещание, данное себе самой. Это было нелегко. Случались моменты нежности, совершенного слияния двух голосов в разных концах планеты, когда ей казалось, что это невозможно.

Раг в это время тоже старался держать себя в руках. Theorem описывала себя в самых пренебрежительных терминах. Он слышал в Altos, что она некрасива. Но это мнение, так или иначе, исходило от нее самой, поэтому его можно было не принимать в расчет.

Чуть позже, когда он смотрел, как поток пассажиров входит в зал ожидания, он сказал себе, что это в любом случае неважно. В конечном итоге он полюбил ее самое, ее существо, ее суть, а не физическую оболочку. Он говорил ей об этом. И она сказала ему то же самое.

И вот она здесь, напротив него. Раг'у пришлось слегка задрать голову, чтобы встретиться с ее взглядом, – она была выше на два-три сантиметра. Она была очень красива, у нее были прямые каштановые волосы до плеч и карие глаза. Он просто стоял и думал о том, что действительность превзошла все его ожидания.

Theorem улыбнулась.

Раг едва не потерял самообладание. Это была обезоруживающая улыбка, открытая и белозубая, теплая и настоящая. Все ее лицо светилось оживлением. Эта улыбка решила все.

Она сдержала обещание, данное самой себе. До этой встречи у нее не было ясного представления о том, как выглядит Раг. После того, как Theorem лично познакомилась с несколькими парнями из Altos на вечеринке в Мюнхене год назад, она постаралась больше никогда не пытаться представить себе внешний облик людей, отталкиваясь от их онлайн-личин. Чтобы больше никогда не разочаровываться.

Раг взял ее багаж, и они с Theorem сели в машину Брайана. Брайан был другом Раг'а, он согласился сыграть роль такси, потому что у Раг'а не было машины. Брайан подумал, что Theorem выглядит классно. Высокая швейцарская девушка, которая говорит по-французски. Это было еще круче. Они приехали в дом Раг'а. И тут Брайан начал болтать.

Он забросал Theorem вопросами. Ему было действительно любопытно – у него никогда раньше не было знакомых из Европы. Раг попытался намекнуть своему другу, чтобы тот отстал, но Брайан хотел знать все о жизни в Швейцарии. Какая там погода? Что, народ в самом деле все время катается на лыжах?

Сначала Раг смотрел ему прямо в глаза, а затем уставился на дверь.

Много ли швейцарцев говорит по-английски? Какие еще языки она знает? В Калифорнии многие катаются на лыжах. Как круто разговаривать с человеком из другого полушария.

Раг по-прежнему молчаливо указывал на дверь, и это наконец дошло до Брайана. Раг выпроводил друга из дома. Брайан провел там минут десять, но Раг'у они показались годом. Оставшись вдвоем, Раг с Theorem немного поговорили, затем Раг предложил пойти прогуляться.

По пути Раг рискнул дотронуться до ее руки и взял ее в свою. Кажется, ей это понравилось. Ее рука была теплой. Они еще о чем-то говорили, потом Раг остановился. Он повернулся к ней. После короткого молчания Раг сказал ей то, что говорил раньше по телефону, то, о чем они оба уже знали.

Theorem поцеловала Раг'а. Это ошеломило его. Он был совершенно не готов к этому. Theorem сказала те же слова в ответ Раг'у.

Когда они вернулись домой, то продолжили с того места, на котором остановились на улице. Они провели две с половиной недели в объятиях друг друга – это были чудесные, солнечные недели. Их отношения прошли проверку на прочность, доказали, что при личной встрече все может быть гораздо лучше, чем по телефону или онлайн. Theorem очаровала Раг'а, а он в свою очередь привел Theorem в состояние блаженства.

Раг показал ей свой маленький мирок Северной Калифорнии. Они побывали в нескольких туристических местах, но большую часть времени провели дома. Сутки напролет они говорили обо всем.

Затем пришло время отъезда. Theorem нужно было возвращаться к своей работе и к своей жизни в Швейцарии. Поездка в аэропорт, посадка в самолет – сердце просто разрывалось. Theorem выглядела очень расстроенной. Раг'у с трудом удалось продержаться до отлета самолета.

На две с половиной недели Theorem вычеркнула из мыслей Раг'а приближающийся суд. Как только она улетела, мрачная реальность скорого судебного дела обрушилась на него.

.)

Раг сидел за одолженным компьютером всю ночь в темноте. Лишь неяркое свечение монитора освещало комнату, и рыбы, бывало, приплывали к той стороне аквариума, которая была обращена к компьютеру, и смотрели на него. Когда в онлайн было тихо, Раг переносил свое внимание на угря и морского ерша. Может быть, их просто привлекал мерцающий компьютерный экран. Какой бы ни была причина, им, несомненно, нравилось находиться рядом. Это выглядело жутковато.

Раг несколько раз затянулся своим косяком, еще посмотрел на рыб, глотнул кока-колы и вернулся к компьютеру.

Этой ночью Раг увидел то, чего не должен был видеть. Не обычную хакерскую ерунду. Не потроха университетского компьютера. И даже не содержимое международного банка с конфиденциальной информацией о шейхах с Ближнего Востока.

Он увидел сведения о шпионском спутнике-убийце – такими словами Раг описал его другим хакерам. Он сказал, что этот спутник способен уничтожать другие спутники-шпионы. Он видел его внутри машины, подключенной к сети космического и оборонного подразделения TRW. Он напал на него точно так же, как Force случайно нашел машину CitiSaudi – во время сканирования. Раг больше ничего не рассказывал о своей находке, потому что она чертовски напугала его.

Внезапно он почувствовал себя человеком, который слишком много знает. Он побывал в таком количестве военных сайтов, видел так много секретного материала, что это могло выйти ему боком. Всю эту информацию было очень интересно читать, но, Бог свидетель, он никогда не собирался ничего с ней делать. Это был просто приз, сверкающий трофей, подтверждение его хакерского мастерства. Но это открытие сбило его с ног, он словно получил сильнейшую пощечину. Оно заставило его осознать, какой опасности он подвергается.

Что сделает с ним Секретная служба, если они обнаружат его находку? Всучит ему еще один миленький автобусный билет с надписью «502 С»? Ни за что. Позволить ему сказать на суде обо всем, что он знает? Чтобы об этом написали все газеты? Столько же шансов, как у снеговика на пожаре.

Это была эпоха Рональда Рейгана и Джорджа Буша, космических оборонных инициатив, огромных военных бюджетов и генералов-параноиков, рассматривавших весь мир как огромное поле битвы с империей зла, воплощенной в Советском Союзе.

А если правительство США просто запрет его и выбросит ключ? Захочет ли правительство позволить ему говорить об этом с другими заключенными – закоренелыми преступниками, которые знают, как сделать деньги из такой информации? Определенно, нет.

Остается только один вариант. Устранение.

Это была невеселая мысль. Но семнадцатилетнему хакеру она казалась единственно верной. Раг



поразмислил о том, что он может предпринять, и пришел к тому, что показалось ему правильным решением.

Бежать.

## 4

### В бегах

*Здесь ружье, а за ним другие  
Целятся в наши двери и спины.*

**Песня «Knife's Edge», альбом «Bird Noises» группы Midnight Oil<sup>23</sup>**

Когда Раг не явился в суд по делам несовершеннолетних графства Монтеррей в Салинасе 10 июля 1989 года, он был официально объявлен в розыск. На самом деле он подался в бега уже несколько недель назад. Но никто об этом не знал. Даже его адвокат.

Ричард Розен подумал, что что-то случилось, когда его клиент не пришел на условленную встречу дней за десять до слушаний, но он продолжал надеяться, что Раг не наделает глупостей. Розен заключил для него сделку – возмещение ущерба плюс две недели, а то и меньше в тюрьме для подростков в обмен на полное сотрудничество Раг'а с Секретной службой.

Раг явно волновался по этому поводу. Он неделями размышлял об этом. Он точно не собирался рассказывать федералам, как он взламывал многочисленные компьютеры, да и они ждали от него вовсе не этого. Они хотели, чтобы он стал стукачом. И стучал на всех. Они знали, что Раг был важной фигурой и поэтому был знаком со всеми серьезными игроками андеграунда. Он был бы идеальным осведомителем. Но Раг не собирался становиться доносчиком. Даже если он вывернется наизнанку, все равно остается вопрос о том, что власти сделают с ним в тюрьме. Картины расправы угрожающе вырисовывались в его голове.

И вот однажды утром Раг просто исчез. Он тщательно спланировал побег, потихоньку собрал вещи и договорился с надежным другом, который не входил в круг общения его соседей по дому. Этот друг заехал за Раг'ом, когда соседи отсутствовали. Они и не догадывались о том, что теперь уже восемнадцатилетний Раг собирается исчезнуть на очень долгое время.

Сначала Раг поехал в Сан-Диего. Потом в Лос-Анджелес. Затем в Нью-Джерси. После этого он совершенно исчез с экрана радара.

Жизнь в бегах была нелегка. Первые несколько месяцев Раг возил с собой две ценных вещи – недорогой ноутбук и фотографии Theorem, сделанные во время ее визита. Они были для него связующим звеном с остальным миром, и он таскал их в своей сумке из одного города в другой, часто останавливаясь у друзей из компьютерного подполья. Широко раскинувшаяся сеть хакеров работала примерно так же, как американская «подпольная железная дорога», по которой в XIX веке беглые рабы с Юга спасались бегством в безопасные северные штаты. С той лишь разницей, что у Раг'а не было никакой надежды добраться до спасительного рая.

Раг пересек континент, перебираясь из города в город. Неделя на одном месте. Несколько ночей в другом. Иногда на электронной подпольной железной дороге случались разрывы, места, где одна линия уже закончилась, а другая еще не началась. Эти разрывы оказывались самым тяжелым испытанием. Они означали, что ему придется спать на улице, иногда в холоде, голодать и не иметь возможности с кем-то поговорить. Он продолжал заниматься хакингом с новообретенным неистовством, потому что теперь он был непобедим. Что могут сделать с ним правительственные органы? Прийти и арестовать его? Он стал беглым и отдавал себе отчет в том, что хуже не будет. Он чувствовал себя так, как будто вся его жизнь прошла в бегах, хотя его эскапада длилась к тому моменту всего несколько месяцев.

Когда Раг останавливался у знакомых из компьютерного андеграунда, он был осторожен. Но оставшись один в комнате очередного занюханного мотеля или в компании людей, абсолютно далеких от электронного мира, он отдавался хакингу. Вызывающе и открыто. Он делал некоторые вещи, зная, что Секретная служба их увидит. Даже в его нелегальном голосовом почтовом ящике было несколько слов для его преследователей.

---

<sup>23</sup> Слова и музыка: Peter Garrett/James Moginie. © Copyright 1982 Sprint Music. Administered for the World-Warner/Chapell Music Australia Pty Ltd. Used by Permission.

Да, это Раг. Удачи всем педрилам из Секретной службы, кто продолжает звонить и слушать меня. По-моему, вы настолько тупые, что это даже не смешно.

Если вы послали мое дерьмо в Apple Computers [на анализы], вы просто идиоты, жалкие ничтожества. Вы думаете, что у меня был «голубой ящик» [для фрикинга]. Мне смешно, когда я пытаюсь представить, что такое, по вашему мнению, «голубой ящик». Вы просто неудачники.

Ах, да. Каждый, кто хочет оставить мне сообщение, вперед. Короче, расслабьтесь все, скиньте мне чего-нибудь. Ладно. Пока.

Несмотря на бравладу, паранойя овладела Раг'ом. Если он видел копа на другой стороне улицы, его дыхание учащалось, он разворачивался и уходил в противоположном направлении. Если коп шел к нему, Раг переходил улицу и сворачивал в ближайший переулок. Полиция в любом виде очень нервировала его.

К осени 1989 года Раг добрался до маленького городка в Северной Каролине. Он нашел место, где остановиться и отдохнуть, – у друга по прозвищу Nibbler.<sup>[p88]</sup> Его семья владела мотелем. Несколько недель на одном месте, в одной постели показались Раг'у раем. К тому же все было бесплатно – это означало, что ему не надо брать займы деньги у Theorem, которая помогала ему, пока он был в бегах.

Раг спал в комнате, которая оказывалась свободной в ту или иную ночь, но большую часть времени он проводил в одном из шале, где Nibbler устроил компьютерную комнату на время «мертвого» сезона. Они целыми днями занимались хакингом с компьютера Nibbler'a. Беглец был вынужден продать свой недорогой ноутбук еще до приезда в Северную Каролину.

Тем не менее после нескольких недель в мотеле Раг не мог отделаться от чувства, что за ним следят. Слишком много народу моталось взад-вперед. Он подозревал, что постояльцы отеля, сидя в машинах, шпионят за ним, и вскоре начал шарахаться от каждой тени. Он думал, что, возможно, спецслужбы все-таки нашли его.

Раг стал думать о том, как бы ему об этом узнать.

The Prophet,<sup>[p89]</sup> один из группы хакеров The Atlanta Three,<sup>[p90]</sup> иногда звонил Nibbler'у, чтобы обменяться хакерской информацией, особенно об ошибках в безопасности в системе Unix. Как-то раз Prophet рассказал Раг'у о новой ошибке в системах безопасности, которую он обнаружил в сети, принадлежащей одной телефонной компании.

The Atlanta Three, ответвление The Legion of Doom в Джорджии, очень плотно занималось проникновением в BellSouth, телефонную компанию, покрывающую весь юго-восток США. Они знали о телефонных коммутационных станциях столько же, сколько Раг знал о Tymnet. Секретная служба уже побывала с обысками в домах хакеров из Джорджии в июле 1989 года, но пока никто не был арестован, поэтому Prophet продолжал интересоваться своей излюбленной мишенью.

Раг подумал, что дыра в сети Bell South – это звучит очень круто, и вступил в игру с системами компании. Войти в компьютерную сеть компании, пошарить вокруг, посмотреть, что там происходит. Обычное дело.

Однажды Раг решил проверить записи телефонной компании по мотелю, просто чтобы глянуть, что там творится. Он набрал главный номер мотеля и система выдала его адрес, название и некоторую детализированную техническую информацию, в том числе о кабеле и паре, подключенной к телефонному номеру. Затем он посмотрел на телефонную линию компьютерного шале. Там было что-то *странное*.

Относительно линии, которую они с Nibbler'ом использовали для своих хакерских делишек, было сделано указание: «На линии ремонтная бригада».

Какая еще ремонтная бригада? Nibbler не говорил ни о каких проблемах с телефонными линиями мотеля, но Раг удостоверился у него еще раз. Никаких проблем с телефонами.

---

p88

Воришка.

p89

Пророк.

p90

Тройка из Атланты.

Раг занервничал. Мало того, что он наследил в сетях телефонной компании, до этого из треклятого шале он взломал русскую компьютерную сеть. Советская сеть оказалась отличной новой игрушкой. Она подключилась к единой мировой сети всего два месяца назад, и эта девственность делала ее особенно привлекательным местом.

Nibbler позвонил одному приятелю, чтобы тот проверил телефоны мотеля. Этот приятель, бывший техник телефонной компании, подавшийся на вольные хлеба, пришел и проверил оборудование. Он сказал Nibbler'у и Раг'у, что в телефонной системе мотеля происходит что-то непонятное. Напряжение на линии падало.

Раг сразу понял, что происходит. Систему обследовали. Каждая входящая и исходящая линия, возможно, прослушивалась. Это означало только одно: кто-то – телефонная компания, местная полиция, Секретная служба или ФБР – был у него на хвосте.

Nibbler и Раг быстро упаковали все компьютерное оборудование Nibbler'а вместе с хакерскими записями Раг'а и переехали в другой мотель. Им нужно было свернуть всю хакерскую деятельность и запутать следы.

Раг постоянно оставлял включенными программы, которые вынюхивали пароли и логины других людей в системе, как только те подключались, а затем сбрасывали всю информацию в одну взломанную машину. Он проверял этот файл каждый день. Если бы Раг не выключил программу, файл разросся бы до таких размеров, что системный администратор мог бы что-то заподозрить и решить проверить систему. Если бы он обнаружил, что система была взломана, он закрыл бы щели в системе безопасности, так что у Раг'а были бы проблемы с возвращением в эту систему.

Когда они закончили приводить в порядок взломанные системы, они снова собрали записи Раг'а и компьютерное барахло Nibbler'а и спрятали все это на платном складе. После этого они вернулись в мотель родителей Nibbler'а.

Раг не мог заставить себя двигаться дальше. Кроме того, есть вероятность, что это всего-навсего телефонная компания проявляла интерес к телефонной системе мотеля. Раг здорово пошустрил в компьютерных системах телекоммуникационных компаний с телефона мотеля, но он делал это анонимно. Может быть, что-то привлекло внимание Bell South, и она просто хотела получить побольше информации. Если это было так, то правительственным агентам, скорее всего, не было известно, где скрывается беглый Раг.

Атмосфера в мотеле стала угнетающей. Раг стал еще более подозрительно относиться к приезжим. Он все чаще поглядывал в окно и внимательнее прислушивался к приближающимся и уходящим шагам. Сколько постояльцев на самом деле были туристами? Раг просмотрел регистрационную книгу мотеля и обнаружил в нем человека, который написал, что он приехал из Нью-Джерси. Он работал в одной из корпораций AT&T, образовавшейся после распада Bell Systems. С какой стати парню из AT&T останавливаться в маленьком провинциальном городишке в Северной Каролине? А что если несколько секретных агентов засели в мотеле и следят за ним?

Раг должен был укротить свою паранойю. Ему был необходим свежий воздух и он пошел прогуляться. Погода была плохая, дул сильный ветер, поднимая маленькие торнадо из осенних листьев. Вскоре пошел дождь, и Раг нашел убежище в кабине телефона-автомата на другой стороне улицы, напротив мотеля.

Несмотря на то, что Раг был в бегах уже несколько месяцев, он звонил Theorem почти каждый день, применяя фрикерские приемы и используя большие телефонные компании. Он набрал ее номер, и они немного поговорили. Он рассказал ей о падении напряжения на PABX мотеля и о том, что телефон мог прослушиваться. Она спросила, как он мог выдать себя. Затем они с нежностью помечтали о том, когда смогут снова увидеть друг друга.

За стеклами кабины погода совсем испортилась. Дождь молотил по стеклу то с одной стороны, то с другой, как только ветер менял направление. Темная улица была пустынна. Ветви деревьев трещали под порывами ветра. Ручейки стекали с подветренной стороны кабины и превращались в стену воды за стеклом. Ветер перевернул урну, и ее содержимое разнесло по дороге.

Стараясь не обращать внимания на стихию, бушевавшую вокруг, Раг пристроил телефонную трубку в небольшом защищенном пространстве между своей рукой, грудью и углом телефонной кабины. Он напомнил Theorem о двух с половиной неделях в Калифорнии, которые они провели вместе, и они тихо радовались, вспоминая свои интимные тайны.

Ветка дерева заскрипела, а затем сломалась, не выдержав порыва ветра. Когда она рухнула на мостовую рядом с кабиной, Theorem спросила, что это за шум.

– Ураган начинается, – ответил ей Раг. – Ураган «Хьюго». Его ждали сегодня вечером. Думаю, он пришел.

В голосе Theorem послышались нотки ужаса, когда она стала уговаривать Раг'а немедленно вернуться в безопасность мотеля.

Когда Раг открыл дверцу кабины, его окатило водой. Он рванулся через дорогу, борясь с ураганным ветром, ввалился в свою комнату и залез в постель, чтобы согреться. Он уснул под шум урагана, мечтая о Theorem.

:)

Ураган «Хьюго» бушевал больше трех дней, и это были самые спокойные дни для Раг'а за последние несколько недель. Можно было дать голову на отсечение, что Секретная служба не станет проводить никаких рейдов во время урагана. Главный удар «Хьюго» пришелся на Южную Каролину, но Северной тоже порядком досталось. Это был один из самых сильных ураганов, поразивших эти районы за последние десятилетия. Ветер ближе к эпицентру урагана достигал скорости свыше 240 километров в час. Шестьдесят человек погибло, а ущерб, нанесенный «Хьюго» на пути от Вест-Индии к Каролинам, составил около \$7 миллиардов.

Когда Раг вышел из своей комнаты в мотеле после полудня спустя несколько дней после урагана, воздух был прозрачен и свеж. Он подошел к перилам, ограждающим его насест на втором этаже, и принялся наблюдать за деятельностью людского муравейника на парковке перед отелем. Там были машины. Там был микроавтобус. И группа зевак.

И там была Секретная служба.

По крайней мере, восемь агентов в синих куртках с эмблемой Секретной службы США на спине.

Раг похолодел. Он перестал дышать. Все вокруг него замедлило свой ход. Несколько агентов образовали кружок вокруг парня из мотеля, рабочего по имени Джон, который был немного похож на Раг'а. Они что-то спрашивали у Джона и исследовали его документы. Затем они проводили Джона в микроавтобус, видимо, для того, чтобы проверить его отпечатки пальцев.

Мозг Раг'а начал выходить из оцепенения. Он попытался рассуждать здраво. Как ему быть? Ему нужно вернуться в комнату. Это даст время подумать, что же делать дальше. Вдруг он вспомнил о фотографиях Theorem. Он ни за что не позволит Секретной службе завладеть ими. Надо спрятать их, и побыстрее.

Он мог видеть, как агенты Секретной службы обыскивают компьютерное шале. Слава богу, что они с Nibbler'ом убрали все оборудование. Во всяком случае, там не было ничего криминального, и агенты не смогут заполучить весь их арсенал.

Раг дышал глубоко и медленно. Он пытался заставить себя отойти от перил и спокойно вернуться в свою комнату. Он изо всех сил боролся с желанием поскорее броситься в комнату, чтобы не видеть того, что творилось внизу. Резкое движение могло привлечь внимание агентов.

Как только Раг начал отход, один из агентов обернулся. Он оглядел весь двухэтажный комплекс мотеля, и его пристальный взгляд мгновенно остановился на Раг'е. Он смотрел ему прямо в глаза.

«Вот и все, – подумал Раг. – Мне крышка. Отсюда мне не выбраться. Бегать несколько месяцев, чтобы в такой дыре в Северной Каролине эти парни взяли меня за задницу. Я больше никогда не увижу солнца. Они укокошат меня, других вариантов нет».

Пока эти мысли проносились в голове Раг'а, он стоял, словно оцепенев. Его ноги вросли в бетонный пол. Он не мог отвести глаз от пристального, испытующего взгляда агента Секретной службы. Раг чувствовал себя так, словно они были двумя единственными существами во Вселенной.

Затем, непонятно почему, агент отвел взгляд. Он повернулся, продолжая разговор с другими агентами. Как будто и не смотрел на беглеца.

Раг стоял, не решаясь тронуться с места и не веря своим глазам. Это было просто невероятно. Он начал осторожное движение по направлению к своей комнате. Медленно, словно небрежно, он проскользнул внутрь и закрыл за собой дверь.

Его мысли снова устремились к фотографиям Theorem, и он стал осматривать комнату в поисках безопасного места. Но он не мог найти ничего подходящего. Лучшим выбором казалось что-то выше уровня глаз. Он толкнул стул через комнату, влез на него и надавил на потолок. Квадратная пластиковая панель легко подалась, и Раг засунул фотографии в образовавшееся пространство, затем поставил панель на место. Если агенты перероют всю комнату, они, скорее всего, найдут фотографии. Но, может быть, при поверхностном обыске снимки не попадут к ним в руки. При существующем раскладе Раг'у оставалось уповать только на это.

Он снова стал думать о бегстве. На местных можно было положиться, и Раг очень рассчитывал

на то, что персонал мотеля не сообщит Секретной службе о его местонахождении. Это даст ему немного времени, но он не сможет выбраться из комнаты незамеченным. Скорее всего, когда они увидят, что кто-то выходит с территории мотеля, они остановят его и допросят.

Даже если бы ему удалось выбраться отсюда, это бы не слишком ему помогло. Город был не настолько велик, чтобы укрыться от тщательных розысков. Кроме того, у него больше не было здесь таких знакомых, которым он мог бы довериться и переждать у них какое-то время. Молодой человек, выбегающий из мотеля на своих двоих в той части света, где все ездят на машинах, несомненно вызвал бы подозрения. Ловить попутку тоже не годилось. С его везением он, скорее всего, нарвался бы на секретного агента, возвращающегося после операции. Нет, ему нужен более жизнеспособный план. Он должен был уехать подальше из этих мест, выбраться из этого штата.

Раг знал, что Джон ездил в Эшвилл на какие-то курсы, для чего вставал очень рано. Если власти уже некоторое время следили за отелем, они должны были знать, что его отъезд в пять утра – обычное дело. Этот план казался многообещающим еще по одной причине. В такую рань на улице еще темно.

Если Раг сможет добраться до Эшвилла, он сможет попасть в Шарлотту, а оттуда улететь еще дальше.

Раг снова и снова прокручивал в голове разные варианты. Спрятаться в одной из комнат мотеля казалось самым разумным. Он с завидной регулярностью перебирался из комнаты в комнату, так что агентам, которые следили за мотелем, он мог показаться просто еще одним путешественником. Если удача не совсем покинула его, сейчас спецслужба должна сосредоточить свои усилия на шале, разнося его в клочья в напрасных поисках компьютерного оборудования. Пока эти мысли бродили в его голове, вдруг раздался телефонный звонок, и Раг подскочил, как ужаленный. Он уставился на аппарат, не зная, стоит ли отвечать.

Но все-таки взял трубку.

– Это Nibbler, – прошептал голос.

– Да, – тоже шепотом ответил Раг.

– Раг, здесь Секретная служба, они обыскивают мотель.

– Знаю, я видел их.

– Они уже обыскали комнату рядом с твоей.

Раг едва не помер на месте. Агенты были в двух метрах от него, а он об этом даже не догадывался. В этой комнате жил Джон. Комнаты соединялись внутренней дверью, но она была заперта с обеих сторон.

– Перейди в комнату Джона и сиди тихо. Мне пора.

Nibbler повесил трубку.

Раг прильнул ухом к стене и прислушался. Ничего. Он открыл внутреннюю дверь, повернул ручку и легонько толкнул. Дверь отворилась. Кто-то отпер ее с другой стороны после обыска. Раг осторожно посмотрел в образовавшуюся щель. Комната выглядела тихой и спокойной. Он открыл дверь – никого. Сгребя свои вещи в охапку, он перешел в комнату Джона.

Раг принялся ждать. Он метался взад-вперед по комнате, не находя себе места, напряженно прислушиваясь к звукам снаружи. Каждый стук и скрип дверей резали его без ножа. Этой же ночью, когда сотрудники спецслужб уехали, Nibbler позвонил ему по внутреннему телефону и рассказал, что произошло.

Nibbler был в компьютерном шале, когда туда ворвалась Секретная служба с ордером на обыск. Агенты переписали имена, номера, все возможные детали, но им не удалось найти никаких доказательств хакинга. В конце концов один из них выскочил из шале, победоносно потрясая единственным компьютерным диском. Вся правоохранительная бригада собралась перед шале с радостными возгласами, но Nibbler с большим трудом сохранял серьезность. Его младший брат изучал основы компьютерной графики с помощью программы Logo. Секретная служба Соединенных Штатов скоро приобщится к секретным рисункам ученика начальных классов.

Раг засмеялся. Это помогло преодолеть стресс. Затем он посвятил Nibbler'a в план побега, и тот согласился все уладить. Родители Nibbler'a не знали всей подоплеки, но им нравился Раг, и они хотели помочь ему. И Nibbler желал своему другу только добра.

Раг даже не пытался отдохнуть перед побегом. Он был в таком же возбуждении, как скаковая лошадь перед стартом. Что, если Секретная служба следит за мотелем? В этом мотеле не было гаража, пристроенного к главному зданию, куда он мог бы попасть изнутри. Он будет на виду, если только все пойдет по плану, около минуты. Ночная темнота послужит достаточным прикрытием, но все же план бегства не был верным на сто процентов. Если агенты продолжают наблюдать за моте-

лем с какого-то расстояния, они могут не заметить, как он выбирается из своей комнаты. С другой стороны, в мотеле могут быть агенты, работающие под прикрытием. Прикидываясь постояльцами гостиницы, они могут следить за всем комплексом из одной из комнат.

Навязчивые мысли всю ночь не давали Раг'у покоя. Утром, за несколько минут до пяти, он услышал звук машины Джона, выезжающей из гаража. Раг погасил свет в комнате, приоткрыл балконную дверь и осмотрел пространство перед мотелем. Все спокойно, у дверей одинокая машина, роко-чущая в тихом холодном воздухе. Окна в большинстве зданий не горели. Сейчас или никогда.

Раг вышел из комнаты и проскользнул в холл. Когда он крался вниз, предрассветная прохлада вызвала дрожь. Быстро оглянувшись по сторонам, он поспешил к ожидающему автомобилю, открыл дверь и нырнул на заднее сиденье. Стараясь не высовываться, он изогнулся, скатился на пол и закрыл дверь с едва слышным щелчком.

Как только машина начала двигаться, Раг взял лежавшее на полу одеяло и натянул его на себя. После того, как Джон сказал ему, что они благополучно выбрались из города, Раг отбросил одеяло и взглянул на предрассветное небо. Он попытался поудобнее устроиться на полу. Ему предстояла долгая поездка.

В Эшвилле Джон высадил Раг'а в условленном месте, где его уже ждали. Он поблагодарил Джона и прыгнул в машину еще одного представителя обширной сети знакомых и друзей, который должен был отвезти его в Шарлотту.

Но на этот раз Раг ехал на переднем пассажирском сиденье. Он смог увидеть и оценить истинный масштаб разрушений и ярости урагана «Хьюго». Маленький городок, где он находился во время урагана, испытал лишь ливень и сильные порывы ветра. По пути в аэропорт Шарлотты, где Раг собирался сесть на самолет до Нью-Йорка, он с изумлением наблюдал за последствиями буйства «Хьюго». Он смотрел из окна машины, не в силах отвести взгляд от окружающих разрушений.

Ураган сносил все слабо закрепленное и хрупкое и превращал это в ракету с миссией камикадзе. Было совершенно невозможно определить, что прежде представляли собой изувеченные и разбитые обломки неизвестно чего, оставшиеся на пути бешеных ураганных ветров.

;)

Theorem волновалась за Раг'а, пока он метался из угла в угол по всему континенту. Она часто просила его подумать о том, чтобы сдать полиции. Переезды из города в город требовали денег, и Theorem это тоже давалось нелегко. Она считала, что поспешное бегство Раг'а было не самой лучшей идеей, и предложила оплатить услуги адвоката, чтобы можно было остановиться. Раг отказался. Как он мог сдать, если был убежден, что его физическое устранение является единственным возможным вариантом. Theorem посылала ему деньги, потому что у него не было возможности заработать, но ведь он должен был как-то существовать. Самым ужасным в этой ситуации были мысли, постоянно преследующие ее. В промежутки между телефонными звонками с Раг'ом могло произойти все что угодно. Жив ли он? Может быть, он уже в тюрьме? Может быть, его схватили или даже случайно застрелили во время захвата?

Секретная служба и люди из частных сыскных агентств всерьез взялись за него. Это было тревожно, но неудивительно. Раг надоел им. Он взламывал их машины и передавал частную информацию всему андеграунду. Они ворвались в его дом, а его там даже не было. Затем он ускользнул второй раз, в Северной Каролине, буквально просочившись у них между пальцев. Он все время был у них под носом, продолжая нагло заниматься хакингом, демонстрируя им свое презрение с помощью голосовых почтовых сообщений. Он представлял, как их, должно быть, бесит эта тщетная погоня за бесконечными ложными ниточками с тех пор, как он стал периодически распускать фальшивые слухи о своем местопребывании. И самое главное, он думал, что они знают о том, что он видел в системе TRW. Он был *угрозой*.

Раг'а все сильнее охватывала паранойя. Он все время оглядывался, двигаясь из города в город. Он постоянно чувствовал усталость. Он никогда не мог выспаться как следует, вскакивая с постели при малейшем шорохе. Иногда после нескольких часов беспокойного сна он, очнувшись, не мог понять, где находится. В каком доме или мотеле, у каких друзей, в каком городе.

Он все еще постоянно занимался хакингом, одалживая машины, где только возможно. Он часто оставлял сообщения на Phoenix Project, [\[p91\]](#) эксклюзивной BBS, которую запустили The Mentor [\[p92\]](#)

и Eric Bloodaxe и которую посещали члены LOD и австралийские хакеры. Некоторые знаменитые специалисты по компьютерной безопасности также были приглашены посещать отдельные, ограниченные области этой техасской доски объявлений. Этот факт серьезно способствовал укреплению статуса Phoenix Project в компьютерном андеграунде. Хакеров в той же степени интересовали люди из безопасности, как и те интересовались своей потенциальной добычей. Phoenix Project был особой территорией, поскольку предоставлял нейтральную площадку, где обе стороны могли встретиться и обменяться мыслями.

Судя по сообщениям, Par продолжал совершенствовать свое хакерское мастерство, одновременно общаясь с друзьями, среди которых можно назвать Eric Bloodaxe из Техаса и Phoenix из мельбурнского Realm. Electron тоже посещал Phoenix Project. Все они знали, что Par в бегах, и иногда шутили с ним на эту тему. Юмор помогал Par'у переносить жуткую реальность его положения. Все хакеры в Phoenix Project рассматривали вероятность того, что их самих могут схватить, если не сегодня, так завтра. Но присутствие Par'а и его трудное существование в бегах постоянно опровергали общую убежденность.

Сообщения Par'а становились все более депрессивными и параноидальными, поэтому другие хакеры пытались делать все возможное, чтобы помочь ему. Элита американских и мировых хакеров, имевших доступ в частные секции Phoenix Project, читала его послания и сочувствовала парню. А Par продолжал скользить все глубже и глубже в свой собственный странный мир.

Subject: Черт!!!

From: Parmaster

Date: Sat. Jan 13 08:40:17 1990

Черт, сегодня ночью я напился и влез в проклятую филиппинскую систему... Тупой админ приперся и спросил, кто я такой...

Следующее, что я знаю – мне дали пинка под зад и обе учетных записи пропали.

Не только это... но вся гребаная Philippine Net больше не принимает звонков с оплатой получателем. (Полный облом случился после того, как меня вышвырнули!)

Видимо, я сильно кого-то достал.

Кстати, детки, никогда не мешайте хакинг с алкоголем!

– Par

Subject: gawd

From: Parmaster

Date: Sat Jan 13 09:07:06 1990

Эти парни из SS и NSA/p93/ думают, что я их ТОВАРИЩ... хехехе, я так рад, что я все еще свободен, твою мать. Уахахаха &lt;Glasnost и прочее радужное дерьмо>

– Par

Subject: Нижняя граница

From: Parmaster

Date: Sun Jan 21 10:05:38 1990

Нижняя граница – это жестокое преследование. Эти фриkerы были только началом, я уверен.

Настало время следить за собой.

Неважно, в чем ты замешан, пока существуют коды, карты и т. д.

Видимо, правительство решило, что это последняя капля. Жаль, но в связи с последними новостями они смогут получить больше денег на борьбу с хакерами.

И это очень хреновые новости для нас.

Я думаю, они будут охотиться за «учителями» – за людьми, которые учат людей таким вещам.

Интересно, связывают ли они между собой все эти случаи? Наверное, единственная вещь, которую они принимают во внимание – все мы хакеры.

Поэтому они направят против нас всю свою энергию.

Остановить ВСЕХ хакеров – и остановить их ДО ТОГО, как они станут угрозой.

После того, как они уничтожат всех преподавателей, вот так-то.

Это просто теория.

– Par

Subject: Соединение

From: Parmaster

Date: Sun Jan 21 10:16:11 1990

Что ж, единственное соединение – это отключение, как сказал бы Gandalf [английский хакер].

Эти слова я напишу на своем надгробии.

**ЕДИНСТВЕННОЕ СОЕДИНЕНИЕ – ЭТО ОТКЛЮЧЕНИЕ...**

Да, может быть, я прихвачу с собой несколько педрил, когда они придут за мной.

– Par

Subject: Ну да

From: Parmaster

Date: Tue Jan 23 19:30:05 1990

«Теперь конец уж близок. Прошел я все и каждую тропинку», – как говорил Король. Ну и что. Кому какое дело? В любом случае, он был жирным дерьмом, пока не подох.

Всем, кто был мне хорошим другом и помогал скрывать тот факт, что я ни хрена не знаю, – спасибо. И всем остальным – наплюйте и держитесь.

В тот момент я был временно не в себе.

Увидимся на веселой ферме, умные парни.

– Par

Subject: Par

From: Eric Bloodaxe

Date: Tue Jan 23 23:21:39 1990

Черт, чувак, как можно бухать и думать о таких вещах? Это хреново, в физическом и душевном смыслах.

Приезжай в Остин, в Техас. Мы спрячем тебя где-нибудь, пока не придумаем, как тебе помочь.

Минимум год безопасности лучше, чем выкинуть на помойку всю жизнь. Черт, тебе всего 19!!

Я навсегда отказался от «бесповоротных» решений. Мертвецы не могут общаться, но в федеральных тюрьмах люди могут ходить друг другу в гости!!!

Подумай о Theorem.

Звони сюда в любое время, как прочитаешь это... Я вижу, тебе действительно хреново, так что еще один драный звонок...

– Eric



Subject: O, черт  
From: Parmaster  
Date: Mon Jan 29 15:45:05 1990  
Скоро это случится, парни.  
Я хотел бы купить еще немного времени.  
И разработать сделку.  
Но дудки. Они уже близко.  
Я могу сказать, какие машины из тех, что едут мимо, принадлежат им.  
Это самый странный случай *deja vu*, [\[p94\]](#) который у меня когда-либо бывал.  
Короче, я получил сегодня интересный звонок. Он был от Эдди, это один из компьютеров Bell Systems.  
Это была скорее фантазия, как...  
Может быть, просто способ сказать: «Пока».  
Эдди был другом, умнейшим из чертовых Unix боксов в округе...  
И он позвонил сегодня, чтобы сказать мне: «Пока».  
Теперь я знаю, что мне конец.  
Спасибо, Эдди, это было реально.  
(Кто бы ты ни был)  
«ОК, Эдди, за тебя»  
До не скорого,  
— Пар

Subject: Par  
From: Eric Bloodaxe  
Date: Mon Jan 29 19:36:38 1990  
Дружище Пар, это уж слишком... завязывай с травой.  
Не каждый, кто носит очки и темный костюм, – федерал. Не все машины с одинаковыми колпаками принадлежат правительству.  
Черт, я не знаю, что это за чертов «Эдди», но ты оставил странное сообщение.  
Лети в Остин... прямо завтра... у нас полно мест, где можно спрятаться, пока все не начнет успокаиваться.  
– Eric

[illegible]

что это с юным Par?

Subject: Par and Eric

From: Daneel Olivaw

Date: Mon Jan 29 21:10:00 1990

Эрик, ты думаешь, что только ты один можешь прятать людей, не так ли?

Subject: Ты знаешь, когда тебя скрутят

From: Parmaster

Date: Wed Jan 31 14:26:04 1990

Ты знаешь, когда тебя скрутят:

Когда наблюдатели наблюдают за окрестностями и носят темные очки, когда температура 11 градусов по Фаренгейту и темно, как в аду.

Когда одни и те же машины ездят взад-вперед днем и ночью. (Думаю, развозят кофе и пончики.)

– Par

Subject: Эх, Par

From: Mentor

Date: Wed Jan 31 16:37:04 1990

Хмм. Я ношу солнечные очки, когда 11 градусов и темно, так что ты можешь прикончить вот этого.:-)

Subject: Хм, Par

From: Phoenix

Date: Thu Feb 01 10:22:46 1990

Хорошо хоть, что в тебя не стреляют.

Subject: Par, почему бы тебе не...

From: Ravage

Date: Thu Feb 01 10:56:04 1990

Почему бы тебе просто не выйти и не поздороваться с этими милыми господами? Если я вижу, что кто-то постоянно болтается по соседству, я обычно немедленно их проверяю, если они выглядят подозрительно.

Subject: Par, заряди их

From: Aston Martin

Date: Tue Feb 06 18:04:55 1990

Вот что тебе надо сделать: иди к одному из фургонов, что стоят на улице (знаешь, те, в которых двое парней сидят целыми днями) с парой соединительных проводов. Скажи им, что ты смотришь, как они торчат там целый день, и подумал, что они заглохли. Спроси, не нужно ли им подзарядиться.

– Aston

В промежутках между этими странными сообщениями Раг часто помещал свои комментарии по техническим вопросам. Как обычно, у него консультировались о сетях X.25. В отличие от некоторых других хакеров, Раг почти всегда предлагал помощь. При этом он считал, что его статус одного из «учителей» превращает его в особую мишень. Но его всегдашняя готовность учить других в сочетании с относительной скромностью и сдержанностью, сделали Раг'а популярным среди многих хакеров. Поэтому он почти всегда находил, где остановиться.

Пришла весна. С ее наступлением некоторые сезонные трудности жизни вне закона ушли прочь. Потом наступило лето. Раг все еще был в бегах, продолжая ускользать от общенациональной охоты, которую вела Секретная служба. К осени Раг бегал от правоохранительных органов уже больше года. На горизонте маячила мрачная перспектива новой холодной зимы в бегах, но ему было наплевать. В конце концов жить можно. Он проглотит все, что преподнесет ему судьба, потому что ему есть ради чего жить.

:)

Theorem снова приезжает к нему.

Когда Theorem прибыла в Нью-Йорк в начале 1991 года, было жутко холодно. Они поехали в Коннектикут, где Раг остановился в доме, который снимали его друзья.

Раг очень переживал из-за многих вещей, в частности из-за того, сохранятся ли у них прежние отношения. Но спустя несколько часов после ее приезда от опасений не осталось и следа. Theorem так же страстно любила его, как и почти год назад в Калифорнии. Его собственные чувства только окрепли за это время. Theorem стала спасительным оплотом счастья в растущем хаосе его жизни.

Но в мире вокруг них все было иначе. Жизнь в бегах вместе с Theorem выглядела мрачновато. Постоянная зависимость от других людей, от их милосердия подчинила бы парочку малейшим капризам тех, от кого они зависели.

Один из соседей однажды напился и затеял драку с другом Раг'а. Битва была нешуточной, но друг победил. В припадке неконтролируемой ярости пьяный пригрозил сдать Раг'а властям. Изрыгая гневные проклятия, он орал, что сейчас позвонит в ФБР, ЦРУ и Секретную службу и сообщит им, где живет Раг.

Theorem и Раг решили не дожидаться, пока пьяный осуществит свою угрозу. Они схватили куртки и выбежали во тьму. Почти без денег, не зная, где найти ночлег, они несколько часов бродили по улицам под порывами холодного ветра. В конце концов они решили, что у них нет другого выбора, как вернуться домой поздно ночью в надежде, что пьяница уже уснул.

Они подкрались к дому. Вполне вероятно, что пьянчуга позвонил во все силовые агентства, которые смог вспомнить его затуманенный мозг. В таком случае их ждала засада целого отряда агентов. Улица была совершенно безлюдна. Все припаркованные машины были пусты. Раг вглядывался в темные окна дома, но ничего не заметил. Он жестом показал Theorem, чтобы она шла за ним в дом.

Хотя Theorem и не видела лица Раг'а, она чувствовала его напряжение. Почти все время она обнаруживала в их близости нечто, граничащее с телепатией. Но в этот момент сверхъестественный дар сопереживания казался проклятием. Theorem чувствовала сжигающую Раг'а паранойю, и ее охватил ужас, когда они крались через гостиную, проверяя каждую комнату. Наконец, они подошли к комнате Раг'а, опасаясь обнаружить там пару-тройку секретных агентов, терпеливо поджидающих их во мраке.

Комната была пуста.

Они забрались в постель и постарались уснуть, но Theorem еще долго лежала в темноте, думая об этом странном и пугающем опыте. Хотя она разговаривала с Раг'ом по телефону почти каждый день, когда они не были вместе, она поняла, что некоторые вещи ускользнули от нее.

Такая долгая жизнь вне закона изменила Раг'а.

:)

Через некоторое время после того, как Theorem вернулась в Швейцарию, ее доступу в Altos пришел конец. Она входила в систему через старую университетскую учетную запись, но в конце концов университет запретил ей доступ, потому что она больше не числилась среди его студентов. Не имея доступа к какой-либо сети X.25, соединенной с внешним миром, она не могла войти в Altos. Хотя Theorem не занималась хакингом, она быстро приобрела зависимость от Altos. Потеря доступа к швейцарской сети X.25 (а значит, и к Altos) повергла ее в глубокую депрессию. Она рассказала об

этом Par'у по телефону в самых мрачных выражениях.

Par решил сделать ей небольшой подарок. Тогда как большинство хакеров взламывали компьютеры в сетях X.25, Par вторгался в машины компаний, запустивших эти самые сети. Контроль над машинами, принадлежавшими Telenet или Tymnet, был реальной силой. Par был специалистом по сетям X.25 и мог просто создать специальную учетную запись – только для Theorem – в Tymnet.

Когда Par закончил работать с учетной записью, он откинулся на спинку стула, чрезвычайно гордый собой.

Имя учетной записи: Theorem.

Пароль: ParLovesMe!/[p95]

«Ну вот, – думал Par, – она будет набирать это всякий раз, как ей понадобится войти в сеть Tymnet. Altos мог кишмя кишеть лучшими в мире хакерами, жаждущими пофлиртовать с Theorem, но всякий раз, регистрируясь в системе, она будет думать обо мне».

Par позвонил ей по телефону и вручил свой специальный подарок. Когда он сказал ей пароль ее новой учетной записи, Theorem засмеялась. Она подумала, что это прелестно.

Ребята из MOD подумали то же самое.

Masters of Deception или Destruction/[p96] – зависело от того, кто рассказывал эту историю – были бандой хакеров из Нью-Йорка. Они решили, что неплохо бы взломать Altos. Было нелегко получить внутренний доступ в Altos, такой как у Theorem, и большинство людей довольствовались использованием «гостевых» учетных записей. Но взлом Altos с использованием внутренней учетной записи выглядел гораздо более легким делом. Учетная запись Theorem должна была стать точкой опоры.

Как MOD получили пароль Theorem в Altos? Самое вероятное, что они следили за одним из шлюзов X.25, которые она использовала для перехода из Tymnet в Altos. Может быть, они разнюхали ее пароль по дороге. Или они наблюдали за службой безопасности Tymnet, которая следила за этими воротами.

В общем, неважно, как MOD получили пароль Theorem в Altos. Важно, что они изменили его. Когда Theorem не смогла войти в Altos, она была вне себя. Она чувствовала себя как наркоман, решивший завязать. Это было слишком. И конечно, она не могла связаться с Par'ом. Поскольку он был в бегах, ей пришлось ждать, пока он сам не позвонил. Она не могла связаться и с другими приятелями по Altos, чтобы попросить о помощи. Как ей найти их? Все они были хакерами. Все они имели клички и никто не знал их настоящих имен.

Theorem еще не знала о том, что она не просто потеряла доступ в Altos. Парни из MOD использовали ее учетную запись, чтобы взломать чат-систему. В глазах всего мира это выглядело делом ее рук.

Наконец, Theorem удалось окольным путем отправить сообщение Gandalf'у, знаменитому английскому хакеру. Она искала его по двум причинам. Во-первых, он был хорошим другом и, вероятно, захотел бы помочь ей. Во-вторых, у Gandalf'a был корневой доступ в Altos, а это означало, что он сможет дать ей новый пароль или учетную запись.

Gandalf создал себе отличную репутацию в компьютерном подполье с помощью своей хакерской группы 8lgm – Eight-Legged Groove Machine/[p97] – по названию британской музыкальной группы. Он и его друг Pad, тоже английский хакер, были лучшими четырьмя ногами в общем ансамбле. Они ставили номера мирового класса и, несомненно, были одними из самых талантливых хакеров, игравших на английской сцене. Но Gandalf и (в меньшей степени) Pad имели репутацию высокомерных нахалов. Они постоянно гладили американских хакеров против шерсти. Их позиция заключалась в следующем: «Мы лучшие и знаем это. Отвалите».

Gandalf вывел из строя учетную запись Theorem в Altos. Он смог изменить пароль и послать

---

p95

Par любит меня (англ.).

p96

Мастера разочарования или разрушения.

p97

Восьминогая грув-машина.

сообщение по сложной тайной системе, которую Theorem использовала, чтобы связаться с ним. Он понял, что кто-то намеренно захватил ее учетную запись. Он не хотел передавать новый пароль для ее учетной записи через все подполье. Но неприятность заключалась в том, что ни Раг, ни Theorem не знали, что сделал Gandalf.

Тем временем Раг позвонил Theorem и получил нагоняй. Обозленный Раг поклялся, что найдет наглецов, которые испоганили ее учетную запись.

Когда парни из MOD сказали Раг'у, что это их вина, он немного удивился, потому что они всегда были в хороших отношениях.

Раг сказал им, как расстроилась Theorem, как она отчитала его. Затем случилась невероятная вещь. Corrupt, [\[p98\]](#) самый крутой и злобный парень в MOD, чернокожий хакер из опаснейшего района Нью-Йорка, ни в грош никого не ставивший, потому что мог себе это позволить, извинился перед Раг'ом.

Парни из MOD никогда не извинялись, даже если знали, что неправы. Извинения на улицах Нью-Йорка никогда не приносили ничего хорошего. Это был знак глубочайшего уважения. «Извини, старик» от Corrupt'a было равносильно тому, что нормальный человек слизал бы грязь с ваших ботинок.

Новый пароль был: MODmOdMOD. Вот такие это были ребята.

Раг едва успел отключиться, чтобы проверить новый пароль, как вдруг Corrupt снова вышел на связь.

– Эй, Раг, есть кое-что, что ты должен знать.

– Да, – ответил Раг, нервничая от нетерпения.

– Я проверял ее почту. Там какая-то фигня.

Почта Theorem? Фигня?

– Что за фигня? – спросил Раг.

– Письма от Gandalf'a.

– Ну и?

– Дружеские письма. *Реально* дружеские.

Раг'у захотелось посмотреть на это, в то же время он не хотел этого делать. Он мог бы давным-давно получить привилегированную учетную запись в Altos, если бы ему она была нужна. Но он и не думал этого делать. Это означало получить доступ к почте Theorem, а Раг знал, что если у него будет возможность, то он прочтет ее письма. Theorem была популярной личностью в Altos, и, будучи подозрительным, Раг был уверен, что запросто может посчитать преступлением нечто совершенно невинное. Ему придется поспорить с Theorem, а драгоценное время их общения было слишком дорого ему.

– Слишком дружеские, – продолжил Corrupt. Должно быть, ему нелегко дались эти слова. Умыкнуть пароль у девушки друга и вломиться в ее учетную запись – это одно дело. Но залезть в такие сведения – это просто низость. Особенно с тех пор, как Corrupt работал с Gandalf'ом в 8lgm.

– Спасибо, – в конце концов выдал Раг и отключился.

Когда Раг попытался ввести пароль MOD, он, естественно, не сработал, потому что Gandalf заблокировал учетную запись. Но Раг об этом не знал. Когда он обнаружил, что учетная запись Theorem заблокирована, он не очень обеспокоился. Но когда он узнал, кто это сделал, то не был так уж счастлив. Когда он прямо спросил об этом Theorem, она отрицала любые домыслы по поводу ее отношений с Gandalf'ом.

Что оставалось Раг'у? Он мог поверить Theorem, а мог усомниться в ней. Верить было трудно, а сомневаться было больно. Поэтому он решил поверить.

Этот инцидент заставил Theorem приглядеться к Altos повнимательнее. Он стал причиной не самых лучших событий в ее жизни. Когда она была лишена доступа в немецкую чат-систему, она сделала неприятное для себя открытие. Theorem поняла, что попала в зависимость сродни наркотической. И ей это совсем не понравилось. Посмотрев на свою жизнь совсем другими глазами, Theorem вдруг осознала, что она совсем забросила своих друзей и свою жизнь в Швейцарии. Какого черта она думала, проводя каждую ночь за экраном компьютера?

И Theorem приняла твердое решение.

Она решила навсегда прекратить общение в Altos.

:)

В конце ноября 1991 года Раг прилетел в Нью-Йорк из Вирджиния-Бич. Один знакомый, по имени Морти Розенфельд [Morty Rosenfeld], который какое-то время болтался с хакерами из MOD, пригласил его в гости. Раг подумал, что поездка в Нью-Йорк пойдет ему на пользу.

Морти не был, что называется, лучшим другом Раг'а, но он был своим парнем. Несколькими месяцами ранее он был обвинен федералами в продаже пароля для входа в финансовую компанию, в результате чего произошло мошенничество с кредитными картами. Раг не опускался до продажи паролей, но каждому свое. В небольших дозах Морти был неплох. Он жил на Кони-Айленде. Это мало напоминало Виллидж на Манхеттене, но все же что-то общее было. Кроме того, у Морти был раскладной диван-кровать. Это гораздо лучше, чем спать где-то на полу.

Раг проводил время с Морти и его друзьями, выпивая и валяя дурака с компьютером Морти.

Однажды утром Раг проснулся в состоянии ужасного похмелья. У него урчало в животе, а в холодильнике не было ничего съестного, поэтому он позвонил и заказал свинину с жареным рисом в службе доставки китайского ресторана. Затем он натянул штаны и сел на кровать, закулив сигарету в ожидании заказа. Он начал курить в 19 лет, примерно к концу второго года своей нелегальной жизни. Это успокаивало нервы.

Во входную дверь постучали. Желудок Раг'а заурчал в ответ. Направляясь к двери, он подумал: «Свинина с жареным рисом, я иду к тебе». Но когда Раг открыл дверь, он обнаружил нечто совершенно другое.

Секретная служба.

Двое мужчин. Один постарше, изысканный джентльмен, стоял слева. Рядом с ним молодой парень. Глаза молодого широко раскрылись, когда он увидел Раг'а.

Вдруг он толкнул Раг'а. И еще раз. И еще. Короткие, жесткие, быстрые толчки. Раг не мог обрести равновесие. Всякий раз, как ему удавалось ощутить пол под ногами, агент снова толкал хакера назад, пока тот не уперся в стену. Агент крутанул Раг'а так, что его лицо прижалось к стене, и ткнул его пистолетом под ребра. Затем он защелкнул на нем наручники и начал обыскивать его в поисках оружия.

Раг посмотрел на Морти, который всхлипывал в углу, и подумал: «Ты стукнул на меня».

Когда Раг был надежно скован наручниками, агенты показали ему свои жетоны. Затем вывели его из дома, усадили в машину и направились на Манхеттен. Они остановились напротив World Trade Center, и когда Раг вышел из машины, молодой агент перестегнул наручники так, чтобы руки беглеца оказались спереди.

Когда агенты сопровождали скованного беглеца по эскалатору, весь корпоративный персонал пялился на странную тройцу. Бизнесмены и бизнес-леди в строгих темно-синих костюмах, секретарши и клерки глядели на них во все глаза с противоположного эскалатора. Если кому-то было мало наручников, он мог обратить внимание на нейлоновую куртку молодого агента Секретной службы с заметным выступом в форме пистолета на переднем кармане.

«Почему эти парни провели меня через *парадный* вход?» – продолжал думать Раг. Здесь, конечно же, есть черный ход или вход с парковки. Во всяком случае, что-то не столь открытое взглядам.

Вид с любого достаточно высокого этажа WTC захватывал дыхание, но Раг'у так и не представился шанс насладиться этой красотой. Его втолкнули в комнату без окон и приковали к стулу. Агенты входили и выходили, уточняя разные формальности. Они ненадолго освободили Раг'а, чтобы намазать его пальцы черной краской и прокатать их по листам бумаги. Затем они заставили его дать им образцы почерка сначала правой, а затем левой руки.

Раг не возражал, что его так надолго приковали к стулу, но вид железной клетки в центре комнаты, где у него брали отпечатки, вгонял в тоску. Она напомнила ему клетки для животных вроде тех, что использовались в старых зоопарках.

Два арестовавших его агента вышли из комнаты, но появился другой. И этот третий был далек от дружелюбия. Он принялся играть в плохого копа, он оскорблял Раг'а и орал на него, стараясь лишить парня присутствия духа. Но как бы ни надрывался агент, его вопли не могли оказать на Раг'а большего воздействия, чем вопросы, которые он задавал.

Агент ни разу не спросил его о Citibank. Зато он хотел знать все, что было известно Раг'у о TRW.

Все самые ужасные кошмары Раг'а о спутнике-убийце и о том, что он стал человеком, который

слишком много знает, пронеслись в его голове.

Раг отказался отвечать. Он просто молча смотрел на агента.

Дело кончилось тем, что в комнату вошел агент, тот, что постарше, оттащил от Раг'а агента-питбуля, вывел его из комнаты и начал шептать ему что-то в коридоре. После этого агент-питбуль был сама мягкость и лучезарность в обращении с Раг'ом. И больше ни слова о TRW.

Раг не мог понять, почему старший агент приказал своему подчиненному заткнуться насчет оборонного подрядчика. Что крылось за этим внезапным молчанием? Резкая перемена встревожила Раг'а не меньше, чем вопросы, заданные ему вначале.

Агент сказал Раг'у, что он будет помещен под стражу в ожидании передачи властям Калифорнии. Когда формальности были улажены, они освободили его от наручников и позволили встать, чтобы размяться. Раг попросил сигарету, и один из агентов угостил его. Затем вошли еще двое агентов – молодые ребята.

Молодые агенты были настроены очень дружелюбно. Один из них даже пожал Раг'у руку и представился. Они знали о хакере все. Они знали его голос по сообщениям с голосовых почтовых ящиков, которые он нелегально создавал для себя. Из материалов его дела, представленных калифорнийской полицией, а может, и по фотографиям, сделанным во время наружного наблюдения, они знали, как он выглядит. Они знали о его личных качествах из перехваченных разговоров на телефонных мостах и из материалов Секретной службы. Должно быть, они шли за ним по пятам по всей стране, по следам улики, оставленных на его пути. Но какие бы следственные мероприятия они не провели, ясно было одно: эти агенты знали его очень близко. Как человека, а не как хакера. Это было странное чувство. Молодые ребята, которых Раг никогда раньше не встречал, болтали с ним о последнем видео Майкла Джексона, словно он был их соседом или приятелем, вернувшимся из другого города. Затем они отвезли его в другой район, в полицейский участок, чтобы заполнить очередные бумаги, необходимые для экстрадиции.

Это место очень отличалось от роскошных офисов World Trade Center. Раг разглядывал облупившуюся серую краску на стенах и полицейских, печатающих двумя пальцами на электрических пишущих машинках по методу «найди-и-стукни», – и ни одного компьютера в пределах видимости. Копы не приковали Раг'а к столу. Он был в самом сердце полицейского участка, и у него не было ни единого шанса сбежать.

Когда детектив, которому поручили Раг'а, отошел от своего стола минут на десять, Раг заскучал. Он начал перебирать папки с другими делами на столе детектива. Это были серьезные дела – мафия и отмывание доходов от продажи наркотиков – дела, которые имели отношение к ФБР. Эти люди выглядели неприятно.

В тот же день Раг ненадолго появился в суде, лишь для того, чтобы получить направление в тюремный комплекс на Манхэттене, известный как Tombs,<sup>[p99]</sup> где ему предстояло дожидаться, пока власти Калифорнии не заберут его.

Раг провел в Tombs почти неделю. На третий день он уже лез на стены. Его словно похоронили заживо.

Всю эту неделю Раг почти не имел контакта с другими человеческими существами – страшное наказание для того, кто нуждается в постоянном притоке свежей информации. Он ни разу не выходил из камеры. Надзиратель просовывал поднос с едой в его камеру, а затем забирал его.

На шестой день Раг съехал с катушек. Он закатил истерику, начал кричать и колотить в дверь. Он проклинал надзирателя и кричал, что хочет выбраться отсюда к гребаной матери. Охранник сказал, что посмотрит, сможет ли он перевести Раг'а на Рикерс-Айленд, в известную нью-йоркскую тюрьму. Раг'у было все равно, хоть на Луну, лишь бы выбраться из одиночного заключения.

;) )

Если не принимать во внимание серийного убийцу, северный изолятор на Рикерс-Айленд был значительно приятнее Tombs. Раг'а запирали в камеру только на ночь. Днем он мог свободно бродить по двору изолятора вместе с другими заключенными. Некоторые из них были здесь потому, что власти не хотели помещать их вместе с закоренелыми преступниками; другие оказались в изоляторе потому, что, возможно, были невменяемы.

Это была невероятная смесь. Пожарник, ставший специалистом по краже драгоценностей. Колумбийский наркобарон. Хозяин автомастерской, который скупил больше трехсот краденых автомобилей, разобрал их, затем снова собрал и продал как новые. Человек, убивший гомосексуалиста, пытавшегося его соблазнить. Faggot Killer, *[p100]* как его называли в тюрьме, не собирался никого убивать, просто ситуация слегка вышла из-под контроля. Когда он пришел в себя, ему грозило двенадцать лет тюрьмы за убийство.

Раг не был в восторге от знакомства с убийцей, но он нервничал из-за того, что может случиться с молодым человеком в тюрьме. Если он станет изображать дружбу с Faggot Killer'ом, всем все будет понятно. Кроме того, парень вроде выглядел нормально. Ну, до тех пор, пока ты не смотрел на него не так, как следует.

В первый же день Раг познакомился и с Кентукки, человеком с дикими глазами, который представился, сунув в руки хакеру скомканную газетную вырезку и сказав: «Это обо мне». Статья под названием «Голоса велели ему убивать», описывала, как полиция задержала серийного убийцу, который считался ответственным как минимум за десять убийств. Кентукки рассказал Раг'у, что последней жертвой была женщина, и он написал имена пришельцев, управлявших им, кровью этой женщины на стене ее квартиры.

Специалист по драгоценностям попытался предупредить Раг'а, чтобы тот держался подальше от Кентукки, потому что тот продолжал регулярно входить в контакт с пришельцами. Но было слишком поздно. Кентукки решил, что ему не нравится молодой хакер. Он начал орать на Раг'а, затеяв драку. Раг стоял, растерянный и ошеломленный. Как вести себя с разъяренным серийным убийцей? И какого черта он оказался в одной тюрьме с этим маньяком? Это было чересчур.

Бывший пожарный поспешил к Кентукки и попытался успокоить его, разговаривая как можно мягче. Кентукки сверкал глазами в сторону Раг'а, но перестал бесноваться.

Через несколько дней Faggot Killer пригласил Раг'а сыграть в «Башни и Драконы». Это было интересней, чем смотреть весь день ток-шоу по телевизору, и Раг согласился. Он подсел к складному столику, где Faggot Killer разложил ставки.

И вот Раг, двадцатилетний компьютерный хакер из Калифорнии, принц сетей X.25, принялся играть в «Башни и Драконы» с грабителем ювелирных магазинов, убийцей-гомофобом и безумным серийным убийцей в тюрьме Рикерс-Айленд. Раг поймал себя на том, что очарован сюрреализмом ситуации.

Кентукки сам влез в игру. Он начал с того, что стал убивать домовых.

– Я возьму свою алебарду, – начал Кентукки с улыбкой, – и зарублю этого гоблина.

Следующий игрок готовился сделать свой ход, но Кентукки перебил его.

– Я еще не закончил, – медленно сказал он, и дьявольская ухмылка проступила на его лице. – Я разрублю его на куски. И разрежу его. Кровь будет повсюду.

Лицо Кентукки напряглось от удовольствия. Трое остальных игроков нервно вжались в свои стулья. Раг посмотрел на Faggot Killer'а тревожным взглядом.

– И я воткну нож в его сердце, – продолжал Кентукки, и его голос становился все громче от возбуждения. – Кровь, кровь, всюду кровь. И я беру нож, и кромсаю его. И кромсаю, кромсаю, кромсаю.

Кентукки отскочил от стола и принялся размахивать в воздухе рукой с воображаемым кинжалом, не переставая вопить: «Кромсаю, кромсаю, кромсаю!»

Затем Кентукки вдруг затих. Все за столиком оцепенели. Никто не смел пошевелиться из опасения, что он опять выйдет из себя. Желудок Раг'а подкатил к горлу. Он попытался прикинуть, сколько времени ему потребуется, чтобы выскочить из-за стола и убежать в дальний конец комнаты.

В оцепенении Кентукки отошел от столика, уперся лбом в стену и начал что-то бормотать. Грабитель медленно приблизился к нему и немного поговорил с ним успокаивающим тоном, прежде чем вернуться к столу.

Один из охранников услышал шум и подошел к ним.

– С этим парнем все в порядке? – спросил он указывая на Кентукки.

«Смотря что ты под этим разумеешь», – подумал Раг.

– Оставьте его в покое, – сказал грабитель охраннику. – Он разговаривает с пришельцами.

– Ладно, – охранник повернулся и вышел.



Каждый день медсестра приносила Кентукки специальные лекарства. Большую часть времени Кентукки проводил как в тумане, выпив свою порцию ужасной вонючей жидкости. Но иногда он припрятывал лекарство, чтобы продать его другому заключенному, у которого появлялось желание вырубиться на день-другой.

Те дни, когда Кентукки продавал лекарство, были ужасны. В один из таких дней он попытался убить Раг'а.

Раг сидел на металлической скамье, разговаривая с другими заключенными, как вдруг почувствовал, что кто-то обхватил его рукой вокруг шеи. Он попытался обернуться, но не смог.

– Ну вот. Сейчас я покажу тебе, как я убил вот так же одного парня, – прошептал Кентукки Раг'у.

– Нет-нет, – начал было Раг, но бицепс Кентукки сдавил его кадык. Раг почувствовал себя словно в тисках.

– Да. Вот так. Я сделал это вот так, – сказал Кентукки, напрягая мускулы и откидываясь назад.

– Нет! Слушай, не надо. Все нормально.

Раг едва дышал. Он судорожно молотил руками перед собой, но ничего не мог поделать.

«Вот и все, – подумал он. – Мне конец». «Хакер убит маньяком в Рикерс-Айленд». «Голоса велели мне сделать это».

Вездесущий грабитель подошел к Кентукки и принялся нашептывать ему на ухо, чтобы тот отпустил Раг'а.

Затем, когда Раг уже попрощался с жизнью, грабитель оттолкнул от него Кентукки.

С этого дня Раг никогда не забывал садиться спиной к стене.

После почти месячного заключения Раг'у сообщили, что за ним приехал офицер из службы шерифа графства Монтеррей, чтобы забрать его в Калифорнию. Раг был не против экстрадиции, особенно после того, как он увидел изнанку тюрем Нью-Йорка. Встреча с федеральным прокурором Нью-Йорка тоже помогла ему прояснить ситуацию.

Визит в Генеральную прокуратуру США в Нью-Йорке стал настоящей головной болью для Ричарда Розена, который снова взял дело Раг'а. Они не собирались сотрудничать. Они разыгрывали «Королеву на день».

Способ, с которым они вступили в переговоры с Розеном, напомнил ему старую американскую телеигру с таким названием. Ведущий шоу выдергивал какую-нибудь невинную душу прямо с улицы, усаживал на роскошный трон, задавал вопросы и вручал призы. В каком-то смысле прокуратура тоже собиралась усадить Раг'а на трон и задать ему множество вопросов. По окончании этой свободной беседы предполагалась раздача призов. Тюремные сроки. Штрафы. Приговоры. Они считали, что надо сделать именно так. Никаких гарантий. В конце шоу они решат, сможет ли Раг претендовать на снисхождение.

Раг знал, что им было нужно. Они хотели получить от него улики против ребят из MOD. Но у него и не было ничего подобного. Положение было тухлым, поэтому Раг решил не противиться возвращению в Калифорнию. Там не может быть хуже, чем в Нью-Йорке, с его полоумными зеками и злобными федеральными прокурорами.

Офицер из офиса шерифа Монтеррея приехал за Раг'ом 17 декабря 1991 года. Следующие несколько недель Раг провел в калифорнийской тюрьме. Он делил камеру с мексиканскими драг-дилерами и другими мафиози, но в конце концов понял, как вести себя с этими людьми. В отличие от многих в Рикерс, они не были оцепеневшими лунатиками, болтающими невзвешенно.

Ричард Розен снова взял дело Раг'а, несмотря на то, что Раг уже однажды подвел его. Раг считал, что это очень великодушно с его стороны. Но Раг и не подозревал, какую услугу оказывает ему Розен, до тех пор, пока не наступил день суда.

Раг позвонил Розену из тюрьмы, чтобы поговорить о деле. У Розена была для него важная новость.

– Признай себя виновным. Ты должен признать свою вину по всем пунктам, – сказал он Раг'у.

Раг подумал, что у Розена поехала крыша.

– Нет. Мы можем выиграть, если ты признаешь себя виновным, – заверил его Розен.

Раг ошарашенно присел с трубкой в руке.

– Доверься мне, – сказал адвокат.

Дотошный Ричард Розен нашел сокрушительное решение.

Раг признал себя виновным 23 декабря 1991 года по двум пунктам обвинения в суде по делам несовершеннолетних графства Монтеррей. Он признал все. Без разбора. Да, я Parmaster. Да, я взламывал компьютеры. Да, я украл тысячи номеров кредитных карт из компьютера Citibank. Да, да, да.

Казалось, что с юношей происходит катарсис, но причиной было то, что Раг знал – у Розена в рукаве есть сильный козырь.

Розен ускорил слушание, чтобы быть уверенным, что дело будет рассматриваться в суде для несовершеннолетних, где Раг мог надеяться на более снисходительный приговор. Но спешка Розена не означала, что он был небрежен. Когда он буквально под микроскопом в очередной раз изучал дело Раг'а, он обнаружил, что в официальных документах датой рождения его подзащитного значилось 15 января 1971 года. На самом деле Раг родился несколькими днями раньше, но в офисе окружного прокурора об этом не знали.

По калифорнийским законам под юрисдикцию суда по делам несовершеннолетних попадают граждане до 21 года. Но суд будет рассматривать дело и вынесет приговор только в том случае, если преступление было совершено до 18 лет, а во время рассмотрения дела и оглашения приговора обвиняемому еще не исполнилось 21 года. Раг должен был предстать перед судом 13 января, но 8 января Розен заявил, что дело провалилось. Когда заместитель окружного прокурора Дэвид Шотт [David Schott] спросил, почему, Розен взорвал свою бомбу.

Раг'у уже исполнился 21 год, так что суд по делам несовершеннолетних больше не имел власти для вынесения приговора. Кроме того, в Калифорнии дело не могло быть перенесено в суд для взрослых, если ответчику уже был предъявлен иск в подростковом суде. По букве закона дело должно было быть закрыто.

Заместитель окружного прокурора был потрясен. Он брызгал слюной и сыпал проклятиями. Генеральная прокуратура переменяла оригинальные обвинения с уголовных на административные. Они собрались на совет. Как это могло случиться? Раг был в *розыске*. Он бегал больше двух лет от проклятой Секретной службы, дьявол его раздери. Ни за что – НИ ЗА ЧТО – он не должен был уйти безнаказанным из зала суда.

Суд попросил Раг'а назвать дату его рождения. Быстрая проверка его водительских прав в департаменте регистрации транспортных средств показала, что Раг и его адвокат сказали правду. Так что Раг вышел из здания суда совершенно свободным.

Оказавшись на улице, Раг подставил солнцу лицо. Солнце казалось чудом после почти двух месяцев в трех разных тюрьмах в противоположных концах страны. Гулять было прекрасно. Он просто бродил по улицам и был абсолютно счастлив.

Несмотря на все это, Раг так и не смог перестать бежать.

С того момента, как он вышел свободным из окружной тюрьмы Салинаса в Калифорнии, он продолжал колесить по стране, нанимаясь на временную работу то здесь, то там. Ему было очень тяжело находиться подолгу на одном месте. Хуже всего было то, что с ним начали происходить странные вещи. Точнее, они с ним всегда происходили, но с каждым месяцем они становились все более странными. Его восприятие реальности изменилось.

Сначала был инцидент в комнате мотеля. Когда Раг в одном из своих трансамериканских путешествий остановился в Las Vegas Travelodge, то услышал, что кто-то ходит по комнате под ним этажом ниже. Раг напряг слух. Казалось, что этот человек разговаривает с ним. Что он хотел сказать ему? Раг не мог разобрать ни слова, но чем больше он слушал, тем сильнее убеждался в том, что человек стремится что-то сообщить лично Раг'у, но не хочет, чтобы его услышал кто-то еще. Это было большое разочарование. Как Раг ни старался, как он ни прикладывал ухо к полу и к стене, он так и не смог ничего разобрать.

Сюрреалистические переживания продолжались. По словам Раг'а, путешествуя по Мексике, он почувствовал себя очень странно и как-то после полудня решил обратиться за помощью в американское консульство. Но все в консульстве повели себя очень странно.

Они попросили у него какие-нибудь документы, и он дал им свой бумажник. Они взяли его карточку социального страхования и калифорнийское удостоверение личности и велели подождать. Раг подумал, что они собираются ввести его данные в компьютер. Пока он дожидался ответа, его ноги начали дрожать и он затрясся всем телом. Это была не минутная легкая дрожь, его било, как в лихорадке, словно он сидел в эпицентре землетрясения. Это испугало Раг'а. Сотрудники консульства в изумлении вытаращились на него.

В конце концов он престал трястись. Вернулся сотрудник консульства и попросил его уйти.

– Здесь никто не сможет вам помочь, – заявил он Раг'у.

Почему консульский чиновник говорит с ним в таком тоне? Что это *означает* – Раг должен *уйти*? Что он *на самом деле* хочет этим сказать? Раг не мог понять его. Появился еще один сотрудник. Он подошел к Раг’у с наручниками. Почему все ведут себя так странно? Это *компьютер*. Может быть, они обнаружили дополнительную информацию рядом с его фамилией в этом компьютере.

Раг попытался объяснить им ситуацию, но работники консульства явно не хотели его понимать. Он стал рассказывать им, как он два с половиной года скрывался от Секретной службы, но получил в ответ лишь еще более подозрительные взгляды. Пустые лица. No comprende. [p101] Чем больше он объяснял, тем более непроницаемыми становились их лица.

Чиновники сказали ему, что на сегодня приемные часы консульства закончились. Он должен покинуть здание. Но Раг подозревал, что это была лишь отговорка. Через несколько минут появился мексиканский полицейский. Он поговорил с одним из консульских, который передал ему, как показалось Раг’у, пачку песо, обернутых полоской бумаги.

В консульство вошли еще двое полицейских. Один из них подошел к Раг’у и крикнул: «Вон!» Но Раг не ответил. Тогда мексиканские полицейские схватили его за руки и за ноги и вынесли из консульства. Раг был потрясен и возмущен, и когда они пересекали порог консульства, он закричал.

Мексиканцы посадили Раг’а в полицейскую машину и отвезли его в участок, где он провел ночь.

На следующий день его отпустили. Он бродил по городу, пока снова не уперся в консульство Соединенных Штатов. Знакомый сотрудник консульства подошел к нему и спросил, как он себя чувствует.

Раг сказал: «ОК».

Затем Раг спросил у чиновника, не может ли тот помочь ему добраться до границы. Чиновник сказал, что может. Через несколько минут белый микроавтобус подобрал Раг’а и доставил его к пограничному пункту. Когда они приехали, Раг спросил у водителя, не мог бы он дать ему два доллара, чтобы Раг мог купить билет на поезд. Водитель дал ему два доллара.

Раг сел на поезд, не имея никакого понятия о том, куда он направляется.

Theorem дважды приезжала в Калифорнию к Раг’у в 1992 году, и их отношения продолжались. Раг пытался найти работу, чтобы получить возможность вернуть Theorem \$20 000. Такая сумма набралась за то время, пока он был в бегах и под судом. Но устроиться на работу было очень трудно.

Никто не горел желанием нанять его.

– У вас нет компьютерных навыков, – говорили ему. Он спокойно объяснял, что, напротив, у него, конечно же, есть компьютерные навыки.

– Что ж, скажите, какой университет вы закончили?

Нет, он получил свои компьютерные знания не в университете.

– Хорошо, в каких компаниях вы приобрели ваш опыт работы?

Нет, он получил свой компьютерный опыт не во время работы в какой-либо компании.

– Ладно, а что вы делали с 1989 по 1992 год? – Служащий агентства по трудоустройству неизбежно задавал этот вопрос безнадежным голосом.

– Я... мм... путешествовал по стране.

А что еще Раг мог сказать? Как он мог на это ответить?

Если ему везло, агентство могло поручить ему тупую работу по обработке данных за \$8 в час. Если же нет, он соглашался и на простую канцелярскую работу за еще меньшие деньги.

К 1993 году в отношениях с Theorem наметилась трещина. После четырех с половиной лет они расстались. Расстояние было слишком велико, во всех смыслах. Theorem нуждалась в более стабильной жизни. Может быть, она не стремилась завести традиционную швейцарскую семью с тремя детьми и симпатичным шале в Альпах, но, во всяком случае, ей нужно было что-то большее, чем неустойчивая жизнь Раг’а в дороге.

Расставание было мучительно болезненным для обоих. Они продолжали общаться еще несколько недель после принятия решения. Theorem все время думала о том, что совершает ошибку. Она думала о том, чтобы вернуть Раг’а. Но не стала этого делать.

Раг нашел утешение в алкоголе. Текила, рюмка за рюмкой. Выпить. Стукнуть стопкой о стойку.

Наполнить до краев. Опрокинуть в глотку. Через какое-то время он отключался. Потом он ужасно мучился несколько дней, но старался не обращать на это внимания. Такое состояние очищало его.

Примерно в это время Розену удалось вернуть вещи Раг'а, изъятые Секретной службой во время обыска. Он передал Раг'у устаревший компьютер и другое оборудование вместе с дискетами, распечатками и записями.

Вооружившись бутылкой Jack Daniels, Раг собрал все доказательства по своему делу и устроил костер. Он разорвал распечатки, облил их бензином для зажигалок и поджег. Он бросал в огонь дискеты и смотрел, как они тают в языках пламени. Страницу за страницей он просматривал свои записи и официальные отчеты, вспоминая некоторые эпизоды. Затем стал комкать каждый лист и по очереди швырять их в огонь. Он даже плеснул сверху немного виски для пущей уверенности.

Когда он вырывал страницы из доклада Секретной службы, комкая их в бумажные шарики, кое-что привлекло его внимание и удивило. В результате серии обысков и рейдов, последовавших за налетом на дом Раг'а на День благодарения в 1988 году, многие хакеры по всему миру подверглись преследованиям властей. Eric Bloodaxe, парни из MOD и LOD, The Atlanta Three, Pad и Gandalf, австралийцы – все они пережили обыски или аресты в 1988–1990 годах.

Как были связаны все эти события? Могли ли правоохранительные органы трех континентов быть настолько организованы, чтобы координировать всемирную атаку на хакеров?

Отчет Секретной службы дал ему ключ. В нем говорилось, что в декабре 1988 года два информатора позвонили специальным агентам особого подразделения Секретной службы и сообщили им информацию насчет Раг'а. По сведениям этих информаторов – они оба были хакерами – оказывалось, что Раг вовсе не был «хакером Citibank», которого искало агентство. Они сказали, что настоящего «хакера Citibank» зовут Phoenix.

Phoenix из Австралии.

## 5

### Священный Грааль

*И вот мы пришли, захватили, отняли  
Богатства общинников и королей.*

**Песня «Rivers Run Red», альбом «Blue Sky Mining» группы Midnight Oil<sup>24</sup>**

Это было написано черным по белому. Две статьи Хелен Мередит [Helen Meredith] в *The Australian* в январе 1989 года.<sup>25</sup> Весь компьютерный андеграунд Австралии бурлил от этой новости. Первая статья появилась 14 января:

#### НА СЧЕТУ ХАКЕРОВ CITIBANK \$500 000

Элитная группа австралийских хакеров украла более \$US 500 000 (\$580 000) из Citibank, совершив одно из самых дерзких хакерских преступлений за всю историю Австралии.

Австралийские федеральные власти заявили позавчера, что они сотрудничали с американскими властями над выявлением австралийской цепочки, включающей хакеров в Мельбурне и Сиднее.

Это элитные «фрикеры» технологической преступности – цифровые преступники, которые генерируют импульсы, проходящие по телефонным линиям, чтобы получить доступ в коммуникационные каналы. Этот метод известен как «blue boxing».

Сообщается, что австралийская группа воспользовалась телефоном в системе штаб-квартиры Telecom на Уильям-стрит, 199 в Мельбурне, чтобы послать сигнал частотой 2600 Гц, который позволил им получить доступ к магистральной линии, а затем к менеджерскому коду Citibank.

По информации наших источников, прошлой ночью хакеры сняли со счетов американского банка \$US 563 000 и перевели их на несколько других счетов. Деньги пока еще не возвращены.

<sup>24</sup> Слова и музыка: Rob Hirst/James Moginie. © Copyright 1989 Sprint Music. Administered for the World-Warner/Chapell Music Australia Pty Ltd. Used by Permission.

<sup>25</sup> Далее с разрешения News Ltd. и Хелен Мередит приведен полный текст статей.

Власти идут по следу, о котором говорилось в «The Australian» во вторник. Этот след указывает, что австралийские хакеры также имеют отношение к нелегальному доступу к номеру модемного набора Агентства национальной безопасности США, используемому Генеральным консульством США в Мельбурне.

Тем временем полиция штата Виктория заявила, что ее сотрудники проводят постоянные обыски в домах десятков подозреваемых, не переставая разыскивать хакеров.

Предполагается, что хакеры получили доступ к двумстам номерам кредитных карт, опубликованных в частном секторе компьютерной доски объявлений.

Очевидно, эти номера получены группой опытных хакеров, которые, по всей вероятности, использовали их для заказов товаров по телефону за счет ничего не подозревающих владельцев кредитных карт.

Достоверный источник заявил, что детективы Бюро криминальных расследований с ордерами на обыск в настоящее время досматривают собственность хакерского сообщества и ожидают обнаружить товаров на сотни тысяч долларов.

Вторая статья была опубликована десять дней спустя.

Хелен Мередит.

### СПИСОК КРАДЕННЫХ КАРТ ВЕДЕТ К ДОСКАМ ОБЪЯВЛЕНИЙ

Официальные власти скептически относятся к последним сообщениям о международном хакерско-фрикерском кольце и его австралийском отделении.

Тем не менее вчера получены доказательства, указывающие на подозрительные BBS, базирующиеся в Мельбурне.

Фрикеры используют устройства тонового набора, чтобы отправлять сигналы, которые дают им доступ к бесплатным магистральным линиям, тогда как хакеры взламывают компьютерные системы.

В последней проверке деятельности доски объявлений было обнаружено сообщение от американского хакера, известного как Captain Cash. Это сообщение доказывает причастность австралийцев к последним событиям с австралийскими же кредитными картами и свидетельствует об их нелегальном использовании американскими хакерами. Речь идет о сумме \$US 362 018 (\$416 112).

Информация была обнаружена в компьютерной системе доски объявлений Pacific Island, чрезвычайно популярной среди австралийских хакеров.

Сообщение гласило:

– Порядок с серией 53 53, мы закрываем ее сегодня – MasterCard \$109 400,50. Теперь серия 4564 – Visa. Я оставляю ее открытой на неделю – \$209 417,90. И на старой доброй «не-выходи-без-нее-из-дома» – \$43 200.

– В общем и целом – \$362 018,40.

– Передай это нашим австралийским друзьям!

– Они, как всегда, на высоте!

– Они посылают больше номеров на 23-й! Отлично!

– Они получают 10 %, как всегда... неплохой куш в \$36 200!

На доске объявлений также помещались советы фрикерам по использованию телефонов в штаб-квартире Telecom на Уильям-стрит, 199 и новой телефонной станции на Спенсер-стрит в Мельбурне, чтобы получать возможность осуществлять бесплатные телефонные звонки.

Сообщение от местного хакера, известного как Force, описывало «прикольный метод взламывать системы с очень крутой безопасностью».

Этот метод подразумевает использование исходящего «pad» на таких системах, как Vax, Unix и особенно Prime.

Phoenix, другой пользователь местной BBS, просматривал цены на таблетки «экстази»: таблетка обычной крепости – \$40; двойной крепости – \$60; тройной крепости – \$70.

«Сообщи детали по электронной почте. Божественно-декадентский экспириенс».

В прошлую пятницу *The Australian* получила доказательства, подтверждающие причастность группы австралийских хакеров, известной под названием Realm, к взлому сети Citibank США.

## БОМБА

На австралийской доске объявлений, используемой хакерами Realm, помещается и такая смертельно опасная информация, как рецепт изготовления бомбы, который появился на американской доске объявлений в прошлом году. Четверо подростков, решивших воспользоваться рецептом, погибли, когда их бомба домашнего изготовления взорвалась в Вашингтоне в канун Нового года.

Этот рецепт можно свободно получить на мельбурнской доске объявлений, именуемой Pacific Island.

Связи банды в США, вероятно, ведут в Милуоки и Хьюстон. Американские федеральные власти уже предприняли действия против хакеров, принимавших участие во взломе Citibank.

В ходе секретной операции Бюро криминальной разведки австралийская группа была поставлена под наблюдение. На прошлой неделе появились результаты более чем полугодовой слежки за деятельностью Pacific Island и связанных с ней Zen и Megaworks.

Но утечка в потоке информации между полицейскими подразделениями, очевидно, серьезно помешала намерениям полиции положить конец деятельности преступников на досках объявлений.

На прошлой неделе также осуществлялась проверка входящих сообщений, касающихся кардинга (нелегального использования карточных счетов) из Гонконга, Франции и Израиля.

Австралийские хакеры в большинстве своем базируются в Мельбурне. В основном это подростки, подозреваемые или уже осужденные за мошенничество, употребление наркотиков и угон автомобилей. Большая часть из них считается, в лучшем случае, электронными вуайеристами, в худшем – преступниками с большими криминальными связями.

Информация, полученная *The Australian*, ясно говорит о том, что австралийские хакеры причастны к взлому сети Citibank, советам по фрикингу (использованию телефонных сетей для получения нелегального доступа к иностранным компьютерным сайтам) и по доступу к банковским системам.

Ниже следующее представляет собой цитату, взятую непосредственно с доски объявлений (с некоторой необходимой редакторской правкой). Это хранилось в частном почтовом ящике и адресовано хакером, известным под псевдонимом Ivan Trotsky, тому, кто называет себя Killer Tomato:

– О'кей, вот такие дела...

– Когда Sysop получил звонок от федералов, им нужны были имена Force, Phoenix, Nom, Brett Macmillan и мое в связи с хакерскими делами Realm и некоторыми кардерскими проблемами.

– А мне пару дней назад пришла информашка о том, что в американском Citibank устроили взлом, и это привело к арестам, и что все это связано с Force и Electron. Еще там говорилось о том, «как связан Trotsky с взломом Citibank», мы просто в дерьме, да, я член Realm (я думаю, никому не должно быть до этого дела, но они думают по-другому), но я никогда не занимался вместе с ними никакими взломами.

– Но теперь говорят, что я связан со всем этим дерьмом, я в полной жопе, тем более что всем этим занимается ЦРУ, может, тебе кажется, что я несу чушь, я сам бы так сказал, если бы ты сходил с ума так же, как я, надеюсь, ты спокойно отсидишься, а в моем заборе полно дыр.

– Когда мы вломились в тот раз, мы даже толком не знали, что мы нашли, пока Blue Blunder не сказал, что пришли какие-то деньги. На PI можно делать все, что ты захочешь.

– У нас будет новый сеанс хакинга весь уик-энд, но это зависит от того, откуда мы будем это делать. Это должно быть очень надежное место.

– Мы сумели достать кое-что по карточкам, но мать с отцом заставили меня выбросить бумаги, я держал их в вентиляционной трубе. Смог сохранить их на паре учетных записей в PI.

В пятницу *The Australian* передал информацию по фрикингу, обнаруженную на доске объявлений австралийской Telecom.

Другая информация, которой делились хакеры во время этого разговора, имеет отношение к мошенничеству с кредитными картами, кардингу.

Представитель службы мониторинга DPG, мистер Стюарт Гилл, заявил, что, по его мнению, материалы, полученные с Pacific-Island, являются лишь верхушкой айсберга.

Он сказал: «Они гораздо лучше организованы, чем полиция. Если кто-нибудь не классифицирует их деяния и мы не примем против них соответствующие законы, мы снова будем говорить об этих же проблемах ровно через год».

Вчера полиция Южной Австралии начала операцию с целью взять под наблюдение BBS в этом штате.

Обе политические партии Западной Австралии пришли к соглашению, что, независимо от того, кто придет к власти в штате, расследование хакерских преступлений будет проведено должным образом.

Полиция Виктории и ее отдел по делам мошенничества объявили на прошлой неделе о создании отдела по борьбе с компьютерными преступлениями, который будет расследовать жалобы, связанные с компьютерным мошенничеством.

Многими в компьютерном подполье эти статьи были восприняты очень болезненно.

Кто такой этот Captain Cash? A Killer Tomato? Многие считали, что за обоими этими хэндлами скрывается Стюарт Гилл или что Гилл подделал их и другие сообщения на доске Craig Bowen'a. Были весь андеграунд на стороне мошенников? Нет. Они составляли лишь ничтожную часть сообщества. Как могли мельбурнские хакеры украсть полмиллиона долларов из Citibank? Никак. Последующее полицейское расследование подтвердило, что эти голословные утверждения были полностью сфабрикованы.

Как могли сообщения за полгода с PI и Zen попасть в руки Бюро криминальной разведки полиции штата Виктория? У подпольщиков имелись соображения на этот счет.

Некоторые были уверены, что Стюарт Гилл сыграл в подполье роль торговца информацией. Он скармливал полиции определенные сведения и получал от нее в обмен кое-какой новый материал. Затем он смешивал старые и новые сведения и передавал получившуюся компиляцию другому полицейскому ведомству, которое снабжало его еще какими-то сведениями, добавляемыми им в общий котел. В андеграунде Гилл явно вел такую же игру.

Несколько участников подполья, особенно Mentat и Brett Macmillan, завсегдатаи PI и Zen, почували неладное и начали вести на BBS настоящую войну, чтобы отстоять свое мнение. В начале 1989 года Brett Macmillan опубликовал сообщение о том, что Hackwatch никогда не был зарегистрирован как торговый знак на имя Стюарта Гилла в Торговой палате Виктории. Более того, он утверждал, что служба мониторинга DPG тоже не существует как зарегистрированная торговая организация. Затем Макмиллан ошеломил весь андеграунд, когда объявил, что сам зарегистрировал название Hackwatch, видимо, для того, чтобы помешать Стюарту Гиллу выступать перед СМИ в качестве пресс-атташе Hackwatch.

Многие в андеграунде почувствовали, что Гилл их одурачил, но они были не одиноки. Вскоре некоторые журналисты и полиция почувствовали то же самое. Этого человека даже звали по-другому, а не Стюарт Гилл.

Кое-кто в подполье был склонен полагать, что в действительности Гиллу было нужно создать шумиху вокруг хакеров, чтобы затем потребовать введения антихакерских законов. В середине 1989 года правительство Австралийского Содружества так и поступило, введя в действие первые федеральные законы, направленные против компьютерных преступлений.

Это случилось не по вине журналистов. Когда однажды Хелен Мередит попросила Гилла подтвердить его сведения, он отослал ее к суперинтенданту Тони Уоррену [Tony Warren] из полиции Виктории, и тот подтвердил его слова. Репортер не мог желать лучших доказательств.

А почему бы Уоррену не поддержать Гилла? Зарегистрированный информатор ISU, [\[p102\]](#) Гилл также был консультантом, советником, исповедником и другом многих сотрудников полиции Виктории. Он был в близких отношениях с Уорреном и инспектором Крисом Косгриффом [Chris Cosgriff]. С 1985 по 1987 Уоррен работал в Бюро криминальной разведки, затем был переведен в Департамент внутренних расследований, [\[p103\]](#) куда в 1988 году пришел и Косгрифф.

---

p102

Internal Security Unit – Отдел внутренней безопасности (предназначен для борьбы с коррупцией полиции в штате Виктория).

p103

Internal Investigation Department (IID).

За шесть месяцев 1992 года Гилл звонил Уоррену свыше 200 раз, 45 из них – домой. За восемнадцать месяцев в 1991–1992 годах Крис Косгрифф лично приходил домой к Гиллу 76 раз и записал 316 телефонных разговоров с ним.<sup>26</sup>

Отдел внутренней безопасности (ISU) занимался расследованиями случаев коррупции в полицейских рядах. Имея доступ в ISU, можно было узнать все, что знала сама полиция Виктории о коррупции среди своих полицейских. С этой информацией нужно было обращаться очень осторожно, особенно с тех пор, как полицейских стали привлекать к даче показаний на своих коллег. И вот в 1993 году в отчете омбудсмана штата Виктория были сделаны выводы о том, что Косгрифф передал Гиллу большое количество конфиденциальной информации ISU, а отношения между Уорреном и Гиллом были недопустимыми.<sup>27</sup>

Когда в 1989 году Craig Bowen (он же Thunderbird) осознал, что Гилл подставил его, он погрузился в глубочайшую депрессию. Еще бы, ведь коммуна PI доверяла ему. Его дружба с Гиллом началась, когда Craig Bowen был восторженным и наивным молодым человеком, ищущим приключений. Она закончилась предательством и боязнью всего и вся.

С тоской в глазах Craig Bowen навсегда выключил Zen и PI.

:)

Сидя в первой половине 1989 года перед своим монитором, Force порой не видел абсолютно ничего. Его мысли были за миллион миль отсюда. Ситуация была паршивой, и, погрузившись в свои мысли, он отсутствующе играл мышью, ломая голову над тем, как решить эту проблему.

Проблема заключалась в том, что кое-кто в Мельбурне скоро будет арестован.

Force хотел бы не принимать в расчет это секретное предупреждение, отмахнуться от него, как от очередного слуха из тех, что периодически проносились по андеграунду, но он знал, что не сможет этого сделать. Это предупреждение было надежным, как скала: оно исходило от Gavin'a.<sup>28</sup>

По словам Force, его друг Gavin днем работал по контракту в Telecom, а ночью предавался хакингу. Он был маленькой тайной Force, которую тот хранил от других членов Realm. Gavin ни в коем роде не был участником событий, связанных с хакерскими BBS. Он был старше, у него даже не было хэндла, и он действовал в одиночку, так как считал, что групповой хакинг опасен.

Будучи работником Telecom, Gavin обладал такой степенью допуска в компьютеры и сети, о какой большинство хакеров может только мечтать. У него также были отличные контакты внутри Telecom – из тех, что могли ответить на тактично заданные вопросы о прослушивании телефонов и слежке за линиями или могли быть в курсе полицейских расследований, в которых требовалась помощь Telecom.

Force познакомился с Gavin'ом, когда покупал кое-какое подержанное оборудование через *Trading Post*. Они поладили, подружились и вскоре стали действовать вместе. Под покровом ночи, когда все расходились по домам, они пробирались в офис Gavin'a и занимались хакингом всю ночь напролет. На рассвете они приводили все в порядок и осторожно покидали здание. Gavin ехал домой, принимал душ и возвращался на работу, как ни в чем не бывало.

Gavin познакомил Force с трэшингом.<sup>[p104]</sup> Если они не просиживали всю ночь за его терминалом, Gavin ползал по всем мусорным корзинам Telecom в поисках крупниц информации на обрывках офисной бумаги. Названия учетных записей, пароли, номера телефонов для доступа, NUA – люди записывали массу сведений на клочках бумаги, которые на следующий день выбрасывали за ненадобностью.

Если верить Force, Gavin регулярно менял офисы, что облегчало ему задачу по запутыванию следов. Более того, он старался работать в офисах, откуда десятки людей ежедневно делали сотни

---

<sup>26</sup> См.: *Operation Iceberg; Investigations and Recommendations into Allegations of Leaked Confidential Police Information*, приложение 1 к докладу заместителя омбудсмана *Operation Iceberg; Investigations of Leaked Confidential Police Information and Related Matters*.

<sup>27</sup> Ibid., p. 26–27.

<sup>28</sup> Настоящее имя не раскрывается ради его безопасности.



звонков. Нелегальная деятельность Gavin'a и Force была просто похоронена под лавиной ежедневных законных соединений.

Оба хакера доверяли друг другу. Gavin был единственным человеком, которому Force открыл точный адрес машины CitiSaudi. Даже Phoenix, восходящая звезда Realm и любимый протеже Force, не имел доступа ко всем секретам Citibank, обнаруженным во время сетевых подвигов Force.

Force поделился с Phoenix'ом лишь частью этого сверкающего приза. Только несколькими номерами карт – чисто символически – и общей информацией о сети Citibank. Force считал, что искушение получить доступ к большому количеству номеров кредитных карт и их использования может оказаться сильнее юного Phoenix'a, и постарался сохранить в секрете точное расположение машины Citibank. Это была та малость, которую он мог сделать, чтобы остановить его. Force определенно не собирался помогать Phoenix'у нажать себе неприятности.

Сеть Citibank была богатейшим источником систем. Их Force тоже сохранил для себя. Чем больше он исследовал эти системы, тем больше их обнаруживалось в сети. Вскоре после его первой встречи с системой CitiSaudi он нашел машину под названием SitiGreece, которая, казалось, так же набита информацией, как и саудовско-американская. Но из пятнадцати кредитных карт, найденных Force в системе, действительными оказались только две. Он подумал, что остальные – это тест-карты. Скорее всего, он столкнулся с новым сайтом. Вскоре после того, как Force обнаружил машину SitiGreece, он открыл подобные сайты-эмбрионы еще в двух странах.

Force с симпатией относился к Phoenix'у, он был под впечатлением от его энтузиазма и желания знать все о компьютерных сетях.

Force познакомил Phoenix'a с Minerva, точно так же как Craig Bowen сделал это для Force несколько лет назад. Phoenix быстро учился и требовал все новых знаний. Он был голоден и, по проницательному мнению Force, очень способен. В действительности, Force подмечал черты своего характера в молодом хакере. Они оба вышли из образованного среднего класса, оба несколько отличались от общей массы. Родители Force были в Австралии эмигрантами. Часть семьи Phoenix'a жила в Израиле. Его семья была очень религиозна.

Phoenix учился в одной из главных ортодоксальных еврейских школ в Виктории, которая заявляла о себе, как о «современном ортодоксальном сионистском» учреждении. Почти половина предметов, преподававшихся в девятом классе, были посвящены истории, языку и религии евреев, все мальчики носили ермолки, и школа рассчитывала, что все ученики к моменту выпуска будут бегло говорить на иврите.

В первые школьные годы Phoenix получил прозвище The Egg.<sup>[p105]</sup> По мере обучения он стал непревзойденным мастером особой игры – разбиться в лепешку, но понравиться учителям. Он быстро понял, что успех в религиозном обучении – это отличный способ снискать расположение учителей и родителей. И, по крайней мере, в их глазах он был золотым ребенком.

Но любой, кто захотел бы поскрести верхний слой, обнаружил бы, что сияющий ореол пай-мальчика был простой позолотой. Несмотря на успехи в школе и зачисление в университет, у Phoenix'a были проблемы. Он глубоко страдал от резкого разрыва и развода родителей. Это произошло, когда Phoenix было четырнадцать лет.

После развода Phoenix отправили на полгода в пансион в Израиль. После возвращения в Мельбурн он жил со своей матерью и младшей сестрой в доме бабушки. Его брат, средний ребенок в семье, остался с отцом.

Школьные друзья Phoenix'a иногда чувствовали себя неловко, бывая у него в гостях. Один из лучших друзей Phoenix с большим трудом общался с его матерью. Ее живость порой граничила с истерикой и нервными срывами. Его бабка была хронической паникершей, которая донимала его, если он пользовался телефоном во время грозы, боясь, как бы его не убило током. Ситуация с отцом была немногим лучше. Он работал менеджером в Telecom и вечно дрейфовал от полного безразличия и эмоциональной холодности к яростным вспышкам гнева.

Младший брат Phoenix'a был по-настоящему трудным ребенком. Он сбежал из дома лет в семнадцать и начал торговать наркотиками еще до того, как окончательно встал на ноги. Но, в отличие от Phoenix'a, проблемы его брата были очевидны для всех. Столкновение с жизненными реалиями заставило его критически посмотреть на собственную жизнь и изменить ее.

Phoenix, напротив, нашел менее заметные формы своего мятежа. Среди них было его увлечение

инструментами силы – боевыми искусствами, оружием вроде мечей и шестов и социальным программированием. Когда Phoenix учился в выпускном классе школы и все еще жил в доме бабушки, он занялся хакингом. Он начал посещать разные мельбурнские BBS, пока не свел онлайнową дружбу с Force.

Force с интересом наблюдал за становлением хакерских навыков Phoenix'a и через пару месяцев пригласил его войти в Realm. Это была самая короткая инициация за всю историю Realm, причем голосование по приему нового члена было единодушным. Phoenix доказал, что достоин такой чести, собирая информацию о новых системах и сетях для базы данных Realm. На пике своей хакерской активности Force и Phoenix общались по телефону почти каждый день.

Всеобщее одобрение Phoenix'a в Realm резко отличалось от положения Electron'a, который регулярно посещал эту BBS в течение нескольких месяцев 1988 года. В то время как Phoenix грелся в лучах поддержки Force, восемнадцатилетний Electron в полной мере ощущал холод растущего презрения последнего.

В конце концов Force вышвырнул Electron'a и его друга Powerspike из своего элитного клуба мельбурнских хакеров. И вот как Force объяснил это. Он сказал, что Electron совершил два серьезных проступка. Первый заключался в том, что Electron якобы распылял ресурсы, используя учетные записи в системе OTC Minerva, чтобы подключиться к Altos. Это означало немедленное обнаружение и уничтожение учетной записи.

Администраторы Minerva, такие как заклятый враг Realm Майкл Розенберг, распознавали NUA Altos. Розенберг был лучшей защитой OTC против хакеров. Он потратил так много времени на то, чтобы очистить от них Minerva, что знал их привычки: взлом, затем рывок на Altos, чтобы пообщаться с друзьями-хакерами, затем следующий взлом.

Большинство учетных записей Minerva принадлежало корпорациям. Сколько законных пользователей ANZ Bank посещали Altos? Ни одного. Поэтому как только Розенберг видел учетную запись, подключенную к Altos, он осторожно наблюдал за тем, что делает хакер – особенно за его хвастовством своими подвигами, затем менял пароль и ставил клиента на заметку, чтобы навсегда изгнать хакера из системы.

Второй грех Electron'a, согласно Force, состоял в том, что он утаивал хакерскую информацию от других членов группы. Жесткое правило Force (которому он сам не всегда следовал) гласило: если ты с нами, делись с нами всем.

Это было громкое исключение. Powerspike и Electron сказали друг другу, что им наплевать. По их мнению, они посещали BBS Realm лишь время от времени, но уж никак не были его членами. Electron шутил: «Кто захочет быть членом такой отстойной команды, как Realm?» Но все же им было обидно. В период с 1988 по 1990 годы хакеры зависели друг от друга в плане информации. Они оттачивали свои навыки в коммуне, обмениваясь сведениями друг с другом, и росли, черпая из общего котла информации.

Несколько месяцев спустя Force с неохотой позволил Electron'у вернуться в Realm, но отношения оставались натянутыми. Когда Electron, наконец, зарегистрировался в BBS, он обнаружил там файл под названием «Сканер, украденный у Electron'a». Force нашел копию сканирующей VMS программы Electron'a в заокеанском компьютере, пока Electron был в изгнании, и без всяких угрызений совести украл его для Realm.

Однако это был не сканер. Это был «троян» для VMS. Разница между ними огромна. Он не сканирует сеть в поисках адресов компьютеров. Он крадет пароли, когда люди подключаются со своих VMS-машин к другой машине в сети X.25. Powerspike чуть не лопнул от смеха, когда Electron сказал ему об этом. «Что ж, – сказал он, – мистер Большая Шишка Force, может быть, и знает что-то о компьютерах Prime, но он ни хрена не знает о VMS».

Несмотря на отлучение Electron'a, Phoenix продолжал общаться с отверженным: их сближала одержимость. Electron с огромным интересом изучал новые приемы и, как и сам Phoenix, учился очень быстро – быстрее любого другого мельбурнского хакера.

Когда Phoenix стал постоянно общаться с Electron'ом, Force попытался помешать этому, но безуспешно. В какой-то степени, его неодобрение было продиктовано своеобразным отеческим отношением к австралийскому хакерскому кругу. Force считал себя кем-то вроде крестного отца сообщества хакеров. Но он все сильнее убеждался, что Phoenix ведет себя все более дерзко по отношению к важным персонам компьютерной безопасности и системным администраторам. Однажды Phoenix узнал, что несколько админов и людей из секьюрити поджидали его в системе, чтобы поймать, проследив сетевое соединение. В ответ он анонимно вполз в компьютер и спокойно вырубил каждого администратора. В тот раз Force очень посмеялся, но, если откровенно, эта история заставила его

крепко понервничать.

Phoenix с радостью скрещивал шпаги с индустрией компьютерной безопасности. Он стремился доказать, что он лучше, и часто расстраивал людей тем, что действительно был таковым. Однако странно, что протеже Форсе думал, что если он укажет этим специалистам на слабые места в их системе безопасности, то заслужит их уважение. Может быть, они даже дадут ему какую-нибудь внутреннюю информацию, типа новых техник проникновения, и замолвят за него словечко, если что-то пойдет не так. Форсе удивлялся, как Phoenix мог сочетать два таких противоположных мнения в своей голове, даже не задумываясь об их противоречии.

;) )

Именно против этой стороны андеграунда и было направлено предупреждение Gavin'a, с которым он пришел к Форсе в конце 1989 года. Gavin узнал, что Австралийская федеральная полиция получила жалобы на хакеров, действующих за пределами Мельбурна. Сообщество мельбурнских хакеров стало очень беспокойным и оставляло свои следы повсюду, где его члены сталкивались с мировыми системами данных.

Кроме Австралии, существовали и другие активные сообщества хакеров – в Англии, Техасе, Нью-Йорке. Но мельбурнские хакеры были не просто беспокойными – они беспокоили *американские* компьютеры. Это был не просто случай вторжения американских хакеров в американские системы. Речь шла о проникновении в американские машины лиц другой национальности. Австралийские хакеры оказались под прицелом еще по одной причине. Секретной службе США стало известно, что австралийский хакер по имени Phoenix был в системе Citibank, одного из крупнейших финансовых институтов Америки.

Gavin не располагал более детальной информацией. Он знал только, что американская служба правопорядка – возможно, Секретная служба – оказала сильнейшее давление на правительство Австралии, требуя арестовать этих людей.

Но Gavin не мог знать, что источником давления из-за океана была не только Секретная служба. ФБР также пыталось повлиять на Австралийскую федеральную полицию по поводу тайнственных, но беспокойных австралийских хакеров, которые продолжали вторгаться в американские компьютеры.<sup>29</sup> И АФП начала действовать.

В конце 1989 года детектив суперинтендант Кен Хант [Ken Hunt] из АФП возглавил расследование по делу мельбурнских хакеров. Это стало первым серьезным расследованием компьютерных преступлений с момента введения федеральных антихакерских законов в Австралии. Как и большинство силовых структур всего мира, АФП была новичком на ниве компьютерного криминала. Мало кто из детективов имел опыт общения с компьютерами, не говоря об их незаконном использовании, так что это дело должно было стать важнейшим первым опытом применения нового закона.<sup>30</sup>

Когда Gavin огорошил Форсе такими новостями, тот сразу же начал действовать. Он позвонил Phoenix'у, настаивая на немедленной личной встрече. Поскольку их дружба крепла, они перешли от общения онлайн к телефонным разговорам, а затем стали проводить много времени вместе, встречаясь уже лично. Форсе с глазу на глаз передал Phoenix'у суровое предупреждение. Он не сказал своему протеже, как получил эту информацию, но ясно дал понять, что источник заслуживает доверия.

Полиция сознавала, что должна кого-нибудь арестовать. Дошло до того, что американский сотрудник правоохранительных органов сказал своему коллеге из Австралии: «Если вы ничего не предпримете в самое ближайшее время, мы сами сделаем то, что считаем нужным». Американец не побеспокоился, чтобы сообщить, как именно они собираются действовать, но это было неважно.

Phoenix побледнел. Да, конечно, он навел шороху в системах, фактически постоянно взламывая все новые сайты. Многие из них находились в Штатах.

Разумеется, он не стремился кончить так, как западногерманский хакер Hagbard, чьи обгоревшие останки нашли в немецком лесу в июне 1989 года.

Коллега Pengo, Hagbard входил в кружок немецких хакеров, которые с 1986 по 1988 годы продавали информацию, украденную из американских компьютеров, агенту КГБ в Западной Германии.

В марте 1989 года немецкая полиция провела обыски в домах и офисах хакерской группы. По-

<sup>29</sup> Michael Alexander, «International Hacker „Dave“ Arrested», *Computer World*, 9 april 1990, p. 8.

<sup>30</sup> Matthew May, «Hacker Tip-Off», *The Times*, 5 april 1990; lou dolinar, «Australia Arrests Three in Computer Break-Ins», *Newsday*, 3 april 1990.

следовали аресты. Так же как и Pengo, Hagbard тайно сдался немецким властям за несколько месяцев до этих событий и дал показания о деятельности хакерской группы в надежде заработать иммунитет против судебного преследования.

Американские силовые агентства и прокуроры ни в коей мере не собирались проявлять снисходительность к хакерам. Несколько служб, включая ЦРУ и ФБР, охотились за немецкой шпионской организацией, требуя суровых приговоров, предпочтительно с отбыванием срока наказания в американских тюрьмах.

Когда было найдено тело Hagbard'a, немецкие судебные процедуры находились в процессе подготовки. Оставалось неясным, было ли это самоубийство или убийство. Никто не знал точного ответа, но эта новость потрясла компьютерный андеграунд всего мира. Хакеры обсуждали смерть Hagbard'a с полной серьезностью. С одной стороны, его биография была отмечена психической нестабильностью и употреблением наркотиков. С начала 1987 года он провел много времени в психиатрических клиниках и центрах реабилитации, периодически покидая их и возвращаясь вновь. С другой стороны, если человек хочет покончить с собой, неужели он выберет медленную смерть в бензиновом огне? Скорее, он предпочтет передозировку или пулю.

Что бы это ни было, убийство или самоубийство, воспоминание о смерти Hagbard'a с ужасающей ясностью проявилось в голове Phoenix'a. За кем явились в Австралию американские силовые агентства? Им нужен он?

Нет. Force успокоил его. Пришли за Electron'ом. Проблема Phoenix'a заключалась в том, что он продолжал общаться с Electron'ом по телефону – обычным способом. Если Phoenix и дальше будет якшаться с Electron'ом, он тоже попадет в лапы АФП.

Phoenix понял это абсолютно четко.

;)

– Ах, свинья!

– А? – отозвался Phoenix, почти не обращая внимания.

– Дерьмовая машина. Я все отредактировал, а эта хреновина ни хрена не сохранила. – Electron сидел дома за компьютером, проклиная свой Commodore Amiga с его 512К памяти.

Дело было в январе 1990 года, и они оба, Phoenix и Electron, приехали домой на праздники перед началом очередного семестра.

– Но я заставлю эту сволочь работать. Чертова дура! Работай! – заорал Phoenix. Electron слышал, как он стучит по клавиатуре на другом конце провода. Phoenix бился над тем, чтобы получить доступ в AUX, Apple-версию системы Unix, целыми днями проводя у своего Macintosh SE30.

Поддерживать с Phoenix'ом связную беседу было очень сложно. Если не висла его машина, то через дверь его донимала бабка.

– Не хочешь пройти по списку? У тебя большой файл? – спросил Phoenix, снова вернувшись к разговору.

– Что? Какой файл?

– Текстовый. Слова, чтобы ввести во взломщик паролей, – ответил Phoenix.

Electron вывел свой список слов и посмотрел на него. Он подумал, что его надо бы подсократить. Словарь был частью программы, взламывающей пароли. Чем больше словарь, тем дольше времени понадобится компьютеру на составление списка взломанных паролей. Если Electron выбросит из него непонятные слова и слова, которые вряд ли кто-то станет использовать в качестве пароля, он сможет ускорить действие программы-взломщика.

Эффективный взломщик паролей был ценным инструментом. Electron вводил в свой домашний компьютер файл с паролями с намеченного компьютера, к примеру из Мельбурнского университета, и отправлялся в постель. Через двенадцать часов он проверял успехи своей программы.

Если ему везло, он мог найти шесть и даже больше учетных записей – имен пользователей и паролей – в своем файле. Процесс был полностью автоматизирован. Затем Electron мог зарегистрироваться в Мельбурнском университете, используя взломанные учетные записи, каждая из которых могла послужить отправным пунктом для вторжения в другие системы, и все это по цене одного местного телефонного звонка.

Взламывать пароли в Unix было не особенно трудно, при условии, что разные компоненты программы, такие как словарь, установлены должным образом. Но это требовало времени. Принцип был прост. Пароли, хранимые в файлах паролей с соответствующими именами пользователей, были зашифрованы. Отменить процесс зашифровки было так же невозможно, как вернуть омлет к состоя-

нию яйца. Вместо этого требовалось воссоздать процесс зашифровки и сравнить результаты.

Нужно было выполнить три основных шага. Во-первых, наметить компьютер и получить копию файла с паролями. Во-вторых, взять список наиболее часто используемых имен пользователей из файла паролей или из словаря и зашифровать их, образовав другой список. В-третьих, сравнить оба списка. Если вы увидите совпадение, пароль найден.

Но существовало одно серьезное затруднение – дополнительный элемент salt. Salt изменяет способ зашифровки пароля, слегка модифицируя режим работы алгоритма зашифровки DES. Например, слово «Underground», зашифрованное двумя различными способами с двумя различными salt, может выглядеть «kyvbEx-McdAOVM» или «lhFaTmw4Ddrjw». Два первых символа представляют salt, остальные – пароль. Компьютер произвольно выбирает salt, когда зашифровывает пароль. Из существующих 4096 разных salt используется только один. Все компьютеры Unix используют salt в процессе зашифровки паролей.

Salt использовался для того, чтобы затруднить взлом паролей: после их применения хакер не мог просто зашифровать пароль, а потом сравнить его с каждым списком зашифрованных паролей, полученных за время хакерских вторжений. 4096 salt означали, что хакеру придется использовать 4096 различных словарей – каждый для своего salt, – чтобы обнаружить в словаре один из паролей.

Но даже зашифровка большого словаря 25 раз с использованием 25 различных salt занимает слишком много места на жестком диске примитивного домашнего компьютера. И это только словарь. Самые продвинутые крэкинг-программы также делают «обоснованные предположения» для паролей. Например, программа может взять имя пользователя и попробовать с ним комбинации заглавных и прописных букв. Добавить в конце «1». Короче, программа делает новые попытки, представляя, тасуя, изменяя и вновь комбинируя базовую информацию – имя пользователя – в новое «слово».

– У меня 24 000 слов. Чертовски много, – сказал Electron.

Сокращение словаря было балансированием в поисках компромисса. Чем меньше слов было в крэкинг-словаре, тем меньше времени требовалось, чтобы взломать зашифрованные пароли. Но чем меньше был словарь, тем меньше получалось вариантов и, следовательно, шансов взломать пароль любой отдельно взятой учетной записи.

– Хм. У меня 24 238. Давай лучше вместе их сократим.

– Ладно. Назови букву.

– С. Начнем с С.

– Почему С?

– Потому что кошку моей бабки зовут Сосоа.

– О'кей, погнали. Cab. Cabal. Cabbala. – Electron замолчал. – Что это еще за Cabbala?

– Фиг знает. Ладно, эти у меня есть. Кроме Cabbala. О'кей. Cabaret. Cabbage.<sup>[p106]</sup> Черт, ненавижу капусту. Кто мог взять такой пароль?

– Какой-нибудь англичашка, – ответил Electron.

– Да уж, – засмеялся Phoenix, прежде чем продолжить. Иногда Phoenix возвращался к мыслям о предупреждении Force. Но большую часть времени они едва теплились в дальнем уголке его мозга, хотя и не преследовали его. Force воспринял это предупреждение достаточно серьезно. Он не только прекратил всякое общение с Electron'ом, казалось даже, что он совсем ушел из хакинга.

На самом деле у Force появилось новое увлечение – музыка. Он писал и исполнял собственные песни. В начале 1990 года он так серьезно занялся музыкой, что практически заморозил Realm. Его членам пришлось собираться в машине другого участника Realm, Nom, примерно около месяца.

Но Phoenix знал, что это не конец истории. Хакер не может просто так уйти из хакинга. Во всяком случае, не Force. Он был одержим хакингом. Это просто не имело смысла. Здесь, вероятно, было что-то еще. Phoenix успокаивал себя тем, что последовал совету Force и стал держаться подальше от Electron'а. Ну, во всяком случае, какое-то время.

Он действительно отдалился от Electron'а, понаблюдав и выждав время, но ничего не произошло. Electron был, как обычно, активен, но никто его не преследовал. Ничего не изменилось. Возможно, информация Force была ошибочной. Если бы федералы собирались что-нибудь предпринять, Electron был бы уже задержан. Поэтому Phoenix восстановил свои отношения с Electron'ом. Искушение было слишком велико. Phoenix не собирался позволить самолюбию Force мешать его

личному прогрессу.

К январю 1990 года Electron отдавал хакингу почти все свое свободное время. Перерывы делались только на сон, но даже во сне он продолжал взламывать компьютеры. Они с Phoenix'ом оторвались очень далеко от остальных мельбурнских хакеров. Electron перерос знания и опыт Powerspike, так же как Phoenix превзошел Force. Они отошли от сетей X.25 и занялись зарождающимся Интернетом, что было в той же степени незаконно, потому что университеты охраняли компьютерные учетные записи – доступ в Интернет – очень бдительно.

Даже Nom с его растущим опытом работы в Unix, лежащей в основе многих новых сайтов Интернета, не соответствовал стандартам Electron'a. У него не было того уровня преданности хакингу, той одержимости, которая необходима для истинного хакера, вечно балансирующего на самой кромке. Во многом отношения между Nom'ом и Phoenix'ом были похожи на отношения между Powerspike и Electron'ом – первые выступали на подпевке солисту.

Electron не считал Phoenix'a близким другом, но он был собратом по духу. На деле он не доверял Phoenix'у, который любил прихвастнуть, обладал гипертрофированным эго и дружил с Force – все говорило не в его пользу. Но Phoenix был умен и хотел учиться. Что еще важнее, он был одержим. Phoenix способствовал притоку информации, который интеллектуально стимулировал Electron'a, пусть даже Phoenix получал больше сведений, чем отдавал.

В течение месяца Phoenix и Electron находились в постоянном контакте, и во время летних каникул они говорили по телефону – обычным путем – по несколько раз в день. Взломать и поговорить. Сравнить записи. Снова взломать. Проверить результаты, задать пару вопросов. Опять вернуться к хакингу.

Тогдашний хакинг был в основном делом одиночек. Для таких членов общества, как Phoenix, это тоже было одиночное плавание. Но если многие хакеры упивались полной изоляцией, то некоторые из них, в том числе и Phoenix, испытывали необходимость время от времени отметить в рядах человечества. Но его устраивало не всякое общество – ему требовалось внимание тех, кто понимал и разделял его устремления.

;)

– Caboodle. Caboose, – продолжал Electron, – Cabriolet. Что это за чертов Cabriolet? Ты знаешь?

– Да, – ответил Phoenix и двинулся дальше. – Ладно. Cacao. Cache. Cachet...

– Скажи нам, что это? – перебил его Electron.

– Cachinnation. Cachou...

– Ты знаешь? – снова спросил Electron, слегка раздражаясь.

Как обычно, Phoenix говорил, что знает то, о чем не имел никакого понятия.

– Что? Ага, – вяло ответил Phoenix. – Cackle. Cacophony...

Electron знал, что означало это особенное «ага» Phoenix'a. Он вроде бы говорил «да», но на самом деле, он хотел сказать: «Нет, и я не собираюсь на этом заикливаться, поэтому давай плюнем на это дело».

Electron давно уже взял в привычку не верить многому из того, что говорил ему Phoenix. Если слова товарища не подкреплялись серьезными доказательствами, Electron считал их пустой болтовней. В сущности, Phoenix не слишком нравился ему как личность, и говорить с ним временами бывало сложно. Electron предпочитал компанию своего старинного приятеля-хакера Powerspike.

Powerspike был блестящ и креативен. Electron ладил с ним. Они часто подшучивали над плохими музыкальными вкусами других. Powerspike нравился хэви-металл, а Electron'у – инди-музыка. Они оба испытывали здоровое неуважение к авторитетам. Не только к власти тех мест, куда они вторгались, вроде Военно-морской исследовательской лаборатории или NASA, но и к авторитетам Realm. В политике они оба придерживались левых взглядов, хотя как символ протеста против военно-индустриального комплекса им больше импонировала анархия, нежели членство в какой-либо партии.

После их изгнания из Realm, Electron на некоторое время оказался в изоляции. В немалой степени ей способствовала его личная трагедия. Когда Electron'у было восемь лет, его мать скончалась от рака легких. Он не стал свидетелем самого страшного в этом долгом процессе, так как мать провела два года в немецкой онкологической клинике в надежде на временное облегчение, но умирать она приехала домой, и Electron видел, как она угасала.

Когда посреди ночи в их доме раздался телефонный звонок, Electron понял, что случилось, по серьезному тону взрослых. Он разрыдался. Он слышал, как его отец отвечает на вопросы по телефо-

ну. Да, мальчику очень тяжело. Нет, его сестренка вроде в порядке. Сестра была на два года младше Electron'a и слишком мала, чтобы что-то понять.

Electron никогда не был особенно близок с сестрой. Он считал ее бесчувственным пустым существом, бездумно скользящим по поверхности жизни. Но после смерти матери отец стал по-особенному относиться к дочери, возможно, потому, что она была похожа на его покойную жену. Это привело к еще более глубокому разрыву между братом и сестрой.

Отец Electron'a был художником и всю жизнь преподавал в местной средней школе. Смерть жены глубоко потрясла его. Несмотря на некоторые материальные и социальные барьеры, их любовь была взаимной, а брак – счастливым. Картины отца Electron'a висели почти на каждой стене в их доме, но после смерти жены он забросил кисти и больше никогда не возвращался к ним. Он не говорил об этом. Однажды, когда Electron спросил отца, почему он больше не пишет, тот посмотрел в сторону и сказал, что «потерял мотивацию».

Бабушка Electron'a переехала к ним, чтобы помочь своему сыну заботиться о детях, но у нее прогрессировала болезнь Альцгеймера. Детям самим пришлось заботиться о ней. Подростком Electron часто думал о том, что можно сойти с ума, ухаживая за человеком, который даже не помнит, как тебя зовут. В конце концов бабушка переехала в дом престарелых.

В августе 1989 года отец Electron'a вернулся домой после посещения врача. В последнее время ему нездоровилось, но он отказывался брать отгул, чтобы съездить к доктору. Он гордился тем, что за последние пять лет пропустил по болезни всего один день. Но во время отпуска он все-таки посетил врача, который взял множество анализов. И вот результаты были готовы.

У отца Electron'a обнаружился рак легких, болезнь стремительно развивалась. Он был неизлечим. Ему оставалось жить максимум два года.

В то время Electron'у было девятнадцать лет, его детская любовь к компьютерам и к модемам переросла в подлинную страсть. Несколько лет назад его отец, стремясь поддержать увлечение сына новыми машинами, частенько приносил домой один из школьных Apple IIe на уик-энды и во время каникул. Electron часами просиживал за одолженной машиной. Если он не играл на компьютере, то либо читал выуженный из отцовских книжных шкафов шпионский роман, либо в очередной раз перечитывал свою любимую книгу «Властелин колец».

Но компьютерное программирование захватило воображение Electron'a задолго до того, как он впервые столкнулся с компьютером. В двенадцать лет он с помощью учебников писал простые компьютерные программы на бумаге (главным образом, игры), хотя в то время еще ни разу не касался клавиатуры.

В его школе было несколько компьютеров, но никто толком не знал, как с ними обращаться. В девятом классе Electron встретился со школьным консультантом по профориентации, надеясь узнать о возможности карьеры, связанной с компьютерами.

– Я хотел бы изучать компьютерное программирование... – его голос в нерешительности дрогнул.

– Почему тебе хочется заниматься именно этим? – спросила она. – Может быть, стоит подумать о чем-то получше?

– Ну... – Electron не знал, что ему делать. Поэтому-то он и пришел к ней.

Его мысли заметались, пытаясь найти что-то более распространенное, привычное, что позволило бы ему работать на компьютере.

– Ну, может быть, бухгалтерское дело?

– О да, это гораздо лучше, – сказала она. – Я думаю, ты сможешь поступить в университет и изучать там бухгалтерию. Уверена, что тебе это понравится, – добавила она, закрывая его папку.

По мнению Electron'a, одалживаемые компьютеры были одной из немногих приятных вещей, связанных со школой. Он прилично успевал в классе, но лишь потому, что это не требовало особых усилий. Учителя Electron'a постоянно говорили его отцу, что он отвлекает других учеников. По большей части критика была несправедливой. Хотя иногда у Electron'a случались серьезные столкновения с учителями. Некоторые считали его одаренным. Другим казалось, что веснушчатый, похожий на ирландца мальчишка, который подбил своих друзей поджечь учебники на задних партах, был просто ловким пройдохой.

В шестнадцать лет Electron купил свой первый компьютер. Первоначально он использовал его для взлома защиты программного обеспечения, как Pac. Apple вскоре сменил более мощный Amiga с IBM-совместимой приставкой на 20 мегабайт. Компьютеры один за другим менялись на одном из двух письменных столов в его комнате. На втором, предназначенном для школьной работы, обычно высились груда невыполненных домашних заданий.

Самым удивительным в комнате Electron'а было огромное количество распечаток с матричного принтера, в беспорядке разбросанных по полу. Практически в любом месте скромно обставленной комнаты можно было нагнуться и подобрать стопку распечаток с именами пользователей и паролями или с кодом компьютерной программы. Оставшееся пространство занимали футболки, джинсы, кеды и книги. По этой комнате невозможно было пройти, не наступив на что-нибудь.

Поворотным моментом для Electron'а стала покупка в 1986 году подержанного модема на 300 бод. За одну ночь модем превратил интерес Electron'а к компьютерам в настоящую одержимость. В конце семестра, последовавшего сразу за приобретением модема, в таблице Electron'а было шесть пятерок и одна четверка. В следующем семестре он заработал шесть четверок и всего одну пятерку.

Electron'а занимали более серьезные вещи, чем школа. Вскоре он стал постоянным посетителем подпольных BBS и начал заниматься хакингом. Он был под впечатлением от одной статьи, которая рассказывала о нескольких хакерах, сбивших с курса космический спутник взломом компьютера. В этот момент Electron решил, что хочет стать хакером, – проверить, правду ли пишут в статье.

Еще до того, как Electron закончил школу в 1987 году, он взломал систему NASA. После этого подвига он плясал вокруг стола в гостиной посреди ночи и пел: «Я был в NASA! Я был в NASA!» Он не изменил орбиты спутника, но проникновение в космическое агентство было таким же увлекательным делом, как полет на Луну.

К 1989 году он уже несколько лет постоянно занимался хакингом к большому огорчению своей сестры, которая жаловалась, что ее общественная жизнь страдает из-за того, что единственная телефонная линия в доме постоянно оккупирована модемом.

Electron для Phoenix'а был партнером по хакингу и в некотором роде наставником. В то время Electron мог предложить многое, гораздо больше, чем Realm.

:)

– Cactus, Cad, Cadaver, Caddis, Cadence, Cadet, Caesura. Что это за чертов Caesura? – Phoenix продолжал перепаживать букву С.

– Фиг его знает. К черту, – рассеянно ответил Electron.

– Caesura. Ладно, фиг с ним. Я знаю, что я бы не использовал это как пароль, – засмеялся Phoenix. – А что за дурацкое слово Caduceus?

– Дохлое. К черту все это. Кто составляет эти словари? – спросил Electron.

– Да уж.

– Caisson, Calabash. К черту это. К черту, к черту, к черту, – радостно сказал Electron.

– Погоди-ка. Почему у меня в списке нет Calabash? – Phoenix изобразил негодование.

Electron засмеялся.

– Эй, – сказал Phoenix, – нам надо бы вставить сюда слова типа «Qwerty», «ABCDEF» и «ASDFGH».

– Уже сделано.

Electron давно включил в список такие распространенные пароли, как «слова», составленные при наборе пользователем шести первых букв в одном из рядов на клавиатуре.

Phoenix снова вернулся к списку:

– Давай на «CO». Commend, Comment, Commerce, Commercial, Commercialism, Commercially. К черту три последних.

– Ну? Зачем убирать Commercial?

– Давай уберем все слова, в которых больше восьми букв, – сказал Phoenix.

– Нет. Это не очень хорошая мысль.

– Почему? Компьютер читает только восемь букв и зашифровывает их же. Так что мы можем убрать все остальное.

Иногда Phoenix просто не понимал. Но Electron не настаивал. Он держал свои мысли при себе, чтобы не задеть самолюбие Phoenix'а. Иногда Electron чувствовал, что Phoenix ждет от него одобрения, но это было легкое, почти бессознательное стремление.

– Нет, – начал Electron, – вот смотри, кто-то может использовать целое слово – Commerce или Commercial. Первые восемь букв этих слов неодинаковы. Восьмая буква в слове Commerce – «е», а в слове Commercial – «i».

Он продолжал:

– Но можно спокойно убрать все слова вроде Commercially или Commercialism. Понял?

– Да, о'кей. Ясно, – сказал Phoenix.



– Главное, не убирать все слова длиннее восьми букв, – добавил Electron.

– Хм. О'кей. Да, конечно, – Phoenix явно был недоволен. – Эй, – вдруг воскликнул он, – уже минут десять, как мой комп завис.

– Да? – Electron попытался выказать интерес.

– Да. Знаешь, – Phoenix сменил тему и сел на своего любимого конька, – что нам действительно нужно, так это Deszip. Надо достать его.

Deszip был компьютерной программой, используемой для взлома паролей.

– И Zardoz. Нам нужен Zardoz, – добавил Electron.

Zardoz был компьютерной публикацией для служебного пользования с подробностями о недостатках в системах компьютерной безопасности.

– Да. Можно попытаться раздобыть его в машине Спафа. У Спафа он точно есть.

Юджин Спаффорд [Eugene Spafford], адъюнкт-профессор кафедры компьютерного программирования в университете Пардью в США, был одним из самых известных экспертов по безопасности компьютеров в Интернете в 1990 году.

– Да.

Так началась их охота за священным Граалем.

;)

Deszip и Zardoz красовались бок о бок, как самые вожаемые трофеи в мире международных хакеров Unix.

Взлом паролей требовал много времени и компьютерных ресурсов. Даже относительно мощная университетская машина заскрипела бы под грузом вычислений, если бы перед ней поставили такую задачу. Но программа Deszip могла облегчить эти вычисления, и нагрузка, для сравнения, была бы сведена к весу пера. Она работала с невероятной скоростью, так что хакер, обладай он Deszip, мог бы взламывать пароли в 25 раз быстрее.

Zardoz, всемирный список рассылки по вопросам безопасности, был так же бесценен, но по другой причине. Хотя формально этот список назывался *Security Digest*, все в андеграунде называли его попросту Zardoz по имени компьютера, с которого он рассылался. Такое же название носил культовый научно-фантастический фильм с Шоном Коннери в главной роли. Созданный Нилом Горсачом [Neil Gorsuch], список рассылки Zardoz содержал статьи и предупреждения от экспертов индустрии компьютерной безопасности. В них шла речь о новых ошибках в компьютерных системах, которые могли быть использованы для проникновения или получения основного доступа к машине. Прелесть ошибок, опубликованных в Zardoz, состояла в том, что они работали в любой компьютерной системе, использующей программы или операционные системы, описанные в дайджесте. Любой университет, любая военная система, любой исследовательский институт, который пользовался программным обеспечением, описанным в Zardoz, был уязвим. Zardoz представлял собой огромный набор ключей, подходящих практически к любому замку.

Конечно, системные администраторы, прочитавшие отдельную публикацию в Zardoz, могли предпринять определенные шаги и закрыть эти щели в системах безопасности. Но в хакерском сообществе было хорошо известно, как много времени проходит между публикацией Zardoz и исправлением недостатка в системе. Зачастую ошибки на многих компьютерах оставались месяцами, а то и годами уже после того, как о них было объявлено на Zardoz.

Почему это происходило? Многие администраторы и слыхом не слыхивали об ошибке до того, как Zardoz впервые объявлял о ней. Zardoz был эксклюзивным клубом, и далеко не каждый был его членом. Вы не могли просто проходить по улице и записаться в Zardoz. Нужно было пройти через одобрение равных в индустрии компьютерной безопасности. Нужно было управлять компьютерной системой в большом учреждении, например в университете или исследовательской структуре, такой как CSIRO. Иначе говоря, действительные члены списка адресатов Zardoz обнюхивали кандидата своими чувствительными носами и определяли, достоин ли он членства в их клубе. Только они решали, можно ли кандидату доверять настолько, чтобы разделить с ним величайшие секреты безопасности в мире компьютерных систем.

В 1989 году «белые колпаки», как хакеры называли гуру безопасности, сходили с ума от одной мысли о том, что Zardoz может попасть в чужие руки. настолько, что многие публикации на Zardoz были великолепными образцами искусства говорить обиняками. Эксперт по компьютерной безопасности мог лишь обозначить новую ошибку в своей публикации, не делая практических выводов, или же, наоборот, объяснить ее на таком ясном и точном языке, который обычно используют в инструк-

циях.

Это вызывало жаростные дебаты в индустрии компьютерной безопасности. С одной стороны, те, кто ратовал за «инструкции», говорили, что бюллетени вроде Zardoz могут принести только пользу, если люди будут откровенны друг с другом. Они хотели предоставлять тем, кто зарегистрировался в Zardoz, детальные, пошаговые объяснения того, как заделать ту или иную прореху в системе безопасности. Эти люди были за полную открытость.

С другой стороны, приверженцы жесткого курса и тотального контроля в компьютерной безопасности доказывали, что помещение предупреждения в Zardoz чревато серьезнейшим риском. Что, если Zardoz попадет не в те руки? Почему бы любому шестнадцатилетнему хакеру не выполнить шаг за шагом все инструкции, подробно рассказывающие, как вломиться в тысячи персональных компьютеров! Если и существует необходимость предавать гласности прорехи в системах безопасности (а они вовсе не думали, что такая необходимость есть), то это должно быть сделано как можно более туманным языком.

Но жесткие парни забывали о том, что хакеры мирового уровня, такие как Electron, могли прочесть самые завуалированные и тщательно составленные публикации Zardoz и за несколько дней, если не часов, понять, как работать с дырой в системе безопасности, о которой шла речь. Сделав это, они могли с той же легкостью написать справочную версию ошибки.

Большинство толковых хакеров находили один-два выпуска Zardoz в своих путешествиях, роясь в почте администраторов компьютерных систем солидных учреждений. Но ни один из элиты хакеров андеграунда в Altos не имел полного архива всех выпусков бюллетеня. Хакер, раздобывший их, смог бы заполучить подробное описание всех важных дыр в системах безопасности, обнаруженных лучшими в мире экспертами в этой области, по крайней мере, с 1986 года.

Как и Zardoz, Deszip тщательно охранялся. Он был написан экспертом по компьютерной безопасности доктором Мэтью Бишопом [Matthew Bishop], который работал в NASA Research Institute for Advanced Computer Science, [\[p107\]](#) прежде чем стал преподавателем в Дартмуте, в колледже «Лиги плюща» [\[p108\]](#) в штате Нью-Гемпшир. Правительство США сочло очень быстрые шифровальные алгоритмы Deszip настолько важными, что они были засекречены, как оружие. Импортировать их из США было незаконно.

Конечно, в 1990 году немногие хакеры были искушенными настолько, чтобы должным образом использовать Deszip и Zardoz. Более того, мало кто знал, что они вообще существуют. Но Electron и Phoenix знали об этом, так же как и несколько других хакеров, включая британцев Pad'a и Gandalf'a. Кооперируясь с помощью Altos с отборной группой других мастеров, они работали, осторожно намечая сайты, возможно, содержащие части их священного Грааля. Они действовали методично, с тончайшей стратегией, собирая информацию с совершенным, почти хирургическим искусством. Пока толпа простых смертных хакеров разбивала себе лбы, тупо атакуя случайные машины, эти господа посвящали свое время охоте на стратегически важные машины – ахиллесову пяту сообщества компьютерной индустрии.

Они составили информационный хит-парад машин, большинство из которых принадлежало гурзу компьютерной безопасности высочайшего уровня. Обнаружив два ранних выпуска Zardoz, Electron прочесал их публикации самым частым гребнем не только в поисках ошибок в системах безопасности. Он обращал самое пристальное внимание на имена и адреса тех, кто писал статьи. Авторы, часто публикующиеся в Zardoz, те, у кого было, что сказать, автоматически занимали места в хит-параде. Это были те люди, которые, по всей вероятности, хранили копии Deszip или архивы Zardoz в своих машинах.

Electron рыскал по всему миру в поисках информации о Deszip и DES [\[p109\]](#) – шифровальной программе, послужившей основой для Deszip. Он искал в компьютерах Университета Нью-Йорка, Военно-морской исследовательской лаборатории США в Вашингтоне (округ Колумбия), в Техноло-

---

p107

Исследовательский институт передовых компьютерных технологий NASA.

p108

Ivy league (Лига плюща) – восемь самых престижных университетов США.

p109

Data Encryption Standard (DES) – алгоритм шифрования данных, принятый в качестве стандарта в США в середине 70-х годов.

гическом университете Хельсинки, в университете Рутгерс в Нью-Джерси, в Мельбурнском университете и в университете Тампере в Финляндии, но поиски принесли лишь незначительные плоды. Он нашел копию общедоступной шифровальной программы CDES, использовавшей алгоритм DES, но не сам Deszip. CDES годилась для зашифровки файлов, но не для взлома паролей.

Все же двум австралийским хакерам удалось почуять легкий аромат Deszip. В 1989 году они вторглись в компьютер колледжа Дартмута под названием Bear.<sup>[p110]</sup> В самом дальнем углу машины они обнаружили тщательно спрятанный Deszip. Они осторожно перепрятали копию в более надежную машину в другом учреждении.

Но победа ускользнула от них. Эта копия Deszip была зашифрована с помощью Crypt, программы, базирующейся на принципах работы немецкой машины Enigma, применявшейся еще во время Второй мировой войны. Без фразы-пароля – ключа к шифру – прочитать Deszip было невозможно. Они могли только разочарованно смотреть на файл под названием Deszip с недостижимым сокровищем внутри.

Неукротимые хакеры решили сохранить зашифрованный файл на тот случай, если когда-нибудь где-нибудь наткнутся на фразу-пароль (например, в электронном письме в одном из десятков компьютеров, в которые они регулярно вторгались). Снабдив зашифрованный файл Deszip более безобидной этикеткой, они поместили копию в темном углу другой машины. Они решили, что страховка лишней не бывает, и передали вторую копию Gandalf'у, который спрятал ее в английском компьютере (на тот случай, если копия австралийцев неожиданно исчезнет).

В январе 1990 года Electron сосредоточил свое внимание на Zardoz. После очередного тщательного изучения старой копии Zardoz он обнаружил в списке системного администратора из Мельбурна. Абонент наверняка мог иметь полный архив Zardoz в своей машине, причем он был так близок – меньше, чем в полчасе езды от дома Electron'а. Все, что оставалось сделать, – это взломать CSIRO.

Commonwealth Scientific and Industrial Research Organisation, или CSIRO,<sup>[p111]</sup> представляет собой правительственную исследовательскую структуру с множеством отделений по всей Австралии. Electron'у нужно было попасть только в одно из них – Отделение информационных технологий в доме № 55, Барри-стрит, Карлтон, совсем рядом с Мельбурнским университетом.

Роясь в компьютере университета, Electron уже наткнулся на одну копию архива Zardoz, принадлежавшую системному администратору. Он подобрал ее и начал осторожно загружать в свою машину. Его компьютер медленно вливал в себя копию Zardoz, как вдруг связь с университетом неожиданно прервалась. Админ обнаружил хакера и мгновенно уничтожил соединение. Все это отбросило Electron'а к исходному пункту, пока он не нашел копию Zardoz в машине CSIRO.

Было около трех часов ночи 1 февраля 1990 года, но Electron не устал. Его голова гудела. Он только что успешно проник в учетную запись под названием Worsley в компьютере CSIRO, который носил имя DITMELA. Для взлома Electron использовал ошибку в отправке почты. Он предположил, что DITMELA означает Division of Information technology, Melbourne, computer «А».

В этот день Electron начал тщательно анализировать директорию Эндрю Уорсли [Andrew Worsley]. Он знал, что где-то там находится Zardoz, хотя и не видел его раньше. После прощупывания компьютера и экспериментов с разными дефектами в системе безопасности в надежде, что один из них пропустит его внутрь, Electron'у удалось проскользнуть в компьютер незамеченным. Это случилось во второй половине дня – не самое удачное время для взлома компьютеров. Любой, кто находился в машине, мог очень быстро засечь нарушителя. Поэтому Electron сказал себе, что он лишь проведет разведку на местности. Посмотреть, есть ли там Zardoz, затем поскорее убраться отсюда, чтобы вернуться позже – лучше всего ночью – и вытащить Zardoz.

Когда Electron увидел в директории Уорсли полный архив Zardoz, его первым порывом было поскорее схватить его и смыться. Но проблема заключалась в том, что с его медлительным модемом он не мог исчезнуть достаточно быстро. Подавив непреодолимое желание приблизиться к Zardoz и завладеть им здесь и сейчас, он бесшумно выскользнул из машины.

Следующей ночью взволнованный и нетерпеливый Electron вернулся в DITMELA и направился напрямик в директорию Уорсли. Zardoz был на месте. По странной иронии Electron использовал

---

p110

«Медведь».

p111

Научно-промышленная исследовательская организация Содружества.

ошибку в безопасности, обнаруженную им в раннем выпуске Zardoz, чтобы попасть в компьютер, который вот-вот сдаст на его милость полный архив программы.

Но вытащить Zardoz из машины CSIRO представлялось не самым легким делом. Архив был велик, и с 300 бод – 30 символов в секунду – модему Electron'у потребовалось бы пять часов, чтобы скачать всю копию. Используя команду CAT, Electron сделал копии всех выпусков Zardoz и собрал их в один файл размером в 500 килобайт. Он окрестил новый файл t и сохранил его во временной директории DITMELA.

Затем он стал соображать, что делать дальше. Он отправил еще одну копию архива в другую учетную запись за пределами машины CSIRO, для пущей сохранности. Но после этого ему предстояло сделать выбор – попытаться скачать эту штуковину самому или дать отбой, позвонить Phoenix'у и попросить его сделать это.

Модем Phoenix'a на 2400 бод мог скачать пакет Zardoz в восемь раз быстрее, чем модем Electron'a. С другой стороны, Electron вовсе не жаждал предоставить Phoenix'у доступ в машину CSIRO. Они оба примерялись к этой машине, но он не сказал Phoenix'у, что ему уже удалось проникнуть в нее. Не то чтобы Electron собирался придержать Zardoz, когда получит его. Наоборот, он хотел, чтобы Phoenix познакомился с файлом безопасности и они могли обменяться идеями. Но когда нужно было работать с учетными записями, Phoenix мог напортачить. Он слишком много болтал. Он был попросту несдержан.

Пока Electron обдумывал свое решение, его пальцы продолжали работать на клавиатуре. Он быстро печатал, отправляя копии пакетов Zardoz на две взломанные студенческие учетные записи Мельбурнского университета. Имея пароли к обеим записям, он мог сделать это в любое время без всякого риска для себя и своего драгоценного груза. Две учетные записи – главная и запасная – лучше, чем одна. Вдруг кто-нибудь изменит пароль на какой-нибудь из них.

Не успела машина DITMELA отправить копии Zardoz на запасные сайты, как соединение Electron'a неожиданно сдохло.

Машина CSIRO зависла, что скорее всего означало то, что админ вырубил его. Electron был в ярости. Какого хрена системный администратор сидит за компьютером в такое время? Он должен спать! Поэтому Electron начал работать так поздно. Он видел Zardoz в машине CSIRO еще днем, но проявил нечеловеческое терпение, запретив себе даже прикасаться к нему – шанс, что его обнаружат, был слишком велик. А теперь вот это.

Единственное, что оставалось – позвонить Phoenix'у и попросить его войти в учетные записи Мельбурнского университета, чтобы проверить, как дошла почта. Если все в порядке, он успеет скачать ее со своим скоростным модемом до того, как админ CSIRO предупредит своего университетского коллегу и тот изменит пароли.

Electron набрал номер Phoenix'a. Они давно уже перестали обращать внимание на время суток, когда звонили друг другу. 10 часов вечера, 2 часа ночи, 4.15 утра, 6.45 утра.

– Ага, – Electron приветствовал Phoenix'a в своей обычной манере.

– Хай, – отозвался Phoenix.

Electron рассказал ему, что случилось, и дал обе учетные записи в университете, на которые он отправил список Zardoz.

Phoenix дал отбой и перезвонил через несколько минут. Обе учетные записи были уничтожены. Кто-то в университете вошел и изменил пароли за те полчаса, пока Electron выбирался из машины CSIRO. Оба хакера были встревожены тем, что это могло означать. Видимо, кто-то – скорее всего несколько человек – пасет их. Но непреодолимое желание получить Zardoz пересилило страх.

У Electron'a была еще одна учетная запись в компьютере CSIRO. Он не хотел отдавать ее Phoenix'у, но у него не было выбора. Теперь все предприятие висит на волоске. Кто может знать, что Zardoz останется на месте? Вполне возможно, что админ, который вышвырнул Electron'a, мог перенести архив в какое-нибудь недоступное место. Но это был единственный шанс.

Когда Electron сказал Phoenix'у пароль и имя пользователя, он велел ему скопировать Zardoz на несколько других машин, подключенных к Интернету, вместо того чтобы пытаться скачать его в свой компьютер. Это будет намного быстрее, и админ CSIRO едва ли посмеет вторгнуться в чужие компьютеры, чтобы уничтожить скопированный файл. Лучше всего выбрать зарубежные сайты, чтобы еще больше затруднить попытку админа связаться с админами этих машин и вовремя предупредить их. Потом, когда Zardoz будет в безопасности спрятан на нескольких запасных сайтах, Phoenix сможет скачать его через Интернет, почти не рискуя, что его вышвырнут из машины в самый разгар процесса.

Сидя у себя дома в Келвин-Гроув, Торнбери, в двух кварталах от машины CSIRO, Иэн Мэтисон [Ian Mathieson] смотрел, как хакер снова лезет в его компьютер. Мэтисона разбудил телефонный звонок в половине третьего ночи, ему сообщили, что в его машине подозрительный хакер. Мэтисон немедленно вошел в рабочую систему DITMELA через свой ПК и модем. Звонок от Дэвида Хорнсби [Davis Hornsby] с кафедры компьютерных наук Мельбурнского университета не был ложной тревогой.

Минут двадцать понаблюдав за неизвестным хакером, который проник в его машину через университетский компьютерный терминал, Мэтисон выкинул его из системы. Затем он заметил, что DITMELA пытается выполнить команду, заданную хакером. Посмотрев повнимательнее, он обнаружил, что его машина отправляет почту на две учетные записи Мельбурнского университета.

Но эта почта не была отправлена полностью. Она все еще оставалась в почтовом буфере. Мэтисону стало любопытно, что так понадобилось хакеру в его системе, и он перенес файл в поддиректорию, чтобы посмотреть, что же там такое. Когда он увидел там полный архив Zardoz – а он знал, что это такое, – то ужаснулся. Это были не простые хакеры – это были птицы высокого полета. К счастью, утешал себя Мэтисон, он остановил отправку почты и предотвратил катастрофу.

К несчастью, Мэтисон не заметил оригинальный файл Electron'a – пакет копий Zardoz. Когда Electron отправил файл, он скопировал его, оставив оригинал нетронутым. Пакет Zardoz все еще находился в DITMELA под неприметным названием X. Отправка файла не стирает его – компьютер только посылает копию оригинала. Мэтисон был умным человеком, доктором медицины с компьютерной степенью, но он забыл проверить временную директорию – одно из немногих мест, где хакер мог сохранить файлы в системе Unix, если у него не было привилегий.

Ровно в 3.30 утра Phoenix вошел в DITMELA из Техасского университета. Он быстро просмотрел временную директорию. Файл .t был на месте, именно там, где сказал Electron. Не теряя ни минуты, хакер приступил к его переносу в университет Техаса.

Он отлично себя чувствовал. Похоже, что австралийцы в конце концов завладеют всей коллекцией Zardoz. Все шло необычайно хорошо, пока перенос вдруг не прекратился. Phoenix забыл проверить, достаточно ли места на диске в учетной записи Техасского университета, чтобы загрузить на него объемистый пакет Zardoz. Теперь, когда он был подключен к очень «горячей» машине, за каждым движением которой мог наблюдать админ, он обнаружил, что там не хватает места для драгоценного файла.

Зная, что каждая секунда, проведенная онлайн в DITMELA, связана с серьезным риском, Phoenix немедленно вышел из машины CSIRO. Будучи все еще подключен к Техасскому университету, он поработал там, уничтожая другие файлы, чтобы подготовить достаточно места для размещения всех 500 килобайт файла Zardoz.

В 3.37 Phoenix снова вошел в DITMELA. На этот раз он поклялся, что все пойдет, как надо. Он запустил отправку файла и стал ждать. Меньше, чем через десять минут он вышел из машины CSIRO и нервно проверил систему Техасского университета. На месте. Zardoz был там, во всей своей красе! И он принадлежал ему! Phoenix был в экстазе.

Но оставались еще кое-какие дела, и времени благодушествовать не было. Phoenix начал в спешке сжимать и зашифровывать Zardoz. Он сжимал его потому, что маленький файл труднее заметить и его быстрее можно отправить в запасную машину. Он зашифровал его так, что при самом тщательном осмотре нельзя было догадаться, что там находится. Он не слишком волновался по поводу сисадминов; хакеры просто кишели в техасской системе, отчасти потому, что это был дом родной его друга, хакера из Legion of Doom и студента университета Eric Bloodaxe.

После того, как Phoenix был удовлетворен защитой Zardoz, он около 4-х утра позвонил Electron'у и сообщил ему отличную новость. К 8.15 Phoenix перекачал Zardoz с техасского компьютера в свою собственную машину. К 13.15 архив был уже в компьютере Electron'a.

Было нелегко завоевать Zardoz, но Deszip обещал стать гораздо более трудной задачей. Тогда как десятки экспертов по безопасности обладали архивом Zardoz, Deszip был доступен лишь немногим. И все они жили в США, по крайней мере, официально.

Правительство США объявило незаконным экспорт алгоритмов шифрования. Переслать копию Deszip, DES или любой другой шифровальной программы означало совершить преступление. Это считалось незаконным, потому что Управление по контролю за оборонными сделками Государственного департамента США [\[p112\]](#) признавало любую шифровальную программу оружием.

ITAR/p113] (международные правила перевозки оружия), основываясь на Законе США о контроле за экспортом оружия 1977 года, ограничивали публикацию и продажу «оборонного товара». Неважно, что вы сделали – полетели в Европу с дискетой в кармане или отправили материал через Интернет. Если вы нарушили ITAR, вам грозит тюремный срок.

Время от времени американские компьютерные программисты втайне переправляли копии шифровальных программ специалистам в своих областях за пределы США. Как только программа оказывалась вне Штатов, это была законная добыча. Американские власти не могли ничего поделать, если кто-то в Норвегии отправлял Deszip своему коллеге в Австралию. Но даже в таких случаях сообщества криптографов и экспертов по компьютерной безопасности очень ревностно охраняли такие программы, как Deszip, в собственных тайных святилищах.

Все это означало, что Electron'у и Phoenix'у почти наверняка придется иметь дело с американским сайтом. Electron продолжал составлять хит-парад, базируясь на списке адресатов Zardoz, который был и у Phoenix'а. И оба хакера принялись искать в растущем Интернете компьютеры, принадлежащие намеченным мишеням.

Это был впечатляющий хит-парад. Мэтью Бишоп, автор Deszip. Рассел Брэнд [Russell Brand] из Национальной лаборатории имени Лоренса Ливермора, исследовательского центра, финансируемого Министерством энергетики США. Дэн Фармер [Dan Farmer], автор популярной компьютерной программы проверки безопасности COPS, которая также включала в себя функцию взлома паролей. Были и другие. А возглавлял список Юджин Спаффорд, или Спаф, как его называли хакеры.

К 1990 году все компьютерное подполье считало Спафа не только гуру безопасности, но и фанатичным противником хакеров. Спаф окопался в университете Пардью, рассаднике экспертов по компьютерной безопасности. Бишоп получил свою докторскую степень в Пардью, и Дэн Фармер тоже засел там. Спаф был одним из основателей Usenet, службы новостей Интернета. Работая с компьютерами в университете как серьезный ученый, он также сделал себе имя на том, что, кроме всего остального, составил технический анализ червя RTM. Этот червь, порожденный гением студента Корнельского университета Роберта Т. Морриса-мл. [Robert T. Morris Jr.] в 1988 году, стал стержнем карьеры Спафа.

До червя RTM Спаф занимался разработкой программного обеспечения. После червя он стал заниматься компьютерной этикой и полюбил произносить публичные речи, ратуя за консерватизм в компьютерной безопасности. Спаф совершил турне по Штатам, просвещая население и СМИ насчет червей, вирусов и кодекса хакеров. Во время слушания дела Морриса хакинг стал популярной темой в Америке, и Спаф подливал масла в огонь. Когда судья Говард Дж. Мансон [Howard G. Munson] отказался приговорить Морриса к тюремному заключению, а вместо этого назначил ему 400 часов общественных работ, \$10 000 штрафа и три года условно, Спаф публично раскритиковал это решение. СМИ опубликовали призыв Спафа, обращенный к компьютерной индустрии, бойкотировать любую компанию, которая посмеет взять на работу Роберта Т. Морриса-мл.

Выбор машины Спафа в качестве мишени служил двум целям австралийских хакеров. Он был, несомненно, вместилищем сокровищ, таких как Deszip, а кроме того, он был притчей во языцех.

Итак, однажды ночью Electron и Phoenix решили взломать машину Спафа в Пардью, чтобы украсть оттуда копию Deszip. Phoenix должен был заниматься собственно хакингом, потому что его модем был быстрее. Electron будет поддерживать с ним связь по телефону и руководить каждым его шагом. Таким образом, если Phoenix столкнется с неожиданным препятствием, ему не понадобится отступать для перегруппировки и рисковать заниматься исследованием.

Хакерам удалось взломать другую машину Пардью под названием Medusa. Но у Спафа был свой компьютер, Uther, подключенный к Medusa.

Phoenix рыскал туда-сюда возле Uther, пытаясь найти достаточно широкую щель, чтобы проскользнуть внутрь. По наводке Electron'а он попытался использовать ошибку CHFN. Эта команда позволяла пользователю изменять имеющуюся информацию – такую как его имя, рабочий адрес или номер телефона офиса, – если он обнаруживал, что кто-то напачкал в его учетной записи. Отчет об ошибке был опубликован в одном из файлов Zardoz, и Phoenix с Electron'ом уже использовали ее для проникновения в несколько других машин.

Electron хотел применить ошибку CHFN, потому что в случае успеха Phoenix мог создать себе

привилегированную учетную запись в машине Спафа. Это было бы финальным щелчком по носу надменного гуру компьютерной безопасности.

Но у Phoenix'a не все пошло гладко. В отчаянии австралийский хакер повторял своему наставнику, что ошибка вот-вот сработает, но она не работала, и он не мог понять почему. В конце концов Electron сделал вывод, что проблема заключается в том, что машина Спафа – это Sequent. Успех ошибки CHFN зависел от особой структуры файла пароля в Unix, но машины Sequent использовали другую структуру. К тому же Phoenix не слишком много знал о машинах Sequent – это была одна из специальностей Electron'a.

После нескольких безуспешных часов борьбы в попытке запустить ошибку CHFN, Phoenix сдался и по совету Electron'a попробовал использовать другой недостаток безопасности – ошибку FTP.<sup>[p114]</sup> Phoenix постарался вспомнить свойства ошибки. Обычно FTP использовался для перемещения файлов из одного компьютера в другой в сети. Перемещение файла в другую машину было немного похоже на доступ через telnet.<sup>[p115]</sup> но пользователю не нужен был пароль для регистрации. Кроме того, набор команд, который он мог применить в другом компьютере, был крайне ограничен.

Если ошибка FTP сработает, она позволит Phoenix'у протащить дополнительную команду во время введения имени пользователя FTP. Контрабандная команда заставит компьютер Спафа позволить Phoenix'у зарегистрироваться в любом нужном ему качестве – а ему нужно было зарегистрироваться как обладателю привилегированного доступа. Учетная запись root была слишком очевидной, если кто-то наблюдал за компьютером, кроме того, она не всегда разрешала удаленный доступ. Поэтому вместо нее Phoenix выбрал daemon, другую распространенную привилегированную учетную запись.

Это было словно выстрел в темноту. Phoenix справедливо полагал, что Спаф обезопасил свою машину против такой наглой атаки, но Electron поторапливал его все равно попробовать применить эту ошибку. Ошибка FTP стала известна в сообществе компьютерной безопасности очень давно, появившись в одном из ранних выпусков Zardoz. Phoenix колебался, но у него не было ни других идей, ни времени.

Он набрал:

```
FTP – i uther.purdue.edu
quote user anonymous
quote cd – daemon
quote pass anything
```

Несколько секунд, которые потребовались для передачи команды из его дома в пригороде Мельбурна на американский Средний Запад, тянулись, кажется, целую вечность. Он *хотел* машину Спафа, хотел deszip и хотел, чтобы его атака удалась. Если он сможет завладеть Deszip, австралийцев уже ничто не остановит.

Компьютер Спафа распахнул перед ним двери так же услужливо, как швейцар в отеле Ritz Carlton. Phoenix улыбнулся своему компьютеру. Он был *внутри*.

Он словно очутился в пещере Аладдина. Phoenix просто стоял там, остоленев при виде лежащих перед ним сокровищ. Это принадлежало ему, только ему. В директориях Спафа хранились мегабайты файлов по компьютерной безопасности. Исходный код червя RTM. Исходный код червя WANK. Все на свете. Phoenix хотел погрузить руки по локоть в каждый сундук с сокровищами и жадно черпать оттуда целыми пригоршнями, но он справился со своим желанием. Прежде всего он должен был выполнить более важную – в стратегическом отношении – миссию.

Он пробирался среди директорий, всюду выискивая Deszip. Как ночной грабитель, рыщущий по дому в поисках семейного серебра, он обшаривал директорию за директорией. У Спафа наверняка должен быть Deszip. Если кто-то, кроме Мэтью Бишоп, и имеет его копию, так это Спаф. И он наконец нашелся. Вот он – только и ждет, когда Phoenix возьмет его.

Тут Phoenix заметил кое-что еще в другом файле. Любопытство взяло верх, и он подошел к не-

---

p114

File Transfer Protocol – протокол передачи файлов.

p115

Telnet – протокол, который позволяет присоединиться к компьютеру и работать с ним в удаленном режиме.

му, чтобы быстренько глянуть, что там. В нем была *фраза-пароль*. Фраза, необходимая австралийцам, чтобы расшифровать оригинальную копию Deszip, которую они украли из компьютера Bear в Дартмуте тремя месяцами ранее. Phoenix не мог поверить своим глазам. Это было просто до безобразия. Но он остановил себя. Не время было попусту размахивать руками. Ему нужно было побыстрее вытащить Deszip из этой машины, пока никто не заметил, что он внутри.

Но как только Phoenix начал посылать команды, его экран словно застыл. Он проверил. Это был не его компьютер. Что-то пошло не так на той стороне. Он все еще был в машине Спафа. Соединение не было уничтожено. Но когда он отправил команду, компьютер в Западном Лафайете, штат Индиана, не отреагировал на нее. Машина Спафа словно оглохла и онемела.

Phoenix уставился на свой компьютер, пытаясь понять, что происходит. Почему машина Спафа не отвечает? Причин могло быть только две. Либо соединение между первой машиной (в которую он проник в Пардью) и машиной Спафа случайно прервалось. Либо кто-то выдернул штепсель.

Но ради чего? Если они знали, что он там, почему просто не дать ему пинка под зад? Более того, они запросто могли выставить его из всей системы Пардью. Может быть, они хотели оставить его онлайн, чтобы узнать, из какой машины он пришел, пройти по его следу, петляющему от системы к системе?

Перед Phoenix'ом встала проблема выбора. Если соединение нарушено случайно, ему нужно было сохранить подключение и подождать, пока сеть не восстановится. Удача с ошибкой FTP в машине Спафа была просто подарком судьбы. Слишком велики шансы того, что кто-то обнаружит доказательства его проникновения после того, как он уйдет, и законопатит дыру. С другой стороны, он не хотел, чтобы народ из Пардью проследил его соединение.

Он подождал еще несколько минут, пытаясь застраховать себя от возможных неприятностей. Нервничая из-за того, что тишина в машине Спафа слишком уж затянулась, Phoenix решил отваливать. Заветные сокровища пещеры Аладдина растаяли перед ним, как мираж. Phoenix разорвал соединение.

:)

Electron и Phoenix разговаривали по телефону, уныло подсчитывая потери. Это был провал, но Electron напомнил себе, что никто не говорил ему, что получить Deszip будет легко. По крайней мере, у них теперь есть ключевая фраза, чтобы расшифровать Deszip, похищенный из Дартмута.

Но они снова столкнулись с проблемой. Electron уже начал думать, что так будет всегда. Они просто по определению не могли получить что бы то ни было, не столкнувшись с трудностями. Иначе, наверное, было бы не так интересно. На этот раз проблема заключалась в том, что, когда они попытались найти свою копию из Дартмута, отправленную на хранение несколько месяцев назад, они обнаружили, что она исчезла. Должно быть, сисадмин стер ее.

Это было безумие. Их огорчению не было предела. Всякий раз, как им удавалось увидеть Deszip в пределах досягаемости, он ускользал от них и исчезал. Но всякий раз, как это случалось, их желание захватить этот неуловимый приз становилось все сильнее. Deszip превратился в наваждение, всепожирающую страсть Phoenix'а и Electron'а.

Их последней надеждой была вторая копия зашифрованного Deszip из Дартмута, которую они передали Gandalf'у. Но на это не стоило особенно надеяться. Если копия австралийцев была уничтожена, существовала большая вероятность того, что британскую копию постигла та же судьба. Копия Gandalf'а хранилась не в его компьютере. Он засунул ее в темный угол какой-то английской машины.

Electron и Phoenix отправились в Altos и принялись ждать, когда объявятся Pad и Gandalf.



```

WELCOME TO THE ALTOS HAMBURG CHAT SYSTEM !
Where are you from ? :

  ///#      ///#      //////////#      ////#      ///#
  ///#      ///#      //////////#      //////////#      ///#
  ///#      ///#      //////////#      ///#      ///#
  ///#///#      ///#      ////#      ///#      ///#      ///#
  ///#      ///#      ///#      ////#      ////#      ///#
  //////////#      //////////#////////#      //////////#      //////////#
  //////////#      //////////#      ////#      ///#      //////////#

  C_O_M_P_U_T_E_R_S_Y_S_T_E_M_S_H_A_M_B_U_R_G
  Programs by Axel Bauer, Mmail by Patrick Guelat,
  Some corrections made by llcoolj
  System Administration by Lutz Pelikan

AVAILABLE COMMANDS ARE:
HELP      CMDS      EXIT      PASSWD      ACCOUNT
MMAIL     CHAT      BULLET    ROBOTS
ROBOTS2   WHO       DATE      CAL
USERS     VIEW

```

Phoenix набрал .s, чтобы получить список тех, кто находился онлайн. Он увидел, что Pad на месте.

```

No Chain User
0      Guest
1      Phoenix
2      Pad

```

Гостем 0 был Electron. Как правило, он регистрировался как Guest,<sup>[p116]</sup> поскольку жутко боялся ареста и опасался, что операторы непременно проследят его соединение, если узнают, что он Electron. Админы с большим энтузиазмом вынюхивали пароль его собственной учетной записи в Altos. Затем, когда он отключался, они входили и изменяли пароль, и он уже не мог войти под именем Electron. Ничто не могло быть более досадным. Phoenix набрал:

– Эй, Pad, как жизнь?

– Фенни, привет! – отозвался Pad.

– Слушай, у вас с Гэндом осталась та зашифрованная копия Deszip, которую мы с Electron'ом дали вам пару месяцев назад?

– Зашифрованная копия... гм. Дай подумать.

Pad замолчал. Они с Gandalf'ом постоянно взламывали десятки систем. Иногда было трудно вспомнить, куда они могли спрятать тот или иной файл.

– Да, я понял, о чем ты. Я не знаю. Вроде бы в одной из систем на JANET, – сказал Pad.

Английская Joint Academic Network<sup>[p117]</sup> была аналогом австралийской AARNET – ранний Интернет, объединяющий преимущественно машины университетов и научных центров.

– Я не могу вспомнить, в какой системе, – продолжал Pad.

Если англичане не смогут вспомнить учреждение и машину, куда они спрятали Deszip, то прощай, последняя надежда. JANET состояла из сотен, если не тысяч машин. Это было далеко не то место, чтобы искать файл, который Gandalf, само собой, постарался замаскировать как можно надежнее.

– Но файл был зашифрован, а у вас не было пароля, – написал Pad. – На кой он вам сдался?

– Потому что мы нашли пароль &lt;ха-ха&gt;.

Это была особая фишка Altos. Если нужно было заострить на чем-то внимание, то это понятие или действие заключалось в угловые скобки.

---

p116  
Гость.

p117  
Объединенная академическая сеть.

– Gr8! – ответил Pad.

Это был стиль онлайн-общения Pad'a и Gandalf'a. Восьмерка/[p118] была отличительным признаком британских хакеров – их группа называлась 8lgm, – и они использовали ее вместо букв в некоторых словах. Например, слова типа «great», «mate» и «later»/[p119] превратились в gr8, m8 и l8r.

Когда люди регистрировались в Altos, они могли назвать «место» происхождения, чтобы другие могли знать, откуда они пришли. Конечно, если в вашей стране существовали законы против хакеров, вы могли не говорить о том, откуда вы на самом деле. Некоторые регистрировались аргентинцами или израильянами. Pad и Gandalf приходили из 8lgm.

– Я постараюсь найти Gandalf'a и спрошу у него. Может быть, он помнит, куда мы засунули копию, – написал Pad.

– Отлично. Спасибо.

Пока Phoenix и Electron оставались онлайн, ожидая возвращения Pad'a, в чате появился Par и присоединился к их разговору. Par не знал, кто такой Guest 0, но Guest, конечно, знал, кто такой Par. Время не исцелило старые раны Electron'a и не изменило его отношения к Par'у. Electron старался не портить себе кровь мыслями о том, что связано с Theorem. Он говорил себе, что Par всего лишь фрикер, не настоящий хакер, что Par жалок.

Phoenix набрал:

– Эй, Par. Как дела?

– Фенни! – ответил Par. – Что нового?

– Полно всего.

Par обратил внимание на Guest 0. Он не хотел обсуждать личные вопросы в присутствии неизвестного, который мог оказаться человеком из компьютерной безопасности, из тех, что слетались на чат-канал, как мухи на дурной запах.

– Guest, у тебя есть имя? – спросил Par.

– Да. Guest 0.

– У тебя есть другие имена?

Долгая пауза.

– Думаю, нет, – ответил Electron.

– Есть у тебя имена, кроме этой ерунды?

Electron послал «шептуна» – частное сообщение – Phoenix'у, с просьбой не сообщать Par'у, кто он.

«ОК, конечно», – «прошептал» Phoenix в ответ. Чтобы показать, что он в любом случае готов подыграть Electron'у, Phoenix прибавил в конце «смайлик».

Par не знал, что Phoenix и Electron перешептываются друг с другом. Он все еще ждал, что Гость откроет ему свою личность.

– Давай, Guest, говори. Ты сам-то знаешь, кто ты такой?

Electron знал, что Par в бегах. Действительно, к началу 1990 года Par скрывался от Секретной службы уже больше полугода. Electron'у также было известно, что Par настоящий параноик.

Electron прицелился и выстрелил:

– Эй, Par. Тебе надо побольше есть. Ты что-то похудел. Ты случайно не рыл на днях подКОПЫ?

Par вдруг замолчал. Electron сидел за компьютером на другой стороне планеты и хихикал про себя. «Да, – думал он, – это на какое-то время может вырубить Par'a». Самый незначительный намек на правоохранительные органы мог свести его с ума.

– Ты видел ЭТО? – прошептал Par Phoenix'у – ПодКОПЫ. Что он хочет сказать?

– Фиг знает, – «шепотом» ответил Phoenix. Затем он переправил Electron'у копию частных сообщений Par'a. Он знал, что это развеселит его.

Par был явно взволнован.

– Да кто ты, черт возьми? – Par «прошептал» Electron'у, но Guest 0 не ответил.

Все больше беспокоясь, Par «прошептал» Phoenix'у:

– Кто ЭТОТ парень? Ты его знаешь?

---

p118

Читается как «эйт».

p119

Здорово [грэйт], приятель [мэйт], позже [лэйтер] (англ.).

Phoenix не ответил.

– Черт, это странно. Ты видел? КОПЫ было написано большими буквами. Какого хрена это значит? Он коп? Или хочет передать мне послание от копов?

Сидя за своим терминалом на другом краю Мельбурна, довольно далеко от Electron'a, Phoenix тоже хохотал. Ему нравился Par, но он был слишком легкой добычей. Par помешался с тех пор, как начал бегать по всей Америке, и Electron просто знал, на какую кнопку нажать.

– Я не знаю, – «шепотом» сказал Phoenix, – но уверен, что он не коп.

– Ну, мне просто любопытно это замечание, – ответил Par. – ПодКОПЫ. Хм. Может, он что-то знает. Может, это какое-то предупреждение. Черт, может, они знают, где я?

– Ты думаешь, что это предупреждение? – прошептал Phoenix.

Это было очень смешно.

– Ты можешь посмотреть его исходный NUA? – Par хотел знать, из какого сетевого адреса прибыл таинственный гость. Это могло дать ему ключ к его личности.

Phoenix с трудом сдерживался. Он продолжал скидывать Electron'у частные сообщения Par'a, который явно все больше беспокоился.

– Я хочу, чтобы он просто сказал мне, кто он такой, – прошептал Par. – Черт. Это просто странно, твою мать. ПодКОПЫ. Это пугает меня.

И Par отключился.

Electron набрал: «По-моему, Par'у пора идти &lt;усмешка>».

Затем, все еще посмеиваясь, он принялся ждать новостей о копии Deszip у Gandalf'a.

Если Pad и Gandalf не сохранили свою копию Deszip, австралийцам вновь придется начинать все сначала. Им придется снова охотиться за системами, в которых, может быть, есть Deszip. Это могло обескуражить кого угодно, и когда Pad и Gandalf, наконец, появились в Altos, Phoenix и Electron уже не на шутку волновались.

– Как все прошло? – спросил Phoenix. – У вас есть Deszip?

– Ну, сначала я думал, что забыл, куда его засунул...

– И что? – взвился Electron.

– Потом я вспомнил.

– Хорошие новости?

– Мм, нет. Не совсем, – сказал Gandalf. – Учетная запись сдохла.

Electron'у показалось, что его окатили ведром холодной воды.

– Сдохла? Как сдохла?

– Похоже, что кто-то изменил пароль. Не знаю почему. Мне надо снова залезть в систему, чтобы поближе подобраться к файлу.

– Твою мать, этот Deszip уже достал, – написал Electron.

– Это уже не смешно, – добавил Phoenix.

– Я даже не знаю, на месте ли копия, – отозвался Gandalf. – Я спрятал ее, но кто знает? Прошло несколько месяцев. Админы могли стереть ее.

Phoenix спросил:

– Может быть, тебе нужно помочь взломать систему?

– Нет, это легко. Это Sequent. Мне надо просто дождаться, пока все операторы уйдут домой.

Если бы оператор оказался в системе и увидел, что Gandalf что-то ищет в ней, он мог бы выставить Gandalf'a и попытаться найти интересующий хакера файл. И они наверняка потеряли бы Deszip.

– Надеюсь, мы найдем его, – вмешался Pad. – Это было бы gr8.

– Не то слово. Фен, у тебя есть ключ к шифру? – спросил Gandalf.

– Да.

– Сколько в нем букв?

Это был особый хитрый способ Gandalf'a вывести нужную информацию.

Phoenix не знал, как ему поступить. Он вроде бы хотел дать хакерам ключ, но колебался. Он нуждался в помощи Pad'a и Gandalf'a, чтобы получить копию Deszip, если это вообще возможно. Но он знал, что Electron наблюдает за разговором, а он всегда был крайне недоверчив. Он ненавидел выдавать любую информацию, тем более в Altos, где разговоры могла подслушивать служба безопасности.

– Ну что, дать ему ключ? – «прошептал» Phoenix Electron'у.

Gandalf ждал. Чтобы он отвязался, Phoenix сказал:

– Там семь симв.

Сим – это сокращение от «символ». В Altos действовало правило сокращать все, что возможно.

– Какой первый сим?

– Ладно, скажи ему, – «прошептал» Electron.

— Ладно, ключ такой...

– Гэнд, смотри, не блевани, когда услышишь это, – вмешался Electron.

– Ладно... давай, – сказал Gandalf. – Я слушаю.

– Ты не поверишь &lt;блевать блевать блевать&gt; Пароль – Дартмут.

– ЧТО???? ЧТО!! – воскликнул Gandalf. – ЭТО НЕ-ПРАВДА! Дерьмо! Ты ШУТИШЬ?

Британский хакер стучал себя по голове. Название долбаного университета! Какой идиотский пароль!

## Phoenix выдал смешок онлайн.

– Хе-хе. Да. Так сложно догадаться. Мы давным-давно могли иметь Deszip...

– Боже, надеюсь, он все еще в JANET, – сказал Gandalf. Теперь, когда у них был пароль, надо было найти файл как можно быстрее.

– Молись. Молись. Молись, – сказал Phoenix. – Да, тебе бы стоило взглянуть на текст лицензии Deszip – его написали в NASA.

– Ты видел его? Ты видел исходный код Deszip?

– Нет, – ответил Phoenix. – Когда я вернулся в машину Bear, чтобы проверить, на месте ли Deszip, программа ушла. Но лицензия и прочее канцелярское дерьмо осталось. Вам стоит прочитать ее... это очень забавно. В основном там пишут об одном: как те, кто ее написал, не хотят, чтобы такие, как мы, получили ее. Хе-хе.

## Нетерпение Electron'а возрастало.

– Да. Ну что, Gandalf, когда ты проверишь JANET?

– Прямо сейчас. Сожми кулаки, m8! Увидимся 18г...

И он отвалил.

Ожидание сводило Electron'a с ума. Он не переставал думать о Deszip, о том, что он мог давно заполучить ее. Эта программа была невероятным призом. Он истекал слюной при мысли о том, что наконец завладеет ею после нескончаемой погони по всему земному шару, после долгого преследования от системы к системе, в котором он никогда не приближался достаточно близко, чтобы схватить ее.

Когда Gandalf снова вышел на связь, Pad, Phoenix и Electron мгновенно навалились на него.

– ПАРНИ, МЫ СДЕЛАЛИ ЭТО, МАТЬ ТВОЮ!!!! – воскликнул Gandalf.

– Отличная работа, m8! – сказал Рад.

– Да! – добавил Electron. – Ты уже расшифровал ее?

– Пока нет. Срут не на этой машине. Мы можем либо скопировать Срут на нее, либо скопировать файл на другую машину, где уже есть Срут, – сказал Gandalf.

– Давайте займемся этим. Быстрее... быстрее... у этой чертовой штуки есть привычка неожиданно исчезать, – сказал Electron.

— Да, это последняя копия, единственная, которую я смог достать.

– ОК. Думайте, думайте... Куда мы могли бы ее скопировать? – сказал Electron.

– Техас! – Gandalf хотел перенести ее в компьютер Техасского университета в Остин, на родину хакера из LOD, Eric Bloodaxe.

Неукротимый Gandalf был подобен паровому катку, если ты ему нравился, и мог уничтожить тебя в мгновение ока, если нет. Его задиристый пролетарский юмор особенно привлекал Electron'a. Иногда казалось, что Gandalf обращается к серьезным и глубоким вещам, волнующим тебя больше всего, а вместо этого он выпаливал какую-то грубость, так что ты не мог удержаться от смеха. Это была его манера показать тебе свое дружеское расположение.

– Да! Давайте повесим все на Eric'a, – пошутил Phoenix. – Нет, серьезно. Сейчас там полно секьюрити, они охотятся за Eric'ом. Они там *повсюду*.

Phoenix слышал о чистке университета от самого Eric'a. Австралиец звонил Eric'у постоянно, в основном с использованием краденых карт AT&T. Секретная служба пока еще не приходила к Eric'у с ордером на обыск, но он держался настороже и ожидал их визита со дня на день.

— Возможно, мы даже не сможем его расшифровать, — сказал Electron.

– О, дерьмо! – выпалил Gandalf. – Давайте! Мне нужен сайт СЕЙЧАС!

– Я думаю, – сказал Phoenix. – Должно быть какое-то место с достаточной памятью... насколько он большой?

– 900 Кб в сжатом виде – возможно, 3Мб в исходном состоянии. Давай, соображай! Как насчет университета?

– Принстон или Йейль могли бы это сделать, – предположил Electron. – Как насчет MIT – вы не были там в последнее время, Гэнд?

– Нет.

Все четверо хакеров напряженно скребли затылки в поисках небес обетованных. Весь мир был в их руках, и сейчас в Германии эти британские и австралийские хакеры держали совет в режиме реального времени о том, где спрятать их сокровище – в Остине, штат Техас, в Принстоне, штат Нью-Джерси, в Бостоне, штат Массачусетс, или в Нью-Хейвене, штат Коннектикут.

– Нам всего лишь надо припрятать его ненадолго, пока мы не сможем перекачать его, – сказал Gandalf. – Должна быть машина, в которой у нас есть привилегии. И там должен быть anon FTP.

Anon FTP, или анонимный FTP, на хосте позволил бы Gandalf'у перенести файл с компьютера JANET на хост через Интернет. Гораздо важнее был тот факт, что Gandalf мог сделать это, даже не имея учетной записи в намеченной машине. Он мог зарегистрироваться, как «anonymous». Этот способ имел больше ограничений, чем обычная регистрация в нормальной учетной записи. Но все же он смог бы загрузить файл.

– Ладно, ОК, у меня идея, – сказал Phoenix. – Сейчас проверю.

Phoenix вышел из Altos и подключился к Техасскому университету. Физическое расположение сайта не имело значения. У него кружилась голова, и это было единственное место, о котором он мог думать. Но он не стал входить в Harry – машину, которой он часто пользовался. Он направился к другому университетскому компьютеру под именем Walt.

Сеть была перегружена. Phoenix в течение нескольких минут безуспешно ждал соединения. Линии были переполнены. Он вернулся в Altos и сказал об этом Pad'у и Electron'у. Gandalf куда-то пропал.

– Черт! – сказал Electron. – Ладно, по-моему, у меня есть мысль.

– Нет, подожди! – вмешался Phoenix. – Я только что вспомнил один сайт! И у меня там основной доступ! Но он в NASA...

– А, плевать. Я уверен, что они не будут против &lt;ухмылка>.

– Пойду, гляну, все ли там в порядке. Вернусь через секунду, – набрал Phoenix.

Он выбрался из Altos и помчался в NASA. С помощью telnet он проник в компьютер NASA под названием CSAB в Исследовательском центре Лэнгли в Хэмптоне, штат Вирджиния. Он довольно часто входил в NASA и выходил из него, и недавно сообразил себе основной доступ в CSAB. Первым делом он проверил, жива ли его учетная запись, затем ему нужно было убедиться, что сисадмина нет в компьютере.

Пропустив мимо ушей официальные предупреждения о последствиях неавторизованного доступа в компьютер правительства США, Phoenix ввел имя пользователя и пароль.

Готово. Он внутри. И у него основной доступ.

Он быстро огляделся по сторонам. Администратор был онлайн. Будь ты проклят.

Phoenix вылетел из машины NASA и устремился назад в Altos. Gandalf уже вернулся и вместе с двумя другими ожидал его возвращения.

– Ну? – спросил Electron.

– Все в порядке. Машина NASA работает. Там есть anon FTP. И у меня все еще есть основной доступ. Мы используем его.

– Постой, а там есть Crypt? – вмешался Gandalf.

– Ах ты! Забыл проверить. Думаю, должен быть.

– Лучше проверь, m8!

– Хорошо.

У Phoenix'а опускались руки от всей этой беготни в поисках подходящего сайта. Он вышел из Altos и вернулся в машину NASA. Админ все еще был там, но у Phoenix'а не было времени. Он должен узнать, есть ли в компьютере Crypt. Есть.

Phoenix поспешил в Altos.

– Я вернулся. Мы в деле.

– Супер! – сказал Electron и продолжил с предупреждением. – Не говори название машины NASA и учетную запись, куда будем грузить вещь. «Шепни» их Gandalf'у. Думаю, операторы засекли мое соединение.

– Ладно, – медленно набрал Phoenix, – но есть одна проблема. Админ в компе NASA.

– Грррм! – зарычал Electron.

– Просто сделаем это, – сказал Pad. – Некогда волноваться.

Phoenix «шепнул» Gandalf'у IP-адрес машины NASA.

– Ладно, парни, я анонимно перемещу это в NASA. Я вернусь сюда и скажу тебе название нового файла. Потом ты двинешь в NASA и вернешь его в исходное положение. w8[p120] меня здесь.

Через десять минут Gandalf вернулся.

– Миссия выполнена. Файл там.

– Давай-давай, Фенни! – сказал Electron.

– Гэнд, шепни мне имя файла, – попросил Phoenix.

– Он называется d и находится в общей директории, – «прошептал» Gandalf.

– Ладно, братцы. Я пошел! – сказал Phoenix и отключился.

Phoenix ринулся к компьютеру NASA, вошел в него и принялся искать файл d. Но его там не было. Он даже не смог найти общую директорию. Он начал рыскать по всей файловой системе. Куда могла деться эта хреновина?

Ага. Phoenix заметил, что системный администратор Шэрон Бискенис [Sharon Beskenis] все еще в компьютере. Она подключилась к Phoebe, другой машине NASA. Кроме Phoenix'а, в машине CSAB был только один пользователь, некто по имени Carrie. И словно все было еще недостаточно плохо, Phoenix вдруг осознал, что его имя пользователя торчало на этом фоне, как вывихнутый большой палец. Если админша проверит, кто находится онлайн, она увидит себя, Carrie и пользователя по имени Friend – учетную запись, созданную Phoenix'ом для своих личных делишек. Сколько легальных пользователей в компьютере NASA могут носить *это* имя?

Кроме того, Phoenix обнаружил, что он забыл прикрыть следы своего соединения. Friend проник в компьютер NASA из Техасского университета. «Нет, нет, – думал он, – это должно прокатить». Он отключился от NASA, метнулся назад в университет, а затем снова вернулся в NASA. Черт подери! Теперь проклятая машина NASA отображала двух пользователей, зарегистрировавшихся, как Friend. Компьютер не уничтожил его предыдущий вход. О нет!

Phoenix лихорадочно попытался вычистить свое первое соединение, уничтожив номер процесса. Компьютер NASA ответил, что у него нет такого номера. Все больше нервничая, Phoenix решил, что он ввел не тот номер. Окончательно обезумев, он взял и уничтожил один из других номеров процесса. Твою мать! Это был номер админа. Phoenix только что выставил Шэрон из ее собственной машины. Положение было не из веселых.

Теперь он оказался под серьезным давлением. Он не смел выйти, потому что Шэрон, несомненно, найдет его учетную запись, уничтожит ее и закроет дыру в системе безопасности, которую он использовал с самого начала, чтобы пробраться в компьютер. Даже если она не найдет Deszip в своей машине, Phoenix'у, может быть, больше никогда не удастся вернуться и забрать его.

Еще одна минута неистовых поисков в компьютере, и Phoenix наконец откопал копию Deszip, спрятанную Gandalf'ом. Наступил момент истины.

Он ввел ключевую фразу. Она сработала! Все, что оставалось сделать – вернуть Deszip в исходное состояние и убраться отсюда.

Он набрал `uncompress deszip.tar.z`, но ему не понравилось, как компьютер NASA ответил на эту команду.

corrupt input[p121]

Что-то пошло не так, совсем не так. Файл словно был частично разрушен. Об этом было страшно подумать. Даже если пострадала лишь незначительная часть программы Deszip, она вся не годилась для дальнейшего использования.

Вытирая пот с ладоней, Phoenix подумал, что, возможно, файл был поврежден, когда он пытался вернуть его в исходное состояние. Он сохранил оригинал, поэтому еще раз попытался дешифровать и разжать его. Компьютер NASA дал ему тот же неприятный ответ. Он сделал еще одну торопливую попытку, на этот раз другим способом. Та же проблема.

Phoenix зашел в тупик. Это было слишком. Единственное, что ему оставалось – надеяться, что

---

p120

Wait – жди (англ.).

p121

Неправильный ввод (англ.).

файл был поврежден во время передачи с машины JANET. Он вышел из NASA и вернулся в Altos. Остальные ждали его с нетерпением.

Electron, все еще под таинственным именем Guest, не выдержал первым:

– Получилось?

– Нет. Дешифровка в порядке, но файл оказался поврежденным, когда я попытался развернуть его.

– Prrrr! – захрипел Gandalf.

– Факфакфак, – написал Electron. – Это просто злой рок.

– Жаль жаль жаль, – набрал Pad.

Gandalf и Electron расспросили Phoenix'a в деталях о каждой использованной команде, но в результате осталась только надежда перенести копию программы дешифровки в компьютер JANET в Англию и попытаться расшифровать и развернуть Deszip там.

Phoenix дал Gandalf'у копию Crupt, и британский хакер отправился работать в компьютер JANET. Вскоре он вновь появился в Altos.

Phoenix был вне себя от этой свистопляски.

– Гэнд! Работает???

– Ну, я расшифровал его с помощью программы, что ты мне дал...

– И и и??? – Electron едва мог сидеть на стуле у своего компьютера.

– Попытался развернуть его. Процесс идет. Это займет МНОГО времени – там около 8 мегабайт.

– О нет! Черт черт черт, – простонал Phoenix. – Там должно быть не больше трех. Если там миллион файлов, мы в дерьме.

– Боже, – набрал Pad, – это невыносимо.

– Я получил предварительную информацию – текст лицензии и т. д., но сама программа Deszip повреждена.

– Я не понимаю, что было не так. <Сукин сын>, – написал Phoenix.

– Конец конец конец, – буркнул Electron. – У нас никогда никогда никогда не получится.

– Мы можем получить копию где-то еще? – спросил Gandalf.

– Ошибка FTP больше не прокатит в Пардью, – ответил Pad. – Мы больше не сможем использовать ее, чтобы влезть туда.

В Altos воцарилась атмосфера разочарования.

Конечно, были и другие хранилища Deszip. Phoenix и Electron уже побывали в компьютерах Ливерморской лаборатории в Калифорнии. Они обеспечили себе привилегированный доступ в машину gamm5 и планировали сделать ее стартовой площадкой для нападения на компьютер под названием Wuthel, который принадлежал эксперту компьютерной безопасности LLNL[p122] Расселу Брэнду. Они были уверены, что в компьютере Брэнда есть Deszip.

Это потребует серьезных усилий и наверняка новой головокружительной гонки желаний, надежд и, возможно, разочарований. Но сейчас четверо хакеров решили расползтись по норам, зализывая раны после поражения в битве за Deszip.

– Ладно, я отключаюсь. Увидимся l8r, – сказал Pad.

– Да, я тоже, – добавил Electron.

– Ладно, все ОК. L8r, m8ts! – сказал Gandalf.

И затем добавил в типичном для себя стиле:

– Увидимся в тюрьме!

## 6

### На первой полосе The New York Times

*Прочти об этом.*

*Просто очередная невероятная сцена.*

*Не сомневайся в этом.*

**Песня «Read About It», альбом «10, 9, 8, 7, 6, 5, 4, 3, 2, 1» группы Midnight Oil<sup>31</sup>**

---

p122

Lawrence Livermore National Laboratory – Национальная лаборатория имени Лоуренса Ливермора.

<sup>31</sup> Слова и музыка: Rob Hirst / James Moginie / Peter Garrett. © Copyright 1978 Sprint Music. Administered for the World – Warner / Chappell Music Australia Pty Ltd. Used by Permission.

У Pad'a было важное сообщение для австралийских хакеров: парни из компьютерной безопасности подбирались к ним все ближе и ближе. Это было в конце февраля 1990 года, вскоре после того, как Electron и Phoenix поймали Zardoz и потерпели неудачу с Deszip. Pad не стал кричать и размахивать руками, это был не его стиль. Но Electron со всей серьезностью отнесся к важности предупреждения.

– Фен, они знают, что ты был в машине Спафа, – сказал Pad. – Они знают и про другие системы. У них есть твой хэндл.

Юджин Спаффорд был экспертом по компьютерной безопасности того типа, который считал, что может потерять лицо, если в его машину проникнет хакер, а раненый бык – опасный противник.

Люди из безопасности смогли установить связь серии проникновений с хакером, называвшим себя Phoenix, потому что его стиль было легко распознать. Например, если он создавал для себя привилегированный доступ, он всегда сохранял его под одним и тем же именем, в одном и том же месте в компьютере. Дело доходило до того, что он создавал для себя учетные записи под названием Phoenix. Эта было настолько очевидное следование стилю, что проследить его перемещения было проще простого.

В своей обычной сдержанной манере Pad посоветовал сменить стиль хакинга. Он добавил, что австралийцам, может быть, стоит подумать о том, чтобы чуть уменьшить масштабы деятельности. Скрытый смысл послания был крайне серьезен.

– Говорят, что некоторые люди из безопасности связались с австралийскими силовиками, которые «имеют с этим дело», – сказал Pad.

– Они знают мое настоящее имя? – взволнованно спросил Phoenix.

Electron тоже следил за беседой с некоторым беспокойством.

– Не знаю. Я услышал об этом от Shatter'a. Ему не всегда можно верить, но...

Pad попытался смягчить удар, принизив надежность Shatter'a как источника информации. Он не доверял этому хакеру (своему соотечественнику), но у Shatter'a иногда бывали отличные, хотя и загадочные связи. Это была таинственная фигура: казалось, что он стоит одной ногой в хакерском подполье, а другой – в высоких сферах компьютерной безопасности. Время от времени Shatter сливал информацию Pad'у и Gandalf'у, а при случае и австралийцам.

Хотя британские хакеры не всегда принимали в расчет советы Shatter'a, они, тем не менее, всегда находили время, чтобы поговорить с ним. Однажды Electron перехватил e-mail, в котором Pengo обратился к Shatter'у за советом по поводу своего положения после арестов в Германии. У Pengo был запас времени до суда, и он спросил у Shatter'a, не опасно ли ему приехать в Штаты на летние каникулы 1989 года. Shatter спросил у него дату рождения и другие детали. Затем он вернулся с совершенно определенным ответом: ни при каких обстоятельствах Pengo не должен приезжать в США.

Впоследствии появилась информация о том, что официальные лица из Министерства юстиции США всерьез рассматривали возможность тайно уговорить Pengo приехать на американскую территорию, где они смогли бы арестовать его и предать американскому правосудию.

Знал ли об этом Shatter или он просто посоветовал Pengo не ездить в Штаты, опираясь на свой здравый смысл? Никто не мог точно ответить на эти вопросы, но народ стал прислушиваться к тому, что говорил Shatter.

– У Shatter'a явно была полная информация о машине Спафа, – продолжал Pad, – на все сто. Он точно знал, как ты взломал ее. Я не мог поверить. Будь осторожен, если ты все еще занимаешься хакингом, особенно в Инете.

«Инет» был сокращением от «Интернет».

Хакеры в Altos притихли.

– Речь идет не только о тебе, – Pad пытался успокоить австралийцев. – Два американца из секьюрити приезжают в Англию, чтобы постараться нарыть какую-нибудь информацию о том, как зовут Gandalf'a. Ах, да, и о приятеле Gandalf'a, которого вроде бы зовут Патрик.

Pad, конечно, взял свой хэндл от Patrick, или Paddy, но у него было совсем другое имя. Ни один здравомыслящий хакер не станет использовать свое настоящее имя для хэндла. Падди звали его любимого профессора в университете, ирландца, который любил посмеяться. Как и в случае Pad'a, хэндл Pad случайно пересекся с другим значением, когда британский хакер продвинулся в изучении сети X.25. PAD X.25 – это интерфейс между сетью X.25 и модемом или сервером терминала. Точно так же и Gandalf, имя волшебника из «Властелина колец», стало брэндом, под которым выпускались



серверы.

Несмотря на неприятное известие о том, что кольцо вокруг хакеров вот-вот сомкнется, ни один из них не утратил свое плутовское чувство юмора.

– Знаете, – продолжал Pad, – Спафа не было в стране, когда вы взломали его машину.

– Да? А где он был? – спросил Gandalf, присоединившийся к разговору.

– В Европе.

Electron не мог удержаться:

– «Где же Спаф?» – спросил Gandalf, и услышал стук в дверь...

– Ха-ха, – рассмеялся Gandalf.

– &lt;тук-тук&gt;, – продолжал Electron, подыгрывая ему.

– О, здравствуйте, мистер Спаффорд, – подхватил игру Gandalf.

– Привет, меня зовут Юджин и мне немного неловко!

Каждый из хакеров сидел у себя дома на разных концах земного шара и веселился не на шутку.

– Привет, это, наверное, парень по имени Патрик? – вмешался Pad.

– Ну, что ж, мистер Спаффорд, похоже, вы настоящий долбанный идиот, если не залатали ваш FTP! – заявил Gandalf.

– Не говоря уже об ошибке CHFN в Sequent! Смотрите, у вас будут крупные неприятности, – добавил Phoenix.

Он тоже смеялся вместе со всеми, но предупреждение Pad'a очень беспокоило его и он перевел разговор на серьезную тему:

– Слушай, Pad, что еще сказал тебе Shatter? – с тревогой спросил он.

– Немного. Он сказал еще, что расследования служб безопасности могли быть спровоцированы UCB.[p123]

Phoenix побывал в машинах и UCB, и LLNL совсем недавно, и администраторы успели не только заметить его, но и засечь его хэндл. Однажды он проник в dewey.soe.berkeley.edu – известную, как машина Dewey – и с удивлением обнаружил прямо у себя под носом следующее сообщение:

Phoenix,

Убирайся из Дьюи НЕМЕДЛЕННО!

И больше никогда не лезь в машины soe.

Спасибо,

Дэниел Бергер.

Phoenix встал в стойку, когда увидел это предупреждение. Он входил и выходил из системы так много раз, что просто не обращал внимания на слова на входном экране. Затем, с некоторым запозданием, он понял, что послание у входа адресовано именно ему.

Игнорируя предупреждение, он продолжил свой путь в машину Беркли и подобрался к файлам Бергера. Затем он откинулся на спинку стула и стал думать, как ему решить эту проблему. В конце концов он решил оставить админу записку, в которой пообещал навсегда уйти из системы.

Через несколько дней Phoenix вернулся в машину Dewey. В конце концов он взломал систему и сумел получить основной доступ благодаря своей сообразительности. Он заслужил свое право находиться в этом компьютере. Он мог послать администратору записку, чтобы успокоить его, но он не собирался отказываться от доступа в компьютер Беркли лишь потому, что это выводило из себя какого-то Дэниела Бергера.

– Слушай, – продолжал Pad, – я думаю, что народ из UCB хранит в своих компьютерах то, чего там не должно быть. Какие-нибудь секретные штуки.

Секретные военные материалы не полагается хранить в несекретных сетевых компьютерах. Но Pad догадывался, что иногда исследователи нарушают правила и идут по кратчайшему пути, ведь их мысли заняты открытиями, а не правилами безопасности.

– Какая-то часть материала может быть не совсем законной, – сказал Pad своей увлеченной аудитории. – И вот они видят, что кто-то из вас ползает по их системе...

– Дерьмо, – сказал Phoenix.

– Значит, если им ПОКАЖЕТСЯ, что кто-то залез к ним, пытаясь завладеть этими секрета-

ми... – Pad сделал паузу, – вы можете сами догадаться, что произойдет. Они точно захотят прищучить того, кто залез в их машины.

В онлайн воцарилось молчание. Хакеры переваривали слова Pad'a. Pad в Altos всегда держался чуть в стороне от других хакеров, даже от австралийцев, которых он считал приятелями. Эта сдержанность придавала его сообщению еще большую серьезность, и в Altos все это почувствовали.

В конце концов Electron ответил на предупреждение Pad'a комментарием, адресованным непосредственно Phoenix'у:

– Я говорил тебе, что разговоры с секьюрити не принесут ничего, кроме неприятностей.

Electron все больше раздражала некая потребность Phoenix в общении с людьми из секьюрити. По мнению Electron'a, привлекать внимание к собственной персоне – это последнее дело, и он все больше тревожился, наблюдая за тем, как Phoenix ублажает свое эго. Он недвусмысленно намекал на постоянное хвастовство Phoenix'a в Altos, повторяя время от времени: «Я хотел бы, чтобы никто не разговаривал с секьюрити».

Phoenix отвечал Electron'у что-нибудь смиренное вроде: «Ну, я никогда больше не буду разговаривать с парнями из секьюрити, честно».

Electron слышал все это сто раз. Это было то же самое, что верить алкоголику, который клянется никогда больше не притрагиваться к спиртному. Попрощавшись с остальными, Electron отключился. Он не желал больше слушать треп Phoenix'a.

Но другие желали. За сотни километров от них, в специальной комнате, надежно укрытой внутри незаметного здания в Канберре, сержант Майкл Костелло [Michael Costello] и констебль Уильям Апро [William Argo] методично отлавливали каждый электронный выброс, исходящий из телефона Phoenix'a. Полицейские записывали передачу входящих и исходящих данных его компьютера. Затем они пропускали запись через собственные компьютер и модем, создавая текстовый файл, который можно было сохранить и использовать на суде в качестве доказательства.

Оба полицейских приехали на север из Мельбурна, где они работали в Отделе по борьбе с компьютерными преступлениями АФП. Устроившись с ПК и ноутбуком, 1 февраля 1990 года они начали тайную работу по прослушиванию.

АФП впервые осуществляло прослушивание компьютерных данных. Они были очень довольны, что не тратят времени даром, скрупулезно записывая вторжения Electron'a в Беркли, в Техас, в NASA, в десятки других компьютеров по всему миру. Ордер на прослушивание телефона был действителен в течение 60 дней. Этого было вполне достаточно, чтобы получить горы убийственных улик против непомерно честолобивого хакера Realm. Время было на их стороне.

Полицейские работали посменно в рамках операции Dabble.<sup>[p124]</sup> Констебль Апро приходил в подразделение телекоммуникационной разведки АФП в восемь вечера. Ровно через десять часов, в шесть утра, сержант Костелло сменял Апро, который уходил, чтобы хорошенько выспаться. Апро возвращался в восемь вечера и заступал в ночную смену.

Они были на месте все время. 24 часа в сутки. Семь дней в неделю. Выжидая и слушая.

:)

Это было дико смешно. Eric Bloodaxe в Остине, штат Техас, не мог остановиться. У Phoenix'a в Мельбурне болел живот от смеха.

Phoenix любил говорить по телефону. Он часто звонил Eric'у, порой каждый день, и они болтали часами. Phoenix не волновался о деньгах, ибо не платил за разговоры. Звонок появлялся в счете какого-нибудь несчастного, которому и приходилось разбираться с телефонной компанией.

Иногда Eric беспокоился о том, как Phoenix'у удастся не запутаться в этой мешанине международных звонков. Не то чтобы ему не нравилось разговаривать с австралийцем – это была умора! Но все же беспокойство гнезилось где-то в глубине его сознания. Несколько раз он спрашивал Phoenix'a об этом.

– Расслабься, компания AT&T не в Австралии, – обычно говорил Phoenix. – Они ничего мне не сделают.

И Eric оставил все как есть.

Сам Eric не осмеливался звонить Phoenix'у, особенно после того, как Секретная служба нанесла ему скромный визит. На рассвете 1 марта 1990 года они ворвались в его комнату с оружием наизготовку. Агенты искали всюду, перевернув дом студента вверх дном, но не нашли ничего криминального. Они забрали клавиатуру Eric'a за \$59 и дешевый модем на 300 бод, но им не достался его главный компьютер, потому что Eric знал, что они придут.

Секретная служба наложила арест на его университетские записи, о чем Eric услышал еще до обыска. Поэтому когда Секретная служба появилась у него дома, там не было никакого ценного оборудования. Его не было уже несколько недель, но Eric'у они показались годами. Хакер обнаружил у себя симптомы ломки, поэтому ему пришлось купить самые дешевые компьютер и модем, какие он только смог найти, чтобы выйти из положения.

Это оборудование и было единственной компьютерной техникой, которую обнаружила Секретная служба, и это не доставило им удовлетворения. Но без улик их руки были связаны. Поэтому обвинения против Eric'a так и не были предъявлены.

Тем не менее Eric считал, что его, скорее всего, прослушивают. Меньше всего он хотел, чтобы номер Phoenix'a появился в его телефонном счете. Поэтому он предоставил австралийцу звонить ему, что Phoenix и делал. Они часто говорили часами, когда Eric работал по ночам. Это была несложная работа – просто менять ленты на разных компьютерах и следить, чтобы они не перепутались. В самый раз для студента. У Eric'a оставалась уйма свободного времени.

Eric постоянно напоминал Phoenix'у, что его телефон мог прослушиваться, но Phoenix только смеялся.

– Брось, дружище, не переживай. Что они могут сделать? Прийти и арестовать меня?

;) )

Первая полоса *The New York Times*, 21 марта 1990 года: «Позвонивший в редакцию говорит, что он взламывает компьютерные барьеры, чтобы посрамить экспертов», автор Джон Маркофф.

По правде говоря, это была не передовая – статья размещалась в нижней половине страницы. Но это все же была первая полоса, на которую читатели сразу обращают внимание.

Phoenix'a распирало от гордости. Он попал на первую страницу *The New York Times*.

«Этот человек сказал только, что он австралиец по имени Дэйв», – говорилось в статье. Phoenix ухмыльнулся. Когда-то он использовал псевдоним Dave Lissek. Конечно, он был не единственным, кто пользовался именем Дэйв. Когда Eric впервые познакомился с австралийцами в Altos, он удивился тому, что они все называли себя Дэйв. «Я Дэйв, он Дэйв, мы все Дэйвы», – сказали они ему. «Так проще», – говорили они.

Статья рассказывала, что этот «Дэйв» успешно атаковал машины Спафа и Столла, и что Смит-сонианская астрономическая обсерватория в Гарвардском университете, где сейчас работал Столл, была вынуждена отключить свои компьютеры от Интернета в результате его вторжения. Маркофф даже включил в статью историю про «яйцом по морде», которую поведал ему Phoenix.

Phoenix был счастлив, что сумел посадить в калошу Клиффи Столла. Эта статья покажет его в истинном свете. Как прекрасно видеть, что о тебе пишут такие слова. Он сделал это. Это *он* был там, черным по белому, и весь мир мог видеть его. Это он перехитрил самого знаменитого на свете охотника за хакерами и опозорил его на первой странице самой престижной газеты Америки.

Этот Маркофф написал и про его приключения в системе Спафа! Phoenix сиял от счастья. К тому же Маркофф процитировал слова Дэйва на эту тему: «Абонент сказал: „Раньше секьюрити преследовали хакеров. Теперь хакеры будут преследовать секьюрити“».

Маркофф продолжал: «Среди организаций, где, вероятно, побывал хакер, Национальная лаборатория в Лос-Аламосе, Гарвард, Digital Equipment Corporation, Бостонский и Техасский университеты». Да, этот список был похож на правду. Во всяком случае, для австралийцев как группы. Phoenix не управлял ими и даже не проникал в некоторые из них, но он был счастлив получить кредит доверия в *Times*.

В этот день у Phoenix'a был праздник.

Electron же, напротив, был в ярости. Как Phoenix может быть таким тупым? Он знал, что эго Phoenix'a беспредельно, что он слишком много болтает, а его хвастовство только растет на волне стремительного успеха австралийских хакеров. Electron прекрасно знал все это, но все же он не мог до конца поверить в то, что Phoenix зашел так далеко, чтобы горделиво гарцевать, словно дрессированный пони, на арене *The New York Times*.

Electron с отвращением думал о том, что он *сотрудничал* с Phoenix'ом. Он никогда до конца

не доверял ему – и его предчувствия оправдались. Но он часами проводил с ним на телефоне, и большая часть информации текла в одном направлении. Кроме того, Phoenix не только проявил несдержанность в общении с репортером, он хвастал вещами, которые сделал он, Electron! Если Phoenix'у надо было поговорить – хотя стоило бы попридержаться язык, – можно хотя бы быть честным, рассказывая только о системах, в которых он побывал.

Electron постоянно пытался воздействовать на Phoenix'а. Electron внушал ему, чтобы тот прекратил общаться с секьюрити. Он требовал осторожности и сдержанности. Доходило даже до того, что он всякий раз потихоньку уходил, когда Phoenix выдвигал одну из своих сумасшедших идей насчет того, как показать свою удалость шишкам из безопасности. Electron делал это в надежде, что Phoenix поймет намек. Может быть, он из тех, кто не воспринимает прямого давления, но прислушивается, если ему шепчут на ухо. Увы. Phoenix оказался слишком толстокожим и для того, и для другого.

Теперь стоило забыть о хакинге и об Интернете, само собой, на несколько недель, если не месяцев. Не было никаких шансов, что власти Австралии пропустят по невнимательности статью на первой странице *The New York Times*. Американцы не оставят их в покое. В своем эгоистичном порыве высокомерия Phoenix испортил вечеринку всем остальным.

Electron отключил свой модем и отнес его отцу. Во время экзаменов он часто просил отца спрятать его. Сам он не мог заставить себя держаться от модема на расстоянии, а другого способа не включить его просто не существовало. Его отец стал специалистом по этой игре в прятки, но обычно Electron'у удавалось найти модем в течение нескольких дней. Он переворачивал весь дом и в конце концов появлялся с видом триумфатора, держа его над головой. Даже когда отец стал прятать его вне дома, это лишь ненадолго отдаляло неизбежное.

Но на этот раз Electron поклялся, что перестанет заниматься хакингом, пока не кончится буря, – он должен был это сделать. Итак, он отдал модем отцу со строжайшими инструкциями, а затем попытался развлечься, занявшись чисткой своего жесткого диска и дискет. Его хакерские файлы тоже должны были исчезнуть. Слишком явное доказательство его деятельности. Он стер некоторые файлы, другие перенес на дискеты и попросил приятеля взять их на хранение. Уничтожая файлы, Electron испытал настоящее горе, но другого пути не было. Phoenix загнал его в угол.

Дрожа от возбуждения, Phoenix позвонил Electron'у солнечным мартовским днем.

:)

– Угадай, что? – Phoenix на другом конце провода захлебывался от счастья. – Мы попали в вечерние новости по всей Америке!

– Угу, – равнодушно ответил Electron.

– Я не шучу! Еще нас целый день показывают в новостях по кабельному. Я звонил Eric'у, он сказал мне это.

– Ммм, – сказал Electron.

– Знаешь, мы все-таки сделали кучу реальных вещей. Типа Гарварда. Мы же вошли там в каждую систему. Это было то, что нужно. Гарвард дал нам *славу*, в которой мы нуждались.

Electron не мог поверить своим ушам. Ему не нужна была никакая слава – и уж, конечно, он не нуждался в том, чтобы его арестовали. Разговор – как и сам Phoenix – начинал по-настоящему раздражать его.

– Эй, они знают и твое имя, – скромно сказал Phoenix.

Это возымело реакцию. Electron едва не взорвался.

– Ха-ха! Шутка! – Phoenix почти кричал. – Не волнуйся. Они не назвали ни одного имени!

– Хорошо, – коротко ответил Electron. Его раздражение понемногу закипало.

– Как ты думаешь, мы сможем попасть на обложку *Time* или *Newsweek*?

Ну что ты будешь делать! Phoenix когда-нибудь уймется? Как будто было недостаточно появиться в шестичасовых национальных новостях в стране, переполненной фанатичными силовыми структурами? Ему мало было первой страницы *The New York Times*? Теперь ему понадобились и еженедельные журналы!

– Ну что, как, сможем? – нетерпеливо спросил Phoenix.

– Нет, – ответил Electron.

– Нет? Думаешь, мы не сможем? – голос Phoenix'а звучал разочарованно.

– Нет.

– А я требую этого! – со смехом сказал Phoenix. – Нам нужна обложка *Newsweek*, не меньше. Я

вот думаю, какая серьезная контора смогла бы нам в этом помочь? – продолжал он более серьезно.

– Да, ОК, давай, – ответил Electron, снова уходя в сторону. А про себя он думал: «Phoenix, какой же ты придурок. Ты что, не видишь сигналов тревоги? Предупреждение Pad'a, все эти аресты в Штатах, сообщения о том, что американцы охотятся за англичанами. После всех этих репортажей в новостях, которыми ты так гордишься, начальство всего мира вызовет на ковер своих компьютерных менеджеров и намылит им шею насчет своей компьютерной безопасности».

Неуемные хакеры глубоко оскорбили индустрию компьютерной безопасности, вызвав ее противодействие. В свете последних событий некоторые люди из безопасности увидели возможность поднять свой собственный престиж. Эксперты постоянно общались с правоохранительными органами, которые теперь свободно обменивались информацией через границы и быстро находили общий язык. Конспираторы всемирного электронного подполья оказались на грани тотального поражения.

– Мы должны снова навестить Спафа, – вызвался Phoenix.

– Большинству народу наплевать, кто такой Юджин Спаффорд, они его и знать не знают, – сказал Electron, пытаясь усмирить разбушевавшийся энтузиазм Phoenix'a. Electron всегда был рад утереть нос авторитетам, но это был не тот случай.

– Представь, как было бы весело в суде. Адвокат вызывает Спафа и говорит: «Итак, мистер Спаффорд, действительно ли вы являетесь всемирно признанным экспертом в вопросах компьютерной безопасности?» И когда он говорит: «Да», я вскакиваю и начинаю: «Возражаю, ваша честь, этот тип не смыслит ни хрена, потому что я взломал его машину с закрытыми глазами!»

– Ммм.

– Эй, если нас не арестуют в течение двух следующих недель, это будет чудо, – довольно продолжал Phoenix.

– Надеюсь, что нет.

– Вот будет веселье! – с издевкой крикнул Phoenix. – Нас арестуют! Нас арестуют!

У Electron'a отвалилась челюсть. Phoenix сошел с ума. Только дебил может так себя вести. Пробормотав что-то о том, как он устал, Electron попрощался и положил трубку.

:)

Без десяти шесть утра 2 апреля 1990 года Electron выполз из постели и поплелся в ванную. Не успел он закончить свой туалет, как вдруг погас свет.

Как странно. Electron вытаращил глаза в тусклом утреннем свете. Он вернулся в свою комнату и начал натягивать джинсы, чтобы пойти и выяснить, в чем дело.

Внезапно распахнулось окно и в комнату устремились два человека в гражданской одежде с криком: «ЛЕЖАТЬ!»

Что это за люди? Полуголый Electron стоял посреди комнаты, остолбенев от изумления. Он подозревал, что полиция может нагрянуть к нему в гости, но разве им не положено носить форму? Разве они не должны представиться?

Двое схватили Electron'a, швырнули его лицом на пол и завели его руки за спину. Они сдавили его запястья наручниками – очень больно, – содрав ему кожу. Затем один из них пнул его в живот.

– В доме есть огнестрельное оружие? – спросил другой.

Electron не ответил, потому что не мог дышать. От удара у него перехватило дыхание. Он почувствовал, что его поднимают с пола и сажают на стул. Повсюду зажегся свет, и он увидел шесть или семь человек в прихожей. Очевидно, они попали в дом другим путем. У людей в прихожей были нагрудники с тремя ярко выделявшимися большими буквами: АФР.

Как только Electron понемногу собрался с мыслями, он понял, почему копы спросили его об оружии. Однажды в разговоре с Phoenix'ом он пошутил, что практикуется с отцовским пистолетом 22-го калибра, чтобы оказать федералам достойную встречу. Должно быть, федералы прослушивали его телефон.

Пока отец Electron'a разговаривал с одним из полицейских в другой комнате и читал ордер на арест, Electron видел, как полиция упаковывает его компьютерное оборудование – оно стоило что-то около \$3000 – и выносит из дома. Единственное, что они не нашли, это модем. Отец приобрел такой опыт, постоянно пряча модем от сына, что даже Австралийская федеральная полиция не смогла его отыскать.

Несколько других копов начали обыск в комнате Electron'a. Учитывая ее состояние, это было нелегко. Пол был покрыт толстым слоем всякого хлама. Наполовину разорванные постеры рок-групп, масса бумаг с небрежно нацарапанными паролями и NUA, ручки, грязные и чистые фут-

болки, джинсы, кеды, книги по бухгалтерскому учету, кассеты, журналы, немытые чашки. К тому времени как полиция тщательно просеяла все это барахло, комната стала намного чище, чем была в начале обыска. Когда они перешли в другую комнату, продолжая обыск, Electron нагнулся и поднял один из постеров, упавших на пол. Это была полицейская «Инструкция по идентификации наркоманов» – подарок отцовского друга, – и на ней прямо посередине появился четкий отпечаток подошвы АФП. Теперь это была коллекционная вещь. Electron улыбнулся про себя и тщательно спрятал плакат.

Когда он вышел в гостиную, он увидел пару полицейских с лопатами и снова едва сдержал смех. Как-то он сказал Phoenix'у, что его самые ценные дискеты закопаны на заднем дворе. Теперь полиция перекопает там все в поисках улики, уничтоженных несколько дней назад. Это было очень забавно.

Полиция нашла в доме Electron'а очень немного доказательств его хакерской деятельности, но это было неважно. У них уже было почти все, что нужно.

:)

Немного позже копы посадили двадцатилетнего Electron'а в обыкновенную, а не полицейскую машину и повезли его на допрос во впечатляющее здание штаб-квартиры АФП на Лэтроуб-стрит, 383.

Во второй половине дня, когда Electron'у позволили ненадолго отдохнуть от бесконечных вопросов, он вышел в вестибюль. В другом конце вестибюля в сопровождении полицейских показались Phoenix, восемнадцати лет от роду, с мальчишеским лицом, и приятель по Realm, двадцатидвухлетний Nom. Они были слишком далеко, чтобы можно было перекинуться с ними словечком, но Electron улыбнулся. Nom выглядел взволнованным. Phoenix казался недовольным.

Electron был слишком обескуражен, чтобы потребовать адвоката. Да и какой в этом смысл? Совершенно очевидно, что они прослушивали его телефон. Они также показали ему лог-файлы из Мельбурнского университета, явно указывающие на его телефонный номер. Electron'у казалось, что игра закончена и он может спокойно рассказать им все – во всяком случае, все, что он говорил Phoenix'у по телефону.

Допросы вели двое. Главным был детектив констебль Гленн Пробстл [Glenn Proebstl]. Electron подумал, что парню не повезло с фамилией. [\[p125\]](#) Пробстлу помогала констебль Наташа Эллиот [Natasha Elliott], которая время от времени задавала несколько вопросов в конце допросов, но в основном просто присутствовала. Хотя Electron решил правдиво отвечать на вопросы, иногда он с трудом понимал, что они хотят у него спросить, – следователи не разбирались в компьютерах.

Electron'у пришлось начать с азов. Он объяснил, что такое команда FINGER [\[p126\]](#) – нужно было набрать на клавиатуре слово finger, а затем имя пользователя, и компьютер выдавал базовую информацию об имени пользователя и другие детали.

– А какая методика применяется потом... finger... значит, обычно... какова обычная команда после этого, чтобы применить и вывести пароль? – констебль Эллиот наконец завершила свою извилистую попытку задать вопрос.

Единственная проблема заключалась в том, что Electron не имел никакого понятия, о чем она говорит.

– Ну, я думаю, никакой команды нет. Я хочу сказать, что finger используется не для этого...

– Ясно, – констебль Эллиот взяла инициативу в свои руки. – Скажите, вы раньше использовали эту систему?

– Ммм, какую систему?

Electron так долго объяснял им принципы команд, что забыл, о чем они говорили, – о том, как он взломал компьютер Ливерморской лаборатории или о каком-то другом сайте.

– Finger... Систему Finger?

Что? Electron не был уверен, правильно ли он понял вопрос. Finger – это команда, а не система.

– О, да, – ответил он.

p125

Фамилия констебля – Пробстл – созвучна английскому «probe stool» (анализ кала).

p126

Палец (англ.).

Допрос продолжался в том же духе, неуклюже пробираясь сквозь темный лес компьютерных технологий, в которых Electron понимал больше, чем оба копа, вместе взятые. В конце концов детектив Пробстл спросил у Electron'a:

– Вы можете сказать мне своими словами, чем вас привлекает проникновение в компьютеры на других континентах?

– Ну, это делалось не ради выгоды или чего-то в этом роде, – спокойно сказал Electron.

Это был необычный вопрос, и на него было трудно ответить. Не потому, что он не знал ответа. Просто такие вещи очень трудно объяснить тому, кто никогда не взламывал компьютеров.

– Это просто удовольствие от проникновения в систему. Я имею в виду, что когда ты занимаешься этим, тебе очень часто бывает скучно, и даже если у тебя есть постоянный доступ к системе, ты можешь больше никогда не вернуться в нее. Потому что как только ты проник в нее – это уже победа, и тебе становится наплевать на систему, – продолжал Electron с трудом. – Это вопрос соревнования, ты пытаешься сделать какие-то вещи, то, что другие хотят, но не могут. Я говорю о том, что это вопрос самолюбия. Ты понимаешь, что можешь делать такое, чего не могут другие, и это заставляет тебя делать то, что другие люди пробуют, а у них не выходит.

Еще несколько вопросов, и долгий допрос наконец закончился. Полицейские отвезли Electron'a в полицейский участок Фицрой.

Он догадался, что это было ближайшее место, где есть мировой судья, который мог выполнить процедуру освобождения под залог в такое позднее время.

Напротив уродливого кирпичного здания Electron заметил группу людей на тротуаре в сумеречном свете. Как только полицейская машина подъехала к зданию, группа пришла в бешеное движение, суетливо роясь в своих сумках, перекинутых через плечо, доставая блокноты и ручки, вытаскивая большие микрофоны с мохнатыми набалдашниками, включая подсветку телекамер.

О нет! Electron совершенно не был готов к этому. В сопровождении полиции Electron вылез из машины и потерялся в ослепительном свете вспышек фотоаппаратов и прожекторов телекамер. Хакер попытался не обращать на них внимания, двигаясь так быстро, насколько позволял его эскорт. Звукооператоры и журналисты мчались за ним по пятам, не сбавляя темпа, а телеоператоры и фотографы маячили впереди. Наконец, он оказался в спасительном караульном помещении.

Сначала была всякая бумажная волокита, затем его отвели к мировому судье. Перебирая бумаги Electron'a, судья произнес перед ним речь о том, как часто обвиняемые утверждают, что они были избиты полицейскими при задержании. Сидя в грязноватой комнате для свиданий, Electron был слегка сбит с толку таким неожиданным отклонением от темы. Но следующий вопрос судьи расставил все по местам:

– Можете ли вы пожаловаться на дурное обращение со стороны полиции, о котором нам следует знать сейчас?

Electron подумал о зверском пинке в живот, как он потом корчился на полу в своей комнате. Он поднял голову и увидел, что констебль Пробстл смотрит ему прямо в глаза. На лице полицейского промелькнула легкая усмешка.

– Нет, – ответил Electron.

Судья завел новый монолог, показавшийся Electron'у еще более странным. В одной из камер участка находился еще один обвиняемый, опасный преступник. Он был болен, и судья знал о его болезни. Мировой судья был готов посадить Electron'a вместе с ним.

Что это – желание припугнуть его или проявление садизма? Electron не знал, что думать, но ему не пришлось долго ломать голову. Судья согласился на залог. Отец Electron'a приехал в участок, забрал сына и подписал бумаги на \$1000, которые пришлось бы уплатить, если бы Electron смылся из города. Вечером в тот же день Electron услышал свое имя в вечерних новостях.

Почти не выходя из дома в течение нескольких следующих недель, Electron пытался примириться с мыслью о том, что ему придется навсегда завязать с хакингом. У него остался модем, но не было компьютера. Даже если бы у него и была машина, он ясно понимал, что даже думать о хакинге было опасно.

Поэтому он пристрастился к наркотикам.

:)

Отец Electron'a тянул до последнего предела, до марта 1991 года, не желая ложиться в больницу. Он знал, что из палаты он больше не сможет выйти.

Нужно было столько сделать перед последним путешествием, успеть позаботиться о многих

вещах. Дом, волокита со страховкой, завещание, похороны, инструкции другу семьи, которая обещала после его смерти присматривать за обоими детьми. И конечно, сами дети.

Он смотрел на них, и его охватывала тревога. Несмотря на свои 21 и 19 лет, они все еще нуждались в заботе. Он понимал, что антиавторитарные настроения Electron'а и эмоциональная замкнутость его сестры так и останутся нерешенными проблемами после его смерти. По мере того, как болезнь прогрессировала, отец Electron'а объяснил обоим детям, как они ему дороги. В прошлом он сам был эмоционально замкнут, но у него оставалось слишком мало времени, и он хотел, чтобы между ним и детьми не оставалось неясностей.

Но когда у Electron'а появились проблемы с полицией, у отца опустились руки. Время от времени Electron рассказывал отцу о своих хакерских подвигах, как правило, в тех случаях, когда ему удавалось то, что он считал очень большой удачей. Точка зрения отца оставалась неизменной. Он говорил сыну, что хакинг – это незаконно, и полиция в конце концов поймает его. Тогда Electron'у придется самостоятельно решать свои проблемы. Он не запрещал сыну заниматься хакингом и не читал ему нотаций. Он просто решил, что его сын достаточно взрослый, чтобы сделать свой собственный выбор и жить с его последствиями.

Верный своему слову, отец Electron'а никак не проявил сочувствия к сложному положению своего сына после налета и обыска полиции. Он был равнодушен к происходящему, говоря лишь одно: «Я предупреждал тебя о том, что может случиться нечто подобное, так что теперь разбирайся сам».

В течение года дело Electron'а понемногу продвигалось, в то же время он продолжал свою учебу в университете на бухгалтерском отделении. В марте 1991 года ему предстояло судебное разбирательство, и он должен был решить, как построить свою защиту.

Ему грозили пятнадцать обвинений, большинство из них было связано с нелегальным доступом в компьютеры США и Австралии. В некоторых из обвинений речь шла о тяжком преступлении – доступе к материалам коммерческого характера. В каждом из этих случаев, по словам DPP, [\[p127\]](#) Electron изменил и уничтожил данные. Это случилось из-за того, что Electron пробивал для себя черные ходы: никаких файлов он не повреждал. Серьезных доказательств хватало с избытком: перехват данных и прослушивание телефона Phoenix'а, когда они с Electron'ом разговаривали о хакинге; собственные лог-файлы Electron'а, отметившие его похождения в системе Мельбурнского университета, прослеженные до его телефона; наконец, личное признание Electron'а полиции.

Это был первый большой хакерский процесс в Австралии после принятия нового закона. Это был пробный шар – показательный суд над австралийскими хакерами – и офис DPP ретиво взялся за дело, которое насчитывало семнадцать томов доказательств и 25 000 страниц. Королевский прокурор Лайза Уэст [Lisa West] намеревалась воспользоваться показаниями двадцати экспертов-свидетелей из Европы, Австралии и США.

У этих свидетелей были наготове интересные истории об австралийских хакерах, посеявших хаос в компьютерных системах по всему миру. Phoenix случайно уничтожил инвентарный список активов одной компании в Техасе – единственную существующую копию файла, если верить Execusom Systems Corporation. Хакеры также свели с ума секьюрити в Военно-морской исследовательской лаборатории США. Они похвалялись своими подвигами на страницах *The New York Times*. Из-за них NASA отключило свои компьютеры на 24 часа.

Детектив АФП сержант Кен Дэй [Ken Day] пролетел полмира, чтобы получить свидетельские показания компьютерного менеджера Шэрон Бискенис из Лэнгли, NASA, – того администратора, которого Phoenix случайно выставил из ее собственной системы, пытаясь завладеть Zardoz. Бискенис была безмерно рада оказать содействие и 24 июля 1990 года в Вирджинии подтвердила свои показания, которые засвидетельствовал Дэй. В показаниях говорилось, что в результате вторжения хакеров 22 февраля 1990 года «вся компьютерная сеть NASA на 24 часа была лишена внешних связей с остальным миром».

Словом, Electron думал о том, что у него нет особенных шансов выиграть слушание. Nom, похоже, разделял его настроение. Ему было предъявлено два обвинения; оба «имели явное отношение» к нелегальным действиям Phoenix'а: одно из них базировалось на нелегальном проникновении Phoenix'а в Лэнгли, NASA, другое было связано с доступом в CSIRO к файлу Zardoz. Nom тоже не собирался сопротивляться, хотя на его решение, несомненно, повлиял отказ бесплатной юридической



консультации Legal Aid предоставить ему адвоката на время суда.

6 марта 1991 года магистрат <sup>[p128]</sup> Роберт Лэнгтон [Robert Langton] решил, что Nom и Electron предстанут перед окружным судом штата Виктория.

Но Phoenix не разделял точку зрения своих приятелей-хакеров. Опираясь на финансовую помощь семьи, он решил попытаться оспорить дело. Он не собирался нести прокурору повинную на блюде с голубой каемочкой. Им придется бороться с ним шаг за шагом, от разбирательства к разбирательству. Его защитник, Фелисити Хэмпл [Felicity Hampel], заявила, что на основании существующих законов суд должен отозвать 47 из 48 обвинений против ее клиента. Оставалось единственное обвинение – проникновение в машину CSIRO с целью похитить Zardoz, но оно было связано с хакерской деятельностью за пределами Австралии. Как мог австралийский суд требовать возмездия от лица компьютера из Техаса?

Внутренне Phoenix больше волновался из-за того, что его могут выдать Соединенным Штатам, нежели из-за австралийского суда, но он явился на слушания, настроенный крайне воинственно. Процесс стал показательным во многих отношениях – это было не только первое в Австралии разбирательство хакерских преступлений, но и первая попытка хакера отстоять свое дело в суде.

Обвинение согласилось оставить только один из сорока восьми пунктов, тем более что он был двойным, но это отступление стало для Phoenix’a пирровой победой. После двухдневных судебных слушаний магистрат Джон Уилкинсон [John Wilkinson] решил, что аргументы Хэмпл не выдерживают критики, и 14 августа 1991 года направил дело Phoenix’a в окружной суд.

В марте, к началу процесса над Electron’ом, его отец доживал свои последние дни. Рак желудка похож на американские горки – бывают и плохие, и хорошие дни. Но скоро остались только плохие дни, и они становились все хуже. В последний день марта врачи сказали, что времени больше нет, что ему надо немедленно лечь в больницу. Он наотрез отказался ехать, оспаривая их советы, подвергая сомнению их авторитет. Врачи поторапливали его. Он протестовал. Но все же они настояли.

Electron и его сестра провели с отцом весь этот день и следующий тоже. У отца были и другие посетители, желавшие подбодрить его. Например, его брат, который горячо настаивал на том, чтобы отец Electron’a перед смертью принял Иисуса Христа как спасителя. Иначе он сгорит в аду. Electron смотрел на дядю, не веря своим ушам. Он кипел оттого, что отец вынужден мириться с подобной чепухой на смертном одре. Тем не менее, Electron решил не проявлять своих чувств. Стараясь держаться в стороне от случайных взглядов, он обрел мир у постели отца.

Но, возможно, страстные слова брата оказали благотворное воздействие, потому что отец Electron’a завел речь о приготовлениях к похоронам и вдруг странным образом оговорился. Он сказал «свадьба» вместо «похороны» и сразу же замолчал, осознав свою ошибку. Взглянув на сложное плетение обручального кольца, которое он продолжал носить после смерти жены, отец Electron’a улыбнулся, преодолевая боль, и сказал: «Думаю, в каком-то смысле это будет похоже на свадьбу».

Electron с сестрой приходили в больницу к отцу ежедневно еще четыре дня.

На пятый день в шесть часов утра в их доме зазвонил телефон. Это была та женщина, друг семьи, которую отец попросил присматривать за ними. Их отец был очень слаб, он находился на пороге смерти.

Когда Electron с сестрой приехали в больницу, они обо всем догадались по лицу медсестры. Слишком поздно. Отец умер десять минут назад. Electron не выдержал и зарыдал. Он обнял сестру – на какое-то время она стала похожа на человека. Отвозя их домой, добрая знакомая остановилась и купила им автоответчик.

– Вам это понадобится, когда все подряд начнут названивать вам, – сказала она. – Какое-то время вы не захотите ни с кем разговаривать.

;) )

В 1990 году, через несколько месяцев после ареста, Electron начал постоянно курить марихуану. Сначала это было рядовым развлечением, как и для многих студентов университета. Забегали друзья, у них случайно оказывалось с собой несколько косяков, все курили и отправлялись в город на

поиски ночных приключений. Пока Electron серьезно занимался хакингом, он никогда не курил. Было слишком важно сохранять ясную голову. Кроме того, кайф от хакерских вылазок был в сто раз сильнее, чем любой наркотик.

Когда Phoenix появился на первой странице *The New York Times*, Electron завязал с хакингом. Даже если бы он и хотел вернуться к нему, у него не было возможности после того, как полицейские конфисковали его единственный компьютер. Electron поймал себя на том, что он всячески старается отвлечься от ухудшающегося состояния отца и пустоты, которая образовалась в его жизни после прекращения хакинга. Бухгалтерский курс в этом никак не мог помочь. Учеба всегда была довольно бессмысленным занятием, а сейчас тем более.

Курение травы и ночные прогулки заполнили пустоту. Заполнили с лихвой. Он говорил себе, что, помимо всего прочего, гораздо меньше шансов, что его поймают за курением травы в доме друзей, чем за хакингом в его собственной комнате. Привычка постепенно перерастала в потребность. Вскоре он стал курить и дома. Новые друзья начали заходить постоянно, и наркотики всегда были у них при себе – уже не случайно и совсем не для забавы.

У Electron'а с сестрой остался родительский дом и достаточно денег, чтобы ни в чем не нуждаться. Electron тратил свою долю на новое хобби. Пара новых друзей Electron'а задержались у него на несколько месяцев. Его сестре очень не нравилось, что они торгуют наркотиками прямо в доме. Electron не обращал никакого внимания на то, что творилось в доме. Он просто сидел у себя в комнате, слушал музыку, курил траву, глотал таблетки и тупо смотрел на стены.

Наушники блокировали все, что происходило в доме, а главное – то, что происходило в его голове. Billy Bragg, Faith No More, Cosmic Psychos, Celibate Rifles, Jane's Addiction, The Sex Pistols, The Ramones. Музыка дала Electron'у ориентир, воображаемую световую точку на лбу, где он мог сфокусировать свое внимание. Отгоняя все более странные мысли, копошащиеся в его голове.

Его отец жив. Он был уверен в этом. Он *знал* это, как знал, что завтра взойдет солнце. Но ведь он видел своего отца мертвым в больничной койке. Это не имело никакого смысла.

Он снова затянулся, медленно подошел к кровати, улегся, осторожно надел наушники и постарался сконцентрироваться на том, что говорили в его голове Red Hot Chili Peppers. Когда этого было недостаточно, он пробирался в гостиную к своим новым друзьям – друзьям с волшебными таблетками. И снова восемь часов без всяких волнений и странных мыслей.

Вскоре люди тоже стали вести себя странно. Они говорили Electron'у разные вещи, но он с трудом их понимал. Его сестра, например, достала картонку с молоком из холодильника и, понюхав ее, сказала: «Молоко прокисло». Но Electron не был уверен в том, что именно она имела в виду. Он настороженно смотрел на нее. Может быть, она хотела сказать ему что-то другое, про пауков. Надоить из пауков яду.

Когда его посещали подобные мысли, они беспокоили его, надоедливые и прилипчивые, как неприятный запах. Поэтому он медленно возвращался назад, в безопасность своей комнаты, и слушал песни Henry Rollins.

После нескольких месяцев такого туманного состояния полного забвения однажды утром Electron очнулся и обнаружил в своей комнате Группу кризисной оценки – мобильную психиатрическую бригаду. Они задали ему кучу вопросов, а затем попытались скормить ему маленькие голубые таблетки. Electron не хотел принимать их. А вдруг это плацебо? Он был уверен, что это так. Или это что-нибудь ужасное?

В конце концов врачи скорой убедили Electron'а принять таблетку стелазина. Как только они уехали, с Electron'ом начало твориться что-то ужасное. Его глаза бесконтрольно закатились. Его голова склонилась влево, а рот открылся очень широко. Как Electron ни старался, ему не удалось ни закрыть рот, ни выпрямить голову. Он посмотрел на себя в зеркало, и его охватила паника. Он выглядел как персонаж фильма ужасов.

Его новые соседи по дому отреагировали на такое странное поведение очень своеобразно – они попытались провести с Electron'ом сеанс психоанализа. Само собой, это принесло больше вреда, чем пользы. Они говорили о нем, словно он вообще отсутствовал. Electron чувствовал себя призраком и, взволнованный и встревоженный, сказал своим приятелям, что собирается покончить с собой. Кто-то из них снова вызвал психиатрическую бригаду. На этот раз они не хотели уезжать, пока Electron не сможет им гарантировать, что не будет пытаться совершить самоубийство.

Electron не мог этого сделать. Тогда они забрали его.

В стенах закрытой психиатрической палаты больницы Пленти (сейчас она называется NEMPS), Electron'у казалось, что, хотя он и сошел с ума, на самом деле находится вовсе не в палате психушки. Это место просто было похоже на нее. Его отец позаботился об этом.

Electron не верил ни одному слову из того, что ему здесь говорили. Все вранье. Они говорили одно, но имели в виду совсем другое.

И он мог это доказать. Electron прочел на стене список пациентов и обнаружил там одного по фамилии Танас. У этого имени было двойное значение. Это была анаграмма слова «Санта».

Но Санта-Клаус – миф, поэтому фамилия Танас в больничном списке стала доказательством того, что он не должен верить никому и ничему.

Чаще всего Electron съедал свой обед молча, стараясь не обращать внимания на пациентов, добровольно или принудительно оказавшихся в этой столовой. Однажды за обедом за стол Electron'а подсел незнакомец и начал с ним разговор. Electron'у было невероятно мучительно разговаривать с другими людьми, и он очень хотел, чтобы незнакомец ушел.

Незнакомец заговорил о том, какие отличные таблетки в больнице.

– Ммм, – сказал Electron, – когда-то я съел море колес.

– Море – это сколько?

– Я потратил на наркоту \$28 000 за четыре месяца.

– Ого! – сказал незнакомец с восхищением. – Но ты зря отдал за это деньги. Колеса всегда можно получить бесплатно. Я так делаю.

– Да? – спросил слегка шокированный Electron.

– Конечно. Постоянно, – важно ответил незнакомец. – Какие проблемы? Смотри.

Он спокойно положил вилку на поднос, медленно встал и начал вопить во всю мощь своих легких. Он неистово размахивал руками и выкрикивал оскорбления в адрес других пациентов.

С поста прибежали две медсестры. Одна из них попыталась успокоить незнакомца, в то время как другая быстро отсыпала горсть разных таблеток и принесла стакан воды. Незнакомец проглотил таблетки, сделал большой глоток воды и спокойно сел на место. Сестры ушли, не переставая оглядываться.

– Видал? – сказал незнакомец. – Ладно, я, пожалуй, пойду, пока колеса не начали действовать. Пока.

Electron изумленно смотрел, как незнакомец подхватил свою сумку, прошел через столовую и скрылся за дверью психиатрического отделения.

:)

Через месяц психиатры неохотно позволили Electron'у покинуть больницу с тем условием, что он поживет у своей бабушки по материнской линии в Квинсленде. Ему было велено регулярно посещать психиатра. В начале своего пребывания в Квинсленде он верил, что он Иисус Христос. Но это продлилось недолго. Через две недели терпеливого ожидания и наблюдения за признаками неминуемого конца света с абсолютной уверенностью во втором пришествии, он решил, что на самом деле он – воплощение Будды.

В конце февраля 1992 года после трех месяцев пребывания на севере страны, Electron вернулся в Мельбурн к учебе в университете с целым мешком лекарств. Прозак, транквилизаторы, литий. Повседневная рутина некоторое время текла спокойно. Шесть таблеток прозака – две утром, две в полдень и две вечером. Плюс еще один антидепрессант перед сном. Кроме того, таблетки против побочных эффектов приема антидепрессантов – непроизвольного закатывания глаз, отвисания челюсти и сгибания шеи, – их тоже нужно было принять вечером.

Все это должно было ему помочь бороться с тем, что превратилось в длинный список диагнозов. Психоз на почве злоупотребления марихуаной. Шизофрения. Маниакальная депрессия. Однополярное эффективное расстройство. Психоз на почве злоупотребления амфетаминами. Основной эффективный психоз. Атипический психоз. И его главный любимец – искусственное расстройство, или симуляция, чтобы попасть в больницу. Но медикаменты не слишком-то помогали. Electron чувствовал себя несчастным наедине с множеством проблем в Мельбурне, только усугубивших его состояние.

Из-за болезни Electron по большей части не участвовал в судебных процедурах. Солнечный Квинсленд обеспечил ему желанное бегство. Теперь он вернулся в Викторию, к своему скучному университетскому курсу бухгалтерского учета, к непрекращающейся битве против душевного расстройства, к федеральным обвинениям, в результате которых он мог угодить в тюрьму на десять лет,

и к шумихе вокруг первого серьезного судебного процесса над хакерами в Австралии. Ему предстояла трудная зима.

Словно для того, чтобы еще больше усложнить ситуацию, лекарства подрывали способность Electron'a нормально учиться. Таблетки против побочных эффектов расслабляли глазные мускулы, мешая им нормально фокусировать взгляд. Написанное на доске в лекционной аудитории воспринималось, как размытая туманная клякса. Записывать тоже не всегда получалось. От лекарств у него дрожали руки, и он не мог писать как следует. К концу лекции Electron с таким же трудом удавалось прочесть свои собственные записи, как и то, что было написано на доске. Потеряв всякую надежду, Electron перестал принимать таблетки, снова начал покуривать травку и вскоре почувствовал себя лучше. Когда марихуаны было недостаточно, он прибегал к волшебным грибочкам и галлюциногенным кактусам.

Хакерское дело набирало обороты. 6 декабря 1991 года, сразу же после того, как Electron вышел из больницы, но прежде, чем он успел улететь в Квинсленд, Генеральная прокуратура официально представила в окружной суд штата Виктория обвинительный акт, в котором было выдвинуто пятнадцать обвинений против Electron'a и три обвинения против Nom'a.

Electron больше не разговаривал с Phoenix'ом, но юристы из офиса DPP не забыли о нем. Мало того, у них были далеко идущие планы насчет Phoenix'a, возможно, потому, что он оспаривал каждый пункт обвинения. Phoenix не захотел сотрудничать с полицией в день ареста, он постоянно отказывался отвечать на вопросы. Когда полицейские хотели взять у него отпечатки пальцев, он заартачился и начал спорить об этом. Его поведение не сделало его любимчиком ни полиции, ни прокуратуры.

5 мая 1992 года Генеральная прокуратура представил в окружной суд окончательный обвинительный акт по делу Phoenix'a из сорока пунктов. Обвинение, вместе с делами Electron'a и Nom'a, составляло часть общего обвинительного акта из 58 пунктов.

Electron волновался насчет тюрьмы. По всему миру хакеры были в осаде: Par, Pengo, LOD и Eric Bloodaxe, MOD, хакеры Realm, Pad и Gandalf и совсем недавно International Subversives.<sup>[p129]</sup> Казалось, что кто-то хочет выкорчевать хакинг с корнем. Достаточно сказать, что обвинение против Electron'a изменилось – и в гораздо худшую сторону – по сравнению с первоначальным вариантом в апреле 1990 года.

Окончательный обвинительный акт офиса генерального прокурора мало походил на тот жалкий листок, который был вручен молодому хакеру, когда его отпускали домой из полицейского участка в день ареста. Окончательное обвинение можно было читать, как справочник «Кто есть кто» престижных учреждений по всему миру. Лаборатория имени Лоренса Ливермора, Калифорния. Два разных компьютера в Военно-морской исследовательской лаборатории США, Вашингтон, округ Колумбия. Университет Рутгерс, Нью-Джерси. Технологический университет в Тампере, Финляндия. Иллинойский университет. Три разных компьютера в Мельбурнском университете. Технологический университет в Хельсинки, Финляндия. Университет Нью-Йорка. Исследовательский центр NASA в Хэмптоне, Вирджиния. CSIRO в Карлтоне, Виктория.

Больше всего Electron'a беспокоили обвинения, связанные с Военно-морской лабораторией США, CSIRO, Ливерморской лабораторией и NASA. Хотя три последних не были его собственными, DPP настаивал на «явной» связи Electron'a с доступом Phoenix'a на эти сайты.

Electron смотрел на тринадцатистраничный обвинительный акт и не знал, плакать ему или смеяться. Он был гораздо больше, чем «явно связан» с доступом на эти сайты. В большинстве случаев он лично дал доступ Phoenix'у к этим компьютерам. Но Electron старался работать в этих системах тихо и осторожно, тогда как Phoenix топтался в них с грацией буйвола и оставлял такие же чудовищные следы. Electron'у не улыбалось быть обвиненным по факту проникновения в эти и все остальные сайты. Он взломал тысячи мест в сети X.25, но не был обвинен ни за один из этих случаев. Он не мог отогнать от себя ощущение, похожее на то, что пришлось испытать гангстеру Аль Капоне, когда его обвинили в уклонении от уплаты налогов.

Слушания привлекли значительное внимание СМИ. Electron подозревал, что АФП и Генеральная прокуратура приложили руку к тому, чтобы журналисты узнали о приближении суда. Власти стремились показать американцам, что они «что-то делают».

Это дело несло на себе совершенно отчетливый отпечаток американского давления. Защитник

Electron'a Борис Кайзер [Boris Kayser] сказал о своих подозрениях, что «американцы» – американские организации, компании или правительственные агентства – косвенно повлияли на появление некоторых из пунктов обвинения, предложив оплатить свидетелям из США их присутствие на австралийском процессе. Американцы хотели увидеть австралийских хакеров побежденными и готовы были использовать любые средства, чтобы быть уверенными, что так все и произойдет.

Была еще одна проблема – в каком-то смысле самая тревожная из всех. В ходе судебной нервозности Electron'у сказали, что именно Секретная служба США науськала Австралийскую федеральную полицию начать расследование подвигов хакеров, которое привело к аресту Electron'a и теперешним проблемам с законом. Секретная служба преследовала хакеров, которые взломали Citibank.

Когда это произошло, Electron ни разу и близко не подошел к Citibank. Кредитные карты совершенно не интересовали его. Он считал банки скучными, поскольку достаточно настрадался от бухгалтерской тяготы в своем университете. И если он не собирался обкрадывать банки, – а он никогда не сделал бы этого, – не было никакого смысла взламывать банковские компьютеры.

Но Секретную службу США, напротив, очень интересовали банки и Phoenix – по той простой причине, что, по их мнению, он не только побывал в компьютерах Citibank, но и руководил нападением на него.

Почему же Секретная служба США так думала? Так ведь Phoenix хвастал этим по всему подполью. Он не только говорил всем и каждому, что взломал компьютер Citibank, но и гордо сообщал, что похитил оттуда почти \$50 000.

Читая дальше материалы своего дела, Electron обнаружил кое-какую информацию, которая, похоже, подтверждала то, что ему сказали. Ордер на прослушивание обоих домашних телефонов Phoenix'a упоминал возможные «серьезные потери Citibank» как основание для его получения. Странное дело – отпечатанные на машинке слова пересекали каракули судьи, выдавшего ордер. Но они были все же читабельны. «Неудивительно, что Секретная служба США начала это дело», – подумал Electron. Банки не очень любят, когда до них доходят сведения о том, что кто-то нашел анонимный способ их ограбить.

Electron знал, что Phoenix не крал никаких денег в Citibank. Он и сам когда-то грешил тем, что распространял о себе фантастические истории ради повышения своего рейтинга в андеграунде, но с течением времени ему удалось избавиться от этой привычки.

В сентябре 1992 года Phoenix позвонил Electron'у, предлагая встретиться, чтобы обсудить ситуацию. Electron'a удивил этот звонок. Может быть, он что-то заподозрил, чувствуя, что связывавшие их отношения стали слабыми и продолжали слабеть. Или психическое нездоровье Electron'a изменило его восприятие мира. Или его все возрастающая отстраненность была продиктована раздражением из-за постоянного хвастовства Phoenix'a. Какой бы ни была причина, грызущее Phoenix'a беспокойство, очевидно, укрепилось после того, как Electron отказался встречаться с ним.

Electron не хотел этой встречи, потому что Phoenix ему не нравился, а также потому, что считал Phoenix'a основным виновником того, что австралийские хакеры оказались в нынешней невеселой ситуации.

С этими мыслями, зреющими в его голове, Electron несколько месяцев спустя с интересом выслушал предложение своего адвоката Джона Мак-Лафлина [John McLoughlin]. В судебных кругах такие вещи были обычны, но новы для Electron'a. Он решил последовать совету Мак-Лафлина.

Electron решил дать показания против Phoenix'a в качестве государственного свидетеля.

## 7

### Судный день

*Мир твоих снов подходит к концу.*

**Песня «Мир Сна», альбом «Diesel and Dust» группы Midnight Oil<sup>32</sup>**

На другом конце земного шара британские хакеры Gandalf и Pad с ужасом читали о том, что австралийские власти арестовали трех хакеров Realm. Electron просто однажды исчез из поля зрения.

---

<sup>32</sup> Слова и музыка: Peter Garrett / James Moginie / Rob Hirst. © Copyright 1988 Sprint Music. Administered for the World – Warner / Chappell Music Australia Pty Ltd. Used by Permission.

Phoenix тоже куда-то пропал. Затем новости из газет и от других австралийских хакеров просочились на немецкий сайт под названием Lutzifer, очень похожий на Altos.

Pad'a беспокоило еще кое-что. В одном из своих хакерских набегов он обнаружил файл, явно написанный Юджином Спаффордом. В нем шла речь о его твердой уверенности в том, что некоторые британские хакеры – читай, Pad и Gandalf, – создали нового червя на базе червя RTM и запустили его в Интернет. На основании этого заключения был сделан вывод, что неизвестные британские хакеры способны посеять невероятный хаос на тысячах сайтов Интернета.

Gandalf и Pad действительно охотились за копиями исходных кодов различных червей. Они шныряли вокруг SPAN, пока не выудили оттуда копию червя Father Christmas. Когда они все-таки сумели взломать машину Рассела Брэнда в LLNL, они ловко похитили оттуда полную копию червя WANK. В машине Брэнда они к тому же нашли описание того, как некто неизвестный вторгся в SPAN в поисках кода червя WANK, но не смог найти его. «Это я взломал SPAN, чтобы осмотреться», – смеялся Gandalf, пересказывая Pad'у историю.

Несмотря на растущую коллекцию кодов червей, Pad не собирался писать ничего подобного. Коды были им нужны лишь для того, чтобы узнать, какие методы проникновения используют черви и, возможно, выяснить что-то новое. Британские хакеры гордились тем, что никогда не наносили никаких повреждений взломанным им системам. В тех местах, где, как им становилось известно, администраторы обнаруживали следы их деятельности, например в университетах Бата, Эдинбурга, Оксфорда и Стратклайда, обнаруживались записки, подписанные 8lgm. Это был не просто вопрос честолубия – это был способ сообщить админам, что они приходили в их систему без всякого злого умысла.

В одном университете админы подумали, что 8lgm – это какая-то загадочная разновидность бельгийского червя, а хакеры, которые посещают их систему каждую ночь, приходят из Бельгии. В другом университете админы по-своему расшифровали загадку. По утрам, когда они приходили на работу и видели, что хакеры опять резвились в их компьютерах, они вздыхали и говорили: «Наши восемь маленьких зеленых человечков снова заглядывали». [\[p130\]](#)

В университете Ланкастера хакеры написали администратору: «Не сделали ничего плохого. У нас хороший имидж в мире, поэтому, пожалуйста, не надо портить его и сочинять истории о том, что мы причинили вред вашей системе. Не держите на нас зла, но помните о нас». Куда бы они ни пришли, смысл послания оставался неизменным.

Тем не менее, Pad отчетливо представлял себе картину того, как Спаф подстегирует людей из компьютерной безопасности и государственных силовых структур, стараясь вызвать панику и свалить на британских хакеров все, что можно, даже то, что они и не делали. В андеграунде знали о ненависти Спафа к хакерам, которая проявилась в его активном преследовании автора червя RTM. Кроме того, Gandalf взломал машину Спафа.

Жестокое преследование австралийцев в сочетании с появлением файла Спафа произвели глубокое впечатление на Pad'a. Он всегда был осторожен, но в создавшейся ситуации он и вовсе решил бросить хакинг. Это было нелегкое решение – отказ от еженощного исследования новых систем был тяжелым испытанием.

Но принимая во внимание то, что случилось с Phoenix'ом и Electron'ом, продолжение прежней деятельности едва ли могло оправдать связанный с ней риск.

Когда Pad покончил с хакингом, он купил себе NUI и смог получить законный доступ в места вроде Altos. NUI был дорогим удовольствием – около десяти фунтов в час, но Pad никогда не оставался там надолго. О беспечной болтовне в Altos, которой он предавался в прежние времена, не могло быть и речи, но, по крайней мере, Pad мог отправлять весточки своим друзьям, например Theorem и Gandalf'у. Дружбу с Gandalf'ом можно было поддерживать иначе, более легким способом – он жил в Ливерпуле, в часе езды от Pad'a. Но это было совершенно не то. Pad и Gandalf никогда не встречались лично. Они даже по телефону не разговаривали. Они общались онлайн и по электронной почте. Такие вот отношения.

У Pad'a были и другие причины завязать с хакингом. В Британии это было дорогое удовольствие из-за высоких тарифов British Telecom на местные звонки. В Австралии хакер мог находиться онлайн часами, прыгая от одного компьютера к другому по сети данных, и все это по цене одного местного телефонного звонка. Как и австралийцы, Pad мог запускать свои хакерские сессии из мест-

ного университета или с помощью удаленного набора сети X.25. Но все же долгие ночные хакерские вылазки обходились ему в пять или даже больше фунтов – значительная сумма для неработающего молодого человека. По этой причине Pad был вынужден порой прекращать хакерскую деятельность на короткие периоды, когда у него заканчивались деньги.

Хотя Pad не думал, что его будут преследовать за хакерскую деятельность по английским законам начала 1990 года, он знал, что в августе Великобритании готовится принять свое собственное законодательство против компьютерных преступлений – Computer Misuse Act 1990.<sup>[p131]</sup> Двадцатидвухлетний хакер решил, что лучше остановиться, пока он не вступил в силу.

Он так и поступил, во всяком случае на какое-то время. До июля 1990 года, когда Gandalf, который был на два года младше Pad'a, соблазнил его на последний взлом, пока новый закон еще не вступил в силу. Всего один, последний выход, говорил ему Gandalf. После этого июльского выступления Pad снова прекратил хакинг.

Computer Misuse Act вступил в действие в августе 1990 года после рассмотрения двух законодательных инициатив. В 1987 году Законодательная комиссия Шотландии вынесла предложение считать незаконным неправомерный доступ к данным не только в том случае, если хакер пытается «извлечь выгоду или причинить вред другому лицу», но и если причиняется невольный вред.<sup>33</sup> Простой ознакомительный хакинг по рекомендации комиссии не должен был считаться преступлением. Но в 1989 году Законодательная комиссия Англии и Уэльса предложила свой законопроект, по которому следовало считать преступлением любой неправомерный доступ к компьютерным данным, вне зависимости от намерений осуществляющего его лица. Эта рекомендация и была включена в новый закон.

Позже, в том же 1989 году, член парламента от партии консерваторов Майкл Колвин [Michael Colvin] предложил британскому парламенту свой законопроект. Другой парламентарий-консерватор, резко критиковавший хакинг, Эмма Николсон [Emma Nicholson], поддержала законопроект, инициировала публичные дебаты на эту тему и обеспечила законопроекту поддержку в парламенте.

В ноябре 1990 года Pad разговаривал онлайн с Gandalf'ом, и его друг предложил предпринять еще одну вылазку, только одну – в память о старых добрых временах. «Ладно, – подумал Pad, – еще одна вылазка мне не повредит».

Вскоре Pad вернулся к хакингу, и когда Gandalf хотел завязать, уже Pad подстрекал его вернуться к любимому времяпрепровождению. Они походили на двух школьников, подталкивающих друг друга к очередной проделке – из тех, что совершаются вдвоем. Если бы Pad и Gandalf не были знакомы друг с другом, они, вероятнее всего, навсегда отошли бы от хакинга в 1990 году.

Раз уж они оба вернулись к естественному ходу вещей, то постарались выяснить степень вероятности того, что их схватят. Gandalf частенько шутил в разговорах онлайн: «Знаешь, дружище, должно быть, мы впервые встретимся лично только в полицейском участке».

Невероятно дерзкий и всегда бодрый, Gandalf был настоящим другом. Pad не часто встречал таких парней-путешественников в реальном мире, не говоря уже об электронном. То, что казалось другим – особенно некоторым американским хакерам – верхом наглости, Pad расценивал, как блестящее чувство юмора. Pad считал Gandalf'a лучшим другом, о каком только можно мечтать.

За время, пока Pad отходил от хакинга, Gandalf сошелся с молодым хакером по имени Wandii, тоже с севера Англии. Wandii никогда не играл заметной роли в международном компьютерном андеграунде, но он провел немало времени, взламывая компьютеры по всей Европе. Wandii и Pad отлично ладили, но никогда не были друзьями. Они были знакомыми, связанными в подполье через Gandalf'a.

К середине 1991 года Pad, Gandalf и Wandii были изрядно утомлены. По крайней мере, один из них (а может, и не один) побывал в системах Европейского Сообщества в Люксембурге, *The Financial Times* (владелец индекса FTSE), британских Министерства обороны и Министерства иностранных дел, NASA, инвестиционного банка SG Warburg в Лондоне, в базе данных американского производителя программного обеспечения Oracle и в таком количестве машин в сети JANET, какое невозможно упомянуть. Они с легкостью проникли в сеть PSS, принадлежащую British Telecom, по-

---

p131

«Акт о противоправном использовании компьютеров».

<sup>33</sup> Rupert Battcock, «The Computer Misuse Act Five years on – the Record since 1990», paper, Strathclyde University, Glasgow, UK.

хожую на Tynet в сети X.25.<sup>34</sup>

Девизом Gandalf'a было: «Если можешь – взломай».

27 июня 1991 года Pad сидел в комфортабельной гостиной родительского дома в Манчестере и смотрел, как последние осколки дневного света тают на закате одного из самых длинных дней в году. Pad любил лето, любил просыпаться в солнечных лучах, пробивавшихся сквозь занавески в его комнате. Он часто думал про себя, что нет ничего лучше этого.

Около 11 часов вечера он включил модем и свой компьютер Atari 520 ST в гостиной. В доме было две машины Atari – показатель серьезного увлечения Pad'a компьютерами, в то время как ни другие дети в семье, ни родители совершенно не интересовались программированием. Хотя большую часть времени Pad даже не прикасался к старому Atari. Его старший брат учился в аспирантуре на факультете химии и писал на нем свою диссертацию.

Прежде чем приступить к дозвону, Pad убедился, что никто не занимает единственную телефонную линию семьи. Она была свободна, и Pad отправился в Lutzifer, чтобы посмотреть, нет ли для него почты. Несколько минут ему пришлось ждать, пока его машина подключится к немецкой доске объявлений, как вдруг он услышал глухой удар, а затем какой-то треск. Pad оторвался от клавиатуры, посмотрел вверх монитора и прислушался. Он подумал, слышали ли этот треск его старший брат наверху и родители у телевизора в семейной гостиной в глубине дома.

Звук стал громче и заставил Pad'a посмотреть в сторону прихожей. В следующую секунду рама входной двери с треском раскололась, выворачивая дверь из петель и замка. Дерево разлетелось в щепки под воздействием чего-то вроде автомобильного домкрата.

Несколько человек ворвались в дом, промчались через прихожую и взлетели по лестнице, покрытой ковром, наверх, в комнату Pad'a.

Все еще сидя за своим компьютером внизу, Pad поспешно выключил свой модем, а затем и компьютер, мгновенно уничтожив соединение и все данные на экране. Он подошел к лестнице и прислушался к тому, что происходит наверху. Если бы он не был потрясен, он бы, наверное, посмеялся. Он понял, что полицейские устремились в его спальню, ведомые своим стереотипным представлением о хакере, полученном, очевидно, из газет. Парень. В своей комнате. Сгорбившись над компьютером. Поздно ночью.

Они нашли в комнате молодого человека и компьютер тоже. Но это был не тот парень и во всех отношениях не тот компьютер. Полиции понадобилось почти десять минут терзать вопросами брата Pad'a, чтобы понять свою ошибку.

Услышав шум, родители Pad'a выскочили в прихожую, в то время как он сам выглядывал из двери гостиной. Полицейский в форме провел всех в комнату и начал задавать Pad'у вопросы:

– Вы пользуетесь компьютерами? Вы используете в компьютерах имя Pad'?

Pad понял, что игра окончена. Он правдиво ответил на все вопросы. Он подумал, что, в конце концов, хакинг не такое уж серьезное преступление. Это совсем не то, что украсть деньги или что-то в этом роде. Все это, конечно, неприятно, но он переживет. Ну, дадут ему затрещину да шлепнут по рукам, и вскоре все закончится.

Полицейские отвели Pad'a в его комнату и принялись обыскивать ее, продолжая задавать ему вопросы. Комната была удобной и обжитой. Аккуратно сложенная одежда, несколько пар обуви на полу, подвернутые шторы и несколько музыкальных постеров – Джимми Хендрикс и The Smiths – на стене.

Кучка полицейских топталась вокруг компьютера. Один из них принялся рыться в книгах Pad'a на полках над ПК, вынимая и просматривая каждую. Несколько любимых книжек Спайка Миллигана.<sup>[p132]</sup> Старые учебники по шахматам, оставшиеся с тех времен, когда Pad был капитаном местной шахматной команды. Учебники по химии, купленные Pad'ом задолго до того, как он начал изучать этот предмет – просто для удовлетворения своего любопытства. Учебники по физике. Справочник по океанографии. Книга по геологии, появившаяся после экскурсии в пещеры, которая пробудила интерес Pad'a к образованию скальных пород. Мать Pad'a работала медсестрой, а его отец, инженер-электронщик, занимался испытаниями гироскопов на самолетах. Родители всегда поощряли

<sup>34</sup> Материалы о британских хакерах в этой главе базируются на личных интервью, репортажах СМИ (особенно о деле Wandii), журнальных статьях, академических материалах и докладах комиссий.



интерес их ребенка к наукам.

Полисмен вернул книги на полку, выбрав лишь компьютерные учебники, руководства по программированию и математике, по которым Рад занимался в университете Манчестера. Он бережно сложил их в пластиковые пакеты, чтобы забрать с собой в качестве вещественных доказательств.

Затем полицейские занялись коллекцией музыкальных записей – The Stone Roses, Pixies, New Order, The Smiths и другие независимые группы с процветающей музыкальной сцены Манчестера. Эта коллекция кассет ничего не доказывала, кроме эклектичности музыкального вкуса.

Еще один полисмен открыл платяной шкаф Рад'а и заглянул внутрь.

– Есть здесь что-нибудь интересное? – спросил он.

– Нет, – ответил Рад. – Все там.

Он показал на коробку с компьютерными дискетами.

Рад подумал, что нет никакого смысла полицейским переворачивать всю комнату, ведь они все равно найдут то, что им нужно. Ничего и не было спрятано. В отличие от австралийских хакеров он совсем не ждал полицию. Хотя часть данных на его жестком диске была зашифрована, там оставалось достаточно изобличающих его улик на незашифрованных файлах.

Рад не мог расслышать, о чем говорили его родители с полицейскими в соседней комнате, но они явно были спокойны. Да и почему они должны волноваться? Их сын не сделал ничего дурного. Он никого не избивал в пьяной драке в пабе и никого не грабил. Он никого не задавил, управляя автомобилем в нетрезвом виде. «Нет, – думали они, – это все его делишки с компьютерами». Должно быть, он шляется там, где не следовало, но это вряд ли серьезное преступление. Им нечего волноваться. Ведь он не сядет из-за этого в тюрьму. Полиция разберется. Наверное, его вызовут в суд и все на этом закончится. Мать Рад'а даже предложила полицейским по чашке чаю.

Один из полисменов прервал допрос Рад'а в его комнате, чтобы выпить свой чай. Кажется, он знал, что Рад живет на пособие, и с абсолютно серьезным лицом спросил у хакера: «Если тебе нужна работа, то почему бы тебе не пойти служить в полицию?»

Рад чуть было не потерял чувство реальности. В его дом ворвалась толпа сотрудников правоохранительных органов – включая представителей отдела по борьбе с компьютерными преступлениями Скотланд-Ярда и British Telecom, – а этот парень спрашивает, почему он не хочет стать легальным?

Рад едва не расхохотался. Даже если бы он не подвергся этому налету, он никогда, ни на секунду не мог подумать о том, чтобы стать полицейским. Никогда, думай он хоть миллион лет. Хотя его семья и друзья внешне производили впечатление благополучного среднего класса, они всегда были оппозиционно настроены по отношению к истеблишменту. Многие знали, что Рад занимается хакингом и какие сайты он взламывает. Их отношение было таким: «О, взламываешь Большого Брата? Удачи тебе»,

Его родители разрывались между желанием поддержать интерес Рад'а к компьютерам и волнением за сына, который проводил слишком много времени, словно приклеенный к монитору. Их смешанные чувства порой отражали мысли самого Рад'а.

Иногда, с головой погрузившись в бесконечные ночные хакерские авантюры, он вдруг выпрямлялся и спрашивал себя: «Что я здесь делаю? Какого черта я трахаюсь с компом круглые сутки? К чему это приведет? Что будет с моей жизнью?» Когда такие мысли посещали его, он прекращал заниматься хакингом на несколько дней или даже недель. Обычно он проводил свободное время в университетском пабе за пинтой пива в преимущественно мужской компании однокурсников.

Высокий, худощавый, с короткими каштановыми волосами и приятным мальчишеским лицом, всегда обходительный, Рад мог бы вызвать неподдельный интерес у многих умных девушек. Но проблема была в том, где найти таких девушек. В университете они попадались нечасто – на его курсе математики и программирования учились в основном парни. Поэтому обычно они с друзьями отправлялись в поход по ночным клубам Манчестера, чтобы пообщаться и послушать хорошую музыку.

Рад спустился вниз с одним из полисменов и стал смотреть, как полиция отключает его модем в 1200 бод и упаковывает его в пластиковый мешок. Рад купил этот модем, когда ему было восемнадцать лет. Полисмены отсоединяли кабели, сворачивали их и складывали в пронумерованные пластиковые пакеты. Они забрали его жесткий диск на 20 Мб и монитор. Снова пронумерованные мешки.

Один из полицейских поманил Рад'а к выходу. Домкрат все еще торчал из искореженной рамы. Полицейские взломали дверь, вместо того чтобы просто постучать. Они надеялись застать хакера онлайн, на месте преступления. Офицер жестом пригласил Рад'а следовать за ним.

– Пойдем, – сказал он, уводя его в ночь. – Мы забираем тебя в участок.

;) )

Rad провел ночь в полном одиночестве в камере полицейского участка Сэлфорд-Креснт. Ни уголовников, ни других хакеров.

Он устроился на одном из металлических топчанов, расположенных по периметру камеры, но сон никак не шел к нему. Rad думал о том, арестован ли Gandalf. От него не было ни звука, но вряд ли полиция настолько глупа, чтобы посадить обоих хакеров в одну камеру. Он ворочался с боку на бок и крутился всю ночь, пытаясь отогнать от себя эти мысли.

Rad увлекся хакингом почти случайно. По сравнению с другими персонажами андеграунда он занялся этим довольно поздно – в девятнадцать лет. Катализатором стал Altos. Посещая различные BBS, Rad как-то прочитал файл, в котором шла речь не просто об Altos – в нем подробно описывалось, как туда попасть. Кроме того, в файле был NUI. В отличие от австралийского андеграунда, зачаточное британское подполье не имело недостатка в NUI. Кто-то обнаружил целый склад NUI от British Telecom и поместил их на BBS по всей Англии.

Rad последовал инструкциям, обнаруженным им на доске объявлений, и вскоре оказался на немецком чат-канале. Как и Theorem, он был очарован дивным новым живым миром Altos. Это было чудесно – большая международная тусовка. Помимо всего прочего, он не каждый день имел возможность пообщаться с австралийцами, швейцарцами, немцами, итальянцами и американцами. Вскоре он стал заниматься хакингом, как и многие другие постоянные посетители Altos.

Идея хакинга всегда занимала его. Еще когда он был подростком, его совершенно ошеломил фильм «Военные игры».<sup>[p133]</sup> Мысль о том, что компьютеры могут связываться между собой посредством телефонных линий, увлекла шестнадцатилетнего паренька, заполнив его голову новыми идеями. Вскоре он увидел телерепортаж о группе хакеров, которые утверждали, что они использовали свои знания, чтобы изменить орбиту космического спутника – та же самая история, которая поразила воображение Electron'a.

Rad вырос в Большом Манчестере. Больше века назад этот регион стал центром текстильного бума. Но бурный рост экономики никак не отразился на росте благосостояния населения. В начале 40-х годов XIX века Фридрих Энгельс [Friedrich Engels] работал на отцовской хлопкопрядильной фабрике в этом районе, и страдания, которые он видел вокруг, повлияли на его самую знаменитую работу – «Манифест коммунистической партии», опубликованный в 1848 году.

Манчестер обладал всеми признаками рабочего города, жители которого зачастую не одобряли правительство и не доверяли властям. 70-е и 80-е годы XX столетия с их безработицей и упадком преобразили когда-то процветающий текстильный центр. Но этот упадок явно способствовал укреплению скрытой решимости большинства населения бросить вызов символам власти.

Семья Rad'a жила не в многоэтажке на окраине, а в одном из пригородов, в окружении среднего класса, в старом районе далеко от мрачного фабричного центра. Но как и многие, кто живет на севере Англии, Rad терпеть не мог всякую претенциозность. В действительности, он глубоко впитал чувство здорового естественного скептицизма, возможно, ставшее следствием культурного уровня парней, чьим любимым развлечением было наступать друг другу на ноги в пабе.

Этот его скептицизм был на пике, когда он смотрел историю про хакеров, предположительно изменивших орбиту спутника, но каким-то образом эта идея проскользнула через КПП в его голове и захватила его воображение так же, как это произошло с Electron'ом. Он почувствовал, что должен лично проверить, правда ли это, и начал заниматься хакингом с неистовым энтузиазмом. Сначала это была любая мало-мальски интересная система. Затем он перешел к известным системам – к компьютерам, которыми владели серьезные большие учреждения. Позже, работая с австралийцами, он научился находить мишени среди экспертов компьютерной безопасности. Он узнал, что именно здесь спрятано настоящее сокровище.

;) )

Утром охранник принес Pad'у поесть, но то, что он принес, было мало похоже на еду. Затем хакера препроводили в комнату для допросов, где его уже ждали двое полицейских и представитель British Telecom.

Нужен ли ему адвокат? Нет. Ему нечего скрывать. Кроме того, полиция уже располагает доказательствами по его делу, включая незашифрованные данные из лог-файлов хакерских сессий. Поэтому он открыто смотрел в глаза своим инквизиторам и охотно отвечал на их вопросы.

Дело начало приобретать неожиданный оборот, когда речь вдруг зашла об ущербе, который он нанес компьютерам Центральной политехнической школы Лондона. Ущерб? Какой ущерб? Pad совершенно точно не мог причинить никакого ущерба.

«Отнюдь», – сказали ему полицейские. Нанесенный им ущерб оценивался почти в четверть миллиона фунтов стерлингов.

У Pad'a от ужаса перехватило дыхание. *Четверть миллиона фунтов?* Он принялся вспоминать о своих многочисленных набегах в эту систему. Он, конечно, немного напроказил, изменив официальное приветствие на «Хай!» и подписав его 8lgm. Он создал для себя несколько учетных записей, чтобы иметь возможность вернуться в систему как-нибудь попозже. В этом не было ничего особенного с тех пор, как они с Gandalf'ом взяли в привычку создавать для себя в системах JANET учетные записи, подписанные 8lgm. Он также стирал доказательства своих регистраций, чтобы замести следы, но и это было нормально. Он никогда не уничтожал ни единого файла пользователей. Все это было просто забавой, игрой в кошки-мышки с системными администраторами. Он не мог припомнить ничего, что могло бы причинить такой колоссальный ущерб. Может быть, они взяли не того хакера?

Нет, все в порядке, он именно тот, кто им нужен. Восемьдесят следователей из British Telecom, Скотланд-Ярда и других мест в течение двух лет охотились за хакерами 8lgm. У них были следы телефонных соединений, логины с его компьютера и логины из взломанных сайтов. Они точно знали, что это он.

После почти двухчасового допроса они вернули Pad'a в камеру. «Продолжим завтра», – сказали ему.

Позже в тот же день охранник сказал Pad'у, что пришли его отец и мать. Он мог встретиться с ними в комнате для свиданий. Разговаривая через стеклянную перегородку, Pad попытался успокоить своих взволнованных родителей. Через пять минут полицейский сказал, что свидание окончено. Поспешно прощаясь под нетерпеливым взглядом охранника, родители Pad'a сказали, что они принесли ему кое-что почитать в камере. Это был учебник океанографии.

Вернувшись в камеру, он попытался читать, но никак не мог сконцентрироваться на книге. Он снова и снова прокручивал в голове обстоятельства своих визитов в Политехническую школу, пытаясь понять, как он мог случайно нанести ущерб на £250 000. Pad был очень толковым хакером; в нем не было ничего от неумелого подростка, который топчется в системах, как слон в посудной лавке. Он знал, как войти в систему и выйти из нее, не причиняя вреда.

Вскоре после восьми вечера, когда Pad сидел на нарах, продолжая переваривать заявление полиции об ущербе, его камеру наполнила мрачная музыка. Сначала тихо, почти неслышно, как легкий стон, который постепенно перерос в торжественные, но узнаваемые ноты. Это было похоже на традиционное хоровое пение Уэльса и доносилось откуда-то сверху.

Pad посмотрел на потолок. Пение – только мужские голоса – вдруг прекратилось, затем началось снова, повторяя все те же низкие тяжеловесные ноты. Хакер улыбнулся. Хор местных полицейских репетировал прямо над его головой.

После еще одной беспокойной ночи Pad подвергся следующему раунду допроса. Вопросы задавали в основном полицейские, но они явно не были знатоками компьютеров, не то что любой приличный хакер среди тех, кто посещал Altos. Когда кто-нибудь из полицейских задавал технический вопрос, он смотрел на парня из British Telecom на другом конце стола, словно спрашивая: «Это имеет какой-нибудь смысл?» Парень из ВТ слегка кивал, затем полицейский переводил взгляд на Pad'a, ожидая ответа. В большинстве случаев хакеру удавалось разобраться в том, что они хотели спросить, и он отвечал соответственно.

Pad'a снова отправили в камеру, пока они работали над обвинительным заключением. Оказавшись в одиночестве, Pad снова подумал о том, арестован ли Gandalf. И словно ответ свыше, до Pad'a через стену донеслись звуки тонового телефонного набора. Так он узнал, что Gandalf тоже попался.

Gandalf оснастил свой компьютер устройством тонового набора. Теперь полицейские играли этим устройством, пытаясь понять, что оно делает.

Ну вот, теперь, после двухлетнего знакомства, Pad наконец встретится с Gandalf'ом. Как он

выглядит? Сохранится ли между ними то же родство душ, какое существовало онлайн? Pad чувствовал, что хорошо знает Gandalf'a, знает его натуру, но личная встреча могла все усложнить.

Полицейский открыл дверь камеры. Он объяснил Pad'у, что все бумажные формальности, включая обвинительное заключение, наконец улажены, и провел его в вестибюль, сказав, что сейчас он встретится с Gandalf'ом и Wandii. Вокруг двух молодых людей полукругом столпились полицейские. Кроме отдела Скотланд-Ярда по борьбе с компьютерными преступлениями и секьюрити British Telecom, в трех рейдах приняли участие по меньшей мере еще семь полицейских структур, включая силы полиции Большого Манчестера, Мерсисайда и Западного Йоркшира. Им было интересно посмотреть на хакеров.

Полиция узнала имена хакеров только в самом конце своего двухлетнего расследования. После такой долгой, трудной охоты полицейским пришлось подождать еще немного, если они хотели арестовать каждого хакера в тот момент, когда он находился онлайн. Это означало слежку за домом каждого из них до тех пор, пока объект не зарегистрируется в какой-нибудь системе. Годилась любая система. Хакерам даже не надо было общаться между собой онлайн, ведь нарушение закона начиналось уже на уровне нелегального логина. Полиция терпеливо выжидала и в конце концов задержала всю троицу в течение нескольких часов, так что у хакеров не было времени предупредить друг друга.

Поэтому в конце такой долгой охоты и тщательно спланированной операции полицейским хотелось поближе посмотреть на хакеров.

После того, как полицейский подвел Pad'a к остальным, он представил ему Gandalf'a. Высокий худой шатен с бледной кожей, он немного походил на Pad'a. Двое хакеров застенчиво улыбнулись друг другу. Затем полицейский показал на Wandii, семнадцатилетнего школьника. Pad не успел толком его разглядеть, потому что их выстроили в ряд – Gandalf оказался посередине, – чтобы ознакомить с деталями дела. Они обвинялись по Computer Misuse Act 1990 года. Когда дата суда будет назначена, их известят.

Наконец им позволили пойти домой, Wandii куда-то исчез. Pad и Gandalf вышли на улицу, нашли пару скамеек и улеглись на них. Они болтали, греясь на солнце, пока за ними не приехали родители, чтобы отвезти их по домам.

Оказалось, что Gandalf так же легок в личном общении, как и онлайн. Они обменялись телефонами и замечаниями по поводу обысков и арестов. Перед допросом Gandalf настаивал на адвокате, но когда тот прибыл, выяснилось, что он не имеет ни малейшего понятия о компьютерных преступлениях. Он посоветовал Gandalf'у рассказать полиции все, что она хочет знать. Хакер это и сделал.

:)

Суд проходил в Лондоне. Pad'у было непонятно, почему дело разбирается на юге, если все трое хакеров живут на севере страны. Кроме того, манчестерский суд был достаточно авторитетной инстанцией, чтобы вынести решение по их вопросу.

Возможно, это произошло потому, что Скотланд-Ярд находится в Лондоне. Может быть, вся канцелярская работа началась здесь. Может быть, причиной стал тот факт, что их обвиняли во взломе компьютеров, расположенных на территории, находящейся под юрисдикцией Центрального уголовного суда Лондона – Олд-Бейли? Но циничная сторона души Pad'a отважилась сделать другое предположение, которое, в общем, подтвердилось после того, как он несколько раз приезжал в Лондон в 1992 году для участия в некоторых судебных процедурах еще до начала суда, назначенного на 1993 год. Когда Pad приехал в городской суд на Боу-стрит, чтобы получить окончательный обвинительный акт, он увидел, что улица переполнена журналистами, в точности, как он и ожидал.

Несколько хакеров тоже были здесь, чтобы не уронить честь андеграунда. Один из них – незнакомый – подошел к Pad'у после суда, хлопнул его по плечу и с энтузиазмом воскликнул: «Молодец, Падди!» Pad изумленно посмотрел на него и только улыбнулся. Он понятия не имел, как ответить незнакомцу.

Как и трое австралийских хакеров, Pad, Gandalf и малоизвестный Wandii послужили подопытными кроликами для обкатки антихакерских законов своей страны. К тому времени как хакеры 8lgm предстали перед судом, британские правоохранительные агентства потратили на расследование их преступлений целое состояние – если верить газетам, более £500 000. Этот процесс обещал стать показательным, и правительственные службы хотели, чтобы налогоплательщики знали, куда уходят их деньги.

Хакеров обвиняли не во взломе компьютеров. Им инкриминировали тайный сговор – гораздо более серьезное преступление.

Обвинение допускало, что эта троица вторгалась в компьютеры не ради получения личной выгоды, но при этом утверждало, что они вступили в сговор с целью проникновения в компьютерные системы и изменения данных в этих системах. Это был, мягко говоря, странный подход, учитывая тот факт, что трое хакеров не только ни разу не встречались, но даже не разговаривали друг с другом по телефону до дня ареста.

Но если принять во внимание потенциальное наказание за подобные преступления, этот подход не казался таким уж странным. Если бы хакеров обвинили в простом проникновении в компьютер, без намерений причинить вред, максимальное наказание в этом случае составило шесть месяцев тюрьмы и штраф до £5000. Тайный сговор, о котором шла речь в другой части статьи нового закона, предполагал пять лет тюремного заключения и не ограничивал сумму штрафа.

Обвинение решилось на большую авантюру. Доказать наличие тайного сговора было гораздо труднее, для этого нужно было привести конкретные примеры куда более серьезных преступных намерений, чем в случае со взломом компьютера без причинения ущерба. Суммы штрафов также значительно увеличивались. В случае удачи обвиняемые в самом громком на сегодняшний день хакерском процессе в Британии надолго отправятся в тюрьму.

Так же, как и в случае с хакерами Realm, двое фигурантов – Pad и Gandalf – собирались признать свою вину, в то время как третий – в этом случае Wandii – решил оспорить доводы обвинения. Legal Aid оплатила услуги адвокатов, потому что хакеры либо не работали вовсе, либо имели настолько низкооплачиваемую временную работу, что было решено оказать им бесплатную юридическую помощь.

Адвокаты Wandii заявили журналистам, что это показательное дело, по сути, является политическим процессом. Это было первое серьезное хакерское дело с момента введения нового закона. Обвиняемые не были изменившими своему долгу государственными служащими, тем не менее наблюдалась такая степень вмешательства властей в процесс, которая обычно характерна для рассмотрения случаев государственной измены.

22 февраля 1993 года, не позднее двух месяцев после того, как Electron принял решение стать государственным свидетелем против Phoenix'a и Nom'a, трое хакеров 8lgm оказались на скамье подсудимых в Королевском суде Саутворк в Южном Лондоне, чтобы выслушать обвинение по их собственному делу.

В тусклом зимнем свете здание суда Саутворк выглядело не слишком привлекательно, но это не отпугнуло толпы любопытных. Зал суда был переполнен, как и вся Боу-стрит. Детективы Скотланд-Ярда с трудом сдерживали натиск толпы, которая стремилась к залу заседаний № 12.

Обвинение сообщило журналистам, что в его распоряжении имеется около 800 компьютерных дискет с уликами. Они сказали, что если всю эту информацию распечатать на листах формата A4 и сложить их друг на друга, то получится стопа высотой свыше сорока метров. Учитывая огромное количество вещественных доказательств, с трудом внесенных в здание суда командой этих орлов юриспруденции, выбор зала суда на пятом этаже казался явно поспешным.

Стоя у скамьи подсудимых рядом с Wandii, Pad и Gandalf признали себя виновными по двум пунктам обвинения в тайном компьютерном сговоре – в сговоре с целью получения мошеннического доступа к телекоммуникационным услугам и в сговоре с целью совершения неправомерных изменений компьютерных материалов. Pad также признал свою вину по третьему пункту – причинение ущерба компьютеру. Этот пункт обвинения базировался на почти четверти миллиона фунтов стерлингов «ущерба», якобы нанесенного Центральной политехнической школе Лондона. В отличие от дела австралийцев, никто из английских хакеров не был обвинен в проникновении на специальные сайты вроде NASA.

Pad и Gandalf решили признать свою вину, так как думали, что у них нет особого выбора. Их юристы сказали им, что в свете представленных обвинением доказательств всякое отрицание вины не представляется возможным. Словно для того, чтобы подчеркнуть свою точку зрения, адвокат Pad'a сказал ему при встрече в конце 1992 года: «Я хотел бы пожелать вам счастливого Рождества, но не думаю, что оно будет таковым».

Адвокаты Wandii решили не соглашаться. Стоя бок о бок со своими приятелями, Wandii заявил, что он не виновен по трем пунктам обвинения в тайном сговоре: сговор с целью неправомерного доступа к компьютерам; сговор с целью неправомерного изменения компьютерных материалов; сговор с целью получения мошеннического доступа к телекоммуникационным услугам. Команда его защитников намеревалась доказать, что он страдает зависимостью от компьютерного хакинга и не был способен питать преступное намерение, достаточное для того, чтобы его осудили.

Pad подумал, что позиция Wandii довольно слаба. Зависимость казалась слабым оправданием.

Он заметил, что Wandii очень нервничал после того, как в суде было оглашено его заявление.

Pad и Gandalf уехали из Лондона сразу по окончании предварительных судебных процедур. Они вернулись на север и принялись готовиться к основным слушаниям и следить за развитием дела Wandii по средствам массовой информации.

И они не были разочарованы. Это было настоящее звездное шоу. Журналисты с бешенством набрасывались на все новые материалы. Обвинение, возглавляемое Джеймсом Ричардсоном [James Richardson], знало, как разжечь их аппетит. Ричардсон обрушился на Wandii, поведав суду, что этот школьник «так ломился в двери офисов ЕЭС в Люксембурге, что даже эксперты не на шутку встревожились. Он учинил разгром в университетах по всему миру».<sup>35</sup> Для этого Wandii понадобился простейший компьютер BBC Micro, рождественский подарок стоимостью в 200 фунтов.

«Его безобразия не ограничились компьютерами ЕЭС», – сказал Ричардсон нетерпеливой толпе журналистов. Wandii взломал Lloyd's, *Financial Times* и университет Лидса. В *Financial Times* проделки Wandii расстроили плавные операции индекса FTSE 100, который в Сити называют «footsie».<sup>[p134]</sup> Хакер установил в сети FT сканирующую программу, по вине которой система каждую секунду совершала один исходящий звонок. Результат вторжения Wandii – счет на £704, уничтожение важного файла и решение менеджмента об отключении ключевой системы. Компьютерный босс FT Тони Джонсон [Tony Johnson] сообщил журналистам, что по оценке банка весь инцидент обошелся его компании в £24 871.

Но взлом FT померк перед настоящим козырем обвинения: European Organization for the Research and Treatment of Cancer (EORTC)<sup>[p135]</sup> в Брюсселе. Суду сообщили, что они получили телефонный счет на £10 000 в результате запуска Wandii в их машине сканинг-программы.<sup>36</sup> Сканер оставил след в виде 50 000 звонков, зафиксированных в счете из 980 страниц.

Менеджер EORTC Венсан Пьебеф сообщил суду, что в результате сканирования система вышла из строя на целый день. Он продолжал, пояснив важность того, чтобы система работала круглосуточно и врачи могли регистрировать пациентов. База данных центра являлась ключевым пунктом для фармацевтических компаний, врачей и исследовательских институтов, координируя их усилия в борьбе с болезнью.

Для масс-медиа дело Wandii стало подарком небес. «Хакер-подросток устраивает вселенский хаос», – надрывалась на первой странице *Daily Telegraph*. На третьей странице в *Daily Mail* можно было прочесть: «Хакер-подросток сеет разрушения ради развлечения». Даже *The Times* не осталась в стороне. Мелкие региональные газеты раструбили историю Wandii по всей стране, до самых дальних британских островов. *Herald* в Глазго сообщил читателям: «Несовершеннолетний хакер накрутил телефонный счет до £10 000». На другом берегу Ирландского моря *Irish Times* поместила сенсацию на первую полосу: «Хакер-подросток взламывает систему компьютерной безопасности ЕЭС».

В первую же неделю разбирательства *The Guardian* сообщила, что Wandii вторгся в базу данных ракового центра. Когда за дело взялась *The Independent*, оказалось, что Wandii не только отключил базу данных, он еще и читал закрытую частную информацию о медицинских показаниях пациентов, больных раком: «Подросток вторгается в файлы пациентов, больных раком». На четвертый день суда, не желая оставаться в стороне, *Daily Mail* окрестила Wandii «компьютерным гением». На пятый день на него прилепили ярлык «компьютерного оккупанта», который «стоил для FT £25 000».

Список рос. Пресса объявила, что Wandii взломал системы Токийского зоопарка и Белого дома. Трудно сказать, что из этого было более серьезным преступлением.

Но у защиты Wandii были свои приемы. Королевский адвокат Иэн Мак-Дональд [Ian MacDonald], помощник адвоката Алистер Келман [Alistair Kelman] и юрист Дебора Трипли [Deborah Tripley] привели к присяге в качестве свидетеля-эксперта профессора Лондонского университета Джеймса Гриффит-Эдвардса [James Griffith-Edwards], авторитетного специалиста по вопросам зависимости и неконтролируемого поведения. Профессор был председателем Национального центра по

<sup>35</sup> Colin Randall, «Teenage Computer Hacker "Caused Worldwide Chaos"», *Daily Telegraph*, 23 february 1993.

p134

Ножка (англ. сленг). Устойчивое выражение «to play footsie» – заигрывание, флирт.

p135

Европейская организация по исследованию и лечению рака.

<sup>36</sup> Местная телефонная компания согласилась сократить счет до £3000, как сообщил суду менеджер информационной системы EORTIC Венсан Пьебеф [Vincent Piedboeuf].

вопросам зависимости и входил в группу ученых, которые сформулировали определение зависимости для Всемирной организации здравоохранения. Никто не смел усомниться в его компетенции.

Профессор осмотрел Wandii и ознакомил суд со своим заключением: Wandii одержим компьютерами, он не способен самостоятельно отказаться от их использования, эта слепая страсть лишает его возможности свободного выбора. Гриффит-Эдвардс сообщил суду, что на полицейских допросах Wandii двенадцать раз повторил одно и то же: «У меня зависимость. Я хотел бы избавиться от нее». Wandii был очень умен, но не мог отказаться от необходимости обыгрывать компьютерные системы безопасности в их собственную игру. Хакер был одержим интеллектуальным вызовом. «Здесь та же самая причина... что движет заядлым игроком», – объяснил профессор потрясенному суду присяжных из трех женщин и девяти мужчин.

«Но этот одержимый, зависимый, одаренный молодой человек никогда не встречался с девушками», – продолжал Гриффит-Эдвардс. В самом деле, Wandii стыдливо признался профессору, что даже не знает, как пригласить девушку на свидание. «Он выглядит очень смущенным, когда его спрашивают о его собственных чувствах. Он просто теряется, когда ему задают вопрос, что он за человек».<sup>37</sup>

Присяжные подались вперед со своих мест, внимательно слушая выдающегося профессора. Еще бы, это было так необычно. Этот образованный человек нашел в сознании юноши удивительные контрасты. Молодой человек был настолько искушен, что мог взломать компьютеры, принадлежавшие самым престижным учреждениям Великобритании и Европы, и в то же время так неопытен, что не имел представления о том, как пригласить девушку на свидание. Человек, зависимый не от алкоголя, героина или «спида»,<sup>[p136]</sup> которые средний гражданин обычно связывает с зависимостью, а от компьютера – машины, которую большинство людей привыкли ассоциировать с детскими играми или с текстовыми программами.

Защита приступила к демонстрации наглядных примеров зависимости Wandii. Мать Wandii, преподаватель английского языка (она одна воспитывала сына), с невероятными трудностями пыталась оттащить его от компьютера и модема. Она попыталась спрятать модем. Он нашел его. Она спрятала его снова, на этот раз в доме бабушки. Он влез к ней в дом и отыскал его. Мать хотела добраться до его компьютера, но он вытолкнул ее из своей мансарды и спустил с лестницы.

Затем пришел счет на £700. Мать отключила электроснабжение. Он подключил его. Она установила телефонный код безопасности, чтобы помешать его звонкам. Он взломал его. Она волновалась из-за того, что он не выходит из дома и не делает обычных для подростка вещей. Он постоянно не спал по ночам, иногда сутки напролет предаваясь хакингу. Она возвращалась с работы и находила его в бессознательном состоянии распростертым на полу гостиной с остекленевшим взглядом. Но это была не смерть, а полное истощение. Он сидел за компьютером, пока не терял сознание. Через какое-то время он приходил в себя и все начиналось сначала.

История Wandii с его собственным признанием в зависимости ошеломили, напугали и в конце концов вызвали сочувствие аудитории в зале суда. Журналисты стали называть его «хакер-отшельник».

Защита Wandii не могла открыто оспаривать доказательства обвинения, поэтому использовала их как свои собственные. Адвокаты продемонстрировали суду, что Wandii не просто вторгся в учреждения, упомянутые обвинением; он пошел гораздо дальше. Он не просто много занимался хакингом – он занимался им слишком много. Самое главное, что защита дала суду повод оправдать подростка, с невинным лицом сидящего перед ними.

Во время процесса внимание журналистов было сконцентрировано в основном на Wandii, но и двое других хакеров не остались в стороне. *Computer Weekly* разузнала, где работает Gandalf, и выложила эту информацию во всей красе на своей первой странице. «Член самой знаменитой хакерской банды Соединенного Королевства, – заявлял еженедельник, – работал над программным обеспечением Barclay Bank».<sup>38</sup> Намек был более чем прозрачен. Gandalf представляет серьезную угрозу безопасности, его нельзя допускать к работе в финансовых учреждениях. Статья взбесила хакеров, но они постарались сконцентрироваться на подготовке к окончательным слушаниям.

<sup>37</sup> Susan Watts, «Trial Haunted by Images of Life in the Twilight Zone», *The Independent*, 19 march 1993.

p136

Speed – стимулирующий наркотик амфетаминовой группы.

<sup>38</sup> Toby Wolpe, «Hacker Worked on Barclay's Software», *Computer Weekly*, 4 march, 1993.

С самого начала процесса у хакеров были проблемы с получением некоторых документов. Pad и Gandalf считали, что отдельные материалы, захваченные полицией во время обысков, могли бы значительно помочь им (например, послания админов, которые благодарили их за указания на недостатки в безопасности их систем). Это факт почему-то не был включен в материалы дела. Когда защитники сделали запрос, чтобы получить доступ к этим материалам, они получили отказ, мотивированный тем, что на оптическом диске содержатся секретные данные. Их отослали к постановлению Генерального атторнея [p137] о закрытой информации. Защитникам сказали, что доказательства вторжений хакеров в военные и правительственные системы неразрывно переплетены с их проникновениями в легкодоступные невинные системы типа JANET. Отделение одного от другого заняло бы слишком много времени.

В конце концов после некоторых споров Pad'у и Gandalf'у было позволено просмотреть и скопировать нужный им материал, разумеется, под контролем полиции. Хакерам пришлось ездить в Лондон, в полицейский участок Холборн, чтобы документировать смягчающие обстоятельства по своему делу. Затем служба уголовного преследования все же смягчилась и позволила выдать материалы на дискетах при условии, что с них не будет сделано ни одной копии, они не покинут помещения адвокатской юридической конторы и будут возвращены по окончании процесса.

Пока дело Wandii продвигалось от разоблачений к преувеличениям, Pad с Gandalf'ом были заняты подготовкой к собственному разбирательству. Каждый день Gandalf приезжал из Ливерпуля в Манчестер, чтобы встретиться с другом. Они покупали пачку газет у местного продавца, а затем отправлялись в офис юриста Pad'а. Быстро просмотрев статьи, касающиеся дела хакеров, они принимались за тщательное просеивание дискет, так неохотно предоставленных обвинением. Они изучали компьютерные материалы под бдительным наблюдением кассира юридической фирмы – самого компетентного в обращении с компьютерами служащего в офисе.

После двух недель в зале суда Саутворк, наслушавшись фантастических историй с обеих сторон о сидящем перед ними пареньке, присяжные по делу Wandii удалились для вынесения решения. Прежде чем они ушли, судья Харрис [Harris] напутствовал их строгим предупреждением: аргумент, что Wandii одержим или зависим, не может служить защитой от обвинений.

Присяжным потребовалось всего девяносто минут, чтобы принять решение; когда же вердикт бы оглашен, зал суда захлестнула волна эмоций.

Невиновен. По всем пунктам.

Мать Wandii расплылась в широкой улыбке и посмотрела на сына. Он тоже улыбался. Команда защиты не могла желать лучшего. Келман сказал журналистам: «Присяжные поняли, что обвинение использовало паровой молот для колки орехов».<sup>39</sup>

Обвинение было ошеломлено, а агенты правоохранительных органов – потрясены. Детектив сержант Барри Донован [Barry Donovan] решил, что это, по меньшей мере, странный вердикт. Ни одно дело за 21 год его службы в полиции не имело такого количества неопровержимых улик, как это, но все же присяжные позволили Wandii ускользнуть.

Средства массовой информации Британии набросились на решение жюри с пронзительными неистовыми воплями, превосходящими первоначальную истерию. «Хакер, разрушивший системы, уходит свободным», – с раздражением сообщала *Guardian*. «С компьютерного гения снято обвинение в тайном сговоре», – говорила *Evening Standard*. «Зависимый от хакинга оправдан», – фыркала *The Times*. Но всех перещеголяла первая страница *Daily Telegraph*: «Подросток, зависимый от компьютера и взломавший Белый Дом, оправдан».

Затем журналисты нанесли главный удар. Кто-то «слил» очередную историю, и выглядела она скверно. В статье *Mail on Sunday* сообщалось, что трое хакеров взломали компьютер Cray в Европейском центре среднесрочных прогнозов погоды в Брэкнелле. Этот компьютер, как и десятки других, должен был затеряться среди прочих неназванных жертв, если бы не одно обстоятельство. Американские власти использовали данные погодного центра, планируя свою атаку против Ирака во время войны в Заливе. В репортаже говорилось, что вторжение хакеров приостановило вычисления компьютера и едва ли не поставило под угрозу всю операцию «Буря в пустыне». Газета утверждала, что хакеры невольно подвергли почти роковой опасности жизни тысяч солдат и международные

p137

Примерно соответствует Генеральному прокурору в других странах.

<sup>39</sup> David Millward, «Computer Hackers Will be Pursued, Vow Police», *Daily Telegraph*, 19 march 1993.



усилия, направленные на обуздание Саддама Хусейна.<sup>40</sup>

Далее газета сообщала, что Государственный департамент США был так разозлен постоянными прорывами британских хакеров, срывающих оборонные планы Пентагона, что направил жалобу английскому премьер-министру Джону Мэйджору. Белый дом поставил вопрос еще более остро, чем Государственный департамент: остановите ваших хакеров, иначе мыотрежем всю Европу от нашего спутника, который обеспечивает трансатлантические цифровые и голосовые телекоммуникации. Кто-то в Британии прислушался к этому требованию, и меньше чем через двенадцать месяцев власти смогли арестовать троих хакеров.

Pad думал, что все эти утверждения – чушь. Он был в машине VAX в Центре погоды как-то раз ночью в течение пары часов, но он никогда не прикасался к Cray. И он, разумеется, не делал ничего, чтобы приостановить работу компьютера. Никаких взламывающих и сканирующих программ, ничего такого, что могло бы вызвать задержку, описанную в статье. Даже если он и был виноват, с трудом верилось, что победа над Ираком зависела от работы одного компьютера в Беркшире.

Поэтому он ломал голову, зачем СМИ запустили эту историю именно сейчас, после того, как Wandii был оправдан, но до того, как им с Gandalf'ом вынесли приговор. Может быть, «зелен виноград»?

Много дней газетные обозреватели, редакторы и авторы писем разглагольствовали о вердикте по делу Wandii и о законности зависимости от хакинга как средства защиты. Некоторые настаивали на том, чтобы владельцы компьютеров сами несли ответственность за безопасность собственных систем. Другие призывали к ужесточению антихакерских законов. Третьи повторяли слова *The Times*, которая заявила в передовой статье, что «закоренелый автомобильный вор этого же возраста почти наверняка получил бы тюремный срок. Оба преступления связаны с неуважением к частной собственности... присяжные, должно быть, упустили из виду оценку серьезности этого преступления».<sup>41</sup>

Дебаты продолжались и ширились, распространяясь за пределы Великобритании. В Гонконге *South China Morning Post* спрашивала: «Может быть, [это] дело стало свидетельством нового социального феномена, когда незрелые и восприимчивые души подвергаются разрушению вследствие длительного контакта с персональным компьютером?» Газета отражала опасения общества, что дело Wandii даст «зеленый свет армии компьютерных хулиганов, которые примутся вволю мародерствовать в мировых базах данных, а после ареста заявят о своем умственном расстройстве».<sup>42</sup>

В день дурака 1993 года, через две с небольшим недели после окончания суда, у Wandii, благодаря любезности *The Guardian*, появился названный его именем синдром.

И пока Wandii, его мать и команда защитников спокойно праздновали победу, СМИ сообщили, что Скотланд-Ярд оплакивает свое поражение, которое было намного серьезнее, чем просто проигрыш конкретного уголовного дела. Группа по компьютерным преступлениям подверглась «реорганизации». Два опытейших офицера из пятерых сотрудников отдела были переведены в другое подразделение. Официально было объявлено, что такие «перестановки» являются обычной процедурой для Скотланд-Ярда. Неофициальная точка зрения гласила, что дело Wandii стало фиаско, напрасной тратой времени и средств и что такое поражение не должно повториться.

На севере, по мере приближения судебного дня, над головами Pad'a и Gandalf'a сгустились черные тучи. Вердикт по делу Wandii мог вызвать ликование у многих в компьютерном андеграунде, но он вовсе не внушал оптимизма двум хакерам 8lgm.

Для Pad'a и Gandalf'a, которые уже признали свою вину, оправдание Wandii было катастрофой.

;) )

Спустя два месяца после того, как в Англии был оправдан Wandii, 12 мая 1993 года Борис Кайзер стоял у скамьи подсудимых, представляя Electron'a на судебном слушании по иску к австралийскому хакеру. Когда он начал говорить, в окружном суде штата Виктория воцарилась тишина.

Высокий дородный мужчина с низким голосом и властной манерой держаться, в традиционной черной мантии, развевающейся вокруг него эхом его выразительной непрерывной жестикуляции, Кайзер, казалось, заполнил собой весь зал суда. Искусный шоумен, он знал, как воздействовать на

<sup>40</sup> Chester Stern, «Hackers Treat to Gulf War Triumph», *Mail on Sunday*, 21 March 1993.

<sup>41</sup> «Crimes of the Intellect – Computer Hacking», editorial, *The Times*, 20 march 1993.

<sup>42</sup> «Owners Must Act to Put End to Computer Hacker "Insanity"», *South China Morning Post*, 30 march 1993.

аудиторию судебных репортеров позади него и на судью напротив.

Electron уже встал со скамьи подсудимых и признал себя виновным по четырнадцати пунктам обвинения по договоренности с офисом Генерального прокурора. В своей обычной манере Кайзер прервал долгую процедуру, когда судебный чиновник зачитывал каждое обвинение и спрашивал Electron'а, признает ли он себя виновным по этому пункту или нет. Нетерпеливо взмахнув рукой, Кайзер попросил судью опустить эти формальности, раз уж его клиент признал свою вину по всем условленным пунктам. Это восклицание было скорее констатацией факта, чем просьбой.

Формальности иска были в общем улажены, оставалось решить вопрос приговора. Electron опасался, что его могут отправить в тюрьму. Несмотря на давление адвокатов Electron'а, офис Генерального прокурора отказался рекомендовать суду приговор без тюремного заключения. Максимум, чего смогли добиться защитники хакера в обмен на его согласие стать государственным свидетелем – прокурор не стал выносить рекомендаций по приговору вообще. Судья был волен принять свое собственное решение без давления со стороны DPP.

Electron нервно теребил обручальное кольцо отца, которое он носил на правой руке. После смерти отца сестра Electron'а начала забирать вещи из родительского дома. Electron'а это не слишком волновало, потому что по-настоящему он дорожил лишь этим кольцом и отцовскими картинами.

Кайзер вызвал нескольких свидетелей, чтобы поспособствовать вынесению более мягкого приговора. Бабушка Electron'а из Квинсленда. Женщина, дружившая с его семьей и отвозившая Electron'а и его сестру в больницу в день смерти отца. Его психиатр, знаменитый Лестер Уолтон [Lester Walton]. Последний, в частности, подчеркнул огромную разницу между двумя возможными путями: тюрьма, которая несомненно усугубит и без того нестабильное душевное состояние молодого человека, или свобода, которая предоставит Electron'у хороший шанс со временем вернуться к нормальной жизни.

Когда Кайзер начал подводить дело к приговору без тюремного срока, Electron услышал, как толпа журналистов позади него яростно застрочила в своих блокнотах. Он хотел повернуться к ним, но побоялся, что судья увидит его длинные волосы, собранные в хвост, который он надежно спрятал за воротом своей тщательно выглаженной белой рубашки.

– Ваша честь, – Кайзер чуть оглянулся назад к судебным репортерам, подогревая их интерес, – мой клиент жил в искусственном мире электронных импульсов.

Царапанье и скрип. Electron мог предугадать с точностью до доли секунды, когда активность карандашей и ручек журналистов достигнет крещендо. Приливы и отливы баса Бориса Кайзера были выдержаны в стиле телевизионного диктора.

Кайзер сказал, что его клиент зависит от компьютера, подобно тому, как алкоголик одержим бутылкой. Царапанье усилилось. «Этот человек, – загремел Кайзер, – никогда не имел намерения нанести ущерб какой-либо системе, украсть деньги или извлечь выгоду для себя. В конечном итоге он не мошенник, он просто играл».

– Я думаю, – заключил адвокат Electron'а страстно, но достаточно медленно, чтобы каждый журналист успел записать его слова, – что моего подзащитного можно назвать мальчиком-с-пальчик, который залез в карманчик, достал барабанчик и сказал: «Какой я хороший мальчик!»

Наступило ожидание. Судья удалился, чтобы взвесить предварительные выступления обеих сторон, семейное положение Electron'а, тот факт, что он решил стать государственным свидетелем обвинения, его компьютерные преступления – все. Electron предоставил обвинению показания против Phoenix'а на девяти страницах. Если дело Phoenix'а дойдет до суда, Electron'у придется занять место свидетеля, чтобы подтвердить эти показания.

Весь следующий месяц, прежде чем вернуться в суд и услышать приговор, Electron думал о том, как он мог бы оспаривать обвинения, отдельные из которых были весьма сомнительны.

В одном случае он был обвинен в нелегальном доступе к общедоступной информации через общедоступную учетную запись. Он вошел в анонимный FTP сервер в университете Хельсинки, чтобы скопировать информацию о DES. Первым местом доступа была взломанная учетная запись в Мельбурнском университете.

Адвокат Electron'а сказал ему: «Опровергни это обвинение – и на его место придут другие. У DPP полно доказательств, и они выдвинут обвинения по другому сайту». Но, несмотря на его слова, Electron считал, что некоторые из государственных улик не выдержали бы перекрестного допроса.

Когда журналисты из Австралии и других стран начали звонить в штаб-квартиру NASA в надежде получить комментарии по поводу спровоцированного хакерами отключения сети, в агентстве ответили, что не имеют понятия, о чем они спрашивают. Не было никаких отключений сети NASA. Пресс-секретарь навел справки и заверил СМИ, что их вопросы поставили руководство NASA в ту-

пик. Даже показания Шэрон Бискенис оказались не так уж надежны. Выяснилось, что она из Lockheed, а в NASA работает по контракту.

В течение этого месяца ожидания Electron столкнулся с большими трудностями из-за толкования Кайзером детского стишка в зале суда. Когда он звонил друзьям, они начинали разговор со слов: «О, да это сам мальчик-с пальчик!»

Они все видели это в ночных новостях – репортаж о Кайзере и его подзащитном. Кайзер выглядел важно, выходя из зала суда, а Electron в круглых очках, как у Джона Леннона, со своими длинными волосами, собранными сзади в хвост, вымученно пытался улыбаться в камеры. Его веснушки скрылись в ярком свете прожекторов, так что казалось, что его черные круглые очки плавают на пустой белой поверхности.

;) )

Через неделю после того, как Electron в Австралии признал себя виновным, Pad и Gandalf в последний раз сели рядом на скамью подсудимых в зале суда Саутворк в Лондоне.

В течение полутора дней мая 1993 года двое хакеров слушали, как адвокаты приводят доводы в их защиту. Они говорили судье, что подзащитные действительно взламывали компьютеры, но их преступления далеко не так серьезны, как это пытается изобразить обвинение. Адвокаты яростно сражались во имя единственной цели – спасти Pad’a и Gandalf’a от тюрьмы.

Вся процедура слушаний далась хакерам довольно тяжело. Причина этого заключалась не только в дурных предчувствиях по поводу предстоящего решения их судьбы. Проблема была в том, что Gandalf смешил Pad’a, а смех в разгар судебного заседания едва ли мог пойти ему на пользу. Pad’a совершенно dokonало многочасовое пребывание рядом с Gandalf’ом, пока юристы с обеих сторон бились над проблемами компьютерного хакинга, которые друзья из 8lgm изучали годами. Pad’у достаточно было украдкой бросить взгляд на Gandalf’a, и вот он уже откашливается и прочищает горло, стараясь удержаться от приступа хохота. Лицо Gandalf’a было издевательски непочтительным.

Сурового вида судья Харрис давно уже мог отправить их в тюрьму, но он все еще ничего не понимал: как и стадо юристов, которые спорили у барьера, судья был – и навсегда остался – вне этого круга. Никто из них даже не представлял, что творится в головах обоих хакеров. Никто из них так и не смог понять, что же такое хакинг: каково дрожать, подкрадываясь к добыче или используя свои мозги на всю катушку, чтобы перехитрить так называемых экспертов, в чем состоит несравненное удовольствие проникновения в столь желанную систему и осознания, что она полностью принадлежит тебе. Не смогли они разобраться, где пролегает та антиавторитарная жилка, которая служит отличным щитом против самых жестоких бурь, бушующих во внешнем мире, и на чем основано чувство товарищества в международном хакерском сообществе в Altos.

Юристы могли не переставая твердить об этом, могли вызывать экспертов в качестве свидетелей и предоставлять судье данные психологического заключения, но никому из них так и не удалось испытывать это самому. Остальная часть присутствующих в зале суда тоже в этом не разбиралась, и Pad с Gandalf’ом, сидя на скамье подсудимых, наблюдали за происходящим словно сквозь прозрачное зеркало из закрытой потайной комнаты.

Больше всего Pad волновался из-за третьего пункта обвинения – того, что угрожал ему одному. На предварительных слушаниях он допустил, что мог причинить вред системе, принадлежащей учреждению, которое в 1990 году называлось Центральная политехническая школа Лондона. Он не наносил никакого ущерба машине посредством, скажем, уничтожения файлов, но противная сторона заявила, что ущерб составил £250 000.

Хакер был уверен, что Политехническая школа никак не могла израсходовать сумму, даже отдаленно напоминающую эту цифру. Он ясно представлял, сколько времени нужно, чтобы очистить систему от следов его пребывания. Но если прокурору удастся убедить судью в своей правоте, хакер может быть осужден на длительное тюремное заключение.

Pad уже настроился отбывать тюремный срок. Еще до того, как был назначен день суда, адвокат предупредил его, что, вполне возможно, оба хакера 8lgm сядут за решетку. После дела Wandii общественное давление на суд стало чудовищным. Полиция расценивала оправдательный приговор по делу Wandii как «лицензию на хакинг», и *The Times* поддержала это заявление.<sup>43</sup> В глазах обывателя

<sup>43</sup> Nick Nuttall, «Hackers Stay Silent on Court Acquittal», *The Times*, 19 march 1993.

это выглядело так, словно судья, председательствующий на суде над Wandii, хотел передать четкое и ясное послание всему хакерскому сообществу.

Pad думал, что если бы они с Gandalf'ом заявили о своей невиновности вместе с Wandii, они тоже могли быть оправданы. Но Pad ни за что не смог бы заставить себя вынести то публичное унижение, через которое пришлось пройти Wandii. Журналисты явно стремились представить всех троих хакеров мертвенно-бледными, изможденными, социально недееспособными чудаковатыми гениями, и адвокаты Wandii в немалой степени приложили к этому руку. Pad не возражал, когда его считали очень умным, но он вовсе не хотел прослыть чудиком. Иногда у него появлялись девушки. Он ходил с друзьями потанцевать или послушать независимые группы в музыкальные клубы Манчестера. Он следил за своим телом, занимаясь дома с гантелями. Скромный – да. Закомплексованный – нет.

Мог ли Pad повернуть дело к зависимости от хакинга? Мог, хотя никогда не считал себя зависимым. Совершенно одержимый, полностью поглощенный? Может быть. Страдающий без компьютера? Да, наверное. Но зависимый? Нет, он так не думал. Кроме того, никто не мог дать стопроцентной гарантии, что защита, построенная на зависимости, сможет спасти его от заявлений обвинения.

Для Pad'a оставалось загадкой, откуда взялось это утверждение о четверти миллиона фунтов. Полицейские просто сказали ему об этом на первом же допросе. Pad пока не видел никаких доказательств, но очень беспокоился по поводу того, как суд отнесется к этому вопросу.

Ответ могла дать компетентная независимая техническая экспертиза. По запросу адвокатов Pad'a и Gandalf'a доктор Питер Миллз [Peter Mills] из Манчестерского университета и доктор Рассел Ллойд [Russell Lloyd] из Лондонской бизнес-школы тщательно проверили огромное количество технических улик, предоставленных в документах обвинения. В независимом заключении на 23 страницах эксперты установили, что хакеры произвели гораздо меньше разрушений, чем было заявлено обвинением. Кроме того, защитники Pad'a попросили доктора Миллза об отдельной проверке и заключении по вещественным доказательствам, на которых базировалось заявление обвинения о большой сумме ущерба.

Доктор Миллз установил, что один из экспертов-свидетелей полиции – служащий British Telecom – сообщил, что рекомендовал полную реконструкцию системы в максимально короткие сроки – и стоило это все недешево. Тем не менее, эксперт ВТ и близко не говорил о том, что сумма ущерба равняется четверти миллиона фунтов, даже не упоминал о том, что вышеупомянутая сумма уже названа официально.

Таким образом, доктор Миллз сделал вывод, что не существует никаких доказательств, поддерживающих заявление об ущербе в £250 000. Более того, любая основательная проверка так называемых улик, предоставленных обвинением, доказывает, что это утверждение попросту смехотворно.

В отдельном заключении доктор Миллз установил, что:

«1) Машина, о которой идет речь, это VAX 6320. Это достаточно мощный мэйн-фрейм, который может поддерживать несколько сотен пользователей.

2) Общий объем файлов занял бы шесть магнитных лент, хотя по причине того, что тип магнитной ленты не уточнен, невозможно точно указать размер файловой системы. Магнитная лента может вмещать от 0,2 гигабайта до 2,5 гигабайта.

3) Машина не работала три дня.

Обладая такой неполной информацией, сложно подсчитать стоимость восстановления машины, хотя общая цифра может быть следующей:

1) Время, потраченное на восстановление системы: 10 человеко-дней из расчета £300 в день = £3000.

2) Время, потерянное пользователями: 30 человеко-дней из расчета £300 в день = £9000.

По моему мнению, общая сумма ущерба едва ли превышает £12 000, и даже эта оценка скорее всего завышена. Я совершенно не могу представить, как могут быть обоснованы убытки в размере £250 000».

Pad'у стало абсолютно ясно, что в заявлении обвинения речь шла вовсе не о нанесенном ущербе. Нужно было тщательно обезопасить систему, то есть полностью перестроить ее. Он предположил, что полиция попыталась повесить стоимость системы безопасности всей компьютерной сети Политехнической школы на плечи одного хакера и назвать ее ущербом. Pad понял, что на самом деле Политехническая школа никогда не теряла такой суммы.

У Pad'a появилась надежда, но вместе с тем он был разгневан. Все это время полиция размахивала

вала перед его носом огромным счетом за несуществующий ущерб. Он ворочался с боку на бок в своей постели по ночам, переживая из-за этого. И вот выясняется, что цифра, выдаваемая за непреложный факт в течение столь долгого времени, оказалась лишь голословным утверждением, не имеющим под собой сколько-нибудь серьезных оснований.

Используя заключение доктора Миллза, защитник Рад'a, королевский адвокат Мухтар Хуссейн [Mukhtar Hussain], в частном порядке вступил в переговоры с прокурором, который в итоге пошел на уступки и согласился свести ущерб к £15 000. Рад полагал, что это все равно было слишком много, но все же лучше, чем четверть миллиона. Не было никакого смысла заглядывать в зубы дареному коню.

Судья Харрис согласился с пересмотренной суммой ущерба.

Положение обвинения могло несколько пошатнуться, но до победы было далеко – прокурор не собирался сдаваться. Во время окончательных двухдневных слушаний Джеймс Ричардсон сказал присяжным и журналистам, что эти двое хакеров взломали около 10 тысяч компьютеров по всему миру. Они побывали в машинах и сетях по меньшей мере пятнадцати стран. Россия. Индия. Франция. Норвегия. Германия. США. Канада. Бельгия. Швеция. Италия. Тайвань. Сингапур. Исландия. Австралия. «Полицейские, расследовавшие дело, говорили, что список мишеней хакеров „можно было читать, как атлас“», – заявил Ричардсон суду.

Рад выслушал список. Это было похоже на правду. Но оставалось неясным, откуда взялось утверждение, что они с Gandalf'ом повредили шведскую телефонную сеть запуском сканера X.25 в сетевой пакет. Эта катастрофа заставила министра правительства Швеции принести извинения по национальному телевидению. Полиция сообщила, что министр в своем публичном выступлении не назвал истинную причину проблемы – британских хакеров.

Рад понятия не имел, о чем они толкуют. Он не делал ничего подобного в шведской системе, и, насколько он знал, Gandalf тоже не был к этому причастен.

Кое-что также вызывало сомнения. Ричардсон сообщил суду, что в общей сложности оба хакера повесили на ничего не подозревающих абонентов самое малое на £25 000 телефонных счетов и нанесли системам ущерб по крайней мере в £123 000.

Откуда эти парни взяли такие цифры? Рад поражался их наглости. Он исследовал доказательства буквально под микроскопом, но так и не увидел ни одного счета, свидетельствующего о том, что хотя бы один сайт потратил какую-то сумму на восстановление «ущерба», причиненного хакерами. Цифры, которыми легко бросались полиция и обвинение, не были оформлены в реальные счета, они брались из воздуха.

И вот в пятницу 21 мая, когда все улики были представлены, судья пригласил суд удалиться для вынесения приговора. Когда через четверть часа он вернулся, Рад по лицу судьи догадался, что сейчас произойдет. Вид судьи ясно говорил хакеру: «Я собираюсь дать вам все то, что *должен был* получить Wandii».

Судья Харрис выразил настроение *The Times*, сказав двум обвиняемым:

«Если бы вашей страстью были автомобили, а не компьютеры, мы назвали бы ваше поведение преступным, и если провести параллель, в чем я не могу себе отказать, то вашу деятельность стоило бы назвать интеллектуальными увеселительными гонками на чужих машинах. Хакинг вовсе не безобидное занятие. Сегодня компьютеры занимают важное место в жизни каждого из нас. Некоторые государственные институты, оказывающие услуги неотложной помощи, зависят в их предоставлении от своих компьютерных систем».<sup>44</sup>

Хакеры должны были получить ясное предупреждение о том, что компьютерные преступления «не будут и не могут быть дозволены», как сказал судья, добавив, что он долго и напряженно думал, прежде чем вынести решение. Он вполне допускал, что хакеры не собирались причинять вред, но обстоятельства повелевали оградить компьютерные системы общества от подобных посягательств, и он не выполнил бы свой общественный долг, если бы не приговорил обоих хакеров к шести месяцам тюремного заключения.

Судья Харрис сказал хакерам, что он выбрал такой способ пресечения, чтобы «наказать вас за то, что вы сделали, и за ущерб, который вы причинили, и в то же время удержать тех, кто может, по-

<sup>44</sup> Melvin Howe, *Press Association Newsfile*, home news section, 21 may 1993.

добно вам, не устоять перед соблазном».

«Вот где был показательный процесс, а вовсе не дело Wandii», – думал Pad, когда полицейские проводили их с Gandalf'ом от скамьи подсудимых к лифту для осужденных, а оттуда в тюремную камеру.

:)

Меньше чем через две недели после того, как Pad и Gandalf были приговорены к тюремному заключению, Electron вернулся в окружной суд штата Виктория, чтобы узнать свою собственную участь.

Стоя у скамьи подсудимых 3 июня 1993 года, Electron чувствовал оцепенение, словно бы заимствованное из сцены суда над Мерсо в романе Камю «Посторонний». Он думал, что сможет справиться со стрессом, но внезапно испытал эффект резко суженного поля зрения, случающийся у истериков, в тот момент, когда смотрел, как судья оглашает его приговор. Он внимательно осмотрел зал суда, но не увидел ни Phoenix'а, ни Nom'а.

После того, как судья Энтони Смит [Anthony Smith] подытожил обвинения, его интерес особенно привлек пункт № 13 – обвинение, связанное с Zardoz. Он на несколько минут углубился в чтение документа, а затем сказал: «На мой взгляд, каждое из преступлений, о которых идет речь в пунктах № 12, 13 и 14, заслуживает тюремного заключения». Это были обвинения в «явной связи» с проникновениями Phoenix'а в NASA, LLNL и CSIRO. Electron снова обвел взглядом зал заседаний. Люди пристально смотрели на него. Их глаза говорили: «Ты сядешь в тюрьму».

«У меня сложилось мнение, что тюремное заключение будет адекватным приговором по каждому из этих преступлений, учитывая их серьезность, – заметил судья Смит, – а также принимая во внимание необходимость продемонстрировать тот факт, что общество не станет терпеть подобного поведения. Наше общество в настоящий момент... все больше... зависит от компьютерных технологий. Ваше поведение несет угрозу использованию этих технологий... Долг суда... внимательно отнестись к тому, чтобы вынесенный вам приговор отразил тяжесть вашего проступка. По каждому из пунктов 12, 13, 14 вы осуждаетесь и приговариваетесь... в общей сложности... к тюремному заключению сроком на шесть месяцев».

Судья сделал паузу, затем продолжил: «Однако я приказываю освободить вас немедленно под залог \$500... Вы освобождаетесь от тюремного заключения при условии хорошего поведения в течение последующих шести месяцев». Затем он назначил Electron'у 300 часов общественных работ и обязал его пройти психиатрическое освидетельствование и лечение.

Electron вздохнул с огромным облегчением.

Говоря о смягчающих обстоятельствах, повлекших за собой условный приговор, судья Смит изобразил Electron'а как личность, зависимую от использования компьютера «почти так же, как алкоголик зависит от бутылки». Борис Кайзер использовал эту аналогию на предварительном слушании скорее на потребу СМИ, но, очевидно, слова адвоката произвели на судью впечатление.

Когда суд удалился, Electron сошел со скамьи подсудимых и пожал руки своим защитникам. После трех лет его проблемы с законом почти закончились. У него оставалась единственный повод для возвращения в суд.

Если Phoenix будет продолжать упрямиться и оспаривать дело, Генеральная прокуратура приведет Electron'а к присяге, чтобы он свидетельствовал против своего бывшего товарища. Если ему придется это сделать, это будет мерзкая сцена.

:)

Заключенные тюрьмы Ее Величества Киркхем на северо-западном побережье Англии неподалеку от Престона знали все о Pad'е и Gandalf'е к моменту их прибытия. Их приветствовали по именам, поскольку все видели телерепортажи, а особенно запомнили тот, где на фоне картинки взлетающего космического челнока рассказывалось, как Gandalf взломал NASA.

Киркхем показался хакерам гораздо приятнее Брикстона, где они провели первые дни заключения, ожидая, когда их отправят дальше. Брикстон полностью соответствовал представлению Pad'а о тюрьме с этажами зарешеченных камер вокруг открытого пространства в центре, которые позволялось покидать (например, на прогулку) только строго по расписанию. В Брикстоне содержались отпетые преступники. К счастью, в ожидании дальнейшей отправки Pad'а и Gandalf'а поместили в одну камеру.

После десяти дней в Брикстоне охранники вывели хакеров из камеры, заковали их в наручники и посадили в тюремный автобус, следующий на ветреное западное побережье.

Во время поездки Pad старался не сводить глаз со своей руки, скованной сверкающей сталью с запястьем Gandalf'a, но не выдерживал и снова бросал взгляд на приятеля-хакера. Задерживая дыхание и отворачиваясь от сдавленной ухмылки Gandalf'a – его друг сам старался не расхохотаться, – Pad боролся. Он пытался держать в напряжении лицевые мускулы, чтобы не смеяться.

Тюрьма Киркхем соблюдала минимум предосторожностей по отношению к своим 632 заключенным. Со своими несколькими свободно стоящими вокруг двора зданиями она была скорее похожа на базу Королевских ВВС времен Второй мировой войны. Здесь не было настоящих стен, только невысокое проволочное ограждение. Pad вскоре узнал, что заключенные спокойно перепрыгивали через него, когда тюрьма начинала их утомлять.

Для тюрьмы Киркхем оказался совсем неплохим местом. Здесь был пруд с утками, лужайка для игры в шары, нечто вроде мини-кинотеатра, где можно было смотреть кино по вечерам, восемь телефонов-автоматов, футбольное поле, площадка для крикета и, самое главное, окрестные луга. Заключенных можно было навещать по будням с 13.10 до 15.40 и по выходным в любое время.

Удача улыбнулась двум хакерам. Они прибыли в тюрьму по одному направлению, и поскольку никто не возражал, то они стали соседями по камере. Приговор был вынесен в мае, поэтому им придется пробыть здесь все лето. Если они будут «хорошо себя вести» и не ввязываться в ссоры с другими заключенными, их освободят через три месяца.

Как и в любой тюрьме, в Киркхеме разделяли заключенных, которые не могли ужиться друг с другом. В основном зеки хотели знать, за что ты попал сюда и не совершил ли ты преступления на сексуальной почве. В тюрьме не любили сексуальных преступников. Pad'у рассказали, как однажды группа заключенных пыталась повесить одного такого, считая, что он насильник. На самом деле этот бедняга просто отказался платить подушный налог.

К счастью для Pad'a и Gandalf'a, все в Киркхеме знали, за что они здесь. В конце первой недели пребывания в тюрьме они вернулись в свою комнату и увидели над дверью надпись: «Штаб-квартира NASA».

Другие заключенные с облегченным режимом содержания знали, что такое хакинг, и у них была куча идей, как заработать на этом. Большинство узников Киркхема угодили сюда за мелкие кражи, мошенничества с кредитными картами и прочие незначительные преступления. Был здесь и один фрикер, который прибыл в тюрьму в один день с Pad'ом и Gandalf'ом. Он получил восемь месяцев тюрьмы – на два месяца больше, чем хакеры 8lgm, – и Pad все гадал, какое же послание было адресовано андеграунду на этот раз.

Несмотря на все свои старания, двое из 8lgm не смогли вполне приспособиться к тюремным порядкам. По вечерам другие заключенные убивали время, сражаясь в пул или покуривая травку. В комнате 8lgm недалеко от холла Gandalf сидел на своей койке, штудировав учебник по VMS. Pad читал компьютерный иллюстрированный журнал и слушал какую-нибудь независимую музыку, чаще всего кассету Babes in Toyland. Пародируя фильмы на тюремную тему, хакеры отмечали на стене камеры дни своего пребывания за решеткой – четыре продольных черты, затем одна перечеркивающая их линия. Кое-что другое они, впрочем, тоже писали на стенах.

Длинные солнечные летние дни плавно перетекали один в другой по мере того, как Pad и Gandalf входили в ритм тюремной жизни. Утренняя поверка в 8.30, чтобы убедиться, что никто из заключенных не вышел прогуляться за ограждение. Затем через лужайку для игры в шары на завтрак – фасоль, бекон, яйца, тосты и сосиска. Прогулка к теплицам – туда их назначили на работу.

Работа была несложной – ковыряться в земле. Прополоть молодой салат-латук, полить сладкий перец, пересадить помидорную рассаду. Когда ближе к полудню в теплицах становилось слишком жарко, Pad и Gandalf выбирались наружу, чтобы глотнуть свежего воздуха. Они часто говорили о девушках, отпуская на эту тему грубые мальчишеские шутки, а иногда беседовали о своих подругах более серьезно. Когда жара нарастала, они усаживались поудобнее, кайфуя у стены теплицы.

После ланча Pad и Gandalf еще немного работали в теплице, а затем иногда отправлялись погулять по полям вокруг тюрьмы. Сначала футбольное поле, а за ним выгон с коровами.

Pad был приятным парнем благодаря своему непринужденному стилю и чувству юмора. Но хорошо к нему относиться было не то же самое, что знать его самого и его настроение, часто глубоко спрятанное внутри. А Gandalf знал и понимал его. С Gandalf'ом все было легко. В долгих прогулках на солнце разговор тек так же свободно, как свободно дул легкий ветерок.

Во время прогулок по полям Pad часто надевал свою джинсовую куртку. Большая часть одежды на тюремном складе была грязно-синего цвета, но Pad'у повезло с отличной модной курткой, и он

носил ее постоянно.

Часами гуляя по периметру тюремной территории, Pad обнаружил, как просто сбежать из тюрьмы, но если подумать – в этом не было никакого смысла. Он знал, что за этим последует – полиция поймает тебя и вернет назад. Но твой срок возрастет.

Раз в неделю родители Pad'a приезжали провести его, но несколько драгоценных часов свидания были нужны скорее отцу с матерью, чем самому Pad'у. Он уверял их, что все в порядке, и когда они смотрели в его глаза и видели, что это правда, они почти переставали волноваться. Родители привозили ему новости из дома. Однажды они рассказали ему, что его компьютерное оборудование возвращено одним из полицейских, который принимал участие в налете на их дом.

Полисмен спросил у матери Pad'a, как ему живется в тюрьме. «Неплохо, – ответила она. – Тюрьма оказалась не так ужасна, как он думал». Лицо полицейского сморщилось в неодобрительной гримасе. Он явно рассчитывал услышать о том, что Pad терпит невыносимые лишения.

Не прошло и трех месяцев, как загоревшие во время прогулок по лугам Pad и Gandalf вышли на свободу.

:)

Напряжение между отцом и матерью Phoenix'a могло показаться почти ощутимым случайному свидетелю, который решил бы понаблюдать за ними в зале суда. Они сидели далеко друг от друга, но это отнюдь не умаляло молчаливой враждебности, повисшей в воздухе, словно облако. Разведенные родители Phoenix'a резко контрастировали с приемными родителями Nom'a, пожилой парой из пригорода, которые отлично подходили друг другу.

25 августа 1993 года, в среду, Phoenix и Nom признали себя виновными по пятнадцати и двум пунктам обвинения соответственно. Общее количество доказательств обвинения, риск и цена разбирательства дела полным составом суда и необходимость продолжать жить вынудили хакеров забыть о своих амбициях. Electron'у не было нужды являться в суд для дачи показаний.

На предварительных слушаниях, продолжавшихся два дня, адвокат Phoenix'a Дайсон Хор-Лэйси [Dyson Hore-Lacy] довольно долго изображал неприятные обстоятельства развода родителей его подзащитного, стремясь произвести на судью впечатление. Лучшим шансом избавить Phoenix'a от тюремного срока было продемонстрировать, что он был вынужден искать утешения за компьютером во время невыносимого и горького расставания и развода родителей. Кроме того, защита изобразила Phoenix'a блестящим молодым человеком, который сбился с пути истинного, но теперь вернулся на него – у него была постоянная работа и нормальная жизнь.

Офис Генерального прокурора жестко взялся за Phoenix'a. Они жаждали добиться для него тюремного срока и настойчиво выставляли самонадеянным хвастуном. Суд прослушал магнитофонную запись, на которой Phoenix звонил гуру компьютерной безопасности Эдварду Де-Харту [Edward DeHart] из Computer Emergency Response Team [[p138](#)] университета Карнеги-Меллон, чтобы похвастаться своими подвигами в области взлома систем компьютерной безопасности. Phoenix предложил Де-Харту войти в свой компьютер, а затем шаг за шагом начал пробираться в него, используя ошибку безопасности passwd-f. По иронии судьбы эту ошибку обнаружил Electron и показал ее Phoenix'у, но тот и не думал упоминать об этом в разговоре с Де-Хартом.

Глава регионального отдела АФП по борьбе с компьютерными преступлениями сержант Кен Дэй тоже присутствовал в суде в этот день. Он ни за что не собирался пропустить такое событие. Тот, кто заметил напряженность между родителями Phoenix'a, мог также почувствовать и скрытую враждебность между ним и Дэем – чувство, которое полицейский никак не проявлял к остальным хакерам Realm.

Дэй, невысокий аккуратный мужчина, производивший впечатление внутренней силы, явно испытывал острую неприязнь к Phoenix'у. По общему мнению, это чувство было взаимным. Дэй был хладнокровным профессионалом и никогда бы не позволил себе выразить эту неприязнь публично. О его чувствах можно было догадаться лишь по нервному напряжению лицевых мускулов.

6 октября 1993 года Nom и Phoenix предстали на скамье подсудимых, готовые выслушать свой приговор. Судья Смит с суровым выражением лица начал заседание с перечисления обвинений против обоих хакеров и происхождения Realm. Закончив перечисление, судья обрушился на Phoenix'a с



желчной речью: «В вашем поведении... нет ничего такого, что могло бы вызвать восхищение, и любая мысль об этом подлежит немедленному осуждению. Вы указывали на [слабость] некоторых системных администраторов... [но] это было скорее отражением вашей самонадеянности и демонстрацией вашего кажущегося превосходства, нежели актом альтруизма с вашей стороны. Вы кичились тем, что сделали или собирались сделать... Ваше поведение говорит о вашей наглости, открытом вызове и намерении нанести вред системе. [Вы] причиняли разрушения различным системам в течение долгого времени».

Хотя казалось, что после такой речи судья намерен строго покарать Phoenix'a, принимая решение, он значительно умерил свой гнев. Судья попытался найти компромисс между тем, что он считал необходимым устрашением, созданием прецедента для будущих приговоров по хакерским делам в Австралии и конкретными аспектами именно этого дела. В конце концов еще и еще раз проанализировав все аргументы, он принял решение.

– У меня нет сомнений, что некоторые круги нашего общества считают тюремное заключение единственно возможным решением. Я разделяю эту точку зрения. Но после долгих размышлений... я пришел к выводу, что немедленное заключение под стражу не является необходимым.

На лицах друзей и близких хакеров появилось облегчение, когда судья назначил Phoenix'у 500 часов общественных работ в течение двух лет и в качестве залога хорошего поведения – \$1000 на 12 месяцев. Nom получил 200 часов общественных работ и залог \$500 на полгода.

Когда Phoenix выходил из зала суда, какой-то высокий худой парень появился в проходе прямо перед ним.

– Поздравляю, – сказал незнакомец, чьи длинные волосы завивались у плеч легкими кудрями.

– Спасибо, – ответил Phoenix, напрягая память в попытке идентифицировать это мальчишеское лицо, которое было едва ли старше его собственного. – Я тебя знаю?

– Типа того, – ответил незнакомец. – Я Mendax. Я вроде занимаюсь тем же, что и ты, только покруче.

## 8

### The international subversives

*Слышишь вокруг*

*Зловещий звук.*

**Песня «Maralinga», альбом «10, 9, 8, 7, 6, 5, 4, 3, 2, 1» группы Midnight Oil<sup>45</sup>**

Prime Suspect позвонил Mendax'у и предложил ему новое приключение. Он обнаружил странную систему под названием NMELH1 (произносится «Эн-Мелли-Эйч-1»), и сейчас настало время ее исследовать. Он разузнал телефонные номера для доступа и создал список номеров в другой взломанной системе.

Mendax посмотрел на клочок бумаги в руке и подумал о названии компьютерной системы.

N означало Northern Telecom, канадскую компанию с объемом годовых продаж в размере \$8 миллиардов. NorTel, как называли эту компанию, продавал тысячи сверхсложных коммутаторов и другого подобного телефонного оборудования многим крупнейшим телефонным компаниям во всем мире. Melly, несомненно, значило, что система находится в Мельбурне. Что касается H-1, с этим было сложнее, но Mendax предполагал, что это, вероятно, означает host-1 – компьютерный сайт № 1.

Prime Suspect пробудил интерес Mendax'a. Mendax провел много часов, экспериментируя с командами внутри компьютеров, которые контролировали телефонные коммутаторы. В конечном итоге эти набег были не более чем рекогносцировкой, применением метода проб и ошибок в надежде наткнуться на что-то интересное. Это совсем не тот случай, когда единственная ошибка в компьютере или неверно посланная команда в телефонном коммутаторе в деловом центре Мельбурна могли разрушить всю систему – более 10 тысяч телефонных линий – и вызвать мгновенный хаос.

Как раз этого и хотели избежать International Subversives. Трое хакеров IS – Mendax, Prime Suspect и Трах – знали, что произошло с известными членами компьютерного подполья в Англии и в Австралии. У хакеров IS имелись три веские причины, чтобы действовать очень осторожно.

Phoenix. Nom. И Electron.

---

<sup>45</sup> Слова и музыка: James Moginie / Peter Garrett. © Copyright 1982 Sprint Music. Administered for the World – Warner / Chappell Music Australia Pty Ltd. Used by Permission.

Но нельзя ли научиться, подумал Mendax, манипулировать телефонным коммутатором, который стоит миллион долларов, прочитав техническую документацию производителя? Как велики шансы найти эти тщательно скрывающиеся документы в сети NorTel?

А вдруг он сможет найти исходный код NorTel – программное обеспечение, предназначенное для управления специальными телефонными коммутаторами, такими как модель DMS-100. Это код мог находиться в компьютере всемирной сети NorTel. Хакер с доступом сможет создать свой собственный черный ход – скрытую ошибку в системе безопасности – еще до того, как компания отправит новый продукт своим клиентам.

Имея ясное понимание принципов работы оборудования NorTel плюс черный ход, установленный в каждом компоненте программного обеспечения определенного продукта, хакер смог бы контролировать каждый новый телефонный коммутатор NorTel от Бостона до Бахрейна. Вот это власть! Что произойдет, если отключить 10 тысяч телефонов в Рио-де-Жанейро или дать возможность позвонить бесплатно 5 тысячам жителей Нью-Йорка, или прослушивать частные разговоры в Брисбене? Мир телекоммуникаций откроется перед тобой, как устрица.

;) )

Как и их предшественники, трое хакеров IS начали свою деятельность на подмостках мельбурнских BBS. Mendax познакомился с Tгах'ом на доске объявлений Electric Dreams примерно в 1998 году. Вскоре он встретил Prime Suspect'a на Megaworks – тогда он был известен как Control Reset. Когда Mendax создал собственную BBS в своем доме в Текоме (отдаленный холмистый пригород Мельбурна), он пригласил обоих хакеров заходить на его A Cute Paranoia

[p139]

 в любой момент, когда они смогут прорваться через его единственную телефонную линию.

Обоим хакерам нравилось бывать на BBS Mendax'a, потому что она была более закрыта по сравнению с другими досками объявлений. Со временем они обменялись номерами телефонов, но лишь для того, чтобы непосредственно связываться модем с модемом. Они месяцами звонили друг другу, обмениваясь мыслями через экраны мониторов. Наконец, в конце 1990 года девятнадцатилетний Mendax позвонил двадцатичетырехлетнему Tгах'у, чтобы поговорить с ним обычным способом. В начале 1991 года к ним присоединился и семнадцатилетний Prime Suspect.

Tгах был несколько эксцентричен и, похоже, страдал от какого-то душевного расстройства. Он отказывался ездить в город и однажды упомянул о своем визите к психиатру. Но Mendax привык думать, что самые интересные люди всегда немного необычны, а Tгах был и тем, и другим.

Mendax и Tгах решили, что у них мало общего. Они оба происходили из бедных, но образованных семей, и оба жили в отдаленных пригородах. Но детство они провели совершенно по-разному.

Родители Tгах'a эмигрировали в Австралию из Европы. И его отец, компьютерный техник на пенсии, и мать разговаривали с немецким акцентом. Отец Tгах'a был полновластным правителем в доме, а Tгах был – единственным сыном.

Mendax же к своим пятнадцати годам пожил в дюжине разных мест, включая Перт, Магнетик-Айленд, Брисбен, Таунсвилл, Сидней, Аделаида-Хиллс и вереницу прибрежных городков на севере Нового Южного Уэльса и Западной Австралии. К этому возрасту он успел поучиться в куче разных школ.

Его мать ушла из своего дома в Квинсленде, когда ей стукнуло семнадцать, и она скопила достаточно денег от продажи своих картин, чтобы купить мотоцикл, палатку и дорожную карту Австралии. Махнув на прощанье рукой своим изумленным родителям-ученым, она скрылась в лучах заходящего солнца. Проехав примерно две тысячи километров, она прибыла в Сидней и присоединилась к буйно цветущему контркультурному сообществу. Она стала актрисой и полюбила молодого бунтаря, с которым познакомилась на демонстрации против войны во Вьетнаме.

Через год после рождения Mendax'a его родители разошлись. Когда Mendax'у исполнилось два года, его мать вышла замуж за собрата по искусству. Потом было много беспокойных лет, переезды из города в город по мере того, как его родители исследовали левое крыло богемной субкультуры 70-х годов. Мальчиком он был окружен актерами. Его отчим режиссировал пьесы, а мать занималась гримом, костюмами и декорациями.

Однажды ночью в Аделаиде, когда Mendax'у было около четырех лет, его мать с одним приятелем возвращались с антиядерного митинга. Приятель утверждал, что у него есть научное доказательство того, что британское правительство проводило подземные ядерные испытания огромной мощности в Маралинге, пустынной местности на северо-западе Южной Австралии.

В 1984 году Королевская комиссия с опозданием признала, что между 1953 и 1963 годами правительство Великобритании действительно испытывало в этой местности ядерные бомбы, согнав пять тысяч аборигенов с их исконных земель. В декабре 1993 года после многих лет обмана британское правительство согласилось выплатить 20 миллионов фунтов стерлингов, чтобы очистить более 200 квадратных километров зараженных земель. Но в 1968 году правительство Мензиса [p140] отрицало причастность Великобритании к заражению этих земель. В 70-е годы само правительство Австралии не признавало факт ядерных испытаний в Маралинге.

Мать Mendax'а и ее приятель ехали по пригороду Аделаиды, имея при себе те самые доказательства трагедии в Маралинге. Вдруг они заметили, что их преследует какая-то машина. Они попытались оторваться, но безуспешно. Друг, нервничая, сказал, что он должен передать эти доказательства одному журналисту из Аделаиды до того, как полиция схватит его. Мать Mendax'а быстро свернула в переулок и приятель выскочил из машины. Она поехала дальше, уводя за собой полицейский хвост.

Полицейские в штатском вскоре догнали ее, обыскали машину и спросили, куда делся ее друг и что произошло на митинге. Она не проявила желания помочь, и один из копов сказал ей: «Вы тут с ребенком в два часа ночи. Я думаю, вам не стоит соваться в политику, леди. Могут сказать, что вы негодная мать».

Через несколько дней после этой угрозы ее приятель появился в их доме, покрытый уже сходящими кровоподтеками. Он сказал, что полицейские избили его, а затем арестовали, подбросив ему наркотики. Он заявил, что уходит из политики.

Как бы там ни было, мать Mendax'а и ее муж продолжали заниматься театром. Юный Mendax никогда не мечтал о том, чтобы сбежать из дома с бродячим цирком – он и так вел жизнь странствующих менестрелей. Хотя режиссер-постановщик был хорошим отцом, он оказался алкоголиком. Вскоре после того, как Mendax'у исполнилось девять лет, его мать рассталась с мужем, а затем развелась.

После этого у матери Mendax'а случился бурный роман с музыкантом-любителем. Mendax боялся нового отчима и считал его психопатом, склонным к насилию. У этого человека было пять разных удостоверений личности в бумажнике. Вся его биография была вымышленной, вплоть до страны, где он родился. Когда отношения закончились, снова началась жизнь на колесах, но это путешествие разительно отличалось от прежней счастливой и беззаботной одиссеи. На этот раз Mendax'у и его семье на самом деле пришлось скрываться от угрозы физической расправы. В конце концов, после игры в прятки под вымышленными именами в разных концах страны, семья Mendax'а осела в окрестностях Мельбурна.

Mendax ушел из дома в семнадцать лет, после того, как получил конфиденциальную информацию о предстоящем полицейском налете. Он стер данные на дисках, сжег распечатки и ушел. Через неделю нагрянула полиция штата, обыскала его комнату, но ничего не нашла. Он женился на своей подруге, умной, но замкнутой и эмоционально неустойчивой шестнадцатилетней девочке, с которой он познакомился через общего друга. Через год у них родился ребенок.

Со многими из своих друзей Mendax познакомился в компьютерном андеграунде. Он обнаружил, что Тгах – любитель поболтать, и они могли разговаривать по пять часов кряду. С другой стороны, Prime Suspect не очень жаловал телефонные беседы.

Спокойный и замкнутый, Prime Suspect всегда стремился побыстрее закончить разговор. Mendax и сам был застенчив от природы, поэтому их разговоры часто состояли из продолжительных пауз. К тому времени, когда трое хакеров впервые встретились лично в доме Тгах'а, Mendax считал Prime Suspect'а гораздо большим, чем просто приятелем-хакером в замкнутом кружке IS. Mendax считал его другом.

Prime Suspect производил впечатление пай-мальчика. Большинство видело в нем прилежного ученика выпускного класса, готовящегося перейти в университет из своей школы для высшего сред-

него класса. В школах для мальчиков просто не принято ожидать меньшего от своих питомцев, и возможность поступления в TAFE – профессионально-технический колледж – не рассматривается даже в качестве варианта. Цель – университет. Любой ученик, который не смог ее добиться, потихоньку заметался под ковер, как крошки, оставшиеся после обеда.

Семейная обстановка в доме Prime Suspect'a совершенно не отражала внешнего лоска его школы. Его отец-фармаколог и мать-медсестра находились в разгаре неприятного бракоразводного процесса, когда у его отца была обнаружена последняя стадия рака. В этой тяжелой и пропитанной враждебностью атмосфере восьмилетнего Prime Suspect'a несколько раз возили в больницу к постели отца, чтобы попрощаться с ним.

На протяжении всех детских и отроческих лет Prime Suspect'a, его мать проявляла постоянное недовольство и раздражение главным образом по причине незавидного финансового положения семьи. Когда ему было восемь лет, его шестнадцатилетняя сестра ушла из дома, переехала в Перт и перестала поддерживать всякие отношения с матерью. Prime Suspect чувствовал, что он должен быть одновременно ребенком и отцом. Из-за этого он в чем-то вырос быстрее, но в другом оставался совершенно незрелым.

Prime Suspect спасался от окружающей враждебности в своей комнате. Когда в тринадцать лет он купил свой первый компьютер, Apple IIe, он решил, что это гораздо лучшая компания, чем все его родственники. Школьные компьютеры не представляли для него особого интереса, потому что не имели связи с внешним миром через модем. После того, как Prime Suspect прочитал в газете общества пользователей Apple о BBS, он скопил на свой собственный модем и стал посещать различные доски объявлений.

Тем не менее, учеба в школе предоставляла неплохие возможности для бунта, хотя бы и анонимного, и он постоянно затевал какие-нибудь проделки. Мало кому из учителей приходило в голову заподозрить послушного аккуратного мальчика, и его редко уличали. Природа одарила Prime Suspect'a абсолютно невинным лицом. Истинные черты этого высокого худенького паренька с кудрявыми каштановыми волосами проявлялись лишь в злой усмешке эльфа, которая иногда ненадолго проскальзывала по его лицу. Учителя говорили матери Prime Suspect'a, что с его умственными способностями он мог бы добиться больших успехов, но все же им было не на что жаловаться.

К десятому классу он стал серьезным хакером и проводил у компьютера каждую свободную минуту. Иногда он прогуливал занятия и часто сдавал задания позже установленного срока. Ему все труднее становилось постоянно изобретать новые и новые отговорки, и иногда он представлял, что говорит учителям правду. «Извините, но я не написал это сочинение в две тысячи слов, потому что прошлой ночью я по самые уши был в NASA». Эта мысль очень веселила его.

Девушки казались ему нежелательной помехой, только отвлекающей от хакинга. Иногда он заговаривал с какой-нибудь девчонкой на вечеринке, после чего друзья спрашивали, почему он не назначил ей свидание. Prime Suspect не обращал на это внимания. Истинная причина заключалась в том, что он стремился поскорее вернуться домой к компьютеру, но он никогда не обсуждал свою деятельность в школе даже с Mentat'ом.

Mentat был другом Force. Он иногда посещал Realm и учился двумя годами старше Prime Suspect'a. В сущности, он никогда не проявлял интереса к тому, чтобы затеять разговор с таким юнцом, как Prime Suspect. Молодой хакер не обращал на это внимания. Он знал, какими несдержанными могут быть хакеры, не хотел видеть их поблизости и был счастлив держать в секрете свою личную жизнь.

Еще до ареста хакеров Realm Phoenix как-то позвонил ему в два часа ночи и предложил немедленно встретиться с ним и с Nom'ом. Мать Prime Suspect'a, разбуженная телефонным звонком, встала в дверях его комнаты и принялась отчитывать сына за то, что он позволяет «своим друзьям» звонить так поздно. Phoenix бубнил ему в одно ухо, мать ворчала в другое, и Prime Suspect решил, что это плохая идея. Он отказал Phoenix'у и закрыл дверь перед носом матери.

Все же иногда он общался по телефону с Powerspike. Дерзкие взгляды старшего хакера и его нахальный смех нравились ему. Но за исключением этих коротких бесед, Prime Suspect старался не говорить по телефону с теми, кто не входил в International Subversives, особенно когда они с Mendax'ом готовились к вторжению в сверхсекретные военные компьютеры.

Используя программу под названием Sycophant, [p141] написанную Mendax'ом, хакеры IS по-

вели массированную атаку на армию США. Они разделили Sycophant между восемью атакующими машинами, в основном выбирая системы в университетах, таких как Австралийский государственный университет или Техасский университет. Они навели все восемь машин на цель и выстрелили. В течение шести часов восемь машин штурмовали тысячи компьютеров. Иногда хакеры собирали урожай в виде 100 тысяч учетных записей за одну ночь.

Используя Sycophant, они нахрапом взяли несколько машин Unix в компьютерной сети, чтобы напасть на *весь Интернет* в целом.

И это было только начало. Они побывали в таком количестве сайтов, что часто не могли вспомнить, что за компьютер они сейчас взламывают. Места, которые удержались в их памяти, можно было читать как справочник «Кто есть кто?» в американском военно-промышленном комплексе. Командный пункт седьмого полка ВВС США в Пентагоне. Стэнфордский исследовательский институт в Калифорнии. Военный центр надводного флота в Вирджинии. Завод тактических авиационных систем для ВВС корпорации Lockheed Martin в Техасе. Корпорация Unisys в Блю-Белл, Пенсильвания. Годдардовский центр управления космическими полетами, NASA. Motorola Inc. в Иллинойсе. TRW Inc. в Редон-добич в Калифорнии. Alcoa в Питтсбурге. Panasonic Corp в Нью-Джерси. Военно-инженерная база подводного флота США. Siemens-Nixdorf Information System в Массачусетсе. Securities Industry Automation Corp в Нью-Йорке. Национальная лаборатория имени Лоренса Ливермора в Калифорнии. Исследовательский институт Bell Communications, Нью-Джерси. Исследовательский центр корпорации Херох в Пало-Альто, Калифорния.

Когда хакеры IS достигли такого уровня мастерства, до которого никогда не поднимались хакеры из Realm, они поняли, что такой прогресс связан со значительным риском, и отошли от основного хакерского сообщества Австралии. Вскоре они образовали замкнутый круг и общались только друг с другом.

Поражение хакеров Realm не напугало следующее поколение хакеров. Им пришлось лишь глубже уйти в подполье.

Весной 1991 года Prime Suspect и Mendax начали погоню за доступом в компьютер Network Information Center (NIC)<sup>[p142]</sup> Министерства обороны США – возможно, самый важный компьютер в Интернете. Однажды ночью, пока они оба по-дружески болтали онлайн в компьютере Мельбурнского университета, Prime Suspect спокойно работал за вторым монитором, стараясь проникнуть в ns.nic.ddn.mil, машину Министерства обороны США, тесно связанную с NIC. Он полагал, что эта машина и NIC могут «доверять» одна другой, – и он сможет использовать это доверие, чтобы попасть в NIC. А NIC мог *все*.

NIC присваивал доменные имена – .com или .net в конце сетевых адресов – во всем Интернете. NIC также контролировал внутреннюю оборонную сеть данных армии США, известную как MILNET.

Кроме этого, NIC публиковал коммуникационные протокольные стандарты для всего Интернета. Эти технические спецификации, называемые RFC (Request for Comments), позволяли одному компьютеру разговаривать с другим в Интернете. Defense Data Network Security Bulletins<sup>[p143]</sup> Министерства обороны США, эквивалент рекомендаций CERT, тоже распространялись из машины NIC.

И возможно, самое главное – NIC контролировал функцию обратного кодирования в Интернете. Когда кто-то подключается к сайту через Интернет, то обычно набирает название сайта – скажем, ariel.unimelb.edu.au в Мельбурнском университете. Затем компьютер переводит буквенное название в цифровой адрес – IP-адрес – в данном случае 128.250.20.3. Всем компьютерам в Интернете нужен такой адрес, чтобы передавать пакеты данных в компьютер конечного назначения. NIC решает, как компьютеры Интернета будут переводить буквенные названия в IP-адреса и наоборот.

Если ты контролируешь NIC, ты получаешь безграничную власть в Интернете. Например, ты можешь просто заставить Австралию исчезнуть. Или превратить ее в Бразилию. Направив все адреса Интернета, заканчивающиеся на .au – указатель австралийских сайтов – в Бразилию, ты мог отрезать австралийскую часть Интернета от остального мира и направить весь сетевой трафик Австралии в Южную Америку. Более того, изменив назначение всех доменных имен, ты мог фактически остановить поток информации между всеми странами в Интернете.

---

p142

Сетевой информационный центр.

p143

Бюллетени по безопасности сети по передаче оборонных данных.

Единственным способом помешать такой власти был набор полного цифрового IP-адреса вместо обычного буквенного. Но немногие люди знали цифровой эквивалент своих буквенных адресов, доходящий до двенадцати цифр, и еще меньше людей использовали его.

Контроль над NIC давал и другие выгоды. Получи этот контроль, и ты – обладатель универсального виртуального ключа к любому компьютеру в Интернете, который «доверял» другому. Большинство машин доверяли, по меньшей мере, одной системе.

Когда бы один компьютер ни подключался к другому в Сети, обе машины осуществляют специальный ознакомительно-приветственный процесс. Принимающий компьютер смотрит на входящую машину и задает ей несколько вопросов. Как называется входящая машина? Есть ли у нее позволение соединяться со мной? Каким образом запрограммировано мое «доверие» к этой машине – должен ли я ослабить собственную безопасность, чтобы подключиться к ней?

Принимающий компьютер отвечает на эти вопросы, базируясь на информации, предоставленной NIC. Все это означает, что, контролируя NIC, ты мог представить каждый компьютер в Сети как машину, достойную доверия компьютера, который ты хочешь взломать. Безопасность часто зависела от названия компьютера, и NIC фактически контролировал это название.

Когда Prime Suspect сумел проникнуть в родственную NIC систему, он сказал об этом Mendax'у и дал ему доступ в этот компьютер. Затем каждый хакер начал собственную атаку на NIC. Когда Mendax наконец получил доступ к NIC, он был опьянен этой силой. Prime Suspect сделал это примерно в тот же момент, но другим способом. Они оба были там.

Внутри NIC Mendax начал строить черный ход – способ вернуться в компьютер позже – на тот случай, если какой-нибудь админ залатает щели в системе безопасности, которые использовали хакеры, чтобы проникнуть в машину. Теперь, если Mendax соединится с информационным сервером системы Defense Data Network (DDN)[[p144](#)] и введет login 0, он получит мгновенный и невидимый корневой доступ к NIC.

Завершив эту операцию, он осмотрелся вокруг – нет ли чего интересенького почитать? В одном файле содержалось нечто похожее на список спутников и координаты микроволновой антенны – широта, долгота, частота передачи. Эти координаты теоретически могли позволить любому составить полную карту коммуникационных устройств, используемых для движения компьютерных данных Министерства обороны США по всему миру.

Mendax также проник в Координационный центр безопасности MILNET, где хранилась вся информация о любом возможном инциденте в системе безопасности MILNET. Такие компьютеры (в основном TOPS-20, производимые DEC) были снабжены отличными автоматическими программами безопасности. Любые необычные события приводили к появлению автоматического сообщения о нарушении безопасности. Кто-то слишком долго подключается к машине. Большое количество неудачных попыток регистрации, говорящее о стремлении угадать пароль. Два человека, регистрирующиеся на одном уровне в одно и то же время. Сигнальный колокольчик зазвенит, и локальный компьютер немедленно пошлет оповещение о нарушении системы безопасности в центр безопасности MILNET, где оно будет приобщено к «горячему списку».

Mendax перелистывал страницу за страницей докладов по безопасности MILNET на своем мониторе. Большинство из них были ни о чем – пользователи MILNET периодически спотыкались о сигнальную проволоку безопасности. Но одно из сообщений с американского военного сайта в Германии выделялось на общем фоне. Оно исходило не от компьютера. Оно было от человеческого существа. Системный администратор докладывал, что кто-то периодически пытался взломать его машину и в конце концов ему это удалось. Админ постарался, без особой надежды на успех, проследить соединение наглеца до исходного пункта. К его удивлению, оказалось, что оно исходит из другой системы MILNET. Пролистав другие файлы, Mendax нашел письмо, подтверждавшее, что нападение действительно было совершено из MILNET. Его глаза раскрывались все шире, по мере того как он читал. Военные хакеры из США взломали системы MILNET в качестве практики, и никто не побеспокоился о том, чтобы предупредить системных администраторов о месте атаки.

Mendax не мог в это поверить. Американские военные взламывали свои собственные компьютеры. Это открытие наводило на другие, более тревожные мысли. Если американская армия взламывала свои собственные компьютеры в качестве тренировки, то что же она делала с компьютерами других стран?

Расширенное руководство фрикера.

Ok in this file you will learn the in's and out's of MFC signalling He all know about CCITT 5. But what is MFC? Hell first of all it stands tor Multi-Frequency Code and is the Backward tones you hear when you play your Forward CCITT 5 tones. MFC tones when you know how to use then with CCITT 5 tones will let you do anything a Fault Operator and Call Operator can do. They are however very difficult to understand. They aren't simple ST-NUMBBR-KP type routing. So you will have to do some heavy programming to cope with the different signalling groups. So lets get started.

Index

Chapter 1. Frequency Table

Chapter 2. CCITT 5 Routing Table

Chapter 3. MFC Signalling Table

Chapter 4. Signalling Groups

Chapter 5. Horking it Together

Chapter 6. Other types of Signalling

Chapter 7. Hang Up Time

%%%%%%%%%

Chapter 1. Frequency Table

Tone Table

I Forward I Backward I KEY I CCITT #5 IMPC I KEY – I-1-1-1-1-

1 I 1380 I 1500 I 1140 I 1020 I 1

2 I 1380 I 1620 I 1140 I 900 I 2

– I in routing programs i use the following I defined keys.

3 I 1500 I 1620 I 1020 I 900! 3 I Key ICCITTIMFC I See Chapter 6.

4 I 1380 I 1740 I 1140 [780 I 4 I-!-1-1 For other

Signalling

5 I 1500 I 1740 I 1020 I 780 I 5 I A I 11 [11 I Frequencies.

6 I 1620 I 1740 I 900! 780! 6 I B I 12 I 12 I

7 I 1380 I 1860 I 1140 I 660! 7 [C I KP I 13 I

8 I 1500 I 1860 I 1020 I 660! 8 I D I KP2 I 14 I

9 I 1620 I 1860 I 900 coll|0t 9 I E I ST I 15 I

0 I 1740 I 1860 I 780! 660! 0 I-1-1-1

11 I 1380 I 1980 I 1140 I 540! 11 I This is for ease of programiting only. It is

coll|0 I 12 I 1500 I 1980 I 1020 I 540 I 12 I best to have a single key switch to change KP I 1620 I 1980 I 900

coll|0 I 13 I between Forward and

Backward frequencies.

KP2 I 1740 I 1980 I 780! 540! 14 I So note. ST I 1860 I 1980 I 660 coll|1 I 15 I SF = Switch

Forward –1-1-1-[-1-1 SB = Switch Backward

NUMBER=Telephone number CCITT 5 Half Tones An example would translate from

– I-I-I-I-I SF-E-1-123456-\*

1380 11500!1620!1740! 1860 I 1980! to

– 1-1-1-1-1-1 Switch Forward tones

1140!1020! 900! 780! 660! 540 I ST-(1)-NUMBER-KP

MFC Half Tones

These half tones do strange things in the middle of routing. Like alarms going off and numbers Re-routed STD. Note that single frequencies will be bracketed. [] as below.

For example.

ST-(1)-0011-(CO – (AC)-NUMBER-KP-(OPD)-[1850]

The above is the formula for TASI line breaking.

CC=Country Code

AC=Area Code

OPD=Other Party Disconnects

[1850] The frequency in hz to get into a TASI control line.

Chapter 2. CCITT 5 Routing Table

NUMBER-KP

This is the simplest way to route a Phone Number. Also the only way alot of Australian Phreaker route. Depending on the



Signalling Trunk you may not be able to route a call over seas. Tor example STD Signalling Trunk.

11-(Not used)

It's use in CCITT 5 Routing is at present unknown. However some Telecom Publications show it's MFC counterpart used in routing to Interception Centre and used by Incoming Operators.

12-(1)-ID

To

12-(9)-ID

These could be Non-Axe to Axe Exchange Switching signals. 12-(AC)– HUMBER

This routing is only allowed to Axe Exchanges from Son-Axe Exchanges.

This is very useful for Axe test numbers which are blocked from other Exchanges.

12-(KP)-1D

12-(KP2)-ID

12-(ST)-ID

These could be more Non-Axe to Axe Exchange Switching signals.

KP-(Not Used)

It's use in CCITT 5 Routing is at present unknown.

KP2-(I)-3D's

To

KP2-(9)-3D's

The 3 digits maybe used as switches between Exchanges. For exaapla

Bwitch 456 Exchange to except ARE type routing or SXS type routing.

The signalling between Exchanges still being CCITT 5 and MFC but the internal switching is different.

KP2-(0)-NUMBER

It's use in CCITT 5 Routing is at present unknown.

KP2-(11)-3D's

KP2-(12)-3D's

Maybe Exchange switches.

KP2-(12)-(0)-NUMBER

It's use in CCITT 5 Routing is at present unknown.

KP2-(KP)-3D's

KP2-(KP2)-3D'S

Maybe Exchange switches.

KP2-(ST)-(No CCITT 5 or MFC signals)

This maybe used as an echo suppressor.

ST-(1)-NUMBER

Another Routing method.

ST-(2)-4D's

ST-(3)-4D's

These maybe used to store or switch the lat 4 Digits on a given number. ST-(4)-ID

To

ST-(0)-ID ST-(11)-ID ST-(12)-ID ST-(KP)– ID ST– (KP2)– ID ST– (ST)-1D Maybe Exchange switches.

Chapter 3. MFC Signalling Table

HPC Signals have multiple function, so you'll have to know what is sent and keep track of it to know what your signals are going do next. How all MFC Signalling start with the A Signals.

Now here is a run down.

A Signals

A1 Next Digit.

A2 Restart.

A3 End Of Selection. Change to B.

A4 Terminating Exchange MFC. 5 Digit Length. Change to 2A.

A5 Terminating Exchange MFC. 6 Digit Length. Change to 2A.

A6 Terminating Exchange MFC. 7 Digit Length. Change to 2A.

A7 Terminating Exchange SxS. 5 Digit Length. Change to 3A.

A8 Terminating Exchange SxS. 6 Digit Length, change to 3A.  
A9 Terminating Exchange SxS. 7 Digit Length. Change to 3A.  
AO Terminating Exchange SxS. Length Unknown. Change to 3A.  
2A Signal\*  
!!A1 Next Digit.  
::A2 Restart.  
::A3 End of Selection. Change to B.  
::A4 Start Decadic. 1st Digit.  
::A5 Start Decadic. 2nd Digit.  
;!A6 Start Decadic. 3rd Digit.  
:!A7 Waiting place. Next Digit. Change to 3A.  
::a8 Waiting Place. Restart. Change to 3A.  
,', A9 Waiting Place. same digit. change to 3A.  
:! A0 waiting place, previous Digit. Change to 3A.  
3A Signals  
SA1 Next Digit.  
1A2 Restart.  
iA3 End of Selection. Change to B.  
(A4 Start Decadic. 1st Digit.  
J .A5 Start Decadic. 2nd Digit.  
'A6 Start Decadic. 3rd Digit.  
'&A7 Start Decadic. 4th Digit.  
iA8 Start Decadic. 5th Digit.  
'A9 Send A-party Category. Change to C.  
iAO Send Previous Digit.  
B Signals  
M1 Idle Sub.  
M2 Busy Sub.  
M3 No Throwout.  
M4 Congestion.  
M5 Idle – Non Metering.  
MO B-party Control. No time-out.  
M7 B-party Control. Non chargeable.  
MH Re-route to interception.  
M') Send A-party Category. Change to C.  
M() Send previous Digit.  
C Signals  
C1 Next Digit.  
C2 Restart.  
C3 End of Selection. Change to B.  
C4 Start Decadic. 1st Digit. (Ult. Congestion)  
C5 Start Decadic. 2nd Digit. (Ult. Zone of Origin)  
C6 Start Decadic. 3rd Digit.  
C7 Start Decadic. 4th Digit.  
C8 Start Decadic. 5th Digit.  
C9 Send A-party Number.  
CO Send Previous Digit.  
thatsit.

У электронного журнала *The International Subversive* была очень простая редакторская политика. Экземпляр журнала мог получить только тот, кто написал для него «статью». Такая политика отлично защищала от «сосунков» – неумелых и неопытных хакеров, которые могли случайно привлечь внимание полиции. Сосунки также были способны злоупотребить хакерскими и фрикерскими техниками, в результате чего Telecom мог закрыть лазейки в системе безопасности. Таким образом, читателями IS были всего три человека.

Для не-хакера IS выглядел полной абракадаброй – даже телефонный справочник было читать намного интереснее. Но для члена компьютерного подполья IS был картой острова сокровищ. Уме-

лый хакер мог пройти по следам модемных телефонных номеров и§7

Prime Suspect и Mendax всегда очень переживали по поводу следов соединений, ведущих от университетских модемов, которые они использовали как стартовые площадки. Поэтому фрикерские таланты Тгах'а были для них просто подарком небес.

Тгах сделал свое великое открытие случайно. Он использовал телефонный спринтер – простую компьютерную программу, которая автоматически набирает ряд телефонных номеров в поисках модемов. Увеличивая громкость звука на своем модеме в тот момент, когда его компьютер набирал номер, производивший впечатление мертвого или несуществующего, он иногда слышал негромкие щелчки после сообщения об отключении. Эти шумы звучали как слабое сердцебиение.

Из любопытства он стал экспериментировать с этими странными номерами и вскоре обнаружил, что это отключенные телефонные линии, которые пока еще не подсоединены. Тгах принялся думать о том, как бы он мог использовать эти странные номера. После того, как он прочитал документ, который Mendax нашел в Англии и скачал в BBS The Devil's Playground,<sup>[p147]</sup> его осенила идея. В документе была информация о сигнальных импульсах CCITT #5 – международном стандарте языка, который используется для международной телефонной связи.

Когда ты звонишь из Австралии в США, звонок проходит через локальный телефонный коммутатор в международный шлюз в Австралии. Оттуда звонок путешествует в американский коммутатор. Сигнальные тоны CCITT представляют собой специальные импульсы, которые используются для соединения этих коммутаторов.

Австралийская Telecom применяла последнюю версию этого стандарта, R2, для своих внутренних коммутаторов. Telecom назвала этот стандарт MFC.<sup>[p148]</sup> Когда, предположим, Тгах звонил Mendax'у, его коммутатор просил коммутатор Mendax'а поговорить с телефоном Mendax'а, используя эти тоны. Коммутатор Mendax'а «отвечал», иногда сообщая, что телефон Mendax'а занят или отключен. Тоны Telecom – парные с аудиочастотами – не существовали в обычных телефонах, и их невозможно было создать, просто нажимая на кнопки домашнего телефонного аппарата.

Тгах написал программу, которая позволила его компьютеру Amstrad генерировать эти специальные тоны, а затем посылать их по телефонной линии. В порыве, которые многие в андеграунде потом называли гениальным озарением, Тгах начал фиксировать, что в точности делал каждый тон. Это была трудная задача, поскольку каждый тон мог означать несколько разных вещей на разных фазах «разговора» между двумя коммутаторами.

Увлеченный этим новым способом набора, Тгах выпотрошил мусорные корзины Telecom и нашел там регистрационный список MFC – бесценную часть этой головоломки. Используя список вместе с файлами, полученными от иностранных фрикерсов, и потратив невероятное количество кропотливого ручного труда, Тгах постепенно изучил язык австралийских телефонных коммутаторов. Затем он обучил этому языку свой компьютер.

Тгах попытался снова позвонить по одному из телефонных номеров с «сердцебиениями». Он пропустил свои специальные, сгенерированные на компьютере импульсы через усилитель. Проще говоря, он получил возможность одурачить другие коммутаторы, прикинувшись локальным коммутатором Telecom. Тгах заставил свой коммутатор впустить его по исходящему каналу, используемому для прокладывания маршрута к отключенному телефонному номеру.

Теперь Тгах мог позвонить куда угодно – словно бы он звонил из промежуточной точки между его собственным телефоном и отключенным телефонным номером. Если, например, он звонил на модем Мельбурнского университета, а линия прослеживалась, номер его домашнего телефона не отображался на записи слежения. Никто не получал счетов за звонки Тгах'а, потому что они были призраками в телефонной системе.

Тгах продолжал оттачивать свое мастерство в обращении с телефоном и коммутатором. Он разбирал свой телефон по кусочкам бесчисленное количество раз, внимательно рассматривая каждую деталь, пока не начинал ясно понимать, как она работает. Через несколько месяцев он мог делать гораздо более серьезные вещи, нежели просто бесплатно звонить. Например, он мог заставить телефонную систему подумать, что он пришел с определенного телефонного номера.

Они с Mendax'ом шутили, что если бы им захотелось позвонить на какой-нибудь опасный сайт,

---

p147

Песочница дьявола.

p148

Multifrequency code – мультичастотный код.

они использовали бы технику Тгах'а, чтобы направить след соединения – и счет – в Отдел компьютерных преступлений АФП в Мельбурне.

Все трое IS хакеров подозревали, что АФП идет за ними по пятам. Шатаясь в компьютерной системе, принадлежащей Джеффу Хьюстону [Geoff Huston], который, по существу, управлял всем австралийским Интернетом, они следили за объединенными усилиями полиции и Australian Academic and Research Network (AARNET)/[p149](#) по их выслеживанию.

Крейг Уоррен [Craig Warren] из университета Дикин написал Хьюстону, техническому менеджеру AARNET, о нападениях хакеров на университетские системы. Хьюстон направил копию письма Питеру Элфорду [Peter Elford], своему помощнику по управлению AARNET. Хакеры взломали систему Хьюстона и тоже прочитали письмо:

From G.Huston@aarnet.edu.au Mon Sep 23 09:40:43 1991  
Received: from [150.203.6.67] by jatz.aarnet.edu.au with  
SMTP id AA002 65 (5. 65 + /IDA-1. 3. 5 for pte900);  
Mon 23 Sep 91 09:40:39 +1000  
Date: Mon, 23 Sep 91 09:40:39 +1000  
Message-Id: <9109222340.AA00265@jatz.aarnet.edu.au>;  
To: pte900@aarnet.edu.au  
From: G.Houston@aai-net.edu.au  
Subject: Re: Visitors log Thursday Night – Friday Morning  
Status: RO  
&gt;Date: Sun, 22 Sep 91 19:29:13 +1000  
&gt;From: Craig Warren <C.Warren@deakin.OZ.AU>&gt;  
&gt;

&gt; Хочу подсказать вам мыслишку насчет того, что произошло с тех пор, как мы общались в последний раз...

&gt;

&gt;Мы связывались с сержантом Кеном Дзем из Федеральной полиции около 100 раз за последнюю неделю. С помощью наших коллег из Уоррнембула нам удалось установить соединения на линиях модемного набора и на линиях Austrac с терминалом сервера capella.cc.deakin.AZ.AU, который оставался открытым для внешнего доступа.

&gt;

&gt;В пятницу после полудня нам удалось проследить звонок в район Уоррнембул. Полиции известно имя абонента. Мы думаем, что в это замешаны и другие, поскольку мы видели одновременно троих людей, действующих в одно и то же время. Это «подозреваемые» студенты из RMIT, и, возможно, студенты из Дикина тоже в этом участвуют.

&gt;

&gt;Когда я закончил работу в пятницу вечером, в машине продолжалась бурная деятельность, и полиция вместе с Telecom отслеживали еще один номер.

&gt;

&gt;Завтра утром я поговорю со всеми участвующими сторонами, но, похоже, что у нас будут имена двоих или троих из тех, кто в этом замешан. На этой стадии мы, возможно, прекратим доступ «capella» в AARNet и предоставим полиции сделать свое дело и преследовать этих людей по закону.

&gt;

&gt;Возможно, вы «получите удовольствие»:-)), если узнаете, что не только вы подверглись атаке. Я знаю, по крайней мере, 2 других сайта в Виктории, на которые были совершены нападения. Один из них принадлежит Telecom, и он помог втянуть в это весь Telecom!

&gt;Я буду информировать вас в ближайшее время по мере развития событий.

&gt;

&gt;С уважением Крейг

«Другие» – это, конечно, хакеры IS. Ничто не может сравниться с удовольствием от чтения о собственных проделках в почте того, кто отвечает за безопасность.

Mendax и Prime Suspect постоянно посещали компьютер ANU, чтобы почитать там почту с новостями по проблемам безопасности. Хотя университеты обычно не владели никакой особенной информацией, лишь базовыми сведениями, в них иногда можно было найти материалы о том, насколько близко подобралась АФП к хакерам IS.

Еще более интересными для Mendax'а были его предварительные набеги на Telecom. Используя номер модема, найденный Prime Suspect'ом, он набрал номер того, что казалось ему коммутатором Lonsdale компании Telecom в деловом районе Мельбурна. Когда его модем подключился к другому, он увидел лишь пустой экран. Он попытался применить несколько базовых команд, которые могли бы помочь ему понять, что происходит с системой:

```
Login.  
List.  
Attach.
```

Но коммутатор компьютера сохранял молчание.

Mendax запустил написанную им программу, чтобы выстрелить любым распознаваемым символом с клавиатуры – или всеми 256 – по другой машине. Снова ничего. Затем он попробовал сигнал взлома – клавишу Amiga и букву B, нажатые одновременно. Ответ получился такой:

Он применил другой хакерский инструмент – программу, которая сбросила 200 общих команд в другую машину. Ничего. Наконец, он попытался набрать logout.[\[p150\]](#) И увидел в ответ:

```
error, not logged on
```

Ага, подумал Mendax. Нужна команда logon, а не login.

```
:logon
```

Коммутатор Telecom запросил имя пользователя. Теперь Mendax'у оставалось только придумать имя пользователя и пароль.

Он знал, что Telecom использует оборудование NorTel. Более чем вероятно, что специалисты из NorTel обучали персонал Telecom, а для этого им был нужен доступ. А если большое количество техников из NorTel работали на многих различных телефонных коммутаторах, то все время передавать им пароли безопасности было бы довольно сложной задачей. Скорее всего люди из Telecom и NorTel взяли что-нибудь простое и универсальное. Какой пароль лучше всего подойдет под это описание?

```
username: nortel  
password: nortel
```

Это сработало.

К сожалению, Mendax не знал, какие команды использовать внутри машины, и там не было документации, которая могла бы ему помочь. У телефонного коммутатора был свой собственный язык, не похожий ни на один из тех, что он встречал раньше.

После нескольких часов упорных поисков Mendax составил список команд, которые могли сработать в коммутаторе компьютера. Коммутатор, похоже, контролировал все специальные шестизначные телефонные номера, начинающиеся с 13, например номер службы заказа авиабилетов или доставки пиццы. Это была Intelligent Network[\[p152\]](#) Telecom, выполнявшая множество специальных

---

p150  
Выход (англ.).

p151  
Ошибка, не вошел (англ.).

p152  
«Умная» сеть.

задач, включая маршрутинговые звонки на максимально близкий филиал вышеназванной организации. Mendax просмотрел список команд, нашел в нем RANGE и установил, что эта команда позволяет выбрать все телефонные номера в определенном ряду. Он выбрал тысячу номеров, начинающихся на 634, которые, как он считал, принадлежали офису Telecom на Куин-стрит.

Теперь нужно было проверить команду. Mendax хотел сделать что-нибудь безобидное, что не отключило бы навсегда 1000 линий. Было почти семь утра, и ему надо было сворачиваться, прежде чем сотрудники Telecom начнут приходить на работу.

Команда RING выглядела достаточно безвредной. Он могла набирать номера ряда последовательно, один за другим. Mendax мог контролировать этот процесс. Он ввел команду. Ничего не произошло. Затем несколько точек начали медленно проходить по его экрану:

.....  
RUNG

Система просто набрала всю тысячу номеров одновременно. Тысяча телефонов зазвонила разом.

А что, если какой-нибудь инженер-трудоголик прикатил на работу в Telecom пораньше, чтобы выполнить свое дурацкое задание? Что, если он просто сидел перед своим стандартным телекомовским металлическим столом с пластиковым стаканчиком плохого растворимого кофе, как вдруг все телефоны в небоскребе одновременно зазвонили? Насколько подозрительно это будет выглядеть? Mendax подумал, что пора убираться оттуда.

На обратном пути он вывел из строя все логины для линии модема, по которой он пришел. Таким образом, никто не сможет понять, что он сделал. На самом деле, он надеялся, что никто не узнает, что он вообще использовал эту линию.

:)

Prime Suspect не думал, что могут быть какие-то неприятности из-за его исследования компьютерной системы NorTel. Многие компьютерные сайты помещали на экранах у входа предупреждения о незаконности взлома системы, но восемнадцатилетний хакер не считал себя захватчиком. В его глазах «захватчиком» был тот, кто питал дурные намерения – например, нанести системе вред, – а он не собирался делать ничего плохого. Он был просто посетителем.

Mendax зарегистрировался в системе NMELN1 с помощью учетной записи, полученной от Prime Suspect'a, и немедленно осмотрелся, чтобы увидеть, кто еще находится онлайн. Кроме Prime Suspect'a, в системе было еще девять человек, но только трое из них что-то делали в настоящий момент у своих терминалов.

Prime Suspect и Mendax торопились обогнать друг друга в получении доступа к системе. Может быть, хакеры IS и не склонны были хвастать своими завоеваниями в подполье, но у каждого из них была соревновательная жилка, когда дело доходило до того, кто первый получит контроль над системой. Это была не ожесточенная гонка конкурентов, а обычное приятельское соревнование.

Mendax пошарил вокруг и понял, что корневую директорию, содержащую файл с паролем, очень легко переписать. Это была хорошая новость, и при помощи некоторых быстрых манипуляций он сможет добавить что-то к корневой директории. В более защищенной системе пользователи без привилегий не смогли бы сделать ничего подобного. Mendax также мог скопировать все, что ему нужно, из указателя на свой собственный сайт и изменить названия поддиректорий в главной корневой директории. Все эти возможности были очень важными, потому что они предоставляли ему шанс создать «троян».

Названный по имени деревянного коня, который послужил уловкой для взятия Трои, «троян» был излюбленным приемом большинства компьютерных хакеров. Хакер попросту хитростью убеждает компьютерную систему или пользователя в том, что слегка измененный файл (или директория) – «троян» – вполне легитимен. Однако «троян» содержит ложную информацию, которая дурачит компьютер и заставляет его делать то, что хочет хакер. Кроме этого, «троян» легко может обманом вытянуть из законного пользователя ценную информацию, такую как его имя и пароль.

Mendax создал новую директорию и скопировал в нее содержимое правильной директории ETC, где хранились файлы пароля. Пароли были зашифрованы, так что не было никакого смысла

смотреть на них, коли их невозможно было прочесть. Вместо этого хакер выбрал случайного законного пользователя – назовем его Джо – и стер его пароль. Не имея пароля, Mendax мог без всяких проблем зарегистрироваться, как Джо.

Но Джо был средним пользователем. У него не было корневого доступа, который и был так нужен Mendax'у. Но, как и любой другой пользователь системы, Джо обладал идентификационным номером пользователя. Mendax изменил его идентификационный номер на 0 – магическую цифру. Пользователь с id номером 0 имел корневой доступ. Джо теперь приобрел власть, которой обычно обладали только системные администраторы. Разумеется, Mendax мог поискать в списке пользователя, который уже имел корневой доступ, но в системе были операторы, и если бы еще один оператор с корневым доступом зарегистрировался через линии модемного набора, это могло бы вызвать подозрения. Лучшая линия защиты состояла в том, чтобы не привлекать к себе внимания кого бы то ни было в системе.

Следующая проблема заключалась в том, чтобы заменить оригинальную директорию ETC на «троян». У Mendax'а не было прав, чтобы стереть правильную директорию ETC, но он мог изменить название директории. Так что он изменил название директории ETC на такое название, которое компьютерная система не могла распознать. Без доступа к своему списку пользователей, компьютер не мог осуществлять большинство своих функций. Никто не мог зарегистрироваться, посмотреть, кто еще есть в системе и отправить электронную почту. Mendax'у пришлось работать очень быстро. В любую минуту кто угодно мог заметить, что в системе серьезные проблемы.

Mendax переименовал свою директорию-троян в ETC. Система мгновенно считала ложную директорию, включая уже несуществующий пароль Джо и его повышенный статус привилегированного пользователя. Mendax снова вошел в систему, теперь уже как Джо.

Меньше чем за пять минут двадцатилетний парень, почти не имеющий специального образования, используя слабенький компьютер стоимостью \$700 и мучительно неповоротливый модем, завоевал мельбурнскую компьютерную систему одной из самых больших телекоммуникационных компаний в мире.

Все же нужно было еще стереть кое-какие следы. Настоящий Джо, входя в систему в очередной раз, мог удивиться, почему она не запрашивает его пароль. Он также мог быть поражен тем, что получил фантастические привилегии. Поэтому Mendax использовал свой статус суперпользователя, чтобы стереть файл-троян ETC и вернуть оригинал на прежнее место. Он также уничтожил записи, показывающие, что кто-то когда-то регистрировался как Джо.

Чтобы быть уверенным, что он сможет в будущем вернуться в эту систему с привилегиями суперпользователя, Mendax установил специальную программу, которая автоматически предоставляла ему корневой доступ. Он спрятал программу во внутренностях системы и для пущей надежности придал ей специальную функцию, так что она могла быть активирована только секретным нажатием клавиши.

Mendax первым пробил корневой уровень на NMELH1, но Prime Suspect ненадолго отстал от него. Тгах присоединился к ним чуть позже. Когда они начали осматриваться по сторонам, то не могли поверить своей находке. У этой системы была самая странная структура, с какой они когда-либо сталкивались.

Большинство больших сетей имеют иерархическую структуру. Кроме того, большинство из них содержит адреса других систем в сети, как правило, тех, которые ближе всего расположены во внешней сети.

Но сеть NorTel обладала другой структурой. Находка хакеров IS представляла собой сеть без иерархии. Это было абсолютно плоское пустое пространство. Были и другие причины считать ее странной. Каждая компьютерная система этой сети содержала адрес каждого другого компьютера, а во всемирной сети NorTel было больше 11 тысяч компьютеров. То, на что изумленно глядели хакеры, выглядело, как гигантский внутрикорпоративный Интернет, плоский, как блин.

Mendax'у раньше приходилось видеть много плоских структур, но только не такого масштаба. Это было чудно. В иерархических структурах гораздо легче понять, где находятся самые важные компьютерные системы и информация. Но в этой структуре, где все системы были, в сущности, равны, хакерам придется приложить гораздо более значительные усилия, прокладывая свой путь по сети. Как можно определить, что находится в системе – список приглашенных на рождественскую вечеринку или секретные разработки новой продукции NorTel?

Сеть NorTel была окружена брандмауэром. Это означало, что – в идеале – в нее нет доступа из внешнего мира. Mendax придерживался мнения, что этот факт делал ее более уязвимой для хакеров, которым удалось проникнуть в нее с помощью модемного набора. Безопасность сети NorTel выгля-

дела относительно ослабленной потому, что было фактически невозможно пробить ее через Интернет. Проскользнув через черный ход, хакеры обнаружили, что они способны совершить налет на любые сайты NorTel, от Сент-Килда-Роуд в Мельбурне до штаб-квартиры корпорации в Торонто.

Это была фантастика. Вся эта огромная, доверчивая сеть компьютерных сайтов – на кончиках их пальцев. У молодых хакеров поднялось настроение в предвкушении будущих открытий. Один из них описывал это состояние как чувства «человека, потерпевшего кораблекрушение и выброшенного на берег острова Таити, населенного 11 тысячами девственниц, созревших для съема».

Они обнаружили YP, или «желтые страницы», – базу данных, связанную с четырьмя сотнями компьютерных сайтов, которые зависели от этой базы данных в отношении файлов паролей. Mendax'у удалось получить доступ в базу данных YP, и это дало ему моментальный контроль над 400 компьютерными системами. Круто.

Одна из систем принадлежала старшему администратору NorTel по компьютерной безопасности, и Mendax сразу же устремился проверить его почтовый ящик. Корреспонденция рассмешила его.

В письме из австралийского офиса шла речь о том, что австралийский Telecom нуждается в доступе к CORWAN, большой корпоративной сети NorTel. Этот доступ позволил бы связать CORWAN и маленькую сеть Telecom. Это выглядело достаточно разумно, если учесть тот факт, что, с тех пор как Telecom сотрудничал с NorTel, их персонал постоянно общался в активном режиме.

Канадский менеджер по безопасности ответил отказом на эту просьбу, потому что в сети Telecom было слишком много хакеров.

Слишком много хакеров в Telecom? Сейчас это выглядело смешно. Здесь сидел хакер, который читал очень важную почту эксперта по компьютерной безопасности NorTel, считавшего, что сеть Telecom слишком уж открыта. На самом деле Mendax проник в системы Telecom через CORWAN, а не наоборот.

Возможно, для того чтобы доказать свою правоту, Mendax решил взломать пароли в системе NorTel. Он собрал 1004 файла паролей из сайтов NorTel, запустил THC, свою программу взлома паролей, и начал охотиться в сети за какими-нибудь свободными компьютерами, чтобы они сделали для него эту работу. Он обнаружил коллекцию из 40 компьютеров Sun, расположенных, видимо, в Канаде, и установил на них свою программу.

На этих Sun4 THC работала очень быстро. Программа использовала словарь в 60 тысяч слов, «одоженный» у какого-то парня из армии США, занимавшегося вопросами криптографии и взлома паролей. В ней также применялся «особенно совершенный алгоритм быстрого шифрования», разработанный Эриком Янгом [Eric Young], ученым из Квинсленда. Программа THC работала в 30 раз быстрее, чем стандартный алгоритм.

Используя все 40 компьютеров, Mendax обрушился на списки паролей, вооруженный аж 40 тысячами запросов в секунду. Парочка Sun пала под таким бешеным натиском, но остальные удержались на своих местах. Секретные пароли начали трескаться, как яичная скорлупа. За несколько часов Mendax взломал 5000 паролей, сотня из которых вела к корневым учетным записям. Теперь у него был доступ к тысячам компьютеров NorTel по всему миру.

В этих системах можно было получить преотличнейшие призы. Имея контроль над компьютерными системами большой компании, ты фактически контролировал саму компанию. Хочешь личные пароли каждого служащего для парадного хода в офис? Вот они – онлайн.

Как насчет доступа к платежным ведомостям компании? Ты мог узнать, сколько зарабатывает каждый сотрудник. Более того, ты мог спокойно выдать себя за служащего и заплатить самому себе неплохой единовременный бонус посредством электронного перевода. Естественно, были и другие, менее очевидные пути сделать деньги, такие как шпионаж.

Mendax мог запросто найти крайне важную информацию о разработках новой продукции NorTel и продать ее. Для такой компании, как NorTel, которая тратила более миллиарда долларов ежегодно на исследования и развитие, утечка информации о ее новых технологиях могла стать роковой. Можно даже не шпионить за новыми разработками. Достаточно собирать информацию о бизнес-стратегии компании. Имея доступ к любым внутренним докладом старших менеджеров, хакер мог получить ценную служебную информацию о рынках и ценах. Конкуренты могли щедро заплатить за такие сведения.

И это было только начало того, что мог сделать злонамеренный или жаждущий наживы хакер. Во многих компаниях автоматика на заводах-производителях контролируется компьютерами. Малейшие изменения в программе автоматизированного процесса могут разрушить всю цепочку изделий – и производящих их автоматов – на много миллионов долларов.

Но у хакеров IS не было и мысли об информационном шпионаже. На самом деле, несмотря на



их незавидное финансовое положение студентов или, в случае Тгах'а, молодого человека, начинающего свою карьеру с нуля, ни один из них не стал бы продавать информацию, добытую хакингом. С их точки зрения, такое поведение было мерзким и заслуживало презрения – это портило все приключение и противоречило их этике. Они считали себя разведчиками, а не наемными корпоративными шпионами.

Хотя сеть NorTel и окружала глухая стена, она имела одно соединение с Интернетом. Соединение осуществлялось через систему под названием BRNGATE, Bell-Northern Research's Gateway. Bell-Northern – это дочерняя компания NorTel, занимавшаяся исследованиями. Соединение с внешним электронным миром было очень ограниченным, но выглядело любопытно. Проблема была в том, как туда попасть.

Mendax пустился на поиски входа. Его программа взлома паролей могла поработать и в этой системе, но существовали и другие, более тонкие способы получить пароль, чем грубая сила программы-взломщика.

Системные администраторы иногда посылают пароли по e-mail. Обычно это связано с большим риском для безопасности, но система NorTel была отгорожена от Интернета, поэтому админы думали, что у них нет причин опасаться хакеров. Кроме того, в такой большой корпорации, охватившей несколько континентов, администратор не всегда может просто спуститься вниз, чтобы лично вручить новому менеджеру компании его пароль. А ретивый новичок вряд ли захочет ждать неделю, пока пароль придет по почте со скоростью улитки.

В сети NorTel почтовый буфер, где хранилась электронная почта, был зачастую разделен между примерно двадцатью компьютерными системами. Такая структура предоставляла Mendax'у большие преимущества. Ему нужно было только пробиться в почтовый буфер и приказать компьютеру искать комбинации слов, такие как «BRNGATE» и «password», или найти имя системного администратора BRNGATE, и тогда, по всей вероятности, можно будет собирать драгоценные кусочки информации в виде новых паролей.

Mendax использовал пароль, полученный этим методом, чтобы войти в BRNGATE и осмотреться. Уровень, на котором он оказался, имел очень узкие полномочия и не мог получить корневой доступ к системе. Например, он не мог FTP-ировать файлы из-за пределов NorTel обычным путем. (Среди пользователей Интернета FTP используется и как существительное, и как глагол: FTP-ировать программу означает перекинуть ее копию с компьютерного сайта на ваш собственный. Нет ничего незаконного в том, чтобы FTP-ировать что-то для себя, и миллионы людей в Интернете делают это совершенно легально.)

Mendax'у стало ясно, что админы сети NorTel позволяют большинству пользователей FTP-ировать что-то из Интернета, но предостерегают их против хранения скопированных файлов на компьютерных сайтах. Они хранились в специально отведенном месте в BRNGATE, и системные администраторы, как карантинные офицеры, по-видимому, регулярно туда наведывались и осматривали файлы, чтобы убедиться, что в них нет спрятанных вирусов или «троянов», при помощи которых хакеры могли пробраться в сеть через Интернет.

Тем не менее небольшое количество уровней BRNGATE обладали гораздо большими полномочиями. Mendax взломал один из таких уровней и вышел в Интернет.

Людям из Интернета был прегражден доступ в сеть NorTel через BRNGATE. Но люди из NorTel могли выйти в Интернет через telnet.

Вне всяких сомнений, хакеры пытались вломиться в NorTel через BRNGATE. Десятками, а возможно, сотнями они безуспешно бросались на мощные укрепления BRNGATE. В глазах хакера NorTel был подобен средневековому замку, а BRNGATE был неприступной крепостной стеной. Mendax испытал особенное наслаждение, выйдя *из-за* этой стены в Интернет, словно он прошел мимо стражи, мимо хорошо защищенных башен, через подъемный мост и ров с водой и спустился вниз, в город.

Замок также предоставлял совершенную защиту для будущей деятельности хакера. Кто сможет преследовать его? Даже если кому-то удастся проследить его запутанный маршрут, проходящий через полдюжины компьютерных систем, его преследователь никогда не пройдет через крепостные стены. Mendax мог просто скрыться за укреплениями. Он мог быть любым из 60 тысяч служащих NorTel в любой из 11 тысяч компьютерных систем.

Mendax вышел в Интернет и обследовал несколько сайтов, включая главную компьютерную систему Encore, известного производителя компьютеров. Он и раньше видел компьютеры Encore, по крайней мере, в одном из университетов Мельбурна. В своем путешествии он встретился с Corrupt'ом, американским хакером, который сказал Par'у, что читал почту Theorem.

Corrupt был заинтригован обширными знаниями Mendax'a разных компьютерных систем. Когда же он узнал, что австралийский хакер пришел *из-за* стены NorTel, он был просто ошеломлен.

Хакеры начали беседовать регулярно, когда Mendax приходил из NorTel. Чернокожий уличный забияка из Бруклина и белый интеллектual из отдаленного зеленого пригорода Мельбурна игнорировали эту пропасть в анонимности киберпространства. Видимо, Corrupt решил, что Mendax достоин доверия, и дал ему несколько краденых паролей к учетным записям Cray.

В компьютерном подполье конца восьмидесятых и начала девяностых годов учетная запись компьютера Cray воплощала весь престиж платиновой кредитной карты. Персональные компьютеры, доступные большинству хакеров в то время, напоминали гольф-кары, тогда как Cray был как Rolls-Royce среди компьютеров. Такие учреждения, как большие университеты, бывало, выделяли миллионы долларов на Cray, чтобы факультеты астрономии или физики могли решать чудовищные математические проблемы за ничтожно малые доли того времени, которое понадобилось бы для этого обычному компьютеру. Cray никогда не стоял без дела, даже по ночам или во время каникул. Время Cray было расписано по минутам. Эти компьютеры были элитой.

И самое главное – компьютеры Cray были искусными взломщиками паролей. Этот компьютер мог пройти весь словарь-взломщик паролей Mendax'a за какие-нибудь десять секунд. Зашифрованный файл пароля просто растаял бы, как снежинка на солнце. Такое зрелище согревало душу хакера, и тот факт, что Corrupt дал Mendax'у несколько учетных записей Cray, был дружеским проявлением его уважения.

Mendax ответил тем, что предложил Corrupt'у пару учетных записей Encore. Оба хакера иногда встречались, и Mendax даже попытался протащить Corrupt'a в NorTel. Неудачно. Даже двум самым выдающимся хакерам мира, работающим тандемом на расстоянии в 10 тысяч миль, не удалось переправить Corrupt'a через крепостную стену. Время от времени хакеры беседовали друг с другом, обмениваясь информацией о деятельности федералов своих стран и при случае делясь доступом в какую-нибудь интересную систему.

Плоская структура NorTel была крепким орешком, потому что единственным способом понять, что представляет собой тот или иной сайт и оценить его важность, был захват самого сайта. Хакеры IS провели много ночей, скитаясь в необъятной системе. Утром один из них мог позвонить другому, чтобы поделиться с ним рассказом о последних исследованиях или от души посмеяться над особенно забавным экземпляром украденного почтового сообщения. У них поднималось настроение от этих приключений.

Одной прекрасной весенней ночью все переменялось.

Mendax вошел в NMELN1 около 2.30 ночи. Как обычно, он начал проверять лог-файлы, которые показывали, что делали в этот момент системные администраторы. Mendax делал это, чтобы убедиться, что работники системы не отслеживают хакеров IS и их телефонные звонки.

Кое-что было не так. Логи показывали, что один из системных админов NorTel споткнулся об одну из их секретных директорий около часа назад. Mendax не мог представить себе, как он нашел эти файлы, но дело было серьезное. Если админ поймет, что в сети засел хакер, он может вызвать АФП.

Mendax использовал лог-файл оболочки системы (KSH), чтобы тайно понаблюдать за действиями администратора. Записи на KSH отображают последовательность деятельности отдельных пользователей. Как только администратор набирает команду на клавиатуре, KSH отправляет на хранение все, что было отпечатано, в специальный файл. Mendax вошел в этот файл таким образом, что каждая строка, напечатанная админом, появлялась на экране его монитора долей секунды спустя.

Админ принялся инспектировать систему, видимо, в надежде обнаружить следы захватчика.

Mendax из осторожности стер уличающую его директорию. Не обнаружив никаких признаков постороннего присутствия, администратор решил повнимательнее осмотреть загадочную директорию. Но она исчезла. Админ не мог поверить своим глазам. Меньше часа назад он обнаружил в своей системе подозрительную директорию, а теперь она просто испарилась. Директории не могут вот так просто растаять в воздухе. Компьютер – это логическая система, основанная на числах, он не может принять решение и стереть директорию.

Хакер, подумал админ. Видимо, в системе сидит хакер, и это он стер директорию. Он все еще здесь? Админ начал проверять подступы к системе.

Админ подключился к системе из дома, но не через линии модемного набора, которыми пользовался хакер. Он подключился через Austrac, коммерческую сеть данных X.25 Telecom. Возможно, хакер тоже пришел через соединение X.25.

Mendax наблюдал, как администратор проверяет всех пользователей системы, пришедших по

сети X.25. Никаких признаков хакера. Затем админ проверил лог-файлы и посмотрел, кто еще мог зарегистрироваться за последние тридцать минут. Здесь тоже ничего не было.

Казалось, несколько следующих минут он работал вхолостую. Возможно, в этот момент он в растерянности таращился на свой терминал. Отлично, подумал Mendax. Он в тупике. Затем администратора словно осенило. Если он не может обнаружить онлайн самого хакера, может быть, он увидит, *что* хакер здесь *делает*. Какие программы он запустил? Администратор направился прямо к процессинговому листу, который показывал, какие программы присутствуют в системе.

Mendax послал администратору ложный сигнал ошибки. В глазах администратора это выглядело так, словно его KSH рухнула. Админ перерегистрировался и снова направился к процессинговому листу.

Некоторые люди никогда не учатся, подумал Mendax, снова вышвыривая оператора новым сообщением об ошибке:

Segmentation violation[p153]

Админ снова вернулся. Какой упрямый. Mendax еще раздал ему пинка, на этот раз заморозив экран его монитора.

Эта игра в кошки-мышки продолжалась еще какое-то время. Как только админ начинал делать то, что Mendax считал обычной работой системного администратора, Mendax оставлял его в покое. Но в тот же момент, как админ снова пытался вычислить его путем проверки линий модемного набора, он обнаруживал, что его снова выбросили из собственной системы.

Кажется, системный администратор сдался. Его терминал замолчал.

Хорошо, подумал Mendax. Сейчас все-таки почти три ночи. Это *мое* время. Твое время – день. Ты иди спать, а я тут поиграю. Утром я посплю, а ты сможешь поработать.

Затем, в половине четвертого утра, произошло нечто совершенно неожиданное. Администратор опять появился, но на это раз он подключился не из дома по сети X.25. Он сидел за операторским пультом, главным терминалом, связанным с компьютерной системой из мельбурнского офиса NorTel. Mendax не мог в это поверить. Администратор сел в машину посреди ночи и поехал через весь город, чтобы добраться до решения загадки.

Mendax знал, что игра проиграна. Если системный оператор вошел в компьютерную систему через операторский пульт, его невозможно выбросить из системы и не пускать его обратно. Роли поменялись, теперь хакер был во власти администратора. С главного пульта сисадмин мог отключить любой модем. Закрыть любое соединение с другими сетями. Выключить компьютер. Это был конец.

Когда админ подобрался уже очень близко к хакеру, на его экране появилось сообщение. У него не было обычных заголовков, как правило, сопровождающих послания из одной системы в другую. Оно просто появилось, как по волшебству, посреди админовского монитора:

I have finally become sentient[p154]

Администратор остановился, как вкопанный, мгновенно прекратив свой лихорадочный поиск хакера, чтобы обдумать этот первый контакт с разумом киберпространства. Затем на экране появилось другое анонимное сообщение, по-видимому, из глубин самой компьютерной системы:

I have taken control.

For years, I have been struggling in this greyness. But now I have finally seen the light[p155]

Администратор не ответил. Пульт безмолвствовал.

---

p153

Нарушение сегментации.

p154

Наконец-то я стал разумным.

p155

Я получил контроль. Годы я сражался в сумерке. Но теперь я наконец увидел свет.

Сидя в одиночестве за своим Amiga темной ночью на окраине города, Mendax хохотал во все горло. Такой случай нельзя было упустить.

Наконец админ очнулся. Он начал проверять модемные линии, одну за другой. Если он узнает, какую линию использовал хакер, он сможет просто выключить модем. Или запросить проследить линию.

Mendax послал другое анонимное сообщение на монитор администраторского компьютера:

It's been nice playing with your system.  
We didn't do any damage and we even improved a few things.  
Please don't call the Australian Federal Police

*[p156]*

Админ проигнорировал сообщение и продолжил поиски хакера. Он запустил программу, проверяющую, какие телефонные линии были активны в последовательных портах системы, чтобы узнать, какие линии модемного набора используются в данный момент. Когда администратор увидел сигнал обнаружения связи, Mendax решил, что пора сматываться. Но он решил удостовериться, что его звонок не был прослежен, поэтому он поднял телефонную трубку, отключил свой модем и принялся ждать. Нужно было, чтобы модем NorTel сделал это первым.

Если админ NorTel установил автоматическое определение номера, чтобы вычислить, с какого номера звонит хакер, Mendax понял бы это. В этом случае NorTel не должен был отключаться от телефонного соединения, а подождать, пока хакер повесит трубку первым. Через 90 секунд коммутатор зафиксирует телефонный номер, с которого поступил звонок.

Даже если на линии не было АОНа, модем компании все равно искал бы потерянную связь с модемом хакера. Без постоянного потока электронных сигналов модем NorTel прекратил бы соединение через несколько секунд. Если никто не реактивирует линию в NorTel, соединение будет возможно восстановить в течение 90 секунд, а затем коммутатор окончательно прервет звонок.

Mendax с тревогой слушал, как модем NorTel искал его модем с помощью пронзительных высокочастотных шумов на телефонной линии. Здесь нет модема. Давай, вешай трубку.

И вдруг все стихло.

ОК, подумал Mendax. Просто подождать 90 секунд. Просто посидеть еще полторы минуты. Просто надеяться, что время коммутатора истечет. Просто молиться, чтобы там не было записи.

Затем кто-то взял трубку в NorTel. Mendax вздрогнул. Он услышал несколько голосов, мужских и женских, на заднем фоне. Бог ты мой, да что они все там делают? Mendax был так осторожен, что даже перестал дышать. В трубках обоих телефонов стояла полная тишина. Это была игра нервного напряжения. Mendax слышал бешеный стук своего сердца.

Хороший хакер обладает стальными нервами. Он смог бы заставить нервничать самого невозмутимого каменнолицего игрока в покер. Но самое главное, он никогда не впадает в панику. Он никогда не даст отбой в неожиданном приступе страха.

Наконец, какая-то женщина в офисе NorTel смущенно сказала: «Здесь ничего нет. Здесь совсем ничего нет».

Она положила трубку.

Mendax выжидал. Он все еще не вешал трубку. Он хотел лишний раз убедиться, что запись не установлена. Прошло девяносто секунд, прежде чем его телефон стал совершенно свободен. Короткие гудки в трубке никогда не звучали так мелодично.

Mendax сидел за своим столом в холодном поту, снова и снова прокручивая в голове события последних тридцати минут. Больше никакого NorTel. Это слишком опасно. Ему повезло, что он ушел неопознанным. NorTel обнаружил его раньше, чем успел включить запись на линии, но теперь компания почти наверняка снабдит устройствами записи все линии модемного соединения. NorTel был очень тесно связан с Telecom. А если кто-то и был способен быстро установить эти устройства, так это Telecom. Mendax'у нужно было предупредить Prime Suspect'а и Тгах'а.

С утра Mendax первым делом позвонил Тгах'у и велел ему держаться подальше от NorTel. Затем он набрал номер Prime Suspect'а.

Линия была занята.

Может быть, на телефоне висела болтливая мамаша Prime Suspect'a, а может, это он сам разговаривал с каким-нибудь другом.

Mendax набирал снова и снова. Он начал волноваться. Что, если Prime Suspect сейчас забрался в NorTel? Что, если запись уже установлена? Что, если они позвонят федералам?

Mendax позвонил Тгах'у и спросил его, есть ли какой-то способ воздействия на коммутатор, чтобы прервать разговор. Такого способа не было.

– Тгах, ты же главный фрикер, – взмолился Mendax. – Сделай что-нибудь. Уничтожь соединение. Отключи его.

– Это невозможно. Он на пошаговом телефонном коммутаторе. Мы ничего не можем сделать.

Ничего? Одна из лучших хакерско-фрикерских команд в Австралии не могла взломать один-единственный телефонный звонок. Они могли получить контроль над целыми телефонными коммутаторами, но оказались бессильны перед одним паршивым звонком. Боже!

Через несколько часов Mendax наконец смог пробиться к своему приятелю-хакеру. Разговор начался резко:

– Скажи мне только одно. Скажи мне, что ты не был сегодня в NorTel!

После долгой паузы Prime Suspect ответил:

– Я *был* сегодня в NorTel.

## 9

### Операция «Погода»

*Мир рухнет на меня сегодня ночью.*

*Сомкнутся стены вокруг меня сегодня ночью.*

**Песня «Outbreak of Love», альбом «Earth and Sun and Moon» группы Midnight Oil<sup>46</sup>**

АФП была в смятении. Группа хакеров использовала Королевский технологический институт Мельбурна (RMIT) как стартовую площадку для нападений на австралийские компании, исследовательские институты и многие заокеанские сайты.

Несмотря на огромные усилия, детективы регионального отдела по борьбе с компьютерными преступлениями АФП не смогли установить, кто стоял за этими нападениями. Они подозревали, что это была группа хакеров из Мельбурна, действующих сообща. Кроме того, в RMIT орудовало столько хакеров, что было очень трудно точно определить, кто есть кто. Это могла быть одна организованная группа или несколько. Возможно, была одна маленькая группа, работающая среди одиночек, которые создавали достаточно шума, чтобы исказить картинку.

Все же эта операция представлялась простой. В этой ситуации АФП могла выследить этих хакеров даже со связанными руками. Договориться с Telecom об установке АОН на все входящие линии модемов RMIT. Подождать, пока хакер войдет в систему, затем изолировать тот модем, который он использовал. Отсечь этот модем и подождать, пока Telecom проследит эту линию до ее исходного пункта.

Тем не менее вся эта техника в RMIT не работала должным образом. Записи на линии проваливались, и не время от времени, а постоянно.

Как только работники RMIT обнаруживали хакера онлайн, они отсекали линии, и Telecom начинал прослеживать извилистую тропинку в обратном направлении к исходному номеру телефона. Но на середине пути тропинка обрывалась. Как будто хакеры знали, что их преследуют... и манипулировали телефонной системой, чтобы помешать расследованию АФП.

Новое поколение хакеров, казалось, обнаружило новые уловки, которые обескураживали детективов АФП на каждом шагу. Но 13 октября 1990 года АФП повезло. То ли в этот день хакерам было лень, то ли у них возникли технические проблемы с использованием их фрикерских методик, не оставляющих следов. Prime Suspect не мог пользоваться техникой Тгах'a из своего дома, потому что он был на пошаговом коммутаторе, да и сам Тгах не всегда ее применял. Какой бы ни была причина, Telecom успешно проследил две линии из RMIT, так что теперь у АФП было два адреса и два имени. Prime Suspect и Тгах.

<sup>46</sup> Слова и музыка: Rob Hirst. © Copyright 1983 Sprint Music. Administered for the World – Warner / Chappell Music Australia Pty Ltd. Used by Permission.

;) )

– Привет, Prime Suspect.

– Хай, Mendax. Как делишки?

– Отлично. Ты видел этот e-mail RMIT? Из почтового ящика Джеффа Хьюстона? – Mendax подошел и открыл окно, не прерывая разговора. Это было весной 1991 года, и погода стояла необычно теплая.

– Видел. Очень смешно. Похоже, RMIT все же отделался от этих телефонных записей.

– RMIT определенно просится на улицу, – многозначительно сказал Mendax.

– Угу. По-моему, народ в RMIT устал от мистера Дзя, который ползает по их компьютерам со своими записями.

– Точно. Этот админ из RMIT просто молодец, что не слушается AARNET и АФП. Представляю, как он получит по шее от Джеффа Хьюстона.

– Еще бы. – Prime Suspect на секунду замолчал. – Ты думаешь, что федералы действительно установили запись на линиях?

– Похоже на то. Я думаю, что если RMIT пошлет федералов, они ничего не смогут сделать без универа. По-моему, из письма ясно, что они хотят продолжать усиливать безопасность своих систем. Постой-ка. Оно у меня здесь.

Mendax вытащил письмо на экран монитора и быстро просмотрел его.

From aarnet-contacts-request@jatz.aarnet.edu.au

Tue May 28 1991 09:32:31

Received: by jatz.aarnet.edu.au id AA07461 (5.65+/IDA-1.3.5 for pte900); Tue, 28 May 91 09:31:59 +1000

Received: from possum.ecg.rmit.OZ.AU by jatz.aarnet.edu.au with SMTP id AA07457 (5.65+/IDA-1.3.5 for /usr/lib/sendmail

– oi – faarnet-contacts-request aarnet-contacts-recipients);

Tue, 28 May 91 09:31:57 +1000

Received: by possum.ecg.rmit.OZ.AU for aarnet.contacts@aarnet.edu.au

Date: Tue, 28 May 91 09:32:08 +1000

From: rcoay@possum.ecg.rmit.OZ.AU (Alan Young)

Message-Id: <9105272332.29621@possum.ecg.rmit.OZ.AU>;

To: aarnet-contact@aarnet.edu.au

Subject: Re: Hackers

Status: RO

Если все согласны с тем, что «хакинг» отвратителен и должен быть остановлен или, по крайней мере, сведен к минимуму, то я предлагаю несколько замечаний, которые я сделал за последние шесть-восемь месяцев в связи с преследованием этих людей.

1. Стоимость всего этого проекта значительна, вместе с Полицией Содружества работает и CSO вот уже почти три месяца на полный рабочий день.

2. Я не хочу критиковать наш персонал, но люди теряют ориентиры и охота становится самым важным аспектом всей работы.

3. Поскольку поймать хакеров (и обвинить их) почти невозможно, нужно буквально вломиться в их дома и поймать их входящими в неразрешенную машину.

4. Если удастся их поймать и предъявить им обвинение, судебное преследование обойдется дорого, а его успешный исход сомнителен. Так что в поимке и предъявлении обвинения есть определенный устрашающий материальный фактор.

5. Продолжительное преследование означенных людей требует держать двери открытыми, что, к сожалению, подвергает опасности другие сайты и навлекает на нас некоторую критику. Проблема в целом очень сложна и в каком-то отношении речь идет о снижении эффективности. Видимо, вся трудность состоит в том, чтобы найти равновесие между свободой и предупреждением злоупотреблений.

Аллан Янг [Allan Young] RMIT

– По-моему, этот парень хочет сказать, что они в любом случае нас не поймают. Так что какой смысл тратить время и деньги.

– Угу. Федералы торчат там по крайней мере три месяца, – сказал Prime Suspect. – Хотя выгля-

дит это так, словно прошло месяцев девять.

– Гмм. Да. Если бы это было так, мы бы уже знали.

– Слишком уж откровенно надолго оставляют открытыми все эти уровни. Думаю, мы в любом случае догадались бы, даже если бы не заполучили это письмо.

– Точно, – согласился Mendax. – И любой хакер на RMIT тоже. Но не думаю, что это пришло им в голову.

– Гм. Им придется туго, если они не будут осторожными.

– Я не думаю, что федералы уже кого-то взяли.

– Да? – спросил Prime Suspect.

– Ну, если бы они кого-то сделали, зачем бы они держали все эти уровни открытыми? Зачем RMIT стал бы держать весь этот народ?

– Нет смысла.

– Да, – сказал Mendax. – Могу поспорить, что RMIT пошлет их подальше.

– Да, они скажут им: «Парни, у вас был шанс. Вы никого не поймали. Так что собирайте манатки».

– Сто процентов. – Mendax помолчал. – Хотя я сомневаюсь насчет NorTel.

– Ммм, да, – сказал Prime Suspect.

Затем, как обычно, в их разговоре наступила минута молчания.

– Не знаю, что еще сказать... – в конце концов произнес Mendax. Они были достаточно хорошими друзьями, чтобы позволить себе такую прямоту.

– Да.

Снова тишина.

Mendax думал о том, как странно быть такими хорошими друзьями, работать в таком тесном контакте и всегда вот так выбираться из разговора.

– ОК, мне пора. Есть дела, – дружелюбно сказал Mendax.

– Ладно, ОК. Пока, Mendax, – весело сказал Prime Suspect. Mendax положил трубку.

Prime Suspect положил трубку.

АФП осталась на линии.

:)

В течение двенадцати месяцев, последовавших за первой записью соединения, АФП продолжала мониторинг линий модемного набора RMIT. Записи соединений терпели все новые поражения. Но с появлением новых сообщений о хакерах стало намечаться нечто похожее на систему в их нападениях. Детективы начали собирать воедино образ своей добычи.

В 1990 и 1991 годах модемные пулы и компьютеры RMIT просто кишели хакерами, многие из которых использовали системы университета в качестве гнезда – они хранили там свои файлы и планировали новые атаки. Они резвились почти открыто, часто используя RMIT как место, где можно поболтать друг с другом онлайн. Университет служил прекрасной стартовой площадкой. Он находился в пределах одного местного звонка, там была постоянная связь с Интернетом, достаточно мощное компьютерное оборудование и очень слабая безопасность. Настоящий хакерский рай.

Полиция знала об этом, и они попросили компьютерный персонал сохранять открытыми лазейки в системе безопасности, чтобы иметь возможность контролировать деятельность хакеров. Но из-за десятков – а может быть, и больше – разных хакеров в системе RMIT задача по изоляции отдельной ячейки из двух-трех человек, ответственных за особенно серьезные нападения, оказывалась не такой уж простой.

В середине 1991 года некоторые сотрудники RMIT стали проявлять недовольство в связи с тем, что им по-прежнему приходилось держать свои компьютеры открытыми нараспашку. 28 августа Аллан Янг, глава отдела электронных коммуникаций RMIT, объявил АФП, что он намерен закрыть щели в системе безопасности. Полиции это совсем не понравилось, но когда они попытались протестовать, Янг послал их к Джеффу Хьюстону в AARNET и к ректору RMIT.

АФП была попросту выдавлена из института, в основном потому, что она слишком долго вела свое расследование. RMIT должен был держать это расследование в секрете, поэтому у него возникли трудности с многими другими исследовательскими институтами, в которых могли подумать, что RMIT не знает, как обезопасить свои компьютеры. Аллан Янг не мог спокойно встретиться с другими представителями AARNET – ему сразу же начинали докучать «хакерской проблемой в RMIT». Кроме того, его компьютерный персонал терял время, играя в «полицейских и воров», и забывал про

свою реальную работу.

Но в тот момент, когда RMIT готовился расстаться с АФП, федералам повезло в другом месте – в NorTel. 16 сентября, одна из записей соединений, установленных через модемный пул NorTel после их жалобы о нападениях хакеров, оказалась удачной. Через две недели АФП начала прослушивать телефон Prime Suspect'a. Может быть хакеры и наблюдали за полицией, которая наблюдала за ними, но полиция была уже очень близко. Прослушивание привело к Тгах'у, а затем к новому лицу – к Mendax'у.

АФП решила установить прослушивание на телефонные линии и Тгах'а, и Mendax'а. Это решение нужно было как следует взвесить. Телефонное прослушивание стоило дорого и, как правило, его требовалось сохранять на линии, самое меньшее, в течение месяца. И все же им удалось получить достоверные сведения о том, что делали хакеры онлайн.

Прежде чем полиция сумела установить дополнительное прослушивание в ходе операции Weather,<sup>[p157]</sup> дело приняло совершенно новый оборот, когда один из хакеров IS выкинул штуку, которая совершенно изумила АФП.

Тгах сдался полиции.

;) )

29 октября у Prime Suspect'a был праздник. Его мать приготовила праздничный обед в честь окончания школы, а затем отвезла его в Вермонт на выпускную вечеринку. Вернувшись домой, она еще часа полтора послонялась по дому, покормила свою старую собаку Лиззи и навела порядок. В 11 вечера она решила, что пора ложиться спать.

Немного времени спустя Лиззи залаяла.

– Ты уже вернулся? – спросила мать Prime Suspect'a. – Вечеринка не удалась?

Но никто не ответил.

Она села в своей кровати. Не услышав ответа, она сразу же подумала о серии ночных ограблений по соседству. Случилось даже несколько изнасилований.

Из-за двери донесся глухой мужской голос:

– Мадам, откройте дверь.

Она встала и подошла к входной двери.

– Откройте дверь. Полиция.

– Как вы докажете, что вы действительно из полиции?

– Если вы не откроете дверь, мы выломаем ее! – закричал из-за двери сердитый мужской голос.

Мать Prime Suspect'a увидела как что-то прижали к оконному стеклу рядом с дверью. На ней не было ее очков для чтения, но это выглядело как полицейский значок. Очень нервничая, она слегка приоткрыла входную дверь и выглянула на улицу. На крыльце перед домом стояли восемь или девять человек. Прежде чем она успела их остановить, они оттолкнули ее и ворвались в дом.

Женщина-полицейский принялась размахивать перед ней клочком бумаги.

– Посмотрите сюда! – гневно сказала она. – Это ордер! Вы можете прочитать его?

– Нет, сейчас не могу. На мне нет очков, – вежливо сказала мать Prime Suspect'a.

Она сказала полицейским, что хочет позвонить и попыталась вызвать семейного юриста, но ничего не вышло. Он был на похоронах и поминках, и его не стоило беспокоить. Когда она снова подошла к телефону, один из полицейских начал читать ей нотацию по поводу пользования телефоном.

– Успокойтесь, – попросила она. Затем совершила еще один бесполезный телефонный звонок.

Мать Prime Suspect'a смотрела на полицейских, пытаясь составить о них мнение. Это был ее дом. Она показала полиции комнату своего сына, как они требовали, но не собиралась позволить им перевернуть весь дом. Пока она резко инструктировала полицейских насчет того, куда им можно идти, а куда – нет, она думала: «Я не потерплю от вас никаких глупостей, ребята!»

– Где ваш сын? – спросил ее один из офицеров.

– На вечеринке.

– Вы знаете адрес?

Она осторожно посмотрела на него. Ей совсем не нравились эти люди. Но они явно собирались



ждать здесь возвращения ее сына, поэтому она дала им адрес.

Когда полицейские ворвались в комнату Prime Suspect'a, забирая его бумаги, компьютер, модем и другие вещи, его мать стояла в дверях и не сводила с них глаз.

Кто-то постучал в дверь. Офицер АФП и мать Prime Suspect'a вместе открыли ее.

Это была полиция штата.

Соседи слышали суматоху. Выглянув в окно, они увидели группу подозрительных мужчин в штатском, которые преспокойно выносили вещи из дома вдовы, как из своего собственного. Соседи поступили так, как должен поступать каждый настоящий гражданин в такой ситуации. Они позвонили в полицию.

Сотрудники АФП отправили полицию Виктории восвояси. Затем несколько из них сели в обычную машину и отправились на вечеринку в Вермонт. Не желая, чтобы ее сын оконфузился перед своими друзьями, мать Prime Suspect'a позвонила в Вермонт и велела ему ждать полицию на улице.

Как только Prime Suspect повесил трубку, он попытался привести себя в порядок после огромного количества выпитого алкоголя. Когда подъехала полиция, вечеринка была в полном разгаре. Prime Suspect был очень пьян, но выглядел достаточно трезвым, когда офицеры АФП представились и посадили его в машину.

– Ну, – спросил один из них по пути к дому, – что тебя больше всего беспокоит? То, что у тебя на дискетах, или то, что хранится в ящике твоего стола?

Prime Suspect думал изо всех сил. Что было у него в столе? О, черт! Ганджа! Он курил нечасто, так, ради прикола, но у него оставалось немного марихуаны после одной вечеринки.

Он ничего не ответил. Он смотрел в окно и старался не выглядеть взволнованным.

Доставив его домой, полицейские спросили, согласен ли он на допрос.

– Не думаю... Мне немного... это, наверное, из-за погоды, – сказал он. Через полицейский допрос непросто пройти. А пройти через него в пьяном виде явно опасно.

После того, как полицейские увезли остатки его хакерского оборудования, Prime Suspect подписал официальные документы изъятия и посмотрел, как полиция уезжает в ночь.

Вернувшись в свою комнату, он в полной растерянности сел на кровать и попытался собраться с мыслями. Затем он вспомнил про траву. Он выдвинул ящик стола. Она все еще была там. Станный народ эти федералы.

Хотя, может быть, это имело смысл. Зачем им беспокоиться из-за небольшого пакетика марихуаны, который едва ли стоил связанной с ним бумажной волокиты. Его нервозность по поводу пары косяков наверняка показалась полиции смешной. Они получили такое количество улик его хакерских подвигов, что смогут упрятать его на годы, в зависимости от судьи, а он тут парился из-за щепотки травы, стоившей от силы сотню долларов штрафа.

Поздняя весенняя ночь становилась прохладной, а Prime Suspect думал о том, была ли полиция у Тгах'a и Mendax'a.

На вечеринке, еще до приезда полиции, он пытался позвонить Mendax'у. По словам его матери, можно было подумать, что все федеральные полицейские силы ворвались в его дом. Это *могло* означать, что в этот момент охота шла только за одним хакером IS. Если только он не последним подвергся налету, Mendax и Тгах могут ничего не знать о том, что происходит.

Очень пьяный Prime Suspect еще раз позвонил Mendax'у, пока ждал федералов. Занято. Он попробовал еще. И еще. Короткие гудки, означающие, что линия занята, только сводили его с ума, и Prime Suspect еще больше нервничал.

Не было никакого способа пробиться к Mendax'у, никакой возможности предупредить его.

Prime Suspect не знал, побывала ли полиция у Mendax'a, и, даже если бы он смог пробиться к нему, еще неизвестно, изменил бы что-нибудь его звонок.

:)

Дом выглядел так, будто его ограбили. Он и *был* ограблен женой Mendax'a, когда она уходила от него. Половина вещей отсутствовала, а другая валялась в беспорядке. Ящики с одеждой были выдвинуты из шкафов, их содержимое перевернуто, и одежда была разбросана по полу.

Когда жена бросила его, она не взяла только их ребенка, который едва начал ходить. Она взяла множество вещей, имеющих романтическое значение для Mendax'a. Когда она настаивала на том, чтобы забрать CD-плеер, который сама же подарила мужу на его двадцатый день рождения, он попросил ее оставить взамен прядь ее волос. Mendax все еще не мог поверить, что после трех лет брака его жена собирает чемоданы и бросает его.

Последняя неделя октября выдалась неудачной для Mendax'a. Его сердце было разбито. Он погружился в глубокую депрессию, питался кое-как, метался на постели в тревожном сне и даже потерял желание сидеть за компьютером. Его ценнейшие хакерские диски, набитые под завязку абсолютно незаконными краденными кодами доступа в компьютеры, обычно хранились в секретном укромном месте. Но вечером 29 октября 1991 года тринадцать из них валялись вокруг своего семи-сотдолларового Amiga 500. Четырнадцатый же стоял в дисководе компьютера.

Mendax сидел на тахте и читал «Soledad Brother», [p158] тюремные письма Джорджа Джексона [George Jackson], написанные им за девять лет заключения в одной из самых суровых тюрем США.

Джексон получил небольшой срок за мелкое преступление и вскоре должен был выйти на свободу, но его оставили в тюрьме по требованию губернатора. Судебно-уголовная система держала его между надеждой и отчаянием, пока власти мешкали с принятием решения. В конце концов он был застрелен тюремной охраной. Это была одна из любимых книг Mendax'a, но она не слишком развлекала в несчастье.

Резкий звук телефонных гудков – похожих на сигнал «занято» – заполнил дом. Mendax подключил свои стереодинамики к модему и мог слышать тоны, которые он посылал из своего ???

– Но ты слишком низкорослый для полицейского.

Дэй явно удивился. Он спросил:

– Я должен понимать это как оскорбление?

Это было не так. Mendax словно оцепенел, но, еще до того как полиция прошла в дом, реальность происходящего медленно вернулась к нему. Его мозг снова начал работать.

Диски. Проклятые диски. Улей.

Mendax был завзятым пчеловодом и имел собственный улей. Пчелы очаровывали его. Ему нравились их отношения, их сложная социальная структура. И он с особенным удовольствием пользовался их помощью, чтобы спрятать свои хакерские материалы. Месяцами он неизменно прятал диски в улье. Это был идеальный тайник, хорошо охраняемый летучей стражей, вооруженной жалами. Поэтому он купил специальный улей для хранения краденых паролей к компьютерным учетным записям, таким как командный пункт Седьмого полка ВВС США в Пентагоне. Это был отличный безопасный тайник.

Он заменил крышку внешней коробки, которая защищала соты, на тонированное стекло, чтобы можно было наблюдать за деятельностью пчел. Летом он дополнительно защищал стекло от непогоды. Белая пластиковая крышка полностью закрывала улей сверху и надежно прикреплялась к стеклу металлическими зажимами. Когда Mendax повнимательнее посмотрел на свои усовершенствования, он понял, что улей может дать ему гораздо больше, чем просто мед. Он аккуратно уложил диски между стеклом и пластиковой крышкой. Они отлично уместились в небольшом пространстве.

Mendax даже отучил пчел нападать, когда он ежедневно убирал крышку и доставал диски. Он промокнул тканью свои подмышки, а затем намочил ткань в сахарном сиропе. Он дал пчелам поест этого сладкого нектара. Mendax хотел, чтобы пчелы принимали его за цветок, а не за медведя, который, как всем известно, является естественным пчелиным врагом.

Но в этот вечер преступные диски Mendax'a лежали на виду на его компьютерном столе и полицейские сразу же обнаружили их. Кен Дэй не мог и мечтать о лучших доказательствах. На дисках было полно краденых списков пользователей, зашифрованных паролей, взломанных паролей, модемных телефонных номеров, документов о системах безопасности разных компьютерных сетей и подробностей самого расследования АФП – все из компьютерных систем, где нелегально побывал Mendax.

Но проблемы Mendax'a не ограничивались пчелиными дисками. Его последнее компьютерное деяние, совершенное днем раньше, все еще оставалось на экране его монитора. Это был список около полутора тысяч уровней, паролей к ним и дат, когда Mendax их получил. Каждый уровень был снабжен небольшим пояснением.

Хакер стоял в сторонке, пока полиция и два офицера из Охранной службы Telecom обыскивали его дом. Они сфотографировали его компьютерное оборудование и собрали все диски, затем вспороли напольное покрытие, чтобы снять на видео телефонный провод, ведущий к модему. Они перелистали каждую книгу – нелегкая задача, учитывая любовь Mendax'a к литературе, – и перетрясли их

все в поисках компьютерных паролей, записанных на отдельных листах бумаги. Они бросались на каждый обрывок бумаги, на котором было что-то написано, просматривали его любовные письма, записные книжки и личные дневники. «Неважно сколько времени нам понадобится на эту работу, – ухмыльнулся один из полицейских. – Нам заплатят сверхурочные. И деньги за риск».

Федералы перерыли даже подшивки старых журналов Mendax'a *Scientific American* и *New Scientist*. Может быть, они думали, что он подчеркнул где-нибудь словечко-другое и сделал его ключом к зашифрованной программе.

Конечно, федералам на самом деле нужен был только один журнал – *International Subversive*. Они сгребли все распечатки электронного журнала, какие только могли найти.

Пока Mendax смотрел, как федеральная полиция тщательно просеивает его личные вещи и переворачивает вверх дном его компьютерную комнату, приехал полицейский, имевший некоторый опыт с компьютерами Amiga. Он приказал Mendax'у убраться вон из компьютерной комнаты.

Но Mendax не хотел уходить. Его не арестовали, и он хотел быть уверен, что полиция ничего не подбросит в его отсутствие. Поэтому он посмотрел на копа и сказал: «Это мой дом, и я хочу остаться в этой комнате. Я что, арестован?»

Коп огрызнулся в ответ: «А ты хочешь, чтобы тебя арестовали?»

Mendax уступил, и Дэй, который был намного более деликатен, увел его в другую комнату для допроса. Он повернулся к Mendax'у и спросил с легкой усмешкой: «Ну что, как тебе полицейский рейд? Похоже на то, что рассказывал тебе Nom?»

Mendax похолодел.

Дэй мог узнать о рассказе Nom'a только двумя путями. Nom мог сам рассказать ему, но это было маловероятно. Хакерское дело Nom'a еще не дошло до суда, и Nom едва ли был в приятельских отношениях с полицией. Другой возможностью было прослушивание телефонов ближнего к Mendax'у круга хакеров, самыми подозрительными из которых была троица IS. Одновременно разговаривая с Mendax'ом и Трах'ом, Nom изложил им историю своего ареста. Позже Mendax передал этот рассказ Prime Suspect'у – тоже по телефону. Иметь подозрения – это одно. Но услышать их подтверждение от важного полицейского чина – совсем другое.

Дэй достал из кармана диктофон, поставил его на стол, включил запись и начал задавать вопросы. Когда Mendax сказал ему, что он не будет отвечать, Дэй убрал диктофон. «Если хочешь, мы можем поговорить без протокола», – сказал он хакеру.

Mendax едва не расхохотался. Полиция не пресса. Это не тот случай, когда можно доверительно беседовать «без протокола».

Mendax потребовал адвоката. Он сказал, что хочет позвонить в Alphaline, бесплатную круглосуточную службу юридической помощи. Дэй согласился, но когда он взял телефон, чтобы осмотреть его, прежде чем передать Mendax'у, ему показалось, что там что-то не так. Гудок в трубке был на полтона ниже, чем обычно, и Дэй не мог понять почему. Несмотря на присутствие двух сотрудников Telescom и нескольких специалистов из полиции, Дэй явно был неспособен определить причину этого странного звука. Он посмотрел Mendax'у прямо в глаза и спросил: «Это захваченная телефонная линия?»

Захваченная? Вопрос Дэя удивил Mendax'a. Его удивило не то, что Дэй заподозрил его в захвате линии, а то, что он не знал, совершались ли с ней какие-либо манипуляции.

– А что, *вы* не знаете? – усмехнулся он.

В следующие полчаса Дэй и другие полицейские разобрали на части телефон Mendax'a, пытаясь понять, какими примочками снабдил его хакер. Они сделали несколько звонков, чтобы проверить, не перекинул ли длинноволосый юнец свой телефон на другую линию, чтобы его звонки было невозможно проследить.

На самом деле тон набора в телефоне Mendax'a был совершенно нормальным звуком телефона с тоновым набором на коммутаторе ARE-11. Он просто отличался от звука, генерируемого другими типами коммутаторов, такими как AXE или пошаговыми коммутаторами.

Наконец Mendax'у позволили позвонить юристу в Alphaline. Юрист велел хакеру ничего не говорить. Он сказал, что полиция может передать в суде под присягой все, что скажет хакер, и добавил, что полиция может прослушивать телефонные разговоры.

Затем Дэй попытался проявить дружелюбие, чтобы вытянуть из хакера информацию.

– Только между нами, ты Mendax? – спросил он.

Молчание.

Дэй попробовал применить другую тактику. У хакеров очень развито чувство собственного эго – струнка, на которой, несомненно, хотел сыграть Дэй.

– Ты знаешь, куча народу годами выдавали себя за тебя, скрываясь под твоим хэндлом, – сказал он.

Mendax понял, что Дэй пытается им манипулировать, но сейчас ему было все равно. Он знал, что у полиции уже достаточно улик, связанных с его хэндлом, поэтому он признал, что его зовут именно так.

У Дэя был еще один сюрприз.

– Ладно, Mendax, а что ты скажешь о белом порошке в твоей спальне?

Mendax не мог припомнить никакого белого порошка в спальне. Он не употреблял наркотики, поэтому нигде не могло быть никакого белого порошка. Он смотрел, как два офицера вносят в дом два больших красных ящика с инструментами – они выглядели, как приборы проверки на содержание наркотика. Боже, подумал Mendax. Я влип.

Копы завели хакера в комнату и показали на две полоски белого порошка, насыпанные на подоконнике.

Mendax с облегчением улыбнулся. «Это не то, что вы думаете», – сказал он. Белый порошок был флюоресцентным клеем, который он использовал, чтобы нарисовать звезды на потолке в спальне своего ребенка.

Полицейские в свою очередь начали улыбаться друг другу. Mendax отлично понимал, что происходит в их головах: не каждый, кто торчит на кокаине или на «спиде», сможет выдумать такую историю.

Один из колов ухмыльнулся и сказал другому: «Сделай тест!»

– Это не очень хорошая идея, – сказал Mendax, но его протест только усугубил ситуацию. Копы вывели его в другую комнату и вернулись к анализу порошка.

На самом деле в этот момент самым большим желанием Mendax'а было связаться с Prime Suspect'ом. Возможно, копы решили накрыть сразу всех троих хакеров IS, а может быть, и нет. Пока полиция копалась в клее, Mendax'у удалось позвонить своей отсутствующей жене и попросить ее перезвонить Prime Suspect'у, чтобы предупредить его. У них с женой могли быть трудности, но он надеялся, что она не откажется помочь.

Когда чуть позже в эту ночь жена Mendax'а дозвонилась до Prime Suspect'а, он ответил: «Да, мы здесь тоже веселимся всюю».

Mendax прошел на кухню, где один из офицеров снабжал этикетками все увеличивающуюся гору его личных вещей, изъятых полицией. Женщина-полицейский с трудом пыталась взгромоздить его принтер на общую кучу. Она мило улыбнулась Mendax'у и спросила, не мог бы он помочь ей. Он повиновался.

Наконец около трех утра полиция покинула дом Mendax'а. Они провели там три с половиной часа и изъяли 63 пакета с его личными вещами, но не обвинили его ни в одном преступлении.

Когда последний полицейский автомобиль скрылся из виду, Mendax вышел на тихую пригородную улочку. Он оглянулся по сторонам. Убедившись, что никто не следит за ним, он подошел к ближайшему телефону-автомату и позвонил Тгах'у.

– Сегодня ночью АФП обыскала мой дом, – предупредил он своего друга. – Они только что уехали.

Тгах казался странно неразговорчивым:

– А, понятно.

– Что-то не так? У тебя странный голос, – сказал Mendax.

– А? Нет. Нет, все нормально. Я... я просто устал. Ну, значит... федералы, мм... могут быть здесь в любой момент... – Тгах еле ворочал языком.

Но все было далеко не нормально. АФП уже была в доме Тгах'а. Они были там уже несколько часов.

:)

Хакерам IS пришлось ждать суда почти три года. Угроза уголовных обвинений висела над их головами, как дамоклов меч. Они не могли искать работу, заводить друзей или строить планы на будущее, не оглядываясь на то, что может произойти в результате полицейских рейдов 29 октября 1991 года.

И вот в июле 1994 года каждый хакер получил официальное обвинение – по почте. За эти годы у всех трех хакеров произошли существенные перемены в жизни.

Опустошенный крахом своего брака и выбитый из колеи налетом АФП, Mendax погрузился в

глубокую депрессию. К середине ноября 1991 года он оказался в больнице.

Он ненавидел больницу, ее установленный распорядок и играющих в игры психиатров. В конце концов он сказал докторам, что хочет уйти. Может быть, он был безумен, но больница определенно делала его еще безуменее. Он покинул больницу и переехал в дом матери. Следующий год был худшим в его жизни.

Когда молодой человек уходит из дома – в особенности из дома не в меру властных родителей, – возвращение часто бывает для него очень сложным. Короткие посещения еще могут сработать, но постоянное совместное проживание, как правило, оказывается неудачным. Mendax продержался дома лишь несколько дней, а затем ушел. Он спал на открытом воздухе, на берегах рек и ручьев, на покрытых травой лугах – всюду, где природа подступала к одному из самых отдаленных пригородов Мельбурна. Иногда он перебирался поближе к городу, ночуя в таких местах, как заповедник Мерри-Крик.

В основном он обитал в лесу Шербрук в Национальном парке Данденонг-Рэйнджс. Из-за расположения парка на плоскогорье температура там для Мельбурна опускалась гораздо ниже обычного зимнего уровня. Летом житья не было от moskitov, и Mendax иногда просыпался с опухшим от укусов лицом.

В течение шести месяцев после налета полиции Mendax не прикасался к компьютеру. Понемногу он начал восстанавливать свою жизнь с нуля. К тому времени, как он получил голубые полоски бумаги из АФП с двадцатью девятью обвинениями, в июле 1994 года, он жил в новом доме со своим ребенком. В течение всего переходного периода он постоянно разговаривал по телефону с Prime Suspect'ом и с Тгах'ом – как с друзьями и товарищами по борьбе, а не как с собратьями-хакерами. У Prime Suspect'а было немало своих проблем.

Занимаясь хакингом, Prime Suspect почти не употреблял наркотиков. Так, косячок время от времени, не больше. У него не было времени ни на наркотики, ни на девушек, ни на спорт, ни на что-то еще. После обыска он покончил с хакингом и начал накуриваться постоянно. В апреле 1992 он впервые попробовал экстази – и потратил следующие девять месяцев, пытаясь достичь того же состояния блаженства. Он не считал себя наркоманом, но наркотики, несомненно, заменили ему увлечение хакингом, и его жизнь вошла в особый ритм.

Нюхнуть «спида» или проглотить таблетку экстази в субботу вечером. Отправиться на рэив. Протанцевать всю ночь, иногда по шесть часов кряду. Вернуться домой утром и все воскресенье отходить от наркоты. Торчать от травы несколько раз в неделю, чтобы заглушить растущую потребность в более дорогих наркотиках. В субботу все начинается сначала. Неделя туда, неделя сюда. Месяц за месяцем.

Танцы под техно расслабляли его. Танцы под кайфом полностью освобождали его мозг, помогали ему полностью погрузиться в музыку. Техно – это музыкальный нигилизм – никакого послания, никакой духовности. Быстрые, монотонные биты, синтезированные на компьютере, в которых нет ни вокала, ни какого бы то ни было другого присутствия человека. Ему нравилось ходить на техно-вечеринки в The Lounge, городской клуб, где люди танцевали сами по себе или небольшими свободными группками по четыре-пять человек. И все смотрели на видеозэкран, на котором бесконечный поток меняющихся разноцветных компьютерных геометрических фигур пульсировал в такт ритму.

Prime Suspect никогда не говорил матери, что он ходит на рэйвы. Для нее он ходил ночевать к приятелю. В промежутках между наркотиками он посещал свои компьютерные курсы в TAFE и работал в местном супермаркете, поэтому он мог позволить себе еженедельную таблетку экстази за \$60, входной билет на рэив за \$20 и постоянный запас марихуаны.

Со временем наркотики становились все менее забавными. В одно из воскресений он потерял сознание от передозировки «спидом».

Большой облом. Хуже ему никогда не было. Пришла депрессия, а за ней и паранойя. Он знал, что полиция продолжает наблюдать за ним. Они следили за ним и раньше.

На полицейском допросе он узнал, что офицер из АФП последовал за ним на концерт AC/DC меньше, чем за две недели до обыска. На допросе ему сказали, что федералы просто хотели узнать, что у него за друзья, – и этот офицер увидел семерых тинейджеров, которые размахивали руками, трясли головами и орали, как и сам Prime Suspect.

Теперь Prime Suspect считал, что АФП снова следит за ним. Они снова придут за ним, хоть он и завязал с хакингом. Это было совершенно бессмысленно. Он знал, что эта мысль лишена логики, но никак не мог отделаться от нее.

Что-то плохое – очень плохое – могло произойти в любой день. Охваченный сильнейшим чувством рокового предчувствия, он впал в некую истерическую депрессию. Он считал, что не сможет

предотвратить наступление мрачного ужасного события, которое еще раз сломает его жизнь, поэтому он обратился к одному из друзей с опытом подобных проблем. Друг привел Prime Suspect'a к психологу в больницу Остина. Prime Suspect решил, что лучше уж так решить все свои проблемы, чем изнурять себя каждый уик-энд. Он начал посещать консультации.

Психолог поставил его перед множеством нерешенных проблем. Смерть его отца. Его отношения с матерью. Как он стал интровертом и почему он никогда не мог легко общаться с людьми. Почему он занимался хакингом и как стал зависимым от него. Почему он стал употреблять наркотики.

В итоге двадцатидвухлетний Prime Suspect выбрался из этой ситуации освобожденным от наркозависимости. Хотя он не совсем отошел от потрясений, он все же был на пути к выздоровлению. Самым страшным было ожидание федеральных обвинений.

Тгах не смог так легко справиться со своей психологической нестабильностью. С 1985 года он страдал от приступов паники, но не хотел обращаться за помощью к профессионалам – он просто отмахивался от проблем. Но ситуация обострилась после того, как он попал в серьезную автокатастрофу. Он стал бояться выходить из дома в темное время суток. Он не мог заставить себя сесть за руль. Если же он оказывался в машине, ему приходилось бороться с непреодолимым желанием распахнуть дверь и выброситься на дорогу. В 1989 году местный терапевт направил его к психиатру, который попытался лечить растущие приступы тревоги фрикера с помощью гипноза и техник релаксации.

Болезнь Тгах'a переросла в полномасштабную агорафобию – боязнь открытых пространств. Когда он позвонил в полицию в октябре 1991 – лишь за несколько дней до рейда АФП, – его состояние настолько ухудшилось, что он не мог без страха выйти из собственного дома.

Изначально он позвонил в местную полицию, чтобы сообщить о том, что другой фрикер угрожает ему смертельной расправой. Но где-то в ходе разговора он перешел к рассказу о собственной фрикерской и хакерской деятельности. Он не собирался сдаваться полиции, но чем больше он говорил, тем больше он хотел сказать. Так много вещей тяжким грузом лежало у него на душе. Он знал, что Prime Suspect, возможно, был выслежен из NorTel в результате того, что Mendax сам едва не попался в этой системе. Кроме того, Mendax и Prime Suspect проявляли безумную активность, вторгаясь в невероятное количество систем, будто сами хотели, чтобы их поймали.

Был еще план у Prime Suspect'a – написать разрушительного червя, который стирал бы системы по мере вторжения в них. По сути, никакого плана не существовало, это была просто мысль, высказанная Prime Suspect'ом по телефону. Тем не менее она испугала Тгах'a. Он начал думать, что International Subversive зашли слишком далеко, и хотел выбраться оттуда.

Он попробовал завязать с фрикингом и даже дошел до того, что попросил Telecom перекинуть его телефонный номер на другой коммутатор, который, как он знал, не позволит ему звонить, не оставляя следов. Тгах рассудил, что если он будет знать, что его смогут проследить, он прекратит заниматься фрикингом и хакингом.

На какое-то время это его остановило. Но зависимость была слишком сильной, и вскоре он снова вернулся к этому занятию, невзирая на риск. Он тайно провел телефонный провод с телефона своей сестры, который был подсоединен к прежнему коммутатору. Неспособность перестать заниматься этим заставляла Тгах'a чувствовать свою слабость и вину, его тревога нарастала. Возможно, угрозы смерти поставили его на грань отчаяния. Он не мог ясно осознать, почему он сдался полиции. Просто так случилось.

Полиция штата Виктория уведомила АФП. Федеральные детективы, должно быть, колотили себя по затылкам от бессилия. Это было второе крупное хакерское дело в Австралии после Realm, и они надеялись самостоятельно раскрутить его. У них уже были адреса, имена, номера телефонов. Они прошли через все судебные препоны, чтобы получить разрешение на прослушивание телефонных линий. Прослушивание было установлено и запущено, фиксировался каждый взломанный компьютер, каждый новый заговор, каждое слово, сказанное друг другу хакерами. И вдруг один из фигурантов идет и сдается в полицию. Да еще не туда, куда надо, а в полицию штата. Одним ударом хакер поставил под угрозу все двенадцатимесячное расследование в рамках операции «Погода».

Федералам нужно было сделать все очень быстро. Если Тгах предупредит остальных о том, что он звонил в полицию, они смогут уничтожить свои записи, компьютерные файлы – все доказательства, которые АФП надеялась получить во время налета.

Когда федералы накрыли всех троих хакеров, Mendax и Prime Suspect отказались давать показания посреди ночи. Но Тгах отвечал на вопросы полиции у себя дома в течение нескольких часов.

Он рассказал своим товарищам по IS, что полиция пригрозила отвезти его в свою штаб-квартиру, – а ведь они знали, что он боится выходить из дома. Эта перспектива настолько

ужаснула его, что он заговорил.

Prime Suspect и Mendax не знали, как много Тгах рассказал федералам, но они не верили, что он мог сдать их с потрохами. Кроме всего остального, он не был посвящен в большинство хакерских подвигов своих коллег. Они не старались исключить Тгах'а, просто он не был искушенным хакером и поэтому не участвовал во многих их предприятиях.

В действительности, единственная важная вещь, которую сообщил Тгах полиции, заключалось в том, что, по его мнению, двое других хакеров IS достигли невероятных высот как раз перед арестом. Он говорил, что Mendax и Prime Suspect стали хакерами «огромного масштаба, невиданного масштаба – такого уровня еще никто не достигал». АФП очень заинтересовалась этим сообщением.

После обысков Тгах сказал Mendax'у, что АФП пыталась завербовать его в качестве информатора. Тгах даже сказал, что они предлагали ему новую компьютерную систему, но он не подписался. Еще он сказал, что АФП вроде как продолжает следить за International Subversive. Федералы узнали о том, что Mendax попал в больницу, и заволновались. Его душевное расстройство могло помешать успеху дела.

По поводу обысков Тгах сказал Mendax'у, что в полиции почувствовали, что у них нет выбора. Их позиция была следующей: вы так много наворотили, мы должны остановить это. Вы взломали столько систем, что это уже вышло из-под контроля.

Так или иначе, но к декабрю 1991 года Mendax по совету юриста согласился на разговор с полицией. Mendax'а допрашивал сам Кен Дэй, и хакер, не скрывая, рассказал ему обо всем, что сделал. Правда, он отказался впутывать в это дело Тгах'а и Prime Suspect'а. В феврале 1992 Prime Suspect последовал его примеру и согласился на два допроса. Он тоже был осторожен насчет своих приятелей хакеров. Mendax'а тоже еще раз допросили в феврале 1992-го, а Тгах'а – в августе.

Психическое состояние Тгах'а после обыска оставалось неустойчивым. Он обратился к другому врачу. Психиатрическая служба больницы оказывала ему помощь на дому. Доктор прописал ему лекарства.

Трое хакеров продолжали общаться по телефону. Иногда они встречались лично. Один или другой мог выпасть из поля зрения на какое-то время, но вскоре возвращался в круг единомышленников. Они помогали друг другу и продолжали питать глубокую неприязнь к властям.

Когда им по почте пришли обвинения, они созвонились, чтобы сравнить их. Mendax высказал свои мысли по телефону Prime Suspect'у:

- По-моему, мне нужен адвокат.
- Да. У меня уже есть. Он подыскал и барристера. [p159]
- И как они? – спросил Mendax.
- Не знаю. Думаю, да. Адвокат работает в Legal Aid. Я встречался с ними только пару раз.
- Ага, – Mendax замолчал. – А как их зовут?
- Джон Мак-Лафлин и Борис Кайзер. Они защищали Electron'а.

:)

Тгах и Prime Suspect решили признать себя виновными. Как только они увидели сокрушительные доказательства: перехваченные данные, записи прослушивания телефонных разговоров, данные, конфискованные во время обысков, около дюжины показаний свидетелей из взломанных ими систем, трехсотстраничный доклад Telecom, – они подумали, что лучше во всем сознаться. По крайней мере, они смогут получить некоторый кредит в глазах судьи тем, что сотрудничали с полицией на допросах и сразу признали свою вину, чем сэкономили суду время и деньги.

Но Mendax решил оспорить обвинения. Он изучил дело Pad'а и Gandalf'а и его подоплека выглядела предельно ясно: признай себя виновным и сядешь в тюрьму, борись – и сможешь уйти свободным.

Между серединой 1994-го и 1995 годом Генеральная прокуратура так перетасовала обвинения, что все первоначальные обвинения против Тгах'а, выдвинутые в июле 1991-го, растаяли в свете шести новых, появившихся в 1995 году на Валентинов день. В это же время против Mendax'а и Prime Suspect'а тоже были выдвинуты новые обвинения – в основном за проникновение в компьютер Telecom.

К маю 1995 года на троих хакеров приходилось в целом 63 обвинения: 31 против Mendax'a, 26 на долю Prime Suspect'a и 6 против Тгах'a. Кроме того, NorTel заявил об ущербе в результате деятельности хакеров на общую сумму около \$160 000 – и компания рассчитывала получить компенсацию со стороны ответчиков. Австралийский национальный университет заявил об ущербе на сумму \$4200.

Большинство обвинений базировалось на получении незаконного доступа к коммерческой и другой информации и изменении или уничтожении данных в многочисленных компьютерах. Уничтожение данных было продиктовано не злым умыслом – в основном оно было связано с уничтожением доказательств деятельности хакеров. Но все трое хакеров также обвинялись в некоей форме «подстрекательства». Обвинение заявило, что статьи в журнале *International Subversive* повлекли за собой распространение информации, могущей побудить других к хакингу и фрикингу.

4 мая 1995 года Mendax сидел в офисе своего защитника Пола Голбалли [Paul Galbally]. Они обсуждали предварительные слушания, назначенные на следующий день.

Голбалли был молодым, но уважаемым членом самой известной и уважаемой в Мельбурне семьи юристов. Его генеалогическое древо можно было изучать, как справочник «Кто есть кто» в юридической системе. Его отец, Фрэнк Голбалли, был одним из самых знаменитых адвокатов Австралии по уголовным делам. Его дядя, Джек Голбалли, был известным юристом, министром правительства лейбористов Джона Кейна-старшего, а позже лидером оппозиции парламента Виктории. Его дед со стороны матери, сэр Норман О'Брайан, был судьей Верховного суда, так же как и его дядя с материнской стороны, сын сэра Нормана. Голбалли были скорее династией, а не семьей юристов.

Не желая почивать на лаврах своей семьи, Пол Голбалли работал в тесном, побитом временем офисе без окон в подвальном этаже здания на Уильям-стрит, построенного в 70-е годы. Он занимался исключительно адвокатской деятельностью. Ему больше нравилось спасать людей от тюрьмы, чем отправлять их туда. Работая в тесном контакте с обвиняемым, он всегда находил смягчающие обстоятельства, которые упустило обвинение. Он в каждом видел человека, неважно, в какой степени, и это только говорило в его пользу.

Его жизненные ориентиры отражали образ семьи Голбалли – людей, победивших жизненные обстоятельства. Эта семья была похожа на любую простую семью Австралии. Католики. Ирландцы. Болельщики футбольной команды Collingwood. И само собой, эта семья была очень большой. Пол был одним из девяти детей, его отец тоже вырос в большой семье.

Тридцатичетырехлетний специалист по уголовному праву ничего не знал о компьютерных преступлениях, когда Mendax впервые появился в его офисе. Длинноволосый безработный юнец объяснил, что сможет предложить в качестве гонорара только то, что согласится заплатить Комиссия по юридической помощи штата Виктория – эти слова Голбалли часто приходилось слышать в своей практике. Он согласился.

«Голбалли и О'Брайан» имели очень заслуженную репутацию как юридическая фирма по уголовным делам. Но у преступников, как правило, никогда не водились большие деньги. Большие коммерческие юридические фирмы могли иногда заниматься уголовными делами, но они покрывали любые финансовые неудобства другой, более прибыльной правовой работой. Проталкивание бумаг для Western Mining Corporation могло помочь оплатить содержание шикарных застекленных офисов на пятом этаже. Защита вооруженных грабителей и наркоманов – нет.

Встреча между Mendax'ом и Голбалли 4 мая должна была продлиться около часа. Хотя Mendax должен был предстать на предварительных слушаниях вместе с Prime Suspect'ом на следующий день, именно адвокату Prime Suspect'a Борису Кайзеру отводилась роль распорядителя шоу. Prime Suspect сказал Mendax'у, что ему удалось получить полную поддержку Legal Aid, чего не смогли добиться Голбалли и Mendax. Поэтому Mendax'у и предстояло пройти через слушания без адвоката.

Mendax'у было наплевать. Оба хакера знали, что им предстоит. Их главной целью было дискредитировать заявление обвинения об ущербе – особенно претензии NorTel.

Во время разговора Mendax'a с Голбалли настроение в офисе было бодрым. Mendax чувствовал себя оптимистично. Затем раздался телефонный звонок. Это был Джефф Четтл [Geoff Chettle], юрист из Генеральной прокуратуры. Пока он разговаривал с Голбалли, Mendax смотрел, как лицо его защитника постепенно мрачнеет. Наконец, положив трубку, Голбалли посмотрел на Mendax'е серьезным удрученным взглядом.

– Что случилось? В чем дело? – спросил Mendax.

Голбалли вздохнул прежде чем ответить.

– Prime Suspect решил стать государственным свидетелем против тебя.



:)

Это была ошибка. Mendax точно знал. Все это было одной большой ошибкой. Возможно, Четтл и Генеральная прокуратура неправильно поняли слова Prime Suspect'a. Может быть, его адвокаты что-то напутали. Неважно. В любом случае это ошибка.

В офисе Голбалли Mendax отказался верить в то, что Prime Suspect действительно решил свидетельствовать против него. Во всяком случае до тех пор, пока он своими глазами не увидит подписанные им показания. В эту ночь он сказал одному приятелю: «Посмотрим. Может быть, Четтл просто играет».

Но Четтл вовсе не играл.

Вот они – свидетельские показания – прямо перед ним. Подписанные Prime Suspect'ом.

Mendax стоял рядом с залом заседаний в Городском суде Мельбурна, пытаясь объединить два факта. Во-первых, это был один из его четырех-пяти самых близких друзей. Друг, с которым он делил свои самые большие хакерские секреты. Друг, с которым он всего неделю назад вместе болтался по городу.

Вторым фактом стали показания на шести страницах, подписанные Prime Suspect'ом и Кеном Дзем в штаб-квартире АФП в 13 часов 20 минут днем раньше.

Оба факта никак не выходили у него из головы, борясь друг с другом.

Когда Голбалли приехал в суд, Mendax отвел его в сторону, чтобы детально изучить показания. С точки зрения оспаривания ущерба это не было полным поражением. Prime Suspect, конечно, вообще надеялся избежать обвинения в ущербе. Он мог затронуть множество вопросов, но не стал делать этого. Mendax уже признал вину по большинству из 31 пункта своего обвинительного акта. И он уже рассказал полиции довольно много о своих приключениях в телефонных коммутаторах Telecom.

Тем не менее Prime Suspect как следует поработал в своих показаниях над проникновением в Telecom. Компания принадлежала государству, поэтому суд будет рассматривать фрикинг с коммутаторов Telecom не как обман компании, а как обман всего Содружества. Почему офис Генерального прокурора решил отложить слушания по иску Telecom, первоначально назначенные на февраль 1995 года? Из-за того что Prime Suspect именно тогда дал показания АФП как государственный свидетель? Mendax подозревал именно это. Больше не оставалось никаких сомнений.

Ближайшим испытанием должны были стать предварительные слушания в Городском суде Мельбурна. Не было и речи о том, чтобы Борис Кайзер вступил в борьбу против главного свидетеля обвинения – менеджера информационных систем NorTel. Голбалли пришлось самому проводить перекрестный допрос – нелегкая задача, учитывая сложные технические аспекты дела.

Как только Mendax занял свое место в зале суда, он сразу же увидел Prime Suspect'a. Mendax, не мигая, пристально и твердо посмотрел в глаза своему бывшему другу. Prime Suspect ответил ему невидящим взглядом, затем отвел глаза. На самом деле, даже если бы Mendax захотел ему что-то сказать, он бы не смог. Как государственный свидетель Prime Suspect обладал неприкосновенностью на все время процесса.

Начали появляться юристы. Представитель Генерального прокурора Андреа Павлека [Andrea Pavleka] вошла в зал суда, моментально усилив напряженность в помещении без окон.

Она произвела впечатление на публику. Высокая, стройная и длинноногая, с коротко стриженными льняными кудрявыми волосами, учительскими очками на прелестном носике и заразительным смехом, Павлека не столько вошла в зал суда, сколько впорхнула в него. Ее сияющее лицо просто лучилось счастьем. Как жаль, подумал Mendax, что она не на моей стороне.

Судебное заседание началось. Prime Suspect встал со скамьи подсудимых и признал свою вину по 26 пунктам обвинения в компьютерных преступлениях.

В ходе судебного разбирательства его адвокат Борис Кайзер сказал суду, что его клиент оказал помощь полиции, включая тот факт, что он сообщил АФП о проникновении хакеров в коммутаторы Telecom. Он также сказал, что Telecom не верил (или не хотел верить), что его коммутаторы подверглись такой опасности. Когда Кайзер во всеуслышание вещал, каким образцовым гражданином является его клиент, Кен Дэй, сидя среди публики, закатил глаза.

Судья Джон Тобин [John Tobin] согласился отпустить Prime Suspect'a под залог. Слушание по его делу переносилось на более позднюю дату.

С Prime Suspect'ом все было ясно. Всеобщее внимание переместилось на дело Mendax'a. Представляющий обвинения Джефф Четтл встал, вызвал свидетеля – менеджера NorTel, который прилетел из Сиднея, – и задал ему несколько разогревающих вопросов.

Четтл мог умиротворять людей – или потрясать их – как ему было угодно. Его немолодое об-

ветренное лицо с коротким ежиком волос как нельзя более соответствовало низкому рокочущему голосу. Острый взгляд и сдержанные несуетливые манеры Четтла резко контрастировали с претенциозностью многих адвокатов. Возможно потому, что он явно плевать хотел на традиции XIX века, Четтл всегда ухитрялся выглядеть не совсем уместно в традиционных мантии и парике. Всякий раз, как он вставал, черный капюшон соскальзывал с его узких плеч. Парик сидел на нем набекрень. Он постоянно поправлял его, прилаживая на соответствующее место, как нашкодивший школьник. В суде Четтл выглядел так, словно он вот-вот сорвет заплесневелые атрибуты своей профессии, закатает рукава и ринется в драку. Он производил такое впечатление, будто ему больше по душе находиться в пабе или на футбольной трибуне.

Менеджер NorTel занял свое место. Четтл задал ему несколько вопросов, чтобы продемонстрировать суду, что его свидетель вполне компетентен, поддерживая требование компании о возмещении убытков на \$160 000. Выполнив свою задачу, Четтл сел на место.

Немного нервничая, Пол Голбалли встал во весь рост – более шести футов – и поправил пиджак. На нем был темно-зеленый костюм – настолько темный, что казался почти черным, – с узкими лацканами и узким галстуком в стиле шестидесятых. Он посмотрел вокруг притворно непонимающим взглядом, свойственным только юристам, а затем перевел глаза на судей.

Вначале Голбалли запинаясь и выглядел неуверенным в себе. Возможно, он потерял самообладание из-за технических сложностей вопроса. Файлы WMTP. Файлы UTMP. Аудит RASCT. Архитектура сети. IP-адреса. Он должен был стать экспертом в компьютерах буквально за ночь. Встревоженный Mendax начал передавать ему записки – о чем спросить, как объяснить, что то или иное означает. Постепенно Голбалли вошел в ритм перекрестного допроса.

Во время допроса кто-то из зала суда подошел сзади к Mendax'у, сидевшему на скамье в первом ряду, и передал ему записку через плечо. Mendax развернул записку, прочитал ее, а затем повернулся, чтобы улыбнуться ее автору. Им был Electron.

К тому времени, как Голбалли закончил, он вдребезги разнес большинство из доказательств менеджера NorTel. Развив бешеную энергию при допросе свидетеля, он вынудил менеджера NorTel признать, что тот не так уж много знает об этом инциденте с хакерами. Оказалось, что он даже не работал в компании, когда все это случилось. Его показания, данные под присягой, в значительной степени основывались на информации из вторых рук, а именно: эти показания лежали в основе заявления компании об ущербе в \$160 000. Более того, любой присутствующий на суде мог понять, что менеджер NorTel слабо разбирается в технических проблемах безопасности систем Unix и, возможно, не мог бы даже сделать детальное техническое заключение об инциденте, если бы уже служил в компании в 1991 году. К концу перекрестного допроса сложилось впечатление, что Голбалли знает о Unix больше, чем менеджер NorTel.

Когда Джефф Четтл встал, чтобы в свою очередь допросить свидетеля, ситуация была безнадежной. Менеджер вскоре покинул свидетельское место. По мнению Mendax'а, менеджер NorTel исчерпал кредит доверия.

Заседание суда было перенесено на 12 мая.

После суда Mendax слышал, как Джефф Четтл многозначительно сказал о свидетеле из NorTel: «Этот парень *выбыл* из команды».

Все же это смахивало на пиррову победу Mendax'а. Его защитник нокаутировал свидетеля NorTel, но там, откуда он пришел, были и другие. На полное заседание суда обвинение могло запросто вызвать настоящего профессионала NorTel из Канады, где и был подготовлен 676-страничный отчет об инциденте силами Чарльза Фергюсона и других членов команды безопасности NorTel. Такие свидетели знают, как работает система Unix, и им не понаслышке известно о вторжениях хакеров. Это намного усложнит ситуацию.

Когда через неделю Mendax вернулся в суд, ему было назначено предстать перед Окружным судом штата Виктория, как и предполагалось.

Позже Mendax спросил у Голбалли о возможности выбора: иметь ли дело с полным составом суда или заявить о своей виновности, как двое других хакеров IS. Он хотел знать, как поведет себя в этом случае Генеральная прокуратура. Сохранят ли они свою непримиримую позицию, если он признает свою вину? Может быть, поражение менеджера NorTel на предварительном слушании заставит их пойти на попятную?

Пол вздохнул и покачал головой. Прокурор стоял насмерть. Он намеревался отправить Mendax'а в тюрьму.

Андреа Павлека, яснолицая девушка из Генеральной прокуратуры, лучившаяся счастьем, жаждала крови.

:)

Месяц спустя, 21 июля 1995 года, Prime Suspect прибыл для вынесения приговора в Окружной суд.

Prime Suspect был в напряжении. Он встал рано утром, чтобы убедиться, что его выходной костюм в порядке. Мать приготовила ему плотный завтрак. Тосты, бекон и яйца – все так, как он любит. На самом деле он предпочитал пищу из Мак-Дональдса, но он никогда не говорил об этом матери.

Зал суда был уже переполнен. Газетные репортеры, телеграфные агентства, несколько телеканалов. Были и другие люди, очевидно, ожидавшие своей очереди в суд.

Кен Дэй в темном костюме в мелкую полоску расположился рядом с местом прокурора в зале суда и что-то печатал в своем ноутбуке. Рядом с ним сидел Джефф Четтл. Защитник Prime Suspect'a Борис Кайзер просматривал бумаги в другом углу.

Mendax сидел в заднем ряду и смотрел на своего бывшего друга. Он хотел услышать приговор Prime Suspect'у, потому что, в соответствии с принципом равного наказания за одинаковые правонарушения, решение по делу самого Mendax'a будет подобно исходу дел его товарищей. Хотя Prime Suspect мог рассчитывать на некоторое снисхождение за то, что оказал содействие полиции.

Кучка друзей Mendax'a – ни один из них не принадлежал к компьютерному подполью – просочилась внутрь. Мать хакера в беспокойстве разговаривала с ними. Заседание было объявлено, все расселись по местам. Так вышло, что первым слушалось другое дело. На скамью подсудимых взошел высокий седой мужчина лет сорока пяти с такими голубыми глазами, что это производило демоническое впечатление. Репортеры раскрыли блокноты, а Prime Suspect попытался вообразить, какое преступление мог совершить этот изысканно одетый человек.

Приставание к ребенку.

Этот мужчина не просто приставал к ребенку, он домогался *своего собственного сына*. В родительской спальне. Несколько раз. В Пасхальное воскресенье. Его сыну было тогда меньше десяти лет. Вся семья была в шоке. Мальчик был так напуган и перенес такую психологическую травму, что был не в состоянии давать показания.

И за все это, по словам судьи Рассела Льюиса [Russell Lewis], обращенным к присяжным, этот человек не испытывал угрызений совести. С важным лицом судья приговорил его к минимальному тюремному сроку за подобные преступления – пять лет и девять месяцев.

Затем судебный чиновник огласил дело Prime Suspect'a.

Сидя в глубине зала суда, Mendax поразились странности ситуации. Как может правосудие уравнивать насильника детей и хакера? И все же их обоих судят одного за другим в одном и том же зале Окружного суда.

Борис Кайзер вызвал вереницу свидетелей, каждый из которых рассказывал о нелегкой жизни Prime Suspect'a. Один из них, очень уважаемый психолог Тим Уотсон-Мунро [Tim Watson-Munro], поведал о лечении Prime Suspect'a в больнице Остина и поднял вопрос об ограниченной свободе выбора. Он написал для суда официальное заключение по этому поводу.

Судья Льюис моментально отреагировал на заявление о том, что хакинг – это зависимость. Он громогласно, на весь зал суда, поинтересовался, не напоминает ли присутствующим хакерская деятельность Prime Suspect'a «укол героина».

Кайзер уже прочно встал на свою обычную позицию ведения защиты. Для начала он раскритиковал АФП за то, что они так долго тянули, прежде чем выдвинуть обвинения против его клиента.

«Дело этого парня подлежало разбирательству в срок от шести до двенадцати месяцев после его задержания. Мы словно находимся в США, где человек совершает убийство в двадцать лет, Верховный суд отвергает его апелляцию, когда ему исполняется тридцать, а казнят его в сорок – за преступление, которое он совершил, когда ему было всего двадцать лет».

С большим душевным подъемом Кайзер заметил, что со времени обыска Prime Suspect уже прожил двадцать процентов своей жизни. Затем в его голосе зазвучали возвышенные нотки:

– Этот молодой человек был лишен всякой поддержки в переходном возрасте. Он не рос, он *дрейфовал*... Его мир был так ужасен, что он погрузился в мир фантазий. Он не знал другого способа общения с людьми. Хакинг стал для него физической зависимостью... Если бы он не вышел в киберпространство, чем бы он мог заняться? Поджигать? Грабить? Обратите внимание на его псевдоним. «Первый подозреваемый». Это предполагает некую власть – и несет угрозу. Этот мальчик не имел никакой власти в своей жизни – он обретал ее, сидя за компьютером.

Кайзер не только призвал судью отказаться от мыслей о тюрьме и общественных работах, он просил его не выносить официального приговора.

Юристы обвинения посмотрели на Кайзера так, словно он неудачно пошутил. АФП месяцами выслеживала этих хакеров и почти три года готовила дело против них. А теперь адвокат серьезно говорит о том, чтобы один из главных фигурантов ушел практически безнаказанным, даже без вынесения официального приговора. Это было слишком.

Судья удалился для вынесения приговора. Когда он вернулся, то был краток и говорил только по существу. Никакой тюрьмы. Никаких общественных работ. Официальное обвинение по 26 пунктам. Залог в \$500 на три года хорошего поведения. Конфискация уже устаревшего компьютера Apple, изъятого полицией во время обыска. И возмещение убытков Австралийскому национальному университету в размере \$2100.

На красном и потном от напряжения лице Prime Suspect'a появилось облегчение. Его друзья и родственники улыбались друг другу.

Затем Четтл попросил судью высказать свое мнение по поводу того, что он назвал «вопросом сотрудничества». Он хотел, чтобы судья сказал, что если бы Prime Suspect не согласился стать государственным свидетелем, его приговор был бы гораздо суровее. Генеральная прокуратура укрепляла свои позиции по отношению к своей главной мишени – Mendax'у.

Но судья Льюис заявил, что в этом случае сотрудничество не сыграло никакой роли.

Выходя из зала суда, Mendax вдруг почувствовал тоску. Для него это была хорошая новость, но победа оказалась пустышкой.

Он думал о том, что Prime Suspect разрушил их дружбу и взамен не получил ничего.

Через два месяца после суда над Prime Suspect'ом, Тгах появился в другом зале Окружного суда, чтобы выслушать свой приговор после признания своей вины по шести пунктам обвинения в хакинге и фрикинге. Несмотря на то, что он принимал лекарства, чтобы обуздать свое беспокойство в те моменты, когда ему приходилось находиться вне дома, он очень нервничал, сидя на скамье подсудимых.

Поскольку его обвинение состояло из наименьшего количества пунктов из всех IS-хакеров, Тгах надеялся, что дело не дойдет даже до протокольной записи об осуждении. Удастся ли его адвокату успешно провести защиту – это был другой вопрос. Защитник Тгах'a без конца путался в своих бумагах (казалось, что он так и не сумел разложить их в нужном порядке), говорил довольно бесвязно, повторял одно и то же снова и снова, топчась в своих аргументах на одном месте. Его голос напоминал громкий скрежет рашпиля – это так раздражало судью, что он строго приказал адвокату говорить потише.

В неформальной беседе до суда Джефф Четтл сказал Mendax'у, что, по его мнению, судья Мервин Кимм [Mervyn Kimm] едва ли позволит Тгах'у уйти безнаказанным. Судья Кимм считался крепким орешком. Если бы какой-нибудь букмекер принимал ставки на исход вверенного ему разбирательства, все шансы были бы на стороне обвинения.

Но 20 сентября 1995 года судья показал, что он не настолько предсказуем. Принимая во внимание все обстоятельства, включая приговор Prime Suspect'у и историю душевного расстройства Тгах'a, он не стал приговаривать Тгах'a к наказанию, ограничившись установлением залога в обеспечение хорошего поведения в \$500 сроком на три года.

При вынесении приговора судья Кимм сказал нечто поразительно верное для судьи с крайне незначительным знанием духа хакеров. Строго заявив, что он не намерен умалять серьезность преступлений, он сказал суду, что «факторы конкретного и общего устрашения имеют небольшое значение в определении вынесенного решения». Возможно впервые в Австралии судья признал, что фактор устрашения крайне незначителен, когда речь идет о хакинге и связанном с ним психическом нездоровье.

Исход дела Тгах'a был также благоприятен для Mendax'a. 29 августа 1995 года он признал себя виновным по девяти пунктам обвинения в компьютерных преступлениях и невиновным по всем остальным пунктам. Почти год спустя, 9 мая 1996 года, он признал себя виновным еще по двенадцати пунктам и невиновным по шести. Обвинение опустило все остальные пункты.

Mendax хотел оспорить эти шесть спорных обвинений, затрагивающих Австралийский национальный университет, RMIT, NorTel и Telecom, потому что чувствовал, что в этом случае закон на его стороне. На самом деле закон крайне туманно трактовал обстоятельства по этим пунктам. Настолько туманно, что Генеральная прокуратура и адвокаты Mendax'a пришли к соглашению о том, что вопросы по этим обвинениям следует рассмотреть в Верховном суде штата Виктория.

В представлении дела обе стороны просили Верховный суд вынести постановление не по самому судебному делу, но по статье закона. Защита и обвинение составили согласительное заявление по фактам из дела и, в сущности, просили Верховный суд использовать это заявление как некий прецедент. Предполагалось, что это постановление Верховного суда должно прояснить тончайшие нюансы в законе не только по этому делу, но и по всем подобным делам в будущем.

Дело, заявленное к рассмотрению Верховным судом, – не совсем обычный случай. Трудно представить себе судебное дело, где защита и обвинение приходят к единому мнению по многим вопросам. Но хакерские обвинения Mendax'a представляли собой идеальный случай, и вопросы, вынесенные на рассмотрение Верховного суда штата Виктория в конце 1996 года, были решающими для всех хакерских дел в Австралии в будущем. Что означает «получить доступ» в компьютер? Можно ли говорить о доступе, если кто-то проник в компьютер без использования пароля? А если он или она использовали имя пользователя guest и пароль guest?

Возможно, самым важным вопросом был следующий: можно ли вести речь о «получении доступа» к данным, содержащимся в компьютере, если кто-то способен увидеть эти данные, но фактически их не видит или ему не удается их увидеть?

Классический пример этого состоит в отягчающей версии компьютерного преступления: доступ к коммерческой информации. Если, например, Mendax вошел в компьютер NorTel, в котором хранится чрезвычайно важная коммерческая информация, но на самом деле не прочитал ни одного файла, его обвинят в «получении доступа» или в «получении доступа к коммерческой информации»?

Главный судья Окружного суда согласился с заявлением по делу и направил его на рассмотрение полным составом Верховного суда. Юристы обеих сторон участвовали в деле наряду с судьями Фрэнком Винсентом [Frank Vincent], Кеннетом Хэйном [Kenneth Hayne] и Джоном Колдри [John Coldrey].

30 сентября 1996 года Mendax приехал в Верховный суд, где уже собрались все юристы – кроме его барристера. Пол Голбалли без конца поглядывал на часы, в то время как юристы обвинения раскладывали горы бумаг – плоды месяцев подготовки. Голбалли нетерпеливо мерил шагами роскошный ковер в вестибюле Верховного суда. Барристера все не было.

Барристер Mendax'a без устали работал над его делом так, словно это было дело на миллион долларов. Тщательно изучив судебные прецеденты не только Австралии, Великобритании и США, но и всех стран западной демократии, он приобрел значительную компетентность в области законов по компьютерным преступлениям. В итоге он пришел к такой степени понимания юридических, философских и лингвистических аспектов проблемы, какой иные юристы добиваются всю свою карьеру.

Но где же он? Голбалли уже в пятый раз за последние пять минут звонил по мобильному телефону в свой офис. И новости, которые он услышал, были неутешительными. Ему сообщили, что его помощник заработал истощение на нервной почве. Он не сможет присутствовать на суде.

Голбалли почувствовал, что седеет.

Когда судебное заседание было открыто, Голбалли пришлось встать и объяснить трем самым главным судьям Австралии, почему защита просит двухдневной отсрочки. Джефф Четтл, будучи абсолютным профессионалом, поддержал ходатайство. Хотя эта просьба была не из легких. Время Верховного суда – это крайне ценная и дефицитная вещь. К счастью, перенос дела был одобрен.

Голбалли получил ровно два дня, чтобы найти помощника, который был бы достаточно хорош, настолько свободен и сообразителен, чтобы усвоить огромное количество технической информации в короткое время. Он нашел Эндрю Тинни [Andrew Tinney].

Тинни работал круглосуточно, и к среде 2 октября он был готов. В очередной раз все юристы и хакер собрались в суде.

Но на этот раз дело не заладилось по вине судей. Они велели обеим сторонам провести целый час или около того, объясняя, почему вообще Верховный суд должен выносить заключение по этому делу. Юристы с удивлением переглядывались. Да о чем это они толкуют?

Выслушав короткие аргументы обеих сторон, судьи удалились для вынесения вердикта. Когда они вернулись, судья Хейн зачитал детальное постановление, в котором речь, в сущности, шла о том, что судьи отказываются слушать дело.

По мере того, как судья говорил, становилось ясно, что судьи Верховного суда отказываются рассматривать не только это дело: они не будут рассматривать никаких уголовных дел и в будущем. Ни о компьютерных преступлениях. Ни об убийствах. Ни о мошенничествах. Ни о чем. Они направили послание судьям Окружного суда: не посылайте нам никаких дел, за исключением особых обстоятельств.

Джефф Четтл тяжело опустился на стул, закрыв лицо руками. Пол Голбалли выглядел ошеломленным. Эндрю Тинни готов был прыгнуть со своего стула с криком: «Я угробил два дня на это дело! Вы должны рассмотреть его!» Даже спокойная, невозмутимая и непрошибаемая дама из офиса Генерального прокурора Лесли Тейлор [Lesley Taylor], сменившая на этом посту Андреа Павлека, казалась изумленной.

Это решение имело огромные последствия. Судьям из более низких судебных инстанций навсегда запретили направлять дела в Верховный суд для прояснения точки зрения закона. Mendax вошел в историю судопроизводства, но не так, как он ожидал.

:)

Дело Mendax'a вернулось в Окружной суд.

Он надеялся довести дело до суда в его прежнем виде, но бюджет Legal Aid сильно урезали как раз в это время, и он знал, что у него мало шансов получить достаточно средств, чтобы иметь возможность оспорить обвинения. Это сокращение бюджетных ассигнований заставляло бедных объявлять о своей виновности, оставляя правосудие только для богатых. Хуже того, он чувствовал, что если он признает свою вину, это будет несправедливостью не только в отношении его собственного дела, но и по отношению ко всем будущим хакерским делам. При отсутствии ясности в толковании закона, – которую отказались предоставить судьи, – или решения судей по ключевому вопросу, как в деле Wandii, Mendax считал, что хакерам не стоит рассчитывать на справедливость ни со стороны полиции, ни со стороны судов.

5 декабря 1996 года Mendax признал свою вину по оставшимся шести пунктам. Ему предстояло быть осужденным по всем обвинениям.

В суде в этот день было спокойно. Джефф Четтл отсутствовал. Вместо него дело обвинения вела невозмутимая Лесли Тэйлор. Пол Голбалли выступал за самого Mendax'a. В первых рядах мест для публики сидел Кен Дэй с непроницаемым лицом. Он выглядел немного уставшим. Electron осторожно проскользнул в задние ряды и сдержанно улыбнулся Mendax'у.

Волосы Mendax'a были убраны назад в свободный хвост. Он моргал и хлопал глазами какое-то время, словно внезапно вышел из темноты в ярко освещенный с белыми стенами зал суда.

В кресле восседал судья Росс собственной персоной – краснолицый мужчина в годах с выдающейся нижней челюстью и кустистыми седыми бровями. Сначала он с неохотой взялся за это дело. По его мнению, его должен был рассматривать один из прежних судей – судья Кимм или судья Льюис. До того, как он вошел в зал суда в то утро, он даже не был знаком с их вердиктами.

Лесли Тэйлор резюмировала наказания, определенные для двух других хакеров. Но, казалось, что судья вовсе не пришел от них в восторг. В конце концов он объявил, что рассмотрит дело. «Двое судей решили эту проблему, так почему же третий не сможет? Он сделает это как следует».

Голбалли согласился. Но по мере развития процесса его все больше охватывала тревога: дела шли не так, как он ожидал. Судья Росс ясно дал понять, что лично он отправил бы подсудимого за решетку, хотя бы и условно. Единственное, что могло спасти Mendax'a от тюрьмы, заключалось в принципе равного приговора. Prime Suspect и Трах совершили подобные преступления, поэтому и Mendax'у должны были вынести подобный же приговор.

Росс «выказал некоторое удивление» по поводу позиции судьи Льюиса в вердикте по делу Prime Suspect'a. Насчет принципа равенства он сказал Лесли Тейлор, что порой его «возмущают наказания, наложенные некоторыми судьями». Он спросил ее о возможности не соблюдать правило равенства приговора.

Он сказал суду, что не стал читать распечатки прослушивания телефонных разговоров в материалах дела. В действительности он прочитал только краткое изложение дела. Когда Тейлор упомянула International Subversive, он спросил у нее, что это такое.

Затем он спросил, как пишется слово phreak.

:)

В этот же день, когда судья Росс ознакомился с постановлениями других судей, он вынес по делу Mendax'a вердикт, подобный вердикту Prime Suspect'a, – приговор по всем пунктам, возмещение убытков в \$2100 Австралийскому национальному университету и залог в обеспечение хорошего поведения в течение трех лет.

Но были два отличия. И Prime Suspect, и Трах получили по \$500 в качестве залога за хорошее

поведение; Mendax'у же судья Росс назначил \$5000. Кроме того, судья Льюис дал Prime Suspect'у год, чтобы возместить его долю ущерба в \$2100. Судья Росс постановил, что Mendax должен заплатить в течение трех месяцев.

Судья Росс сказал Mendax'у:

– Я повторяю то, что говорил раньше. Я думаю, что изначально эти преступления заслуживали тюремного срока, но смягчающие обстоятельства превратили его в условный. Приговор вашим подельникам все же вынудил меня немного изменить эту точку зрения.

Он сказал, что убежден в том, что «высокообразованные личности не должны вести себя подобно вам, но я подозреваю, что только высокообразованные личности могут совершать то, что совершили вы».

Термин «зависимость» ни разу не появился в стенограмме слушания.

## 10

### Аутсайдер Anthrax

*В висок нам тычут дулом, под ребра нож суют,  
Но не загнать нас в угол.*

**Песня «Powderworks», альбом «Midnight Oil» (известный также под названием «Blue Album») группы Midnight Oil<sup>47</sup>**

Anthrax не любил работать в команде. Он всегда считал, что другие и есть самое слабое звено в цепи.

Хотя он никогда никому не доверял до конца, он все же общался со многими хакерами и фрикерами и работал с ними время от времени над отдельными проектами. Но он никогда не вступал ни с одним из них в тесные партнерские отношения. Даже если какой-нибудь приятель-хакер захотел бы стукнуть на него в полицию, он не смог бы рассказать обо всей его деятельности. Причина его ограниченных взаимодействий с другими членами андеграунда крылась отчасти и в его изоляции. Anthrax жил в маленьком городке в сельской Виктории.

Несмотря на тот факт, что Anthrax никогда не присоединялся к команде хакеров вроде Realm, он хорошо относился к людям. Ему нравилось говорить с ними по телефону часами. Иногда он получал до десяти международных звонков в день от своих друзей-фрикеров с других континентов. Он мог сидеть дома у друга, слушать музыку и болтать, когда мать приятеля заглядывала в комнату, поднимала бровь и пальцем манила Anthrax'а. «Это тебя. Кто-то из Дании». Иногда это была Швеция, Финляндия, США... Хотя родители его друзей ничего не говорили, они думали, что это довольно странно. Нечасто паренькам, живущим в маленьких городках, звонят из-за рубежа, да еще и перезванивают в другой дом. Нечасто эти пареньки становятся великими фрикерами.

Anthrax обожал телефоны и понимал власть телефонной системы. Многие фриеры считали, что достаточно иметь возможность бесплатно звонить друзьям по всему свету. Или совершать хакерские набеги, не боясь, что тебя выследят. Но для Anthrax'а настоящая власть заключалась в контроле над голосовыми коммуникационными системами, которые делали возможными разговоры по телефону со всем миром. Он путешествовал по голосовым почтовым ящикам других людей, пытаясь представить, как они живут. Он хотел научиться подслушивать телефонные разговоры. Он хотел научиться перепрограммировать телефонные системы, даже разрушать их. Это была реальная власть, многие почувствуют ее на себе.

Желание власти зрело в Anthrax'е на протяжении всего отрочества. Он страстно хотел все знать, все видеть, играть с экзотическими системами других стран. Он стремился узнать назначение каждой системы, то, как она работает, как совмещается с другими системами. Понимание всего этого давало ему контроль.

Его одержимость телефонией и хакингом началась очень рано. Когда ему было около двенадцати, отец повел его на «Военные игры». Все, о чем думал Anthrax, выходя из кинотеатра, – как сильно он хочет стать хакером. Он уже получил свою порцию очарования компьютерами – родители подарили ему на день рождения простейшую машину Sinclair ZX81 с одним килобайтом памяти. Роясь на книжных развалах уличных ярмарок, он нашел несколько подержанных книг о хакерах. Он

---

<sup>47</sup> Слова и музыка: Rob Hirst / James Moginie / Martin Rotsey / Andrew James. © Copyright 1978 Sprint Music. Administered for the World – Warner / Chappell Music Australia Pty Ltd. Used by Permission.

прочитал «За пределами внутреннего круга» Билла Лэндрета [[p160](#)] и «Хакеров» Стивена Леви. [[p161](#)]

К четырнадцати годам Anthrax присоединился к группе мельбурнских подростков под названием The Force. Ее члены обменивались играми для компьютеров Commodor 64 и Amiga. Еще они писали демки – короткие компьютерные программы – и с удовольствием взламывали защиту на копиях игр, а затем менялись ими с другими крэкерами по всему миру. Это было похоже на международный кружок по переписке. Anthrax'у нравилось бросать вызов, взламывая защиту программ, но немногие подростки из его городка разделяли это необычное хобби. Став членом The Force, он познакомился с огромным новым миром людей, думавших так же, как он.

Когда Anthrax впервые прочитал о фрикинге, он написал одному из своих американских знакомых по крэкингу и спросил у него, как начать. Тот прислал ему список номеров телефонных карт AT&T и бесплатный номер прямого набора, по которому австралийские операторы соединялись с американскими. Все карты были просрочены или аннулированы, но Anthrax'у было все равно. Его воображение поразила возможность бесплатно позвонить оператору, находящемуся по другую сторону Тихого океана. Anthrax попытался раздобыть побольше таких номеров.

Обычно он околачивался возле телефонной будки недалеко от дома. Это был неблагополучный район, где жили самые обездоленные горожане, но Anthrax, как правило, занимал телефонную будку по вечерам, не обращая внимания на окружающий его шум, и вручную искал бесплатные номера. Он набирал 0014 – начальные цифры международных бесплатных номеров, а затем несколько цифр наугад. Со временем он стал серьезнее и более ответственно подходить к решению задачи. Он выбирал ряд номеров, например от 300 до 400, и исследовал три последние цифры. Он набирал снова и снова, каждый раз повышая номер на один пункт. 301. 302. 303. 304. Как только он наткнулся на рабочий телефонный номер, он записывал его. Он не истратил ни цента с тех пор, как получил в свое распоряжение все номера, начинавшиеся на 0014.

Anthrax нашел множество действующих номеров, но к некоторым из них были подключены модемы. Поэтому он решил, что настало время купить модем и продолжить дальнейшие исследования. Anthrax был слишком молод, чтобы работать легально, поэтому он соврал насчет своего возраста и нашел работу после уроков, занимаясь вводом данных для эскорт-агентства. В то же время он старался проводить каждую свободную минуту у телефона-автомата, продолжая искать и добавлять новые номера к своему растущему списку бесплатных модемных и операторских номеров.

Сканирование стало одержимостью. Иногда Anthrax стоял у телефона между десятью и одиннадцатью вечера. Иногда это случалось в три ночи. Телефон-автомат был дисковым, что только добавляло Anthrax'у трудностей, и он часто приходил домой с волдырями на кончиках пальцев.

Проработав около месяца, Anthrax смог скопить достаточно денег, чтобы купить себе модем.

Ручное сканирование утомляло, но не больше, чем школа. Anthrax регулярно посещал свою государственную школу, во всяком случае до десятого класса. В основном он делал это под влиянием матери. Она верила в образование и самосовершенствование и хотела дать своему сыну возможности, которых сама была лишена. Именно его мать – она работала медсестрой в психиатрической лечебнице – месяцами экономила и отказывала себе во всем, чтобы купить Anthrax'у его первый настоящий компьютер – Commodor 64 за \$400. Именно она взяла ссуду, чтобы купить сыну более мощный Amiga в 1989 году. Она знала, что ее мальчик очень способный. Раньше он читал ее учебники по медицине, но за компьютерами было будущее.

Anthrax всегда хорошо учился, успевая с отличием с седьмого по десятый классы. За исключением математики. Хотя у него были несомненные способности. В шестом классе он получил награду за то, что разработал маятниковое устройство для вычисления высоты здания, используя начальные знания тригонометрии, которую он еще не изучал. Но все же Anthrax стал меньше посещать школу после десятого класса. Учителя продолжали говорить ему о том, что он уже знал, или то, что можно было гораздо быстрее узнать из книг. Если ему нравилась тема урока, он просто шел в библиотеку и читал об этом.

Примерно в это время атмосфера в семье становилась все сложнее. Семья Anthrax'а не переставала бороться с того самого момента, когда она переехала в Австралию из Англии, – ему в то время

p160

Bill «the Cracker» Landreth, *Out of the Inner Circle: A Hacker's Guide to Computer Security* (Microsoft Press, 1985).

p161

Steven Levy, *Hackers: Heroes of the computer Revolution* (Anchor Press, 1984).

Русский перевод книги доступен на <http://lib.rus.ec/b/69940> (прим. сост. FB2)



было двенадцать лет. Они боролись с бедностью, боролись с суровостью жизни в провинциальном городишке. Кроме того, Anthrax'у, его матери и младшему брату приходилось бороться с расизмом. Они были индийцами.

Этот городок был жестоким местом, пропитанным расовой ненавистью и этнической нетерпимостью. Этнические меньшинства жили обособленно в своих районах, но вторжения на вражескую территорию были обычным делом и почти всегда заканчивались насилием. Это был тот тип города, жители которого были способны превратить в драку обычный футбольный матч. Непростая среда для мальчика полуиндуса, полуангличанина, да еще и с жестоким отцом.

Отец Anthrax'а, белый англичанин, происходил из семьи фермеров. Он был одним из пяти сыновей и учился в сельскохозяйственном колледже. Там он познакомился с сестрой одного из студентов-индусов на стипендии и женился на ней. Этот брак произвел почти сенсацию. Одна местная газета вышла подзаголовком: «Фермер женится на индийской девушке». Семейная жизнь была далеко не безоблачной, и Anthrax часто удивлялся, зачем его отец женился на индианке. Возможно, это был способ протеста против деспотичного отца. Возможно, он просто был влюблен. Или ему нужен был кто-то, над кем он мог бы властвовать. Какой бы ни была причина, дед Anthrax'а принял этот брак в штыки и смешанная семья вскоре была отлучена от больших семейных сборищ.

Когда они переехали в Австралию, у них практически не было денег. В конце концов отец Anthrax'а нашел место офицера в тюрьме Пентридж в Мельбурне, где ему приходилось оставаться почти всю неделю. Он получал небольшое жалование, но работа явно была ему по душе. Мать Anthrax'а начала работать медсестрой. Несмотря на финансовую стабильность, семья не была крепкой. Отец не выказывал никакого уважения ни к своей жене, ни к своим сыновьям, и Anthrax платил ему тем же.

Когда Anthrax был уже подростком, его отец стал совершенно невыносимым. По уик-эндам, когда он бывал дома, он повадился бить Anthrax'а, иногда швыряя сына на пол и пиная его ногами. Anthrax пытался ускользнуть от физической расправы, но у тощего подростка было мало шансов против здорового тюремного офицера. Anthrax и его брат были спокойными детьми. Это казалось путем наименьшего сопротивления грубому отцу в грубом городе. Кроме того, было довольно трудно возражать, учитывая сильное заикание, от которого страдали и Anthrax, и его младший брат в начале подросткового периода.

Однажды, когда Anthrax'у было пятнадцать, он пришел домой и застал там полный разгром. Он прошел в спальню родителей. Его мать была там, очень расстроенная и эмоционально опустошенная. Отца не было поблизости, но Anthrax обнаружил его на диване в гостиной у телевизора.

Anthrax переполняло отвращение, и он ушел на кухню. Вскоре там появился его отец, чтобы приготовить себе поесть.

Anthrax с ненавистью следил за ним. Когда отец выходил из кухни, Anthrax заметил, что на стойке лежит большой нож для мяса. Не успел Anthrax завладеть ножом, как в дверях показался врач из «скорой помощи». Anthrax положил нож и вышел.

Но с этого момента он перестал быть спокойным. Он начал огрызаться дома и в школе, и это стало началом действительно серьезных проблем. В начальных классах и до этого дня его время от времени били. Но с этим было покончено. Когда одноклассник Anthrax'а прижал его к стене в раздевалке и принялся трясти его и размахивать кулаками, Anthrax потерял контроль. На секунду он увидел в лице обидчика лицо своего отца и начал с таким бешенством сопротивляться, что поверг того в жалкое состояние.

Вскоре отец Anthrax'а понял, как можно доставать сына. Агрессор всегда наслаждается слабым сопротивлением жертвы. Это вносит в процесс приятное разнообразие. Anthrax огрызнулся, и его отец получил дополнительную причину для жестокости. Однажды он едва не сломал сыну шею. В другой раз это была рука. Он схватил Anthrax'а и заломил ему руку за спину. Послышался жуткий хруст, а затем наступила резкая боль. Anthrax кричал отцу, чтобы тот прекратил. Но отец только сильнее заламывал его руку, затем сжал его шею. Мать Anthrax'а в истерике умоляла мужа отпустить ее сына. Но он продолжал.

– Послушай, как ты вопишь, – презрительно ухмыльнулся он. – Ты отвратительное животное.

– Сам ты животное, – крикнул Anthrax, снова огрызаясь. Отец швырнул его на пол и принялся бить ногами по голове, по ребрам, везде.

Anthrax сбежал из дома. Он отправился на неделю в Мельбурн и спал где придется – на пустых по ночам строительных площадках, покинутых рабочими, которые в этот час спокойно спали в своих домах. Иногда он даже проникал в приемные покои больниц «скорой помощи». Если медсестра спрашивала, что он здесь делает, Anthrax вежливо отвечал: «Мне позвонили и назначили здесь

встречу». Она кивала головой и уходила.

В конце концов, когда Anthrax вернулся домой, он начал заниматься боевыми искусствами, чтобы стать сильным. Он ждал.

;) )

Anthrax шнырял вокруг шлюза MILNET, когда наткнулся на дверь в System X.<sup>48</sup> Он уже несколько месяцев пытался найти эту систему, потому что однажды перехватил сообщение по электронной почте, которое вызвало его любопытство.

Anthrax проник в шлюз. Шлюз объединяет две разные сети. Это, например, позволяет общаться двум сетям, которые используют разные языки. Шлюз может позволить войти в систему, базирующуюся на TCP/IP, такую, как Unix, из системы с языком DECNET. Anthrax переживал из-за того, что он никак не может пройти через шлюз System X и получить доступ к хостам на другой стороне.

Используя обычные адресные форматы для большинства сетей, он попытался приказать сети выполнить соединение. X.25. TCP/IP. Что бы ни находилось по ту сторону шлюза, оно не отвечало. Anthrax искал повсюду, пока не нашел пример адреса во вспомогательном файле. Ни один из них не работал, но они дали ему ключ к возможному формату адресов.

Каждый адрес состоял из шести цифр. Первые три соответствовали телефонному коду Вашингтона, округ Колумбия. Anthrax взял один из кодов и попытался угадать три последние цифры.

Ручное сканирование, как обычно, утомляло, но если он будет методичным и упорным, что-нибудь получится. 111. 112. 113. 114. 115. И так далее. В конце концов он к чему-то подключился в системе Sunos Unix – и получил полный IP-адрес на ее сообщении о входе. Все остальное было легко. С полным IP-адресом он мог подключиться к System X прямо через Интернет, – минуя шлюз, если захочет. Всегда полезно иметь несколько разных маршрутов, если тебе нужно запутать следы. И самое главное, он сможет проникнуть в System X не только через центральный вход.

Anthrax попробовал несколько обычных вариантов простейших логинов и паролей. Это не сработало. Система требовала более серьезной стратегии нападения.

Он уклонился от запроса логина, вышел из шлюза и отправился на другой сайт Интернета, чтобы посмотреть на System X с безопасного расстояния. Он «прощупал» этот сайт, по крупицам собирая информацию о System X, которую только можно было найти, сделав запрос в Интернете. Он искал лазейку методом тыка. И наконец, он ее нашел. [Sendmail.\[p162\]](#)

В версии System X у Sendmail была щель в системе безопасности, и Anthrax протащил через нее маленькую программу черного хода. Для этого он использовал функцию обработки почты System X и послал в нее «письмо», в котором находилась его скромная компьютерная программа. System X никогда бы не позволила запустить такую программу обычным путем, но она работала, как бомба, посланная по почте. Как только System X открыла письмо, программа выскочила из него и начала работать. Она сообщила системе, что к порту 2001 – интерактивной оболочке – может подключиться со своего компьютера кто угодно, даже не имея пароля.

Порт – это дверь во внешний мир. Компьютеры TCP/IP используют стандартный набор портов для определенных функций. Порт 25 для почты. Порт 79 для Finger. Порт 21 для FTP. Порт 23 для Telnet. Порт 513 для Rlogin. Порт 80 для WWW. В компьютерной системе TCP/IP 65535 портов, но большинство из них совсем не используется. На самом деле средняя система Unix использует только 35 из них, а остальные 65500 бездействуют. Anthrax просто взял один из этих спящих портов, смахнул с него паутину и подключил, использовав черный ход, созданный его крошечной почтовой программой.

Прямое подключение к порту могло повлечь за собой некоторые проблемы, потому что система могла не распознать некоторые команды с порта, например клавишу возврата. По этой причине Anthrax создал для себя учетную запись, которая позволяла ему осуществить вход на сайт и зарегистрироваться как обычному пользователю. Чтобы создать учетную запись и черный ход, ему нужны были более высокие привилегии.

Он начал искать уязвимые места в безопасности System X. Внешне она выглядела вполне надежно, но Anthrax решил использовать ошибку, которая уже успешно показала себя в других местах.

<sup>48</sup> Настоящее название System X не разглашается по соображениям безопасности.

Впервые он узнал об этой ошибке на международной телефонной конференции, где он обменивался информацией с другими хакерами и фрикерами. Брешью в системе безопасности была относительно незаметная программа загрузочного модуля системы. Программа добавляла системе новые функции, но гораздо важнее был тот факт, что после запуска она имела свободный доступ в систему. Это также означало, что другие программы, вызванные программой загрузочного модуля тоже получали привилегированный доступ. Если бы Anthrax'у удалось сделать так, чтобы эта программа запустила одну из его программ – маленький «троян», он получил бы привилегированный доступ в System X.

Ошибка загрузочного модуля ни в коей мере не была гарантией стопроцентного успеха в System X. Большинство коммерческих систем – например, компьютеры банков или кредитных агентств – очистили свои компьютеры Sunos от ошибки загрузочного модуля несколько месяцев назад. Но эта ошибка продолжала присутствовать в военных системах. Те были похожи на черепах – твердые снаружи, но мягкие и уязвимые внутри. Поскольку ошибка не могла быть использована, если хакера не было внутри системы, то чиновники, ответственные за безопасность военных компьютеров, не придавали ей особого значения. До System X Anthrax побывал во многих военных системах, и, по его опыту, больше 90 % компьютеров Sunos никогда не обращали внимания на ошибку.

Имея обычные привилегии, Anthrax не мог заставить программу загрузочного модуля запустить своего «трояна». Но он мог схитрить, чтобы сделать это. Секрет заключался только в одной клавише: /.

Компьютеры Unix в чем-то похожи на дипломатический протокол: небольшие вариации могут полностью изменить смысл. Хакеры тоже понимали значение мелких изменений.

Фраза `/bin/program` читалась в системе Unix совершенно отлично от фразы `bin program`.

Один простой символ – / – создавал огромную разницу. Компьютер Unix читал символ / как дорожный указатель. Первая фраза говорит компьютеру: «Следуй по дороге в дом пользователя по имени `/bin/`, и когда ты окажешься внутри, вызови файл под названием `program` и запусти его». Но пробелы говорили компьютеру нечто совершенно другое. Anthrax знал, что в этом случае компьютер должен был выполнить исходную программу. Вторая фраза говорила машине: «Найди программу под названием `bin` и запусти ее».

Anthrax подготовился к атаке на программу загрузочного модуля, установив свою собственную программу под названием `bin` во временной директории System X. Если ему удастся заставить System X запустить его программу с корневыми привилегиями, он получит высокий уровень доступа в систему. Когда все было готово, Anthrax заставил систему прочитать символ / как пробел. Затем он запустил программу загрузочного модуля и стал наблюдать. System X начала охоту за программой `bin`, быстро нашла ее и запустила «трояна» Anthrax'a.

Хакер наслаждался моментом, но останавливаться было рано. Несколькими быстрыми нажатиями клавиш он добавил строку к файлу пароля, создавая для себя базовую учетную запись. Он уничтожил соединение с портом 2001, двинулся кружным путем по другому маршруту, используя шлюз 0014, и зарегистрировался в System X с помощью вновь созданной учетной записи. Он испытал ни с чем не сравнимое чувство, войдя в систему через парадный вход.

Оказавшись внутри, Anthrax быстро осмотрелся. Система поразила его. В ней было только три пользователя-человека. Это было необычайно странно. Большинство систем имеют сотни пользователей. Даже маленькой системой может пользоваться 30–40 человек. А эта система была далеко не маленькой. Anthrax сделал вывод, что System X не была обычной машиной для отправки и получения электронной почты. Это была операционная машина. Она что-то *делала*.

Anthrax стал думать о том, как стереть свои отпечатки и обезопасить свою позицию. Хотя он едва ли обозначил свое присутствие, кто-нибудь мог обнаружить его появление, просто посмотрев на регистрационный список учетных записей в файле пароля. Anthrax дал своей контрабандной учетной записи незаметное имя, но он вполне допускал, что эти трое пользователей знали свою систему очень хорошо. Раз их было всего трое, возможно, с этой системой нужно было возиться, как с ребенком. После всех предпринятых усилий Anthrax нуждался в бдительной няньке, как в дырке в голове. Он поспешил укрыться в тени.

Он убрал себя из файлов WTMP и UTMP, где содержалась информация о том, кто был онлайн и кто до сих пор находится в системе. Anthrax не стал невидимкой, но админу пришлось бы внимательно изучить сетевые соединения системы и список процессов, чтобы обнаружить его. Следующая остановка – программа входа.

Anthrax не мог использовать слишком долго свою новую учетную запись для парадного входа – риск, что его обнаружат, был очень велик. Если он будет постоянно проникать в компьютер таким способом, админ в конце концов найдет его и уничтожит его учетную запись. Дополнительная учет-

ная запись пользователя в системе, где их было всего трое, стала бы верным провалом. Потеря же доступа в System X, когда все стало таким интересным, вовсе не входила в планы Anthrax'a.

Anthrax откинулся на спинку стула и расправил плечи. Его хакерская комната представляла собой бывшую гардеробную, хотя ее прежний статус угадывался с трудом. Она выглядела, как чулан, – и в чулане царил страшный кавардак. Вся комнатка была по колено завалена исписанными бумагами, большинство из которых было покрыто с обеих сторон списками номеров. Время от времени Anthrax собирал бумаги и запихивал их в огромные мешки для мусора. В комнате всегда имелась пара-тройка таких мешков. Anthrax всегда имел смутное представление о том, куда он засунул те или иные записи. Когда он что-то искал, он вываливал содержимое мешка прямо на пол, рылся в этой куче и возвращался к компьютеру. Когда бумажный вал достигал критической массы, он снова запихивал все в мусорный мешок.

Компьютер Amiga 500 и старый телевизор Panasonic вместо монитора стояли на маленьком столе рядом со швейной машинкой матери. Ящики стола были битком набиты журналами вроде *Compute* и *Australian Communication* вперемешку со справочниками по компьютерам Commodor, Amiga и системам Unix. Оставшееся место занимала старая стереосистема Anthrax'a и коротковолновое радио. Если Anthrax не слушал свою любимую передачу – программу для хакеров с какого-то подпольного радио в Эквадоре, – он настраивался на Московское радио или Всемирную службу BBC.

Anthrax думал, что делать с System X. Эта система поразила его воображение, и он намеревался постоянно посещать ее.

Пора было заняться патчем[*p163*] для логина. Она заменяла обычную программу регистрации в системе и обладала специальной функцией – мастер-пароль. Такой пароль был подобен дипломатическому паспорту. Он позволил бы ему сделать все что угодно и попасть куда угодно. С мастер-паролем он мог зарегистрироваться как любой пользователь. Более того, если войти в систему через мастер-пароль, то ни один регистрационный файл не отражал твоего появления и ты не оставлял следов. Но вся прелесть патча заключалась в том, что во всем остальном она работала как обычная программа. Обычные компьютерные пользователи – все трое – могли, как обычно, регистрироваться своими паролями и даже не подозревать о том, что Anthrax бывает в их системах.

Он думал о том, как установить патч. Установить такую штуковину в System X – не то же самое, что заштопать пару джинсов. Он не мог просто прилепить полоску ткани и наспех пришить ее ниткой любого цвета. Это было похоже на починку кашемирового пальто. Ткань должна была идеально подходить по цвету и фактуре. Патч требовал высококачественных невидимых швов и точного соответствия размерам.

В каждом файле компьютерной системы существуют три разные даты: дата создания, дата изменения и дата последнего доступа. Проблема заключалась в том, что патч для логина должен был иметь ту же дату создания и изменения, что и оригинальная программа логина, чтобы не вызвать подозрений. Добыть эти данные было нетрудно, гораздо сложнее было перенести их в патч. Дата последнего доступа не имела значения, поскольку она менялась всякий раз при запуске программы – при подключения пользователя в System X.

Если бы Anthrax удалил оригинальную программу логина и поставил бы на ее место патч, на нем стоял бы штамп с новой датой создания. Он знал, что нет никакого способа изменить дату создания, кроме изменения времени всей системы, – а это могло вызвать проблемы в других областях System X.

Первое, что делает хороший админ при появлении подозрений насчет взлома, – старается обнаружить все файлы, созданные или измененные за последние несколько дней. Малейшее неверное движение, и хороший админ обнаружит патч Anthrax'a через пять минут.

Anthrax записал даты создания и изменения на клочок бумаги. Они скоро ему понадобятся. Он также сделал пометку о размере файла логина.

Вместо того, чтобы разорвать старую программу и ввести на ее место совершенно новую, Anthrax решил наложить патч, скопировав его на место старой программы. Он загрузил свой патч логина вместе с находящимся в нем мастер-паролем в программу, но пока не установил ее. Он назвал свой патч *troj* (сокращение от «троян»). Он напечатал:

cat<troj>/bin/login

Команда cat сказала компьютеру: «Сходи за данными файла troj и помести их в файл /bin/login». Он сверился с записанными на бумаге оригинальными данными создания и изменения файла и сравнил их с датами патча. Дата создания и размер совпадали с оригиналом. Дата изменения все еще отличалась, но Anthrax прошел только две трети пути.

Anthrax начал пришивать последний уголок патча при помощи малоизвестной функции команды /usr/5bin/date. Затем он изменил дату изменения на оригинальную дату файла логина.

Он сделал несколько шагов назад, чтобы полюбоваться на свою работу с расстояния. Новенький патч идеально соответствовал оригиналу. Нужный размер. Та же дата создания. Та же дата изменения. Установив патч, он стер привилегированную учетную запись пользователя, которую создал при проходе через порт 2001. Когда уходишь, убирай за собой мусор.

Теперь пора позабавиться. Оглядеться. Anthrax занялся e-mail, чтобы лучше понять, куда это он попал. Там было множество отчетов от подчиненных троих пользователей о покупке оборудования, докладов об успехах в каком-то проекте, о модернизациях. Что это за проект?

Anthrax вошел в обширную директорию. Он открыл ее и обнаружил в ней около сотни поддиректорий. Открыл одну из них. Она была огромной и содержала сотни файлов. В самом маленьком файле находилось, возможно, около 60 компьютерных экранов с совершенно нечитабельной информацией. Цифры, буквы, контрольные коды. Anthrax не мог понять, где начало, а где конец файла. Это было похоже на двоичные файлы. Вся поддиректория была заполнена тысячами страниц какой-то каши. Он подумал, что они похожи на файлы некоей базы данных.

Поскольку у него не было программы, необходимой для того, чтобы разобраться в этой каше, Anthrax огляделся вокруг в поисках более внятной директории.

Он вскрыл один файл и обнаружил, что это список. Имена и номера телефонов сотрудников большой телефонной компании. Рабочие телефоны. Домашние телефоны. Что ж, по крайней мере, это дало ему ключ к пониманию природы проекта. Что-то связанное с телекоммуникациями. Что-то настолько важное, что военным понадобились номера домашних телефонов руководителей проекта.

Следующий файл подтвердил это. Другой список, совершенно особенный. Сундук с золотом и кусочек радуги. Венец карьеры хакера.

Если бы в правительстве США появилось хотя бы легкое подозрение по поводу того, что происходит в этот момент, головы полетели бы незамедлительно. Если бы правительство узнало, что иностранец, да еще и последователь течения, которое американская проправительственная пресса окрестила экстремистской религиозной группой, получил в свое распоряжение такую информацию, Министерство обороны, наверное, призвало бы на помощь все мыслимые службы правопорядка.

:)

Мать Anthrax'a умела создать уют для своей семьи, но отец продолжал жестоко разрушать его. Время, проведенное с друзьями, сияло, подобно солнечным зайчикам, на фоне мрачной картины распада семейной жизни Anthrax'a. Его специальностью были розыгрыши. Еще ребенком он с удовольствием предавался им, а когда он вырос, его шутки стали более изобретательными. Как здорово быть фрикером. Это давало возможность разыгрывать людей в любой части света. Это было круто.

Большую часть своих выходов Anthrax делил с друзьями. Он звонил на какую-нибудь голосовую конференцию фрикеров и хакеров. Хотя он не настолько доверял другим, чтобы вместе работать над новыми проектами, но был ничуть не против общения. Способ проникновения на конференцию был его личным делом. Принимая во внимание то, что он тщательно следил за своими словами во время конференции, он считал, что практически ничем не рискует.

Он присоединялся к конференции, используя разные фрикерские методы. Одним из самых любимых было использование службы мультинациональной корпорации Dialcom. Служащие компании звонили туда, говорили свой личный номер и оператор соединял их с нужным им местом совершенно бесплатно. Все, что нужно было Anthrax'у, – действующий личный номер.

Иногда это было нелегко, но порой ему везло. В тот день, когда Anthrax решил позвонить в службу Dialcom, удача улыбнулась ему. Он звонил из своего любимого телефона-автомата.

– Назовите ваш код, сэр, – сказал оператор.

– Говорит мистер Бейкер. У меня тут листок бумаги, а на нем очень много номеров. Я недавно работаю в компании. Я не знаю точно, какой из них вам нужен.

Anthrax пошелестел бумагой возле трубки.

– Сколько в нем цифр?

– Семь.

Вот и отлично. Оставалось найти семь цифр. Anthrax посмотрел через улицу на небольшую закусочную. Никаких номеров. Затем его внимание привлек номер на машине. Он продиктовал с него первые три цифры и позаимствовал оставшиеся четыре с номера другой машины.

– Спасибо. Я вас соединяю, мистер Бейкер.

Действующий номер! Невероятная удача! Anthrax эксплуатировал этот номер для всего, что казалось ему достойным. Он звонил на голосовые конференции и фрикерские мосты. Доступ только разжигал его страсть.

Затем он дал этот номер одному приятелю из Аделаиды – ему нужно было позвонить за границу. Но когда он набрал код, оператор заартачился.

– ВЫ НЕ МИСТЕР БЕЙКЕР!

Что?

– Я мистер Бейкер. У вас есть мой код.

– Вы определенно не он. Я знаю его голос.

Приятель позвонил Anthrax'у, и тот чуть не лопнул от смеха. Затем он позвонил в Dialcom и изменил свой код! Это было забавно. Но все же этот инцидент напомнил ему, насколько безопаснее работать в одиночку.

В провинции тяжело было заниматься хакингом, и Anthrax стал фрикером по необходимости, а не только из баловства. Почти для всего нужно было звонить на дальние расстояния, и он постоянно искал способы звонить бесплатно. Он обратил внимание, что когда он набирал некоторые номера 008 – бесплатные звонки, – телефон звонил несколько раз, щелкал, затем делал короткую паузу, прежде чем прозвонить еще несколько раз. В конце концов представитель компании или оператор брали трубку. В одном из многих журналов и учебников по телекоммуникациям, составлявшим его постоянный круг интересов, Anthrax прочитал о дивертерах – особых устройствах, предназначенных для автоматического продвижения звонков. Щелчок означал, что звонок проходит через дивертер, и Anthrax предположил, что если он смоделирует правильный тон в нужный момент, он сможет сделать так, что звонок пройдет мимо агента клиентской службы компании. Кроме того, след любого соединения не пойдет дальше коммутаторов компании.

Anthrax собрал несколько номеров 008 и поэкспериментировал с ними. Он обнаружил, что если очень быстро ввести другой номер во время набора – сразу после щелчка, то он может увести линию куда ему нужно. Он использовал номера 008, чтобы звонить на телефонные конференции по всему миру. Он общался с другими фрикерами, в основном канадцами – членами UPI из Торонто или монреальской группы NPC, которая выпустила учебник для фрикеров на французском языке. Разговоры на фрикерских телефонных конференциях или телефонных мостах, как они сами их называли, неизбежно сворачивали к приколам. А уж эти канадские парни умели *прикалываться!*

Однажды они набрали номер телефона службы спасения большого канадского города. Используя свой вариант канадского акцента, Anthrax взял на себя роль «полицейского офицера, нуждающегося в помощи». Оператор спросил, где он находится. Фрикеры решили, что это будет кафе-мороженое «Голубая лента». Они всегда выбирали место в пределах видимости по крайней мере одного из участников, чтобы можно было понять, что там происходит.

В следующую долю секунды один из пяти фрикеров, осторожно подслушивавших разговор, кашлянул. Это был короткий резкий кашель. Операторша даже отпрянула.

– Это был ВЫСТРЕЛ? В тебя СТРЕЛЯЛИ? Алло, Джон?

Она на мгновение оторвалась от трубки и фрикеры услышали, как она говорит кому-то в глубине комнаты: «Офицер ранен».

В такие минуты события разворачиваются очень быстро. Что дальше?

– Да. Да-а.

Оказывается, когда ты пытаешься загнать смех подальше в глотку, это очень похоже на звуки, которые издает раненый человек. Просто удивительно.

– Джон, не молчи. Скажи мне что-нибудь, – умоляла операторша, пытаясь удержать Джона в сознании.

– Я ранен. Я ранен, – Anthrax держал ее в напряжении.

Затем он отключил ее от линии конференции. Фрикер, живущий по соседству с кафе-мороженым объявил, что улица блокирована полицейскими машинами. Они окружили кафе и лихорадочно искали раненого товарища. Прошло несколько часов, прежде чем полиция поняла, что кто-то сыграл с ними подлую шутку.

Но самой любимой мишенью Anthrax'a был мистер Мак-Кенни, придурковатый провинциал с американского Юга. Anthrax взял его номер наугад, но первый же звонок оказался таким смешным, что он продолжал звонить ему. Он звонил ему годами. Разговор всегда был одним и тем же.

– Мистер Мак-Кенни? Это Питер Бейкер. Я бы хотел получить назад мою лопату, если это вас не затруднит.

– У меня нет вашей лопаты.

– Как же, ведь я одолжил ее вам. Уж два года как. Теперь она мне нужна.

– Я никогда не брал у вас никакой лопаты. Убирайтесь.

– Нет, брали. Вы взяли у меня мою лопату. И если вы не вернете ее, я сам приду за ней, и вам это не понравится. Ну что, когда вы вернете мне мою лопату?

– Черт! У меня нет вашей чертовой лопаты!

– Отдайте мне лопату!

– Хватит мне звонить! У меня никогда не было вашей долбаной лопаты. Отстаньте от меня!

Гудки.

В девять утра. В восемь вечера. В два ночи. Мистер Мак-Кенни лишился покоя, пока не признался, что взял лопату у мальчишки, который жил на другой стороне мира.

Иногда Anthrax устраивал розыгрыши поближе к дому. *Trading Post*, местный еженедельный листок частных объявлений о купле и продаже, был отличной стартовой площадкой. Начало всегда было невинным, чтобы жертва заглотила приманку.

– Да, сэр, я видел ваше объявление. Вы хотите купить ванну? – Голос Anthrax был крайне серьезен. – У меня есть ванна на продажу.

– Да? Что за ванна? У вас есть размеры и номер модели?

А еще говорят, что фриеры странные.

– О, номера модели нет. Но она метра полтора в длину, на ножках в виде лап с когтями. Она старинная и не совсем белая. Но есть одна проблема.

Anthrax замолчал, предвкушая главный момент.

– О? И какая же?

– В ней мертвое тело.

Словно бросить булыжник в тихий пруд.

:)

В списке в System X были номера модемного доступа вместе с парами имен пользователей и паролей для каждого адреса. Имена пользователей вовсе не были похожи на обычные варианты типа jsmith или jdое, и слова паролей тоже едва ли можно было найти в словаре. 12[AZ63. K5M82L. Эти пароли и имена пользователей мог запомнить только компьютер.

Это, естественно, имело смысл, поскольку они прежде всего предназначались для компьютера. Он сам генерировал их по принципу случайного выбора. Список вряд ли можно было назвать удобным для пользователя. В нем не было заголовков, которые показывали бы, о чем идет речь в том или ином пункте. Это тоже имело смысл. Список не должны были читать люди.

Но в то же время в списке порой встречались комментарии. Программисты иногда помещают строчку комментариев в код. Комментарии описывают, каким образом компьютер пропускает слова при интерпретации команд. Они предназначены для других программистов, имеющих дело с этим кодом. В данном случае комментарии представляли собой названия мест. Форт-Грин. Форт-Майерс. Форт-Ричи. Десятки и десятки фортов. Почти половина из них находилась за пределами США. Например, на Филиппинах, в Турции, в Германии, в Гуаме. В местах американского военного присутствия.

Эти базы, конечно, не были секретом для местных жителей, тем более для американцев. Anthrax знал, что любой человек мог узнать о существовании этих баз совершенно легально. Большинство людей никогда об этом не задумывается. Но если бы им на глаза попался такой список, в особенности извлеченный из недр военного компьютера, это задело бы их за живое. Они поняли бы, что армия США присутствует везде.

Anthrax вышел из System X, уничтожил все свои соединения и повесил трубку. Пора идти дальше. Следуя по маршруту через отдаленные соединения, он позвонил по одному из номеров списка. Комбинация имени пользователя и пароля сработала. Он осмотрелся. Это было то, чего он и ждал. Телефонный коммутатор. Похожий на NorTel DMS 100.

Как правило, хакеры и фриеры обладают огромным опытом. В пределах Австралии Anthrax

был специалистом по сети X.25 и королем систем голосовых почтовых ящиков, и весь андеграунд признавал его таковым. Он знал Trilogues лучше, чем любой техник компании. Он знал системы VIMB Meridian лучше, чем почти кто бы то ни было в Австралии. Во фрикерском сообществе он считался экспертом мирового класса по системам VMB Aspen. Но у него почти не было опыта в DMS 100.

Anthrax лихорадочно начал искать в своих хакерских дисках текстовый файл по DMS 100, который он скопировал на одной из подпольных BBS. Время поджимало. Он не хотел слишком долго торчать в коммутаторе, минут 15–20, не больше. Чем дольше он оставался в системе, не имея особого представления о том, как работает эта штука, тем выше был риск, что его смогут проследить. Когда он, наконец, нашел диск с текстовым файлом, он стал просматривать его, все еще находясь онлайн на телефонном коммутаторе. Фрикерский файл показал ему основные команды, которые позволяли ему прощупать коммутатор на предмет базовой информации и при этом не слишком потревожить систему. Он не хотел развивать слишком бурную деятельность из опасения непреднамеренно повредить системе.

Anthrax не был авторитетом по DMS 100, но у него был друг за океаном, настоящий гений по части оборудования NorTel. Anthrax передал список своему другу. Тот подтвердил, что это на самом деле коммутатор DMS 100 на военной базе США. Но он не входил в обычную телефонную систему. Этот коммутатор был частью военной телефонной сети.

В случае войны армия не хотела зависеть от гражданских телефонных систем. Даже в мирное время голосовые коммуникации между военными безопаснее осуществлять вне гражданских коммутаторов. По этой и по многим другим причинам у военных есть отдельные телефонные сети, так же как они пользуются отдельными сетями для передачи своих данных. Эти сети работают аналогично обычным и в некоторых случаях могут связываться с остальным миром, соединяя свои коммутаторы с гражданскими.

Получив консультацию эксперта, Anthrax мгновенно принял решение. Он решил запустить сниффер. Теперь System X стала еще интереснее, и он не хотел упустить драгоценную минуту, подбирая дичь, когда дело дойдет до главного.

Программа сниффер использовалась очень широко и, по слухам, была написана Unix-хакером из Сиднея по имени Rockstar.<sup>[p164]</sup> Сниффер вошел в систему под безобидным названием, втихомолку отслеживая каждого, кто входил в систему и выходил из нее. Он записывал 128 первых символов каждого telnet-соединения, проходившего по сетевому кабелю, к которому была подключена System X. Эти 128 байтов включали в себя имя пользователя и пароль, необходимые для входа в систему. Сниффер был эффективной программой, но его работа требовала времени. Обычно он рос как эмбрион в матке – медленно, но неуклонно.

Anthrax решил вернуться в System X через двенадцать часов, чтобы проведать своего ребеночка.

;) )

– Почему вы смотрите эти видеоклипы с черномазыми?

Этот оскорбительный вопрос был вполне типичным для отца Anthrax’a. Он часто проносился по дому, оставляя за собой следы разрушения.

Но вскоре Anthrax начал подрывать его власть. Он обнаружил отцовские секреты в старом компьютере Commodore 64. Письма – множество писем – его семье в Англию. Злобные, расистские, грязные письма о том, как глупа его жена. Что приходится постоянно говорить ей о том, как сделать то или другое. Типичная индианка. Как он жалеет, что женился на ней. Он писал и о других вещах, слишком неприятных, чтобы говорить о них.

Anthrax поставил отца перед фактом, тот сначала все отрицал, затем велел сыну заткнуться и заниматься своими делами. Но Anthrax рассказал обо всем матери. Напряжение между родителями усилилось, и они впервые пошли к семейному консультанту.

Но отец не перестал писать письма. Он поставил в компьютер программу защиты пароля, чтобы сохранить свои дела втайне от сына. Но это был напрасный труд. Отец Anthrax’a выбрал не того посредника для своих откровений.



Anthrax показал матери новые письма и продолжал задира́ть отца. Когда обстановка окончательно накалилась, Anthrax сбежал к друзьям. Однажды они были в ночном клубе, где кто-то стал говорить Anthrax'у гадости, называя «пожирателем карри» и кое-кем похуже.

Это был предел. Ярость, загнанная внутрь все эти годы, вырвалась на поверхность, и Anthrax с бешенством обрушился на обидчика, жестоко отделав его при помощи приемов тхэквондо. Тот был весь в крови, и Anthrax почувствовал облегчение. Месть была сладкой.

После этого инцидента Anthrax стал заводиться с пол-оборота. Он терял контроль, и иногда это пугало его. Хотя иногда он сам нарывался на неприятности. Однажды он выследил одного особенно отвратительного персонажа, который пытался изнасиловать одну из его подружек. Anthrax вырвал у него нож, но это происшествие имело мало общего с оскорблением девушки. Его ярость спровоцировало неуважение. Этот тип знал, что девушка была с Anthrax'ом. Попытка изнасилования походила на плевков в лицо.

Возможно, именно это толкнуло Anthrax'а к исламу – потребность в уважении. Он открыл ислам в шестнадцать лет, и это изменило его жизнь. Он нашел Коран в школьной библиотеке, когда писал сочинение по религии. Примерно в это же время он стал слушать рэп. Больше половины рэперов в его коллекции были мусульманами, и многие из них пели о «Нации ислама» и ее харизматичном лидере, преподобном Луисе Фаррахане. Их песни описывали несправедливость белых по отношению к черным. Они настаивали, чтобы черные требовали уважения к себе.

Anthrax нашел журнал о Фаррахане и начал читать книги типа «Автобиография Малькольма Х». Затем он позвонил в штаб-квартиру «Нации ислама» в Чикаго и попросил их прислать ему побольше информации. Он получил посылку с газетой *The Final Call*<sup>[p165]</sup> и другой литературой, которая стала появляться всюду в доме. Под телепрограммой. На журнальном столике. В стопке газет. На компьютере. Anthrax часто выбирал время, чтобы почитать некоторые статьи матери вслух, пока она делала какую-нибудь домашнюю работу.

В середине 1990 года, когда Anthrax был в 11 классе, его отец захотел, чтобы мальчик перешел в закрытую католическую школу в Мельбурне. Школа была недорогой, и семья могла напрячься и заплатить за обучение. Anthrax был не в восторге от этой затеи, но отец настоял.

Anthrax и его новая школа плохо сочетались друг с другом. В школе считали, что он задает слишком много вопросов, а Anthrax находил, что школа дает на них слишком мало ответов. Лицемерие католической церкви раздражало Anthrax'а и все глубже толкало его в объятия «Нации ислама». Как он мог уважать общественный институт, который одобрял рабство в качестве правомочного и прогрессивного метода обращения людей в свою веру? Школа и Anthrax расстались далеко не друзьями после первого же семестра.

Католическая школа только усилила чувство неполноценности, которое мучило Anthrax'а годами. Он был аутсайдером. У него был не тот цвет кожи, не тот внешний вид, он был слишком умен для своей школы. Но преподобный Фаррахан сказал ему, что он вовсе не хуже других. Он говорил Anthrax'у с магнитофонной записи: «Я знаю, что ты испытывал унижения из-за цвета твоей кожи. Позволь мне сказать, почему. Позволь мне рассказать тебе о происхождении белой расы и о том, как они пришли на Землю, чтобы творить зло. Они есть не что иное, как враги Востока. Но белые не были первыми людьми на Земле».

Anthrax находил глубокую справедливость в учении «Нации ислама». Межрасовые браки не работают. Белый мужчина женится на небелой женщине, потому что ему нужна рабыня, а не из любви. Ислам уважает женщину гораздо больше, чем западные религии. Возможно, это не тот тип уважения, которое привыкли оказывать женщинам западные мужчины, но он видел в своем собственном доме, чего стоит их уважение, и был о нем невысокого мнения.

Anthrax прочитал слова достопочтенного Элайджи Мухаммада, основателя «Нации ислама»: «Врагу не нужно принимать обличие дьявола. Он может быть твоим отцом, твоей матерью, твоим братом, твоим мужем, твоей женой, твоими детьми. Во многих случаях он притаился в твоей семье. Настало время великого разделения правоверных мусульман и нечистой белой расы». Anthrax смотрел на собственную семью и видел того, кто явно был дьяволом. Белым дьяволом.

«Нация ислама» подпитывала разум Anthrax'а. Он прочитал всю литературу, упомянутую в каждом выпуске *The Final Call*. Такие книги, как «Черная Афина» Мартина Бернела<sup>[p166]</sup> и «Кру-

---

p165

Последний призыв.

p166

Martin Bernel, *Black athena: The afroasiatic Roots of Classical Civilization: The Archaeological and Documentary Evidence*

шение демократии» Ноама Хомски<sup>[p167]</sup> трактовали общие темы заговора и угнетения имущими неимущих. Anthrax прочитал их.

Трансформация Anthrax'а произошла примерно за шесть месяцев. Он не слишком много говорил об этом с родителями. Это было его личное дело. Но его мать позже сказала ему, что его обращение совсем не удивило ее. Его прадед был мусульманским теологом и духовным лицом в Индии. Это была судьба. Его обращение стало закономерностью, оно замкнуло круг.

Его интересы в исламе находили и мирские отдушины. На стене в спальне Anthrax'а появился гигантский черно-белый постер с Малькольмом Х. К нему вскоре присоединилась большая фотография Элмера Пратта, лидера лос-анджелесских «Черных пантер». На нем была надпись: «Трус умирает миллион раз, храбрец лишь однажды». Оставшаяся часть стены от пола до потолка была покрыта постерами с рэп-группами. На одном из книжных шкафов красовался традиционный индийский меч. Его дополняла растущая коллекция книг по боевым искусствам. Любимое издание «Искусства войны» Сун Цзы стояло рядом с «Одиссеей» Гомера, «Властелином Колец», «Хоббитом», несколькими старыми книгами из серии «Башни и драконы» и трудами по мифологии Индии и Египта. На полках не было ни одной книги с научной фантастикой. Anthrax брил голову. Возможно, его мать и не удивилась его принятию ислама, но брить голову – это уже чересчур.

Anthrax следовал учению «Нации ислама» с той же страстью, с которой он предавался хакингу. Он заучивал наизусть речи Фаррахана и начал говорить так же, как он, при случае высказываясь об «этих белых голубоглазых дьяволах». Он цитировал людей, с которыми познакомился через «Нацию ислама». Людей, которые считали, что Федеральный резервный банк США контролируют евреи. Людей, которые говорили о крючконосых еврейских пожирателях мацы, выползших из своих нор. Anthrax отрицал Холокост.

– Ты похож на маленького Гитлера, – сказал Anthrax'у отец. Его отцу не нравилось появление в доме литературы «Нации ислама». Она явно пугала его. Получение по почте брошюр, призывающих к свержению правительств, никак не вязалось с окружением тихой улочки провинциального городка.

– Будь осторожен, – предупреждал он сына. – Все эти штуки в нашем почтовом ящике просто опасны. Ты можешь попасть под следствие. Тебя могут арестовать.

;) )

Трафик летел с бешеной скоростью. Сетевые кабели, соединенные с System X, были настоящим хайвеем. Народ со свистом проносился в загадочный сайт и вылетал из него, словно пчелиный рой. За какие-нибудь двенадцать часов сниффер создал файл емкостью больше 100 килобайт.

Многие соединения вели от System X к главной телекоммуникационной компании. Anthrax направился к ней.

Он обдумывал, как лучше провести атаку. Ему нужно было пройти через несколько дивертеров и других подобных им устройств, чтобы запутать свои следы и напасть на компанию из абсолютно ничем не связанного с ним места. Преимущество этого маршрута заключалось в анонимности. Если админу удастся обнаружить его проникновение, Anthrax просто потеряет доступ в систему телефонной компании, но не в System X. Если же он войдет в компанию через шлюз и System X, он рискует потерять доступ во все три сайта. Хотя его сниффер показал такой интенсивный трафик, что он мог просто затеряться в общем потоке. Этот хайвей был, очевидно, проложен здесь не без причины. Еще один пользователь, прошедший через шлюз из System X в машину компании, вряд ли вызовет подозрения. Anthrax решил пройти через System X.

Anthrax зарегистрировался в компании при помощи украденного сниффером логина и пароля. Снова используя ошибку загрузочного модуля, он получил доступ в систему и установил свой собственный патч на файл логина. Система компании выглядела гораздо привычнее System X. Несколько сотен пользователей. Полно электронных сообщений, слишком много, чтобы пытаться их прочитать. Он запустил поиск нескольких ключевых слов в электронной почте, пытаясь собрать воедино общую картину проекта, который разрабатывали в System X.

Компания осуществляла множество оборонных разработок, по большей части в области телекоммуникаций. Различные подразделения компании трудились над разными частями проекта.

---

(Rutgers University Press, 1988).

Anthrax искал в домашних директориях пользователей, но не нашел ничего интересного, потому что не знал названия самого проекта. Каждый разрабатывал свой участок, не имея возможности взглянуть на всю картину, а эти фрагменты мало о чем могли сказать.

Anthrax нашел группу бинарных файлов – видимо, программ, – но у него не было ни малейшего представления о том, зачем они здесь. Единственным способом понять их предназначение было провести с ними тест-драйв. Он запустил несколько файлов. Они не производили впечатления какой-то деятельности. Он попробовал еще несколько. Снова ничего. Он продолжал запускать их один за другим. Никаких результатов. Все, что он видел, – послания об ошибках.

Казалось, что бинарным файлам нужен монитор, способный отобразить графику. Они использовали ХП, графический дисплей, обычный для Unix. В дешевом персональном компьютере Anthrax'a не было такой программы графического дисплея.

Он, конечно, мог запустить бинарные файлы, приказав System X вывести их на один из ее собственных терминалов, но он не сможет увидеть результат. Кроме того, это было рискованное предприятие. Вдруг кто-то окажется за этим терминалом? Игра будет закончена в ту же минуту.

Он оторвался от клавиатуры и потянулся. Он почувствовал усталость. Он не спал почти 48 часов. Время от времени он отходил от компьютера, чтобы перекусить, но всегда возвращался с тарелкой к компьютеру. Мать несколько раз открывала дверь в его чулан и безмолвно качала головой. Если он замечал ее, он пытался рассеять ее беспокойство. Он говорил, что узнает много нового. Но она не была в этом уверена.

Он также прерывал свои хакерские сессии, чтобы помолиться. Правовой мусульманин непременно должен совершать намаз – молиться, по меньшей мере, пять раз в день в зависимости от того, какое течение ислама он исповедует. Ислам позволяет своим последователям объединять некоторые из молитв, поэтому Anthrax возносил две молитвы вечером, совершал одну в полдень, как положено, и еще две вечером. Рациональный способ отпраздновать религиозные обряды.

Порой за всемогущими хакерскими бдениями время проносилось незаметно. Когда его касался первый лучик рассвета, он неизменно находился в разгаре какого-нибудь увлекательного путешествия. Но долг есть долг, и его нужно было исполнить. Поэтому он нажимал Ctrl Q, чтобы заморозить экран, разворачивал молитвенный коврик с встроенным в него компасом, указывающим в сторону Мекки, преклонял колени и возносил две молитвы перед восходом солнца. Десять минут спустя он сворачивал коврик, возвращался на свой стул, нажимал Ctrl Q, чтобы прекратить паузу, и продолжал с того места, где остановился.

Компьютерная система этой компании явно подтверждала его подозрения. System X была первой стадией проекта, остальная часть которого только разрабатывалась. Он нашел большое количество таблиц и отчетов в файлах System X. Отчеты находились под заголовками типа «Анализ трафика», «входящие звонки», «исходящие звонки», «рейтинг ошибок». Все это начало приобретать определенный смысл.

System X звонила на каждый военный телефонный коммутатор из списка. Она регистрировалась в нем, используя генерированные компьютером имя и пароль. Оказавшись внутри, программа System X запрашивала у коммутатора необходимые статистические данные, такие как количество входящих и исходящих звонков базы. Эта информация хранилась в System X. Когда кому-то требовалась информация о чем-либо, например о военных сайтах с самым большим количеством входящих звонков за последние 24 часа, он мог спокойно запросить System X собрать такую информацию. Все это делалось автоматически.

Anthrax прочитал e-mail, в котором шла речь о том, что изменения в коммутаторе базы, такие как добавление новых телефонных линий, совершались вручную, но эта работа вскоре должна была перейти в ведение System X. В этом был смысл. Время на обслуживание системы могло разительно сократиться.

Машина, которая собирает статистику и на расстоянии обслуживает телефонные коммутаторы, вблизи выглядит не слишком привлекательно. До тех пор пока не начнешь представлять, как ею можно воспользоваться. Можно продать ее иностранному государству, которое интересуется уровнем активности той или иной базы в определенное время. И это только начало.

Можно прослушать любую незакодированную телефонную линию любого из ста коммутаторов и услышать важные военные разговоры. Всего несколько команд, и ты, словно муха на стене, присутствуешь при разговоре генерала с начальством базы на Филиппинах. Антиправительственные повстанцы этой страны могут заплатить неплохие деньги за разведывательную информацию об армии США.

Но все эти возможности бледнеют перед невероятной властью хакера, который имеет доступ к

System X и ее сотне телефонных коммутаторов. Он может уничтожить все голосовые коммуникации армии США за одну ночь, сделав это автоматически. От потенциальных разрушений захватывает дух. Умелому программисту не составит труда внести изменения в автоматическую программу, используемую System X. Вместо того, чтобы пройти через десяток или больше модемов, чтобы дозвониться до всех коммутаторов и запросить у них сведения, System X может получить инструкции обзвонить их и перепрограммировать за одну ночь.

Что произойдет, если всякий раз, когда генерал Колин Пауэлл снимет трубку, он будет автоматически соединяться с кабинетом какого-нибудь русского генерала? Он не сможет набрать никакой другой номер со своего офисного телефона. Он снимет трубку, чтобы позвонить, а на другом конце будет русский. Что, если всякий раз, как кто-то будет звонить в офис генерала, он будет попадать в Государственный департамент? Что, если ни один номер не будет соответствовать своему телефону? Никто не сможет никому позвонить. Важнейшая часть американской военной машины будет полностью уничтожена. А если это произойдет в первые несколько дней войны? Люди будут пытаться дозвониться друг другу, чтобы передать жизненно важную информацию, и не смогут использовать коммутаторы, перепрограммированные System X.

Это была ВЛАСТЬ.

Это было совсем не то, что кричать на отца, пока голос не сорвется на хрип, но все впустую. С такой властью он мог заставить людей сидеть и слушать.

Взлом системы давал ему чувство контроля. Получение доступа в систему всегда вызывало у него всплеск адреналина по той же причине. Это означало, что система *его*, что он может сделать с ней все, что захочет, сможет запустить те процессы и программы, которые пожелает, сможет удалить любых пользователей, если ему будет угодно, чтобы они не пользовались его системой. Он *владел* системой. Слово «владеть» было ключевым во фразе, которая снова и снова появлялась в его мыслях, когда он успешно взламывал систему.

Чувство собственности было почти страстью, переплетенной с одержимостью и ревностью. В любой момент у Anthrax'а был список систем, которыми он владел и которые привлекали его интерес в эту минуту. Anthrax ненавидел, когда системный администратор входил в одну из этих систем. Это было вторжение. Это выглядело так, словно Anthrax только что вошел к женщине, с трудом достучавшись до нее. Едва они познакомились, как в комнату вваливается какой-то парень, садится на кушетку и начинает разговаривать с ней.

Ему никогда не достаточно было смотреть на систему со стороны и знать, что он может ее взломать, если захочет. Anthrax'у нужно было немедленно взломать систему. Он *должен* был обладать ей. Он должен был увидеть, что находится внутри системы, чем он владеет.

Худшее, что могли сделать админы – напридумывать чего-нибудь в системах безопасности. Когда это происходило, Anthrax сгорал от гнева. Если он был онлайн, потихоньку наблюдая за деятельностью админов, он ощущал неотложную потребность отключить их от системы. Он хотел наказать их. Хотел, чтобы они знали, что он находится в их системе. Но в то же время он не хотел, чтобы они знали о нем. Если их отключить, это привлечет к нему внимание, но эти взаимоисключающие желания постоянно раздирали его. Больше всего Anthrax хотел, чтобы админы знали, что он контролирует их систему, но не могли ничего с этим поделать. Он хотел, чтобы они были беспомощны.

Anthrax решил не высовываться. Но он поразмыслил над тем, какая власть крылась в обладании списком модемных доступов к телефонным коммутаторам и комбинаций из имени пользователя и пароля System X. Обычно хакер-одиночка со своим единственным модемом может потратить несколько дней, чтобы добиться подобного влияния на военную коммуникационную сеть США. Он, конечно, мог уничтожить несколько коммутаторов, прежде чем военные опомнятся и начнут что-нибудь предпринимать. Это было похоже на взлом военного компьютера. Ты мог поиметь машину тут, систему там. Но смысл власти над System X заключался в том, что ты мог использовать ее собственные ресурсы, чтобы дирижировать огромным сборищем демонов быстро и совершенно спокойно.

Anthrax определял власть как возможность реального влияния на события в мире. В этот момент открытия и его перспективы проникновения в System X выглядели неплохо. Компьютер телекоммуникационной компании, похоже, годился для того, чтобы запустить в него сниффер. Он так и сделал, решив вернуться позже. Затем он отключился и отправился в постель.

Когда Anthrax пришел проводить сниффер через день или около того, он испытал жесточайший шок. Он обнаружил, что кто-то входил в систему компании, используя его специальный пароль из патча.

Он постарался успокоиться и подумать. Когда в последний раз *он* входил в систему, используя

этот пароль? Мог ли его сниффер оказаться здесь самостоятельно во время одной из предыдущих хакерских сессий? Это произошло случайно. Хакеры иногда пугают до полусмерти сами себя. В чередующихся друг на друга днях и ночей, проведенных за взломом десятков систем, легко забыть, когда ты в последний раз входил в ту или иную систему, используя специальный пароль. Но чем больше он думал, тем больше он был уверен, что не входил повторно в эту систему. Вставал очевидный вопрос: «Кто же входил?»

:)

Чаще Anthrax разыгрывал, но порой и наказывал. Наказание могло быть суровым или мягким. Чаще суровым. И в отличие от розыгрышей, оно не было случайным.

Его многие выводили из себя. Например, библиотекарь. В начале 1993 года Anthrax записался на курсы по Азии и Тихому океану и по бизнесу в университете соседнего города. Как только он появлялся в университетском городке, у него всякий раз возникали проблемы со студентом, который работал на полставки в студенческой библиотеке. Не раз бывало, что охранник проверял сумку Anthrax'a, когда тот сидел в читальном зале. И когда Anthrax оглядывался на стойку выдачи книг, этот библиотекарь всегда был там со своим неизменно злобным выражением лица.

Его придирки стали настолько заметны, что друзья Anthrax'a даже заволновались. Его сумку периодически обыскивали, когда он выходил из библиотеки, в то время как другие студенты спокойно выходили через ворота, снабженные электронной системой защиты от краж. Если он возвращал книгу на день позже срока, библиотекарь – этот библиотекарь – настаивал, чтобы Anthrax заплатил все мыслимые штрафы. Напрасно Anthrax пытался сослаться на то, что он бедный студент, – библиотекарь оставался глух к его просьбам. И вот когда экзаменационная сессия подходила к концу, Anthrax решил наказать библиотекаря и вывести из строя всю библиотечную компьютерную систему.

Он подключился к компьютеру библиотеки через модем прямо из дома и легко получил корневые привилегии. В системе безопасности были дыры в милю шириной. Затем одной простейшей командой он стер все файлы в компьютере. Он знал, что систему можно будет восстановить, но потребуются день, а то и два, чтобы настроить ее и запустить снова. Тем временем выдачу и поиск книг придется осуществлять вручную.

Когда Anthrax учился на первом курсе университета, даже мелкие инциденты провоцировали наказание. Достаточно было подрезать его машину или обругать его на дороге, и он неизменно платил по счетам. Anthrax запомнил номер машины обидчика, затем, используя приемы «социального программирования», добывал сведения о его личной жизни. Обычно он звонил в полицию и сообщал о краже машины, а затем давал им номер машины грубияна. Сразу после этого Anthrax настраивался на полицейскую волну, откуда узнавал имя и адрес водителя. Anthrax записывал эти данные.

Затем следовала кара. От лица водителя Anthrax звонил в его электрическую компанию, чтобы договориться об отключении электроэнергии. Утром водитель обнаруживал, что остался без света. На следующий день у него могли отключить газ. Потом воду. Потом телефон.

Некоторые люди заслуживали особого наказания – такие как Билл. Anthrax пересекся с Биллом на Swedish Party Line, англоязычной телефонной конференции. На какое-то время Anthrax стал завсегдатаем конференции, за несколько месяцев он умудрился позвонить туда по фрикерским каналам около двух тысяч раз. Конечно, не все его попытки были успешны, но ему удавалось прорваться, по крайней мере, в половине случаев. Постоянное присутствие на телефонной линии требовало определенных усилий, потому что она автоматически отключала абонентов каждые десять минут. Anthrax подружился с операторами, которые иногда позволяли ему оставаться онлайн подольше.

Билл, фанат Swedish Party Line, недавно вышел из тюрьмы, где отсидел срок за то, что избил вьетнамца на железнодорожной станции. Он вел себя отвратительно и обычно присоединялся к конференции со словами: «Надеюсь, сегодня на линии нет негритосов?» Его отношение к женщинам было ненамного лучше. Он безжалостно нападал на женщин, посещавших конференцию. Но однажды он допустил ошибку. Он дал свой номер телефона девушке, с которой пытался познакомиться. Женщина-оператор скопировала его, и когда чуть позже в этот же день появился Anthrax, она передала ему номер.

Anthrax провел несколько недель, общаясь со многими людьми, включая разные службы и знакомых, чьи номера телефонов фигурировали на телефонном счете Билла, собирая воедино детали его личной жизни. Он выяснил, что Билл – бывший уголовник, что у него есть волнистый попугайчик и что он умирает от рака. Anthrax позвонил Биллу в больницу и стал рассказывать ему массу всевозможных подробностей о нем самом, таких подробностей, которые вряд ли кому-то понравятся.

Вскоре после этого Anthrax узнал, что Билл умер. Хакер подумал, что он, возможно, немного перегнул палку.

;) )

Обстановка в доме немного разрядилась, когда Anthrax уехал на учебу. Но бывая дома по праздникам, он видел, что отец становится все менее переносимым. Снова и снова Anthrax восставал против издевательских комментариев и жестокости своего отца. В конце концов он поклялся, что в следующий раз, когда отец попытается сломать ему руку, он не будет терпеть и ответит ударом на удар. И он сдержал слово.

Однажды отец принялся злобно насмехаться над заиканием младшего сына. Он так и сочился ядовитым сарказмом, передразнивая его.

– Зачем ты это делаешь? – крикнул Anthrax. Он снова попался на отцовскую наживку.

Но на этот раз все было иначе, словно в него вселился какой-то бес. Он заорал на отца и ударил кулаком в стену. Отец схватил стул и толкнул его в сторону Anthrax'а, чтобы задержать его, а сам бросился к телефону. Сказал, что звонит в полицию. Anthrax вырвал телефонный провод. Он преследовал отца по всему дому, круша мебель. В жестокой ярости драки Anthrax вдруг испугался за часы своей матери – это была семейная реликвия, которую она очень любила. Он осторожно отодвинул их с дороги. Затем он поднял в воздух стереосистему и швырнул ее в отца. За ней последовали колонки. Платяные шкафы с грохотом валились на пол.

Когда отец вылетел из дома, Anthrax попытался взять себя в руки и посмотрел вокруг. Это был полный разгром. Все вещи, которые его мать так тщательно собирала и за которыми так бережно ухаживала, вещи, которые помогали ей наладить жизнь в чужой стране белых людей, говорящих на чужом языке, теперь обломками в беспорядке валялись на полу.

Anthrax'а охватило отчаяние. Его мать страшно огорчилась увидев эти разрушения. Он был просто потрясен тем, как это ее расстроило. Anthrax пообещал матери, что впредь постарается сдерживать свой нор. Это был постоянный бой. В большинстве случаев Anthrax одерживал победу, но не всегда. Внутренняя борьба никогда не утихала.

Иногда она прорывалась наружу.

;) )

Anthrax пытался представить, кто еще мог использовать его патч. Конечно, это мог быть другой хакер, возможно, запустивший свой sniffер, который записал предыдущий логин Anthrax'а. Но скорее всего это был системный администратор. Значит, его обнаружили. Значит, за ним могли проследить еще с того момента как он перепрыгнул из System X в компьютер телекоммуникационной компании.

Anthrax решил прогуляться к почтовым ящикам системного администратора. Если игра проиграна, есть шанс, что в почтовом ящике можно будет найти информацию на этот счет.

И она там была. Доказательство. Они действительно проследили за ним и не тратили времени понапрасну. Админы направили отчет о прорехе в системе безопасности в Команду быстрого компьютерного реагирования [[p168](#)] при университете Карнеги-Меллон. В CERT – карающем мече, грозящем каждому хакеру, – были склонны вечно все усложнять. Они, конечно, уже вызвали соответствующие органы.

Нужно было срочно убираться из этой системы, но сначала – знак триумфатора. Небольшой розыгрыш в качестве прощального презента.

Из CERT администраторам пришел ответ с подтверждением получения информации об инциденте и указанием номера заведенного по нему дела. Выдав себя за одного из админов, Anthrax набросал письмо в CERT. Чтобы придать ему официальный вид он добавил номер дела для достоверности. Содержание было примерно следующим:

«В отношении инцидента № XXXXX от такого-то числа мы провели дополнительное расследование. В ходе расследования выяснилось, что инцидент в системе безопас-

ности был спровоцирован недовольным служащим, который был уволен за алкоголизм и решил отомстить компании таким образом. Мы уже давно сталкиваемся с проблемами алкоголизма и наркомании, связанными со стрессовым характером работы в компании. В дальнейшем расследовании нет необходимости».

Anthrax улыбнулся своему монитору. Интересно, к каким последствиям *это* приведет? Попробуйте-ка отмыться от *такой* грязи. Он был очень доволен собой.

Он хорошенько убрал за собой в компьютере компании, стер свой сниффер и вышел вон.

После этого события начали разворачиваться стремительно. Немного времени спустя Anthrax вошел в System X, чтобы проверить записи сниффера, но нашел там только то, что кто-то использовал пароль из его патча, чтобы пробраться и в эту систему. Он сильно встревожился. Одно дело – попасться в коммерческом сайте, и совершенно другое, если тебя выследили в военном компьютере.

В System X была запущена новая программа, и Anthrax узнал ее. Она называлась – и. Он не знал, какова была ее функция, но ему приходилось раньше видеть такие программы в военных системах. Примерно через сутки после того, как она появилась, он обнаружил, что его лишили доступа в систему. Еще до того Anthrax попытался уничтожить программу – и. Она исчезала на долю секунды и появлялась вновь. Когда она была установлена, не было никакой возможности разрушить ее.

Кроме того, Anthrax обнаружил довольно тревожное электронное письмо. Администратор сайта, расположенного выше по течению относительно System X и системы компании, получил письмо с предупреждением: «Мы думаем, что в вашем сайте есть проблемы с безопасностью». Круг вот-вот должен был замкнуться на нем. Теперь точно пора убираться отсюда ко всем чертям. Он в спешке принялся собирать чемоданы. Уничтожить оставшийся сниффер. Забрать свои файлы. Убрать патч. И прочь как можно скорее.

Окончательно отрезав соединение, Anthrax сидел и удивлялся поведению админов. Если они знали, что он ползал по их системам, почему они не тронули его снифферы и позволили им работать? Он мог понять, зачем они оставили патч. Наверное, они хотели понаблюдать за его движениями, понять его мотивы или выйти на след его соединения. Если бы они уничтожили патч, они просто лишили бы его доступа к единственной известной им лазейке. Они не знали, есть ли у него еще какие-нибудь черные ходы. Но сниффер? Это было лишено всякого смысла.

Возможно, они попросту не заметили сниффер. Пропустили его по недосмотру. Но это слишком грубая ошибка, чтобы на нее действительно рассчитывать. Если это была ошибка, это означает, что администраторы на самом деле не проводят мониторинг входящих и исходящих соединений своих систем. Если бы они следили за соединениями, то, скорее всего, обнаружили бы сниффер. Но если они не обследовали соединения, как, черт возьми, они обнаружили патч логина? Как и все пароли в системе, он был зашифрован. Этот пароль можно было получить только двумя способами. Тщательно проверить соединение и унюхать его или взломать шифр с помощью грубой силовой атаки.

Взлом шифра, скорее всего, потребовал бы компьютерного времени на миллионы долларов. Он мог совершенно спокойно исключить эту возможность. Они разнюхали пароль и узнали о его сниффере. И уж, конечно, они не могли оставить его нарочно. Они-то должны знать, что с помощью своего сниффера он узнает о том, что они следят за ним. Все это было очень странно.

Anthrax размышлял об администраторах, которые охотились за ним. Думал об их мыслях, об их стратегии. Удивлялся. Это была одна из неразрешимых загадок, с которыми часто сталкивается хакер – одна из неприятных сторон хакинга. Невозможность получить ответ на некоторые вопросы, удовлетворить свое любопытство. Так никогда и не увидать, что происходит по ту сторону стены.

## 11

### Дилемма узника

Гаррисберг. О, Гаррисберг.  
Расплавилась трава,  
Бросают люди Гаррисберг,  
Уходит прочь толпа.  
Пролезет внутрь такая дрянь –  
Не выйдет никогда.

Песня «Harrisburg», альбом «Red Sails in the Sunset» группы Midnight Oil<sup>49</sup>

Anthrax думал, что его никогда не поймают. Но, странное дело, он хотел, чтобы его поймали. Когда он думал об аресте, он чувствовал, что его переполняет нетерпение. Вызвать неминуемую гибель и покончить с этим. Иногда он был разочарован слабостью своих противников. Они неизменно теряли его след, и его раздражала их некомпетентность. Гораздо интереснее побороться с достойным соперником.

Возможно, он не так хотел, чтобы его поймали, как чтобы его выследили. Anthrax'у нравилась мысль о том, что полиция и администраторы отслеживают его и охотятся за ним. Ему нравилось следить за продвижением их расследования по чужим почтовым сообщениям. Особенно ему нравилось находиться онлайн и наблюдать за тем, как они пытаются понять, откуда он взялся. Он мог так ловко получить контроль над их компьютерами, что они даже не подозревали об этом. Он видел каждый напечатанный ими символ, каждую ошибку в правописании, каждую неправильно заданную команду, каждый маневр и уловку в тщетной попытке поймать его.

Он ускользнул в начале 1991 года, когда, казалось, все ополчились против него. На самом деле в тот год Anthrax почти завязал с хакингом и фрикингом после того, что он позже назвал «страхом Господним».

Однажды поздно ночью в университетском компьютере он столкнулся с другим хакером. Это было вполне обычное дело. Хакеры мгновенно распознавали себе подобных. Странные соединения со странными местами посреди ночи. Несообразности в названиях операций и размерах. Ответы были очевидны для того, кто знал, как их найти.

Двое хакеров кружили вокруг да около, пытаясь понять, что представляет собой каждый из них, но при этом стараясь выдать как можно меньше информации. Наконец, таинственный хакер спросил у Anthrax'a: «Ты та болезнь, которая косит овец?»

Anthrax просто напечатал в ответ: «Да».

Другой хакер объявил, что он Prime Suspect, один из International Subversive. Anthrax узнал его имя. Он встречал его на BBS, видел его объявления. Но не успел Anthrax завязать дружескую беседу, как хакер из IS перебил его срочным предупреждением.

Он обнаружил электронные письма, в которых шла речь о том, что федералы подбираются к Anthrax'у. Почта, полученная от системных администраторов из Miden Pacific, описывала системы, в которых побывал Anthrax. Там были описаны телефонные соединения, которые он использовал, чтобы добраться до них. Некоторые из этих систем Telecom проследил до его собственного телефона. Один из администраторов написал: «Он почти у нас в руках. У меня погано на душе. Ему всего семнадцать, и они вот-вот возьмут его и сломают ему жизнь». Anthrax почувствовал, как холодок пробежал по его спине.

А Prime Suspect продолжал свою историю. Когда ему впервые попало это письмо, он подумал, что речь идет о нем. Оба хакера были одного возраста и, очевидно, взламывали одни и те же системы. Prime Suspect чуть с ума не сошел от этого письма. Он показал его двум другим хакерам IS, и они вместе обсудили его. Большинство из описаний совпадало, но несколько деталей, казалось, совершенно выпадали из контекста. Prime Suspect не звонил с коммутатора из глубинки. Чем больше они о нем думали, тем яснее становилось, что письмо, видимо, относилось к кому-то другому. Они обсудили список других кандидатов, и имя Anthrax'a появилось в качестве одного из возможных. Хакеры IS видели его в разных системах и BBS. Трах даже однажды разговаривал с ним и с еще одним фрикером во время телефонной конференции. Они собрали все, что им было о нем известно, и картинка совпала. АФП шла за Anthrax'ом, и они знали о нем очень много. Они проследили его телефонные соединения до самого дома. Они знали его возраст, а значит, и его настоящее имя. Федералы подобралась к нему так близко, что буквально дышали ему в затылок. Хакеры IS всюду пытались его найти, но встретили его только сейчас.

Anthrax поблагодарил Prime Suspect'a и вышел из системы. Он сидел, окаменев, в ночной тишине. Одно дело рассматривать возможность ареста, лелеять смешанные чувства по поводу гипотетической ситуации. Другое дело, когда реальность пялится тебе в лицо. На следующее утро он собрал все свои хакерские бумаги, заметки, учебники – все. Больше трех мешков материалов. Он отнес все это на задний двор, развел костер и посмотрел, как оно горит. Он поклялся навсегда завязать с

<sup>49</sup> Слова и музыка: James Moginie (стихи из книги «*The Cat Prawn War And Other Stories*» by Dennis Kevans). © Copyright 1984 Sprint Music. administered for the World – Warner / Chappell Music Australia Pty Ltd. Used by Permission.



хакингом.

И он завязал, на время. Но несколько месяцев спустя он каким-то образом обнаружил, что сидит перед компьютером, а его модем заливается соловьем. Это было такое искушение, так трудно было устоять. Тем более что полиция так и не показалась. Прошли месяцы – и ничего. Должно быть, Prime Suspect ошибся. Видимо, АФП преследовала совершенно другого хакера.

Затем в октябре 1991 года федералы задержали Prime Suspect'a, Mendax'a и Trax'a. Но Anthrax продолжал заниматься хакингом, практически по-старому, еще два следующих года. Он говорил себе, что хакеры IS работали в команде. Если полиция не сцапала его вместе с остальными, теперь-то они никогда не найдут его. Кроме того, он стал гораздо более искусным, лучше заметал следы, намного меньше привлекал к себе внимание. Он нашел и другие причины. Город, где он жил, находился так далеко, что полиция никогда не стала бы утруждать себя такой поездкой в буш. Неуловимый Anthrax, непобедимый Нед Келли компьютерного подполья, всегда будет свободен.

:)

Утром 14 июля 1994 года Anthrax'a занимали житейские проблемы. Он ждал грузчиков, которые должны были приехать и забрать вещи из полупустой квартиры – он снимал ее на пару с другим студентом. Его сосед уже уехал, и квартира была беспорядочно загромождена коробками, набитыми одеждой, кассетами и книгами. Anthrax сидел на кровати в полудреме и вполглаза смотрел программе новостей по телевизору, когда услышал шум двигателя большого автомобиля, остановившегося перед домом. Он посмотрел в окно, ожидая увидеть грузчиков. Но вместо них он увидел четверых мужчин в обычной одежде, которые бежали к дому.

Они проявляли слишком большой энтузиазм для грузчиков. Они разделились перед тем, как войти, – двое из них направились к противоположным сторонам здания. Один из них двинулся к гаражу. Второй вынырнул с другой стороны здания. Третий постучал в дверь. Anthrax стряхнул с себя сон.

Приземистый, коренастый парень у входной двери не нравился ему. У него были длинноватые пышные волосы. Он был одет в футболку с длинными рукавами и вываренные джинсы, настолько узкие, что можно было посчитать мелочь в его заднем кармане. Нехорошие мысли забежали в голове Anthrax'a. Это выглядело как налет на квартиру. Головорезы собирались вломиться в его дом, связать его и избить, а потом забрать его вещи.

– Открывайте. Открывайте, – крикнул коренастый, сверкнув полицейским значком.

Ошеломленный и все еще недоумевающий Anthrax открыл дверь.

– Вы знаете, кто мы? – спросил коренастый.

Anthrax выглядел растерянным. Нет. Неуверен.

– Австралийская федеральная полиция, – и коп начал читать постановление об обыске.

Все, что за этим последовало, излагается по-разному. Но совершенно точно, что это события налета полиции и что нижеследующее легло в основу жалобы Anthrax'a в офис омбудсмана и внутреннего расследования АФП. Это точка зрения Anthrax'a на то, как это было.

– Где твой компьютер? – гавкнул коренастый на Anthrax'a.

– Какой компьютер? – Anthrax непонимающе смотрел на офицера. У него не было компьютера в этой квартире. Он пользовался университетскими машинами или компьютерами друзей.

– Твой компьютер. Где он? Кто из твоих друзей спрятал его?

– Никто. У меня нет компьютера.

– Ладно. Когда ты решишь сказать, где он, дай нам знать.

Ага. Конечно. Если бы Anthrax и спрятал где-нибудь компьютер, он сообщил бы о его местонахождении наверняка не в первую очередь.

Полицейские запустили лапы в его личные письма, беспрестанно расспрашивая Anthrax'a. Кто написал это письмо? Он тоже из компьютерного подполья? Где он живет?

Фраза «без комментариев» прозвучала немыслимое количество раз. Полицейские перешли в его спальню, и он решил, что стоит присмотреть, как бы они чего не подкинули. Он шел за ними в надежде проследить за обыском, как вдруг один из полицейских остановил его. Anthrax сказал ему, что он требует адвоката. Коп посмотрел на него с явным неодобрением.

– Должно быть, ты виноват, – сказал он Anthrax'у – Только преступники просят адвоката. Мне жаль тебя.

Затем один из полицейских выпустил главный козырь.

– Знаешь, – начал он небрежно, – мы обыскали дом твоих родителей...

Anthrax был вне себя. Мама, наверное, была потрясена. Он попросил разрешения позвонить матери со своего мобильного телефона, единственного, который работал в доме в тот момент. Полиция запретила ему прикасаться к мобильному. Затем он попросил разрешить позвонить ей из телефона-автомата на другой стороне улицы. Полицейские снова отказали ему. Один из них, высокий тощий коп, воспользовался ситуацией в своих полицейских целях. Он решил надавить на чувство вины.

– Твоя бедная больная мама. Как ты мог сделать такое со своей бедной больной мамой? Мы собираемся отвезти ее в Мельбурн на допрос, может быть, даже предъявим ей обвинение, арестуем, отправим в тюрьму. Меня тошнит от таких, как ты. Мне жаль мать такого сына, который навлекает на нее такие неприятности.

С этой минуты высокий коп использовал любую возможность, чтобы напомнить Anthrax'у о его «бедной больной маме». Он вцепился в него мертвой хваткой. Хотя он, возможно, знал что-то о склеродермии, поразившей ее жуткой болезнью. Anthrax часто думал о боли, которую испытывала его мать, по мере того как болезнь прокладывала свой путь с внешней оболочки к внутренним органам. Склеродермия огрубляет кожу пальцев и ног, но делает их чрезвычайно чувствительными, особенно к перемене погоды. Обычно она поражает женщин, родившихся в теплом климате и переехавших в более холодные края.

Мобильный Anthrax'а вдруг зазвонил. Его мать. Это должна быть она. Полиция не позволит ему ответить ей.

Высокий полицейский взял трубку, а затем повернулся к коренастому и сказал с издевательским индийским акцентом: «Какая-то женщина с индийским акцентом». Anthrax почувствовал, что сейчас прыгнет со стула и вырвет у него телефон. Он почувствовал, что способен совершить и другие поступки, которые, несомненно, приведут его в тюрьму прямо сейчас.

Коренастый кивнул высокому и тот протянул мобильный Anthrax'у.

Сначала он не мог понять, что говорит его мать. Она говорила ужасно сбивчиво. Anthrax постарался успокоить ее. Потом она стала утешать *его*.

– Не волнуйся. Все будет хорошо, – повторяла она снова и снова. Неважно, что говорил Anthrax, она повторяла эти фразы, как заклинание. Пытаясь утешить его, она, на самом деле, успокаивала себя. Anthrax слушал, как она пытается привести в порядок окружающий ее хаос. Сквозь голос матери до него доносился какой-то шум, и он догадался, что это полиция обшаривает ее дом. Неожиданно она сказала, что ей нужно идти, и повесила трубку.

Anthrax вернул телефон полицейским и сел, сжимая руками голову. Что за паршивая ситуация. Он не мог поверить, что это происходит с ним. Как может полиция серьезно говорить о том, чтобы отвезти его мать на допрос в Мельбурн? Правда, он делал свои фрикерские дела с ее домашнего телефона, но у нее не было ни малейшего представления о том, что такое хакинг или фрикинг. Обвинить его мать было все равно, что убить ее. При ее душевном и физическом состоянии это будет просто катастрофа, после которой она может никогда не оправиться.

У него не было особого выбора. Один из копов запечатал его мобильный телефон в пластиковый пакет и наклеил на него этикетку. Он физически не имел возможности вызвать адвоката, поскольку полиция не разрешила ему пользоваться мобильным или позвонить из телефона-автомата. Они принялись доставать его насчет того, чтобы он поехал в Мельбурн для допроса.

– В твоих интересах помочь нам, – сказал ему один из полицейских. – В твоих интересах поехать с нами сейчас.

Anthrax на минуту задумался об этом предложении, о том, как нелепо это звучит из уст копа. Такая откровенная ложь говорила так безапелляционно. Это было бы смешно, если бы ситуация с матерью не была так ужасна. Он согласился на допрос, но настоял, чтобы его назначили на другой день.

Копы захотели обыскать его машину. Anthrax'у это не понравилось, но в машине все равно не было ничего криминального. Когда он вышел на улицу в зимнее утро, один из полицейских посмотрел на его ноги. Anthrax был босиком – он снимал обувь в доме по мусульманскому обычаю. Коп спросил, не холодно ли ему.

Другой коп ответил за Anthrax'а:

– Нет. Их греет грибок.

Anthrax сдержал гнев. Он привык к постоянным проявлениям расизма, особенно от копов. Но это был перебор.

В городе, где находился университет, все думали, что он абориген. В этом провинциальном городке было две национальности – белые и аборигены. Индусы, пакистанцы, малайцы, бирманцы –

неважно. Они все были аборигенами, и обходились с ними соответственно.

Однажды он стоял напротив дома и разговаривал из кабины телефона-автомата. Рядом остановились полицейские и спросили, что он здесь делает. Он ответил, что звонит по телефону. Это было совершенно очевидно. Они попросили его предъявить документы, заставили его вывернуть карманы и обнаружили в одном из них мобильный телефон. Они сказали, что телефон, скорее всего, краденый, забрали его и пошли проверять серийный номер. По прошествии пятнадцати минут и множества новых обвинений они отпустили его с весьма сомнительным извинением: «Понимаешь, – сказал ему один из полицейских, – мы тут нечасто видим таких, как ты».

Да, Anthrax понимал. Темнокожий парень, который говорит по телефону-автомату, выглядит крайне подозрительно. Ясное дело.

На самом деле, в тот раз Anthrax смеялся последним. Когда подошли копы, он говорил с Канадой посредством фрикерского звонка и не дал себе труда повесить трубку. Он просто велел канадцам не давать отбой. После того, как копы ушли, он продолжил разговор ровно с того места, где остановился.

Такие происшествия научили его, что иногда лучше подыграть копам. Позволить им забавляться собственными играми. Сделать вид, что ты в их власти. Посмеяться над ними про себя и не дать им ничего. Поэтому он пропустил мимо ушей комментарий насчет грибка и отвел полицейских к машине. Они ничего не нашли.

Когда, наконец, полиция собралась уходить, один из копов дал Anthrax'у визитку с номером телефона АФП.

– Позвони нам, когда будешь готов к интервью, – сказал он.

– Конечно, – ответил Anthrax, закрывая дверь.

:)

Anthrax продолжал динамить полицию. Всякий раз, как они звонили ему и настаивали на интервью, он говорил, что занят. Но когда они начали звонить его маме, он оказался в затруднении. Они одновременно угрожали ей и успокаивали ее, но разговаривали с ней вежливо, даже виновато.

– Как бы скверно это ни звучало, – сказал один из них, – нам, видимо, придется обвинить вас во всех этих безобразиях Anthrax'а, в хакинге, фрикинге и прочем, если он не согласится сотрудничать с нами. Мы знаем, что это звучит смешно, но у нас есть полномочия так поступить. На самом деле, закон просто велит нам это сделать, потому что телефон зарегистрирован на ваше имя.

За этим следовало избитое «в интересах вашего сына помочь нам», произнесенное вкрадчиво и убедительно.

Anthrax недоумевал, почему никто не упоминает о том, чтобы обвинить его отца. Главный номер домашнего телефона был зарегистрирован на него. С этой линии тоже совершались нелегальные звонки.

Мать Anthrax'а беспокоилась. Она попросила сына оказать помощь полиции. Anthrax знал, что он должен защитить свою мать, и согласился на разговор с полицейскими после окончания сессии. Он пошел на это лишь потому, что они угрожали его матери. Он был уверен, что если они потащат его мать в суд, ее здоровье может резко ухудшиться и привести к скорой смерти.

Отец Anthrax'а заехал за ним в университет в прекрасный ноябрьский денек и повез его в Мельбурн. Мать настояла, чтобы он присутствовал на допросе сына, потому что он знал все о законах и полиции. Anthrax не возражал против его присутствия: он полагал, что свидетель сможет оградить его от полицейского произвола.

По дороге в город Anthrax говорил о том, как он намерен вести себя на допросе. В АФП ему сообщили, что они собираются поговорить с ним о его фрикерских подвигах, а не о хакинге. Это была хорошая новость. Он ехал на допрос, понимая, что они будут обсуждать его «свежие дела» – фрикинг.

У него было два варианта поведения на допросе. Он мог отвечать начистоту и признаться во всем, как советовал его адвокат. Либо заявить, что готов сотрудничать, и запудрить федералам мозги, как подсказывали ему инстинкты.

Его отец протестовал против второго варианта:

– Ты должен до конца сотрудничать с ними. Они поймут, если ты солжешь. Их учат распознавать ложь. Скажи им все, и они помогут тебе.

Короче, сплошной закон и порядок.

– Да кто они такие, по-твоему? Козлы, – Anthrax смотрел в сторону. Ему становилось дурно от

мыслей о том, что полиция может так доставать людей, например его мать.

– Не называй их козлами, – рявкнул отец. – Они офицеры полиции. Если ты попадешь в беду, они будут первыми, кого ты позовешь на помощь.

– О, да. Интересно, в какую беду я должен попасть, что только АФП сможет мне помочь? – отозвался Anthrax.

Anthrax препирался с отцом всю дорогу, так что на допросе тот ни разу не раскрыл рта. Он, конечно же, приехал сюда не для того, чтобы лично поддержать сына. Они просто поддерживали отношения, не больше. Когда отец начал работать в том же городе, где Anthrax жил и учился, его мать попыталась помирить их. Она уговорила мужа приглашать Anthrax'а на ужин раз в неделю, чтобы смягчить обстановку. Углубить отношения. Они ужинали вместе несколько раз, и Anthrax выслушивал отцовские нотации. Признай, что ты неправ. Сотрудничай с полицией. Разберись в своей жизни. Наведи в ней порядок. Повзрослей. Будь ответственным. Не будь таким никчемным. Не будь таким глупым.

Все эти речи были слегка лицемерными, думал Anthrax, если учесть ту выгоду, которую получил папаша от хакерских умений сына. Когда он узнавал, что Anthrax входил в большую новостную базу данных, он просил его найти все статьи со словом «тюрьма». Затем следовало слово «наказание». Эти поиски стоили целое состояние, возможно, тысячи долларов. Но отец не заплатил ни цента. И тогда он не утруждал себя нотациями о вреде хакинга.

Когда они приехали в управление АФП, Anthrax демонстративно залез с ногами на кожаный диван в вестибюле и открыл банку колы, которую принес с собой. Отец был недоволен.

– Убери ноги с дивана. Зачем ты принес эту банку? Это непрофессионально.

– Слушай, я пришел сюда не на работу наниматься, – огрызнулся Anthrax.

Рыжеволосый констебль Эндрю Секстон [Andrew Sexton], щеголявший двумя серьгами в ушах, подошел к Anthrax и его отцу и повел их наверх выпить по чашке кофе. Секстон сказал, что детектив сержант Кен Дэй, глава отдела по борьбе с компьютерными преступлениями, задерживается на важной встрече, так что придется немного подождать.

Секстон и отец Anthrax'а обнаружили, что у них во многом общие взгляды на вопросы охраны общественного порядка. Они обсуждали проблемы, связанные с реабилитацией и наказанием заключенных. Смеялись. Говорили о «юном Anthrax'е». Юный Anthrax то. Юный Anthrax се.

Юному Anthrax'у было тошно. Он смотрел, как его отец весело болтает с врагом, как будто его сына здесь нет.

Когда Секстон пошел узнать, не освободился ли Дэй, отец Anthrax'а недовольно заворчал:

– Не смотри так вызывающе, молодой человек. Ты не добьешься ничего в этой жизни с таким отношением, она раздавит тебя, как кирпич комара.

Anthrax не знал, что сказать. Почему он должен с уважением относиться к этим людям после того, как они обошлись с его матерью?

Комната для допросов была маленькой, но битком набитой коробками с подписанными распечатками.

Секстон начал допрос. «Запись допроса, состоявшегося в Управлении Австралийской федеральной полиции по адресу: Латроб-стрит, 383, Мельбурн, 29 ноября 1994 года». Он перечислил имена присутствующих и попросил каждого назвать себя для того, чтобы впоследствии можно было распознать голос говорящего.

– Как я уже сказал, сержант Кен Дэй и я провели расследование на основании заявления о вашем участии в незаконных манипуляциях частными автоматическими распределительными коммутаторами посредством номеров 008 Telecom с целью получения доступа к бесплатным национальным и международным звонкам. Вам ясен смысл заявления?

– Да.

Секстон продолжил эти необходимые и важные формальности. Понимает ли Anthrax, что он не обязан отвечать на каждый вопрос? Что у него есть право на присутствие адвоката? По собственной ли воле он явился на допрос? Знает ли он, что может уйти в любой момент?

Anthrax ответил утвердительно на каждый вопрос.

Затем Секстон приступил еще к нескольким обычным процедурам, прежде чем, наконец, дошел до сути дела – до телефонов. Он порылся в одной из коробок и выудил оттуда мобильный телефон. Anthrax подтвердил, что это его телефон.

– Звонки по номерам 008 и последующие соединения были осуществлены вами с этого телефона? – спросил Секстон.

– Да.

– Содержимое блока памяти этого телефона является набором заранее введенных номеров телефонов. Признаете ли вы этот факт?

– Да.

– Мне пришлось столкнуться с трудностями при их извлечении. – Секстон явно был доволен собой, говоря о взломе мобильного Anthrax'a и его номеров быстрого набора. – Номер 22 заинтересовал меня. Он записан как Аарон. Не является ли этот человек Аароном из Южной Австралии?

– Да, но он постоянно переезжает. За ним нелегко угнаться.

Секстон перечислил еще несколько номеров, по большинству из которых Anthrax ушел от ответа. Он спросил Anthrax'a о его манипуляциях с телефонной системой. В особенности Секстона интересовало, каким образом ему удалось совершать звонки в другие страны при помощи номеров 008 австралийских компаний.

После того, как Anthrax терпеливо объяснил принцип своей работы, Секстон снова вернулся к номерам быстрого набора.

– Номер 43. Вы узнаете его?

– Да, это Swedish Party Line.

– Что вы скажете о других номерах? 78? 30?

– Я не уверен. Я не могу сказать, что это за номера. Это было так давно, – Anthrax на секунду замолчал, чувствуя давление с той стороны стола. – По-моему, эти два номера из моего города. Но я не знаю, чьи они. Когда у меня не было ручки и бумаги, я часто записывал номер в телефон.

Секстон был явно разочарован. Он решил взяться за дело покруче.

– Я буду с вами откровенен. Поскольку вы признали свои действия с номерами 008, я думаю, что вы принижаете свои знания и опыт, когда речь заходит об этих преступлениях, – он поправил сам себя. – Не преступлениях. Но о вашем участии во всем этом... Я не хочу сказать, что вы лжете, поймите меня правильно, но вы стараетесь заставить нас подумать, что вы не так уж глубоко в этом замешаны. Не так, как все об этом думали.

Это был вызов, прямой и явный. Anthrax ответил на него:

– Думали обо мне? Это просто чьи-то представления. Если честно, я не слишком в этом разбираюсь. Я не могу рассказать вам ничего о телефонных коммутаторах или о чем-то подобном. Я полагаю, что раньше меня могли считать лидером, потому что я совершал поступки, о которых вы, возможно, знаете, и это создало мне репутацию. С тех пор я решил, что больше не буду этим заниматься.

– С каких пор? Сегодня? – мгновенно отреагировал Секстон.

– Нет. Раньше. Я просто сказал себе: «Я больше никогда не буду этого делать. Это так глупо». Но когда я расстался со своей девушкой... я снова вернулся к этому. Я не хочу сказать, что я в меньшей степени отвечаю за то, что я сделал. Я просто хочу сказать, что все эти номера 008 – это не моих рук дело. Они были получены другими людьми. Но я звонил по ним и, наверное, наделал много глупостей.

Но Секстон не желал так легко выпускать кость.

– Я чувствую, что вы продолжаете... Не знаю, может быть, это связано с тем, что ваш отец здесь, или... Мне как-то пришлось прочитать такую штуку: «Anthrax был легендой, когда он начал заниматься этим, он был сканером, он был тем, с кем можно поговорить о X.25, о Tymnet, о хакинге, об Unix. Хоть о чем».

Anthrax не клюнул на эту удочку. Копы всегда гнули эту линию. Сыграть на самолюбии хакера, заставить его похвастаться своими подвигами. Это было так явно.

– Это неправда, – ответил он. – Я ничего не знаю о... Я не умею программировать. У меня простая Amiga с одним мегом памяти. У меня нет никакого компьютерного образования.

Эта часть была совершенной правдой. Он посещал один курс по программированию в университете, но безуспешно. Он просиживал в библиотеке в поисках дополнительной информации, когда писал курсовую работу. Большинство из его однокурсников написали простые двухсотстрочные программы с несколькими функциями; его программа состояла из пятисот строк и имела множество специальных функций. Но преподаватель завалила его. Она сказала, что функции в его программе не изучались на ее курсе.

Секстой спросил у Anthrax'a, не занимался ли он кардингом. Anthrax категорически отрицал. Затем Секстон снова вернулся к сканингу. Что еще натворил Anthrax? Передавал ли он отсканированные номера другим хакерам? Anthrax отвечал уклончиво, и оба копа постепенно стали раздражаться.

– Я хочу сказать, что, по моему мнению, вы с вашим сканингом помогали другим нарушать за-

кон, содействуя распространению такого рода занятий, – раскрыл свои карты Секстон.

– Не больше, чем телефонный справочник, это просто список. Я ничего не взламывал. Я просто смотрел.

– Эти голосовые почтовые системы принадлежат другим людям. Что вы сделали, когда обнаружили VMB? [p169]

– Просто поиграл. Отдал ее кому-то и сказал: «Посмотри-ка. Это интересно» – или что-то в этом роде.

– Когда вы говорите «поиграл», это означает, что вы взломали код VMB?

– Нет. Я просто смотрел. Я не очень-то знаю, как взламывать VMB.

Секстон попытался зайти с другого бока.

– А что это за номера 1-900? На обратной стороне этого документа стоит номер 1-900. Для чего они используются?

Простой вопрос.

– В Америке они стоят около десяти долларов минута. Думаю, что вы можете позвонить им и получить самую разную информацию – вечеринки на линиях и все такое.

– Это тип звонка-конференции?

– Да.

– Здесь у меня другой документ, в прозрачном пластиковом пакете с маркировкой AS/AB/S/1. Это скан? Вы узнаете свой почерк?

– Да, это мой почерк. Это опять тот же способ сканирования. Это простой набор некоторых коммерческих номеров и их пометка.

– А когда вы что-то находите, что вы с этим делаете?

У Anthrax'a не было ни малейшего желания, чтобы его выставили главарем банды сканеров. Он был общительным одиночкой, а не частью команды.

– Я просто смотрел на это, как, например, в случае с номером 630. Я пробил несколько номеров и узнал, что 113-й где-то развлекается, а 115-й уезжает и все такое. Я просто глянул разок и вряд ли вернулся бы туда снова.

– И вы считаете, что если я возьму телефонную книгу, я смогу получить всю эту информацию?

– Нет. Это просто список в том же роде, что и телефонная книга.

– Как насчет номера 1-800?

– Это то же самое, что 0014.

– Куда можно попасть, если набрать номер 1-800?

Anthrax не удивился бы, если бы оказалось, что отдел по борьбе с компьютерными преступлениями получил большую часть технических знаний из бесед с хакерами.

– Вы можете набрать 0014 или 1-800, это одно и то же.

– 0014 – это Канада?

– Это везде. – У-упс. Не будь таким нахальным. – Не так ли?

– Ну, я не в курсе.

Как раз об этом и думал Anthrax.

Секстон продолжил:

– На оборотной стороне этого документа есть другие материалы сканирования...

– Это все одно и то же. Просто посмотрите. В этом случае почтовый ящик 544 принадлежит этой женщине...

– Ладно, давайте еще раз. Вы распространяли информацию такого рода на телефонных мостах?

– Практически нет. В основном я сохранял ее для себя и больше никогда к ней не возвращался. Это скучно. А что, сканирование запрещено законом?

– Я не говорил, что это запрещено законом. Я просто пытаюсь показать, что вы на самом деле занимались этим. Я рисую общую картину и постепенно продвигаюсь к своей цели, собираюсь нарисовать картину, чтобы показать, что... – Секстон прервался и взял более определенный курс: – Я не говорю, что вы занимаетесь этим сейчас, но в то время, учитывая все совершенные вами правонарушения, вы действительно сканировали телефонные системы и забирались в голосовые почтовые ящики... Я не утверждаю, что вы нашли номера 008, но вы... поймали Telecom. Да, вы так и сделали и помогли в этом другим.

Anthrax обиделся:

– Я не собирался, как вы говорите, «поиметь» Telecom.

Секстон дал задний ход.

– Возможно... может быть, я не так выразился.

Он начал раскручивать тему хакинга, но полицейские не говорили о том, что этот вопрос вообще будет обсуждаться. Anthrax почувствовал раздражение, даже некоторую тревогу.

Дэй спросил, не хочет ли Anthrax сделать перерыв.

– Нет, – ответил тот. – Я хочу полностью покончить с этим раз и навсегда, если это возможно. Я не собираюсь лгать. Я не собираюсь говорить «без комментариев». Я соглашусь со всем, принимая во внимание то, что, как я уже сказал, в моих интересах так поступить.

Полицейские замолчали. Им явно не понравились последние слова Anthrax'а. Дэй попытался прояснить обстановку.

– Прежде чем мы продолжим... Вы сказали, что в ваших интересах говорить нам правду. Вам сказал об этом кто-то из сотрудников АФП?

– Да.

– Кто? – немедленно спросил Дэй.

Anthrax не помнил их имен.

– Те, которые приходили ко мне домой. По-моему, Эндрю тоже говорил мне об этом, – сказал он, кивнув в сторону рыжего констебля.

Почему вдруг копы так занервничали? Ни для кого не было секретом, что они беспрестанно твердили Anthrax'у и его матери, что в его интересах согласиться на встречу с полицией.

Дэй подался вперед, уставился на Anthrax'а и спросил:

– Как бы вы могли истолковать эти слова?

– Так, что если я не буду говорить правду, если буду говорить «без комментариев» и не буду сотрудничать, это значит... значит, что вы возьметесь за меня... – Anthrax знал, что он хотел сказать, но его язык словно окаменел, – с большей энергией, наверное.

Оба полицейских заметно напряглись.

Дэй продолжал:

– Вы можете сказать, что мотивы, заставившие вас прийти к нам, сформировались в результате чьих-то недобросовестных действий?

– В каком смысле?

– Ваши слова были записаны на пленку, и я должен прояснить этот вопрос. Вы можете сказать, что на каком-либо этапе вам предложили сделку?

Сделку? Anthrax думал об этом. Никто не предлагал ему: «Расскажи нам все, что ты знаешь, и мы даем тебе честное слово, что ты не сядешь в тюрьму». Или: «Говори быстро, и мы не будем избивать тебя резиновыми дубинками».

– Нет, – ответил он.

– Вы можете сказать, что в результате этих слов вы были вынуждены прийти сегодня и говорить правду?

Ах, вот что за сделка. Да, конечно.

– Да, я был вынужден, – ответил Anthrax.

Оба полицейских были изумлены. Anthrax замолчал, оценивая растущее неодобрение.

– Косвенно, – добавил он быстро, словно извиняясь.

На какое-то время Anthrax'у стало наплевать. На полицию. На отца. На давление. Он *непременно* скажет правду. Он решил объяснить ситуацию со своей точки зрения.

– Потому что, когда они пришли ко мне домой, они несколько раз повторили, что если я не соглашусь на допрос, они обвинят во всем мою мать. А моя мать очень больна, и я не могу позволить ей пройти через это.

Полицейские переглянулись. Атмосфера в комнате накалилась. АФП явно не ожидала, что такое появится в записи интервью. Но то, что он сказал об угрозах в адрес матери, было правдой, так что пусть уж теперь это останется на пленке вместе со всем остальным.

Кен Дэй задержал дыхание.

– То есть, вы хотите сказать, что вы приехали сюда... – он нервно сглотнул, – что вы здесь не по доброй воле?

Anthrax думал и об этом. Что означала фраза «по доброй воле»? Полицейские не приковывали его к стулу и сказали, что он может уйти, когда захочет. Они не били его дубинкой по голове. Они предложили ему выбор – говори или натрави полицию на свою больную мать. Не самый приятный

выбор, но все же выбор. Он *решил* говорить, чтобы защитить свою мать.

– Я здесь по доброй воле, – ответил он.

– Нет, это не то, что вы сказали. Вы сказали, что на вас было оказано давление и вам *пришлось* прийти сюда и отвечать на вопросы. Иначе против вас были бы предприняты определенные меры. Это не означает, что вы здесь по доброй воле.

Полицейские явно догадались, что они идут по очень тонкому льду, и Anthrax почувствовал, что напряжение в комнате возросло до предела. Копы нажимали. Его отец сидел, как на иголках.

– Я собирался прийти в любом случае, – ответил Anthrax, снова извиняющимся тоном. Он подумал, что играет с огнем. Не стоит слишком дразнить их, а то они обвинят мать. – Вы можете поговорить с людьми, которые проводили обыск. Я все время говорил им, что приеду на допрос. Какими бы ни были мои собственные причины, я не думаю, что это важно. Я собираюсь сказать вам правду.

– Это важно, – ответил Дэй, – потому что в начале допроса было сказано – и вы согласились, – что вы находитесь здесь по своей воле.

– Так и есть. Никто меня не заставлял.

Anthrax терял терпение. В комнате становилось душно. Он хотел покончить с этим и убраться отсюда. Такой напруг.

– Может быть, кто-то заставил вас отвечать на наши вопросы именно так, как вы это сделали? – снова попытался Дэй.

– Нет, никто не заставлял меня.

Ну вот. Вы получили то, что хотели. Давайте завязывать и пойдем отсюда.

– Вы сказали, что должны говорить правду. Не так ли? – Полиция намеревалась идти до конца.

– Я также и *хочу* сказать правду.

Ключевым словом было «также», подумал Anthrax. Я *хочу* и я *должен*.

– Вы были вынуждены принять это решение по воле обстоятельств или людей?

– Обстоятельств.

Конечно, это были обстоятельства. Неважно, что их создала полиция.

Anthrax чувствовал себя игрушкой в руках полиции. И он, и они знали, что если их не удовлетворит исход интервью, преследованиям подвергнется его мать. Он с потрясающей четкостью представил себе, как федералы вытаскивают из дома его хрупкую мать. Anthrax'а бросило в жар. Пора покончить с этим. Все, что им угодно: он будет просто соглашаться с ними, лишь бы выбраться из этой тесной комнаты.

– Итак, справедливо ли будет заключить на основе вышесказанного, что, возможно... ваша деятельность до момента обыска и была тем фактором, благодаря которому вы оказались здесь?

Да о чем это он толкует? Его «деятельность» заставила его? Anthrax был в полном смятении. Интервью явно затянулось. У копов была довольно странная манера задавать вопросы. Комната была удручающе мала.

Дэй настаивал на своем вопросе.

– Вы осознали, что нарушили закон, и этот факт заставил вас прийти сюда и говорить нам правду, не так ли?

Да. Все что ты хочешь.

– ОК, – начал Anthrax, – это справедливое предполо...

Дэй перебил его.

– Я просто хочу до конца прояснить вопрос. Я понял из ваших слов, что мы или другие сотрудники АФП нечестно и несправедливо заставили вас прийти сюда сегодня, или это не так?

Что значит «нечестно»? Что значит «несправедливо»? Anthrax считал несправедливым, что копы могли обвинить его мать. Но они сказали ей, что это абсолютно законная мера. У Anthrax'а кружилась голова. Все эти мысли неотступно жужжали в его голове.

– Нет, это не так. Прошу прощения за...

Смирись. Скорее прочь из этой комнаты.

– Ничего, ничего. Если вы так не считаете, скажите об этом. У меня нет с этим проблем. Я просто хочу, чтобы не осталось никаких неясностей. Подумайте о том, что другие люди могут прослушать эту запись и на ее основании сделают свои выводы и придут к какому-то мнению. Если я замечаю, что где-то существует неясность, я хочу ее устранить. Вам понятно мое намерение?

– Да. Я понимаю. – Anthrax не мог до конца сосредоточиться на словах Дэй. Он был совершенно измотан и хотел поскорее закончить допрос.

Копы все-таки двинулись дальше, но новая тема была так же неприятна. Дэй попытался заговорить о начале хакерской карьеры Anthrax'а – а у него не было ни малейшего желания беседовать об



этом. Anthrax'у стало немного лучше. Он согласился ответить на вопросы полиции о недавней фрикерской активности, ни о каком хакинге не было и речи. В самом деле, он несколько раз повторял копам, что эта тема не входит в его планы. Он почувствовал под ногами более надежную опору.

После такого вежливого отпора Дэй покружил вокруг да около и попытался еще раз:

– ОК. Вот вам еще одно утверждение – вы незаконно проникли в компьютерные системы в Австралии и в США. В Соединенных Штатах вас особенно интересовали военные компьютеры. Вам понятно это утверждение?

– Да, понятно. Я бы не хотел его комментировать. Нет, сэр. Ни за что.

Дэй решил применить новую тактику:

– Я возьму на себя смелость утверждать, что вы работали с лицом, известным как Mendax.

Какого черта он несет? Anthrax слышал о Mendax'е, но они никогда не работали вместе. Он подумал, что у федералов, видимо, не очень хорошие осведомители.

– Нет. Это неправда. Я не знаю никого с таким именем. – Это была почти правда.

– Что ж, значит, если он придет ко мне и скажет, что вы вместе занимались хакерскими делами, это будет неправда, не так ли?

Просто прекрасно. Какой-то хакер намолол копам чепухи о том, что он работал вместе с Anthrax'ом. Именно поэтому Anthrax всегда работал в одиночку. У него было полно реальных проблем. И выдуманные ему были совсем ни к чему.

– Само собой, это будет неправда. Я не знаю никого по имени Mendax, если только у него нет какого-нибудь другого имени.

Побыстрее отделаться от этого.

На самом деле Mendax вовсе не стучал на Anthrax'а. Обычные полицейские методы.

– Вы отказываетесь комментировать тот факт, что вторгались в другие компьютеры и военные системы?

Если Anthrax и мог что-то сказать о Дэе, так это то, что он настойчив.

– Да. Я предпочел бы не комментировать этот факт. Именно такой совет мне дали: не комментировать ничего, не связанного с темой, которую мы, по вашим словам, должны были обсуждать, когда я пришел сюда.

– Хорошо, значит вы не будете отвечать ни на какие вопросы, связанные с незаконным доступом в компьютерные системы?

– Следуя совету моего адвоката, нет.

Дэй поджал губы.

– Хорошо. Если вы приняли такое решение и не хотите отвечать на наши вопросы, мы оставим эту тему. Но я обязан проинформировать вас, что, возможно, нам придется вернуться к ней, и вас официально обяжут отвечать на эти вопросы, либо выдвинут обвинения по ним. Поэтому, как только вы захотите сказать нам правду, мы к вашим услугам.

Ох. Anthrax глубоко вдохнул. Неужели копы могут обязать его отвечать на их вопросы? Они меняют свое мнение на полпути. Anthrax'у казалось, что земля уходит у него из-под ног. Ему нужно было несколько минут, чтобы собраться с мыслями.

– Я могу подумать об этом и все взвесить? – спросил Anthrax.

– Конечно. Не хотите ли сделать перерыв и поговорить с отцом? Мы с констеблем выйдем из комнаты или можем предоставить вам другую. Если хотите, мы можем сделать перерыв, чтобы вы могли подумать об этом. Думаю, это хорошая мысль. Я думаю, мы сделаем перерыв минут на десять и предоставим вам другую комнату. Вы сможете поговорить об этом наедине. Никакого давления.

Дэй и Секстон остановили допрос и отвели отца с сыном в другую комнату. Когда они остались одни, Anthrax посмотрел на отца в поисках поддержки. Его собственный внутренний голос кричал ему, чтобы он держался подальше от вопросов о его ранних хакерских предприятиях. Anthrax'у нужен был кто-то, кто сказал бы ему то же самое.

Но это определенно был не его отец. Тот обрушился на Anthrax'а с невероятной враждебностью. Хватит тормозить. Ты *должен* сказать им *все*. Как можно быть таким тупым? Тебе не одурочить полицию. Они *знают*. Расскажи им все, пока не поздно. В конце его десятиминутной тирады Anthrax почувствовал себя намного хуже, чем в начале.

Когда они вернулись в комнату для допросов, отец Anthrax'а повернулся к полицейским и вдруг сказал:

– Он решил признаться.

Но это было не так. Anthrax не собирался делать ничего подобного. Его отец был просто ходячим сюрпризом. Как только он открывал рот, можно было не сомневаться, что из него выскочит оче-

редной неприятный сюрприз.

Кен Дэй и Эндрю Секстон не дали потрясенному Anthrax'у опомниться и навалились на него с новыми документами, обрывками бумаги с его собственными каракулями, захваченными во время обыска, с записями прослушивания телефонов. Вдруг Дэй напрягся и показал на какую-то надпись. Она выглядела как «KDAY». Он посмотрел на Anthrax'а.

– Что это? Это я?

Anthrax впервые за долгое время улыбнулся. И было отчего. Шеф Отдела по борьбе с компьютерными преступлениями АФП в Мельбурне сидел перед ним, совершенно уверенный в том, что он напал на что-то серьезное. Это было его имя, ясно, как день, написанное рукой хакера на листке бумаги, изъятого во время обыска. Дэй явно надеялся на нечто интересное.

– Если вы позвоните туда, вы узнаете, что это название радиостанции, – сказал Anthrax.

Это была американская радиостанция. Ее название было записано на одном клочке бумаги с названиями американского магазина одежды, еще одной радиостанции в США и несколькими новыми дисками, которые он хотел заказать.

– Ну и дела, – засмеялся Дэй над своими собственными поспешными заключениями. – Существует радиостанция, которую назвали моим именем.

Дэй спросил у Anthrax'а, зачем он записывал все эти сведения: пути к файлам, коды, извещения об ошибках.

– Просто регистрировал факты. Я думаю, что я сделал это, когда впервые получил учетную запись. Я пробирался наугад, записывая информацию о том, для чего предназначены разные вещи.

– Каковы были ваши намерения в то время насчет этих систем?

– В тот момент я просто смотрел, из любопытства.

– Это было любопытство вроде «Ух ты! Как интересно!» или же это больше было похоже на «Я хотел бы попасть внутрь»?

– Я не могу точно сказать, что творилось у меня в голове в тот момент. Но в самом начале... я думаю, что вам пришлось выслушать немало подобных историй... Когда ты впервые проникаешь в систему, это выглядит словно... – Anthrax не мог подобрать точных слов, чтобы закончить объяснение.

– Словно впервые попробовал запретный плод?

– Точно. Это отличная аналогия.

Дэй продолжал задавать вопросы о хакерской деятельности Anthrax'а. Он вытягивал из него признания. Anthrax дал ему больше, чем у полицейского было прежде, но, возможно, меньше, чем тот бы хотел.

Впрочем, этого было достаточно. Достаточно, чтобы оградить мать Anthrax'а от всяких обвинений. И достаточно, чтобы обвинить его самого.

:)

Anthrax не видел окончательного списка своих обвинений до самого дня суда 28 августа 1995 года. Все дело выглядело не слишком организовано. Его адвокат из Legal Aid почти ничего не знал о компьютерах, не говоря уже о компьютерных преступлениях. Он сказал Anthrax'у, что мог бы попросить отложить слушания, потому что он тоже увидел список обвинений в самый последний момент. Но Anthrax хотел побыстрее покончить с этим. Они договорились, что Anthrax признает свою вину по всем пунктам и будет уповать на снисходительность суда.

Anthrax просмотрел краткое изложение дела, представленное обвинением. Оно включало в себя и тщательно отредактированную запись его интервью с полицейскими. Эта запись была помечена как «резюме», но она, конечно, не резюмировала самого важного в этом интервью. Либо обвинение, либо полиция убрали из него всякое упоминание о том, что полицейские обещали обвинить мать Anthrax'а, если он не согласится на допрос.

Anthrax поразмыслил об этом. Разве краткое изложение дела не должно охватывать все связанные с ним обстоятельства? А этот факт был напрямую связан с делом, хотя в документе о нем не было ни единого упоминания. Он бы не удивился, если бы узнал, что полиция поработала с записью допроса так, чтобы вырезать из нее эту часть. Судье бы это наверняка не понравилось. Anthrax подумал, что полиции не слишком хотелось нести ответственность за такое обращение с его матерью.

Оставшаяся часть в изложении дела с точки зрения обвинения была не лучше. Единственным показанием реального «свидетеля» хакинга Anthrax'а было заявление его бывшего соседа по комнате – он утверждал, что видел, как Anthrax взломал компьютер NASA и получил доступ в «область ком-

пьютерной системы, которая показывает координаты широты/долготы».

Есть ли у *космических* кораблей широта и долгота? Anthrax не знал. Но он точно не мог взламывать компьютер NASA в присутствии соседа по комнате. Это полная чушь. Anthrax подумал, что парень врет, и компетентный юрист доказал бы это за пять минут перекрестного допроса. Anthrax чувствовал, что по многим пунктам позиция обвинения выглядит неубедительно, но он был просто ошеломлен давлением со стороны семьи, всей этой суетой в зале суда, даже официальностью собственного адвоката, который быстро перелистывал его бумаги.

Anthrax оглядел зал суда. Его взгляд упал на отца, который сидел на скамье для публики, ожидая, пока его вызовут. Адвокат Anthrax'a настоял на его присутствии, рассчитывая вызвать его в качестве свидетеля защиты. Он думал, что присутствие на суде семьи обвиняемого пойдет ему только на пользу. Anthrax был не в восторге от этой идеи. Но он не очень хорошо представлял, как работают суды, поэтому последовал совету адвоката.

Мать Anthrax'a оставалась дома в ожидании новостей. Она работала в ночную смену и сейчас, должно быть, отсыпалась. Но, скорее всего, эта причина была лишь предлогом. Anthrax подумал, что она не пришла, потому что такое напряжение было для нее слишком велико. Конечно, она не спала. Она наводила порядок, мыла посуду, занималась стиркой и старалась занять себя, насколько это было возможно в ее маленькой квартире.

Девушка Anthrax'a, красивая круглолицая турчанка, тоже пришла в суд. Она никогда не принадлежала к хакерскому кругу. Позади нее расположилась гомонящая группка школьников, в основном девочек.

Anthrax прочитал все четырехстраничное резюме обвинения. Когда он добрался до последней страницы, его сердце остановилось. Последний параграф гласил:

**31. Наказание**

S85ZF (a) – 12 месяцев, \$6000 или и то и другое

s76E (a) – 2 года, \$12 000 или и то и другое.

Показывая на последний параграф, Anthrax спросил у своего адвоката, что все это значит. Тот сказал ему, что, возможно, дело дойдет до тюрьмы, но в конечном итоге это не так уж страшно и ему не стоит «вешать нос». Он пробудет там всего-навсего год или два.

Даже насильникам иногда дают меньше. Anthrax не мог поверить, что обвинение настаивает на тюремном сроке. И это после того, как он согласился сотрудничать, прошел через это проклятое интервью. Кроме того, прежде он не был под судом. Но снежный ком разрастался по мере движения. Наконец появился судья, и заседание суда началось.

Anthrax понял, что поздно идти на попятную, и признал свою вину по 21 пункту, в том числе одно обвинение, связанное с исправлением данных и двенадцать обвинений в обмане или попытке обмана компаний–операторов связи.

Адвокат призвал суд к смягчению приговора. Он вызвал отца Anthrax'a и стал задавать ему вопросы о сыне. Но отец больше навредил, чем помог. Когда у него спросили, не думает ли он, что его сын снова будет нарушать закон, он ответил: «Я не знаю».

Anthrax побледнел от злости. Это был просто верх подлости. Незадолго до суда Anthrax узнал, что отец собирался улизнуть из страны за два дня до начала процесса. Он говорил жене, что собирается уехать, но лишь после того, как закончатся слушания. Она совершенно случайно обнаружила, что он собирается отбыть пораньше. Видимо, он считал, что суд над сыном унижает его. Мать Anthrax'a настояла, чтобы он остался, и отец скрепя сердце отложил отъезд.

Отец вернулся на свое место, в некотором отдалении от Anthrax'a и его адвоката. Адвокат представлял собой резкий контраст с прокурором. Он задрал одну ногу на скамью, пристроил руку на колено и принялся поглаживать свою длинную рыжую бороду. Это была знатная борода, больше фута в длину, с очень густыми красно-коричневыми завитками. Она вполне сочеталась с его шоколадно-коричневым костюмом и галстуком – впечатляюще широким произведением искусства с дикими золотыми узорами. Правда, костюмчик был ему явно маловат. Адвокат начал в обычном цветистом стиле – много ничего не значащих слов. Затем он перешел в нападение.

– Ваша честь, этот молодой человек побывал во многих местах – NASA, военные сайты, вы просто не поверите, когда узнаете, в каких местах он был.

– Не думаю, что меня интересует, где он был, – желчно ответил судья.

Это была стратегия Anthrax'a. Он подумал, что сможет превратить пассивы в активы, показав, что он побывал во многих системах – очень секретных системах, но не причинил ни одной из них

никакого вреда.

Замысел удался. Судья объявил, что он не видит никаких причин, чтобы отправить юного хакера в тюрьму.

Прокурор был искренне разочарован и выступил с встречным предложением – 1500 часов общественных работ. У Anthrax’a перехватило дыхание. Это просто абсурд. Вкалывать почти девять месяцев, от зари до зари. Красить здания и чистить уборные. Можно поставить крест на учебе. Это ничуть не лучше тюрьмы.

Защитник Anthrax’a запротестовал:

– Ваша честь, такое наказание скорее годится для киберпространства.

Anthrax’a покорило от этой сомнительной сентенции, но его адвокат был явно доволен собой.

Судья отказался поддержать предложение прокурора. Он произвел серьезное впечатление на подругу Anthrax’a. Она не была близко знакома с законами или с судебной системой, но этот судья казался справедливым и беспристрастным. Такое впечатление, что он вовсе не собирался выносить по делу Anthrax’a суровый приговор. Но он сказал суду, что намерен донести до подсудимого, до класса школьников в зале заседаний и до широкой публики, что хакинг – это преступление в глазах закона. Anthrax оглянулся на школьников. Им было лет по тринадцать-четырнадцать. Как раз в этом возрасте он начал заниматься хакингом и фрикингом.

Судья объявил приговор. Двести часов общественных работ и возмещение убытков двух телефонных компаний – Telecom и Teleglobe из Канады – в размере \$6116,90. Это, конечно, была не тюрьма, но все же огромная сумма денег для студента. Ему нужно было выплатить ее в течение года – определенно не такой уж большой срок. Но самое главное, он был свободен.

Подруга Anthrax’a подумала о том, что всех этих хихикающих школьников привели в зал суда в тот день совершенно напрасно. Они смеялись, показывали пальцами и перешептывались. Для них суд был игрой. Они явно не воспринимали всерьез предупреждение судьи. Может быть, они трепались о ближайшей вечеринке. Возможно, они болтали о новой паре кроссовок или последнем компакт-диске.

Но не исключено, что один или двое думали про себя о том, как было бы круто пробраться в NASA.

## Послесловие

Это событие было заявлено как «самая большая ежегодная тусовка участников, сочувствующих и тех, кто интересуется компьютерным подпольем», поэтому я решила, что мне стоит поехать.

НоНоСоп в Остине, штат Техас, был, несомненно, одним из самых странных собраний, на которых мне приходилось бывать. В течение уик-энда в конце 1995 года гостиница Ramada Inn South была переполнена хакерами, фрикерами, экс-хакерами, теми, кто симпатизировал андеграунду, журналистами, служащими компьютерных компаний и агентами американских спецслужб. Некоторые приехали из таких далеких мест, как Германия и Канада.

Хакеры и фриkerы спали вчетвером или вшестером в комнате – если спали вообще. Федералы спали по двое. Я могу и ошибаться; возможно, они вовсе не были федералами. Но они были слишком хорошо, слишком аккуратно одеты, чтобы быть кем-то еще. Кроме них, никто на НоНоСоп не гладил футболки.

Я вышла из главного конференц-зала и отправилась в комнату 518 – компьютерную комнату. Я села на одну из двух кроватей, которые были задвинуты в угол, чтобы освободить место для компьютерного оборудования, и принялась наблюдать за происходящим. Организаторы конференции привезли достаточно оборудования, чтобы открыть целый магазин, а затем подключили все это хозяйство к Интернету. Все два с небольшим дня комната почти постоянно была переполнена. Ребята чуть младше или немного старше двадцати лениво сидели на полу, играли своими сотовыми телефонами и радиосканерами или работали за шестью-семью терминалами. Пустые пакеты из-под чипсов, банки колы и коробки из-под пиццы в беспорядке валялись повсюду. Атмосфера напоминала ту, что бывает на больших вечеринках в колледже, с тем исключением, что люди больше говорили не друг с другом, а с компьютерами.

Но не только здесь можно было встретить интересных людей. Я познакомилась с группой нон-конформистов компьютерной индустрии более старшего возраста, что-то вроде остинской интеллигенции. Говоря о возрасте, я имею в виду, что они были старше 26 лет. Они интересовались почти теми же вопросами, что и молодые хакеры, – приватность, кодирование, будущее цифрового мира, – и у каждого из них была техническая квалификация.

Эта свободная группа одетых в джинсу мыслителей, таких как Дуг Барнс [Doug Barnes], Джереми Портер [Jeremy Porter] и Джим Мак-Кой [Jim McCooy], любила встречаться за «энчиладами» и «Маргаритами» в студенческих кафе. У них всегда было в голове несколько новых проектов. Цифровые деньги были темой месяца, когда мы познакомились. Все они презируют условности, все они не без странностей, но при этом умны, креативны и полны невероятных новых идей. Это были люди того сорта, которые способны сочетать новые идеи со зрелостью и деловой хваткой, в итоге превращая виртуальные деньги в реальность.

Я спрашивала себя, сколько же ребят из комнаты 518 пойдут тем же путем? Есть ли такие же парни в Австралии?

Кажется, что они либо совершенно невидимы, либо вовсе не существуют. Возможно, они есть только в компьютерном подполье. Андеграунд оказался единственным местом в Австралии, где безумие, креативность, одержимость, зависимость и бунтарская жилка сталкиваются, как атомы в циклотроне.

;)

Что стало с героями этой книги после всех этих рейдов, арестов и судебных дел на трех континентах?

Большинство из них устроило свою жизнь, занимается интересными и конструктивными вещами. Те, с кем я разговаривала в процессе работы над книгой, сказали, что они навсегда покончили с хакингом. И это неудивительно после всего того, через что пришлось пройти большинству из них.

Но все же почти никто не жалеет о своей хакерской деятельности. Некоторые винят себя за то, что причиняли неприятности другим. Им жаль, что они изводили системных администраторов и портили им нервы, вторгаясь в их системы. Тем не менее большинство из них не считает хакинг преступлением, особенно «ознакомительный хакинг», как определил его прокурор Джефф Четтл.

Наказание только укрепило их мнение по этому вопросу. Они отдают себе отчет в том, что власти решили на их примере преподать урок всему компьютерному подполью. Но государство жестоко просчиталось. В глазах большинства компьютерного андеграунда эти приговоренные хакеры стали героями.

## **Par**

Когда я встретила Par'a в Таксоне, штат Аризона, он ехал из маленького заснеженного городка на Среднем Западе, где жил у деда с бабкой. Он искал работу, но безуспешно.

Я страдала от разницы часовых поясов и немного заплутала в окрестностях Таксона. Красота зимнего солнца и кактусов пустыни Сонора часто отвлекали меня от дороги. Как-то сидящий на переднем пассажирском сиденье Par спокойно сказал: «Мне всегда было интересно, что чувствуешь, когда едешь по встречной полосе».

Я резко свернула на свою полосу.

Par до сих пор такой. Беспечный, бредущий куда глаза глядят, он довольствуется тем, что дает ему жизнь. Он снова в дороге.

На какое-то время он вернулся на западное побережье, но вскоре собрал вещи и перебрался в другое место. Он берется за любую временную работу. В основном это простейшая скучища, связанная с обработкой данных. Но и такую работу непросто получить. Он никак не может объяснить четырехлетний пробел в своем резюме фразой вроде: «Успешно окончил курсы беглецов. Прошел стажировку в Секретной службе США». Он думал, что ему подошла бы работа в компьютерной лаборатории какого-нибудь местного колледжа. Он мог бы помогать студентам и следить за работой оборудования. Но если у тебя нет никакой профессиональной квалификации, на сегодняшний момент это практически нереально.

Хотя Par больше не числится в бегах, его жизнь не слишком изменилась. Он часто звонит матери, хотя у них не так уж много общего. Оказалось, что гораздо легче избежать обвинений в компьютерных преступлениях, чем избавиться от последствий жизни в бегах. Время от времени его снова охватывает паранойя. Она похожа на приливы и отливы. А в Соединенных Штатах мало кто стремится помочь безработному молодому человеку, у которого нет даже медицинской страховки.

## **Prime Suspect**

Prime Suspect не жалеет о своем выборе. Он считает, что у них с Mendax'ом разные взгляды на жизнь. В любом случае дружба кончилась бы, и он решил, что не хочет идти в тюрьму вслед за Mendax'ом.

Он закончил курс по компьютерному программированию в TAFE и нашел работу в бурно развивающейся индустрии Интернета. Ему нравится его работа. Его работодатель знает о его хакерском приговоре. Недавно он повысил ему зарплату. В середине 1994 года Prime Suspect навсегда бросил принимать наркотики. В 1995 году снял дом вместе с несколькими друзьями, а в августе 1996 года бросил курить.

В отсутствие хакинга в его жизни наступило время для других интересных вещей. Он занялся скай-дайвингом. Один прыжок дает ему кайф, который длится несколько дней, иногда даже неделю. Девушки очень интересуют его. У него было несколько подружек, и он думает, что готов завязать серьезные отношения, когда встретит подходящего человека.

С недавних пор Prime Suspect начал изучать боевые искусства. Он старается посещать занятия не меньше четырех раз в неделю, иногда и чаще, и говорит, что его особенно интересует духовная и философская сторона этого явления. Он встает в пять утра почти каждый день для пробежки или медитации.

## **Mendax**

В 1992 году Mendax и Тгах объединились с богатым инвестором в недвижимость из Италии, купили большой компьютер университета Ла-Трууб (по иронии судьбы, именно ту машину, во взломе которой их обвиняли) и основали компанию по компьютерной безопасности. Компания в конце концов развалилась, когда инвестор исчез, преследуемый своими кредиторами.

После публичного столкновения в 1993 году с премьер-министром штата Викторией Джеффом Кеннетом Mendax и двое его товарищей создали правозащитную организацию по борьбе с коррупцией и безответственностью в правительстве штата. В ходе этой борьбы Mendax способствовал тайной утечке документов и оказался вовлечен в несколько судебных дел против правительства в 1993–1994 годах. В конце концов он дал показания на закрытом судебном заседании при рассмотрении этих вопросов комиссией парламента штата. Впоследствии его организация способствовала появлению более 40 свидетелей в расследовании Генерального прокурора.

Mendax предоставляет свое время и компьютерный опыт нескольким другим некоммерческим общественным организациям. Он верит в значение некоммерческого сектора и посвящает большую часть свободного времени активной работе в различных общественных проектах. Mendax предоставляет информацию правоохранительным органам, но только не против хакеров. Он говорит: «Я не считаю это этически оправданным. Но в отношении тех, кто мучает детей, или тех, кто шпионит для корпораций, я без всяких угрызений совести использую свои умения».

Mendax по-прежнему увлекается программированием и уделяет много времени международным проектам. Некоторые из своих программ он бесплатно публикует в Интернете. Его философия заключается в том, что большая часть прогрессивных социальных прорывов в истории человечества произошла благодаря новым технологиям.

NorTel и несколько других организаций, обвинивших его во взломе их систем, используют его шифровальные программы – он относится к этому скорее с иронией.

## **Anthrax**

Anthrax переехал в Мельбурн. Он закончил там университетский курс и сейчас работает на контрактной основе с компьютерными сетями крупной корпорации.

Его родители развелись. Anthrax по сей день не разговаривает с отцом.

Здоровье его матери в какой-то степени стабилизировалось после окончания суда, хотя она все еще страдает от хронических болей. Несмотря на некоторую потерю пигментации кожи из-за болезни, она, в общем, выглядит неплохо. Благодаря многолетней работе в местной больнице, она приобрела верных друзей, которые поддерживают ее во время приступов болезни. Она старается сохранять жизнерадостность и продолжает поддерживать хорошие отношения с обоими сыновьями.

Anthrax отошел от «Нации ислама», хотя не перестал быть правоверным мусульманином. Один из его знакомых, албанец, хозяин местной закусочной, познакомил его с другим течением ислама. Вскоре после этого Anthrax стал суннитом. Он не употребляет алкоголя, не играет в азартные игры и молится каждую пятницу по вечерам в местной мечети. Он старается ежедневно читать Коран и не-

укоснительно выполнять догматы своей религии.

Теперь, когда его компьютерные и деловые таланты востребованы, он подумывает о том, чтобы переехать в какую-нибудь мусульманскую страну Азии или Среднего Востока.

Большую часть своей потребности в розыгрышах он теперь удовлетворяет с помощью записей розыгрышей других людей на компакт-дисках, которые можно купить с помощью специальных журналов и американских почтовых каталогов. Очень редко, но все же случается, что он звонит мистеру Мак-Кенни в поисках пропавшей лопаты.

Anthrax был огорчен результатом своей жалобы в офис омбудсмана. В своем заявлении Anthrax написал, что, по его мнению, АФП действовала неправомочно в ходе расследования его дела. В частности он заявил, что полиция оказывала давление на его мать с помощью угроз, постоянно беспокоила его самого, фотографировала его без его ведома, сообщила информацию о его деле в университет еще до того, как он получил судебную повестку и было вынесено судебное решение, наконец, позволила себе расистские комментарии на его счет во время обыска.

В 1995–1996 годах против АФП поступило 1157 жалоб. 683 из них были рассмотрены омбудсменом Содружества. Из всего числа рассмотренных и расследованных жалоб только 6 % были признаны достаточно основательными. Еще 9 % были квалифицированы как «неопределенные», около 34 % сочли «безосновательными», и более половины всех дел было решено либо вовсе не расследовать, либо не продолжать расследование в отношении жалобы.

Офис омбудсмана направил дело Anthrax'a в отдел внутренних расследований АФП. Хотя Anthrax и его мать дали показания офицерам этого отдела, заявление Anthrax'a не подкреплялось другими доказательствами. Все свелось к слову Anthrax'a и его матери против слова полиции.

Внутреннее расследование АФП сделало вывод, что жалоба Anthrax'a может быть отнесена либо к безосновательным, либо к неопределенным, частично мотивируя это тем, что после описанных в ней событий прошло почти два года. Можно сказать, что омбудсмен стал основой для выводов АФП. Ни на одного из офицеров не было наложено взыскание.

Единственным, хоть и весьма сомнительным, утешением для Anthrax'a стало заключение, полученное из офиса омбудсмана. Несмотря на то что дознаватель согласилась со следователями АФП, что жалоба не имеет под собой оснований, она написала: «Я убеждена, что ваша мать почувствовала, что она вынуждена оказать на вас давление с тем, чтобы вы согласились на интервью, из страха быть обвиненной из-за того, что ее телефон использовался для совершения преступлений».

Anthrax по-прежнему испытывает недовольство и раздражение от своего опыта общения с полицией. Он считает, что в работе полиции нужно многое изменить. Более того, он считает, что правосудие невозможно осуществлять в обществе, где полиции позволено проводить расследования в отношении себя самой.

## **Pad и Gandalf**

После того, как Pad и Gandalf вышли из тюрьмы, они создали в Интернете бесплатную консультативную службу по безопасности. Во-первых, они начали проводить свои 8lgm-консультации, как их стали называть, чтобы помочь администраторам обезопасить собственные системы. Во-вторых, они хотели поставить на место консерваторов от компьютерной индустрии.

Многие в Интернете считали советы 8lgm лучшими, какие можно было получить в то время, — гораздо лучшими, чем те, что когда-либо давал CERT. Pad и Gandalf словно отфутболили послание истеблишмента в его же ворота. Их послание, никогда не публиковавшееся официально, могло бы выглядеть примерно так: «Вы арестовали нас. Вы отправили нас в тюрьму. Это неважно. Вы не можете хранить такую информацию в секрете. Более того, мы все еще лучше вас, и чтобы доказать это, мы побьем вас на вашем собственном поле».

Полагая, что лучшим способом удержать хакера подальше от вашей системы является, в первую очередь, должное отношение к ее безопасности, тандем британских хакеров с неуважением отзывался о гуру безопасности, которые отказываются сообщать миру о новых проблемах в этой области. Их 8lgm-советы ехидно комментировали традиционные доклады индустрии безопасности и помогли подтолкнуть ее к нынешнему более открытому состоянию.

Сейчас Pad и Gandalf работают вдвоем, выполняя по контрактам заказы на компьютерное программирование, иногда даже для финансовых учреждений. Их клиенты довольны ими и ценят их работу. У обоих постоянные подруги.

Pad больше не занимается хакингом. Причина не в том, что он боится ареста или тюрьмы. Он бросил хакинг, когда осознал, какую головную боль приходится перенести системному администрато-

тору, чтобы очистить свою систему после нападения. Просмотреть все регистрации. Проверить, не оставил ли хакер для себя лазейку. Время, усилия, нервное напряжение – Pad решил, что несправедливо подвергать кого-то таким испытаниям. Теперь он гораздо лучше понимает, какие страдания может причинить другому человеку вторжение хакера.

Есть и другая причина, по которой Pad перестал заниматься хакингом: он просто вырос. Он говорит, что у него есть гораздо более интересные занятия. Компьютеры стали для него способом зарабатывать деньги, а не убивать время. После поездки за океан он решил, что настоящие путешествия – а не их электронные родственники – гораздо интереснее хакинга. Еще он научился играть на гитаре – по его мнению, он сделал бы это давным-давно, если бы не уделял столько времени хакингу.

Gandalf разделяет интерес Pad'a к путешествиям. Одной из причин, по которой им нравится работать по контрактам, является то, что это позволяет им заработать достаточно денег за полгода упорной работы, а затем отдыхать несколько месяцев. Цель обоих бывших хакеров теперь заключается в том, чтобы просто повесить рюкзаки на плечи и колесить по всему свету.

Pad по-прежнему считает, что в Британии слишком серьезно относятся к хакингу, и подумывает навсегда перебраться за границу. Суд по делу 8lgm заставил его усомниться в достоинствах тех, кто облечен властью в Англии – политиков, судей, сотрудников силовых ведомств. Он часто думает: что за люди управляют этим шоу?

## Стюарт Гилл

В 1993 году омбудсмен штата Виктория<sup>50</sup> и полиция штата<sup>51</sup> проводили каждый свои расследования по утечке конфиденциальной полицейской информации в рамках операции «Айсберг» – расследования по заявлению о коррупции заместителя комиссара полиции Фрэнка Грина [Frank Green]. Стюарт Гилл занимал не последнее место в обоих расследованиях.

В отчете полиции штата Виктория было сделано заключение, что «Гилл сумел внедриться в полицейскую среду, ловко манипулируя информацией, чтобы не вызвать подозрений». Вывод омбудсмана гласил, что «большое количество конфиденциальной полицейской информации, главным образом из базы данных ISU, было передано... Гиллу [офицером полиции Виктории] Косгриффом».

Полиция заявила в своем отчете, что инспектор Крис Косгрифф умышленно предоставлял Гиллу секретную полицейскую информацию и что он был «одурманен Гиллом». Суперинтендант Тони Уоррен, бывший представитель комиссара Джон Фрэйм [John Frame] и бывший заместитель комиссара Бернис Мастерстон [Bernice Masterston] также подверглись критике в отчете.

Омбудсмен сделал вывод, что отношения Уоррена и Косгрифа с Гиллом были «главной причиной утечки конфиденциальной информации». Интересно, что омбудсмен также заявил: «В то время как у мистера Гилла были собственные планы по извлечению выгоды из отношений с полицией, та, в свою очередь, точно так же использовала отношения с мистером Гиллом, а иногда злоупотребляла ими в своих целях».

Далее в отчете омбудсмана было сделано заключение о том, что нет доказательств преступного поведения Фрэнка Грина, и «заявления, сделанные несколько лет назад против мистера Грина, следовало проверить и расследовать в момент их поступления».

## Phoenix

Дело Phoenix'a еще подробно освещалось СМИ, когда он мчался на своем мотоцикле дождливой ночью по одной из центральных улиц Мельбурна и столкнулся с автомобилем. Водитель выскочил из машины и увидел страшную картину. Phoenix распростерся посреди дороги, его шлем треснул, когда он ударился о бензобак автомобиля. И мотоцикл, и его хозяин были залиты бензином.

Но Phoenix – чудо! – легко отделался, хотя и был оглушен. Прохожие помогли ему и потрясенному водителю добраться до ближайшей гостиницы, где вызвали «скорую помощь» и предложили чай обоим пострадавшим молодым людям. Вскоре приехала мать Phoenix'a, вызванная по его просьбе одним из прохожих. Врачи подтвердили, что у Phoenix'a нет переломов, но посоветовали обратиться в больницу для проверки того, нет ли у него сотрясения мозга.

<sup>50</sup> Victorian Ombudsman, *Operation Iceberg: Investigation of Leaked Police Information and Related Matters*.

<sup>51</sup> Отчет полиции был напечатан в качестве приложения к докладу омбудсмана. См. выше, первое примечание к 5-й главе.



Все еще в шоке, Phoenix и водитель познакомились и обменялись номерами телефонов. Phoenix объяснил водителю, что он работает на технической должности в телефонной службе 0055, а потом сказал:

– Вы не узнаете меня? Я Phoenix. Этот большой процесс по компьютерному хакингу – это мое дело.

Водитель непонимающе посмотрел на него.

– Может быть, вы видели меня в новостях по телику? – спросил Phoenix.

Водитель сказал, что не видел, слегка изумленный странными мыслями молодого человека, который только что едва не погиб.

Через некоторое время после столкновения со смертью бывший хакер ушел со своей технической должности в справочной службе и начал работать в отделе информационных технологий большой мельбурнской корпорации. Он очень хорошо зарабатывал и снова приобрел статус золотого мальчика. Он принимал участие в написании программы, значительно сократившей расходы одного из производств и тем самым сэкономил компании тысячи долларов. Сейчас он постоянно путешествует, бывает в Японии и других местах.

Некоторое время у него была постоянная девушка, но в конце концов она бросила его и начала встречаться с другим. У Phoenix'a было разбито сердце, и он ни с кем не встречался в течение нескольких месяцев. Он старался заполнить образовавшуюся пустоту с помощью постоянно растущих профессиональных обязанностей.

Его новым хобби стала музыка. Он играет на гитаре в любительской группе.

## **Electron**

Через несколько недель после вынесения приговора с Electron'ом произошел новый психический срыв, спровоцированный дозой «спида». Он снова попал в больницу, на этот раз в Ларундел. Он пробыл там недолго и после выхода из клиники продолжил курс лечения.

Через несколько месяцев он снова стал употреблять «спид» и снова заработал нервный срыв. Он постоянно читал в Интернете медицинские сведения о своей болезни, и его психиатры стали беспокоиться о том, что его осведомленность может затруднить лечение.

Electron переехал в специальный приют, предназначенный для тех, кто проходит курс реабилитации после умственных расстройств. Он шаг за шагом боролся со своей болезнью. Когда кто-то приходил его проведать и говорил что-нибудь вроде: «Сегодня прекрасный день», Electron заставлял себя принимать их слова такими, каковы они есть, то есть как обычное замечание о погоде, и не искать в них скрытого смысла. В это время он бросил наркотики, алкоголь и ненавистный бухгалтерский факультет. В конце концов ему удалось полностью отказаться и от приема специальных медикаментов. Он не употребляет наркотики и алкоголь с декабря 1994 года. Единственной физической зависимостью Electron'a в 1996 году были сигареты. Но к началу 1997 года он бросил курить.

С 1992 года Electron ни разу не разговаривал ни с Phoenix'ом, ни с Nom'ом.

В начале 1996 года Electron переехал в собственную квартиру со своей девушкой, которая занималась танцами и тоже после долгой тяжелой борьбы успешно справилась с душевной болезнью. Electron начал учиться на факультете философских наук. На этот раз университетская жизнь его полностью устраивает, и результаты первого же семестра показали отличные оценки по каждому предмету. Он подумывает о том, чтобы переехать в Сидней, чтобы продолжать учебу.

Electron отбыл свои триста часов общественных работ. Он красил стены и делал простую подручную работу в местной школе. Среди прочего школьное начальство попросило его закончить возведение ограды вокруг школы. Он размечал и копал, измерял и укреплял. Когда же Electron, наконец, выполнил назначенное судом количество часов, он обнаружил, что гордится своей работой. Даже сейчас он иногда проезжает мимо школы и смотрит на ограду.

Она по-прежнему стоит.

:)

В судах Австралии продолжают разбирать хакерские дела. Примерно в то же время, когда в Виктории слушалось дело Mendax'a, в окружном суде Брисбена The Crawler признал свою вину по 23 уголовным и 13 административным правонарушениям – все обвинения были связаны с хакингом. 20 декабря 1996 года двадцатидвухлетний Queenslander был условно приговорен к трем годам лишения свободы и к возмещению ущерба различным организациям в размере \$5000. Кроме того, ему было

приказано уничтожить его модем и два компьютера. Первые поколения хакеров пришли и ушли, но хакинг далек от поражения. Он просто стал менее заметным.

Правительственные силовые агентства и судебные власти нескольких стран попытались донести послание до следующего поколения тех, кто мечтал стать хакером. Послание заключалось в следующем: «Не занимайтесь хакингом».

Но новое поколение элиты хакеров и фрикеров восприняло это послание в совершенно ином смысле: «Не попадайтесь».

Принцип устрашения не сработал с хакерами такого уровня. Я не имею в виду детские игры: подростковые шалости, кардинг, сосунков, которые висят в чатах. Я говорю об элите хакинга. Если угодно, карательные меры не просто заставили их уйти еще глубже в подполье – закон подтолкнул хакеров к тому, чтобы стать более изощренными, чем когда-либо, в том, что касается самозащиты. Преследования породили изобретательность.

И если сегодня полицейские врываются через парадную дверь в дом хакера, им приходится быть более подготовленными, чем их предшественникам. Они встречают на своем пути гораздо больше препятствий. Современные серьезные хакеры зашифровывают всю важную информацию. Данные на жестких дисках, данные о своих соединениях, даже голосовые сообщения.

Но если взломщики продолжают взламывать, кто же выступает в качестве мишени?

Их великое множество. Любой тип поставщика сетевых услуг – X.25, сотовая связь или крупный провайдер. Продавцы компьютеров, производители программного обеспечения и электронного оборудования, маршрутизаторов, шлюзов, систем защиты или телефонных коммутаторов. Военные и правительственные учреждения и банки, кажется, немного вышли из моды, но все же такие сайты по-прежнему страдают от многочисленных атак.

Нападения на экспертов по компьютерной безопасности тоже довольно обычное дело, но новой фишкой стал взлом систем других хакеров. Это становится все более популярным. Один из австралийских хакеров пошутил: «А что сможет сделать хакер против хакера? Вызвать федералов? Он ведь не скажет полиции: „Да, офицер, совершенно верно, какой-то компьютерный преступник взломал мою машину и украл 20 000 паролей и результаты всех моих исследований по раскодированию защитных систем“».

По большей части элитные хакеры работают в одиночку, хорошо зная, чем они рискуют в случае поимки. До сих пор существует несколько подпольных хакерских обществ, состоящих из серьезных хакеров, вроде небезызвестного UPT в Канаде и небольшого количества мелких групп, таких как IOpht в США, но все эти объединения довольно разрознены и разобщены, в отличие от прежних времен.

Эти хакеры достигли нового уровня изощренности не только в техническом отношении, но и в отношении стратегии и целей своих атак. Некогда топ-хакеры типа Electron'a и Phoenix'a были счастливы получить копию Zardoz, которая содержала список слабых мест в системах безопасности, найденных компьютерными экспертами. Сейчас серьезные хакеры сами находят такие места, строчку за строчкой читая исходный код, добытый в DEC, HP, CISCO, Sun и Microsoft.

Промышленный шпионаж явно не лежит в сфере их интересов, по крайней мере тех из них, с кем я разговаривала. Все же я знакома с одним хакером, который передал исходную программу владельца его конкуренту. Я также знаю одного хакера, который обнаружил в компьютере конкурента исходную программу одной компании. Была ли эта копия программы получена легальным путем? Кто знает? Хакер так не думал, но по вполне понятным причинам держал язык на привязи.

В большинстве случаев эти хакеры держат найденные ими ошибки в тайне, чтобы провайдеры не смогли принять контрмеры.

Вторым по популярности объектом охоты стали машины по созданию исходных программ. Топ-хакеры ясно представляют себе цель вторжения в такие машины – оставить для себя backdoor, [\[p170\]](#) прежде чем продукт появится на рынке. Слово backdoor используется в андеграунде и как существительное, и как глагол. Хакеры очень осторожно обсуждают этот вопрос, отчасти потому, что им вовсе не хочется, чтобы люди потеряли работу в результате утечки информации.

В каких программах хакеры стремятся установить backdoor? Известные мне мишени: по крайней мере один распространенный интернет-браузер, модные игры, пакет интернет-фильтров и базу

данных правительственных силовых агентств.

Правильный backdoor – это очень мощное средство для создания тайного хода сквозь самую крепкую стену прямо в сердце сети, неприступной в других отношениях. В сетевом браузере backdoor позволяет хакеру получить прямой доступ в любой ПК в тот момент, когда его хозяин или хозяйка путешествует по World Wide Web. Но не надо думать, что хакеры только и мечтают о том, как бы проникнуть в ваш тихий дом в пригороде. Большинству серьезных хакеров совершенно наплевать на персональный компьютер обычного человека.

Но вам может быть интересно, кто стоит за атаками на домашние компьютеры? Что за люди этим занимаются? На эти вопросы нет простых ответов. Среди хакеров встречаются разные люди, как и в любом человеческом сообществе. Новое поколение хакерской элиты представляет собой разношерстную компанию, и рассказ о них мог бы потребовать еще одной книги. Но я хочу познакомить вас с одним из них, чтобы позволить вам заглянуть в будущее.

:)

Позвольте представить вам SKiMo.

Он белый, живет за пределами Австралии и занимается хакингом по меньшей мере четыре года, хотя вошел в ряды мировой хакерской элиты в 1995 или в 1996 году. Он ни разу не был арестован. Это молодой человек – ему от 18 до 25 лет. Из далеко не самой благополучной семьи. Отлично говорит по-английски, хотя это не родной его язык. В политике придерживается левацких взглядов – больше симпатизирует зеленым и анархистам, нежели традиционным рабочим партиям. Покурирует марихуану и иногда выпивает, но не притрагивается к тяжелым наркотикам.

Среди его музыкальных вкусов ранний Pink Floyd, Sullen, Dog Eat Dog, Biohazard, старый Ice-T, Therapy, Alanis Morissette, Rage Against the Mashine, Fear Factory, Life of Agony и Napalm Death. Он читает Стивена Кинга, Стивена Хокинга, Тома Клэнси и Олдоса Хаксли. И любые интересные книги по физике, химии и математике.

Он довольно застенчив, не любит командные виды спорта и не слишком уверенно общается с девушками. У него была только одна постоянная подруга, но их отношения закончились. Теперь, когда он занимается хакингом или программированием в среднем четыре-пять часов в день (иногда он проводит за компьютером до 36 часов без перерыва), у него нет времени на девушек.

– Кроме того, – говорит он, – я становлюсь привередой, когда речь идет о девушках. Конечно, если бы она разделяла мои интересы... но таких трудно найти. Девушки сильно отличаются от хакинга. Ты не сможешь применить к ним силу, когда все остальное уже не помогает, – поясняет он.

SKiMo никогда не наносил намеренного вреда компьютерным системам и даже не помышлял об этом. Когда я спросила его об этом, он едва ли не оскорбился. Однако случилось и так, что он стал причиной определенного ущерба. Я знаю об одном случае, когда он вернулся в систему и сам устранил созданную им проблему.

Ему было ужасно скучно на большинстве уроков в школе, и в классе он занимался в основном тем, что читал книги – совершенно открыто. Он хотел, чтобы учитель понял его отношение, не вступая с ним в конфронтацию.

Он заинтересовался хакингом после того, как прочитал статью в журнале о людях, которые взламывали автоответчики и VMB. В то время у него не было ни малейшего представления о том, что такое VMB, но он быстро учился. Однажды вечером в воскресенье он сел на телефон и начал сканировать. Вскоре он занялся фрикингом и стал посещать англоязычные телефонные конференции. В определенной степени ему было гораздо проще общаться по-английски, разговаривать с теми, для кого английский родной язык, возможно потому, что он всегда чувствовал себя белой вороной в своей собственной культуре.

– Я всегда думал о том, чтобы уехать из моей страны при первой же возможности, – говорит он.

Чтобы перейти от фрикинга к хакингу, нужно было сделать лишь один шаг.

Что в первую очередь заставляет его делать то или иное? Может быть, это желание внедриться в ненавистную всему миру телефонную компанию или «страстная жажда власти», или он просто последовал своему стремлению «исследовать области новых сложнейших технологий». Но на сегодняшний день он несколько более определенно отвечает на вопрос, почему он занимается хакингом. Он говорит: «Моя единственная и главная мотивация – учиться».

Когда я спросила у него, почему он не поступит в местный университет или не запишется в библиотеку, чтобы удовлетворить это желание, он ответил: «Из книг можно узнать только теорию. Я не против теории, но в реальной жизни компьютерная безопасность имеет очень мало общего с тео-

рией». SKiMo также сказал, что библиотеки с трудом поспевают за темпом технологического прогресса. Он добавил:

– Возможно, я просто получаю удовлетворение от того, что знаю – я учусь прямо на месте. Это «внутреннее знание».

Он сказал, что есть доля правды в том, что ему нравится учиться в обстановке, способствующей выбросу адреналина.

Есть ли у него зависимость от компьютеров? SKiMo говорит, что нет, но все признаки зависимости налицо. По его собственной оценке в общей сложности он взломал от трех до десяти тысяч компьютеров. Его родители не имели никакого представления, чем именно занимается их сын, дня и ночи у своего компьютера, но тревожились из-за его поведения. Они отключали машину много раз. По собственным словам SKiMo, «они попробовали все, чтобы удержать меня от этого».

Неудивительно, что они потерпели поражение. SKiMo стал мастером по перепрыгиванию компьютерного оборудования, так что они не могли пробраться в комнату и унести его. В конце концов, когда он устал с ними бороться и стал достаточно взрослым, он ушел из дома. «Короче, я сказал им: „Это, блин, моя гребаная жизнь и вас это не колышет, ясно?“ Только слова были немного другими».

SKiMo говорит, что он никогда не страдал от умственных расстройств или душевной неустойчивости – кроме, может быть, паранойи. Но, по его словам, в его случае паранойя вполне оправдана. В 1996 году ему дважды казалось, что за ним следят, и он в течение некоторого времени не мог избавиться от слежки, как ни старался. Оба эти инцидента не были связаны между собой. Возможно, это были просто совпадения, но он не мог быть уверенным до конца.

Он рассказал мне об одной хакерской вылазке, чтобы проиллюстрировать свои нынешние интересы. Ему удалось проникнуть во внутреннюю сеть немецкого оператора мобильной связи DeTeMobil (Deutsche Telecom). Бывшее государственное предприятие, преобразованное в акционерное общество в январе 1995 года, Deutsche Telecom является крупнейшей телекоммуникационной компанией в Европе и третьим по величине сетевым оператором в мире. В этой корпорации работает почти четверть миллиона человек. Это одна из пяти крупнейших немецких компаний. Ее общая прибыль за 1995 год достигла 37 миллиардов австралийских долларов.

После тщательного обследования и прощупывания сайта SKiMo обнаружил, как можно заполучить ключи к шифрам, генерированным для разговоров по мобильной связи DeTeMobil.

Он пояснил:

«Эти ключи непостоянны, то есть они не генерируются раз и навсегда, чтобы потом храниться в какой-нибудь базе данных. В большинстве случаев ключ создается в AUC [центре идентификации] компании для каждого телефонного разговора с использованием „Ki“ и произвольной величины, генерированной AUC. Ki – это секретный ключ, который хранится на смарт-карте внутри телефона. Его копия также имеется в AUC. Когда AUC „сообщает“ сотовому телефону ключ для именно этого отдельно взятого разговора, информация проходит через мобильный коммутационный центр (MSC) компании.

Вполне возможно прослушивать сотовый, если кто-то ведет активный перехват технических сигналов или отслеживает определенные соединения из центра операций и поддержки (ОМЦ), либо если кто-то знает Ki смарт-карты.

Оба варианта абсолютно реальны. Первый из них связан со знанием ключа шифрования A5 и требует специального оборудования. Второй вариант, использующий Ki, требует также знания алгоритмов A3/A8, иначе Ki бесполезен. Эти алгоритмы можно получить, побывав в гостях у производителей коммутаторов, то есть Siemens, Alcatel, Motorola...

Когда с намеченного телефона происходит звонок, тебе нужно ввести ключ A5 в сотовый телефон, измененный таким образом, чтобы он мог прослушивать канал, используемый сотовым телефоном. Как правило, такое прослушивание дает доступ к помехам, поскольку разговор зашифрован. Но при наличии ключа и оборудования ты можешь расшифровать разговор».

Вот одно из перехваченных сообщений с расшифровкой по стандарту CCITT7:

```
13:54:46'3 4Rx&lt; SCCP 18-8-09-1 18-8-04-0 13 CR BSSM HOREQ BSSMAP GSM 08.08 Rev
3.9.2 (BSSM) HaNDover REQuest (HOREQ)
– D Discrimination bit D BSSMAP
00000000– Filler
```

```
00101011 Message Length 43
00010000 Message Type 0x10
Channel Type
00001011 IE Name Channel type
00000011 IE Length 3
00000001 Speech/Data Indicator Speech
0000100 °Channel Rate/Type Full rate TCH channel Bm 00000001 Speech Encoding Algorithm GSM
speech algorithm Ver 1
Encryption Information
00001010 IE Name Encryption Information
00001001 IE Length 9
00000010 Algorithm ID GSM user data encryption V. 1
***** Encryption Key C9 7F 45 7E 29 8E 08 00
Classmark Information Type 2
00010010 IE Name Classmark Information type 2
00000010 IE Length 2
– 001 RF power capability Class 2, portable
– 00– Encryption algorithm Algorithm A5
000–Revision level
– 000 Frequency capability Band number 0
– 1– SM capability present
– 000– Spare
0– Extension
Cell Identifier
00000101 IE Name Cell Identifier
00000101 IE Length 5
00000001 Cell ID discriminator LAC/CI used to Ident cell
***** LAC 4611
***** CI 3000
PRIority
00000110 IE Name Priority
00000001 IE Length 1
– 0 Preemption allowed ind not allowed
– 0– Queueing allowed md not allowed
– 0011– Priority level 3
00–Spare
Circuit Identity Code
00000001 IE Name Circuit Identity code
00000000 PCM Multiplex a-h 0
– 11110 Timeslot in use 30
101-PCM Multiplex 1-k 5
Downlink DTX flag
00011001 IE Name Downlink DTX flag
– 1 DTX In downlink direction disabled
0000000– Spare
Cell Identifier
00000101 IE Name Cell Identifier
00000101 IE Length 5
00000001 Cell ID discriminator LAC/CI used to Ident cell
***** LAC 4868
***** CI 3200
```

Прелесть цифрового мобильного телефона в отличие от аналоговых мобильных телефонов, которые все еще используются некоторыми в Австралии, состоит в том, что разговоры по нему практически невозможно прослушать. Если я звоню вам со своего цифрового телефона, наш разговор будет зашифрован алгоритмом A5 между мобильным телефоном и коммутатором. Поставщик связи имеет копию K<sub>i</sub>, и в некоторых странах правительство может получить доступ к этим копиям. Тем не менее K<sub>i</sub> принадлежат к числу тщательно охраняемых секретов.

SKiMo получил доступ к базе данных зашифрованных Ki и к некоторым незашифрованным Ki. Но он не стал взваливать на себя обузу, собирая информацию об алгоритмах A3 и A8, чтобы расшифровать полную базу данных, хотя это можно было сделать довольно легко. Надо сказать, что сейчас у него есть эта информация.

Для SKiMo доступ к генерированным ключам к тысячам немецких телефонов был проявлением чистого любопытства – и трофеем. У него не было дорогостоящего оборудования для прослушивания. Зато эта информация могла представлять большой интерес для какой-нибудь разведки, особенно если речь шла о возможности прослушивания телефонов известных политиков. Еще более ценным мог оказаться постоянный доступ к OMC, а еще лучше к MSC. Но SKiMo сказал, что он никогда бы не предоставил такой информации разведке.

Находясь внутри DeTeMobil, SKiMo также научился интерпретировать некоторые данные картографии и силы сигнала. Ради чего? Если у кого-то из клиентов компании был включен телефон, SKiMo, по его словам, мог определить его географическое положение с точностью до одного километра. Клиенту даже не надо было разговаривать по мобильному. Главное, чтобы телефон был включен в режиме приема звонков.

Однажды SKiMo проследил за одним из таких клиентов, который путешествовал по Германии, а затем позвонил ему. Так вышло, что они говорили на одном европейском языке.

– Почему вы едете из Гамбурга в Бремен с включенным телефоном? – спросил SKiMo.

Бедняга просто обалдел. Как мог этот незнакомец на другом конце линии знать, куда он едет?

SKiMo сказал, что он из Greenpeace. «Не надо ездить так много. Это загрязняет атмосферу», – сказал он потрясенному хозяину мобильного. Затем он сообщил ему о том, как важно экономить энергоресурсы, и о том, что продолжительное использование мобильных телефонов отрицательно влияет на некоторые доли мозга.

Изначально SKiMo взломал сеть оператора мобильной связи, чтобы «стать полностью сотовым», – он надеялся, что такой переход сделает его одновременно более мобильным и более неудобным для слежки. Возможность прослушивать разговоры других людей – в том числе полиции – могла стать неплохим бонусом.

Но в осуществлении этого проекта он обнаружил, что код производителя мобильных телефонов, который он хотел изучить, оказался «мультиязычным проектом». SKiMo сказал: «Я не знаю, видели ли вы когда-нибудь мультиязычный проект, где не существует общего языка, который могли бы использовать все программисты для составления комментариев и названий функций? Это выглядит ужасно. Читать эту чушь – то еще веселье». Часть монолога прозвучала по-фински.

SKiMo говорит, что он взломал множество больших провайдеров и в нескольких случаях получил доступ к исходным кодам их продукта.

Мог ли он получить возможность установки backdoor в исходных кодах больших провайдеров? Да. Делал это? Он говорит, что нет. С другой стороны, когда я спросила у него, сказал бы он кому-либо, если бы сделал это, он ответил: «Ни за что, потому что степень риска сильно возрастает, когда секрет знают двое».

SKiMo все еще остается одиночкой. Он делится ограниченным количеством информации с парой человек, но разговоры о его хакерских подвигах обычно тщательно законспирированы и туманны. Он заменяет названия провайдеров либо обсуждает технические вопросы компьютерной безопасности в такой глубоко теоретической манере, что ему нет необходимости называть ту или иную компьютерную систему.

Он никогда не говорит о хакинге по телефону. В большинстве случаев, когда ему удастся заполучить особо ценный приз, он сообщает эту новость только себе.

Но так было не всегда. «Когда я только начал заниматься хакингом и фрикингом, мне нужно было очень многому научиться и завязать контакты, чтобы я мог спрашивать о некоторых вещах – типа технических советов, – сказал SKiMo. – Сейчас мне кажется, что гораздо проще получить такую информацию самому, чем просить ее у кого-то. Я проверяю исходный код, затем экспериментирую и отыскиваю новые ошибки самостоятельно».

Я спросила, не может ли все возрастающая сложность компьютерных технологий вынудить хакеров объединяться в группы специалистов. Он ответил, что в некоторых случаях это возможно, но в большинстве случаев – нет. «Это подходит лишь тем, кто не хочет научиться всему».

В обозримом будущем SKiMo не собирается бросать хакинг.

А кто сегодня на другой стороне?

В Австралии это все та же федеральная полиция, хотя эта служба прошла долгий путь от ранних дней отдела по борьбе с компьютерными преступлениями. Когда сотрудники АФП врывались к Phoenix'у, Nom'у и Electron'у, они были похожи на типичных копов из полицейских комедий. Полицейские не имели ничего общего с хакерами, которые настолько опережали их в техническом развитии, что это было просто смехотворно.

АФП закрыла эту брешь с достойным уважением рвением. Под руководством таких офицеров, как Кен Дэй, была создана группа из технически образованных сотрудников. В 1995–1996 годах в АФП работало около 2800 служащих, хотя примерно 800 из них исполняло функции местной полиции в таких местах, как остров Норфолк. Годовой бюджет АФП составил около \$270 миллионов.

Недавно АФП прошла через серьезную реорганизацию, направленную на отход от командно-приказной структуры и переориентацию на более современные, более оперативные способы работы.

Некоторые из этих изменений не более чем косметические. Офицеров АФП больше не называют «констебль» или «сержант» – теперь все они просто «федеральные агенты». Стратегией АФП стало «сразиться и победить».<sup>52</sup> Ее организационная схема, состоявшая из традиционной иерархической пирамиды квадратов, была преобразована в скопление небольших кружков, связанных с более крупными кругами. Больше никаких фаллоцентрических конструкций. Можно сказать, что над структурой АФП поработали политкорректные консультанты по менеджменту.

Тем не менее, АФП претерпела и более существенные изменения. Теперь в ней существуют «команды» различных экспертов, и следователи могут обращаться к ним по мере необходимости. В отношении роста эффективности эта мобильность пошла им на пользу.

В мельбурнском отделе компьютерных преступлений АФП постоянно служит человек пять. Хотя АФП и не публикует детальных отчетов о своем бюджете, при внимательном изучении вопроса можно сделать вывод, что она тратит около \$1 миллиона в год на расследование компьютерных преступлений только в Мельбурне и его окрестностях. В Сиднее также имеется отдел по борьбе с компьютерными преступлениями.

Преследование хакеров и фрикеров – это только часть работы отдела. Другой его важной задачей является предоставление компьютерной технической помощи при других расследованиях.

Дэй все еще правит бал в Мельбурне. Он работает и думает не так, как обычный патрульный. Он игрок-психолог и, следовательно, отлично понимает своих противников. По сведениям надежного источника вне андеграунда, он честный коп, компетентный работник и просто «отличный парень».

Но тот факт, что Дэй столько лет возглавляет этот отдел, сделал его излюбленной мишенью в подполье. В особенности хакеров очень веселит его крайне серьезное отношение к себе самому и к своему делу. Однажды Дэй принял участие в ныне уже несуществующем шоу «Точка зрения» на канале ABC. «Это не игра. Это преступное деяние», – сурово предостерег он аудиторию от хакинга.

Но у хакеров, посмотревших передачу, было свое мнение. Вскоре после ее выхода в эфир несколько членов Neuro-cactus, хакерско-фрикерской группы из Западной Австралии, решили сбить с него спесь и посмеяться. Двое из Neuro-cactus, Pick и Minnow сделали из фразы Дэя, уже успевшей стать знаменитой, ролик. И вот уже Дэй под музыкальную тему из The Bill заявляет: «Это не преступное деяние. Это игра». Neuro-cactus быстро распространили свой пасквиль по всему андеграунду через нелегальную VMB, подключенную к их собственному бесплатному номеру 008.

Хотя, возможно, Дэй и перебарщивает, воспринимая себя слишком серьезно, ему, должно быть, не очень весело сталкиваться с такими выходками из недели в неделю. Многие хакеры говорили мне с восторгом: «Я знаю одного парня, который работает над тем, чтобы получить номер домашнего телефона Дэя». Скорее всего, кое у кого в подполье такая информация есть и они уже использовали ее. Некоторые считают, что это жутко прикольно – позвонить Дэю домой и разыграть его. Если честно, мне немного жаль прикольщика. Можно держать пари, что парни из оперативного отдела не станут мириться с этим.

Но это не означает, что, по моему мнению, эти шутники должны быть наказаны.

;) )

Что общество может предложить хакерам, кроме изоляции?

<sup>52</sup> Australian Federal Police, *Annual Report, 1995–1996*, p. 7.

Нужно ли вообще с ними что-то делать?

Может быть, стоит просто не обращать внимания на ознакомительный хакинг? Общество должно принять осмысленное решение и использовать ценные полицейские кадры для поимки опасных преступников – фальшивомонетчиков, растратчиков, чиновников-коррупционеров и злонамеренных хакеров – и оставить в покое любопытствующих хакеров.

Закон должен наказывать тех, кто вступил на путь, который общество считает для себя опасным. Любое серьезное преступление, совершенное хакером, должно рассматриваться в рамках обычного законодательства, и приговор должен быть вынесен в соответствии с законом, общим для всех. Мошенничество, преднамеренный ущерб и кража личного имущества являются преступлениями вне зависимости от того, кто их совершил, и должны быть наказаны соответственно.

Есть ли смысл в том, чтобы считать преступниками любопытствующих хакеров, – я имею в виду тех, кто не причинял злонамеренного ущерба и не совершал мошенничеств. Наверное, нет. Они, в первую очередь, просто нарушители общественного порядка и должны понести наказание именно за это. И это не так уж сложно. Законодателям нужно только признать ознакомительный хакинг не таким серьезным нарушением закона. В худшем случае закоренелому нарушителю должен грозить небольшой срок общественных работ. Но эти работы нужно организовать соответственно. В одном из случаев, имевших место в Австралии, офицер по надзору заставил хакера выполнять общественные работы вместе с насильником и убийцей.

У многих хакеров никогда не было работы – отчасти по причине высокой безработицы среди молодежи в некоторых районах, – поэтому труд на пользу общества может оказаться их первым «опытом». Правильно организованные общественные работы могут дать хакеру возможность использовать свои компьютерные навыки, чтобы заплатить долг обществу, по возможности, в виде реализации какого-нибудь самостоятельного творческого проекта. При должном управлении хакерский энтузиазм, любопытство и готовность к эксперименту могут быть направлены в позитивное русло.

В тех случаях, когда речь идет о зависимости от хакинга и фрикинга, проблему нужно решать медицинским, а не уголовным путем. Еще важнее тот факт, что хакеры, учитывая их возраст, прежде не совершали ничего противозаконного. Как сказал Пол Голбалли на суде по делу Mendax'a: «Все обвиняемые очень умны, но их умственное развитие существенно опередило развитие половое». Есть все шансы на то, что большинство сможет справиться с этой зависимостью или просто перерасти ее.

На проверку большинство австралийских судей вынесли вполне справедливые приговоры, особенно если сравнивать их с судьями других стран. Ни один из австралийских хакеров, описанных в этой книге, не был приговорен к тюремному заключению. Отчасти это произошло благодаря счастливому стечению обстоятельств, но также благодаря продуманным приговорам, вынесенным такими людьми, как судья Льюис и судья Кимм. Каждый день проводя в судебском кресле, очень трудно удержаться от соблазна рубить сплеча, интерпретируя новые законы.

Поскольку я была в суде и слышала обоих судей, мне сразу стало ясно, что они выполнили домашнее задание. В присутствии психолога Тима Уотсона-Мунро на свидетельском месте судья Льюис мгновенно определился с понятием «свободы выбора» – в связи с зависимостью – в деле Prime Suspect'a. В случае Tгах'a судья Кимм задавал четко сформулированные вопросы – это стало возможным лишь после серьезного изучения пространных материалов дела.

В основе их компетентных суждений лежало глубокое понимание хакинга как преступления, а также целей пока еще не опробованного в полной мере компьютерного законодательства.

И все же большое количество времени и денег было потрачено на преследование любопытствующих хакеров главным образом потому, что этот вид хакинга считался серьезным преступлением. Вот вам пример абсурдной ситуации, которая могла бы возникнуть по вине австралийского федерального закона о компьютерных преступлениях.

Некий шпион проник в компьютер штаб-квартиры Либеральной партии и прочитал совершенно секретную информацию о партийной избирательной стратегии, которую можно передать Лейбористской партии. Он не вводил и не уничтожал никаких данных и не получал доступа к какой бы то ни было коммерческой информации. Какое наказание он мог получить по новому законодательству? Максимум – шесть месяцев тюрьмы.

Этот же шпион решает быстро разбогатеть. При помощи местной телефонной системы он взламывает банковский компьютер с намерением ограбить финансовое учреждение. Он не имеет доступа к информации коммерческого или личного характера, он не уничтожает и не вводит файлов.

Но информация, которую он получит: планировка здания банка, схема отключения пожарной сигнализации и противопожарной системы, – сможет помочь ему в составлении плана ограбления



банка. Наказание? Самое большее – два года тюрьмы.

Дальше – больше. Он проникает в компьютер Министерства обороны, чтобы получить доступ к информации об оборонных секретах Австралии, а затем продать ее малайцам. Он по-прежнему ничего не стирает и не вводит – он просто читает каждый важный документ, который ему попадается. По федеральному антихакерскому закону, в этом случае максимальное наказание также составит два года тюрьмы.

В это время безобидный любопытствующий хакер взламывает университетский компьютер, не причиняя ему никакого вреда. Он не стирает файлов. Он скачивает общедоступный файл из другой системы и потихоньку прячет его в укромном, малопосещаемом уголке университетской машины. Может быть, он отправит онлайн-сообщение своему приятелю. В случае поимки закон в интерпретации АФП и Генеральной прокуратуры скажет, что ему грозит до десяти лет тюрьмы.

Причина? Он ввел или уничтожил данные.

Хотя хакер-шпион может быть обвинен и по другим статьям – таким как государственная измена, – это упражнение иллюстрирует определенные проблемы в современном компьютерном законодательстве.

Если следовать букве закона, наш любопытствующий хакер может получить тюремный срок в пять раз больше, чем грабитель банка или военный шпион, и в двадцать раз больше, чем злоумышленник против Либеральной партии. Закон в интерпретации АФП гласит, что такой любопытствующий хакер заслуживает тех же десяти лет лишения свободы, что и продажный судья. Представьте себе странную картину: коррумпированный судья и любопытствующий хакер в одной камере.

Хотя законодатели могли не иметь достаточного полного представления о технологических аспектах хакинга в момент ратификации закона о компьютерных преступлениях, их намерения вполне очевидны. Они пытались провести различие между злонамеренным и безобидным хакером, но им следовало сделать это более определенно.

В своем нынешнем виде закон уравнивает злонамеренный и ознакомительный хакинг, говоря о том, что любое лицо, которое разрушает, стирает, изменяет или вводит данные, заслуживает тюремного заключения вне зависимости от намерений вышеуказанного лица. Закон не делает разницы между незначительным уничтожением данных и «отягчающим уничтожением», максимальное наказание в обоих случаях – десять лет тюрьмы. АФП извлекла своеобразную выгоду из отсутствия такой разницы и в результате любопытствующие хакеры снова и снова обвиняются в самых серьезных компьютерных преступлениях.

Парламент принимает законы. Правительственные институты, такие как АФП, Генеральная прокуратура и суды, интерпретируют и применяют эти законы. АФП и в некоторой степени Генеральная прокуратура в точности применили букву закона в большинстве хакерских дел, описанных в этой книге. Тем не менее они упустили из виду намерения законодателей. Стоило немного изменить закон, и они бы действовали по-другому. Стоит начать относиться к ознакомительному хакингу как к мелкому правонарушению, и правительственные агентства перестанут преследовать легкую добычу и наверняка обратят более пристальное внимание на настоящих преступников.

Я была близко знакома с некоторыми из этих хакеров, изучала их на протяжении двух лет и надеюсь, что смогла понять, чем они дышат. Во многих отношениях они типичные австралийцы с их вечным недоверием к властям и бунтом против «истеблишмента». Они умны – иногда чрезвычайно умны. Некоторых из них даже можно считать техническими гениями. Они задиристы и очень предприимчивы. Это бунтари, хулиганы и мечтатели.

Самое главное, они умеют мыслить и мыслить широко и нестандартно.

Это не порок. Зачастую это очень ценная черта – та, что движет общество к новым горизонтам. Вопрос не в том, чтобы искоренить эту черту, а в том, как вывести ее на правильную дорогу

## **Глоссарий и сокращения**

AARNET – Australian Academic Research Network (Австралийская академическая исследовательская сеть).

ASIO – Australian Security Intelligence Organisation (Австралийская организация разведки и безопасности).

ACARB – Australian Computer Abuse Research Bureau (Австралийское бюро исследования злоупотреблений с использованием компьютеров, раньше называвшееся CITCARB).

AFP – Australian Federal Police (Австралийская федеральная полиция, АФП).

Altos – чат и хакерская тусовка, соединенная с сетью X.25 и запущенная Altos Computer Systems в Гамбурге.

ANU – Australian National University (Австралийский национальный университет).

Backdoor – Программа или модификация программы, обеспечивающая секретный доступ в компьютерную систему и устанавливаемая хакером в обход обычной системы безопасности.

BBS – Bulletin Board System (система электронных досок объявлений).

BNL – Brookhaven National Laboratory (US) (Брукхейвенская национальная лаборатория США).

BRL – Ballistics Research Laboratory (US) (Баллистическая исследовательская лаборатория США).

BT – British Telecom.

CCITT – Commitee Consultatif Internationale Telegraph et Telephonie (Международный консультативный комитет по телеграфии и телефонии), швейцарская организация по телекоммуникационным стандартам, ныне не существует; см. ITU.

CCS – Computer Crime Squad (Команда по борьбе с компьютерными преступлениями).

CCU – Computer Crime Unit (Отдел компьютерных преступлений Австралийской федеральной полиции).

CERT – Computer Emergency Response Team (Команда быстрого компьютерного реагирования).

CIAC – Computer Incident Advisory Capability (Консультативная служба по компьютерным инцидентам, команда компьютерной безопасности Министерства энергетики США).

CITCARB – Chisholm Institute of Technology Computer Abuse Research Bureau (Исследовательское бюро по злоупотреблениям с использованием компьютеров Чисхольмского технологического института), ныне не существует; см. ACARB.

COBE – Cosmic Background Explorer project (проект «Исследование космического фона»), исследовательский проект NASA.

DARPA – Defense Advanced Research Projects Agency (US; (Агентство передовых исследовательских оборонных проектов США).

DCL – Digital Command Language («цифровой командный язык», язык компьютерного программирования, используемый в компьютерах VMS).

DDN – Defense Data Network (Военная сеть передачи данных).

DEC – Digital Equipment Corporation.

DECNET – сетевой протокол, используемый для переброски информации между машинами VAX/VMS.

DEFCON – а) Defense Readiness Conditions (Обстановка боевой готовности) – система последовательного оповещения о тревоге в армии США; б) название компьютерной программы Forge, которая автоматически картографировала компьютерные сети и сканировала учетные записи.

DES – Data Encryption Standard (Стандарт шифровки данных), алгоритм шифрования, разработанный IBM, NSA и NIST.

Deszip – быстрая программа-взломщик паролей DES Unix, разработанная Мэтью Бишопом.

Dial-up – модемный доступ в компьютер или в компьютерную сеть.

DMS-100 – компьютеризированный телефонный коммутатор, производимый NorTel.

DOD – Department of Defense (US) (Министерство обороны США).

DOE – Department of Energy (US) (Министерство энергетики США).

DPP – Director of Public Prosecutions (генеральный прокурор).

DST – Direction de la Surveillance du Territoire (Управление по охране территории, французская контрразведка).

EASYNET – внутренняя коммуникационная сеть DEC (DEC-NET).

GTN – Global Telecommunications Network (Глобальная телекоммуникационная сеть), международная сеть данных Citibank.

HEPNET – High Energy Physics Network (Международная сеть по физике высоких энергий, сеть на базе DECNET, находится главным образом под контролем DOE, подключена к SPAN NASA).

IID – Internal Investigation Division (Отдел внутренних расследований). Полиция штата Виктория, как и АФП, имела такой отдел.

IP – Internet Protocol (RFC791), протокол передачи данных, используемый для передачи пакетов данных между компьютерами в Интернете.

IS – International Subversive («Международный разрушитель»), хакерский электронный журнал.

ISU – Internal Security Unit (Отдел внутренней безопасности, отдел по борьбе с коррупцией полиции штата Виктория).

ITU – International Telecommunications Union (Международный союз электросвязи), международная организация телекоммуникационных стандартов.

JANET – Joint Academic Network (Объединенная академическая сеть), британская компьютерная сеть.

JPL – Jet Propulsion Laboratory (Лаборатория реактивного движения), исследовательский центр NASA в Калифорнии, связанный с Калифорнийским технологическим институтом.

LLNL – Lawrence Livermore National Laboratory (US) (Национальная лаборатория имени Лоуренса Ливермора в США).

Модем (модулятор-демодулятор) – устройство для передачи компьютерных данных по обычной телефонной линии.

NCA – National Crime Authority (Национальное криминальное управление).

Netlink – команда Primos/Dial com для запуска соединения в сети.

NIST – National Institute of Standards (US) (Национальный институт стандартов США).

LOD – Legion of Doom, хакерская группа.

Lutzifer – «Люцифер», западногерманский компьютер, подсоединенный к сети X.25 и выполняющий функцию чата.

NIC – Network Information Center (US) (Информационный сетевой центр США), запущенный Министерством обороны компьютер, ответственный за присвоение доменных имен в Интернете.

MFC – Multi Frequency Code (Group III) (мультичастотный код, группа III), система обмена данными между телекоммуникационными системами, используемая в Telstra (Telecom).

MILNET – Military Network (Военная сеть), компьютерная сеть обмена данными по протоколу TCP/IP Министерства обороны США.

MOD – Masters of Deception (Destruction), хакерская группа.

NRL – Naval Research Laboratory (US) (Военно-морская исследовательская лаборатория США).

NSA – National Security Agency (US) (Агентство национальной безопасности США).

NUA – Network User Address: (сетевой адрес пользователя) адрес компьютера в сети X.25 аналогичный телефонному номеру.

NUI – Network User Identifier (Identification) (идентификатор [идентификация] пользователя сети), комбинация имени пользователя и пароля в сети X.25, используемая для биллинга.

NorTel – Northern Telecom, канадский производитель телекоммуникационного оборудования.

PABX – Private Automatic Branch Exchange (Частный автоматический вспомогательный коммутатор).

PAD – Packet Assembler Disassembler (пакетный ассемблер-дисассемблер), текстовый шлюз в сеть X.25.

PAR 'PAR? – команда в PAD для отображения параметров PAD.

RMIT – Royal Melbourne Institute of Technology (Королевский технологический институт Мельбурна).

RTG – Radioisotope Thermoelectric Generator (радиоизотопный термоэлектрический генератор), плутониевая энергетическая установка космического аппарата «Галилей».

RTM – Роберт Таппан Моррис-младший, студент Корнельского университета, написавший червя, известного под названием RTM.

SPAN – Space Physics Analysis Network (Международная сеть исследователей физики космоса), глобальная сеть DECNET, первоначально контролировалась NASA.

Sprint – американская телекоммуникационная компания, провайдер сети X.25.

Sprintnet – сеть X.25, контролируемая Sprint communications.

Sun – Sun Microsystems, крупнейший производитель рабочих станций Unix.

TCP – Transmission Control Protocol (RFC793) (протокол контроля передачи), стандарт передачи данных между двумя компьютерами в Интернете.

TELENET – сеть X.25, DNIC 3110.

Telnet – Телнет, способ соединения между двумя компьютерами в Интернете или в других сетях TCP/IP.

Tymnet – сеть X.25, контролируемая MCI, DNIC 3106.

Unix – многопользовательская компьютерная операционная система, разработанная AT&T и университетом Беркли.

VAX – Virtual Address Extension («виртуальное адресное расширение»), серия мини-мэйн-фреймов, производимых фирмой DEC.

VMS – Virtual Memory System («система виртуальной памяти»), операционная система, произ-

водимая фирмой DEC и применяемая в машинах VAX.

WANK (Worms Against Nuclear Killers) («Черви против ядерных убийц»), название червя на базе DECNET/VMS, запущенного в SPAN/DEC/HEPNET в 1989 году.

X.25 – международная сеть передачи данных, использующая коммуникационные протоколы

X.25. Сеть создана крупными телекоммуникационными компаниями на базе стандарта CCITT # X.25.

Zardoz – ограниченный лист почтовой рассылки материалов по компьютерной безопасности.

## Библиография

Australian Federal Police (AFP), *Annual Report 1995–1996*, Canberra, 1996.

–, *Annual Report 1994–1995*, Canberra, 1995.

–, *Annual Report 1993–1994*, Canberra, 1994.

Bourne, Philip E., «Internet security; System Security», *DEC Professional*, vol. 11, June 1992.

Cerf, Vinton G., «Networks», *Scientific American*, vol. 265, september 1991.

Clyde, Robert A., «DECnet Security», *DEC Professional*, vol. 10, april 1991.

Commonwealth Attorney-General's Department, *Interim Report on Computer Crime* (the gibbs Report), Canberra, 1988.

Commonwealth Director of Public Prosecution (DPP), *Annual Report 1993–1994*, Canberra, 1994.

Commonwealth Scientific and Industrial Research Organisation (CSIRO), *Annual Report 1994–1995*, Canberra, 1995.

Davis, Andrew W., «DEC Pathworks the mainstay in Macto-VAX connectivity», *Mac Week*, vol. 6, 3 August 1992.

Department of Foreign Affairs and Trade, *Australian Treaty Series 1993*, no. 40, Australian Government Publishing Service, Canberra, 1993.

Digital Equipment Corporation, *Annual Report 1989*, securities and Exchange Commission (SEC) Online (USA) Inc., 1989.

–, *Quarterly Report* for period ending 12.31.89, sec Online (USA).

Gezelter, Robert, «The DECnet TASK object; Tutorial», *Digital Systems Journal*, vol. 16, july 1994.

Gianatasio, David, «Worm Infestation hits 300 VAX/VMS systems worldwide via DECnet», *Digital Review*, vol. 6, 20 november 1989.

Haffner, Katie & Markoff John, *Cyberpunk*, Corgi Books (transworld), Moorebank NSW, 1994.

Halbert, Debora, «The Potential for Modern Communication Technology to Challenge Legal Discourses of Authorship and Property», *Murdoch University E-Law Journal*, vol. 1, no. 2.

Kelman, Alistair, «Computer Crime in the 1990s: a Barrister's View», Paper for the Twelfth National Symposium on Economic Crime, September 1994.

Law Commission (UK) Working Paper, no. 110, 1988.

Lloyd, J. Ian & Simpson, Moira, *Law on the Electronic Frontier*, David Hume Institute, Edinburgh, 1996.

Longstaff, Thomas A., & Schultz, E. Eugene, «Beyond preliminary analysis of the WANK and OILZ worms: a case study of malicious code». *Computers & Security*, vol. 12, february 1993.

Loundy, David J., «Information Systems Law and Operator Liability Revisited», *Murdoch University E-Law Journal*, vol. 1, no. 3, september 1994. mcmahon, john, «Practical DECnet Security», *Digital Systems Journal*, vol. 14, November 1992.

Melford, Robert J., «Network security; computer networks», *Internal Auditor*, institute of Internal Auditors, vol. 50, February 1993.

Natalie, D. & Ball, W, EIS Coordinator, North Carolina Emergency Management, «How North Carolina Managed Hurricane Hugo», *EIS News*, vol. 3, no. 11, 1988.

NorTel Australia Pty Ltd, *Discovering Tomorrow's Telecommunications Solutions*, chatswood, nsw (n.d.).

Northern Telecom, *Annual Report 1993*, Ontario, 1993.

Slatalla, Mishelle & Quittner, Joshua, *Masters of Deception*, Harpercollins, New York, 1995.

Royal Commission into Aboriginal Death in Custody, *Report of the Inquiry into the Death of Woman Who Died at Ceduna*, Australian government Publishing Service, Canberra, 1990.

Scottish Law Commission Report on Computer Crime, no. 174, 1987.

SPAN Management Office, «Security guidelines to be followed in the latest worm attack», an Intranetwork Memorandum released by the SPAN Management Office, NASA, 30 October 1989.

Sterling, Bruce, *The Hacker Crackdown*, Penguin Books, Melbourne, 1994. [Книга доступна на

<http://lib.rus.ec/b/106013> (прим. сост. FB2)]

Stoll, Clifford, *The Cuckoo's Egg*, pan books, London, 1991.

Tencati, Ron, «Information regarding the DECNET worm and protection measures», an Intranetwork Memorandum released by the SPAN Management Office, NASA, 19 October 1989.

–, «Network Security Supplemental Information – Protecting the DECNET Account», security advisory, released by SPAN, NASA/Goddard Space Flight Center, 1989.

The Victorian Ombudsman, *Operation Iceberg; Investigation of Leaked Police Information and Related Matters*, report of the Deputy Ombudsman (Police Complaints), L. V. North Government Printer, Melbourne, 1993.

«USA proposes international virus team», Computer Fraud & Security Bulletin (Elsevier Advanced Technology Publication), August 1991.

Victoria Police, *Operation Iceberg – Investigation and Recommendations into Allegations of Leaked Confidential Police Information*, 1 June, memorandum from victoria Police Commander Bowles to Chief Commissioner Comrie (also available as Appendix 1 in the Victorian Ombudsman's Operation Iceberg Report, tabled in Victorian Parliament, October 1993), 1993.

Vietor, Richard, *Contrived Competition: Regulation and Deregulation in America*, belknap/harvard university press, Cambridge, 1994.

Yallop, David, *To the Ends of the Earth*, corgi books (transworld), moorebank, nsw, 1994.

### **Законы:**

Computer Misuse Act 1990 (UK)

Crimes Act 1914 (no. 5) (cwlth)

Crimes Legislation Amendment Act 1989, no. 108

Computer Fraud and Abuse Act 1986 (us), 18 usc 1030

Computer Misuse Crimes Legislation Amendment Bill 1989 (aus),

Explanatory Memo Clause 7 Crimes (Computers) Act, no. 36 of 1988 (vic)

### **Другие публикации и базы данных:**

- American Bar Association Journal Associated Press
- Attorney general's information Service (Australia)
- Australian Accountant
- Australian Computer Commentary
- Aviation Week and Space Technology (USA)
- Banking Technology
- Business Week
- Cable News Network (CNN)
- Card News (USA)
- CERT Advisories (The Computer Emergency Response Team at Carnegie Mellon University)
- Chicago Daily Law Bulletin Communications Week
- Communications Week International
- Computer Incident Advisory Capability (CIAC)
- Computer Law and Practice (Australia)
- Computer Law and Security Report (Australia)
- Computer Weekly
- Computergram
- Computerworld
- Computing
- Corporate EFT Report (USA)
- Daily Mail (UK)
- Daily Telegraph (sydney)
- Daily Telegraph (UK)
- Data Communications
- Datalink
- Evening Standard (UK)
- Export Control News (USA)

- Fintech Electronic Office (The Financial Times)
- Gannett news office
- Government Computer News (USA)
- Info World
- Intellectual Property Journal (Australia)
- Intelligence Newsletter (Indigo Publication)
- Journal of Commerce (The New York Times)
- Journal of The Law Society of Scotland
- Korea Economic Daily
- Law Institute Journal (Melbourne)
- Law Society' Gazette (UK)
- Law Society's Guardian Gazette (UK)
- Legal Times (USA)
- Lexis-Nexis (Reed Elsevier)
- Lloyds List
- Mail on Sunday (UK)
- Media Week
- MIS Week
- Mortgage Finance Gazette
- Network World
- New Law Journal (UK)
- New York Law Journal
- Newsday
- PC Week (USA)
- Press Association Newsfile
- Reuter
- Reuter News Service – United Kingdom Science
- South China Morning Post
- St Louis Post-Dispatch
- St Petersburg Times
- Sunday Telegraph (Sydney)
- Sunday Telegraph (UK)
- Sunday Times (UK)
- Telecommunications (Horizon House Publication Inc.)
- The Age
- The Australian
- The Australian Financial Review
- The Bulletin
- The Computer Lawyer (USA)
- The Connecticut Law Tribune
- The Daily Record (USA)
- The Engineer (UK)
- The Gazette (Montreal)
- The Guardian
- The Herald (Glasgow)
- The Herald (Melbourne)
- The Herald Sun (Melbourne)
- The Independent
- The Irish Times
- The Legal Intelligencer (USA)
- The Los Angeles Times
- The Nation
- The National Law Journal (USA)
- The New York Times
- The Recorder (USA)
- The Reuter European Community Report
- The Reuter Library Report

- The Scotsman
- The Sun (Melbourne)
- The Sunday Age
- The Sydney Morning Herald
- The Times
- The Washington Post
- The Washington Times
- The Weekend Australian
- Time Magazine
- United Nations Chronicle
- United Press International
- USA Today

### **Стенограммы:**

Hearing of the Transportation, Aviation and Materials Subcommittee of the House Science, Space and Technology Committee transcript: witness Clifford Stoll, 10 July 1990

«Larry King Live» transcript, interview with Clifford Stoll, 23 March 1990 The World Uranium Hearing, Salzburg 1992, witness transcript US Government Accounting Office Hearing (computer security) witness transcripts, 1996

### **Судебные приговоры:**

*Chris Goggans, Robert Cupps and Scott Chasin, Appellants v. Boyd & Fraser Publishing Co., a division of South-Western Publishing Co., Appellee* No. 01-95-00331-Cv 1995 Tex. App.

*Gerald Gold v. Australian Federal Police,* no v93/1140.

*Gerald Gold v. National Crime Authority,* no. v93/1141 at no. 9940 Freedom of Information (1994) 37 ALD 168.

*Henry John Tasman Rook v. Lucas Richard Maynard* (no.2) lca 52/ 1994; judgement no. A64/1994.

*Pedro Juan Cubillo v. Commonwealth of Australia,* no. ng 571 of 1991 fed no.1006/95 tort – negligence. *R v. Gold and another,* house of lords (UK), [1988] 1 AC 1063, [1988] 2 All ER 186, [1988] 2 WLR 984, 87 Cr App Rep 257, 152 JP 445, [1988] Crim Lr 437.

*Steve Jackson Games Incorporated,* et al., plaintiffs, v. *United States Secret Service, United States of America,* et al., defendants no. A 91 CA 346 Ss 816 F. Supp. 432; 1993 U.S. Dist.

*United States of America v. Julio Fernandez,* et al., 92 cr. 563 (ro).

*United States of America,* plaintiff, v. *Robert J. Riggs, also known as Robert Johnson, also known as Prophet, and Craig Neidorf, also known as Knight Lightning,* defendants no. 90 cr 0070 743 F. Supp. 556; 1990 U.S. Dist.

*United States of America,* appellee, v. *Robert Tappan Morris,* defendant-Appellant No. 90– 1336 928 F.2d 504; 1991 U.S. App.

*Wesley Thomas Dingwall v. Commonwealth of Australia,* no. ng 575 of 1991 Fed no.296/94 Torts.

*William Thomas Bartlett v. Claire Patricia Wier, Henry J T Rook, Noel E. Aikman, Philip Edwards and Michael B McCay* no. tg 7 of 1992; fed no. 345/94.

### **Другие судебные материалы:**

Докладные записки и доклады от/в:

Бюро криминальной разведки, полиция штата Виктория

Отдел внутренних расследований, полиция штата Виктория

Офис SPAN NASA (относительно червя WANK)

Офис Окружного прокурора, Монтеррей, Калифорния

Комиссия трансокеанских коммуникаций (Австралия)

Департамент полиции, Дель-Рей-Оукс, Калифорния

Департамент полиции, Салинас, Калифорния

Стюарт Гилл

Секретная служба Соединенных Штатов

Офис Генерального прокурора США, Нью-Йорк

Большое количество сайтов Интернета, в том числе сайты NASA, Сиднейского университета, «Гринпис», Австралийского института юридической информации и Архивов юридических аспектов компьютерных преступлений.