Phrack RU issue 005

Русская версия Phrack, выпуск 005. Полный текст статей с кодом и таблицами.

Темы выпуска: сети, маршрутизация, TCP/IP, Cisco, телефония и телеком-инфраструктура; Unix/Linux, BSD, Windows NT и администрирование систем; культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; социальная инженерия, carding, физический доступ и практические схемы.

Материалы выпуска: Intro to Phrack V!; Phrack Pro-Phile II: Broadway Hacker; Взлом системы DEC-10; Рукопашный бой; Digital Multiplex System (DMS) 100; Новая анархистская игрушка!; Wide-Area Networks, часть 1; Short-Wave Radio Hacking; Mobile Telephone Communications; Phrack World News IV, часть 1; Phrack World News IV, часть 2; Закат фрикинга во Флориде: история Teltec.

Intro to Phrack V!

Дата: 18 апреля 1986 года
Автор: Taran King, sysop of Metal Shop Private

Добро пожаловать в Phrack Inc. Issue Five. Благодаря вам, читателям, у нас появилась хорошая аудитория, и мы продолжим выпускать новые issues. Ваша поддержка была фантастической, и я рад сказать, что всё больше людей, которые действительно знают своё дело, выходят из тени и пишут philes для распространения вместе с Phrack Inc.

Недавно я получил письмо от юридической фирмы в New York с жалобой на phile о Master Lock Picking из Issue One of Phrack Inc. Его написали Ninja NYC и Gin Fizz, оба из The Punk Mafia. Это был первоклассный phile, и он работал... но именно это и стало проблемой. Они хотели, чтобы я что-то сделал с указанным материалом. Подробности этой истории можно прочитать в данном выпуске Phrack World News.

Тем не менее позвольте мне заявить здесь: все philes, распространяемые вместе с Phrack Inc., всего лишь передаются нами, и мы не несём ответственности за содержание philes больше, чем сами читатели. Philes являются ответственностью авторов. Я не пытаюсь переложить вину на Ninja NYC и Gin Fizz, см. письмо, которое я написал фирме с изложением своей позиции, но нас не будут обвинять в преступлении, которое не было совершено.

Ждите ещё многих выпусков Phrack Inc. в далёком будущем.

```
TARAN KING
Sysop of Metal Shop Private

#1      Phrack V Intro by Taran King
#2      Phrack Pro-Phile of Broadway Hacker by Taran King
#3      Hacking Dec's by Carrier Culprit
#4      Hand to Hand Combat by Bad Boy in Black
#5      DMS-100 by Knight Lightning
#6      Bolt Bombs by The Leftist
#7      Wide Area Networks Part 1 by Jester Sluggo
#8      Radio Hacking by The Seker
#9      Mobile Telephone Communications by Phantom Phreaker
#10-12  Phrack World News IV by Knight Lightning
```

Phrack Pro-Phile II: Broadway Hacker

Автор и составитель: Taran King
Дата: 5 апреля 1986 года

Добро пожаловать в Phrack Pro-Phile II. Phrack Pro-Phile создан, чтобы приносить вам, пользователям, информацию о старых или очень важных и спорных людях. В этом месяце я представляю вам одного из самых controversial users нашего времени и прежних дней:

```
Broadway Hacker
```

Broadway Hacker — sysop of The Radio Station, phreak/hack bulletin board в Brooklyn, N.Y., area code 718.

Личные данные

```
Handle: Broadway Hacker
Call him: Mike
Past handles: None, except his sysop handle, "The Program Director"
Handle origin: Thought it up while on Compu-Serve
Date of birth: April 22, 1965
Age at current date: 20 years old
Height: 6'2"
Weight: About 150 lbs.
Eye color: Green/Hazel
Hair color: Brown
Computer: Commodore 64 with 3 disk drives and 300/1200 baud modem
Sysop/Co-Sysop of: The Radio Station, The Night Stalker
```

Broadway Hacker начал в мире BBS в конце 1983 года, когда впервые получил модем. 23 марта 1985 года **The Broadway Show**, его первая bulletin board, была запущена в BBS world. Она началась с одного disk drive на 300 baud и невероятно выросла. Изначально это была phreak board, как и сейчас.

Свой C-64 computer он получил в начале 1985 года. Разные участники elite world, включая King Blotto, Lex Luthor и Dr. Who, заходили на его board и сделали её той запоминающейся board, какой она была до смены формата.

Его phreak experience начался в 1981 году через CB radios, когда один CB'er дал ему code over the line. Среди запомнившихся phreak boards, на которых он был, были Blottoland, The AT&T Phone Center of 312 и Dark Side of the Moon of 818. Основную заслугу в своих phreak knowledge он отдаёт conferences.

Mike работает на очень большой radio station. На работе о его phreaking не знают. Он не особенно интересуется programming, кроме модификации The Radio Station.

Сейчас у Broadway Hacker нет времени для hacking. Broadway иногда посещает TAP meetings в New York, хотя раньше был постоянным участником. Он посетил TelePub meeting 1986 года в New York, где должна была решаться судьба TAP Magazine.

Broadway лично встречал разных phreaks, включая BIOC Agent 003, Lex Luthor, Dr. Who, King Blotto, Cheshire Catalyst, The Sprinter, The Saint, Micro Ghoul, людей из 2600 Magazine, Paul Muad'Dib и TUC. Были и другие, но он не смог вспомнить их в 9:00 AM EST.

Он сделал принципом не вступать в группы, хотя в прошлом его приглашали во многие.

Интересы

```
Traveling
Radio
Telecommunications: modeming, phreaking
Trashing
Meeting other phreaks
BBS'ing
Running The Radio Station
```

Любимые вещи Broadway Hacker

```
Women: No names mentioned but yes...
Cars: Fieros
Foods: Ray's Pizza (West 11th and 6th Ave.), Steve's Ice Cream
Music: Any top 40 groups in general
```

Самые запомнившиеся события

```
Getting almost kidnapped by a gay bellhop in Denver
Getting stranded in California
```

Люди, которых стоит упомянуть

```
Sigmund Fraud
```

Sigmund Fraud — up-and-coming phreak, который многому научился за короткое время.

Broadway Hacker хочет, чтобы все знали: он больше совсем не participates in conferences, потому что conferencing деградировал со старых дней и теперь в основном стал местом для сбора gossip.

Надеюсь, вам понравился этот phile. Ждите новых Phrack Pro-Philes в ближайшем будущем. А теперь регулярный вопрос, который задают всем interviewees:

Из общей массы phreaks, которых вы встречали, считаете ли вы большинство phreaks, если вообще кого-то, computer geeks?

По большей части Broadway говорит: «No».

Спасибо за ваше время, Mike.

```
TARAN KING
SYSOP OF METAL SHOP PRIVATE
```

Взлом системы DEC-10

Автор: Carrier Culprit

Исправленное издание....

Примечание: Этот файл был распространён по ошибке — он не был завершён. Перед вами новое исправленное издание. Если вы видите мой файл на каком-либо AE, BBS, Catfur и это не исправленное издание — пожалуйста, попросите сисопа удалить его. Спасибо.

Часть I: Вход в систему и основные команды

Примечание: Сисопы могут скачать этот файл, но пожалуйста сохраняйте соответствующие указания об авторстве.

Добро пожаловать в мир взлома DEC-10!

Есть один способ распознать DEC-10: вы увидите приглашение ".". Сначала появится небольшое приветственное сообщение, похожее на приветствие при входе на BBS. Например:

```
NIH Timesharing

NIH Tri-SMP 7.02-FF  19:57:11 TTY12
system 1378/1381/1453 Connected to Node Happy(40) Line # 13
Please LOGIN
.
```

Итак, вы уже дошли до того, что нашли DEC (Digital Equipment Corp). Вам необходимо знать формат входа в систему.

[Формат входа]

У пользователей есть номера, называемые PPN — «Номер проекта/программы» (Project/Program Number). Формат номера PPN: [X,X]. Первое число — номер проекта, второе — номер программы.

Например:

```
.Log 12,34

 Job 64 NIH 7.01 KL 64-UC TTY12
Password:
```

Пароль может содержать от 1 до 8 символов: цифры, инициалы или что-то подобное. Попробуйте подумать: если бы я был пользователем, каким был бы мой пароль? Сомневаюсь, что этот метод сработает, но попробовать стоит.

Допустим, вы впервые на системе DEC-10. Если хотите узнать больше о системе и её командах, введите:

```
.Help
```

Это позволит узнать немного больше о системе. Вам сообщат, как получить информацию по конкретной теме. Там может быть также указан номер голосового дозвона на случай возникновения трудностей. Этот голосовой номер может пригодиться, если вы умеете убедительно болтать. Обычно команда Help предлагает обратиться к «руководству по системе DEC-10» для получения дополнительной информации.

Если вам нужен список доступных команд, введите:

```
.Help *
```

Вы получите список команд — их слишком много, чтобы перечислять здесь, но вы узнаете их, когда выполните Help *.

После вывода всех команд система покажет, как войти в систему. Демонстрационного аккаунта вам не дадут, но пример входа будет примерно таким: «Команда Login используется для доступа к системе разделения времени Decsystem-10.»

Для входа введите пару номеров проекта и программиста:

```
LOGIN XXX,XXXX
```

Система запросит пароль. Если ваш PPN или пароль неверны, вы увидите сообщение:

```
Enter Project,programmer #xxx,xxxx
Password:
```

На этом с форматом входа всё.

Есть и другие полезные команды, доступные даже без аккаунта. Вы можете получить доступ к Decnet, о котором я расскажу позже — это очень интересно для хакера.

Также существует команда "Help Phone". Она выводит список телефонных номеров различных служб, связанных с DEC. Например:

```
.Help Phone

DCRT/CCB/DECsystem-10 Information Phone numbers (4/86)

Recorded message       Dial xxx-xxxx
Dec-10 operator        Dial xxx-xxxx
Dec-10 staff           Dial xxx-xxxx
Terminal Repairs       Dial xxx-xxxx
Classes/Courses        Dial xxx-xxxx
Users Area Phone       Dial xxx-xxxx
Project Control Office Dial xxx-xxxx

NOTE:This is the same area code as the Decsystem.
```

Наиболее важными для вас будут номера оператора DEC-10 и персонала DEC-10.

Самая важная команда на DEC-10 — "Systat": она выводит список PPN, время, выполняемое задание и время работы. Получив PPN, можно начинать подбирать пароли. Использование systat — самый простой и лёгкий способ узнать PPN. Проще набирать "SY" вместо "Systat" — это одно и то же, просто сокращение.

Вот небольшой пример того, что вы получите, выполнив команду "sy":

```
.SY

Status of Brown University 603A at 11:52:33 on 29-Jan-86

Uptime 187:12:22, 80%Null time = 80%idle + 0%Lost
7 Jobs in use out of 128. 19 logged in 4 detached out of 89   (LOGMAX)
Job    Who    What    Run Time

 1    [OPR]   OPSER     3:22
 2    [OPR]   DIALOG    1:29
 3    [OPR]   BATCON    4:01
 4    [OPR]   SYSINF   51:13 01
 5    24,2    SYSTAT    4:52
 6  2332,21   DIRECT    2:22
 7    32,22   SYSTAT    8:19
```

Вместе с вышеуказанным будет и ещё кое-что, но вдаваться в это не нужно — вот почему я это не включил. Также будет больше подзаголовков помимо Run Time, Who, What и Job — не заморачивайтесь и на этом.

Всё достаточно наглядно. Для начинающих поясню: столбец Job не важен. Столбец Who показывает, кто находится в системе. [OPR] означает оператора, а числа вроде 24,2 — обычные пользователи с PPN. Следующий столбец — "What" — показывает, что они выполняют или чем занимаются в данный момент. Run Time — время входа в систему, в военном формате. В systat также можно найти: структуры файловой системы, занятые устройства, сегменты высоты и структуру диска. Пока не беспокойтесь об этом.

Итак, вы наконец получили несколько PPN. Следующий шаг — войти в систему с помощью описанной процедуры Log, ввести PPN вида xx,xx и попытаться подобрать пароли.

Ниже приведу список паролей, которые я лично использовал для входа в DEC-10. Если они не подойдут — извините, придётся попробовать свои собственные.

Примечание: Можно также написать небольшую программу, перебирающую различные PPN и пароли.

```
Список паролей--
-----------------------------------
Sex           Dec           Decnet
Games         Test          Dcl
System        Computer      Password
Help          Link          List
Secret        Default       Modem
Account       Terminal      Acsnet
Ppn           Operator      Connect
-----------------------------------
```

Есть ещё много паролей, которые используют люди, — я перечислил лишь наиболее распространённые.

Можно также пробовать случайные пароли: AA, AAB, AB, CC и т.д.

На этом тема входа в систему исчерпана. Я потратил на неё немного больше времени, чем планировал, но поскольку файл будет двухчастным, во второй части я рассмотрю команды, до которых здесь не добрался. Этот файл рассчитан на новичков, так что опытные взломщики DEC уже скучают или заскучают позже.

Примечание: При подключении через Acsnet просто введите AcsDec10 для доступа к DEC. Всё остальное, упомянутое мной при описании входа, по-прежнему актуально.

[В системе]

Допустим, вы наконец вошли в систему после долгих попыток. Вот как это выглядит:

```
.Login 21,34
Password:
```

Примечание: Обычно даётся две попытки ввода PPN и пароля.

DEC представится, сообщив, когда вы в последний раз были в системе, и т.д.

Иногда вход выглядит так:

```
.Log 12,34
JOB 51 NIH 7.01 KL 64-UC TT12
Password:[c/r]
Other jobs detached with same PPN:
Job 34 running SYSTAT in ^C state
Do you want to ATTACH to this job? yes


Attaching to job 34
```

Здесь вы присоединяетесь к незанятому PPN. Когда кто-то другой находится в системе, примерно за 10 минут (максимум 15 минут) до вас он может ввести команду, позволяющую выйти из системы

с возможностью подключиться обратно к этому PPN при повторном входе. Тогда этот человек попадёт именно в то место, где вышел. Если я использовал 'sys' и вышел из системы, я бы использовал команду 'detach'. После этого у пользователя будет 15 минут, чтобы позвонить снова и подключиться к своему PPN. Есть ещё один способ подключиться к аккаунту: если человек долго ничего не вводит, он автоматически выходит из системы, и если вы позвоните в течение 15 минут — сможете подключиться к его PPN.

Примечание: Вам всё равно может потребоваться войти в систему.

Итак, мы в системе после её верификации. Что делать? Для начала ещё раз посмотрим на "systat". Мы замечаем, что ещё один пользователь вошёл в систему, но он находится в "exe" — это значит, что он ничего не делает или отключён. Иными словами, не обращайте на это внимания.

Если захотите сменить пароль, введите:

```
/Password
```

После этого система запросит старый и новый пароль. Однако лучше не трогать пароль, чтобы не быть обнаруженным. Но знать об этом полезно.

Теперь можно посмотреть файлы других пользователей:

```
Dir [*,*]
```

*=Метасимвол (wildcard)

Это покажет файлы пользователей, открытые для общего доступа. Допустим, мы хотим просмотреть чьи-то файлы:

```
Dir [12,11]
```

Если 12,11 — номер интересующего нас пользователя, вводим его в скобках.

Существует много типов файлов. Просматривая чей-то каталог или используя метасимвол, вы можете заметить различные файлы. В большинстве из них встречаются расширения 'txt' или 'exe'.

Для exe вводите:

```
[PPN]filename.exe
```

Для txt:

```
type filename.txt
```

Также встречаются файлы с расширениями: dat, bas, cmd, pcl, bin, hlp и другие.

1. Exe — исполняемые файлы, которые можно запускать из приглашения ".".

2. Txt — текстовые файлы, которые могут содержать информацию, данные и многое другое. Это самые распространённые файлы, которые вы встретите у большинства пользователей с публичным каталогом — и, по моему опыту, наиболее популярные на DEC-10.

3. Bas — файлы на языке Basic; разумеется, их нужно использовать в Basic. Чтобы войти в него на DEC-10, просто введите Run Bas или, если не сработает, просто basic.

Примечание: Файлы Basic используются как обычные файлы Basic — загружайте и запускайте их.

Это наиболее распространённые типы файлов. Освоив их, можно переходить к изучению остальных.

Ещё один способ чтения файлов:

```
File:[*,*]<command>
```

Здесь '*' снова является метасимволом.

[Создание каталога]

Для создания каталога введите в основном приглашении: 'Credir'

Для каталога существует 2 уровня: первый — Class, второй — Tvedit.

Если у нас есть привилегированный аккаунт, мы можем создать двухуровневый каталог:

```
Create Directory:[,,class,tvedit]
```

DEC-10 ответит:

```
Created Dska0:[x,x,class]Sfd/protec:775
Created Dska0:[x,x,class,tvedit]sfd/protec:755
```

x,x — используемый PPN; Dska0 — устройство.

Чтобы дать имя каталогу:

```
/Name:<нужное название>
```

Примечание: Скобки не нужны.

Для защиты каталога:

```
/Protect:<name>
```

Есть и другие команды с '/'; просмотреть их можно с помощью '/help'.

Достаточно о каталогах.

[Привилегии]

Почти каждый хакер, входя в систему, мечтает о привилегированном аккаунте. Имея его, можно создать собственный аккаунт и делать другие полезные вещи. На DEC-10 привилегированный аккаунт почти всегда начинается с '1', например 1,10. Просмотрев состояние системы (sys), проверьте, есть ли там аккаунт вида 1,x. Если есть — начинайте взламывать пароль. Если вы войдёте под '1,2' — ну, это совсем другая история. Хехе. Допустим, вам удалось войти под привилегированным аккаунтом. Для активации привилегий введите 'enable' — вы получите приглашение '$' или '#'. Неважно какое — делать можно всё то же самое.

Допустим, мы хотим создать новый аккаунт:

```
$Build[x,x] or Create[x,x]
```

После этого можно отредактировать этот PPN или, если он новый, задать собственные настройки.

Должен был упомянуть раньше: если вы вошли на аккаунт 1,x — убедитесь, что под ним не авторизован другой пользователь. Если кто-то там есть, он может сменить пароль, но даже если он в 'exe' и, возможно, отключён — рисковать не стоит. Рекомендую заходить поздно вечером, рано утром или в середине дня в учебный день, если вы дома.

Существуют различные уровни привилегий: оператор, wheel и CIA. CIA — наивысший уровень, позволяющий делать всё что угодно. Имея привилегии оператора, можно создать аккаунт и организовать хороший каталог. Это также пригодится при попытке получить доступ к Decnet.

Если вы создали привилегированный аккаунт, введите в основном приглашении:

```
Help Phones <как я упоминал ранее>
```

Вы получите список телефонных номеров, включая номер системного оператора и системного администратора. Обычно они работают с 10:00 до 17:00. Позвоните в это время и попросите руководство пользователя Decsystem. Вас спросят имя, PPN и пароль — будьте готовы. Если спросят, почему вы ещё не получили руководство, скажите, что аккаунт у вас недавно и вас не предупредили о мануале.

Это руководство очень полезно: там есть команды с подробными описаниями, новые возможности, игры и т.д. Не заказывайте руководство в день получения аккаунта — подождите дней четыре, затем звоните. Обычно его отправляют на следующий день, если только операторы не ленятся. Отправка на домашний адрес обычно безопасна, но если нервничаете — попросите отправить в другое место.

[Почтовая подсистема]

Иногда ваш знакомый также имеет аккаунт на том же DEC-10. Если его сейчас нет в системе, отправить ему сообщение не получится. Но есть одна альтернатива — отправить письмо. Для этого нужно знать имя получателя. Для доступа к почте введите:

```
Run Mail
```

Вы получите приглашение 'MailC'. При этом приглашении введите:

```
MailC:Send
```

Затем система задаст вопросы о получателе. Это выглядит примерно так:

```
.Run Mail
MailC:Send

to:Death Hatchet
Subject:Disk Crash
Text:

Yo! My file disk got ruined with //e Writer. See ya.
```

Закончив текст, введите '.done' или '.d' на пустой строке, чтобы указать завершение. DEC-10 ответит:

```
Death Hatchet--Sent
```

...и вернёт вас к приглашению 'MailC'. Если нужно отправить то же сообщение двум людям, сделайте всё как описано выше, но в поле 'to:' введите:

```
To:Death Hatchet,The Rico
```

Единственное отличие — запятая. ОБЯЗАТЕЛЬНО разделяйте два имени запятой, иначе система воспримет их как одно имя. После отправки письма пользователь Death Hatchet получит его при входе в систему. После стандартных приветственных сообщений и статистики последнего сеанса письмо будет автоматически прочитано ему:

```
From:Carrier Culprit             Postmark:20-Mar-86-08:12:27
  to:Death Hatchet
Subject:Disk Crash

Yo! My file disk got ruined with //e Writer. See ya.
```

Затем будут прочитаны другие письма, если они есть. Если нет — просто перейдёт в основное приглашение. Если хотите перечитать письмо — зайдите в раздел почты и введите 'read' вместо send. Вы сможете сохранить его для следующего сеанса или удалить. Иногда почта не появляется при первом входе, поэтому в любом случае зайдите в раздел почты и проверьте.

На некоторых старых системах DEC-10 почта не использовалась — сообщения просто отправлялись напрямую. Почта была добавлена в систему DEC-10 в середине 70-х. Не особенно важно, но стоит знать. Если Run Mail не открывает почтовый раздел — попробуйте 'run mai'. Эта команда используется в некоторых более ранних системах, но обычно система принимает обе.

Никогда не отправляйте угрожающих писем системным операторам — вас отключат и удалят ваш аккаунт. Если всё-таки отправите — рекомендую иметь запасной аккаунт (PPN). На некоторых более новых системах DEC-10 можно пересылать почту, введя 'Frd Mail' при приглашении 'MailC'. Система спросит, куда переслать, их пароль и ваш пароль. Системный оператор проверяет это,

согласует с обеими сторонами и оставит письмо с подтверждением. Эта функция ещё тестируется, но я видел её в работе на некоторых DEC-10 в зоне 714.

[Информация]

Это ещё одна полезная команда. Она даёт информацию о заданиях и PPN — паролей не предоставляет, но позволяет получить неплохую статистику. Введите 'info' или 'help info', и получите список примерно такого вида:

```
To look at one of the following do-- Info XXXX

  Switch                          Meaning
  ======                          =======
    .                             Information on your job
  [??,??]                         Information on that PPN
  ALL                             Information on all PPN's
  ALL:LOPR                        Information on all Local Operator Jobs(1,2)
  ALL:OPR                         Information on all Operator jobs (1,2)
  ALL:ROPR                        Information on all Remote Operator jobs
  ALL:Users                       Information on all users
  Batch                           Information on all batch jobs
  Detached:ALL                    Information on all Detached PPN'S
  Detached:OPR                    Information on all Detached Operator jobs
  Detached:Users                  Information on all Detached users
  Detached:LOPR                   Information on all Local Operator jobs
```

Список продолжается. Для полного списка введите 'Help Info'. Команда также предоставляет информацию о дисковых устройствах, каталогах и другом. Некоторые системы DEC-10 не поддерживают это, но большинство — поддерживают.

'1,2' рядом с операторами — это аккаунты системных операторов. Я упоминал об этом ранее, чтобы не было путаницы. Большинство файлов хранится под этим аккаунтом, поэтому если вы туда попадёте — вам будет чем заняться... хехехе.

[Watch]

Эта команда покажет вашу статистику. Её можно переключать: включить отображение в верхней части экрана или просмотреть один раз. Watch показывает:

• Run — время работы процессора.
• Wait — прошедшее время с момента запуска.
• Read — количество прочитанных дисковых блоков.
• Write — количество записанных дисковых блоков.

Если у вас системные привилегии, введите:

```
Watch[x,x]
```

Вы можете наблюдать за другим пользователем, имея эти привилегии. Команда также выводит дополнительную информацию. Многие операторы используют её, так что будьте осторожны в том, что вводите.

[Другие команды]

Чтобы узнать информацию о ком-то, введите:

```
Who Their name  job#  TTY
```

Например:

```
Who Carrier Culprit  4  #7
```

Это означает, что Carrier Culprit вошёл под заданием 4 и использует TTY #7. Монитор также покажет PPN пользователя и другую информацию о его состоянии в системе.

Если вы заметили, что ваш знакомый находится на TTY10, и хотите отправить ему сообщение:

```
Send TTY10  Congratulations on passing your exam
```

Пользователь на TTY10 получит сообщение и, возможно, сможет ответить. Это также можно использовать для знакомства, особенно если системный оператор окажется нормальным человеком и даст аккаунты — но не рассчитывайте на это.

Если хотите поговорить с кем-то тет-а-тет:

```
Talk TTY10
```

Вы сможете общаться в реальном времени. Но, как уже сказано, иногда следите за тем, что пишете — только не становитесь параноиком насчёт того, что системный оператор наблюдает. Обычно если оператор находится в 'Watch' или 'Exe', он может следить за конкретным пользователем. Это по сути система чата — наслаждайтесь.

Если у вас привилегированный аккаунт, войдите в 'enable' и введите:

```
Whostr
```

Это выдаст информацию о вошедших пользователях и каталогах.

Чтобы узнать время, просто введите 'time'. Если нужна помощь с математикой — введите 'aid' для настольного калькулятора.

```
Ctrl-символы                        Команды регистра
===============                     =============
ctrl-s  = пауза               Если поддерживается нижний регистр:
ctrl-q  = продолжение         'Set Terminal LC'
ctrl-c  = прерывание
ctrl-h  = backspace
```

Decnet

Поддерживается всеми компьютерами Digital. Для доступа введите 'Decnet' и попробуйте подобрать пароль. Decnet поддерживает такие узлы, как VMS, TOPS10 (операционная система для DEC-10), TOPS20 и другие. Аккаунты системных операторов могут пригодиться, если нужен пароль Decnet: попробуйте их пароль. Нередко пароль к Decnet — просто "Decnet". Формат: Set Host xxxx

Acsnet

Это, пожалуй, моё любимое. Поддерживает DEC-10 и многие другие компьютеры. При входе вы увидите что-то вроде:

```
ACSNET
Fri Mar 13 19:30:23 1986
Port ID:  dialup C502  at   300 baud

dialup C502 with even parity

>
```

Чтобы получить меню, введите '?'. Появится список имён групп. Для входа в DEC-10 введите 'Acsdec10'; Decnet обычно в списке не значится, но введите Decnet в любом случае. Другие команды ACSNET:

```
  Connect       Daytime
  Hangup        Disconnect
  Info          Help
  Release       Resume
  Set           WhoamI
```

Хм. Чуть не забыл. Для выхода из DEC-10 введите:

```
  Bye or Kjob (kill job)
```

Часть II: Будет посвящена PPN 1,2 и расширенным командам с использованием Enable.

Удачи,

```
  $$$$$$$$$$$$$$$$$$$$->Carrier Culprit<-$$$$$$$$$$$$$$$$$$$$
```

[КОНЕЦ]
Исправленное издание

Рукопашный бой

Автор: bad boy in black

3/31/86

Этот файл научит вас, как можно убить другого человека голыми руками. Представленная здесь информация будет очень полезна новичкам, а также послужит напоминанием для тех, кто уже знаком с предметом.

Я начну с разговора об основных вещах: стойка, что следует и чего не следует делать в бою, а также другая информация, необходимая новичку. Затем я приведу список из более чем 20 уязвимых точек, которые всегда следует стараться атаковать в схватке, вместе с описанием способов атаки этих точек. Наконец, я дам ещё несколько советов по бою и расскажу, как вы можете продолжить изучение рукопашного боя.

^*^

Итак, позвольте обсудить некоторые основы, которые вам необходимо знать в любой боевой ситуации.

Стойка

Лучшая стойка при встрече с противником — поставить ноги на ширину плеч, руки вытянуть вперёд параллельно друг другу и согнуть в локтях. Держите колени слегка согнутыми и стойте на подушечках стоп.

Помните: вы всегда должны сохранять эту стойку в те моменты, когда не наносите удары по противнику.

Равновесие

Всегда важно сохранять равновесие. Если вы используете описанную выше стойку, вам не придётся об этом беспокоиться. Если же вы всё-таки потеряете равновесие хотя бы на секунду — можете попрощаться с жизнью, поскольку противник, скорее всего, убьёт вас.

Агрессивность

Всегда будьте агрессивны и всегда атакуйте. Не просто стойте в стороне и защищайтесь от ударов противника — в конечном счёте он всё равно убьёт вас. Если вы не проявляете агрессии, противник решит, что вы боитесь, и получит над вами преимущество.

Отличный приём — кричать на противника. Если вы начнёте орать на него, это здорово его напугает, а кроме того, позволит набрать больше кислорода в лёгкие, что придаст вам больше сил.

Природное оружие

Ваше природное оружие — это: ребро ладони любой руки, основание ладони, пальцы, согнутые во втором суставе, ваш ботинок, локоть, колени, зубы, указательный и средний пальцы, образующие форму «V», и кулак. Только эти части тела являются одними из мощнейших видов оружия, которые вы можете использовать.

^*^

Теперь, когда вы знаете основы боя, позвольте перечислить лучшие места для ударов по противнику.

Висок

Сильный удар в висок обеспечивает мгновенную смерть, поскольку там близко к поверхности кожи проходят крупная артерия и нерв. Удар средней силы вызовет сильную боль и сотрясение мозга, тогда как сильный удар убьёт противника мгновенно. Лучший способ ударить в висок — ребром ладони, а если противник лежит на земле, можно ударить его носком ботинка.

Глаза

Глаза — отличное место для удара, поскольку хороший удар в глаза вызывает временную или постоянную слепоту. Чтобы ослепить противника, сложите указательный и средний пальцы в форму «V» и вонзите их в его глаза, удерживая пальцы прямыми. Также можно выдавить глаза большим пальцем.

Нос

Нос — ещё одно превосходное место для атаки. Ударьте по переносице ребром ладони — это вызовет перелом, сильную боль, временную слепоту и даже смерть. Или можно ударить основанием ладони снизу вверх, вбив нос в мозг. При достаточной силе удара носовая кость пробьёт мозг, и противник погибнет.

Верхняя губа

В верхней губе близко к поверхности кожи расположено множество нервов, поэтому удар ребром ладони вызывает сильную боль, а при достаточной мощи — потерю сознания.

Рот

Если противник лежит на земле, ударьте его по рту каблуком ботинка. Поскольку в зубах проходит множество вен и артерий, будет обильное кровотечение, которое напугает противника и нарушит его концентрацию при защите других частей тела.

Подбородок

По подбородку следует бить только основанием ладони, поскольку о подбородок противника можно сломать пальцы. Используйте основание ладони и нанесите противнику очень мощный удар снизу

вверх. Это вызовет сильнейший дискомфорт.

Кадык

Обычно противник хорошо защищает эту часть тела, но если вам выпадет возможность — нанесите резкий удар ребром ладони. При достаточной силе удара вы раздробите его трахею, и он умрёт. Также можно сдавить кадык пальцами.

Пищевод

Если вам удастся схватить противника за шею, надавите большими пальцами на пищевод (расположен ниже кадыка). Сильное давление будет очень болезненным, перекроет доступ кислорода в лёгкие, и противник быстро умрёт.

Шея

Очень сильный удар ребром ладони по основанию шеи обычно её ломает. Однако если удар недостаточно силён, противник может просто потерять сознание — поэтому обязательно ударьте его в висок или сверните шею, чтобы убедиться, что он мёртв. Шея — лучшее место для удара, если вам нужна тишина: это быстро, и противник падает без единого звука.

Ключица

Ключица — чрезвычайно чувствительная часть тела. Резкий удар по ней ребром ладони или локтем причиняет противнику невыносимую боль. Также, надавив пальцем на ключицу, можно поставить противника на колени.

Плечо

Плечо легко вывихнуть, и для этого требуется немного силы. Однако делать это нужно быстро. Схватите руку противника и заведите её ему за спину, затем резко дёрните вверх. Должен послышаться хлопок — это значит, что вы вывихнули плечо противника. Существуют и другие способы сделать это, но данный — самый простой.

Подмышка

Хотя добраться до неё сложно, в подмышке расположена разветвлённая нервная сеть. Если противник лежит на земле, поднимите его руку и ударьте его ногой в подмышечную впадину. Это вызовет сильную боль. Тем не менее это не самое распространённое место для удара в драке, но всё же стоит держать его в уме.

Рёбра

Удар по рёбрам пальцами, согнутыми во втором суставе, весьма болезнен, а при достаточной силе вызывает сильнейшую боль и переломы. Используйте только пальцы, согнутые во втором суставе, — это причиняет наибольший вред.

Солнечное сплетение

Солнечное сплетение расположено на груди, в маленькой «V»-образной точке, где заканчивается рёберная дуга. Там сосредоточено большое количество нервов, поэтому удар суставом среднего пальца может вызвать сильную боль и даже потерю сознания.

Плавающие рёбра

Плавающие рёбра — это нижние рёбра, расположенные спереди и по бокам тела противника. Используйте ребро ладони, каблук или носок ботинка. Удар причинит боль и оглушит противника.

Позвоночник

Удар каблуком ботинка по позвоночнику может парализовать или убить противника. Нижняя часть позвоночника между почками противника — лучшее место для удара, поскольку это наименее защищённый участок. Атаковать позвоночник вы сможете только тогда, когда противник лежит на земле или повернулся к вам спиной.

Почки

В почках проходят два крупных нерва, близко к поверхности кожи. Сильный удар по почкам вызывает смерть. Для удара по почкам можно использовать кулак или ребро ладони. Также подойдёт удар каблуком ботинка.

Пах

Пах — хорошее место для удара, если вам выпадет такая возможность. Как правило, противник защищает эту область лучше всего, но если шанс представится — ударьте коленом снизу вверх или кулаком. Боль, которую при этом испытает противник, вам нетрудно представить.

Копчик

Копчик расположен над анусом и является очень чувствительной частью тела, поскольку там сосредоточено множество спинномозговых нервов. Бейте по копчику носком ботинка. Боль от такого удара — невыносимая.

Локоть

Локоть легко сломать или вывихнуть. Заведите руку противника ему за спину и основанием ладони надавите на его локоть вовнутрь, пока он не хрустнет или не выскочит из сустава. Когда рука противника выйдет из строя, вы получаете значительное преимущество над ним.

Пальцы

Пальцы следует ломать, поскольку со сломанными пальцами противник практически беспомощен. Схватите руку противника одной рукой, а другой отгибайте пальцы вверх, пока они не сломаются. Достаточно сломать первые два пальца. Это также помогает разорвать захват.

Колено

Колено можно уничтожить, ударив по нему боковой частью ботинка снизу вверх. Это разорвёт связки и хрящи. Такой удар вызывает невыносимую боль и лишает противника возможности передвигаться. Когда колено выведено из строя, вы получаете значительное преимущество.

Лодыжка

Если противник лежит на земле, схватите его за лодыжку и скручивайте, пока она не сломается. Это сделает ходьбу для него практически невозможной, и тогда его будет легко добить.

^*^

Позвольте поговорить ещё о нескольких важных вещах, которые следует помнить в бою.

Тактика

Всегда старайтесь выбить противника из равновесия. Для этого можно броситься на него и сделать вид, что наносите удар. Это заставит его отпрянуть и потерять равновесие.

Всегда ищите слабое место и атакуйте его. Как только он оставит какую-либо уязвимую часть тела незащищённой — атакуйте её со всей силой. Делая это, вы вынудите его прикрывать только что поражённое место, тем самым открывая для атаки другие части тела.

Используйте любые подручные предметы. Имеется в виду следующее: бросьте ему в глаза песок, отбивайте его удары с помощью толстой ветки или любого другого материала, который можно использовать против него в качестве оружия.

Запрещённые приёмы

В ситуации жизни и смерти не существует ни запрещённых приёмов, ни правил. Хотя удар в пах в школе считается подлым приёмом, это весьма действенный способ вывести противника из строя. Просто бейте, где можете, и добивайте его, когда он упал. Тогда он уже не поднимется.

^*^

Я изложил вам основы боя и лучшие места для атаки на теле противника. Но только потому, что вы прочитали этот файл, не значит, что вы сможете сразу выйти и надрать кому-то задницу. Все эти методы требуют длительной практики для правильного исполнения.

Если вам понравился этот файл и вы хотите отработать описанные приёмы — найдите партнёра, которому тоже это интересно, и отрабатывайте каждый вид удара. Поначалу действуйте медленно и помните, что эти методы смертоносны и для своей эффективности не требуют большой силы — так что не перестарайтесь с партнёром.

Некоторые из вас могут решить, что одной практики недостаточно и хотелось бы узнать больше, чем я изложил выше. Что ж, существует несколько хороших книг с иллюстрациями по этой теме, которые освещают её куда подробнее, чем я могу сделать в этом файле. Книга, которую я главным образом использовал при написании этого файла, — «Полевое руководство Корпуса морской пехоты по физической безопасности» ("The Marine Corps Field Manual on Physical Security"). Её можно достать в хорошем книжном магазине, или, если у вас есть знакомый морской пехотинец, он легко раздобудет вам экземпляр.

Также существуют лагеря, где можно провести 1–2 недели и научиться всевозможным вещам: обращению с оружием, детальному рукопашному бою, проведению рейдов и многому другому. Инструкторы, ведущие эти программы, отлично подготовлены и имеют многолетний опыт. Однако, как правило, для участия в этих программах необходимо быть старше 18 лет, а также относиться к делу очень серьёзно. Это не из тех программ, где можно сказать: «Тайм-аут, мне нужно отдохнуть». Они не остановятся ради вас. Подробнее об этих программах можно узнать из журналов вроде "Soldier of Fortune" и других изданий аналогичной тематики.

^*^

Ну что ж, на сегодня всё. Возможно, в будущем я смогу рассмотреть более занятные темы — например, бой с ножом и другое летальное оружие, применяемое в схватке. Если вам понравился этот файл — дайте знать, и я продолжу эту тему.

Digital Multiplex System (DMS) 100

Автор: Knight Lightning
Источник: Metal Shop Private/AE/Brewery

Этот файл, конечно, о DMS-100. Полноразмерные файлы о других вариантах DMS, DMS-200 и DMS-250, ожидайте позднее. Значительная часть информации в этом файле была получена из manuals, приобретённых у Jester Sluggo.

Примечание: **IBN** означает **Integrated Business Network**.

DMS-100

DMS-100/IBN состоит из electronic business sets и standard telephones, data units и attendant consoles, находящихся на premises клиента; а также DMS-100 digital switching и supporting hardware/software, находящихся на premises телефонной компании. Вместе они создают integrated business communications network, предоставляющую необычное сочетание функций и преимуществ.

• DMS-100/IBN интегрирует voice and data в единую business communications system.
• Эффективно обслуживает организации любых размеров: от малых предприятий с несколькими линиями до самых сложных сетевых систем с числом линий до 30 000.
• IBN system автоматически monitors and controls свои операции, диагностирует проблемы и в некоторых случаях сама выполняет repairs.
• Система полностью modular: она покрывает текущие потребности и позволяет добавлять новые features по мере необходимости.
• Cost effective: помогает контролировать communications costs за счёт более эффективного использования facilities, централизации attendant service там, где это нужно, Call Dial Rerouting (CDR) для контроля и ограничения long-distance calling, а также network management.
• Worry-free operation: цифровые коммутаторы DMS-100 от Northern Telecom поддерживаются хорошо обученным персоналом телефонной компании.

Некоторые другие features DMS-100:

• **Automatic Route Selection**: автоматически маршрутизирует long distance calls по самому экономичному доступному route.
• **Station Message Detail Recording**: предоставляет подробную запись long distance charges, включая originating number, time and duration, authorization code и т. д.
• **Direct Inward System Access (DISA)**: позволяет персоналу компании использовать экономящие средства company facilities для long distance calling даже вне компании.

System features and benefits

Примечание: ниже перечислены все features, но подробно выделены только важные.

Attendant console

```
Call Waiting Lamp
Loop Keys - 6 loop keys, each with its associated source and destination lamp
```

to indicate the calling and called party states
Alphanumeric Display
Multiple Directory Numbers
Feature Keys - up to 42 total; some may be used for Speed Calling and Paging System
Incoming Call Identifier
Exclude Source/Exclude Destination - privacy keys
Signal Source/Signal Destination
Release Source/Release Destination

Console features

Access to paging
Call detail entry
Call Selection
Camp-on
Conference - 6 port
Non-delayed operation
Locked loop operation
Manual and automatic hold
Busy verification of trunks
Trunk group busy indication
Multiple listed directory numbers
Secrecy
Serial call
Lockout
Position busy
Through dialing
Call hold
Remote console
Console display
Automatic recall
Two-way splitting
Attendant transfer
Busy verification of lines
Multiple console operation
Switched loop operation
Uniform call distribution from queue
Control of trunk group access
Night service
Speed calling
Delayed operation
Interposition calling

Electronic business sets

LCD Indicators
Call Forwarding
Automatic Line
Call Pick-up
Ring Again - automatically redials busy numbers until they are free
Multiple Directory Numbers
Intercom
Speed Call
Call Transfer/Conference
On-Hook Dialing

Additional programmable features

Automatic Hold
Listen-on Hold
Multiple Appearance Directory Numbers (MADN)
 - Single Call Arrangement
 - Multiple Call Arrangement
Privacy Release
Tone Ringing with Volume Control
End-to-End Signaling
Call Park
Make Set Busy
Malicious Call Trace
Busy Override
Attendant Recall
Call Waiting
Stored Number Redial
Private Business Line
32 Character Alphanumeric Display

Data unit

DMS-100/IBN Data Unit делает доступ к информации таким же простым для изучения и использования, как телефон. Он может применяться как standalone device или подключаться к Business Set либо standard telephone для integrated voice and data telephone telecommunications.

Он передаёт данные по simple 2-wire loops на скоростях до 56 kb/s, используя proprietary Time Compression Multiplexing technology от Northern Telecom. Он совместим с существующим computer and data terminal equipment и доступен в разных low-speed and high-speed models, соответствующих existing terminal capacity.

Benefits

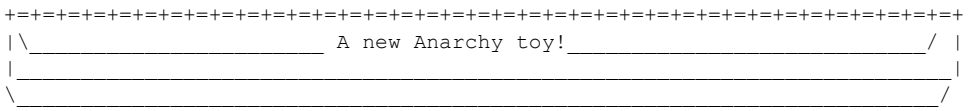
• Комбинируется с Business Set или standard telephone, предоставляя integrated voice/data communications.
• Data unit и telephone могут работать одновременно вместе или полностью независимо друг от друга.
• Полностью digitalized, что устраняет bulky analog modems.
• Ring Again, то есть постоянный redial busy numbers.
• Speed Calling.

Контакты для дополнительной информации

```
Digital Switching Systems Sales
Northern Telecom Inc.
P.O. Box 13010
4001 East Chapel Hill -- Nelson Highway
Research Triangle Park
North Carolina 27709
Tel: (919) 549-5000

Switching Group Sales, Department S-70
Northern Telecom Canada Limited
8200 Dixie Road, P.O. Box 3000
Brampton, Ontario
L6V 2M6
Tel: (416) 451-9150
```

Новая анархистская игрушка!



(иначе известная как «Знай своё железо»)

Автор: The Leftist

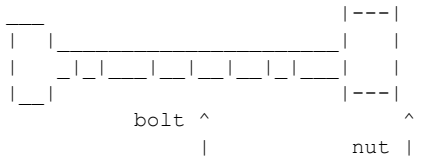
Эта новая «бомба» на самом деле не особо разрушительна, хотя я бы не хотел получить летящий осколок прямо в голову. Используйте её, чтобы пугать собак и просто устраивать переполох.

Материалы

Вам понадобятся: 1 гайка достаточно большого размера, 2 болта одинакового размера, оба подходящие по размеру для этой гайки. Также понадобится коробка деревянных кухонных спичек типа «чиркай о любую поверхность».

Конструкция

Итак, всё нашли? Приступим. Возьмите один из болтов и гайку и вкрутите болт примерно на 1/4 длины гайки. Должно выглядеть примерно так:



Теперь возьмите спички — на их конце должен быть двухцветный кончик. Аккуратно срежьте верхний слой (это удобно делать лезвием бритвы), стараясь не поджечь спички. Готово? Отлично. Теперь возьмите примерно четыре-пять головок, а если хочется чего-то поэкстремальнее и они туда помещаются — попробуйте шесть. Вставьте головки (белую часть) в зазор между свободным концом болта и гайкой. Затем осторожно вкрутите второй болт с другой стороны достаточно плотно. Теперь у вас есть два болта, соединённых гайкой, а между ними зажаты спичечные головки.

И что дальше?

Возьмите эту штуку и бросьте её во что-нибудь твёрдое — например, в асфальт — и бросайте достаточно сильно и на достаточное расстояние. Это может быть очень весело, а делается за считанные секунды.

Wide-Area Networks, часть 1

Автор: Jester Sluggo

Часть 1 содержит информацию об ARPANET и CSNET.
Часть 2 содержит информацию о BITNET, MFENET, UUCP и USENET.

Лучше читать оба файла, чтобы лучше понимать связь между ними.

Эти файлы покрывают общую информацию о wide-area networks, например ARPANET, CSNET, BITNET, MFENET, UUCP и USENET, но могут содержать сведения, относящиеся и к другим сетям, на которых здесь не делается основной акцент.

Эти файлы **не** являются hacker's tutorial или guide по этим системам.

ARPANET

ARPANET, являющаяся крупным компонентом NSFnet, National Science Foundation Network, началась в 1969 году как R&D project под управлением DARPA, Department of Defense Advanced Research Projects Agency. ARPANET была экспериментом по resource sharing и предоставляла survivable, multiply connected, high bandwidth communications links со скоростью 56 kilobits per second между крупными существующими computational resources и computer users в academic, industrial and government research laboratories.

ARPANET managed and funded by DCA, Defense Communications Agency, a user services предоставлялись network information center в SRI International.

ARPANET служила испытательной площадкой для разработки advanced network protocols, включая TCP-IP protocol suite, введённый в 1981 году. TCP-IP, и особенно IP, internet protocol, ввёл идею internetworking: возможность связывать networks разных technologies and connection protocols вместе, при этом предоставляя unified internetwork addressing scheme и общий набор transport and application protocols.

Эта разработка позволила подключать к ARPANET networks of computers and workstations, а не только single-host computers. TCP-IP остаются наиболее доступными и advanced non-vendor-specific networking protocols и сильно повлияли на текущую international standards activity. TCP-IP предоставляют разнообразные application services, включая remote logon (Telnet), file transfer (FTP) и electronic mail (SMTP and RFC822).

Технология ARPANET оказалась настолько успешной, что в 1982 году Department of Defense, DOD, отказался от своего network project AUTODIN II и принял ARPANET technology для Department of Defense Data Network, DDN. Современная MILNET, отделённая от original ARPANET в 1983 году, является operational, unclassified network component of the DDN, тогда как ARPANET остаётся advanced network R&D testbed for DARPA.

На практике ARPANET также была operational network, поддерживающей исследователей DOD, DOE, Department of Energy, и некоторых computer science researchers, спонсируемых NSF. Это сообщество стало зависеть от доступности сети. До появления NSFnet доступ к ARPANET был ограничен этим сообществом.

Как operational network в scientific and engineering research community, и с ростом доступности affordable super-minicomputers, ARPANET всё меньше использовалась как инструмент sharing remote computational resources и всё больше как средство sharing information. Главный урок опыта ARPANET состоит в том, что information sharing является ключевым преимуществом computer

networking. Более того, можно утверждать, что многие крупные достижения в computer systems and artificial intelligence стали прямым результатом enhanced collaboration, сделанного возможным ARPANET.

Однако ARPANET имела и отрицательный эффект: она создала ситуацию have and have-not в experimental computer research. Scientists and engineers, выполнявшие такие исследования в учреждениях за пределами примерно двадцати ARPANET sites, находились в явном невыгодном положении при доступе к relevant technical information и при привлечении faculty and students.

В октябре 1985 года NSF и DARPA, при поддержке DOD, подписали memorandum of agreement о расширении ARPANET, чтобы пользователи NSF supercomputer могли использовать ARPANET для доступа к NSF supercomputer centers и общения друг с другом.

Немедленным результатом соглашения стало то, что все NSF supercomputer users на campuses с существующим ARPANET connection получили возможность использовать ARPANET. Кроме того, NSF supercomputer resource centers в University of Illinois и Cornell University подключены к ARPANET.

В целом существующие ARPANET connections находятся в departments of computer science или electrical engineering и не так легко доступны другим researchers. Однако DARPA попросила campus ARPANET coordinators облегчить доступ relevant NSF researchers.

В рамках NSFnet initiative ряд университетов запросил connection to ARPANET. Каждый такой campus обязался установить campus network gateway, доступный всем, чтобы со временем пользователи могли использовать ARPANET для доступа к NSF supercomputer centers из своей собственной local computing environment. Дополнительные запросы на подключение к ARPANET рассматриваются NSF.

CSNET

Создание сети для computer science research впервые было предложено в 1974 году advisory committee for computer science при NSF. Целью сети должна была стать поддержка collaboration among researchers, resource sharing и, в частности, support isolated researchers in the smaller universities.

Весной 1980 года CSNET, Computer Science Network, была определена и предложена NSF как logical network, состоящая из нескольких physical networks различной мощности, производительности и стоимости. NSF ответила пятилетним контрактом на разработку сети при условии, что CSNET должна стать financially self-supporting к 1986 году.

Первоначально CSNET была сетью с пятью основными компонентами: ARPANET, Phonenet, telephone-based message relaying service, X25Net, support for the TCP-IP protocol suite over X.25-based public data networks, public host, centralized mail service, и name server, online database of CSNET users для поддержки transparent mail services.

Общая service, предоставляемая через все эти networks, — electronic mail, интегрированная на специальном service host, который действует как electronic mail relay между component networks. Таким образом, CSNET users могут отправлять electronic mail всем ARPANET users и наоборот. CSNET при поддержке DARPA установила ARPANET connections на CSNET development sites в University of Delaware, University of Wisconsin и Purdue University.

В 1981 году Bolt, Beranek, and Newman (BBN) заключила контракт на предоставление technical and user services и на эксплуатацию CSNET Coordination and Information Center. В 1983 году general management of CSNET перешёл к UCAR, University Corporation for Atmospheric Research, с

subcontract to BBN.

С тех пор CSNET быстро выросла и сейчас является independent, financially stable and professionally managed service для computer research community. Импульс, созданный первоначальным успехом CSNET, привёл к широкой community support, которой она теперь пользуется. Сейчас к CSNET принадлежат более 165 university, industrial and government computer research groups.

Из опыта CSNET можно извлечь ряд уроков:

1. Сеть теперь financially self-sufficient, показывая, что research community готово платить за benefits of a networking service. Users платят usage charges плюс membership fees от 2000 долларов для small computer science departments до 30 000 долларов для larger industrial members.
2. Хотя simple electronic mail and mailing list services, то есть Phonenet service, дают researchers значительные benefits, большинство researchers хочет намного более высокий уровень performance and service, предоставляемый ARPANET.
3. Customer support and information service критически важны для успеха сети, даже, или, возможно, особенно, когда users сами являются sophisticated computer science professionals.

Уроки CSNET дадут ценный input для design, implementation, provision of user services, operation and management of NSFnet и, в частности, для разработки appropriate funding model for NSFnet.

CSNET при поддержке NSFnet program сейчас разрабатывает проект CYPRESS, изучающий способы улучшения уровня CSNET service для research departments при низкой стоимости. CYPRESS будет использовать DARPA protocol suite и предоставлять ARPANET-like service на low-speed 9600-bit-per-second leased line telephone links.

Сеть будет использовать nearest neighbor topology по модели BITNET, одновременно предоставляя users более высокий уровень service и более высокий уровень interoperability with ARPANET. Проект CYPRESS призван заменить или дополнить использование CSNET сетей X.25 public networks, которое оказалось чрезмерно дорогим. Этот подход также может использоваться для предоставления low-cost connection to NSFnet для smaller campuses.

```
/
\
/ luggo !!
```

Пожалуйста, полностью указывайте credit for references следующим людям:

```
Dennis M. Jennings
Lawrence H. Landweber
Ira H. Fuchs
David J. Faber
W. Richards Adrion
```

Любые вопросы, комментарии или Sluggestions можно отправлять мне e-mail на Metal Shop или snailmail по следующему адресу до 31 декабря 1986 года:

```
J. Sluggo
P.O. Box 93
East Grand Forks, MN 56721
```

Short-Wave Radio Hacking

Автор: The Seker
Написано эксклюзивно для: Metal Shop Private

Каждый день по радиоволнам обмениваются огромными объёмами информации. Я находил news agencies, military computers, businesses и даже hacks.

Стандартный метод обмена называется **RTTY**, Radio Teletype. Обычно он используется на скорости 66/7 words per minute. Вместо ASCII чаще применяется Baudot, 5-bit character set. Также существует множество его вариаций.

Есть и много других transmission standards, кроме RTTY, которые широко используются. Несколько известных:

• **FAX**, Facsimile.
• **Helshcrieber**: используется для передачи pictogram-type alphabets, например Chinese, Japanese и т. п., вместо American letters.
• **SSTV**: похож на Viewdata. Используется для передачи high-resolution pictures, смешанных с text.

Для начала нужен receiver с coverage не менее 500 kHz-30 MHz и resolution больше 100 Hz, а также high quality antenna. Обычно их можно найти в electronics stores. Также потребуется interface и RTTY software для конкретного computer. Ищите дополнительную информацию в журналах вроде *Amateur Radio* или *Ham Radio Today*. Ещё одно хорошее место для проверки — CB store.

News agencies

От них можно найти всевозможные материалы. Можно даже перехватить story, отправляемую в press. Они обычно работают на скорости 66/7 words a minute, 50 baud.

Некоторые более распространённые fixed bands, на которых они передают:

```
at kHz:

3155-3400      3950-4063
9040-9500      12050-12330
13800-14000    15600-16360
19800-19990    25210-25550
```

Простой способ понять, что вы нашли news agency, — это какая-нибудь бессмысленная transmission, постоянно повторяемая:

```
RYRYRYRYRYRYRYRYRYRY
```

Это делается, чтобы держать channels открытыми для reception.

Conferences

Ещё одна интересная вещь, которую я нашёл, — channels, вокруг которых собирались amateurs. Я часто сталкивался с людьми из других стран, которые даже не говорили по-английски. Я даже встречал других hackers со всего мира.

Несколько более популярных мест, где собираются amateurs:

```
at kHz:
```

```
3590  14090  21090  28090

at MHz:

432.600  433.300

at VHF/UHF:

144.600  145.300
```

Packet radio

Новое развитие в radio transmission — packet radio. Судя по тому, что я видел, это похоже на digital packet switching networks, например Compuserve, Telenet, Tymnet и т. д., только медленнее.

Фактически Compuserve исследовала способ дешёвой передачи своих services.

```
--tS
```

Mobile Telephone Communications

Автор: Phantom Phreaker
Представлено: The Alliance, (618) 667-3825

Mobile telephone communications — это не то же самое, что cellular. Mobile telephone service не так развит, как cellular, и не так эффективен. Mobile telephone service резко ограничивает число клиентов, тогда как cellular designed to solve the problems of mobile telephone service.

Сигналы для mobile communications передаются high-power transmitters and antennas, которые обеспечивают service на площади примерно 20-30 miles.

Base unit mobile communications system передаёт и принимает на разных frequencies одновременно. Типичная мощность transmitter radio base station составляет 200-250 watts.

Mobile telephone facilities соединяются с обычной fixed-position telephone system, однако base units могут принадлежать Radio Common Carrier (RCC). RCC, управляющие mobile telephone systems, получают charges от telephone company за использование обычной phone system.

Diagram

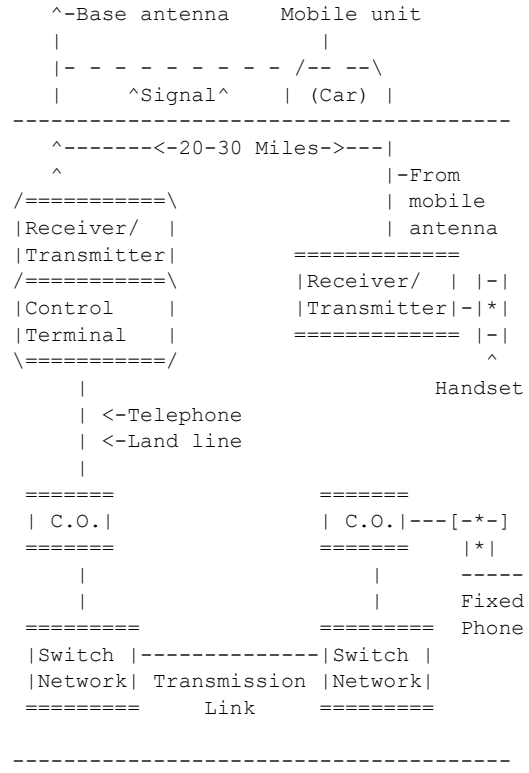


Диаграмма выше взята из *Understanding Telephone Electronics*, chapter 10.

Как видно из диаграммы, calls, сделанные с fixed-position telephone, routed through a Central Office как обычно, через Switch Network, к другой Switch Network и к другой CO. Из второй CO, ближайшей к mobile unit, signals отправляются по telephone line к control terminal, затем к receiver, потом к base unit, то есть antenna. Из base unit radio signals отправляются к месту mobile telephone.

Calls с mobile telephone работают тем же образом. Выбирается idle radio channel, примерно как seizure of a trunk for a long-distance call, и signals отправляются по mobile network.

Если channel для использования недоступен, triggering busy indication, похожий на re-order. Если channel доступен, customer получает dial tone, похожий на обычный fixed-position telephone service.

Область, где это работает, называется subscriber's home area. Когда subscriber mobile telephone service покидает service area, он называется roamer. Поскольку mobile unit находится вне service area, нужны special preparations, чтобы продолжить communications to/from that mobile unit.

Signalling

Mobile signalling tones выбираются, как touch tones, так, чтобы избежать возможного reproduction of the signalling tone on the voice link, которое могло бы вызвать signalling mistake. IMTS, Improved Mobile Telephone Service, использует in-band signalling tones from 1300 Hz to 2200 Hz.

Другой метод signalling — MTS, Mobile Telephone System. MTS старше IMTS и использует in-band signalling tones from 600 Hz to 1500 Hz, а некоторые используют 2805 Hz в manual operation.

Call completion

В этом примере предположим, что call placed from a normal telephone to a mobile unit. Сначала base station выбирает один idle channel и помещает на него 2000 Hz idle tone. Все on-hook mobile units, active in that service area, находят и lock onto channel, который несёт 2000 Hz idle tone. Теперь каждый mobile unit listens for its specific number on that channel. Когда idle channel становится busy, выбирается новый channel для использования, и процесс повторяется.

Call caller отправляется через telephone network тем же способом, что и обычный telephone call. Когда call достигает control terminal, terminal seizes уже отмеченный idle channel, который слушают все on-hook mobile units, и applies 1800 Hz seize tone. Этот tone не даёт другим mobile units использовать channel для завершения других calls.

Called number outpulsed over the base station transmitter at ten pulses per second, где idle tone представлен как mark, a seize tone как space.

Поскольку каждый idle mobile unit ждёт на этом channel, они сравнивают outpulsed number со своим собственным number. Если первая цифра called mobile unit равна three, а конкретный mobile unit, listening on the channel, имеет первую цифру four, он перестаёт слушать этот channel и переходит к следующему channel with 2000 Hz applied.

Когда mobile unit получает правильный destination number, все остальные mobile units больше не слушают этот конкретный channel. Когда 7-digit number received, mobile supervisory unit turns on the mobile transmitter and sends acknowledgement signal, 2150 Hz guard tone, обратно к control terminal.

Если этот signal не получен через three seconds after outpulsing, seize tone удаляется с channel, and the call is dropped. Если signal received at the control terminal, then mobile phone rings, standard two seconds on, four seconds off. Если called mobile unit не отвечает за forty-five seconds, call также drops.

Когда человек отвечает на mobile phone и снимает его off hook, mobile supervisory unit sends a connect tone of 1633 Hz as an answer signal. Когда control terminal получает его, ringing stops, and a voice path between the two phones is established.

Когда mobile subscriber hangs up, отправляется disconnect signal, состоящий из alternating disconnect/guard tone signals: 1336 Hz and 2150 Hz respectively. Затем mobile unit begins searching for another idle channel и готовится к новым calls.

Для outgoing call placed by the mobile subscriber, mobile unit must already be locked on the idle channel. Если unit не locked, warning light flashes, сообщая пользователю о problem. Это похоже на re-order signal. Если unit уже на idle channel, calling number будет отправлен control terminal for billing purposes.

Cellular telephones

Чтобы улучшить mobile telephone service, решив проблемы вроде малого числа users и высокой цены, AT&T invented the Cellular Concept, or AMPS, Advanced Mobile Phone System. Это cellular phone concept, используемая в major cities. Los Angeles, California, сейчас имеет крупнейшую cellular communication system in the world.

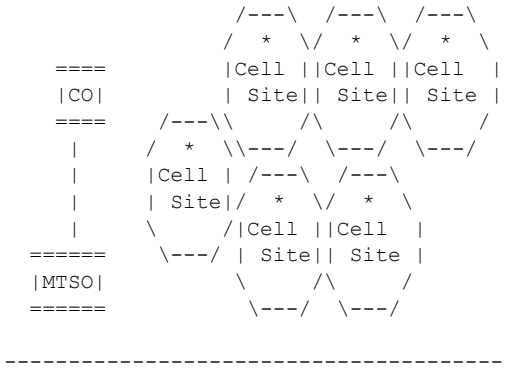
Calls, отправленные на cellular telephones, идут через MTSO, Mobile Telecommunications Switching Office. MTSO handles all calls to and from cellular telephones and handles billing.

Все incoming calls from the MTSO отправляются на cell site в каждой cell, затем к actual cellular telephone. Главное различие между mobile и cellular состоит в том, что cellular может использовать один и тот же channel гораздо больше раз, чем mobile telephone system, предоставляя service большему числу customers и делая его менее expensive.

Когда vehicle выходит за range одного cell site, signal immediately transferred, with no signal loss, to another cell site, где call продолжается without interruption. Это называется cellular hand-off.

Cellular communications areas divided into several cells, like a honeycomb.

Diagram



More cell sites are used for the area they are needed for. Signals sent from the MTSO to each cell site. Если вы едете в cell site at the far left, signal from the MTSO будет отправлен в эту cell. По мере движения signal moves.

Цитата из pamphlet AT&T's Cellular Telephones:

> *Передача по AT&T cellular phone звучит так же хорошо, как ваш домашний и офисный телефон. В основе это простая концепция. Каждая metropolitan area divided into sectors, forming a honeycomb of cells. Each cell включает собственные transmitter and receiver, connected to the local phone network. Когда вы едете от cell к cell, sophisticated electronic equipment transfers, or hands off, the call to another cell site. Эта automatic sequence поддерживает service quality throughout the conversation without interruption.*

Надеюсь, этот файл оказался полезен всем, кому любопытны более technical aspects of the telephone system.

References


```
Understanding Telephone Electronics by Texas Instruments, 1983
TELE Magazine issues three and four
AT&T Mobile communications pamphlet
AT&T Cellular concept pamphlet
```


```
End of file
4/14/86
```

Phrack World News IV, часть 1

Составил: Knight Lightning

1 апреля 1986 года

Да, дата говорит 1 апреля, но это **не** шутка. Ниже письмо от Chadbourne & Parke. Я заменяю настоящее имя Taran на `Taran King`.

```
March 26, 1986
```

Уважаемый Mr. King,

Наша юридическая фирма представляет Master Lock Company. Недавно наш клиент был уведомлён о распространении через Bulletin Board Computer Service, расположенный по вашему адресу, информации, потенциально вредной для его commercial interests and business relationships. Более конкретно мы имеем в виду публикацию этим computer service инструкций по вскрытию combination locks, производимых Master Lock Company.

Мы пишем, чтобы уведомить вас о concern Master Lock Company по поводу действий computer service и о seriousness, с которой компания относится к этим действиям. Master Lock Company имеет твёрдое намерение сохранять и защищать reputation and goodwill, связанные со своими products, и, если необходимо, воспользуется всеми доступными legal recourse.

При нынешних обстоятельствах, однако, наш клиент сначала хотел бы дать вам возможность принять меры, предотвращающие activities, которые он может рассматривать только как malicious и по отношению к себе, и по отношению к своим customers. Поэтому мы просим вас обеспечить immediate and permanent cessation of the actions described above. Ваше compliance with this request — всё, что требуется для amicable resolution of this matter.

Ваше сотрудничество будет высоко оценено.

```
Very truly yours,

Terrence J. Farrell
```

Это письмо, конечно, говорит о phile 6 из Phrack Issue I, озаглавленном **How To Pick Master Locks**. Было довольно смешно, что даже в своём письме они допустили misspelled word, которое я исправил выше. Они отправили его Taran King certified mail, за которое ему пришлось расписаться. С тех пор Taran ответил следующим письмом:

```
Dear Sirs,                                    4/1/86
```

Меня зовут Taran King, как вы так легко выяснили, и раньше я вёл Metal Shop, electronic bulletin board system. Сейчас я веду private line для моих личных друзей и, если меня просят, распространяю для них `general files`.

Сам факт того, что я распространял файл, едва ли является главным. Я всего лишь получил его от авторов файла и распространил в другие sources, которые, по-видимому, распространили его в другие места. Если я ответственен за этот файл, думаю, вам следует найти и ряд других authors.

Информация о `secret` to picking Master locks содержится не только в этом файле, о котором вы мне написали, но и в ряде других файлов, циркулирующих годами. Это старая информация, кто-то просто republished it. Хотя я не очень хорошо осведомлён по этой теме, я считаю, что печатать информацию на такую тему законно. Мы не одобряем actions, promoted by the files, а лишь информируем public по этому topic. Не хочу растекаться мыслью, но хочу выразить свою point as clearly as possible.

Если я, как один из людей, через которых этот файл прошёл, ответственен за today's crime rate людей, вскрывающих Master, American или замки любой другой компании, то я считаю, что любой, кто имеет этот файл или читал книги, должен быть arrested по этому поводу. Думаю, Paladin Press публикует ряд books на эту тему. Я видел одну из книг типа **Picking Master Locks in 3-Easy Steps!**, и, насколько я знаю, она всё ещё публикуется и распространяется.

Надеюсь, я не звучу disrespectful or condescending, но меня очень раздражает, когда отец должен расспрашивать меня о письме, пришедшем по почте от law firm in New York. Пожалуйста, ожидайте письма от него с inquiries по теме, о которой вы мне написали. Если вы хотите further discussion, не стесняйтесь звонить мне на voice line когда угодно по `(314) XXX-XXXX`. Только, пожалуйста, не играйте смешно, как с письмом, и не делайте reverse charges или что-нибудь столь же entertaining.

```
Sincerely,

Taran King
```

Если кто-то из вас задаётся вопросом, как они нашли Taran, то CN/A существует не только для phone phreaks, а номер Metal Shop был опубликован в Phrack I в большинстве файлов. Моя теория о том, как они нашли этот файл:

A. Какой-нибудь agent type смотрит вокруг, видит файл и передаёт его Master Lock Company.

B. Какой-нибудь rodent dork type, чей отец работает в Master Lock Company, видит его и говорит: «Эй, пап, смотри, это реально круто!»

Думаю, это не имеет особого значения.

```
Knight Lightning
```

Lex Luthor говорит о TWCB

Воскресенье, 22 марта 1986 года

Ниже сообщение от Lex Luthor по поводу TWCB Inc.

Мне стало известно, что TWCB Inc. `throwing around large amounts of BS involving me`. Я **никогда** не разговаривал с ними: ни на conference, ни на BBS, ни где-либо ещё.

Они не связаны ни с phreak group The Legion of Doom, ни с hack group The Legion Of Hackers. Любые references, которые они делают относительно меня или любого участника LOD или LOH, следует игнорировать, поскольку это, вероятно, bullshit.

TUC работает над Project Educate, но дат выпуска issue пока нет. Он выбросил старый первый выпуск и работает над newsletter лучшего качества. Я не имею почти никакого отношения к Project Educate, кроме того, что могу внести какой-нибудь материал.

Я просто хотел это прояснить, и если кто-то услышит что-то другое, пожалуйста, отправьте мне email с информацией.

Ещё одна вещь, которая у меня на уме: как некоторые phreaks/hacks принижают 2600 Magazine, говоря, что он не так хорош, не даёт достаточно technical info или даёт слишком technical и т. д. По сравнению с другими rags, 2600 делает чертовски хорошую работу и очень consistent. Вам никогда не приходится беспокоиться, что они вас ripped off, и им можно доверять. Я не согласен с некоторыми их методами, но в целом они довольно хороши.

Я просто хотел высказать пару вещей.

```
Lex
```

TRASk, Animator, Ogre Ogre busted

408 under siege

Всё это произошло ближе к концу недели после Phoenix Phortress Sting Operation.

TRASk, sysop of Shattered World Elite, carded an IBM PC. Человек, к дому которого его должны были доставить, оказался дома, когда доставка прибыла. Владельцы немедленно вызвали полицию, которая устроила stakeout и стала ждать ничего не подозревающего TRASk, который должен был прийти и забрать его. TRASk пришёл и, конечно, был caught red-handed.

Animator подошёл к дому, но остался на улице. Ситуация ему не понравилась, и он не остановился. Он пошёл домой к BelGarion и Ogre Ogre, brothers. Неизвестно ему, за ним проследили. Поскольку в тот день он прогулял школу, он оставался там до 4 PM.

BelGarion и Ogre Ogre пошли к дому Animator, забрали всё его computer equipment and illegally carded stuff и спрятали всё это в своём доме. Через несколько минут после того, как Animator покинул дом BelGarion, его picked up by the police. Затем его доставили в Juvenile Detention, где он нашёл TRASk.

Тем временем полиция сначала пошла к дому TRASk и забрала всё его имущество, включая BBS, затем к Animator. Когда они добрались до дома Animator и ничего не нашли, его little brother рассказал им, что BelGarion и Ogre Ogre забрали всё. Затем они пошли к дому BelGarion, где нашли не только carded material Animator, но и вещи BelGarion и Ogre Ogre.

Все четверо провели weekend вместе в Juvenile Detention.

Обвинения включали:

• Fraudulent use of a credit card.
• Grand theft.
• Possession of stolen property.

Merchandise, найденный у BelGarion, превышал 3000 долларов.

Поскольку BelGarion исполнилось 18 лет, Ogre Ogre, его младший брат, взял полную responsibility for the crimes. В результате обвинения против BelGarion были dropped.

Судебное дело ожидается в середине апреля 1986 года.

Интересная часть этой истории в том, что TRASk и остальные были members of the Nihilist Order. У этой группы большинство участников уже были busted или under surveillance из-за Phoenix Phortress Sting Operation in Fremont, California. Есть ли связь?

BelGarion говорит, что нет, и что Nihilist Order на самом деле была loosely connected bunch. Однако её основали TRASk и The Highwayman.

TRASk был released with a $100 fine, probation and 100 hours of community, civil, service work. Его BBS, The Shattered World Elite, снова поднимется когда-нибудь в будущем.

Информацию о Phoenix Phortress Sting Operation см. в Phrack World News Issue III.

Информация предоставлена: BelGarion 408 в интервью с Knight Lightning.

Robin Hood и The Sultan busted

408 under siege

Это событие произошло примерно в последнюю неделю марта в California, area 408.

Robin Hood вывихнул ankle на wrestling meet и в результате несколько дней лежал дома. В один из таких дней он проснулся в 1:30 PM и услышал людей снаружи, пытающихся force his doors open. Ковыляя на crutches, он добрался до кухни, где столкнулся с тремя police officers, двумя special investigators и одним человеком из PacBell Security.

Его первым криком было: «У вас лучше бы был warrant!» Разумеется, он у них был. Он заметил на нём MCI codes and dialups, а также passwords to TRW. Примечание редактора: очевидно, именно это они искали. Они пошли в его комнату и просмотрели computer disks, один из которых был labeled phreaking and hacking, printouts, notebooks и всё остальное, что могли найти. Они забрали всё, включая modem, printer, phone and computer.

Среди конфискованного были printouts of Phrack Issues I-III, Hack Newsletter, all issues to date, tons of other G-philes и Lex Luthor's Hacking Cosmos series. Также были взяты все board numbers, где он был, и все passwords. К счастью для Metal Shop PRIVATE, он ещё не получил новый general password. Boards, которым следует быть настороже, включают The Alliance и P-80.

Его обвинения включают:

• Annoying Calls, scanning prefixes.
• Defrauding the phone company.
• Illegal entry, hacking.
• Scanning MCI dialups, legal name неизвестен автору.

Его и Sultan court case назначено на 18 апреля 1986 года, 1:00 PM.

Что касается Sultan: после своего bust Robin Hood пытался связаться с ним в школе, не зная, что группа, посетившая его, пришла от Sultan earlier, примерно в 11:30 AM. Когда он наконец дозвонился до него около 4:00 PM после школы, на swim practice, было уже слишком поздно. Отец Sultan, предположительно, имел government-related job. Автор не знает, была ли она political.

Полиция забрала у Sultan всё, включая телефон. После bust его phone line была disconnected.

Robin Hood сказал, что ему сообщили: он находился under surveillance за 2-3 months до arrest.

Он также вспомнил, что у полиции был третий warrant на кого-то в другом town. Он не узнал имени и позже ничего об этом не слышал.

Примечание редактора: их accounts на Metal Shop PRIVATE давно удалены, так что users MSP могут не беспокоиться.

Информация предоставлена: Robin Hood во время интервью с Knight Lightning.

TWCB: Peter снова арестован

TAP trouble

В последнюю неделю марта, во время spring break, Peter из TWCB Inc. был arrested, или, может быть, просто picked up, за то, что покинул дом, находясь под court order оставаться confined there under his mother's reconnaissance.

Его picked up тот же detective, который изначально busted TWCB Inc. Очевидно, он некоторое время вёл stakeout у их condominium.

Это не только добавляет к их large record and current charges, но и будет использовано, чтобы показать суду, что мать TWCB не контролирует их. Это повредит их defense.

Возникло много вопросов о предстоящем court case against TWCB. Самый заметный: как они смогут публиковать TAP Magazine с таким record и constant surveillance? Поскольку их bust был в основном non-phreak/hack related, возможно, нет реальной причины опасаться problems arising of information trading for a lighter sentence, if or when found guilty.

Однако их bust также касался fraudulent use of a credit card. Что, если это свяжут с phreak/hack bulletin boards?

Раз уж тема TWCB уже поднята, я хотел бы упомянуть и другие происходившие вокруг них вещи.

Fights между ними и Sigmund Fraud утихли. Это не обязательно означает, что они не возобновятся. Fights with Slave Driver, из-за которых их kicked off Stronghold East Elite, тоже утихли. Не желая иметь reputation for kicking people off SEE for personal reasons, Slave Driver позволил TWCB вернуться. Пока неизвестно, сделали ли они это.

С другой стороны, имея co-sysop access, TWCB kicked Broadway Hacker off Spectre III, sysoped by The Overlord of 815. Он, в свою очередь, kicked them off the Radio Station BBS. Hostilities между ними бушевали, но Broadway Hacker publicly apologized on Metal Shop, and I suppose on several other BBSes as well, to TWCB, and asked them to remove their vulgar posts about him. TWCB не дали комментария.

Broadway Hacker действительно kicked TWCB off The Radio Station. Позже он welcome them back on, но теперь, из-за их refusal to call, его invitation больше не действует.

SBS Acquisition Completed

Март 1986 года

28 февраля MCI завершила acquisition of Satellite Business Systems from IBM в обмен примерно на 47 million shares of MCI Common stock, или 16.7 percent of the 282 million shares now outstanding. Federal Communications Commission, FCC, approved the transfer to MCI of authorizations held by SBS 14 февраля. Transaction была объявлена as an agreement in principle 25 июня 1985 года.

Большинство сотрудников SBS joined MCI, доведя employment MCI до 14 800.

Изначально для 200 000 customers SBS acquisition не приносит изменений в service or rates. Eventually, SBS system будет объединена с более extensive domestic and international network MCI.

```
Taken from MCI World, March 1986
```

Phrack World News IV, часть 2

Составил: Knight Lightning

More Computel

Воскресенье, 29 марта 1986 года

Следующий post был замечен на Stronghold East Elite в указанную дату и касался Computel. Я перепечатываю его в Phrack с единственной целью: распространить эти важные новости, помочь 2600 Magazine разобраться в этой mess и помочь всем вернуть свои деньги.

Люди,

пожалуйста, расскажите нам всё, что знаете о Computel, даже если это не кажется важным. Мы full speed ahead ведём наше investigation и уже обнаружили кое-какие wild things, но не можем раскрывать то, что у нас есть, пока не закончим. Нам также нужна информация о старом журнале под названием *Tel* из 70-х.

Да, мы установили, что между ними была связь, но это всё, что мы сейчас можем сказать. Любая информация или даже back copies помогли бы. Нам нужны люди, которые действительно готовы пожаловаться на потерю денег. До сих пор это оказалось самой трудной частью. Phone phreaks, как правило, не хотят ставить своё имя ни на что, но если вы потеряли деньги, это единственный способ, которым мы можем вернуть их вам и одновременно остановить эту operation.

Нам нужны люди, живущие near or in Van Nuys, California. Нам нужно, чтобы те из вас, у кого есть special access to credit information or phone information, связались с нами. **Please don't delay.** Отправляйте нам e-mail или звоните по `(516) 751-2600`.

```
Information posted by 2600 Magazine
```

Примечание редактора: Thomas Covenant добавил, что слышал, будто Computel is unregistered and plans on staying that way. Поэтому Better Business Bureau ничего не может сделать.

Dr. Who in trouble

Вторник, 31 марта 1986 года

Ниже interpretation and information Lex Luthor по истории Dr. Who. Он также обсуждает Twilight Zone и Catch 22. Сообщение было posted in several places, most notably Stronghold East Elite, и подтверждено в интервью Lex Luthor с Knight Lightning 4 апреля 1986 года.

Twilight Zone вернётся через 1-2 недели. Те, кого Marauder хочет видеть там, будут contacted with all the new logon info вместе с номером для доступа. Он делал некоторые mods to the software, поэтому board была down.

Silver Spy, sysop of Catch-22, имел phone problems, и как только phone company это исправит, он поднимет board снова. Обе boards действительно ушли down на несколько дней после Doctor Who bust, но после того как мы выяснили, почему его busted, boards вернулись.

Secret Service пришла в дом Who и забрала всё. Его тогда не было дома, но через 1-2 дня они наконец добрались до questioning him. Как вы знаете, Secret Service проводит много credit card investigations. Изначально Pit Fiend of CA был busted for carding, см. quick notes прошлого issue, и в

то время он время от времени разговаривал с Who. Поэтому некоторые считают, что bust Who был результатом того, что P.F. leaked info to the S.S.

LOD/H не был слишком shaken up из-за bust Who, главным образом потому, что это было not phreak/hack related, a merely credit related, чем LOD/H не занимается. Who не carded anything, но мы считаем, что motive S.S. для bust was use of TRW. Кстати, у Who был DNR on his line for 7 months; некоторые говорят, что больше года, но в любом случае это hell of a long time. Вот и всё. Если кому-то нужны specific details или если кто-то слышал otherwise, дайте мне знать.

```
Lex
```

Информацию предоставил: Lex Luthor.

Примечание редактора: Lex Luthor также упомянул, что Dr. Who is being sued by AllNet.

Members of 2300 Club busted

Cleveland

Двое были caught for fraudulent use of a credit card, и один был arrested for car theft.

2300 Club теперь сравнивается и treated as a miniature mafia местными властями. Это главным образом из-за other crimes, including the blowing up of cars. King Blotto был, по крайней мере в какой-то момент, member of this group. Нет абсолютно никакой информации о том, что King Blotto был busted или всё ещё является member of the 2300 Club.

New phreak/hack group

6 апреля 1986 года

The Dark Creaper (916), Brew Associates (215), Major Havoc (301) и ещё один человек, handle которого сейчас мне неизвестен, формируют новую phreak/hack group. Её название — **The IBM Syndicate**.

Сейчас они ищут members. Их bulletin boards, которые сейчас более или менее public, очень скоро станут private, что усложнит becoming a member. Eventually group будет иметь 2 BBSes and 2 AEs, mainly for the exchange of files and IBM kracked wares. Все эти BBSes, конечно, будут run on IBM, и я предполагаю, что наличие IBM является requirement to become a member.

Информация предоставлена: Dark Creaper through interview by Knight Lightning.

Oryan Quest busted / 415 gets hit again

6 апреля 1986 года

В среду, 2 апреля 1986 года, Oryan Quest был arrested on charges of computer invasion. Технически у них было только одно charge, но later evidence accounted for the other two.

Oryan Quest был busted for hacking AT&T Mail, roughly similar to MCI Mail. У него было three different accounts, но San Mateo Police and FBI подозревали только один. Когда они searched his home, они нашли ещё два written down.

Обвинения против Oryan Quest были dropped по нескольким причинам:

1. Illegal search, у них не было warrant.
2. Police brutality and harassment, ero pushed around and slammed his head into a car.

Власти searched his house, пока Oryan Quest был в школе, где его позже и arrested.

Что было taken:

```
Loads of computer disks
All printouts, his entire g-phile library
10 meg drive
Assorted boxes: blue, red, green, silver
```

Его passwords, BBS numbers, codes и т. д., как он считает, не были discovered.

Court date ещё не была set, и считается, что prosecuting attorney drop the case из-за earlier illegal proceedings by the SMPD.

До arrest SMPD monitored his line и обнаружила, что он scanning prefixes. Однако это inadmissible in a court of law, потому что в момент monitoring his line не было sufficient evidence for such action.

AT&T Mail была accessible through an 800 number, which Oryan Quest did call direct.

Несколько слов от Oryan

> *I have no intention of quitting hacking.*
>
> *My mistake was calling an 800 number direct and for fucking around with AT&T in the first place.*
>
> *I am more of a hacker than a phreak.*

Примечание редактора: когда его спросили, что он чувствует по поводу происходящего, он ответил: «I'm not worried about it».

Ещё один интересный факт об Oryan: он имел part-time job as a PacTel Operator. Ему было 15 лет, он солгал о возрасте, сказав, что ему 16, но теперь был fired.

Также SRI сделала ему job offer for computer security. Он думает об этом, но не планирует принимать предложение.

Информация предоставлена: Oryan Quest through interview by Knight Lightning.

Overlord 815 arrested for check fraud

> *The only reason I got caught was greed.*

Это было первое statement Overlord (815) мне во время interview 6 апреля 1986 года. Он говорит, что изначально, давно, концентрировался на Western Union, но позже turned to credit card fraud. По мере продвижения он понял, что credit card fraud работал только примерно в 5% случаев. Ему хотелось чего-то, что работает 100% of the time. Он нашёл это: check fraud.

В своём hometown он acquired около 4000 долларов equipment из трёх stores. Среди merchandise были Apple //e, with every card possible, the best drives, monitors и т. д., complete Commodore 128 system и десять packs of disks for good measure. Его downfall состоял в том, что на следующий день он вернулся в один из тех же stores and tried it again.

Его instantly caught and tricked by the police to reveal more than he would have if he had really known his rights.

Check fraud is a felony crime. Хотя я сам uninformed as to how to perform the art of check fraud, it must require a phone, потому что Overlord (815) сообщает мне, что police labeled his crime as Telefelony. Actual charge, however, is for `theft by deception`.

Его дом не searched, и он вернул all merchandise.

Он сказал мне, что планирует stop running his bulletin board Spectre III and sell his computer. Это главным образом для того, чтобы его нельзя было назвать computer hacker. Например, prosecuting lawyer спросил бы: «Do you have a computer?!» Он сможет truthfully say no.

Он планирует, что BBS будет run from the home of The Master (815), a number would stay the same.

Другая версия этой истории от TWCB Inc. говорит, что Overlord передумал and is not selling his computer or taking down Spectre III.

Court date назначена на 9 апреля 1986 года. Overlord (815) говорит, что худшее, что может случиться, — probation, fine, civil service work или any combination of the three.

Информация предоставлена: Overlord (815) during interview with Knight Lightning.

TAP: latest news from TWCB

8 апреля 1986 года

Как многие из вас могли заметить, TWCB Inc. не выполнили promise выпустить TAP Magazine by April 7, 1986. Когда их спросили об этом в тот день, они ответили, что весь stuff у них есть, но его нужно typeset, format, print and distribute. Они estimated, что смогут сделать это ещё за four days. Этот secondary deadline также не был achieved.

Writers, according to TWCB, include:

```
Abbie Hoffman
Ace
Final Impulse
Gary Seven
Knight Lightning
Mark Tabas
Taran King
Susan Thunder
The Bootleg
The Cracker
The Firelord
The Metallian
TUC
```

Magazines supporting TAP include:

```
Mad Mad Magazine
High Times
Bootlegger Magazine
Hacker Magazine
```

Scan Man dropped himself from the TAP Staff.

К issue 6 TWCB планирует иметь 112-page magazine. Это связано с тем, что к тому времени они ожидают получать many more articles and have several more companies advertising.

Первый issue of TAP Magazine будет иметь articles on the following topics:

```
ISDN: parts by Taran King and The Bootleg
Fiber Optics
Cellular Phones
Satellite Jamming
Moving Satellites
```

```
The Teltec Bust: Surfer Bill / The Firelord / TWCB Inc. / Knight Lightning
Dr. Who Bust
History of TAP
RSTS 8.0
Signalling Systems: taken from Phrack Inc. Newsletter
Introduction to PBXs: by Knight Lightning, taken from Phrack Inc. Newsletter
ROLM: by Monty Python, taken from Phrack Inc. Newsletter
MCI Overview: by Knight Lightning, taken from Phrack Inc. Newsletter
New BBS Laws: by Sally Ride, taken from Bootlegger Magazine
Cosmos: by Lex Luthor and the Legion of Hackers, taken from Bootlegger Magazine
Private Audience: by Final Impulse, taken from Phrack Inc. Newsletter
UNIX: by The Cracker
MAX Profile: by Phantom Phreaker, taken from Phrack Inc. Newsletter
Crashing Dec 10s: by The Mentor, taken from Phrack Inc. Newsletter
Pak Time: by Kerrang Khan
Techniques of Tracing
ESS: by Mark Tabas
```

Информация предоставлена: TWCB Inc. during interview with Knight Lightning.

Quick notes

23 марта 1986 года The Radio Station BBS in New York celebrated its one year anniversary. Теперь у неё one meg of storage online.

Слух о том, что Taran King был на talk/news program in New York discussing hacking, completely wrong. Dead Lord started it, but as yet no one knows why.

The Tempest in 805 was burglarized in March. Его computer и всё прочее equipment, among other things, были stolen. Это, конечно, объясняет его absence from the BBS world for a while.

Довольно новая IBM kracking group, formerly the Imperial Warlords, now known as Five-O, re-kracking software and claiming it to be original by themselves. Furthermore, они размещают insulting messages inside the software toward certain individuals.

The Kidd of 408 got busted for selling codes at his school for five dollars apiece. Конкретная company не упоминалась.

Video Stalker (408) carded some stuff to the home of Sinbad. Sinbad told him that he would sign for the stuff, and when he did, he was arrested. Больше details unavailable.

The Tunnel, одна из старейших phreak/hack boards in Austin, Texas, вышла из closet. The Tunnel revealed on the local news to be run by the computer crime division of the Austin Police Department. Две главные цели board были: A) catch carders и B) catch Mentor and Cisban Evil Priest trying to sell those stolen computers. Они были очень successful at A.

Stronghold East Elite announced its new advisors. Hack advisor: Lex Luthor. Phreak advisor: Blue Buccaneer. Soon they plan to have a name change, because Apple Commander of Stronghold North insists the two boards are affiliated, while Slave Driver and Equalizer of Stronghold East feel differently. With instruction from Lex Luthor, SEE enacted new security measures.

Thanks to 2600 Magazine, Stronghold East Elite now has the complete court transcripts of the bust that took place early last summer, most notably concerning Private Sector and six others, online for viewing.

Sigmund Fraud has been discharged as co-sysop of the Radio Station BBS.

Captain Crunch of 512 stated that an auto-dial program he wrote and uploaded was copied by TWCB Inc., who then claimed it as their own and signed their name in it.

Закат фрикинга во Флориде: история Teltec

Автор: Knight Lightning

Интервью с Surfer Bill, проведённое The Firelord

Записано и оформлено Knight Lightning

Firelord (FL): Билл, я хотел расспросить тебя про тот арест, о котором ты рассказывал.

Surfer Bill (SB): Ага, что конкретно хочешь знать?

FL: Кого вообще взяли?

SB: Если хочешь знать, кто в курсе куда лучше меня — это Jack Flack. У него есть повестка, страниц сорок, там перечислены все имена и все обвинения слово в слово — невероятно.

FL: Jack Flack не принимает звонки, оно и понятно — наверное, не лучшая идея.

SB: Teltec базируется в Майами, и они реально взбесились из-за того, что все злоупотребляли их услугами. То есть пользовались их кодами и всем таким прочим. Эти люди не дураки. Они знают, если на систему посадили последовательный хакер. Знают, потому что их компьютер фиксирует каждый неверный код. Если они видят 20000, 20001, 20002 — и это продолжается, всё регистрируется как неверные коды, а потом вдруг 20011 не регистрируется, зато 20012 — регистрируется, они понимают: 20011 — рабочий код. После этого они начнут мониторить код и следить за аномальным использованием. Они будут сидеть и говорить: «Эй, этот код в последние дни работает на полную катушку». Потом поставят трассировщик, вычислят человека, прослушают линию и начнут собирать информацию о владельце. Это всё равно что самому надевать петлю на шею!

По сути, то, что я слышал о происходящем здесь: я думаю, под удар попали пять досок объявлений в районе Майами/Форт-Лодердейл/Бока-Ратон.

• Caeser's Palace (сисоп — Caeser D, его настоящее имя Джон Кесслер)
• Parasec (сисоп — Mark Barochich)
• COPS
• Apple Tree — не Apple Tree I и не Apple-Tree II, а именно Apple Tree Phreak BBS, которую теперь все знают как Catfur.
• И Plovernet (305).

FL: Ты не говорил, что Teltec засылала агентов на все эти борды?

SB: Да, именно к этому я и вёл. Точно не знаю, но, по слухам, сотрудники Teltec притворились подпольными хакерами или фрикерами и зарегистрировались на перечисленных бордах. У них были хэндлы, они внедрились в систему и убедили всех, что они фрикеры. Потому что они явно знали, о чём говорят — в конце концов, они работали в компании. Они постили действительно

грамотную информацию. И, я думаю, на каком-то этапе сами разместили коды Teltec. Опять-таки, часть из этого — слухи, часть — факты, и что есть что, я вам точно не скажу.

FL: Кого в итоге взяли?

SB: Jack Flack, Caeser D (Джон Кесслер), Demetrius Cross, Dave Peters и ещё несколько человек. Одну целую семью повязали: отца, сына и дочь. Есть список из тридцати восьми человек — их настоящие имена были опубликованы в Miami Review, юридической газете, которая рассылается всем адвокатам и судьям Майами. Ещё интересный момент: в списке упомянуты некий Джон Доу и Джейн Доу. Там была оговорка, что эти двое будут названы позднее, так что кто это — неизвестно, и не факт, что их именно двое.

FL: Ты говорил, что Lex Luthor успел ускользнуть?

SB: Да, именно.

FL: Они собирались его схватить, но он сбежал в Калифорнию.

SB: Я точно не знаю, поймали ли его или только собирались, но знаю, что он не упомянут.

FL: Может, он и есть один из Джон или Джейн Доу.

SB: Большая часть того, что я знаю, — в общем-то публичная информация, так что про этих Джон и Джейн Доу мне нечего добавить.

SB: Важный момент: агенты Teltec сами разместили коды, а потом следили за ними. Я думаю, за использование этих номеров вас арестовать не могут, потому что это провокация. Вместо этого они мониторят звонки, трассируют их и таким образом узнают, с кем имеют дело.

FL: Они подключат регистратор набранных номеров (DNR) к линии.

SB: Вся эта история — это что-то вроде перекладывания вины. Оба неправы: Teltec неправа, используя провокацию, чтобы вас поймать, и вы неправы, пользуясь их кодами для фрикинга. Поэтому они просто наблюдают. Потом говорят: «Ага, вот этот парень, Джон Доу, использует этот код. Мы знаем, что он злоупотреблял нашей системой, и теперь будем за ним следить». Когда код умрёт — посмотрят, не перейдёт ли он на другие, и если перейдёт — возьмут.

Главное, что выйдет из этого судебного дела: они пойдут за пятью людьми, которые были системными операторами бордов. За рядовыми пользователями они особо не охотятся — я думаю, рядовых пользователей используют как свидетелей против сисопов.

Пугает в этом деле то, что оно действительно крупное — оно может стать прецедентом. Если судья вынесет решение в пользу Teltec и та предъявит обвинения, в повестке указан минимальный ущерб в 5000 долларов, и именно столько они требуют. Значит, реальный ущерб явно превышает 5000 долларов. Скажу одно: судя по тому, сколько денег и сил Teltec вложила в это дело, они полны решимости довести его до конца. Они потратили немало на адвокатов и следователей. Ещё один пугающий момент: Teltec не раскрыла публично доказательства против тридцати восьми человек — по крайней мере, насколько мне известно, — и именно этого все боятся. Рядовой пользователь не знает, с чем столкнётся.

FL: Спорю, большинство людей с тех бордов сейчас обделались от страха.

SB: О, да, все в шоке — как будто весь Майами в панике. Ещё слышал, что Sprint и MCI в будущем тоже закрутят гайки. Скорее всего, ждут, чем закончится это дело.

FL: Teltec — это основная служба у вас там, которой все пользуются?

SB: Не особо, одна из многих. Популярная сейчас — MCI, у неё только пятизначные коды.

FL: Слышал, у Teltec отвратительное качество связи.

SB: Да, смешно: я разговаривал с Jack Flack и сказал — если хочешь рассмешить зал суда, и ты знаешь, что тебя точно посадят, и виновность не вызывает сомнений, — пошути: если тебя спросят, что ты знаешь о Teltec, скажи: «Всё, что я знаю о Teltec, — это то, что связь с Калифорнией у них реально дерьмовая!» Не знаю, обрадуются ли они такому ответу!

FL: Значит, они серьёзно всё это раскрутят?

SB: Да, но главная цель Teltec — именно системные операторы. Надо бы почитать эту повестку: там про сисопов написано, что они «организовывали, финансировали, руководили и осуществляли надзор за незаконным размещением и распространением кодов Teltec». «Они не удаляли сообщения, содержавшие незаконную информацию». Понимаете? Сисопы виноваты, потому что не удалили сообщения.

FL: Всё это можно было предотвратить, если бы люди пользовались случайными хакерами и случайными номерами назначения, как MegaPhreak.

SB: Ещё один момент: даже если вы используете случайный хакер, большинство людей не будут сидеть в системе с 3 до 4 ночи. Лучшее время для сканирования — обычные рабочие часы.

FL: Это верно, в конце концов, вам не нужно 10 000 кодов.

SB: В общем, я думаю, что они реально охотятся за сисопами. И если Teltec выиграет это дело — оно станет прецедентом. Если всё так и случится, ожидаю, что подобных дел по всей стране станет намного больше.

Примечания редактора: Есть разговоры о том, что на самом деле было взломано не 5, а 6 бордов. Кроме того, упоминание о какой-либо причастности Lex Luthor к Teltec или о его «близких звонках» — лишь слухи. Другие источники из кода 305, пожелавшие остаться неизвестными, подтверждают, что MCI действительно усилила борьбу с фрикерами и хакерами. Сисопы, пожалуйста, тщательно проверяйте, кого допускаете.

Помните: фильтр или плата за вход на борду легко обходятся агентами и следователями. Лучший способ проверить людей — через рекомендации.

TWCB также присутствовал в сети во время этого интервью, но поскольку он почти или совсем не внёс вклада в реальное содержание файла, все его реплики были отфильтрованы как не представляющие ценности.

Исходное интервью было проведено на конференц-связи и записано на кассету, которую мне доставили. После этого я написал этот файл. Разрешение на публикацию в Phrack World News предоставлено The Firelord из кода 307 NPA.

— Knight Lightning

Телефонные показания, март 1986 года

Председатель Билл МакГоуэн обратился к Подкомитету Палаты представителей по телекоммуникациям. В ходе показаний на недавно возобновившихся слушаниях по конкуренции в телефонной отрасли МакГоуэн выступил против «диверсификационной лихорадки» компаний Bell Operating Companies (BOCs). Он сообщил парламентскому подкомитету, что отрасль всё ещё находится в процессе перехода к полной конкуренции, и предостерёг от замены регулируемой монополии семью нерегулируемыми.

Информация взята из MCI World, март 1986 года

Арест Kaptain Krash

Kaptain Krash был пойман на краже конференц-связи компании American Telephone & Telegraph (AT&T) через 800-й PBX, опубликованный на P-80. Родители изолировали его от других членов андерграунда.

Примечание от Forest Ranger:

ПУСТЬ ЭТО СТАНЕТ УРОКОМ ДЛЯ ТЕХ, КТО ПОЛЬЗУЕТСЯ 800-НОМЕРАМИ PBX. ЗВОНКИ НА 800-НОМЕРА PBX — ВСЁ РАВНО ЧТО ЗВОНКИ ЗА СЧЁТ ВЫЗЫВАЕМОГО: ВАШ НОМЕР АВТОМАТИЧЕСКИ СТАНОВИТСЯ ИЗВЕСТЕН. ПОЭТОМУ ОЧЕНЬ ЛЕГКО ОТСЛЕДИТЬ ВАС ВО ВРЕМЯ КОНФЕРЕНЦИИ, ИЛИ ЭТО БУДЕТ УСТАНОВЛЕНО ПРИ ПОСЛЕДУЮЩЕЙ ПРОВЕРКЕ.

Информация предоставлена F.R. Communications Newsline Service (c) 1986

Metal Shop Private наводит порядок

13 апреля 1986 года Taran King и Knight Lightning провели очередную чистку журнала пользователей, удалив более 100 аккаунтов с Metal Shop Private. Это было сделано главным образом для того, чтобы устранить «мёртвые» аккаунты, засоряющие журнал, и исключить лишние записи, снижающие безопасность борды.

Желающие стать членами Metal Shop Private должны связаться с Taran King или Knight Lightning по электронной почте. После этого их кандидатуры будут обсуждены со Staff Metal Shop и т. д.

Дэн Паскуале ищет новых развлечений

Это сообщение главным образом адресовано сисопам бордов. Замечаете ли вы увеличение звонков из кода 415 NPA? В разговоре с Дэном Паскуале (см. статью о Phoenix Phortress в PWN III) High Evolutionary узнал, что Дэн планирует попробовать свои силы на иногородних бордах — «ради развлечения». Стоит помнить, что Дэн Паскуале управлял Phoenix Phortress BBS и как таковой видел посты для других фрик- и хак-бордов. К тому же, по нехорошей привычке, многие пользователи бордов, по всей видимости, используют одинаковые пароли в нескольких местах. Поэтому существует вероятность, что Дэн сможет войти на борды под чужим именем.

«Инцидент с радиостанцией»

Oryan Quest попросил Broadway Hacker удалить его из журнала пользователей ради безопасности самой Radio Station. Однако BH решил не делать этого в тот момент. Примерно через неделю кто-то, используя пароль Oryan Quest, вошёл на Radio Station BBS. Этот человек был совершенно безграмотен в компьютерном отношении. Например, он набрал «HELP» вместо «?» для вызова меню. Когда Broadway Hacker прервал его в режиме чата, этот «Oryan Quest» сбросил связь.

Обратите внимание: хотя полиции и пришлось снять обвинения с Oryan Quest из-за незаконного обыска, это не означает, что полиция не могла обнаружить его пароли.

Broadway также упомянул о волне новых пользователей, регистрирующихся из кода 415 NPA.

Сисопы, будьте бдительны.

Часть информации предоставлена Broadway Hacker / High Evolutionary / Oryan Quest

---

Максфилд высказывается

В детройтской газете Джон Максфилд дал интервью репортёру. Хотя у меня нет ни самой статьи, ни всех относящихся к ней фактов, известно, что среди упомянутых имён значатся: Phantom Phreaker, High Evolutionary, Scan Man, Music Major, The Bootleg и Slave Driver.

Предполагается, что Максфилд получил эти имена с P-80. Впрочем, это чистые домыслы.

Информация предоставлена различными источниками