Phrack RU issue 006

Русская версия Phrack, выпуск 006. Полный текст статей с кодом и таблицами.

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

Материалы выпуска: Introduction; Phrack Pro-Phile 3: User Groups and Clubs; The Techno-Revolution; Как развлечься с зажигалкой Bic (или любой другой); Пакости в Unix; Дымовая бомба; Cellular Telephones; Wide-Area Networks, часть 2; Phrack World News V, часть 1; Phrack World News V, часть 2; Phrack World News V, часть 3; Требуются законы для взрослых против компьютерных преступников; Дэниел Зигмонд: настоящий журналист или внештатный агент ФБР?.

Introduction

Автор: Taran King, sysop of Metal Shop Private

Добро пожаловать в Phrack Inc. VI. Мы несколько задержались с выпуском из-за проблем в моей домашней жизни, подробности см. в PWN этого выпуска, но вот мы здесь.

Сейчас Metal Shop Private down, но когда я вернусь к real life, он должен снова появиться с новой BBS program и, надеюсь, будет лучше, чем когда-либо.

Теперь, с выходом Telecomputist Newsletter, у нас появилась возможность иметь Phrack Inc. printed out.

Если вы чувствуете, что хотели бы subscribe на что-то подобное, это работало бы таким образом: одним из наших положительных пунктов будет то, что оно до некоторой степени бесплатно. Вы, subscriber, будете платить за postage и, если необходимо, envelopes, а также P.O. Box rental, но всё это не должно составить много.

Если вам интересно получить это, пожалуйста, свяжитесь с любым member of the Metal Shop Family или Phantom Phreaker of The Alliance и сообщите свои opinions. Если мы получим достаточно support, мы запустим это. Later on.

```
TARAN KING
Sysop of Metal Shop Private

Title by Author (amount in K)

1     Index by Taran King (1k)
2     Pro-Phile on Groups by Knight Lightning (14k)
3     The Technical Revolution by Dr. Crash (4k)
4     Fun with Lighters by The Leftist (2k)
5     Nasty Unix Tricks by Shooting Shark (4k)
6     Smoke Bombs by Alpine Kracker (2k)
7     Cellular Telephones by High Evolutionary (5k)
8     Wide Area Networks by Jester Sluggo (10k)
9-13  Phrack World News by Knight Lightning (16,15,15,16,15K)
```

Phrack Pro-Phile 3: User Groups and Clubs

Авторы: Knight Lightning and Taran King
Дата: 10 июня 1986 года

Добро пожаловать в третий выпуск Phrack Pro-Phile. Информация здесь изначально должна была появиться как специальный выпуск PWN, но вместо этого стала Phrack Pro-Phile данного выпуска. Taran King и я собрали много сведений о разных clubs and groups сегодняшнего и вчерашнего дня и скомпилировали их в форме, которую вы сейчас увидите.

Extasyy Elite

История Extasyy Elite печальна: group буквально была destroyed by its own members. The Poltergeist сдал всю Extasyy после того, как его busted for carding. Это привело authorities к The Mentor, который украл 30 Apple //e. Bust Mentor почти привёл к The Protestor, но, к счастью, The Mentor успел предупредить Protestor. См. Phrack World News Issue III.

Membership of the club included:

```
Bit Blitz                   Cisban Evil Priest
Crustaceo Mutoid            Kleptic Wizard
The Mentor                  The Poltergeist
The Protestor
```

Crustaceo Mutoid позже joined the Racketeers, но теперь он и The Mentor пишут для California newsletter под названием *Underground Informer*.

Extasyy hanging out on Hack Net BBS and FWSO, BBS in Colorado.

Fargo 4A

Эта group started on a conference, состоявшей из Bioc Agent 003, TUC, Big Brother, Quasi-Moto, Video Warhead и Wizard of Arpanet. Они подключили к conference несколько Directory Assistants, и каждый участник assumed a role of some sort of telco agent.

Они сказали DA, что все их calls will be re-routed to a different location. Некоторых DA удалось заставить поверить им, и некоторых из них almost laid off because of this conference. Кстати, Fargo находится in North Dakota; именно оттуда была первая DA.

Считается, что Wizard of ARPAnet был busted by John Maxfield, a BIOC completely retired from the phreak world. Эта group была unofficially disbanded, но несколько её members всё ещё active.

Five-O

Довольно новая IBM kracking group, formerly the Imperial Warlords. Сейчас они re-kracking software and claiming it to be original by themselves. Они известны тем, что помещают insulting messages toward certain people inside their re-kracked software.

IBM Syndicate

Эта group была formed around April 6, 1986. Charter members included Dark Creaper (916), Brew Associates (215), Major Havoc (301) и ещё один человек, handle которого сейчас мне неизвестен. Это была new phreak/hack/pirate group. К сожалению, эта group, как и многие другие, умерла within its first month.

Icub (International Computer Underground Bandits)

Это hack/phreak group, whose main emphasis is on phreaking. Она based in Memphis, Tennessee. В ней 10 members, и единственный semi-active member left is Doc Holiday. Больше о группе известно мало, кроме того, что она inactive и никаких announced plans to revive it не было.

LOD/H: Legion Of Doom / Hackers

Эти две groups очень тесно переплетены. Обе были formed on Plovernet. Founding member был Lex Luthor. Through the years были LOD/H bulletin boards вроде Blottoland, LOD, FOD и т. д. Сегодня есть Catch 22 и новая LOD BBS, supposedly being run by King Blotto.

Current member list:

```
Legion Of Hackers                   Legion Of Doom
-----------------                   --------------
Blue Archer                         Phucked Agent 04
Gary Seven                          Compu-Phreak
Kerrang Khan
Lex Luthor
Master Of Impact
Silver Spy (Sysop of Catch 22)
The Marauder
The Videosmith
```

LOD/H известна как одна из oldest and most knowledgeable of all groups. В прошлом они написали many extensive g-philes about various topics. Please forgive any mistakes in the member list, since this list was provided by Lex Luthor approximately 1 1/2 - 2 months ago.

Metal Communications

Очень большая group, написавшая many files throughout its existence. Некоторые boards в её menagerie включают Speed Demon Elite, Metal AE, Metal Works AE, Metalland I и несколько других.

Membership of Metal Communications includes:

```
Cobalt 60
Crimson Pirate
Dr. Local
Red Pirate
Shadow Lord
The Angel Of Destiny
The Apothecary
The Byte
The Byte Byter
The Dark Wizard
The Duke
The Dutchman
```

```
The Man In Black
The Prophet
The Pink Panther
The Voice Over
The Radical Rocker
The Warlock Lord
White Knight
```

Red Pirate, Crimson Pirate и Dr. Local являются main ware distributors группы.

Subsidiary of Metal Communications — Neon Knights, whose membership includes:

```
Baby Demon
Jolly*Roger
The Blade aka Killer Kurt
The Master of Reality
The Metallian
The Outland
Zandar Zan
```

PAG / PAP

PAG: Phreaks Against Geeks.
PAP: Phreaks Against Phreaks Against Geeks.

PAG была formed by TWCB Inc. as a joke on a conference in December 1985. Charter members were TWCB Inc., taRfruS, Blue Adept, The Clashmaster and a few others. Later, Catcher in the Rye and the Slovak wanted to join.

PAP была formed in resistance to PAG by Boston Stangler and Micro Man. Несколько других sided with them, но never formal members.

Вся эта nonsense really started on the Dartmouth system и была mainly a feud between phreaks in the Boston (617) area until TWCB got involved.

The Administration

Эта group была sort of in two parts: The Administration and Team Hackers '86. Membership:

```
Adolph Hitler..............Team Hackers '86
Alpha Centauri
Author Unknown.............Team Hackers '86
British Bloke..............Team Hackers '86
Dark Priest
David Lightman (214).......Administration Leader / Team Hackers '86
Dr. Pepper
Hewlett Hackard
Major Havock...............Team Hackers '86
Mane Phrame
Mark Twain
Phoneline Phantom 1 - *Not* a member of Phoneline Phantoms
Red Baron
Renegade Rebel
Sasha Kinski...............Team Hackers '86
The President
Walter Mitty
```

Group temporarily disbanded for reasons dealing with security, but now is back together. Другие новости об этой group см. в текущем PWN.

The Nihilist Order

Эта group на самом деле была loosely connected bunch of friends and phreaks, not a true club. Она based in Fremont and Sunnyvale, California. Её started by TRASk and The Highwayman.

Membership includes:

```
BelGarion
Ogre Ogre
The Animator
The Highwayman
TRASk
```

Все members of the group были busted or involved in busts in the past few months. The Highwayman bit it in the Phoenix Phortress Sting Operation, and the others all got caught on a carding scam, although BelGarion was later released with no record.

Одна из boards in the Nihilist Order's network — Shattered World Elite, sysoped by TRASk. The group is currently inactive.

The P.H.I.R.M.

Довольно новая group, recently accused, without proof, of being fed invested.

О ней известно немного, поскольку они disclosed very little information. Некоторые boards that are now P.H.I.R.M operated include Thieve's Underworld, sysoped by Jack The Ripper, World's Grave Elite, sysoped by Sir Gamelord, and SATCOM IV.

The P.H.I.R.M. reportedly will be releasing a newsletter.

Membership supposedly includes:

```
Archangel
Blade Runner
Jack The Ripper
Sir Gamelord
The Stingray
```

Rumored that Blade Runner is the same person as Archangel and/or The Stingray.

TPM (The Punk Mafia)

При последней проверке в этой group было eight members. Полный список:

```
Arthur Dent                 Creative Chaos
Erik Bloodaxe               Gin Fizz
Ninja NYC                   Peter Gunn
Rudolph Smith (703)         The Godfather (703)
```

Group will be going through a rebirth this summer. Их main goals include burglary, fraud, hacking and phreaking. Most recently The Godfather retired and Ninja NYC came very close to being busted. См. Phrack World News Issue V.

The Racketeers

Новая Apple pirating group была assembled by Apple Rebel. Membership now includes:

```
Apple Rebel
Crustaceo Mutoid
Hot Rod
The Micron
The Warezird
```

Tribunal Of Knowledge

Эта group formed very recently by Blue Buccaneer and High Evolutionary with one purpose in mind: get together to trade knowledge and information, and discuss this information until all members had a good working knowledge of it. Final result would be g-philes written by the group about the topic. В целом это была хорошая идея.

Complete membership includes:

```
Blue Buccaneer          Chef Boy R Dee
Cyclone II              High Evolutionary
Night Stalker           Paradox
Professor Pixel         Slave Driver
The Inspectre           The Seker
The Wild Phreak
```

2300 Club

Based in Cleveland, Ohio. 2300 Club теперь compared and treated as miniature mafia by local authorities. Это mainly for crimes including the blowing up of cars. Two of the members were caught for fraudulent use of a credit card and one has been arrested for car theft. Which members that refers to, I don't know, but membership included:

```
Dr. Gorey                   Dr. No
Eagle Eyes                  Judge Dredd
King Blotto                 Mr. Modem
Prince Squid                Spectreman
The Formatter
```

2600 Club / New 2600 Club

Both groups are no longer in existence. Originally started as a local group of friends in St. Louis, Missouri, it gained members quickly, too quickly. As membership grew, unity and productivity lessened until the groups finally broke up.

However many members of 2600 Club now write, or have in the past written, for Phrack Inc. Among them:

```
Cheap Shades
Data Line
Dr. Crash
Forest Ranger
Gin Fizz
Jester Sluggo
Knight Lightning
Monty Python
Phantom Phreaker
Taran King
The Clashmaster
```

2600 Club had no relation to 2600 Magazine.

Warelords

There are 13 members in the Warelords, based in California, Maryland, Tennessee, Washington D.C. and Wyoming. Billibuster, a member of the group, said that the Warelords are a phreaking and carding group that also writes programs and sells them. He claims that they are not pirates. The group isn't very active.

Other groups

```
Catholics Anonymous: A pirate group
Elite Phreakers and Hackers Club: From World of Cryton
Feds R Us: Joke by King Blotto
High Mountain Hackers
Imperial Warlords: See Five-O
Inner Circle: The Cracker (author of "Out of The Inner Circle")
Kaos Inc.
Knights of Shadow: Sir Knight
MPG: Midwestern Pirates Guild
NASA Elite: Captain Kid
Neon Knights: See Metal Communications
Phlash: A relatively new Amiga kracking group
Phoneline Phantoms: The Colonel, The Duke, The Executioner, and The Sprinter
Phreak Hack Delinquents: Metro Man and the Reaper (212)
Project Genesis: Sigmund Fraud
RDTF: Red Dawn Text-Files, Saltheart Foamfollower (SE) and Brain Gadget (Ca.)
Shadow Brotherhood
65C02 Elite (612): Wizard of ARPAnet and The Count
BBSes: Irongate, North Pole, The Guild, and The Graveyard
The Dange Gang: Maxwell's Demon
Triple Entente
2601 Club: Formed by taRfruS to combat 2600 Club
1200 Club
Ware Brigade
```

The Techno-Revolution

Автор: Doctor Crash

Hacking. Это full-time hobby, отнимающее бесчисленные часы в неделю на изучение, эксперименты и исполнение искусства penetrating multi-user computers. Почему hackers тратят значительную часть своего времени на hacking? Кто-то скажет, что это scientific curiosity, другие — что mental stimulation. Но истинные корни hacker motives лежат гораздо глубже. В этом файле я опишу underlying motives aware hackers, покажу связи между hacking, phreaking, carding and anarchy и обозначу `techno-revolution`, которая закладывает семена в сознании каждого hacker.

Чтобы полностью объяснить истинные motives behind hacking, сначала нужно быстро взглянуть в прошлое. В 1960-х группа студентов MIT построила первую modern computer system. Эта wild, rebellious group of young men стала первой, кто носил имя `hackers`. Systems, которые они разработали, intended to be used to solve world problems and to benefit all of mankind.

Как мы видим, всё пошло не так. Computer system оказалась исключительно в руках big businesses and government. Wonderful device, meant to enrich life, стала weapon, dehumanizing people. Для government and large businesses люди — не больше чем disk space, а government использует computers не для организации aid for the poor, а для control nuclear death weapons. Average American может получить доступ только к small microcomputer, worth only a fraction of what they pay for it. Businesses держат true state-of-the-art equipment away from the people за steel wall of incredibly high prices and bureaucracy. Именно из-за такого state of affairs hacking был born.

Hackers осознают, что businesses — не единственные, кто entitled to modern technology. Они tap into online systems and use them to their own advantage. Конечно, government не хочет, чтобы monopoly of technology была broken, поэтому outlawed hacking and arrest anyone who is caught. Ещё хуже government — security departments of businesses and companies. Они действуют как own private armies, and their ruthless tactics are overlooked by the government, поскольку это также serves government needs.

Hacking — major facet of the fight against the computer monopoly. Один из способов, которыми hackers accomplish their means, developed into an art in itself: phone phreaking. Важно, чтобы every hacker also be a phreak, because it is necessary to utilize the technology of the phone company to access computers far from where they live. Phone company — another example of technology abused and kept from people with high prices.

Hackers often find that their existing equipment, due to monopoly tactics of computer companies, is inefficient for their purposes. Из-за incredibly high prices legally purchase the necessary equipment impossible. Эта need породила ещё один segment of the fight: credit carding. Carding — способ obtaining the necessary goods without paying for them. Это again due to the companies' stupidity that carding is so easy, and shows that the world's businesses are in the hands of those with considerably less technical know-how than we, the hackers.

Есть последний метод этой war against computer abusers. Он менее subtle, less electronic, но much more direct and gets the message across. Я говорю о том, что называется anarchy. Anarchy, как мы её знаем, не относится к истинному значению слова, no ruling body, а к process of physically destroying buildings and governmental establishments. Это very drastic, yet vital part of this techno-revolution.

Hacking must continue. Мы должны train newcomers to the art of hacking. Мы также должны increase computer crashing. Я знаю, что crashing a computer seems a waste, but when there is no other way to subvert a business, their system must be shut down.

Как я stated above, this is only on the motives. Если вам нужен tutorial on how to perform any of the above stated methods, please read a file on it. И что бы вы ни делали, continue the fight. Знаете вы это

или нет, если вы hacker, you are a revolutionary. Don't worry, you're on the right side.

Если у вас есть question or comment about this file or the techno-revolution, just leave mail for me on the Metal Shop AE (314) 256-7284 или на любой другой BBS, где я могу оказаться.

Как развлечься с зажигалкой Bic (или любой другой)

=-=

Автор: The Leftist

=-=

Прежде всего хочу сказать, что я не несу никакой ответственности за любой ущерб, причинённый в результате использования информации из этого файла.

Дождь искр из ниоткуда

Этот трюк обычно выполняется с пустой зажигалкой. Разберите верхнюю часть, стараясь не потерять кремень и пружину, которые находятся под колёсиком поджига. Выбросьте всё остальное, если только в зажигалке не осталось немного жидкости, которую можно использовать для некоторых других вещей из этого файла. Сохраните кремень и пружину.

Итак, возьмите пружину и слегка потяните за конец, растянув её чуть длиннее кремня. Затем возьмите кремень и как бы намотайте конец пружины вокруг него. Должно получиться примерно как на рис. А. Теперь самое интересное. Возьмите пружину за конец, на котором нет кремня, и нагрейте кремень до раскалённого состояния. Не волнуйтесь, жар не обожжёт вам пальцы. Затем бросьте конструкцию кремнём вперёд в жертву, тротуар или что угодно.

```
Рис. А
               \/\/\//\/\/\/\/\/\/\/\/\------
               /\/\/\/\/\/\/\/\/\/\/\/\------ <- нагревать этот конец
                    ^                     ^
                    |                     |
                  пружина              кремень
```

Что делать с оставшимся корпусом зажигалки

Подожгите одну из опор колёсика поджига, положите зажигалку перевёрнутой в угол и бегите со всех ног! Она неплохо рванёт. Можно также взять корпус, слегка обернуть его бумажным полотенцем, подожечь полотенце, отойти назад и выстрелить в него из пневматики. Весело. Экспериментируйте, но никогда не прокалывайте зажигалку, пока держите её в руках — это было бы неразумно.

• -

Вопросы и комментарии? Свяжитесь со мной на 2400 Baud Exchange 404-925-9657.

The Leftist.
^*^

Пакости в Unix

Автор: Shooting Shark

Написано 3 апреля 1986 года

Краткое содержание: Методы саботажа вашей любимой Unix-системы.

Предисловие: Я не призываю использовать НИ ОДИН из методов, описанных в этом файле. Unix — крутая операционная система, возможно, одна из лучших систем из когда-либо разработанных во многих отношениях. Если у вас есть доступ к Unix-системе, вам следует ИЗУЧИТЬ UNIX И ИЗУЧИТЬ C, потому что именно там деньги в компьютерном мире. Однако Unix — относительно незащищённая операционная система, которую легко испортить. Данный файл объясняет несколько способов сделать это.

Обвал системы

В Unix нет встроенных ограничений на максимальный объём дискового пространства для каждого пользователя. Таким образом, один пользователь может захватить всё дисковое пространство системы и фактически лишить всех остальных возможности записи на диск. Простой способ захватить всё дисковое пространство — создавать подкаталог за подкаталогом, пока это будет возможно. Вот несколько способов сделать это.

1. Создайте файл со следующими строками:

```
mkdir subdir
cd subdir
source /u1/mydir/crash
```

Назовите его crash. Последнюю строку (`source /u1/mydir/crash`) нужно изменить так, чтобы она указывала на файл в вашем каталоге. Если ваш каталог — `/u3/students/jeff`, последняя строка должна гласить `source /u3/students/jeff/crash`. После того как вы запишете этот файл, введите:

```
% source crash
```

и ждите... через несколько минут программа завершится с ошибкой, потому что на диске больше не будет места. Ни у кого другого тоже.

2. Вот более элегантный способ сделать то же самое. Создайте следующий shell-скрипт «бесконечного цикла»:

```
while : ; do
mkdir subdir
cd subdir
done
```

затем запустите файл через `source`. Если вы используете оболочку `sh` (в этом случае у вас, скорее всего, приглашение `$`), можно набрать `while : ; do` прямо в командной строке с `$`. После этого появится приглашение >. Введите следующие три строки и откиньтесь на спинку кресла.

3. Если вы хотите запустить процесс и отключиться, и файл называется crash, введите:

```
% nohup source crash &
```

и выйдите из системы. Это запустит процесс в фоновом режиме, что позволит вам отключиться. Однако выходите из системы БЫСТРО, поскольку если вы использовали первый вариант файла

crash, он также будет безудержно пожирать фоновые процессы, что тоже в некоторой степени навредит системе. Что подводит нас к следующему разделу...

Значительное замедление системы

Существует много способов сделать это — метод заключается в создании достаточно большого числа фоновых процессов. Вот один конкретный пример. Создайте файл с именем `slow1` со следующими строками:

```
w &
source slow1
```

создайте файл с именем `slow2` со следующим содержимым:

```
source slow1 &
source slow2
```

и запустите slow2 командой

```
% slow2
```

или

```
% slow2 &
```

Это создаст 25 фоновых процессов, каждый из которых запустит ещё 25 фоновых процессов. После того как все они будут запущены, система едва будет двигаться.

Порча каталога

Многие команды работы с файлами используют параметры с «-». Создайте файл, имя которого начинается с «-», следующим образом:

```
cat > -filename
```

[теперь введите несколько строк, можно что-нибудь дерзкое вроде «ха-ха, ты не можешь удалить этот файл».] Нажмите ^D (control-d) для завершения ввода. Теперь в вашем каталоге есть файл с именем `-filename`. Удалить его будет ОЧЕНЬ сложно. Если попытаться выполнить `rm` (удаление) `-filename` или `mv` (переименование) `-filename`, программа `rm` или `mv` воспримет `-filename` как параметр, а не как имя файла, и выдаст сообщение об ошибке, что `-filename` не является допустимым параметром... и файл останется торчать как заноза.

Создайте пару сотен файлов, имена которых начинаются с «-»... тому, кому посчастливится иметь дело с этими новыми файлами, придётся по-настоящему помучиться — скорее всего, ему просто придётся завести новый логин.

Заключение

Использование любого из этих методов крайне безответственно, и если бы кто-нибудь проделал это с моей Unix-системой, я бы был очень зол. Именно поэтому я настоятельно рекомендую никогда не использовать эти трюки.

Всего доброго,
Shooting Shark

«Некоторые люди плохо воспитаны, и я говорю: если они хотят вести себя по-крутому — надавайте им по шее!» — Blue Oyster Cult

---

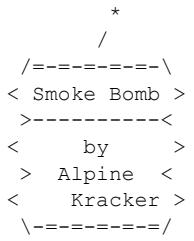
Для получения дополнительной информации о саботаже и взломе UNIX смотрите следующие статьи:

Ritchie, Dennis M. [он написал Unix] "On the Security of UNIX." Programmers Manual for UNIX System III Volume II. Supplementary Documents.

Filipski, Alan and Hanko, James. "Making UNIX Secure." BYTE Magazine, April 1986, pp 113-128.

Дымовая бомба

Автор: Alpine Kracker



Ингредиенты

• Селитра (нитрат калия)
• Сахар
• Спирт (100% — наилучший вариант, но обычный медицинский тоже подойдёт)
• Порох (или измельчённые ракетные двигатели)
• Спички (возьмите коробку из 50 упаковок — они могут очень пригодиться)
• Жестяная банка из-под кофе
• Сигарета

Инструкция

Смешайте сахар и селитру в соотношении 3:1 (сахар:селитра) и нагревайте на слабом огне до полного расплавления смеси. (Когда смесь готова, она выглядит как липкие белые комки.) В процессе нагревания необходимо постоянно помешивать, а при первых признаках дыма — немедленно снять с огня. Однажды у меня партия рванула прямо в лицо, и рабочая комната была заполнена дымом добрых полчаса. С небольшими партиями работать проще и безопаснее.

Теперь высыпьте весь этот «дымовой порошок» в кофейную банку, добавьте несколько спичечных головок, слегка увлажните небольшим количеством спирта и добавляйте порох до тех пор, пока весь дымовой порошок не окажется им покрыт. Затем вставьте сигарету между спичечными головками в нераспечатанной спичечной книжке. Вдавите книжку в смесь.

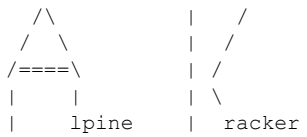
Подожгите окурок и неторопливо уйдите — у вас есть около 5 минут, чтобы обзавестись надёжным алиби.

Примечания

Селитру можно найти в местной аптеке.

Весь порох, спичечные головки и спирт нужны лишь для обеспечения надёжного воспламенения. Без них можно обойтись, но если они есть под рукой — добавьте их для надёжности. В качестве фитиля можно использовать описанный выше вариант, а также пушечный фитиль либо ракетный воспламенитель в сочетании с электрической системой.

Говорят, что четверти фунта этого вещества достаточно, чтобы заполнить дымом целый городской квартал. Не знаю, так ли это на самом деле, но общественный туалет оно точно заполняет на ура.


lpine
racker

Cellular Telephones

Автор: The High Evolutionary

Я предполагаю, что большинство из нас знает многие technical aspects of cellular phreaking, поэтому этот файл intended for general information о том, как работают эти unique devices.

Cellular, вероятно, будет successful, потому что даёт dramatic improvements по сравнению с historic automobile phones. На протяжении лет mobile radio-telephone service была крайне limited proposition. Было доступно только forty-four radio channels, а максимум около thirty назначалось на одну area. Это означало, что если все thirty channels заняты, one conversation per channel, а вы thirty-first mobile phone user, желающий сделать call, вам пришлось бы ждать thirty minutes or more, даже в городе размером с New York.

Как можно представить, mobile radio-telephone service в таком виде не могла стать очень popular. Даже при limited number of channels, long delays in making calls during busy periods и часто poor quality transmission, существовали большие waiting lists for mobile service. Но с fully equipped cellular radio-telephone system можно сделать в 5000 раз больше calls simultaneously in the same metropolitan area, opening up the service to anyone that can pay the hefty prices.

Это потому, что cellular radio-telephone systems technically quite different from traditional mobile telephones. Во-первых, FCC, Federal Communications Commission, allocated far more channels to cellular: 666 in all. Во-вторых, эти 666 channels broadcast from many different locations.

В старых mobile telephone systems была одна powerful radio station с large antenna, serving an entire city. В новой системе geographical area honeycombed with many cells, hence the name `cellular`. Каждая cell имеет собственный low-powered radio transmitter and receiver. Когда car with a cellular telephone или person carrying a portable moves from one cell to the next, call transferred automatically. Вы, скорее всего, не заметите, когда transfer takes place, хотя ваш phone suddenly switched to a different radio station and to another channel while you are talking.

Поскольку cellular signal low-powered, он не уходит далеко. Это позволяет использовать тот же channel, по которому вы говорите, for calls in other parts of the same metropolitan area without interference. Это означает, что cellular radio-telephone systems can serve a very large number of customers in an area, because there are more channels than before, and the larger number of channels are reused.

В отличие от local telephone service, provided by a monopoly, в cellular есть competition. Two classes of companies allowed to offer cellular telephone service in every market. One cellular system can be owned by a telephone company, the other by someone else. Two-company rule была adopted by FCC so that AT&T, which developed cellular, could not monopolize the whole thing.

Cellular telephones come in two basic versions: car phones and portable phones, with a briefcase hybrid. Car phones by far the most common, because they are much cheaper. Но большинство считает, что ultimately portables will be the most popular.

Richard Simmons, president of Washington Post Company, whose company is a partner in several cellular systems, даже predicts that by the early 1990s:

> *There will be phones roughly the size of calculators that you carry around in your pocket. They will cost no more than five hundred dollars. They will emancipate people from the necessity of locating a phone to make calls. The bad news is, you will never be able to get away from the phone, and we'll call it progress.*

Car telephones include a small transmitter-receiver unit, usually mounted in the trunk, an antenna and a control head including the handset. В большинстве cellular systems telephone touchpad located on the

handset. Many domestic and foreign manufacturers make cellular car phones, but so far only Motorola makes portables, the DYNA T-A-C 8000X and 8000S. Motorola's portables look like a slightly enlarged, somewhat chunky telephone handset, with a stubby antenna at one end.

Portables less powerful than car units, so they can't be used with some cellular systems. Другое limitation portable — battery life. Portable can listen for calls for about eight hours, but can transmit for only thirty minutes. After that it must be charged for a minimum of an hour.

Следующие American cities имеют cellular telephone service или soon will get it:

New York	Denver
Los Angeles	Seattle
Chicago	Milwaukee
Philadelphia	Tampa
Detroit	Cincinnati
Boston	Kansas City
San Francisco	Buffalo
Washington	Phoenix
Dallas	San Jose
Houston	Indianapolis
St. Louis	New Orleans
Miami	Portland
Pittsburgh	Cleveland
San Diego	Atlanta
Baltimore	Minneapolis

Wide-Area Networks, часть 2

Автор: Jester Sluggo

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

Лучше прочитать оба файла, чтобы лучше понимать их связь друг с другом.

Эти файлы covering general information on wide-area networks, например ARPANET, CSNET, BITNET, MFENET, UUCP and USENET, но могут содержать информацию, связанную и с другими networks, не выделенными здесь особо. Эти файлы **не** являются hacker's tutorial/guide по этим systems.

BITNET

В 1981 году City University of New York (CUNY) surveyed universities on the East Coast of the U.S. and Canada, asking whether there was interest in creating an easy-to-use, economical network for interuniversity communication between scholars. Response was positive. Многие разделяли CUNY belief in the importance of computer-assisted communication between scholars. Первый link новой network, called BITNET, был established between CUNY and Yale University in May 1981.

Network technology chosen for BITNET была determined by availability of RSCS software on IBM computers at the initial sites. Название BITNET означает **Because It's Time NETwork**. RSCS software simple but effective, and most IBM VM-CMS computer systems have it installed for local communications, supporting file transfer and remote job entry services.

Standard BITNET links are leased telephone lines running at 9600 bps. Хотя все initial nodes were IBM machines in university computer centers, network in no way restricted to such systems. Any computer with an RSCS emulator can be connected to BITNET. Emulators available for DEC VAX-VMS systems, VAX-UNIX systems, Control Data Corp. Cyber systems and others. Today, more than one-third of the computers on BITNET are non-IBM systems.

BITNET is a store-and-forward network, with files and messages sent from computer to computer across the network. Она предоставляет electronic mail, remote job entry and file transfer services, supports an interactive message facility and a limited remote logon facility.

Most BITNET sites use the same electronic mail procedures and standards as the ARPANET. As a result of electronic mail gateway systems installed at the University of California at Berkeley and at the University of Wisconsin-Madison, most BITNET users can communicate electronically with users on CSNET and the ARPANET.

BITNET expanded extremely rapidly, a clear indication that it is providing service people need and want. Simplicity of connection to the network, acquiring a 9600-bps leased line to the nearest neighboring computer node and installing an additional line interface and modem, provides the service at the right price.

By the end of 1985 the number of computers connected was expected to exceed 600, at more than 175 institutions of higher education throughout the U.S. BITNET open without restriction to any college or university. Она не limited to specific academic disciplines and may be used for any academic purpose. However, use for commercial purposes is prohibited.

In special cases, connection of commercial organizations may be sponsored by universities. Particular case is the connection of Boeing Computer Services to BITNET, as part of NSFnet initiative, to provide remote job entry services to their Cray X-MP/24 to NSF supercomputer grantees who have access to

BITNET.

Until recently BITNET had no central management structure and was coordinated by an executive board consisting of members from the major institutions participating. This worked because most connected computers were managed and operated by professional service organizations in university computer centers.

However, network growth made it impossible to continue in this ad hoc fashion, and a central support organization was established with support from an IBM grant. Central support organization, called BITNET Network Support Center, BITNSC, has two parts: a user services organization, the network information center, which provides user support, a name server and a variety of databases; and the development and operations center, BITDOC, to develop and operate the network. Major question facing BITNET members is how funding of this central organization will continue when IBM grant expires in 1987.

BITNET, with support from the NSFnet Program, is now examining ways to provide ARPANET-like services to existing BITNET sites. The project, similar to CSNET CYPRESS project, will explore a strategy to provide an optional path to the use of TCP-IP procedures on existing 9.6-kbps leased lines. The possibility of upgrading these lines to multiple alternate links, providing higher reliability and availability, or to higher-speed 56-kbps links is also being studied. The project will offer a higher level of service to BITNET sites choosing this path and also enable a low-cost connection to NSFnet.

MFENET

MFENET, DOE's magnetic fusion energy research network, was established in the mid-1970s to support access to the MFE Cray 1 supercomputer at Lawrence Livermore National Laboratory. The network uses 56-kbs satellite links and is designed to provide terminal access to the Cray Time-Sharing System, CTSS, also developed at Lawrence Livermore Laboratory.

The network currently supports access to Cray 1, Cray X-MP/2, Cray 2 and Cyber 205 supercomputers. It uses special-purpose networking software developed at Livermore and, in addition to terminal access, provides file transfer, remote output queuing and electronic mail. It also includes specialized application procedures supporting interactive graphics terminals and local personal computer based editing. Access is generally restricted to DOE-funded researchers. Recently the network expanded to include the DOE-funded supercomputer at Florida State University. MFENET funded by DOE and managed by Livermore.

MFENET has been successful in supporting DOE supercomputer users. However, specialized nature of the communications protocols is now creating difficulties for researchers who need advanced graphics workstations using UNIX BSD 4.2 and TCP-IP protocols on LANs. For these and other reasons, DOE is examining how best to migrate MFENET to TCP-IP, and later to OSI protocols.

The combination of CTSS operating system and MFENET protocols creates an effective interactive computing environment for researchers using Cray supercomputers. For this reason, two new NSF national supercomputer centers, San Diego (SDSC) and Illinois, chose CTSS operating system. In SDSC's case, MFENET protocols were also chosen to support SDSC Consortium network. In Illinois case, a project to implement TCP-IP protocols for CTSS has been funded by the NSFnet program, and these developments will be shared with SDSC and DOE to provide a migration path for SDSC Consortium network.

UUCP and USENET

UUCP network started in the 1970s to provide electronic mail and file transfer between UNIX systems. The network is host-based store-and-forward network using dialup telephone circuits and operates by having each member site dial up the next UUCP host computer and send and receive files and electronic mail messages. The network uses addresses based on the physical path established by this sequence of dialup connections.

UUCP is open to any UNIX system choosing to participate. There are informal electronic mail gateways between UUCP and ARPANET, BITNET or CSNET, so users of any of these networks can exchange electronic mail.

USENET is a UNIX news facility based on the UUCP network that provides a news bulletin board service. Neither UUCP nor USENET has central management; volunteers maintain and distribute routing tables for the network. Each member site pays its own costs and agrees to carry traffic. Despite reliance on mutual cooperation and anarchic management style, the network operates and provides a useful, if somewhat unreliable, low-cost service to its members. Over the years the network grew into a worldwide network with thousands of computers participating.

Other wide-area networks

Of necessity this file on wide-area networks has been incomplete. Other networks of interest include:

• **Space Plasma Analysis Network (SPAN)**: a network of DEC VAX computers using 9.6-kbps links and DECNET protocols for National Aeronautics and Space Administration researchers.
• **Planned Numerical and Atmospheric Sciences (NAS) network** centered at Ames Research Center: expected to use existing and planned NASA communications links and TCP-IP protocols.
• **Planned high-energy physics network**: based largely on VAX computers and using standard X.25 network level protocols plus the so-called `coloured books` protocols developed in the United Kingdom.

Also, many high-energy physicists at Stanford Linear Accelerator, Lawrence Berkeley Laboratory, Fermi Laboratory and elsewhere used DECNET to connect their DEC VAX computers together.

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

Please give full credit for references to the following:

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

Any questions, comments or Sluggestions can be emailed to me at Metal Shop, or sent via snailmail to the following address until 12-31-1986:

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

Phrack World News V, часть 1

Составил и написал: Knight Lightning

Where is Taran King?

10 мая 1986 года

Taran King обычно считается very mellow, easy-going person. В большинстве случаев это правда. Однако он также gets into major fights with his dad. Когда Taran really gets pissed, he gets violent. В прошлом он punched a hole into his bedroom door and put dents in his refrigerator with his fists.

Совсем недавно его отец узнал о его collection of illegal knives, including stilettos, butterflies and survival knives. Они поспорили об этом, и eventually it turned into a fight. Taran stormed off to his room. Meanwhile, unknown to him, his dad called the police. Его отвезли в nearby hospital's adolescent psychiatric ward, supposedly for evaluation. As of June 14, 1986, he has been there for five weeks and the end isn't in sight.

Некоторое время у него не было phone or visitor privileges, и связаться с ним было невозможно. Теперь это changed, но problems have not been solved.

23 мая 1986 года его отпустили on a pass to go see Judas Priest in concert, it was great. С тех пор его несколько раз отпускали on pass, mostly on weekends.

Что касается Metal Shop Private...

12 мая 1986 года `/\/impha` и я решили пойти к Taran домой, чтобы collect the Phrack files and add a few new modifications to the BBS, so that I could control it better remotely. Sister Taran впустила нас без проблем. К сожалению, до того как мы закончили, домой вернулся father Taran. Он сразу spotted my car outside and burst into the house. Он был pissed that we were there and made sure we weren't stealing anything, as if I were really going to steal from my best friend. Он assumed that the BBS had crashed and that we were there fixing it. Затем он decided that he didn't want us to come over every time the board crashed and took it down.

Metal Shop Private вернётся, когда Taran выйдет, hopefully sometime in June.

Metal Shop AE

27 апреля 1986 года

Metal Shop AE теперь proud possessor of a full 40 megs of online storage. Он также добавил individual password system для большей board security и теперь имеет email messaging service online.

Metal Shop AE sysoped by Cheap Shades. Это один из main distribution centers for Phrack Inc. У него online вся серия Phrack, а также almost 1000 other files.

Чтобы стать member of Metal Shop AE, contact Cheap Shades, Taran King or Knight Lightning.

Чтобы upload files for distribution in Phrack Inc., обязательно upload them to drive E, which will save your file to a non-public viewable drive, where it will stay until it is edited for Phrack.

Mark Tabas and Karl Marx busted

2 мая 1986 года

История такова: Mark Tabas worked at a plant in Denver where credit card blanks are manufactured. Он решил take a few. Затем он и Karl Marx начали искать someone with an embossing machine, чтобы print some stuff onto the blanks. Они нашли такого человека и agreed to meet at a motel to do the work.

Всё прошло хорошо. Они смогли print card numbers, names and expiration dates, которые получили, onto the blanks. Чтобы отпраздновать, они ordered a bottle of champagne from room service and paid for it with one of the cards. At that point the guy with the embosser pulled his badge: Secret Service. Теперь Mark Tabas and Karl Marx are facing forgery and carding charges along with theft for the blanks.

```
Information provided by Sally Ride...Space Cadet
```

Примечание редактора: в момент получения этой информации Sally Ride commented that it may be a rumor. Any inconsistencies are not his fault.

15 мая 1986 года

С тех пор мы в Phrack uncovered more information about this bust. Apparently a guy named Will Bell, whose handle was Jack Bell, set up Karl Marx and Mark Tabas. Will Bell had the embossing machine and was not a member of the Secret Service. Instead, he was the son of a member of the Secret Service, although maybe he was the son of a member of the FBI. Since he was not a fed, this was not a case of entrapment. Считается, что Will/Jack Bell originally from the 312, Chicago, area.

```
Information provided by Jester Sluggo and The Sprinter
```

FBI/Wylon in action

2 мая 1986 года homes of Cheap Shades and Kleptic Wizard received visits from Edward P. Nowicki, Special Agent of the Federal Bureau of Investigation.

Это никак не было bust. Agent пытался gain evidence for a telecommunications company known as Wylon, mainly based in the Colorado/Wyoming area. Apparently someone or several people had been calling Kleptic Palace AE and Metal Shop AE illegally, and Mr. Nowicki wanted to know who had been placing these calls.

Что касается Kleptic Palace AE, calls in question were made on `2/9/86 5:12 AM`, `2/9/86 4:33 PM` and `2/10/86 7:30 AM`, although no specific order is mentioned. Times of calls made to Metal Shop AE are not available. A third place called was the home of TWCB Inc. At the time of these calls Whackoland was still up.

Agent expected all of them to have a caller log on the board, but of course neither of their AEs kept caller logs. Not to mention the fact that no one would keep a caller log for three months anyway.

Kleptic Wizard got a message to Taran King, which was then sent to me. Within the hour I arrived at Klepto's house, where I discovered the FBI still around. After killing another 45 minutes, I went inside and met with Klepto.

Mr. Nowicki left behind two things: his business card and a list of four suspects that he was specifically trying to bust. Apparently all four had been caught for Wylon abuse in the past.

I recognized the name at the top of the list almost instantly and, as a result, saved a fellow phreak from a possible bust. Two of the others are rumored to have been warned as well. However, if this is untrue, the other three still may be in great danger as of this writing. All suspects live in the Wyoming/Colorado area.

Homes of Cheap Shades and Kleptic Wizard were not searched, and their boards were not looked at. The FBI agent even declined an invitation from Kleptic Wizard to see the BBS. This may be because he didn't have a warrant.

```
Information provided by Kleptic Wizard and Cheap Shades
```

Administration nominations?

6 мая 1986 года

In late April 1986, The Administration decided to have their yearly membership drive for the group. Phreaks/hackers being voted on for membership included:

```
Blade Runner
Jester Sluggo
Knight Lightning
Oryan Quest
Phlash Gordon
Recent Change
Sally Ride
Slave Driver
Taran King
The Marauder
```

Many of the above and others had thought that they had been voted into The Administration without even being asked. However this was not the case.

David Lightman stated that nominations were made public so that Administration members would know of the vote taking place on Administration BBS 1. Once the nominations were voted on, then the phreaks/hacks would be formally invited.

Now I pose an important question. If David Lightman is the only regular board caller of The Administration, then how would the other members know how to vote?

So far the results of the votes have not been made public. Not that it matters much, because The Administration has now more or less completely fallen apart. It would appear that this new membership drive was an attempt to revive the group with new blood. However the group has been revived on its own, since the former members regrouped again, at least temporarily.

```
Some information provided by David Lightman
```

Trouble in Texas

2 июня 1986 года

In the last week of May, David Lightman decided to do a credimatic check on Blade Runner. To his great surprise, he found that Blade Runner worked for Southwestern Bell Security. He confronted Blade Runner with this information and shortly afterward received a visit from Southwestern Bell Security, who confiscated his terminal programs, user files, notebooks and g-phile disks. He claims that his user files and g-philes were scrambled, so no one should worry too much.

Later that day, Sir Gamelord, sysop of World's Grave Elite, called David Lightman and said that Blade Runner was on the board and acting really strange. David Lightman told him what happened, and they then hung up. The next day Blade Runner is a cosysop of World's Grave Elite as well as Thieve's Underground, sysoped by Jack The Ripper. Now Sir Gamelord denies the incident ever occurred. At this writing, David Lightman is laying low and retiring from the phreak world until things clear up.

Sir Gamelord's side to this story is quite different. Sir Gamelord said that he, Blade Runner and Jack the Ripper were forming a group called P.H.I.R.M., see Phrack Pro-Phile 3 in this issue, and that Lightman wanted to be in and to lead the group as a subsidiary of The Administration, like Team Hackers '86. They refused and took away his cosysop access on their boards. Sir Gamelord says that Lightman is making this whole Southwestern Bell Security story up to get revenge on them.

However, Lightman claims that he was asked to be a member of P.H.I.R.M., but refused because he didn't have the time. He did, however, recommend Digital Logic, Ford Prefect and The Lineman, sysop of the Lost City Of Atlantis.

David Lightman has since received his disks back but will not be around on boards very much. The decision is up to you. I will try to get more information out on boards as soon as possible.

```
Information provided by David Lightman and Sir Gamelord
```

Ninja NYC / Sigmund Fraud: close calls

Sigmund Fraud, famous for his incredible proficiency at `social engineering`, is now laying incredibly low after what is considered the closest call of his life.

The following must be regarded as pure rumor for the sake of non-incrimination of those involved. You readers know what I mean.

The story goes like this: Sigmund Fraud and a friend, the same one who went to TelePub'86 in New York, though he has no handle, were able to convince their local Bell company that they were another part of the same company and were able to acquire Call Forwarding, Call Waiting, Speed Calling and Three Way Calling onto Sigmund Fraud's personal phone line. Since SF's friend lived in a Cross Bar, X-Bar, area he could not get these services, so they decided to get them for Ninja NYC. They told him about it later.

Less than a week later, on the first Thursday of May 1986, Ninja NYC came home to discover two telco agents awaiting his return from school. What it boiled down to was that `he` had committed several felonies, and to make matters worse, the people at the local Bell company identified Ninja NYC's voice as being the caller, and he isn't the one who made the call. What it finally boiled down to was that Ninja NYC had really received a very scary personal warning.

About this same time Sigmund Fraud was getting home and, to his great dismay, all of his new found phone features had been turned off. Sometime later, most likely after the telco agents had left, Sigmund got a call from Ninja NYC. Ninja NYC told him everything that had happened and warned him that he was next. Sigmund immediately called me. We both thought Sigmund was doomed and would be picked up very soon.

However this was not the case. The agents didn't show up, and Sigmund had been given a golden opportunity to dump all his illegal items and get his story right. That night I received a call from Slave Driver, and Sigmund called me on three-way, and we discussed what to do next. The problem was that Sigmund didn't want to get rid of his illegal items. He had boxes, manuals, notebooks and even a PBX in his room. I told him he had two choices: get rid of the stuff somewhere, anywhere, so the telcos don't get any more evidence, or leave it where it is and risk the telcos coming over, taking it and making things worse for him.

When I left the conversation, SF was still discussing what he should do. The next day he was not visited by the telcos, was not busted, but instead received a call from his local Bell company and was given a very strong verbal warning.

Since that time he has stopped answering his personal phone and believes that line to be monitored. Ninja NYC is almost definitely being monitored, and people have been asked not to call him.

Of course that didn't stop Daniel Zigmond from calling him. This was in an attempt to help Sigmund Fraud, but regardless may have done more damage than good.

```
Information provided by Sigmund Fraud, Slave Driver and Knight Lightning
```

Telecomputist: printed newsletter

8 июня 1986 года

From: Forest Ranger and `TeleComputist` staff
To: You

I have drafted the idea for a newsletter, and I stress the word newsletter. TWCB had promised everyone a 40+ glossy page magazine for an outrageous amount. I do not want to say that we are taking TAP over because we are not, but instead making amends for what TWCB did not do.

To show our sincerity, we will be offering the first issue free. It will be your basic newsletter with exceptional articles from experienced phone phreaks, computer hackers and telecom buffs. Each issue will be a set four pages, but since this is the grand opening issue it will be longer, 20 pages.

For the first free issue please send a postage-paid, self-addressed envelope to:

```
TeleComputist Newsletter
P.O. Box 2003
Florissant, Mo. 63032
```

Also, please send subscriptions to the same address. The subscription fee for the newsletter will be twelve dollars a year, fifty cents for back issues. This is a monthly circulation, and we encourage letters.

The `TeleComputist` staff includes:

```
Forest Ranger
Data Line
Reverend Enge
Ax Murderer
Chris Jones
Knight Lightning
Taran King
Mad Molester

Information provided by Telecomputist Staff
```

Phrack World News V, часть 2

Составил и написал: Knight Lightning

Captain Midnight's sneak attack

12 мая 1986 года

> *A daring intruder airs the beefs of dish owners*

В старые времена у людей с жалобами на media было мало средств воздействия: строгое письмо редактору, возможно, или протестующий phone call. `Captain Midnight`, возмущённый consumer of the space age, выбрал более дерзкое действие. Во время sneak attack в воскресенье прошлой недели self-appointed video avenger вклинился в показ HBO фильма *The Falcon and the Snowman* с cryptic message:

```
Good evening HBO
From Captain Midnight
$12.95/Month?   No Way!
(Showtime/The Movie Channel Beware)
```

Таинственное сообщение, которое несколько минут видели на East and Midwest hundreds of thousands of subscribers pay-cable service, явно intended as a rallying cry для более чем 1.5 million owners of home satellite dishes in the U.S. Эти video free-lancers angry because many TV signals, which they had been plucking from the sky, are done by one tuning into jumble.

В январе HBO and Cinemax, both owned by Time Inc., стали первыми двумя cable services, которые scrambled their signals, preventing dish owners from watching them without paying a monthly subscription fee. Showtime and The Movie Channel begin similar scrambling on May 27, and most other satellite-beamed cable channels, including ESPN, MTV, Disney Channel, Cable News Network and Superstation WTBS, follow suit before the end of the year. Their actions set off a heated battle over who has the right to TV signals bouncing through the skies.

Одним ударом Captain Midnight стал folk hero in that struggle, though his identity remains a mystery. Ordinary home dishes can only receive signals, not send them; therefore experts think the pirate signal probably came from a TV station or other commercial facility.

Wherever the stunt originated, TV executives were not amused. HBO lodged a complaint with the FCC, threatened to prosecute the pirate and made technical adjustments that it claims will prevent any repeat attack.

> *He probably thinks this was a prank, says HBO Vice President Dave Pritchard. But the fact is someone has interfered with authorized satellite transmissions.*

Incident raised concerns that other satellite-borne communications, including sensitive data transmitted by business and the military, could be similarly disrupted. Representatives of the three broadcast networks insist that a `hacker` would have difficulty breaking into their programming. But any satellite signal could theoretically be disrupted, experts say.

> *Most satellites are built with some safety measures, explains Karl Savatiel, director of satellite communications for AT&T. But all satellites, including military satellites, are vulnerable if a person knows where the satellite is located, the frequency it uses for satellite transmissions, and the sender's code.*

This wasn't the full article, just the important part.

```
Taken from Time Magazine, May 12, 1986
Reported by Jim Byers / Los Angeles and Jerome Cramer / Washington
Typed for PWN's usage by The Seker
```

News on Captain Midnight

28 апреля 1986 года

> *Search for Cable TV Prankster Leads to North Texas*

The search for Captain Midnight, disgruntled video prankster who briefly commandeered Home Box Office's satellite transmissions over the eastern two-thirds of the country early Sunday, has led federal investigators to North Texas, a Justice Department official said Monday.

John K. Russell, Justice Department spokesman in Washington, told Knight-Ridder Newspapers that `the perpetrator is believed to be in North Texas`. Later he said the search was in Texas `as well as other areas`.

Other authorities told Knight-Ridder that investigators in the Dallas field offices of the FBI and FCC have been focusing on a tip that Sunday's four-minute cable interruption originated in North Texas.

FBI and FCC officials in Dallas could not be reached for comment Monday.

Captain Midnight interrupted a movie broadcast Sunday with a message protesting new fees being charged the owners of satellite dishes for access to HBO. Five-line message, superimposed on a test pattern, said:

```
Good evening HBO from Captain Midnight.
$12.95 a month?  No way!
(Showtime-Movie Channel Beware.)
```

In January, HBO began scrambling its broadcasts to prevent owners of satellite dishes from unauthorized interception of the signal as it bounced from a satellite to cable television systems.

HBO told dish owners that they would have to buy a descrambler for 395 dollars and pay 12.95 dollars a month.

> *While the man on the street may have once thought that Captain Midnight's message was limited to being a prank, it does represent a very serious threat to any company or entity using satellites to transmit information, said Alan Levi, HBO's manager of corporate public relations.*

Other:

```
Alan Levi:             [212] 512-1659 (Corporate affairs)
David Pritchard:       [212] 512-1413 (Corporate affairs)
Tim Larker:            [212] 512-5666 (Network scrambler assistant)
New York City FCC:     [212] 620-3438 (Federal Communications Commission)
HBO Corporate Offices: [212] 512-1000
```

David Lightman

I have spoken with several people about Captain Midnight. I have spoken to everyone above. David Pritchard tried to tell me this:

```
DP = David Pritchard
DL = David Lightman
```

DL: Where do you think this Captain Midnight is?

DP: Would assume he is in the North Texas region. Possibly 214.

DL: What makes you think this?

DP: We believe this is true due to a tip from a Dallas resident.

DL: How do you know that he was not lying to lead you away from the real Captain Midnight?

DP: I know he was probably not lying because he left us his mailbox number.

DL: Which is?

DP: I cannot release that information right now.

This conversation went on for a while, possibly 10-15 minutes.

David Lightman earlier had spoken with Alan Levi.

DL: Yes. Do you have any idea who this Captain Midnight might be?

Alan: No, but we are fairly certain it is someone in the 212 area with access to the scrambling offices of HBO. The knowledge necessary for what this guy did could not be gotten very easily without getting it from our departments.

DL: Well, I believe I know who this Captain Midnight is.

Alan: Could you please tell me who you think Captain Midnight is?

DL: No. If it is the person I suspect, I would rather not cause any trouble for them.

Alan: You wouldn't cause much trouble for him.

DL: Isn't what this guy did a federal offense?

Alan: Well, yes it is, but you would be surprised how many people get away with breaking federal laws.

He actually said that, guys.

DL: Hmm. What would happen to him?

Alan: We would just let him know that what he did was not a prank. It was very serious. It could possibly change the entire industry, and unless he stops transmitting over our satellites, we will ask the Department of Defense to handle it from then on.

DL: Well, I would need to think about it a little more. Can I call you back a little later?

Alan: Could you just give me your number and I will have David Pritchard call you back?

DL: It depends on who else will get my number.

Alan: Just me. I will consider this conversation and all of the conversations that follow to be an anonymous tip.

DL: Sure then. It is `(214) 733-5162`.

Alan: Thanks. Then I will have David call you if you do not call me back before tomorrow evening.

DL: That would be fine. Thanks.

Alan: Thank you.

End of conversation.

Well, as you may have guessed, my number, mailbox, was given to the FCC, FBI and David Pritchard as well as Tim Larker. I got pretty pissed, so I called David Pritchard. That was the first conversation I posted. We, Alan Levi, David Pritchard, Tim Larker, the FCC, the FBI, Knight-Ridder Newspapers and I, now have the country believing that the transmission originated in Dallas. Of course it did, but you may see that changed soon. I plan on another conversation with these intelligent people tomorrow at 5:00 PM.

If you do call these guys, please do not mention The Administration, Team Hackers '86, any member of either group or me as being the transmitter. You have no proof at all about that. I did not say if we were involved or not. That will be left up to your imagination.

```
Information and interviews provided by David Lightman
```

Captain Midnight busted!

6 июня 1986 года

Captain Midnight, probably, isn't sleeping too well these days. His name, still publicly unannounced, is probably known by many, including the FBI. He has already been reported to have been fired from his job at an uplink facility, of which there are only around 100 in this country. The facility is east of the Rockies and does not operate after midnight. Also, a newer type of equipment was used, of which there are only a few in the country.

We expect charges to be filed any day now, possibly just in time for the June 12 congressional hearings on signal jamming. Penalties could include a one-year jail sentence and up to 50 000 dollars in fines, 10 000 dollars maximum of which would be for jamming only.

We expect FM America to come to Captain Midnight's rescue financially by raising defense money. All segments of the TVRO industry condemned the signal jamming. It is interesting to note the grins and smiles while discussing the subject, however. FM America knows who Captain Midnight is and even interviewed him live on the air on FM America. Tapes of FM America, including Captain Midnight's interview, have been turned over to federal investigators.

Several benefits can be realized by Captain Midnight's signal interruption. Mainly, the fact is now known by everyone that it can be done. There are no secrets either in that a transponder can easily be confused into locking onto another signal and ignoring the correct signal as interference. Also, the signal that controls the satellite's positioning could also be accessed. The overall possibility that our entire satellite system in general can be rendered ineffective from the ground is kind of unnerving.

Signal scrambling did not interfere with the HBO signal lockout because a higher-wattage beam overpowered it. The networks all use pretty powerful beams, which are used 24 hours a day, so they would be harder to jam. If we had to guess which uplink was used to jam HBO, we would pick one that was already locked into the same satellite, such as one of the superstations.

```
Information provided by Handsomest One
```

Who is Ralph Meola?

20 мая 1986 года

Ralph Meola is the Head of AT&T Security in New Jersey and theoretically everywhere else as well. He is known to have a computer file on hackers and phreaks, and an investigative team, that rivals John Maxfield's BoardScan.

How did Meola enter into the public eye? We at Phrack aren't completely sure, but the general idea is that a friend of Sigmund Fraud, see TelePub'86 in PWN Issue III, using social engineering in order to gain information from AT&T, somehow came into contact with Ralph Meola.

Later, Sigmund Fraud was also brought into this and decided to give Ralph Meola a call himself. With Gin Fizz on Sigmund's three-way, he got Meola on the phone and said: `Hey! This is Sigmund Fraud!` Typing sounds could be heard in the background, and in a few seconds Meola responded with Sigmund

Fraud's real name, address, phone numbers and the names of several BBSes that he was on.

Meola then insisted that Sigmund Fraud give him his account on Stronghold East, or at the very least all of the newuser logon procedures and passwords. Failure to do so would mean big trouble for Sigmund Fraud. Sigmund, of course, gave Meola the always nice `fuck you` and hung up on Meola.

Although Sigmund Fraud was, at the time, on Metal Shop Private, Meola didn't know it, or at least he didn't mention it as a BBS that Sigmund was on. This means that Meola has no agents on Metal Shop Private. It is also known that Meola has no agents on Stronghold East. Otherwise he wouldn't have needed the password information from Sigmund. It is believed that Meola was on Stronghold East before the massive purge several months ago.

```
Information provided by Sigmund Fraud / Gin Fizz / Slave Driver
The assumptions and theories are my own - KL
```

Slave Driver has since sent Ralph Meola the following letter:

```
TO:  Ralph Meeola
     Head AT&T Security

From: Slave Driver

Re: My user
```

Hello. I find it rather hard to get in touch with you through normal means, but give me some time.

I was told you have been threatening my users, trying to get access here. That is not good. Ralph, if you want access just ask for it, don't go threatening my users. That was not an intelligent idea, Ralph.

If you are such a big guy, in your mind, and uh, hand, why not give me a call. I'm sure you have my number. I would be very interested in talking to you. So, you decide, Ralph. Either way, we'll talk one day.

```
Bye Ralph,

Slave Driver
```

Phrack World News V, часть 3

Составил и написал: Knight Lightning

Cracking down on abuse

Эта статья взята из январского выпуска *MCI World*, monthly newsletter, published by MCI for its employees.

Nationwide attack on telephone fraud got a boost recently when the U.S. Secret Service joined the effort to curb the crime that costs the industry millions in lost revenue annually.

Secret Service used new jurisdiction over telephone fraud for the first time to arrest five individuals in raids on four illegal `Call-Sell` operations in New York City last November.

The five suspects are awaiting trial in federal court on charges based on a Secret Service investigation conducted in cooperation with MCI and other members of the long distance telephone industry.

Defendants were charged with violation of a law on Fraud In Connection With Access Devices, which carries maximum penalties of 15 years imprisonment and a fine of 50 000 dollars, or twice the value of the fraudulent activity.

Several other investigations are under way and future arrests are expected, according to a Secret Service spokesman.

MCI cooperated in the investigation as a company and through membership in the Communications Fraud Control Association, CFCA, made up of some 35 telephone industry firms.

> *Because it's an industry-wide problem, we have organized to crack down on all kinds of fraud, from the isolated hacker to more organized schemes to use long distance lines illegally, said Everick Bowens, senior manager of MCI security investigations and president of CFCA.*

The Secret Service said that in the New York cases, the defendants operated Call-Sell businesses out of their homes and charged customers a flat fee for making long distance calls. They used Blue Boxes and stolen or compromised authorization codes or credit card numbers to use the long-distance networks of several companies.

Blue Boxes are electronic tone-generating devices used to bypass billing systems and gain access to company networks. They can be assembled from generally available electronic parts, or purchased ready-made through illegal sources.

In the New York raids, agents seized unauthorized codes and credit card numbers, four Blue Boxes and more than 20 telephones.

It is estimated that in 1984 fraud in the telecommunications industry totaled 500 million dollars nationwide, and approximately 70 million dollars in the New York City area.

CFCA members are primarily inter-exchange carriers, such as MCI, but resale carriers and some Bell Operating Companies, BOCs, are also members, along with representatives of computer services and credit card companies.

Bowens says CFCA is intensifying efforts to stop the spread of fraud. Among other things, CFCA is developing educational packages for carriers and the public to promote widespread understanding of telephone fraud and ways to counter the crime.

> *Our aim is jointly to prevent, detect, investigate and prosecute any fraudulent use of our long-distance networks, Bowens said.*

Authorization codes are obtained by theft from individuals and by hackers who randomly try combinations of numbers by telephone or through computer scanning of number combinations until a working code is hit. Illegally obtained codes are fraudulently used by boiler-room telemarketing operations, for example, or passed along for use by individuals.

MCI had developed software to detect illegal entry into its network, and it is expected that the spread of dial 1 service, in which authorization codes are not used, will help reduce the incidence of telephone fraud.

Comments from The Bootleg

You reckon they mean us?

What's wrong with them, can't they take a joke?

The many faces of fraud

Следующая статья взята из январского выпуска *MCI World*, monthly newsletter, published by MCI for its employees.

This new year will see a stepped-up MCI attack on telephone fraud, illegal use of the long distance network through access by stolen authorization codes or electronic devices. Offensive is led by Everick Bowens, senior manager of MCI's security investigations department and president of the industry-wide Communications Fraud Control Association, CFCA.

Success in curbing this theft of service has earned MCI security investigators a reputation as super sleuths at headquarters and in the divisions.

New teeth were added to the attack on telephone fraud when the U.S. Secret Service was assigned to augment continuing investigative efforts by the FBI and other law enforcement agencies.

Because telephone fraud is outright theft from the company, MCI is determined to prevent, detect, investigate and prosecute any illicit use of its network. To learn more about how MCI conducts its anti-fraud campaign, *MCI World* talked with Bowens.

MCI World: Is it true that MCI has systems that can detect fraudulent activity while it is occurring?

Bowens: Yes, our fraud systems detect abnormal usage and hacking. The systems also help us to track down offenders even when we have only the authorization code he or she is abusing. Because we can profile abusers and trace phone calls, it is easier for us to prepare cases for prosecution.

MCI World: Abuses involving computer hacking to get authorization codes seem to attract public attention. But there are other types of fraud equally damaging to the telecommunications industry. Would you identify some of these?

Bowens: The primary form of abuse is by hackers, who use computer programs to derive customers' authorization codes. These codes can be widely disseminated via electronic bulletin boards. Because many of these boards are public, the codes fall into the hands of anyone with access to the boards. We also encounter electronic toll fraud, which involves tone-generating devices that allow offenders to place fraudulent calls.

MCI World: Is one type of fraudulent activity more prevalent than another?

Bowens: Nationwide, fraud most frequently originates from military posts, college campuses and prisons, places where there are numbers of people far from home, or who have little else to do but manipulate the telephone. This type of abuse prompts the bulk of our investigations.

MCI World: Who is most likely to commit fraud? Is there a general profile of the common offender?

Bowens: Computer crime typically occurs in affluent, metropolitan suburbs and involves juveniles. Electronic fraud also occurs in major metropolitan areas. Other abusers, such as high-pressure telemarketeers, usually follow the coast lines: California and Florida, for boiler-room operations in which phone service is used illegally to sell merchandise. However, fraud can't be totally attributed to any specific group at any particular time.

MCI World: How can you keep up with code abuse and fraud? Don't offenders change frequently?

Bowens: Interestingly enough, the patterns don't change much. Those who commit fraud form a finite community that doesn't expand a great deal over time. Casual offenders, individuals who may take advantage of a hot toll-free number, will use the number only when it's hot. Once the number no longer works, they're not likely to repeat the offense. On the other hand, repeat offenders are dedicated to getting something for nothing. They're somewhat easier to identify because they commit the same offense over and over.

MCI World: How does MCI know when it is the target of fraudulent activity?

Bowens: Our systems generally alert us, or an employee or a customer informs us. People know the MCI name. When they recognize something happening illegally with an authorization code, they'll get in touch with us. People generally feel that a cheat is a cheat, a crook is a crook, and if they have to pay full value for a phone call they see no reason why someone else shouldn't. There also are professional tipsters who go from one company to another offering information for a price. However, we rarely deal with them.

MCI World: Which MCI people, by the nature of their jobs, are most likely to detect or at least suspect fraudulent activity?

Bowens: Our switch technicians have been very instrumental in detecting abuse. They're in a position to identify extensive busy signals on circuits, abnormal calling patterns and code use. They've identified many hackers just by reviewing their daily call statistics. Employees in our billing department are also good at spotting unusually large bills and abnormal patterns. Though most fraud is detected by the systems we have in place, the human eye continues to be extremely helpful.

MCI World: In addition to working with internal people to help detect fraudulent activity, you also rely on the expertise of external agencies. Which outside agencies assist you with investigations?

Bowens: When fraudulent activity involves the theft or illicit use of authorization codes or credit calling cards, MCI and the Secret Service work together to investigate the case. If other activity is involved, such as the use of our service in furtherance of other crime, MCI works with the FBI. When the U.S. Postal Service is manipulated in a fraud case, MCI and postal inspectors investigate together. Additionally, Bell Operating Companies often provide hard evidence in cases that MCI prosecutes.

MCI World: When you are alerted to suspected fraudulent activity, what steps do you take to open and pursue the case?

Bowens: Security investigators contact the customer whose code is being abused, advise them of MCI's suspicions and attempt to confirm them. If the response confirms their suspicion of fraud, they open the case. Normally, an investigation entails much research into toll records to identify abusers, unusual call patterns and the parties who might be involved in illicit activity. We also interview parties receiving the calls and document their statements. Once we collect sufficient evidence, we decide whether a case should be pursued as a criminal or civil action.

MCI World: How long does it normally take MCI's investigators to crack a case?

Bowens: Typically, investigators can crack a case within hours. Identifying fraud suspects is the easy part. Amassing the evidence, dotting all of the legal i's and crossing the t's, is tougher. Gathering evidence may take weeks, and large cases involving many parties can take months to solve.

MCI World: With fraudulent activity knowing no geographical restrictions, how do you segment the problem divisionally?

Bowens: The security investigations department acts primarily in an advisory capacity, helping investigators in the divisions with procedural matters. The divisions generally take responsibility for investigating fraudulent activity within their jurisdictions, and corporate investigators pursue cases that are large in scope or require specific expertise. Corporate also takes on cases involving offenders operating in more than one division.

MCI World: Can you elaborate on MCI's goals for reducing the level of fraudulent activity?

Bowens: We want to reduce fraud to the lowest possible level. One of MCI's goals is to cut fraud by more than half in 1986. We want to be the industry leader in curbing this illegal activity.

Broadway Hacker turned fed informant?

2 июня 1986 года

Broadway Hacker recently called Phreakers Quest and left feedback to the sysop of that system, Shawn, saying: `I do believe that some of this information here is illegal.` Shawn called Dark Creeper and reported this to him, who then later told it to me.

Sometime later, Broadway Hacker called Knight Bandit to voice validate him for The Radio Station. He claimed he was some sort of fed and that KB would be hearing from someone in Bell Security.

The Radio Station is down because Broadway Hacker has sold his computer, his disks and everything else, and is moving to his new job at an unknown destination. When I spoke with him, he went on that he sold his user log, but would not comment on that any further. He wanted me to print that he was a fed and that all of his former users would soon be receiving visits from the FBI. This is exactly what he told Phantom Phreaker and several others, which started a mass riot in the phreak world. One result was the takedown of Alliance for fear of its safety. It has since been put back up.

Broadway justified his actions by saying that by telling rodents he was a fed, it would keep them off his board. Later he said that since he is leaving the phreak world and no one knows where he is going, `To hell with the phreak world, let it fall apart and die for all I care.` So this fed scare is an attempt to do just that. Was it a joke? Did he really mean that? I don't know. Maybe he did mean it then but now has changed his mind.

No one should be worried about this, everything is okay, and Broadway is not working with the FBI. He now claims that he needed his line free for business calls and all of the above were attempts to get people not to be calling him, as he didn't have the time or patience. Use your own judgement.

Broadway Hacker still has his Vic 20 and an old modem and is attempting to get back on boards. He has also stated that The Radio Station BBS will be put back up at the end of the summer. Where it will be run from is unknown, although Broadway speculated that when it returns it would be run off an Amiga.

`Information provided by Broadway Hacker / Dark Creeper / Knight Bandit / Phantom Phreaker`

Требуются законы для взрослых против компьютерных преступников

Автор: Knight Lightning

По материалам Дейва Скидмора (Associated Press)

ВАШИНГТОН. Подростки-компьютерные хакеры уступают место новому поколению людей, которые крадут информацию из компьютеров ради прибыли, а не ради забавы — заявил в среду председатель подкомитета Палаты представителей по борьбе с преступностью.

«Хакеры были первым поколением, с которым мы столкнулись. Теперь среди нас всё больше профессионалов, занявшихся бизнесом на доступе к компьютерным базам данных», — сказал представитель Уильям Дж. Хьюз, демократ от штата Нью-Джерси [609/645-7957 или 202/225-6572], инициатор законопроекта, призванного помочь правоохранительным органам эффективнее справляться с этой проблемой.

Хьюз выступил с этим заявлением в ходе рассмотрения подкомитетом Палаты представителей по борьбе с преступностью, который он возглавляет, предложенного Закона о компьютерном мошенничестве и злоупотреблениях.

Подростки-компьютерщики, движимые желанием развлечься и завоевать авторитет среди сверстников, используют домашние компьютеры и телефон для «взлома» государственных и корпоративных баз данных.

Теперь, по словам Хьюза, хакерские техники всё активнее берут на вооружение промышленные шпионы, продающие коммерческие секреты, похищенные из корпоративных компьютеров, и воры, изменяющие банковские записи ради кражи миллионов долларов.

«Компьютерная преступность, пожалуй, является одной из наиболее быстро растущих областей криминала. Это заставит старое доброе ограбление и взлом слегка устареть в глазах определённых профессионалов», — сказал он.

Законопроект Хьюза, соавторами которого выступили представители Билл Макколлум, республиканец от Флориды [202/225-2176], и Билл Нельсон, демократ от Флориды [202/225-3671], предусматривает три новых состава преступления.

1. Запрет несанкционированного доступа к компьютеру и отмена требования доказывать факт использования или изменения хранящейся в нём информации.

2. Запрет «пиратских досок объявлений», используемых хакерами для обмена секретными компьютерными кодами и паролями.

3. Признание уголовным преступлением (с наказанием до пяти лет лишения свободы и штрафом в 250 000 долларов) умышленного причинения ущерба компьютерной программе или базе данных на сумму свыше 1 000 долларов.

Данное положение законопроекта будет применяться к так называемым программам-«троянским коням», которые при получении доступа к чужому компьютеру уничтожают все данные и программы на нём.

Законопроект призван устранить лазейки в антикриминальном законодательстве, принятом Конгрессом в 1984 году, пояснил Хьюз. Он распространяется на компьютеры, используемые федеральным правительством или его подрядчиками, а также на компьютеры банков и

ссудно-сберегательных ассоциаций.

Хьюз сообщил, что рассчитывает вынести свой законопроект и аналогичное законодательство, инициированное сенатором Полом С. Трайблом-младшим, республиканцем от Вирджинии [804/771-2221 или 202/224-4024], на рассмотрение Палаты представителей и Сената где-то в мае.

Информацию предоставил Blue Buccaneer

Ниже приводится критический разбор вышеизложенной статьи.

Blue Buccaneer:

По поводу этого закона: я всегда думал, что взламывать ради денег было бы интереснее, ну да ладно... Так или иначе, три новых состава преступления — это именно то, что меня не особо радует:

1) «Запрещает несанкционированный доступ к компьютеру» (Да неужели?) «и отменяет требование доказывать, что информация в компьютере была использована или изменена». Что это вообще за закон?! Правительство может просто арестовать человека и при этом ничего не доказывать? ДА ВЫ ШУТИТЕ!

2) «Запрещает "пиратские BBS"». Когда же эти люди наконец выучат правильную терминологию? Пираты торгуют варезом, а не «секретными паролями и кодами». Суть в том, что поскольку это федеральный закон, он будет действовать во всех штатах. Речь идёт уже не об игрушечных законах штатов. Разве не ужасно будет, если само по себе содержание BBS станет преступлением? Кроме того, я думал, у нас есть свобода слова и печати. Снова: ДА ВЫ ШУТИТЕ!

3) «и штраф в 250 000 долларов за умышленное причинение ущерба компьютерной программе или базе данных на сумму свыше 1000 долларов». Прошу прощения, но разве можно «умышленно» уничтожить данные? И разве четверть миллиона долларов — не слишком много для подростка на карманных деньгах? И такая сумма за ущерб в 1000 долларов? Чёрт, вот бы моя страховая компания так же платила, когда я разбиваю машину. Ещё раз: ДА ВЫ ШУТИТЕ!

И ещё — это уже, наверное, вина журналиста, — какое вообще отношение имеет тот абзац про «троянских коней» ко всему остальному? Неужели кто-то думает, что обычный прохожий скажет: «Уф, я уже боялся, что в новом законопроекте про троянских коней забыли». Мне казалось, что «троянские кони» и без того подпадают под правило «умышленного» уничтожения данных.

Написано Blue Buccaneer

Компьютерные дети — или преступники?

Мистер Слиппери, 12 лет, никогда не думал, что игра на домашнем компьютере — что-то большее, чем безобидное развлечение, пока однажды таинственный звонок от незнакомца не доказал обратное. «Мне позвонил какой-то чудак и предложил деньги за то, чтобы я уничтожил банковские записи», — рассказал Слиппери, упомянутый под своим хакерским псевдонимом. «Тут я понял, что это невероятный способ отмывать деньги. И что по-настоящему умный человек в такие дела не лезет, потому что это явно попахивало организованной преступностью».

Хакерство — использование персонального компьютера для проникновения по телефонным линиям в закрытые компьютерные системы корпораций, фондов, университетов и банков — это новая форма организованной преступности, говорят эксперты. За последний год-два появилась

новая, изощрённая порода хакеров. Их возраст варьируется: от ранних взломщиков, начавших в 14 лет и к тому времени поступивших в колледж, до взрослых, управляющих компьютерными криминальными сетями, но их мотивы схожи: преступный умысел.

Когда мистер Слиппери семь лет назад начал хакерствовать, он был исключением среди прыщавых любопытных мальчишек, для которых компьютеры были игрушками ради дешёвых, как правило безобидных, приколов. На протяжении четырёх лет он жил в соответствии со своим псевдонимом, в итоге проникнув в засекреченные правительственные компьютеры Министерства обороны (МО) и Агентства национальной безопасности (АНБ). Мистер Слиппери оставался незамеченным вплоть до последних нескольких недель своей хакерской деятельности. Его так и не поймали, так и не осудили. Под конец он понял, что сотрудники государственной безопасности ведут за ним слежку, и решил навсегда убрать телефонный модем.

«Однако примерно через четыре года я начал замечать, что появилась совершенно новая публика», — замечает мистер Слиппери, ныне 19-летний экс-хакер. «Теперь завелись 14-летние, которые носятся и всё крушат, проверяя, сколько неприятностей они смогут натворить». Эксперты по компьютерной преступности говорят, что проблема с хакерами усугубляется, хотя компании всё неохотнее обсуждают эту тему. «Проблема злоумышленных хакеров продолжает стремительно нарастать и становится значительно серьёзнее», — сказал Донн Б. Паркер, автор книги «Борьба с компьютерной преступностью» и консультант по компьютерной безопасности в SRI International, некоммерческом исследовательском институте в Калифорнии.

«Снижение стоимости оборудования, привлекательность хакерства как обряда посвящения для новичков — всё это указывает на растущую уязвимость американского бизнеса перед хакерской угрозой». Экспертиза Паркера привела к тому, что его наняли техническим консультантом для фильма «Военные игры» о двух подростках-хакерах, взламывающих оборонные компьютеры. Свидетельства серьёзных хакерских преступлений сосредоточены на электронных досках объявлений (BBS), где хакеры делятся разведданными. «Телефонные компании вложили огромные средства в своё оборудование, которое крайне уязвимо для хакеров, научившихся их обходить и использующих пиратские доски для своих разведывательных целей», — сказал Паркер из SRI International.

«Значительная часть этих детей — фактически малолетние правонарушители с другими записями об арестах». Недавно хакер разместил такое сообщение на местной BBS:

```
Я живу в Кливленде, и везде кишат федералы. Некий парень под ником
Lou Zer попался, и ему сказали: если он настучит на 5 человек, отделается
пробацией, что он и сделал. Теперь полклуба 2300 залетело, и у этого
пацана большие проблемы в будущем. Ещё я видел переодетых ментов,
прикинувшихся курьерами Federal Express. Старайтесь их избегать.
Кстати, вот несколько PBX, можете побаловаться. Они принадлежат
Standard Oil.

                                                --Later, Sir Gallahad
```

Другие BBS публикуют списки телефонных номеров компаний из Fortune 1000, банков, кредитных бюро, университетов и фондов.

По словам экспертов, многие из этих номеров недействительны. Хотя существуют BBS, принимающие участников исключительно по приглашениям и действующие как часть компьютерного андерграунда, другие доступны любому, у кого есть компьютер и телефонный модем. Нередко доски носят зловещие названия вроде The Sanctuary, Future World, Dark Side, Deathtrap и Speed Demon Elite. Компьютерное преступление порой называют идеальным злодеянием. Его исполнители — анонимные хакеры под псевдонимами вроде Phantom Phreaker,

Big Brother, Bootleg, Sigmund Fraud и Scan Man.

Джон Максфилд — консультант по компьютерной безопасности, живущий в пригороде к югу от реки. Бóльшую часть рабочего времени Максфилд проводит за сканированием BBS и известен среди экспертов по компьютерной преступности как охотник за хакерами. Его расследовательская работа по сканированию досок привела к большему числу судебных преследований хакеров, чем у кого-либо другого в этой области, говорят знакомые с его работой источники. Максфилд, воспринимающий угрозы расправой и прочие запугивания как часть профессии, говорит, что главное — знать врага. Помимо своей огромной самодельной компьютерной системы, Максфилд может похвастаться единственным существующим досье на хакеров. В нём содержится несколько тысяч псевдонимов, многие из которых сопровождаются настоящими именами и домашними телефонами. Всё это — результат четырёх лет неустанной слежки за хакерами, утверждает Максфилд. «Я достиг того, о чём большинство хакеров мечтали бы», — сказал он. «Взломать хакера — это настоящий взлом».

По оценке Максфилда, в настоящее время в компьютерном андерграунде действуют около 50 000 хакеров и почти 1 000 подпольных досок объявлений. Из них, по его подсчётам, около 200 досок «опасны»: на них публикуются номера кредитных карт, телефоны компаний из Fortune 500, региональных телефонных компаний, банков и даже авторские пособия по изготовлению бомб и взрывчатки. Одна растущая группа серьёзных хакеров — студенты колледжей, как правило начавшие взламывать в 14 лет и к тому времени втянувшиеся в наркоторговлю, преимущественно ЛСД и кокаин, по словам Максфилда. Вот пример недавнего сообщения на BBS:

```
КУПЛЮ: ЛСД любого вида. Пишите мне, если готовы обсудить цены, возьму
хоть до 5 долларов за дозу. 3 доллара — лучше.

                                                    --urlord
```

BBS — это ещё и универсальные обучающие инструменты. Хакеры публикуют подробные пособия по:

ХАКЕРСТВУ (HACKING): использование персонального компьютера и модема для проникновения в закрытые компьютерные системы корпораций, фондов, университетов и банков.

КАРДИНГУ (CARDING): использование действительных номеров кредитных карт, полученных из выброшенных чеков, аккаунтов, вывешенных в видеопрокатах, или путём взлома компьютеров кредитных бюро.

ТРЭШИНГУ (TRASHING): рытьё в мусоре в поисках выброшенных чековых корешков, квитанций, компьютерных паролей, кодовых слов, конфиденциальных телефонных справочников компаний.

ФРИКИНГУ (PHREAKING), или **ФОНИНГУ (FONING):** манипулирование телефонными системами, как правило для бесплатных звонков на дальние расстояния.

Ниже приводится отрывок из четырёхчастного пособия по мошенничеству с кредитными картами, опубликованного на эксклюзивной восточнопобережной BBS для элитных хакеров высокого уровня:

```
Кардинг! Автор: Music Major. Хотите верьте, хотите нет, но без кардинга
американским (и особенно канадским) компьютерщикам пришлось бы туговато.
Вы можете представить, что пришлось бы откладывать деньги, чтобы КУПИТЬ
модем на 2400 бод и винчестер на 30 мегабайт для BBS? О, конечно,
это возможно, но учитывая, что большинство активных пользователей
компьютеров ещё учатся в школе и не имеют постоянной работы, простому
человеку понадобится слишком много времени и денег, чтобы поднять BBS.
```

```
Работая неполный рабочий день за минимальную зарплату, нужно ПОСТОЯННО
откладывать 30 недель, чтобы запустить BBS (с нормальным модемом и
нормальным диском). Невесёлая перспектива! Когда становится совсем туго,
крутые идут в кардинг!

Далее Music Major вдаётся в детали и предупреждает молодых хакеров
о возможных рисках при попытке использовать метод, который он, по его
словам, изобрёл: «Я назвал этот метод "фонингом за картами". Чтобы быть
убедительным, вы ОБЯЗАНЫ свободно говорить и иметь умеренно низкий голос
(пропустите эту часть, если голос ещё ломается, — вернитесь, когда
обзаведётесь настоящим голосом)».
```

Операция Максфилда называется BoardScan. Крупные корпорации и учреждения платят ему за сбор и предоставление им актуальных разведданных о компьютерном андерграунде. Максфилд также привлекает реформировавшихся хакеров. Благодарственные письма от VISA и McDonald's украшают стену в его офисе наряду с фотографией с автографом Скотти — инженера звездолёта «Энтерпрайз» из сериала «Звёздный путь».

Нередко он сам выходит на потенциальных клиентов по деловым вопросам. «Чаще я звоню им и говорю: я обнаружил хакера в вашей системе», — рассказал Максфилд. «К тому моменту они уже прочно обосновались. Как только хакеры проникают в ваш компьютер, вы в беде. Это похоже на тараканов или мышей в стенах вашего дома. Поначалу они себя не обнаруживают. Но в один прекрасный день вы открываете холодильник, и оттуда вываливается пригоршня тараканов».

До того как заняться слежкой за хакерами, Максфилд около двадцати лет проработал в железном секторе бизнеса, устанавливая и обслуживая компьютеры и телефонные системы. Когда несколько лет назад ФБР завербовало его для работы под прикрытием в роли хакера и телефонного фрикера, Максфилд пришёл к выводу, что борьба с хакерской преступностью — его жизненная миссия.

«Так я стал хакером, которым всегда боялся стать», — сказал он. Максфилд считает, что проблема с хакерами становится всё серьёзнее. По его оценке, в 1982 году хакеров было всего 400–500. По его словам, каждые два года их число увеличивается в 10 раз. Ещё одна тревожная тенденция, наметившаяся в последнее время, — появление взрослых компьютерных хакеров. Некоторые взрослые в компьютерном андерграунде играют роль факинов — персонажа из романа Чарльза Диккенса, возглавлявшего банду малолетних преступников, — завлекая молодых хакеров в свои подпольные криминальные сети.

Предоставлено Galaxy Girl и Silicon Thief
Существенное редактирование — Knight Lightning
Автор оригинала — Лиза Олсон (штатный автор Detroit News)

Несколько замечаний от KL: я предполагаю, что кардинговое пособие Music Major представляло собой четыре сообщения, опубликованных на подборде по кардингу на Stronghold East. Если это так, то в момент написания статьи или незадолго до него Максфилд находился на SE. Этот пост, по всей видимости, был сделан ещё до МАССОВОЙ чистки пользователей на Stronghold East.

Список узлов BITNET

[Список из 2491 записи — опущен как справочные данные]

Дэниел Зигмонд: настоящий журналист или внештатный агент ФБР?

Автор: Knight Lightning

---

20 мая 1986 г.

Данная статья не отдаёт предпочтение ни одной из вышеупомянутых точек зрения, однако попытается рассмотреть свидетельства и факты, касающиеся обоих утверждений.

Дэниел Зигмонд хочет написать статью о хакерах и фрикерах, о нашей социальной среде и о нашей стороне истории. Он действительно является приглашённым редактором журнала Amiga World Magazine и проживал по адресу 6735 Forest Glen Road, Squrill Hill, Пенсильвания, с телефонными номерами (412)422-1979/7515 как минимум три года. По имеющимся сведениям, у него есть аккаунты в ARPAnet, Private Sector и на BBS журнала Byte Magazine.

Он участвовал в нескольких конференциях и разговаривал с рядом фрикеров по всей стране. Вот некоторые из них: Blue Buccaneer, Cap/N/Crax, Compu-Phreak, Dark Cavalier, Dead Lord, Final Impulse, Holophax Phreaker, Knight Lightning, Ninja NYC, Scan Man, Sigmund Fraud, Slave Driver, The Bootleg, The Clashmaster, The Infiltrator, The Firelord, The Seker и TUC.

Он записывает все свои разговоры и пытался убедить людей позвонить другим фрикерам по трёхстороннему соединению, стремясь таким образом узнать их номера телефонов. Тем не менее он предпринял некоторые попытки помочь Sigmund Fraud после его почти состоявшегося ареста (см. соответствующую статью в этом выпуске).

О господине Зигмонде есть несколько весьма странных вещей.

1. Он хочет, чтобы все присылали ему коды, экстендеры, АТС (PBX), переадресаторы и тому подобное — даже если они уже не работают. На вопрос о причине он ответил, что ему нужно что-то показать редактору, иначе тот откажет, сочтя материал беспочвенным.

Почему бы ему просто не придумать что-нибудь? Ведь он сам сказал, что достоверность не обязательна. Его ответ состоял в том, что редактор может несколько проверить. Но если бы это были нерабочие коды или PBX, он в любом случае оказался бы в затруднительном положении.

Ладно, оставим это на минуту. Зигмонд также просил людей фотокопировать свои записные книжки и отправлять ему эти копии, обещая оплатить пересылку и само копирование. Это, разумеется, означает, что он получает ваш адрес — или как минимум ваш район по штемпелю (даже если вы не укажете обратный адрес).

2. Он отказывается давать номер телефона, по которому его можно застать на работе или в Amiga World. Более того, он не планирует публиковать статью в Amiga World — напротив, заявил, что продаст её в Washington Post.

Я разговаривал с людьми в Washington Post, и они ничего об этом не знают. Я общался с сотрудниками из нескольких разных отделов и везде получил отказ. Они даже не знали, кто такой Зигмонд.

Это оставляет две возможности: либо он никогда не имел намерения отправлять им статью, либо просто бахвалился в поисках славы и внимания.

3. PBX, который Sigmund Fraud обнаружил во время взлома UNIX, был передан Зигмонду. До этого он ни разу не использовался — если не считать единственной конференции для проверки, — а спустя неделю после передачи Зигмонду исчез.

4. Ещё один весомый момент: Зигмонд утверждает, что когда в августе 1986 года он сдаст статью (куда бы то ни было) и получит за неё 900 долларов, он едва выйдет в ноль — с учётом расходов на телефон и прочих затрат на материал.

Выйти в ноль после всего этого времени, труда и усилий кажется мне бессмысленным — зачем ему это делать? Говорят, что информаторам ФБР платят очень хорошо. Не то чтобы я утверждал, что Зигмонд является информатором ФБР.

Ещё кое-что, что может оказаться интересным: Зигмонд настаивает на том, что получит аккаунты на Metal Shop Private и Stronghold East, хотя Taran King и Slave Driver уже дали ему весьма твёрдые «нет». Он продолжает рассказывать об этом окружающим. Автоответчик его телефона даёт менее десяти секунд на сообщение — возможно, для защиты от взлома, хотя это в любом случае раздражает.

Прошу всех отнестись к этому файлу так, как он задуман. Здесь не утверждается, что Дэниел Зигмонд помогает федеральным агентам; вполне возможно, что он искренне интересуется и хочет познакомиться с нашим сообществом. Из всего этого я заключаю, что он узнает: в сообществе фрикеров мы стараемся защищать друг друга от арестов, и такой журналист, как он, буквально мог бы уничтожить мир фрикеров, если бы сотрудничал с федералами и оставался без вопросов и контроля.

Эта статья является предупреждением всем, кто может вступить в контакт с Зигмондом: руководствуйтесь собственным здравым смыслом при общении с ним. Уверен, что как только он ответит на вопросы, поднятые в этой статье, всё будет в порядке.

Единственное, что я ещё хотел добавить: в целом журналисты в прошлом наносили огромный ущерб миру фрикеров и хакеров. Они привлекают к фрикерам слишком много внимания и выставляют нас на всеобщее обозрение. В результате принималось всё больше законодательных актов, создающих новые законы против нас. Некоторые примеры очевидны прямо в этом выпуске PWN. Blue Buccaneer указывает на всевозможные вещи в статье о новых законах о хакерстве. Помните новые законы об ответственности сисопов за свои доски? Видели, как это было использовано в деле об арестах Teltec? Там становится невероятно опасно, друзья — давайте постараемся не усугублять ситуацию.

:Knight Lightning

Как одолеть Ричарда Проктора в 4 простых шага!

10 июня 1986 г.

Кто этот новый следователь в Атланте? Что делает его сегодня новейшей и, возможно, наибольшей угрозой для мира фрикеров? Следующая информация касается следователя MCI по имени Ричард Проктор, также известного как Джон Проктор.

Ричард Проктор, который также представляется другим как Джон Проктор, — один из многочисленных следователей MCI, ныне рыскающих по стране. Он руководит большей частью отделов безопасности и расследований MCI, а также отвечает за расследования MCI на

юго-востоке, восточном побережье и северо-востоке. Он также имел дело с фрикерами на Среднем Западе и Юго-Западе.

Я не уверен в пределах его «юрисдикции», однако все пользователи MCI должны быть осторожны вне зависимости от своего местоположения. Holophax Phreaker и The Infiltrator могут лично рассказать вам, как он ведёт расследования MCI — они уже дважды находились под следствием. Holophax Phreaker в настоящее время всё ещё находится под следствием Проктора и даже своей местной телефонной компании (BOC).

Первое, что большинство следователей делает при обнаружении злоупотребления кодом доступа, — ждут, пока не накопится крупный счёт (что может и не случиться). Это объясняется тем, что преследовать человека, наговорившего менее чем на 500 долларов, для службы дальней связи невыгодно (в зависимости от оператора).

Ричард Проктор — совершенно иной случай. Как только он обнаруживает злоупотребление кодом доступа, он незамедлительно принимает меры. Ниже описана последовательность событий, которые произойдут после того, как Проктор обнаружит скомпрометированный аккаунт.

В следующих шагах «вы» — это фрикер, о котором идёт речь, совершавший звонки (не дай бог). Перечисленные шаги касаются как «вас», так и лица (лиц), получавших незаконно совершённые звонки.

Шаг 1: Проктор лично позвонит на *КАЖДЫЙ* номер назначения в аккаунте и попросит информацию о том, кто звонил им в дату(ы) совершения звонка(ов). Если это BBS, он свяжется с сисопом по голосовому каналу, а если голосового номера нет — направит одного или нескольких следователей из ближайшего отдела расследований MCI для допроса сисопа. Он попросит предоставить информацию о фрикере. Будем надеяться, что ваши страдающие амнезией друзья каким-то образом забудут о вас и не смогут сообщить Проктору ничего.

Шаг 2: Проктор ждёт пару дней, затем снова связывается с лицами, получавшими звонки, и говорит, что нашёл вас и что вы сообщили ему: люди, с которыми «вы» разговаривали, также совершали эти звонки, — и что Проктор арестует этих лиц, если только они не захотят оплатить звонки. (Если этот пункт касается вас — то есть если вы были тем, кто получал звонки, и Проктор или какой-либо агент сказал вам это, — вам следует немедленно обратиться к адвокату, поскольку это является телефонными домогательствами — федеральным преступлением, совершённым через межштатного перевозчика связи, — и вы можете подать в суд на MCI или соответствующую компанию.)

Шаг 3: Если некоторые из лиц, которым вы звонили, оказались не такими амнезийными, как вам хотелось бы, когда Проктор с ними говорил, и Проктор затем позвонил вам или вашим родителям — отрицайте всё, в чём он вас обвиняет, сколько бы людей он ни заявил, что сдали вас. Проктор будет лгать (будем надеяться), поэтому отрицайте всё.

Шаг 4: Проктор снова позвонит вам через пару дней и скажет, что у вас последний шанс явиться с повинной. Когда вы снова откажетесь, Проктор постарается вас запугать, заявив, что MCI сделает из вас показательный пример и будет преследовать вас в полной мере закона. Если Проктор так поступает, знайте: у него нет против вас улик или в лучшем случае есть лишь косвенные.

После этого вы можете получить ещё несколько звонков. Продолжайте всё отрицать и обязательно прекратите фрикинг приблизительно на 1,5–2 месяца. Если вам позвонит местная телефонная компания — прекратите как минимум на 6 месяцев — год. Скорее всего, они установят на вашей линии пен-регистратор или DNR.

У Проктора есть учёные степени в области психологии и криминальной психологии, поэтому будьте очень осторожны! Он ничего не сможет вам сделать, если вы будете следовать приведённым выше

рекомендациям, — если только он не поставил трассировку на используемый вами аккаунт. В таком случае он появится у вашей двери и арестует вас. Лучший вариант — держаться от этого подальше в принципе. Домашний телефон Проктора не указан в справочнике (разумеется), однако его рабочий номер можно получить у любого оператора MCI.

Информация предоставлена Holophax Phreaker и The Infiltrator

Кратко

Stronghold East теперь работает на новом Apple //e — благодаря своим друзьям из AMEX. Прежде SE работал на Franklin Ace. *3 мая 1986 г.*
Совсем недавно жёсткий диск SE вышел из строя, и до приобретения нового ProDos Apple net они работают на Phlash-Net, написанном Phlash Gordon.

Ходят слухи, что Apple Wizard был арестован за торговлю и употребление кокаина.

Некий пользователь под ником CPTN был арестован в Неваде за что-то связанное с инцидентом «Капитан Полночь» (Captain Midnight). Он также был арестован за кардинг и задержан с незаконно полученными модемами. *Информация от Death Angel.*

Один из участников Underworld Elite, которой руководит Night Stalker, был арестован за звонок в Белый дом с угрозой взрыва. Секретная служба пришла к нему домой, зная, что он использовал незаконные экстендеры для совершения звонков. Этот пользователь решил выдать им номер и пароли к Underworld Elite. Он был удалён. *Информация от Night Stalker, 11.05.86... The Underworld (216)356-9464*

Telenet Bob был арестован. Полная история появилась в апрельском номере журнала 2600 Magazine. Девятнадцатилетний из Нью-Джерси. Имя — Роберт Давенпорт. Штраф 500 долларов, возмещение ущерба AT&T в размере 890 долларов. *Информация от Sally Ride:::Space Cadet*

Bad Boy In Black отказался от BBS и фрикинга (в основном), так что вы, скорее всего, больше не услышите о нём. По его словам, ему наскучил BBSing, и с приближением лета у него стало мало времени. Поэтому он решил бросить это насовсем. *Информация от [bad boy in black], 11.05.86*

Shooting Shark также покинул мир фрикеров примерно по тем же причинам, плюс тот факт, что поступает в колледж. *Информация от Shooting Shark.*

В Техасе какой-то полицейский вёл BBS под названием The Tunnel. Никто арестован не был, однако были собраны имена и никнеймы тех, кто публиковал незаконные коды. Полицейский получил несколько угроз убийством.

The Slayer был арестован 25 апреля 1986 года. По имеющимся сведениям, к нему явились агенты Metrophone, MCI, New Jersey Bell и ФБР. Его арест был связан со злоупотреблением Metro. The Godfather из Род-Айленда также был причастен к этому аресту, и на данный момент он уже покинул мир фрикеров — хотя дополнительная информация по этому поводу отсутствует. Совсем недавно выяснилось, что The Slayer был нанят оператором TSPS.

Ещё новости о The Sprinter: когда всё было сказано и сделано, Sprinter пошёл на сделку с правосудием (как и ожидалось) и признал себя виновным по предъявленным обвинениям. Он провёл 14 дней в тюрьме, получил штраф 2000 долларов, 2 года испытательного срока, 200 часов общественных работ и, разумеется, расходы на адвоката. На данный момент он не принял предложение о работе от MicroSoft. *Информация от Jester Sluggo.*

Сообщается, что The Mentor и Crustaceo Mutoid теперь пишут для информационного бюллетеня в Калифорнии под названием The Underground Informer.

The Arabian Knight был арестован за организацию конференций.

The Guardian Demon (215), по всей видимости, был арестован за злоупотребление Metrophone, однако официальные обвинения ещё не предъявлены.

Jester Sluggo официально завершил работу со всеми досками и теперь занимается исключительно хакингом. Он сохранит свои контакты в мире фрикеров. Сисопы просят удалить его аккаунты.