Phrack RU issue 010

Русская версия Phrack, выпуск 010. Полный текст статей с кодом и таблицами.

Темы выпуска: Unix/Linux, BSD, Windows NT и администрирование систем; культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; справочники, индексы, аббревиатуры и архивные материалы.

Материалы выпуска: Введение; Phrack Pro-Phile 7; The TMC Primer; Руководство для начинающих: IBM VM/370; Circuit Switched Digital Capability; Взлом Primos. Часть I; Automatic Number Identification; Часть первая; На домашнем фронте — 25 декабря 1986 г..

Введение

Дата: 1 января 1987 года

Что ж, мы добрались до этого: начала нового года и начала нового тома Phrack Inc. Выпуск давно ожидался, его подготовка заняла довольно много времени, и мы немало откладывали, так что я приношу извинения тем, кто терпеливо ждал. Мы намеренно немного подождали, но также выпускаем этот Phrack примерно в то же время, что и `Legion of Doom/Hackers Technical Journal`, еще один высококачественный информационный бюллетень, который работает с нами, а не против нас. Лично я рекомендую эти документы как весьма информативные. Мне они очень понравились, и я надеюсь, что вы продолжите поддерживать нас обоих.

Если вы хотите писать для Phrack Inc., просто свяжитесь со мной, Knight Lightning, Cheap Shades, Beer Wolf или кем-то, кто знает нас либо находится на любой из досок MSP, и мы либо ответим вам, либо каким-то образом свяжемся с вами. Темы файлов могут быть связаны с телекоммуникациями, операционными системами или каким-нибудь уникальным аспектом либо изъяном безопасности. Ждите новых выпусков Phrack в близком и далеком будущем. До встречи.

ТК

В этот выпуск Phrack Inc. входят следующие материалы:

1. Introduction to Phrack 10, Taran King, 2,2K.
2. Pro-Phile on Dave Starr, Taran King, 7,5K.
3. The TMC Primer, Cap'n Crax, 6,1K.
4. A Beginner's Guide to the IBM VM/370, Elric of Imrryr, 3,5K.
5. Circuit Switched Digital Capability, The Executioner, 11,9K.
6. Hacking Primos Part I, Evil Jay, 10,9K.
7. Automatic Number Identification, Phantom Phreaker и Doom Prophet, 9,2K.
8. Phrack World News 9 Part I, Knight Lightning, 22,7K.
9. Phrack World News 9 Part II, Knight Lightning, 14,8K.

Phrack Pro-Phile 7

Написал и создал: Taran King
Дата: 15 декабря 1986 года

Добро пожаловать в Phrack Pro-Phile 7. Phrack Pro-Phile создан, чтобы приносить вам, пользователям, информацию о старых или особенно важных и спорных людях. В этом месяце я представляю вам пользователя из золотых лет хакинга и фрикинга.

Dave Starr

Dave - один из старых фрикеров и хакеров, которые многого добились через голосовой фрикинг и буквальный хакинг, а не через чтение чужих находок. Мастер-инженер; voice phreaking - это отдельное искусство. У Dave есть докторская степень по B.S.

Личное

```
              Handle: Dave Starr
           Call him: Dave Starr
       Past handles: Micronet Phantom and Big Brother
      Handle origin: Micronet Phantom появился из работы с компьютером
                     The Source, а Big Brother, конечно, из "1984"
                     Джорджа Оруэлла.
      Date of Birth: 5/6/62
Age at current date: 24
             Height: 6' 0"
             Weight: 170 lbs.
          Eye color: карие
         Hair Color: светло-коричневые
          Computers: TRS-80, версия 4K, Apple ][, ][+, ][e
  Sysop/Co-Sysop of: Starcom Network
```

Dave начал с The Source и держался там 6-8 месяцев, копаясь в системе, потому что с точки зрения безопасности система была очень медленной; оттуда, конечно, он вовлекся во взлом Prime. Один из сотрудников безопасности по имени Paul из Dialcom связался с Dave и обсудил с ним хакинг Dave на The Source, то есть на его системе. После разговора они обнаружили общие интересы, включая хакинг и фрикинг. Paul дал Dave его первый код к местному dial-up для Sprint. Он также направил его к 8BBS, что позволило ему познакомиться с лучшими фрикерами и хакерами страны того времени, включая Susan Thunder, Roscoe DuPran и Kevin Mitnick.

Susan и Roscoe были близкими друзьями Dave, с которыми он встречался лично, как и Kevin, но Kevin он никогда не встречал. Susan он встретил в здании суда округа Лос-Анджелес, давая против нее показания; Susan и Roscoe использовали эти handles как настоящие имена в обвинениях о домогательствах. Самыми памятными фрикерско-хакерскими BBS для Dave были 8BBS и его собственная Starcom Network, где были скрытые команды для доступа к фрикерскому разделу. Starcom Network была национально связанной системой, которую Dave создал и вел. Это была фактически копия The Source, из-за чего он попал в суд. Они заявляли, что это их система, но он подавил их угрозой огласки.

Modem Over Manhattan была еще одной памятной доской на TRS-80. Свои знания фрикинга он приписывает Paul из Dialcom, свои хакерские способности - The Source, а информацию по RSTS - Susan Thunder.

Dave Starr занимается разведывательной и контрразведывательной работой для любого, у кого есть деньги и кто не выступает против Соединенных Штатов или взглядов Соединенных Штатов.

Dave всегда действовал независимо, никогда не был членом клуба или группы и сам выбирал своих партнеров.

Интересы

Телекомпьютинг, включая фрикинг и хакинг; кино; увлечение системами подбора пар, вроде Dial-Your-Match; веселье; видеокомпоненты.

Любимые вещи Dave

```
Женщины: тихий вечер с подругами. Примечание: множественное число.
 Машины: Mercedes 450-SL, принадлежащий его подруге.
   Еда: итальянская.
 Музыка: все, кроме acid rock/heavy metal.
  Досуг: курение, но сигареты он ненавидит.
```

Самые памятные впечатления

Поставить систему The Source на колени.

Хакеры The Source выдвинули требования о снижении тарифов минимум на 33 процента. Это было отправлено с комментарием: “Я в бизнесе, так что понимаю деньги, но вы становитесь слишком чертовски жадными”. Также требовалась статья в журнале `Source-World`, больше той, что была в прошлом выпуске. В ней должно было содержаться следующее: как долго они были на The Source, почему они это делают, безумная точка зрения The Source, их правильная точка зрения, как долго они терроризировали The Source, извинение за ложь всем пользователям о том, что повышение тарифов было необходимо, и открытое извинение перед The Pirate и Micronet Phantom с сожалением обо всех неприятностях, которые The Source причинила им в их стремлении к честному и свободному Sourcing. Они хотели две учетные записи seclev 4, при том что обычный уровень - 3. Они заверили The Source, что могут получить их бесплатно, и, надо же, они действительно могли создать что угодно, но не хотели травли. Если бы их стали травить, они немедленно вошли бы под seclev 7 и убили систему. Они угрожали, что разные учетные записи будут уничтожены, все с seclev 4 и выше. Человек из The Source написал: “На это когда-нибудь ответили?” Затем они продолжали говорить, что не будут больше терроризировать, если ответ поступит на их учетную запись в течение 20 минут.

За удаление учетной записи он отправил ответное сообщение: “Fuck you”. Он объяснил, насколько они бессильны против The Pirate и Micronet Phantom, и что The Source не стоит даже пытаться их поймать. Они собирались продолжать атаковать “Империю”, The Source, пока она не станет честной по отношению к пользователям.

И множество других писем, сыгранных на ту же мелодию.

Люди, которых стоит упомянуть

TCA Vic из The Source. Руководитель обслуживания клиентов и гестаповской полиции; он его искренне ненавидел и всегда думал о том, чтобы засунуть ему метлу в задницу.

Paul из Dialcom. Познакомил его с фрикингом и успокоил его паранойю.

Susan Thunder. За то, что научила его RSTS и другим вещам.

Bruce Patton. В его списке для травли из-за разногласия. Он получил отключение электричества и отключение телефонной системы в своем юридическом офисе, а также переадресацию всех звонков на 8BBS.

Roscoe DuPran. За то, что пошел с ним в суд, познакомил его с Susan лично и за многие другие вещи, здесь не упоминаемые.

The Pirate из Las Vegas. За его полезную постоянную травлю The Source.

Kevin Metnick. За его редкие, но полезные услуги.

Larry из Modem Over Manhattan. За то, что был там, и за то, что его BBS была там.

Bernard из 8BBS. За то, что был там, и за то, что его BBS была там.

Надеюсь, вам понравился этот файл. Ждите новых Phrack Pro-Phile в ближайшем будущем. А теперь регулярный опрос, который задается всем интервьюируемым.

Из общей массы фрикеров, которых вы встречали, считаете ли вы большинство фрикеров, если вообще кого-то, компьютерными гиками? Только The Pirate, тринадцатилетний, подходил под это описание.

Спасибо за уделенное время, Dave.

Taran King
Sysop of Metal Shop Private

The TMC Primer

Автор: Cap'n Crax

17 декабря 1986 г.

Изначально этот файл задумывался как «информационный» — с данными о портах TMC, формулах и т.д., однако я решил, что в виде учебного пособия он принесёт больше пользы. Но сначала немного предыстории...

Кто такие TMC?

TMC (TeleMarketing Communications) — межгородская телефонная служба, работающая во всех 50 штатах. Хотя она не так известна, как MCI или Sprint, это довольно крупная компания. TMC способна организовывать корпоративные системы связи, АТС (PBX) и обслуживание частных абонентов. В отличие от большинства операторов дальней связи (LDC), TMC работает по принципу «франчайзинга»: каждое подразделение практически ничего не знает о других, хотя все они используют одни и те же линии и одно и то же оборудование.

Чем это может быть полезно?

Для большинства из нас TMC открывает множество новых возможностей для изучения. Одно из главных уязвимых мест компании — форматы кодов, которые она решила использовать. Коды на всех портах TMC состоят из семи цифр. Если бы они генерировались случайно, система была бы достаточно защищена от последовательного перебора. Но TMC не использует случайные коды. Вместо этого применяется система формул на основе контрольных сумм, причём на каждом порту — своя формула. Предполагаю, что это сделано ради широкого разброса кодов внутри семизначного диапазона, чтобы при последовательном переборе нельзя было получить 2–3 рабочих кода подряд. Или же они попросту очень недальновидны. В любом случае, примечательно, что они, похоже, никогда не задумывались о том, что может произойти, если кто-нибудь сумеет разгадать любую из этих формул. Собственно, об этом и данный файл.

Что ещё можно добавить?

TMC, судя по всему, использует какую-то версию системы PBX Dimension для выставления счетов (в их рекламе сказано, что коммутационное оборудование цифровое). Это позволяет легко идентифицировать порты TMC по характерному звуковому сигналу «Hi-Lo» при вводе неверного кода. Для тех, кто беспокоится о подобных вещах: TMC — одна из «более безопасных» компаний. Это во многом объясняется тем, что в отличие от «единых» компаний вроде MCI, франшизы TMC не особо заботятся о том, теряет ли деньги другая франшиза. Поскольку каждое подразделение независимо от прочих, существует множество 800-портов — по одному на каждую франшизу. При использовании иногороднего 800-порта можно не беспокоиться, например, об ANI (автоматическом определении номера), которое я, впрочем, никогда не считал серьёзной угрозой для пользователей кодов. Кроме того, TMC предоставляет богатые возможности для начинающего специалиста по безопасности (хехехе).

Реальная информация

Объясню всё, что знаю о взломе TMC, не раскрывая при этом конкретных кодов. Для начала — пример порта. В качестве примера я использую 800-порт Луисвилла, штат Кентукки:

```
1-800-626-9600
```

Это и есть порт. Если вы не знакомы с TMC, можете позвонить и послушать, как он звучит. Допустим, вы позвонили и опознали его как TMC. Что дальше? Хорошим вариантом будет запустить стандартную программу перебора кодов: настроить её на семь цифр, набор с 1+, и учесть, что коды TMC начинаются с 0 более чем на 50% портов, которые я видел. Предположим, в итоге вы получаете следующий список (вымышленных) кодов:

```
0347589
0347889
0348179
0350358
0355408
```

На первый взгляд это может показаться набором «случайных» чисел. Но присмотритесь внимательнее. Эти числа основаны на контрольной сумме. Она выглядит следующим образом:

```
Формат кода: 03xabcy
x + y = 13
(В первом коде x=4 и y=9, и, разумеется, 4+9=13)
a + c = 15
(Здесь a=7 и c=8, и 7+8=15)
b = от 1 до 9
(Цифра "b" не связана с остальными числами. Например, её можно перебирать
от 1 до 9, чтобы найти дополнительные рабочие коды)
```

Обратите также внимание, что 0+5 даст 15, поскольку 0 на самом деле означает 10. Серьёзно!

Обратите внимание: приведённая выше формула является лишь вымышленной. Не хотелось бы нанести ущерб TMC, раскрывая коды их системы!

Это всё?

Нет, конечно. TMC, в своей любви к энтузиастам телекоммуникаций, также спрятала дополнительный приз в коробке с «Krackerjack». На подавляющем большинстве портов TMC есть коды «внешней линии» (Outside Line) — двух- или трёхзначные числа, которые при вводе после определённых кодов дают гудок AT&T. По всей видимости, это наследие от использования оборудования PBX. Если кто-то спрашивает, зачем нужен гудок AT&T (кому-то ещё нужно объяснять?), — это позволяет звонить без ограничений: на номера 976, 900, через Alliance Teleconf., международные звонки и т.д. Само собой, перечислять конкретные коды я не буду, но могу сказать: если код двузначный, он начинается с любой цифры от 2 до 9 и заканчивается на 8 или 9. Если трёхзначный, он почти всегда начинается с 6 и продолжается любыми двумя цифрами. Возможные примеры кодов внешней линии: 59, 69, 89, 99, 626, 636, 628 и т.д. Это, разумеется, лишь примеры возможных кодов. Как уже упоминалось, коды внешней линии вводятся после семизначного кода. Они работают только после определённых семизначных кодов, и, по моему опыту, семизначные коды, с которыми они работают, как правило, не годятся для обычного набора 7 цифр + 1 + номер. Никакой очевидной закономерности в том, с какими кодами они работают, я не нахожу, поэтому искать придётся методом проб и ошибок.

Ещё несколько 800-портов

1-800-433-1440	1-800-227-0073	1-800-331-9922	1-800-451-2300
1-800-354-9379	1-800-248-4200	1-800-531-5084	1-800-351-9800

Заключение

Обратите внимание, что данная статья задумана лишь как общий обзор ТМС и анализ того, насколько компания подходит или не подходит для ваших нужд в сфере дальней связи. И, ради всего святого, не используйте эту информацию в незаконных целях!

Руководство для начинающих: IBM VM/370

Или что делать после того, как вы вошли.

Монография: Elric of Imrryr
Представлено: Lunatic Labs UnLimited

Примечание: этот файл отформатирован для печати на принтере с 80 колонками и 55 строками.

Предисловие: о чем это руководство

Оно было написано, чтобы помочь хакерам изучить основы работы на IBM VM/370. Это не руководство о том, как попасть внутрь, а руководство о том, как пользоваться системой после того, как вы уже вошли.

Комментарии приветствуются на RIPCO: 312-528-5020.

Примечание для хакеров VM/370: не стесняйтесь дополнять этот файл, просто указывайте меня и Lunatic Labs в качестве авторов наших частей.

Часть 1: вход и выход

Когда вы подключаетесь к системе VM/370, нажимайте `RETURN`, пока не увидите:

```
VM/370
!
```

Чтобы войти, введите:

```
logon userid
```

`logon` можно сократить до `l`.

Если вы введете недопустимый `userid`, система ответит сообщением:

```
userid not in cp directory
```

Если он допустим, вы получите:

```
ENTER PASSWORD:
```

Введите свой пароль, затем вы внутри, будем надеяться.

Выход:

```
log
```

Часть 2: загрузка CMS и настройка

Когда вы входите, если вы не видите сообщение:

```
VM/SP CMS - (date) (time)
```

вам нужно загрузить CMS. CMS - это командный интерпретатор.

Введите:

```
cp ipl cms
```

Затем вы должны увидеть что-то вроде:

```
R; T=0.01/0.01 08:05:50
```

Теперь вы сможете использовать команды и CP, и CMS.

Некоторые системы могут считать, что вы используете терминал IBM 3270. Если вы можете эмулировать 3270, например с помощью Crosstalk, сделайте это. Если нет, введите:

```
set terminal typewriter
```

или:

```
set terminal dumb
```

Вы можете вывести список своих файлов, набрав:

```
filelist
```

Можно использовать wildcard-символы, поэтому:

```
filelist t*
```

выведет все файлы, начинающиеся с t.

Имена файлов состоят из FILENAME и FILETYPE.

Вы можете вывести файл, набрав:

```
listfile filename filetype
```

Другие файловые команды: copyfile, erase и rename; все они работают с FILENAME FILETYPE.

Я оставлю только основы и обсужу лишь один редактор, XEDIT. Чтобы использовать XEDIT, введите:

```
xedit filename filetype
```

Оказавшись в XEDIT, введите команду input, чтобы вводить текст. Нажмите RETURN на пустой строке, чтобы вернуться в командный режим, затем введите команду FILE, чтобы сохранить файл.

Часть 5: общение с другими пользователями системы

Отправка и получение NOTES.

Чтобы отправить NOTE другому пользователю, введите:

```
note userid
```

После этого вы окажетесь в подсистеме XEDIT, см. часть 4.

Когда закончите писать свой NOTE, сохраните файл и введите:

```
send note
```

Это отправит NOTE пользователю userid.

Вы также можете использовать команду SEND, чтобы отправлять другие файлы:

```
send filename filetype userid
```

Отправка сообщений.

Вы можете использовать команду `TELL`, чтобы общаться с пользователем, который сейчас вошел в систему:

```
tell userid Help me!
```

Часть 6: получение помощи

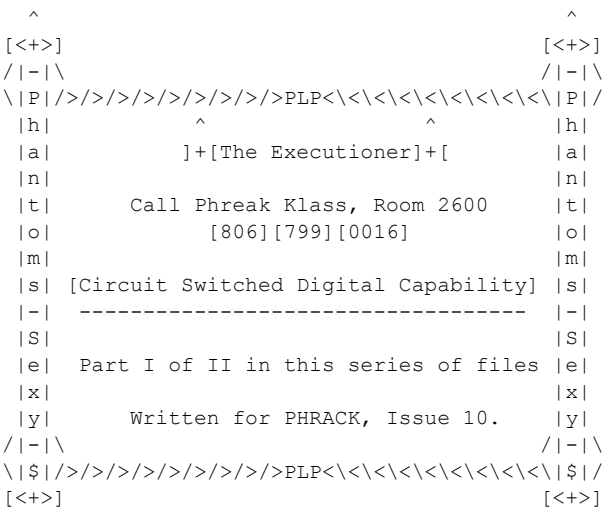
Введите:

```
help
```

Вот и все, удачи.

Circuit Switched Digital Capability

Автор: The Executioner
Серия: часть I из II
Для: PHRACK, выпуск 10



Часть I

Circuit Switch Digital Capability, CSDC, позволяет выполнять сквозную цифровую передачу данных со скоростью 56 килобит в секунду, kb/s, и, в качестве альтернативы, передачу аналоговых голосовых сигналов на основе коммутации каналов.

Сетевая перспектива

Функция CSDC раньше была известна как PSDC, Public Switched Digital Capability. Эти два термина можно использовать как синонимы. Функция CSDC обеспечивает альтернативную возможность голос/данные. Если используется SLC Carrier System 96, цифровые сигналы передаются сигналом T1. Если шлейф является двухпроводным, CSDC использует time compression multiplexing, TCM, что позволяет передавать цифровые сигналы по общему пути с отдельным временным интервалом для каждого направления.

Во время CSDC-вызова конечный пользователь может переключаться между голосовым режимом и режимом данных столько раз, сколько пожелает. Функция CSDC может поддерживать субпеременные скорости данных от оборудования на стороне клиента, но в сети используется скорость 56 kb/s. Некоторые возможные применения CSDC:

1. аудиографические телеконференции;
2. защищенный голос;
3. факсимильная связь;
4. массовая передача данных;
5. медленное сканирующее телевидение.

Коммутатор ESS предоставляет конечному пользователю доступ и выполняет функции сигнализации, коммутации и транкинга между обслуживающим коммутатором ESS и другими

CSDC-станциями. Конечным пользователям CSDC требуется цепь network channel terminating equipment, NCTE, то есть SD-3C476 или эквивалент. Доступ конечного пользователя осуществляется по двухпроводным металлическим шлейфам, завершающимся на metallic facility terminal, MFT, или SLC Carrier System.

Конечные пользователи, не обслуживаемые напрямую прямой CSDC ESS-станцией, могут получить доступ к оборудованию CSDC через схему доступа RX, Remote Exchange, с использованием D4 Carrier System и, если требуется, SLC Carrier System. T-Carrier trunks служат для передач на короткие расстояния, а дальние передачи обслуживаются цифровой микроволновой радиосвязью и другими цифровыми системами.

Если интерфейс NCTE используется с оборудованием на стороне клиента, для подключения NCTE к другому оборудованию применяется миниатюрный восьмипозиционный последовательный разъем. Контакты разъема разбиты на пары: пара передачи данных, пара приема данных, голосовая пара и пара переключения режима. Пары данных поддерживают одновременную передачу и прием цифровых данных в биполярном формате на 56 kb/s. Пары данных также обеспечивают передачу управляющей информации в сеть и из сети. Голосовая пара поддерживает передачу аналогового сигнала и обеспечивает установку вызова, разъединение и функции звонка. Пара управления режимом подает сигналы в сеть, когда клиент запрашивает изменение режима, голос в данные или данные в голос.

CSDC-вызов начинается по двухпроводному шлейфу, который также может использоваться для Message Telecommunication Service, MTS. Линии могут быть помечены как `MTS/CSDC` или только `CSDC`. Для инициирования CSDC-вызова нужен touch tone. Вызовы могут инициироваться вручную или с помощью Automatic Calling Equipment, ACE, если оно доступно. Прием цифр, передача и сигнализация следуют тем же процедурам, что используются для исходящего MTS-вызова по CCIS- или non-CCIS-транкам. Однако CSDC-вызовы всегда маршрутизируются по цифровым средствам передачи.

Долгосрочный план также допускает сигнализацию EA-MF, Equal Access-Multi Frequency, и улучшенные записи automatic message accounting, AMA. CSDC-вызов проверяется, чтобы убедиться, что вызывающая сторона имеет CSDC-сервис и что используемый оператор предоставляет возможность 56 kb/s voice/data. Заблокированный вызов направляется на специальное сервисное сообщение об ошибке. Non-CSDC-вызовы не допускаются к маршрутизации через CSDC-only carriers. Проверка неплательщика не допускается для CSDC-вызовов, использующих сигнализацию CCIS.

CSDC-вызов маршрутизируется напрямую к оператору или косвенно через Access Tandem, AT, или Signal Conversion Point, SCP. Вызов завершается напрямую от оператора к оконечной станции или косвенно через AT или SCP. Сигнализация для прямой маршрутизации - либо CCIS, либо EA-MF, и назначается на основе trunk group.

AT - это коммутатор ESS, который позволяет оконечной станции получать доступ к операторам без необходимости прямых транков. Сигнализация между оконечными станциями и AT - либо EA-MF, либо CCIS. Группы транков, использующие EA-MF, могут иметь объединенный операторский трафик. Для сигнализации CCIS требуются отдельные trunk groups для каждого оператора.

SCP - это коммутатор ESS, позволяющий получать доступ к операторам с использованием только сигнализации CCIS из станций без возможности CCIS. Между исходной оконечной станцией и SCP используются отдельные trunk groups для каждого оператора. Отдельные trunk groups между SCP и завершающей оконечной станцией являются необязательными. Сигнализация между оконечной станцией и SCP - MF. SCP должен иметь прямое соединение с оператором, использующее сигнализацию CCIS.

Remote Switching System

RSS может использоваться как удаленная точка доступа для CSDC. Совместимость RSS и CSDC повышает рыночную привлекательность обеих функций. Конструкция RSS предусматривает поддержку plug-in-модулей D4 special service channel bank. Это позволяет такие применения, как удаленные расширения, foreign exchange lines и private lines. Таким образом, RSS может использоваться как точка доступа CSDC в конфигурации, похожей на схему CSDC RX.

Centrex/ESSX-1

Функция CSDC опционально доступна клиентам Centrex/ESSX-1. Большинство возможностей Centrex-сервиса можно применить к линиям Centrex, которым назначена функция CSDC. В голосовом режиме линия Centrex/CSDC может использовать любые групповые функции Centrex, назначенные этой линии. В режиме voice/data несколько функций Centrex не работают или работают только на некоторых вызовах. Функция CSDC может предоставляться для группы Centrex следующим образом:

1. на основе Message Network, MTS;
2. на основе группы IntraCentrex;
3. на основе группы InterCentrex;
4. в любой комбинации перечисленного.

Пользовательская перспектива CSDC

Чтобы установить CSDC-вызов, пользователь CSDC снимает трубку, получает тон набора и набирает номер. Формат набора для CSDC/MTS в промежуточном плане следующий:

```
#99 AB (1+) 7 or 10 digits (#)
```

Клиент набирает `#99`, чтобы получить доступ к функции CSDC. Цифры `AB` - это код обозначения оператора. После цифр `AB` тон набора не возвращается. `1+` перед 7- или 10-значным directory number должен использоваться, если он требуется для MTS-вызовов. `#` в конце необязателен; если он не набран, конец набора сигнализируется тайм-аутом.

Долгосрочный формат набора для CSDC/MTS следующий:

```
#56 (10XXX) (1+) 7 or 10 digits (#)
```

Набор `#56` указывает на 56 kb/s альтернативную передачу voice/data. `10XXX` идентифицирует оператора, который должен использоваться для вызова. Если `10XXX` не набран на inter-LATA-вызове, используется основной оператор абонента. Если `10XXX` не набран на intra-LATA-вызове, вызов обрабатывает telco. Долгосрочный план также допускает несколько сокращенных форм. Набор `#56 10XXX #` разрешен для маршрутизации вызова, который предлагает клиенту набирать согласно плану набора оператора. Также разрешен набор `#56 10XXX` с последующим speed call. Если клиент предварительно подписан на оператора, способного переносить CSDC-вызовы, и CSDC access code сохранен как часть номера speed calling, клиент набирает код speed calling, чтобы сделать CSDC-вызов.

На вызываемую линию подается обычный звонок, а на вызывающий терминал - слышимый сигнал вызова. После установления голосового соединения любая сторона может инициировать переключение в режим данных, если пожелает. Чтобы инициировать изменение режима,

пользователь CSDC должен подать команду mode switch через замыкание NCT.

Пример переключения режима:

Предположим, сторона A хочет переключиться на данные. Сторона A выдает команду mode switch и получает сигнал called far end voice, FEV, который является биполярной последовательностью, 2031 Hz при 60 ipm. Сторона A может положить трубку в любое время после инициирования команды mode switch. Сторона B получает far end data, FED, tone, 2031 Hz при 39 ipm, указывающий, что сторона A хочет переключиться на данные. Если сторона B соглашается переключиться на данные, сторона B должна инициировать команду mode switch. Сторона B теперь может положить трубку. Передача данных теперь возможна.

Чтобы переключиться в голосовой режим, инициировать это может кто угодно. Для переключения сторона A поднимет трубку, инициирует команду mode switch и получит FED tone. Сторона B получает FEV tone, указывающий, что сторона A хочет перейти на голос. Теперь сторона B должна поднять трубку и инициировать команду mode switch. Чтобы завершить вызов, любая сторона может просто оставить трубку на месте и указать mode switch. Если завершение выдано во время конфликта режимов, тайм-аут разъединит вызов, обычно примерно через 10 или 11 секунд.

Клиенты Centrex/ESSX-1 могут использовать CSDC-сервис несколькими способами, если у них есть CSDC-терминалы с необходимым оборудованием на своей площадке. Стандартный CSDC-вызов инициируется набором кода доступа к message network, `9`. Затем последовательность набора идентична плану для MTS:

```
#99 AB (1+) 7 or 10 digits (interim plan)

#56 (10XXX) (1+) 7 or 10 digits (#) (long term plan)
```

Шаблон набора для установления interCentrex- или intraCentrex-CSDC-вызовов следующий:

```
CSDC access code + extension
```

IntraCentrex/CSDC-вызов инициируется набором trunk access code, назначенного для маршрутизации loop-around Centrex/CSDC trunk group. Затем набирается extension нужной станции. Чтобы установить interCentrex-вызов, нужно использовать другой trunk access code для маршрутизации CSDC-вызовов к другой группе Centrex вместо станции.

Схема обслуживания CSDC имеет набираемый цифровой loopback. Этот loopback очень полезен при тестировании CSDC. Клиент может проверить свою линию доступа, набрав тестовый DN. Шлейф автоматически активируется, когда на вызов отвечают.

Конец части I

Часть II: аппаратное обеспечение CSDC и структуры данных станции.

```
=====================================================
= (c) 1986 The Executioner and The PhoneLine Phantoms =
=====================================================
```

Взлом Primos. Часть I

Автор: Evil Jay

Phone Phreakers of America
(C) 1986–87

Примечание автора

Сразу скажу: в сети есть другие файлы о взломе Primos, в том числе написанные совсем недавно, однако глубокого понимания системы они не дают — фактически это пустышки. Такие файлы следовало бы удалить и заменить этим. Данный материал — первый из серии статей о Primos. В последующих выпусках я рассмотрю сетевую инфраструктуру, различные подсистемы и многое другое. Приятного чтения!

Получение доступа. Часть 1

Получение доступа — как всегда, самое сложное.

При подключении к системе Primos вы увидите примерно следующее:

```
PRIMENET 19.2.7F PPOA1
```

Если приветственное сообщение не появилось, введите что-нибудь вроде `XXZZZUUU` и нажмите Enter — система должна ответить:

```
Invalid command "XXZZZUUU".  (logo$cp)
Login please.
ER!
```

Для входа в систему введите:

```
LOGIN <USER ID> <RETURN/ENTER>
```

Или просто:

```
LOGIN <RETURN/ENTER>
```

(Тогда система запросит «User ID?»)

Идентификаторы пользователей различаются от системы к системе, однако учётные записи по умолчанию встречаются везде. На запрос «User ID?» попробуйте:

```
SYSTEM   (Учётная запись оператора — как правило, даёт полные права.)
LIB
DOS
```

После ввода идентификатора система запросит:

```
Password?
```

Здесь вводится пароль. Для учётной записи `SYSTEM` попробуйте:

```
SYSTEM
SYSMAN
NETLINK
PRIMENET
```

```
MANAGER
OPERATOR
```

И всё, что придёт в голову. Это лишь наиболее распространённые пароли к стандартным учётным записям.

Для `LIB` попробуйте:

```
LIBRARY
SYSLIB
LIB
SYSTEM
```

Для `DOS`:

```
DOS
SYSDOS
SYSTEM
```

И так далее — включайте голову.

Старые версии

В старых версиях Primos — 18 и ниже — можно было ввести одну из стандартных учётных записей, а вместо пароля нажать Ctrl-C один или два раза, и система пускала без пароля. Баг это или намеренное поведение — не знаю, но иногда срабатывает. Чтобы узнать версию Primos, посмотрите на приветственное сообщение:

Здесь `19` — номер версии. В данном примере описанный выше трюк не сработает.

Если приветственное сообщение не появилось и версия неизвестна — попробуйте его всё равно.

Неверный логин

Если система отвечает:

```
Invalid user id or password; please try again.
```

Нужно пробовать другой пароль. Обратите внимание: система сообщает лишь то, что идентификатор, пароль или оба сразу неверны, не уточняя что именно. Не беспокойтесь об этом — просто перебирайте стандартные учётные записи. Ходят слухи о типовых паролях вроде PHANTOM, PRIMOS, PRIME и FAM, но, на мой взгляд, это чепуха — ни разу их не встречал. PRIMOS и PRIME иногда существуют как учётные записи, но стандартными я бы их не назвал. Также попробуйте DEMO и GUEST — они встречаются, хотя и редко.

В отличие от Tops 20 и DEC, Primos не ограничивает количество команд до входа в систему, поэтому взлом сводится к простому перебору.

Пустые пароли

Некоторые пользователи устанавливают в качестве пароля просто нажатие Enter: вводишь идентификатор — и ты в системе. Иногда такие пустые пароли назначаются оператором по

умолчанию, хотя это редкость. Если вам известен формат обычных идентификаторов (например, у вас уже есть своя учётная запись), попробуйте пароли вроде:

```
NETLINK
SYSTEM
PRIME
PRIMENET
PRIMOS
```

А также типичные пользовательские пароли: sex, hot, love и тому подобное. По моим наблюдениям, студентки университетских систем Primos чаще всего выбирали что-то связанное с сексуальной тематикой — sex оказывался самым популярным.

Формат идентификаторов

Формат идентификатора пользователя — практически произвольный, каждый оператор задаёт его по своему усмотрению. Как правило, это нечто бессмысленное на первый взгляд: комбинации цифр, букв, возможно управляющих символов. Регистр значения не имеет — система переводит всё в верхний. Длина пароля — до 16 символов.

Вы вошли!

При успешном входе вы увидите нечто подобное:

```
PPOA1 (user 39) logged in Monday, 15 Dec 86 02:29:16.
Welcome to PRIMOS version 19.4.9.
Last login Friday, 12 Dec 86 08:29:04.
```

Поздравьте себя — это настоящее достижение!

Следующая часть будет посвящена базовым командам для начинающих. Напоследок добавлю: да, Primos непросто взломать, но при достаточном терпении почти любая система имеет демонстрационные учётные записи и поддаётся. Большинство хакеров обходят Primes стороной, не подозревая, как эта система затягивает. Удачи и не останавливайтесь!

Самое интересное

Изначально эта часть задумывалась как введение в команды Primos для начинающих. Однако я решил написать о том, как с низкоуровневой учётной записью получить системный доступ. Также хочу поблагодарить PHRACK Inc. за отличную работу — без PHRACK я вряд ли нашёл бы способ распространять свои материалы. Среди всех изданий подобного рода именно с PHRACK достаточно было связаться с кем-то из редакции — а их почтовый ящик хорошо известен в хак/фрик сообществе. Призываю все BBS поддерживать PHRACK, и ещё раз — отличная работа, ребята. Продолжаем.

Что нужно знать

Описанное ниже работает не всегда — примерно в 60% случаев. Раз я первым изложил это «в печатном виде», прошу операторов систем, читающих этот файл, сохранять указание на авторство меня и моей группы.

Ещё немного подготовки

Этот файл рассчитан не на новичков. Перед тем как продолжать, желательно знать команды `ATTACH` и `SLIST` — они несложные, и без них в принципе можно обойтись, но всё же это важные команды в Primos. Справку по ним можно получить так:

```
HELP SLIST
```

или

```
HELP ATTACH
```

Поиграйте с этими командами, пока не освоитесь.

Приступаем

Файл не объясняет каждый мой шаг — я просто покажу, как получить привилегированные учётные записи SYS1.

Войдите в систему под своей учётной записью с низким уровнем доступа.

Введите:

```
ATTACH MFD
```

Затем выведите список директорий:

```
LD
```

Вы видите каталог с множеством поддиректорий. В корневом каталоге, как правило, находятся только `BOOT` и `SYS1` — игнорируйте их. Ищите директорию с именем `CCUTIL` или что-то, содержащее слова UTILITY, UTIL, UTILITIES и подобное.

Перейдите в найденную директорию:

```
ATTACH <ИМЯ ДИРЕКТОРИИ>
```

Снова выведите список через `LD` и изучите файлы. Дальше — элемент случайности: поскольку наборы утилит на разных системах различаются, ищите файлы с расширением `.CPL`. Может оказаться файл `USRLST.CPL`. Введите:

```
SLIST USRLST
```

(Расширение `.CPL` вводить не нужно.)

Программа начнёт выводить большой массив данных. Среди него должна быть строка вида:

```
A CCUTIL X
```

Здесь `CCUTIL` — имя текущей директории утилит (оно, разумеется, может быть другим). Если директория называется `UTILITY`, строка будет выглядеть так:

```
A UTILITY X
```

Символ `X` — это **пароль этой директории**. Он может быть любым. Например, если пароль совпадает с именем директории:

```
A UTILITY UTILITY
```

Или если пароль `SECRET`:

```
A UTILITY SECRET
```

Поздравьте себя — теперь у вас есть доступ SYS1. Войдите снова командой `LOGIN` (или выйдите через `LOGOUT` и войдите заново). В качестве идентификатора укажите имя директории (`UTILITY`, `CCUTIL` или любое другое), а в качестве пароля — найденный пароль. Если войти не удалось, попробуйте другие поддиректории из корневого каталога MFD и выполните `SLIST` для других файлов с расширением `.CPL`. В одном из следующих файлов о Primos я подробно объясню логику этих действий и другие способы получить пароли директорий и идентификаторов.

Если строка вида:

```
S <ИМЯ ДИРЕКТОРИИ> <ПАРОЛЬ>
```

в программе не нашлась — просматривайте другие программы из каталога утилит или пробуйте другие директории. Описанным способом я получал доступ SYS1 примерно в 60% случаев, причём не всегда именно через директорию с утилитами.

На этом данный файл заканчивается. Следите за следующими выпусками PHRACK — там появится ещё один мой файл о Primos. Если не передумаю, следующий будет посвящён базовым командам для начинающих.

```
-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-
!                                               !
#          This Has Been An:                    #
!                                               !
#       Evil Jay Presentation                   #
!                                               !
#     Phone Phreaks of  America                 #
!                                               !
#             (C) 1986-87                       #
!                                               !
-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-
```

Automatic Number Identification

Авторы: Doom Prophet и Phantom Phreaker

Automatic Number Identification, ANI, - это не более чем автоматическое средство немедленного определения Directory Number вызывающего абонента. Этот процесс сделал возможным использование систем CAMA, Centralized Automatic Message Accounting, в станциях SxS, Panel и Xbar #1.

Идентичность вызывающей линии определяется цепями ANI, установленными в упомянутых выше типах центральных станций. Станции Xbar #5 имеют собственное оборудование AMA, Automatic Message Accounting, и используют AMA translator для автоматического определения вызывающей линии.

До разработки ANI у каждой абонентской линии, также называемой local loop, было механическое маркирующее устройство, которое отслеживало междугородные начисления. Эти устройства вручную фотографировались в конце расчетного периода, и на основании этого определялась сумма счета абонента. Этот процесс занимал много времени, поэтому была разработана новая система, ANI.

Основные компоненты системы ANI, используемой в SxS и Crossbar #1:

• directory number network и bus arrangement для подключения sleeve, провода, добавляемого к проводам R, ring, и T, tip, кабельной пары на MDF, Main Distribution Frame;
• провод каждого номера линии через identifier connector к identifier circuit;
• outpulser и identifier connector circuit для захвата свободного identifier;
• identifier circuit для определения номера вызывающей стороны и отправки его в outpulser для последующей передачи через outpulser link к ANI outgoing trunk;
• ANI outgoing trunk к tandem office, оборудованному системой CAMA.

Ниже приведен краткий обзор операций ANI применительно к междугородному вызову через станцию #1Xbar. Вызов обрабатывается обычным образом оборудованием центральной станции и маршрутизируется через ANI outgoing trunk к tandem office. Процесс идентификации начинается, как только CAMA sender в tandem office получает все цифры вызываемого номера и когда district junctor в Xbar office переходит в свое cut-through положение, то есть положение соединительных цепей или путей между line-link и trunk-link frames в центральной станции.

Получив сигнал начала идентификации от оборудования CAMA, ANI outgoing trunk, OGT, устанавливает соединение через outpulser link со свободной цепью outpulser. Затем свободный identifier захватывается цепью outpulser через внутренний блок Identifier connector. После этого identifier через connector unit подключается к directory number network и bus system.

В то же время identifier подаст сигнал ANI trunk, чтобы тот применил идентификационный тон 5800 Hz к sleeve lead ANI trunk. Тон передается на уровне двух вольт по путям S lead через directory number network и bus system. К моменту достижения цепи identifier он ослабляется, или уменьшается, до микровольтного диапазона, что требует усиления напряжения на 120 dB оборудованием amplifier detector в identifier для обеспечения правильной идентификации цифр и операций регистрации.

Одна установка ANI может обслуживать до шести центральных станций в многостанционном здании. Identifier начинает поиск номера вызывающей линии, последовательно тестируя или сканируя тысячи secondary buses каждой центральной станции. Когда сигнал 5800 Hz обнаружен, identifier заземляет соответствующие провода к outpulser, чтобы сначала зарегистрировать цифру вызывающей станции, а затем тысячную цифру номера вызывающего абонента. Outpulser немедленно переводит цифру, представляющую код вызывающей станции, в свой

соответствующий трехзначный код станции.

Identifier продолжает процесс сканирования последовательно по группам сотен, десятков и единиц secondary buses в вызывающей станции, а идентифицированные цифры вызывающего номера также регистрируются и переводятся в релейном оборудовании outpulser для передачи в tandem office.

Outpulser оборудован проверочными и временными функциями, чтобы быстро обнаруживать и записывать возникающие неисправности. Этот процесс может быть причиной некоторых карточек, найденных при копании в мусоре. После завершения процесса сканирования он освобождает identifier и продолжает выдавать полную информацию о номере вызывающего абонента в CAMA-оборудование tandem office в MF-тонах в формате:

```
KP+X+PRE+SUFF+ST
```

где `X` - информационная цифра. Информационные цифры следующие:

```
0 - Automatic Identification, нормально
1 - Operator Identification, ONI
2 - Identification Failure, ANIF
```

Существуют также другие типы outpulsing ANI-информации, если на вызывающей линии есть какое-либо ограничение.

Когда все цифры переданы и ANI trunk переведен в разговорное состояние, outpulser освобождается.

В tandem office номер вызывающей стороны записывается на ленту в CAMA-оборудовании вместе с другими данными, необходимыми для биллинга. Эта информация, включая время ответа вызываемой станции и время разъединения, попадает на AMA-ленты.

Сами ленты обычно являются стандартными магнитными reel-to-reel лентами и отправляются в Revenue Accounting Office, RAO, в конце расчетного периода.

Итак, если суммировать весь процесс ANI:

Совершен междугородный вызов. Центральная станция маршрутизирует вызов через ANI trunks, где захватывается свободный identifier, который затем подключается к directory number network и bus system, одновременно сигнализируя ANI trunk подать необходимый тон 5800 Hz на sleeve. Identifier начинает процесс сканирования и определяет номер вызывающей станции и цифры номера вызывающего абонента, которые через outpulser в MF-тонах отправляются в CAMA-оборудование tandem office. Информация о вызове записывается на AMA-ленты и используется для определения биллинга.

Обратите внимание, что ваш номер действительно появляется на AMA-ленте, если обстоятельства правильные: любой междугородный вызов, будь он с message-rate line или flat-rate line. Однако AMA-ленты не записывают номер вызывающей линии в каком-либо отдельном формате. Они записываются в порядке first-come, first-serve.

Разные сноски

Сноски в основной статье отмечены звездочкой.

ANIF, Automatic Number Identification Failure. Это ситуация, когда оборудование ANI не работает должным образом; она может возникать из-за широкого набора технических причин. Когда происходит ANIF, используется так называемый ONI, Operator Number Identification. Вызов передается оператору TSPS, который запрашивает номер вызывающей линии, говоря что-то вроде: “С какого номера вы звоните?”

CAMA, Centralized Automatic Message Accounting. CAMA - система, записывающая детали вызова для целей биллинга. CAMA используется из централизованного места, обычно tandem office. CAMA обычно применяется для обслуживания class 5 end offices в сельской области рядом с крупным городом, где есть tandem или toll office. CAMA похожа на LAMA, за исключением того, что LAMA локализована в конкретной центральной станции, а CAMA - нет.

Directory Number Network и bus system. Это сеть, участвующая в процессе ANI. Она представляет собой решетку вертикальных и горизонтальных шин, сгруппированных и классифицированных как Primary или Secondary. В Primary system есть 100 вертикальных и 100 горизонтальных шин. В Secondary system есть две подгруппы: bus system #1 и bus system #2, каждая из которых имеет десять горизонтальных и вертикальных шин. Эти шины в целом связаны с identifier в ANI trunk и отвечают за определение цифр десятков, сотен, тысяч и единиц вызывающего номера после того, как identifier начинает процесс сканирования.

MDF, Main Distribution Frame. Это область, где встречаются все кабельные пары определенной станции и добавляется третий провод, sleeve wire. Sleeve wire используется при сборе ANI-информации, а также для определения состояния вызываемой линии, снята или положена трубка, в некоторых коммутационных системах по наличию напряжения. Напряжение есть на sleeve - линия занята; напряжения нет - линия свободна.

ONI, Operator Number Identification. См. сноску ANIF.

Примечание: существуют также другие формы Automatic Message Accounting, например LAMA, Local Automatic Message Accounting. LAMA используется в class 5 end office, в отличие от CAMA в toll office. Если бы на вашей end office была LAMA, ANI-информация записывалась бы на местном уровне и отправлялась оттуда. Схема LAMA может быть компьютеризированной; тогда она обозначается с включенной буквой C, LAMA-C или C-LAMA.

Источники и благодарности

`Basic Telephone Switching Systems`, second edition, David Talley.

`Understanding Telephone Electronics`, Radio Shack/Texas Instruments.

Конец файла.
12 июля 1986 года.

Часть первая

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                                     PWN
PWN                        <-=*} Phrack World News {*=->                PWN
PWN                                                                     PWN
PWN                              Issue IX/Part One                      PWN
PWN                                                                     PWN
PWN                      Compiled, Written, and Edited by               PWN
PWN                                                                     PWN
PWN                              Knight Lightning                       PWN
PWN                                                                     PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

В PWN, выпуск 7/Часть Первая, была статья под названием «Maxfield наносит удар снова». Речь шла о системе под названием «THE BOARD» в детройтском коде NPA 313. Номер был 313-592-4143, пароль для новых пользователей — `HEL-N555,ELITE,3` (затем Enter). Система была примечательна тем, что работала на компьютере HP2000. 20 августа 1986 года на «THE BOARD» появилось следующее сообщение.

```
                Welcome to MIKE WENDLAND'S I-TEAM sting board!
                   (Computer Services Provided By BOARDSCAN)
                             66 Megabytes Strong

                                300/1200 baud - 24 hours.

                           Three (3) lines = no busy signals!
                             Rotary hunting on 313-534-0400.


Board:   General Information & BBS's
Message: 41
Title:   YOU'VE BEEN HAD!!!
To:      ALL
From:    HIGH TECH
Posted:   8/20/86 @ 12.08 hours
```

Приветствуем!

Вы находитесь на «THE BOARD» — «ловушечной» BBS, которую ведёт MIKE WENDLAND из I-Team телеканала WDIV-TV. Цель? Продемонстрировать и задокументировать масштабы преступной и потенциально незаконной хакерской деятельности и телефонного мошенничества так называемого «хакерского сообщества».

Спасибо за содействие. За последние полтора месяца мы получили от вас всевозможную информацию, уличающую многих из вас в мошенничестве с кредитными картами, телефонном мошенничестве, вандализме и возможных взломах правительственных или компьютеров систем общественной безопасности. И что самое замечательное — у нас есть ваши сообщения, ваша электронная почта и — самое главное — ваши НАСТОЯЩИЕ имена и адреса.

Что мы собираемся с этим делать? Следите за каналом News 4. Я планирую специальный цикл репортажей о нашем опыте с «THE BOARD», которой пользовались абоненты со всего побережья и из Канады в возрасте от 12 до 48 лет. Для наших постоянных пользователей: меня знали под ником High Tech и под другими именами. Джон Максфилд из Boardscan выступал нашим консультантом и предоставил HP2000, на котором работала эта «ловушка». Благодаря переадресации звонков и другим удобствам, которые обеспечивают современные телефонные технологии, BBS работала

удалённо здесь, в районе Детройта.

Когда выйдут наши репортажи? Через несколько недель. Теперь мы свяжемся со многими из вас напрямую, а также поговорим с сотрудниками правоохранительных органов и службами безопасности компаний, выпускающих кредитные карты, и телефонных компаний.

Должна получиться отличная серия. Спасибо за помощь. И не тратьте время на преследования. Помните: у нас есть ВАШИ настоящие имена.

Mike Wendland
The I-team
WDIV, Detroit, MI.

Таков был результат:

Phrack World News с гордостью представляет...

Mike Wendland & the I-Team Investigate
"Electronic Gangsters"

Carman Harlan: Мы все слышали о компьютерных хакерах — этих электронных гангстерах, которые пытаются взламывать чужие компьютерные системы. Сегодня вечером, в первой части трёхсерийного специального выпуска News 4 [WDIV-TV, канал 4 в Детройте], Майк Уэндленд и I-Team расследуют, как подобные компьютерные выходки угрожают нашей частной жизни. Майк сейчас расскажет нам о том, что поначалу могло казаться невинным развлечением, а теперь бьёт нас по карману.

Mike Wendland: Итак, Carman и Mort, благодаря СМИ и кино о хакерах и телефонных фрикерах знают почти все. Подключив свои Apple, Atari и Commodore к телефонным линиям, эти электронные энтузиасты разработали новую форму общения — компьютерные доски объявлений (BBS). Сегодня по всей стране насчитывается, вероятно, около 10 000 таких досок для обмена сообщениями, большинство из которых безобидны и полезны. По оценкам, существует около 1 000 пиратских или хакерских досок, где основной деятельностью являются электронное вторжение и преступления [оценки предоставлены Джоном Максфилдом].

[Фрагмент из фильма «Военные игры»]

В таких фильмах, как «Военные игры», компьютерные хакеры изображаются невинными исследователями-любителями, движимыми скорее озорством, нежели злым умыслом. Но сегодня выросло новое поколение хакеров — хакеров, использующих знание компьютеров для совершения преступлений. Хакеры в электронном виде взламывали банки, грабили телефонные компании на миллионы долларов, торговали украденными номерами кредитных карт и через сеть компьютерных досок объявлений обменивались информацией обо всём — от изготовления бомб до организации терроризма.

[Фотография Джона Максфилда]

John Maxfield: Ну что ж, теперь это электронные гангстеры, а не просто электронные исследователи — они самые настоящие гангстеры. Эти хакеры встречаются в электронном пространстве через телефонные линии или компьютерные доски объявлений. Обычно они не встречаются лично, но это полуорганизованная деятельность, похожая на банду, — что-то вроде уличной банды или мотоциклетной группировки.

Mike Wendland: Джон Максфилд из Детройта — ведущий американский «охотник за хакерами». Он сотрудничал с ФБР и различными другими правоохранительными и охранными организациями, помогая поймать десятки хакеров по всей стране, использовавших компьютеры в незаконных

целях. Чтобы выяснить, насколько широко распространились эти электронные гангстеры, мы привлекли Джона Максфилда в качестве консультанта для организации так называемой «ловушечной» доски объявлений [THE BOARD].

Мы написали и разработали специальную программу, позволявшую нам отслеживать поступающие звонки и тщательно контролировать публикуемую информацию. Мы назвали нашу тайную операцию «The Board» и дали знать в хакерском подполье, что для «элитных хакеров» открылась новая доска объявлений. После этого мы просто сидели и наблюдали за потоком звонков.

В общей сложности наша «ловушечная» доска проработала около полутора месяцев — 24 часа в сутки, 7 дней в неделю. Мы получили буквально сотни звонков от хакеров со всего побережья в возрасте от 17 до 43 лет. При всём своём разнообразии они имели одну общую черту: все они искали способы обмануть систему.

Хакеры представлялись псевдонимами или никами — как радиооператоры в эфире, — называя себя Ax Murderer, Big Foot и Captain Magic. Они оставляли сообщения на самые разные сомнительные темы: например, один хакер рассказал, как тайно прослушивать радиопереговоры служб борьбы с наркотиками. Нью-йоркский хакер под ником The Jolter обменивался информацией о бесплатных международных звонках с использованием похищенных кодов доступа, а многие другие предлагали номера кредитных карт для незаконных покупок за чужой счёт.

John Maxfield: Эти дети торгуют номерами кредитных карт через компьютерные доски объявлений примерно так же, как обменивались бы бейсбольными карточками в школе. За последние несколько лет мы наблюдаем череду хакерских банд под руководством взрослого — этакого мозгового центра, который держится в тени и сбывает товары, которые дети заказывают с помощью краденых кредитных карт.

Mike Wendland: Затем появились злобные сообщения, способные причинить серьёзный вред. Repo Man из Западной Вирджинии оставил послание с точными инструкциями о том, как взломать больничный компьютер в районе Чарлстона, Западная Вирджиния.

[Фотография больницы]

Именно туда ведёт этот номер — в Charleston Area Medical Center. Мы немедленно уведомили больницу о том, что её компьютерная безопасность была нарушена. Через пресс-секретаря больница сообщила, что хакер действительно взломал её компьютер и изменил платёжные записи. Меры безопасности были немедленно ужесточены, и началось расследование. Хакера поймали; он согласился возместить ущерб. Однако Максфилд считает, что «большинство подобных взломов так и остаются нераскрытыми».

John Maxfield: Когда речь заходит об электронном компьютерном вторжении — это идеальное преступление. Всё делается анонимно, всё идёт по проводам, нет следов ног, нет отпечатков пальцев, нет пятен крови, нет дымящегося ствола, вообще ничего. Вы можете даже не знать, что система была взломана.

Mike Wendland: Наш опыт с «ловушечной» доской объявлений неожиданно и резко оборвался. Наше прикрытие было раскрыто, когда хакеры каким-то образом получили доступ к конфиденциальным записям телефонной компании. В результате последовали домогательства и угрозы, которые породили серьёзные вопросы о том, насколько в действительности частными являются наши якобы личные данные. Об этом — завтра. [Подробнее о том, как было «раскрыто» их прикрытие, — в PWN, выпуск 7/Часть Первая, «Maxfield наносит удар снова». Хе-хе-хе-хе.]

Mort Crim: Значит, это уже не просто дети, развлекающиеся ради забавы. Но кто же такие хакеры?

Mike Wendland: Я бы сказал, большинство из них — подростки. Наше расследование позволило связать с этим районом около 50 из них из числа наиболее активных, но большинство очень молоды.

Mort Crim: Это уже далеко за пределами простого вандализма!

Mike Wendland: Да.

Небольшое примечание между выпусками: «THE BOARD» организовали Майк Уэндленд и Джон Максфилд. Carman Harlan и Mort Crim — телеведущие новостей.

Кроме того, если кого-то интересует тупость Майка Уэндленда: он засветил на экране сообщение с номером телефона больницы, Bad Subscript нажал паузу на видеомагнитофоне и зафиксировал номер. Желающие — обращайтесь к Bad Subscript, Ctrl C или ко мне.

Часть вторая

Carman Harlan: Сегодня вечером во второй части специального выпуска News 4 [WDIV-TV, канал 4 в Детройте] Майк Уэндленд и I-Team рассказывают о том, как они организовали ловушечную доску объявлений, чтобы собрать компромат на этих хакеров-преступников. Майк сейчас расскажет нам, что собранная информация оказалась не единственной вещью, которую они получили.

Mike Wendland: Всё верно, Carman и Mort. Наша так называемая ловушечная доска объявлений получила сотни звонков от хакеров со всей Америки и даже из Канады. Они предлагали краденые кредитные карты и рассказывали, как в электронном виде взламывать секретные правительственные компьютеры. Но наше расследование внезапно прервалось, когда наша ловушка сама оказалась в ловушке. Прикрытие было раскрыто, когда хакер обнаружил, что этот человек — эксперт по компьютерной безопасности Джон Максфилд — является консультантом I-Team в ходе расследования. Максфилд специализируется на отслеживании хакеров и сотрудничал с ФБР и различными другими полицейскими и охранными ведомствами. Хакер раскрыл нашу ловушечную доску, раздобыв якобы конфиденциальные телефонные записи Максфилда.

John Maxfield: И в процессе этого он обнаружил настоящий номер компьютера. Мы использовали другой телефонный номер с переадресацией на истинный номер — он вычислил его и позвонил, обнаружив, что попал на ловушечную доску.

Mike Wendland: Но хакер не остановился на разоблачении ловушки: вместо этого он разместил копии конфиденциального телефонного счёта Максфилда на других хакерских досках объявлений по всей стране.

John Maxfield: Началось преследование: все люди из моего телефонного счёта получили звонки от хакеров. В некоторых случаях были также похищены их телефонные записи, их друзья и родственники получали звонки от хакеров. Происходило всевозможное другое преследование: мне позвонила служба общепита из Лос-Анджелеса с вопросом, куда доставить 500 фунтов тыкв. Некоторые из этих детей разгуливают с оружием, несколько человек угрожали приехать в Детройт и застрелить меня и Майка Уэндленда.

Mike Wendland: Представитель Michigan Bell заявил, что брешь в системе безопасности, повлёкшая утечку конфиденциальных записей Максфилда, не имела прецедентов.

Phil Jones (MI Bell): Я думаю, как компания мы очень обеспокоены, потому что прилагаем большие усилия для защиты конфиденциальности данных клиентов. [Ну да, конечно.]

Mike Wendland: Хакер, добравшийся до конфиденциальных телефонных записей Максфилда, находится далеко от Мичигана — он живёт в Бруклине, Нью-Йорк, и действует под ником Little David [Bill From RNOC]. По его словам, получить конфиденциальные записи у Michigan Bell или любой

другой телефонной компании — детская игра. Little David — ему 17 лет. Он отказался появляться перед камерой, но признал, что выманил записи у телефонной компании, просто представившись Максфилдом. По его словам, он также продавал пиратские коды доступа к международной связи и конфиденциальную информацию, полученную путём взлома потребительских кредитных файлов T.R.W. Little David утверждает, что среди его клиентов есть скип-трейсер — частный детектив из Калифорнии, специализирующийся на поиске пропавших людей. Максфилд, в свою очередь, говорит, что его собственные данные подтверждают слова Little David.

John Maxfield: Насколько я могу судить, скип-трейсер использовал хакера — этого 17-летнего парня — для установления местонахождения людей, которых ему платили найти. Он делал это, получая доступ к данным кредитного бюро для частного сыщика. Это является нарушением частной жизни, но, по моим сведениям, этот парень получал плату за свои услуги.

Mike Wendland: На Лонг-Айленде в Нью-Йорке телефонные записи Максфилда были также размещены на доске объявлений, которую спонсирует Эрик Корли, издатель хакерского бюллетеня [журнал 2600]. Корли не отрицает домогательств, которым подвергся Максфилд.

Eric Corley: Любая группа может преследовать любую другую группу; отличие хакеров состоит в том, что они умеют использовать определённые технологии для этого. Если разозлить злонамеренного хакера, можно только гадать, что он может натворить.

Mike Wendland: Что может случиться? Ну, помимо того что хакеры получат номер вашей кредитной карты или спишут что-то с вашего счёта, известны случаи, когда они изменяли кредитные рейтинги людей. Это действительно серьёзно! А завтра вечером мы услышим о хакерской философии, согласно которой любая существующая информация о вас является добычей.

Mort Crim: «1984» в 1986-м.

Mike Wendland: Именно так!

Часть третья

Carman Harlan: Специальный выпуск News 4 [WDIV-TV, канал 4 в Детройте]: Майк Уэндленд и I-Team смотрят, как эти хакеры выходят из-под контроля.

Mike Wendland: Проблема хакеров уже не ограничивается простыми проказами: бессовестные хакеры не только вторгаются в вашу частную жизнь, но и опустошают ваши кошельки. Наглядный пример — ваши телефонные счета: поскольку американские телефонные компании давно стали мишенью компьютерных хакеров и воров, мы платим больше, чем должны. По словам экспертов, компании дальней связи теряют десятки миллионов долларов в год из-за этих самопровозглашённых «телефонных фрикеров».

Например, в Лансинге Мичиганская ассоциация государственных служащих получила телефонный счёт почти на триста двадцать одну тысячу долларов — за звонки, незаконно списанные хакерами с её кредитной карты. Такие жертвы редко обязаны оплачивать эти счета, поэтому хакеры утверждают, что их пиратство — невинное развлечение.

Phil Jones (Ml Bell): Ничто не может быть дальше от истины: это становится весьма дорогостоящим развлечением. Дело в том, что большинство клиентов, которые платят свои счета вовремя и пользуются нашими услугами законно, в итоге отказываются от них после получения такого счёта.

Mike Wendland: Это ещё не всё: хакеры регулярно вторгаются в нашу частную жизнь, оставляя на досках объявлений пиратские номера кредитных карт и инструкции о том, как взламывать

электронные банки данных. Тысячи таких электронных центров сообщений существуют по всей стране, большинство из которых управляются подростками.

John Maxfield: Нет ни правоохранительного контроля, ни родительского надзора — они предоставлены сами себе и могут делать всё что угодно. Так что немногие плохие, которые умеют воровать и совершать компьютерные преступления, обучают остальных.

Mike Wendland: Хакерам практически нет ничего недоступного — от банкоматов и банков до внутренних телефонных систем Белого дома. Хакеры нашли способы обойти их все; у хакеров есть даже своего рода собственное подпольное издание, которое рассказывает им, как это делать.

[Крупный план издания]

Оно называется 2600 [журнал 2600] — по частоте 2600 герц, которую телефонные фрикеры использовали для обхода тарификационного оборудования телефонных компаний. Там рассказывается, как находить номера кредитных карт и конфиденциальные записи в мусорных баках, взламывать частные мейнфреймы, получать доступ к компьютерам авиакомпаний и разыскивать финансовую информацию о других людях через крупнейшее кредитное бюро страны — TRW. Журнал 2600 издаётся в полуразвалившемся старом доме на дальнем конце Лонг-Айленда, Нью-Йорк, этим человеком — Эриком Корли. Он утверждает, что хакеры — не электронные гангстеры.

Eric Corley: Мы предпочитаем называть их борцами за свободу. Хакеры — истинные индивидуалисты компьютерной революции: они идут туда, куда им запрещают идти, и узнают то, что им не положено знать.

Mike Wendland: Бюллетень Корли поддерживает хакерскую доску объявлений под названием Private Sector. В прошлом году ФБР провело там обыск.

Eric Corley: Им удалось предъявить оператору системы обвинение в незаконном хранении орудия взлома в виде компьютерной программы.

Mike Wendland: Тем не менее доска объявлений по-прежнему работает. Корли возмущён подозрениями в том, что хакеры причастны к преступной деятельности.

Eric Corley: Хакеры — это не те люди, которые рыщут в поисках кредитных карт и воруют товары. Это обычное воровство. Хакеры — это те, кто исследует. По сути, мы говорим о том, чтобы больше знаний стало доступно большему числу людей. Это сделает жизнь лучше для всех.

Mike Wendland: Он утверждает, что хакеры по-своему действительно защищают наши права, обнажая наши уязвимости. Ну что ж, хакеры, возможно, и обнажают наши уязвимости, но они также вторгаются в нашу частную жизнь. Их деятельность действительно обострила весь вопрос о конфиденциальности, поднятый огромными файлами, которые теперь хранятся в электронных банках данных. Значительная часть информации, которую мы считаем личной и конфиденциальной, нередко оказывается доступной всему миру.

Original transcript gathered and typed by

Ctrl C & Bad Subscript

Major editing by Knight Lightning

На домашнем фронте — 25 декабря 1986 г.

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                                     PWN
PWN                        <-=*} Phrack World News {*=->                PWN
PWN                                                                     PWN
PWN                              Issue IX/Part Two                      PWN
PWN                                                                     PWN
PWN                      Compiled, Written, and Edited by               PWN
PWN                                                                     PWN
PWN                              Knight Lightning                       PWN
PWN                                                                     PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

С наступающими праздниками всех от имени Phrack Inc. и Metal Shop Private!

Ну вот, мы снова добрались до этого времени года, и совсем скоро нас накроет новая волна самопровозглашённых хакеров, получивших модемы в подарок на Рождество.

Несколько важных дат:

• 17 ноября 1986 г. — 1-я годовщина Phrack Inc.
• 2 января 1987 г. — 1-я годовщина перехода Metal Shop в статус ПРИВАТНОЙ BBS.
• 10 января 1987 г. — 1-я годовщина Metal Shop AE, ныне известной как Quick Shop.
• 25 января 1987 г. — 1-я годовщина Phrack World News.

Голосовой почтовый ящик Phrack Inc./Metal Shop Private снова в работе. Если у вас есть вопрос для Taran King, Cheap Shades или меня лично, а обычными способами связаться не получается — оставьте нам сообщение на VMS.

Благодаря стараниям Oryan Quest, в одном из ближайших выпусков Phrack Pro-Phile будет материал о Стиве Возняке.

Подготовка к Summer Con '87 уже ведётся. Конференция пройдёт в Сент-Луисе, штат Миссури, в последнюю неделю июня. Её организаторами выступают TeleComputist Newsletter, Phrack Inc. и Metal Shop Private. Forest Ranger отвечает за планирование и вкладывает немало собственных средств в аренду необходимых конференц-залов. Вход на Summer Con '87 будет платным — $10 у двери. Если вы планируете посетить конференцию, то в знак доброй воли и ради скидки 50% можете заранее отправить $5 по адресу:

```
J. Thomas
TeleComputist Newsletter
P.O. Box 2003
Florissant, Missouri 63032-2003
```

Письма редактору и любые другие материалы для TeleComputist можно направлять по тому же адресу. Связаться с TeleComputist также можно через Easylink по номеру 62195770, MCI Telex — 650-240-6356, CIS — 72767,3207 и PLINK — OLS 631. В первую очередь пробуйте MCI и Easylink.

Особо добавить нечего… так что продолжайте учиться и старайтесь не нарываться на неприятности.

:Knight Lightning

Внимание, компьютерные хакеры! — Сенат принял Закон о компьютерном мошенничестве и злоупотреблениях

2 октября 1986 г. Сенат США единогласно принял Закон о компьютерном мошенничестве и злоупотреблениях 1986 года. Законопроект S. 2281 предусматривает штрафы до $500 000 и/или лишение свободы на срок до 20 лет за взлом компьютеров государственных органов или финансовых учреждений.

Только федеральное правительство эксплуатирует более 18 000 средних и крупных компьютеров примерно в 4 500 различных местах. По оценке Управления по оценке технологий, инвестиции правительства в компьютерную технику за последние четыре года составили порядка $60 миллионов. По прогнозу Администрации общих служб, к 1990 году федеральные ведомства будут использовать от 250 000 до 500 000 компьютеров.

В 1984 году интерес законодателей к проблеме компьютерного мошенничества значительно возрос благодаря докладу рабочей группы Американской ассоциации юристов по компьютерным преступлениям. Согласно докладу, основанному на опросе 1 000 частных организаций и государственных учреждений, сорок пять процентов из 283 респондентов пострадали от той или иной формы компьютерного преступления, а более 25 процентов понесли финансовые потери, общая сумма которых за один двенадцатимесячный период составила, по оценкам, от $145 миллионов до $730 миллионов.

Для решения этой проблемы в 1984 году Сенат и Палата представителей приняли первый компьютерный закон (18 U.S.C. 1030). В начале этого года обе палаты внесли законопроекты о расширении и изменении данного закона.

В соответствии с текущим законопроектом, который, как ожидается, на следующей неделе подпишет президент Рейган, санкции будут применяться к тому, кто сознательно или умышленно осуществляет несанкционированный доступ к компьютеру либо превышает авторизованный доступ и при этом:

1. Получает из государственных компьютеров сведения, касающиеся национальной обороны и внешней политики.

2. Получает информацию из финансовых записей финансовых учреждений.

3. Нарушает работу государственного компьютера в каком-либо департаменте или ведомстве, предназначенного исключительно для использования правительством США.

4. Получает что-либо ценное, за исключением случаев, когда объектом мошенничества и предметом получения является только использование самого компьютера.

5. Изменяет, повреждает или уничтожает информацию в любом федеральном компьютере, представляющем общественный интерес, либо препятствует авторизованному использованию такого компьютера или информации.

По закону лицо будет признано виновным в компьютерном мошенничестве, если причинённый им ущерб за любой однолетний период составит $1 000 или более.

В зависимости от тяжести правонарушения предусмотрены штрафы: до $100 000 за проступок (misdemeanor), $250 000 за тяжкое преступление (felony), $500 000 если преступление совершено организацией, а также лишение свободы на срок до 20 лет.

Законопроект также запрещает торговлю паролями и иными сведениями из компьютеров, задействованных в межштатной или международной торговле. Эта часть закона позволяет федеральным прокурорам преследовать пиратские доски объявлений и аналогичные ресурсы, поскольку действие закона распространяется на бизнес-компьютеры, онлайн-сети, а также новостные и информационные онлайн-сервисы — всё это относится к сфере межштатной торговли.

Информация предоставлена

P - 8 0 S y s t e m s

Новости GTE — 20 декабря 1986 г.

«GTE разработала высокоскоростной мультиплексор GaAs, объединяющий четыре канала передачи данных»

В стремлении достичь скорости передачи данных в несколько гигабит в секунду GTE Labs (Уолтем, Массачусетс) сочетает высокую ёмкость волоконной оптики со скоростью схем на арсениде галлия. Исследовательское подразделение GTE разработало мультиплексор GaAs, способный объединять четыре канала передачи данных — каждый со скоростью 1 гигабит в секунду — в один канал. Кроме того, GTE недавно разработала технологию под названием MOVPE (металлоорганическая газофазная эпитаксия) для эффективного выращивания тонкоплёночных кристаллов GaAs.

Новые устройства должны сыграть важную роль в будущих системах связи, которые будут предполагать подключение домов и офисов к высокоёмким волоконно-оптическим кабелям через телефонные коммутационные центры. Скорость передачи данных по таким кабелям может достигать 20 гигабит в секунду. Помимо стандартных компьютерных данных, они способны поддерживать множество видеоканалов, каждый со скоростью почти 100 мегабит в секунду. Мультиплексоры GaAs, вероятно, окажутся единственными устройствами, достаточно быстрыми для соединения домов и офисов через эту волоконно-оптическую сеть. В будущих суперкомпьютерах [некорректное употребление термина — прим. ред.] эти мультиплексоры также найдут применение для высокоскоростной волоконно-оптической передачи данных между различными платами компьютера, заменяя медные провода. Благодаря высокой скорости волоконно-оптического канала подобные технологии могут использоваться даже для межчипового взаимодействия.

GTE сообщила, что прототип мультиплексора GaAs готов, а финальная версия должна быть завершена менее чем через год.

Комментарий: И пока GTE строила мультиплексоры на гигабит в секунду, Bell Labs в AT&T всё ещё экспериментирует с нейронными сетями из мозга улиток…

Источник: журнал Byte, декабрь 1986, стр. 9
Набрано и откомментировано: Mark Tabas

Технический журнал LOD/H

The Legion Of Doom/Hackers Technical Journal — бесплатный электронный информационный бюллетень, основная цель которого — расширять знания тех, кто интересуется такими темами, как телекоммуникации, передача данных, компьютерная и физическая безопасность/незащищённость, а также различными техническими аспектами телефонной системы.

Все статьи являются полностью оригинальными, если не указано иное. Все источники информации для конкретной статьи перечислены во введении или заключении статьи. Неоригинальные, плагиатные или содержащие недостоверную информацию материалы не принимаются. Статьи принимаются от любого, кто отвечает этим критериям. Редакция не зависит от читателей в плане материалов, поскольку основными авторами являются члены LOD/H и избранный круг других лиц,

однако любой желающий может присылать статьи.

Фиксированной даты выхода номеров нет, поскольку перед читателями нет ни денежных, ни юридических обязательств. Предполагается, что номера будут выходить каждые 2–3 месяца — то есть 4–6 выпусков в год при условии продолжения работы, что авторы намерены делать.

Доски объявлений, спонсирующие LOD/H TJ:

```
Atlantis
Digital Logic Data Service
Hell Phrozen Over (HPO)
Metal Shop Private
Private Sector
The Shack //
```

Первый номер будет включать следующие материалы:

• Введение в LOD/H Technical Journal и оглавление
• Редакционная статья: «Является ли закон сдерживающим фактором для компьютерных преступлений?» — Lex Luthor
• Local Area Signalling Services (LASS) — The Videosmith
• Выявление и преодоление физической защиты и систем обнаружения вторжений. Часть I: Периметр — Lex Luthor
• Traffic Service Position System (TSPS) — The Marauder
• Взлом DEC TOPS-20: введение — Blue Archer
• Сборка собственного Blue Box (со схемой) — Jester Sluggo
• Процессы разведки и допроса — Master Of Impact
• Внешняя распределительная петля. Часть I — Phucked Agent 04
• Внешняя распределительная петля. Часть II — Phucked Agent 04
• Каталог LOH Telenet: обновление №4 (09.12.86), часть I — LOH
• Каталог LOH Telenet: обновление №4 (09.12.86), часть II — LOH
• Новости и заметки о сетях — «Редакция»

Итого 13 файлов.

На этом предварительный обзор завершён. Ожидается, что бюллетень выйдет до 1 января 1987 г. — следите за новостями!

```
Информация предоставлена
Lex Luthor & The Legion Of Doom/Hackers Technical Journal Staff
```

Слухи в Техасе разбушевались — 24 декабря 1986 г.

Помните всю ту шумиху вокруг версии о том, что Sir Gamelord — это Videosmith?

Вот как это было на самом деле.

Всё началось на конференц-мосту, где группа людей — в том числе Evil Jay, Line Breaker (который косвенно и положил этому начало) и Blade Runner — вели беседу.

Line Breaker рассказывал историю о том, как Videosmith якобы был федеральным агентом, как он сдал всех на фрик-конференции (или что-то в этом роде), и как сам Line Breaker с несколькими другими людьми позвонили Videosmith, притворившись федами, и вынудили его признаться в содеянном.

Blade Runner был страшно зол на Sir Gamelord (который незадолго до этого пытался захватить P.H.I.R.M. — группу Blade Runner). В качестве ответного удара и наслушавшись этой клеветы на

Videosmith, Blade Runner начал рассказывать людям, что Sir Gamelord и есть Videosmith. С тех пор истории обрастали всё большими преувеличениями, но в действительности произошло именно это.

[Говорят, в Техасе всё крупнее… видимо, это касается и чуши!]

```
Информация предоставлена Evil Jay
```

Крэкер исчезает — 27 декабря 1986 г.

Вокруг исчезновения некоего Билла Лэндрета, известного под псевдонимом The Cracker, ходят самые разные слухи и истории.

Билл Лэндрет — автор книги «Out Of The Inner Circle» о хакерах, изданной несколько лет назад.

По данным газетных статей в районе Сан-Франциско, Билл работал над какой-то компьютерной программой в доме своего друга. Друг ненадолго вышел, а когда вернулся, обнаружил на экране кучу мусора и сообщение о самоубийстве.

На Ripco BBS было опубликовано сообщение о Билле Лэндрете: говорилось, что он исчез и снова разыскивается ФБР. В сообщении просили всех, кто поддерживает контакт с Биллом, передать ему просьбу связаться с «друзьями».

Большинство нынешних сообщений — пустые слухи. Возможно, продолжение этой истории появится в следующем выпуске PWN.

```
Информация предоставлена
The Prophet / Sir Frances Drake / Elric Of Imrryr
```

U.S. Sprint оплошала — 24 декабря 1986 г.

По материалам Fort Lauderdale Sun Sentinel

«Ему пришёл счёт на 1 400 страниц!»

В Монтрозе, штат Колорадо, Брэд Суитцер решил, что посылка от компании U.S. Sprint Long Distance — это ранний рождественский подарок, пока не вскрыл её и не обнаружил внутри телефонный счёт на 1 400 страниц.

Счёт на $34 000 был доставлен к порогу Суитцера в понедельник. Он позвонил в денверский офис U.S. Sprint, где представители компании заверили его, что он «избавлен от крючка» (Off the Hook). Представитель U.S. Sprint пояснил, что Суитцер по ошибке получил собственный счёт U.S. Sprint за дальние переговоры.

```
Набрано для PWN: The Leftist
```