Phrack RU issue 021

Русская версия Phrack, выпуск 021. Полный текст статей с кодом и таблицами.

Темы выпуска: культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; сети, маршрутизация, TCP/IP, Cisco, телефония и телеком-инфраструктура.

Материалы выпуска: Содержание выпуска; Phrack Pro-Phile XXI; Тени прошлого в будущем; The Tele-Pages; Спутниковая связь; Организации, обеспечивающие работу телекоммуникационных сетей: Центр управления сетью; Неопубликованные номера; Блокировка междугородных звонков; Шоу Эда Шварца на радио WGN 720 AM; Phrack World News; Phrack World News.

Больше крутых материалов в моём телеграм канале @grogrigs

Содержание выпуска

Авторы: Taran King и Knight Lightning

4 ноября 1988 года

Добро пожаловать в двадцать первый выпуск Phrack Inc. До сих пор мы весьма продуктивно собирали материалы и готовили выпуски на будущее. Если вы хотите предложить свой материал для Phrack Inc., пожалуйста, свяжитесь с The Mentor или Epsilon — они переправят файлы нам. Если вы подключены к одной из смежных сетей, отправляйте письма и/или файлы на адрес Taran King: `C488869@UMCVMB.BITNET`. Мы рады представить трилогию, посвящённую безопасности сообщества фрикеров и хакеров, а также различным её аспектам. Первый файл — «Тени прошлого будущего» — опубликован в этом выпуске, следующие два войдут в последующие, так что следите за обновлениями. Здорово снова быть «в деле».

— Taran King & Knight Lightning

Phrack Pro-Phile XXI

Автор: Taran King

Цель рубрики Phrack Pro-Phile — познакомить читателей с биографиями старых или известных хакеров и фрикеров, существующих ныне или в прошлом. Герой этого месяца — пользователь ушедшей эпохи... Modem Master, он же Napoleon Solo.

Личные сведения

```
        Хэндл:  Napoleon Solo
     Зовите:  Скотт
Прошлый хэндл:  Modem Master
Происхождение хэндла:  Я был настоящим фанатом сериала «Человек из U.N.C.L.E.»
  Дата рождения:  29 марта 1970
  Текущий возраст:  18 лет
         Рост:  182 см
          Вес:  93 кг
        Глаза:  Ореховые
       Волосы:  Светло-каштановые
   Компьютеры:  Apple //+, Apple //gs, стандартное дополнительное железо, модем 2400 бод
```

Я вступил на путь хакерства в начале 1983 года, когда купил свой первый модем — Networker на 300 бод (что за чудо техники!) — для своего Apple II+. Я попросил продавца дать номера местных досок (в то время их было целых три, и одна из них была доска пользователей IBM). Как оказалось, одна была Apple-доской, работавшей на старой версии Networks II, с сисопом, который был известен тем, что изредка нагревал один местный экстендер. Поговорив со мной какое-то время, он понял, что я из тех жадных до знаний школьников-семиклассников, и свёл меня с несколькими другими пользователями своей доски. Одним из них оказался Simon Templar, который впоследствии стал сисопом Pearly Gates — и, пожалуй, самым близким другом, какой только может быть у фрика, живущего в тысяче миль от тебя.

Simon дал мне мой первый код (к номеру 800, принадлежавшему LDX) и номера нескольких досок, где можно было набраться дополнительных знаний (IC's Socket, AT&T Phone Center и Sherwood Forest). Поистаскав буквально каждого, кто хоть что-то знал, я встал на верный путь. Вскоре я бывал как минимум на одной доске в каждом телефонном коде. Я также усвоил преимущество сканирования АТС — нашёл несколько местных АТС и Sprint indial, о котором никто, казалось, не знал. Это ещё больше облегчило мою «привычку», и я обнаружил небольшой Diversi-Dial под названием «Beandial». Именно там я по-настоящему взлетел. Там собирались многие знающие фрики, и благодаря этому, а также всем BBS, на которых я сидел, у меня под рукой была целая сокровищница знаний на любой вопрос.

Beandial принёс мне и нескольких хороших друзей, из которых наиболее примечателен Lord Kahz. Кроме того, он свёл меня с весьма известным человеком — King Blotto (надо было видеть моё лицо той ночью, когда мне позвонили и голос на другом конце произнёс: «Привет, это King Blotto, хочешь быть на моей доске?» — и дал номер!). В последние несколько лет я ушёл из мейнстримного фрикерства и лишь изредка заглядываю туда через старых друзей. Теперь это может измениться, поскольку Taran King и Knight Lightning показали мне, что настоящие фрики всё ещё существуют. Я начинал сомневаться в этом — отсюда и моё отсутствие.

Запоминающиеся доски, на которых я бывал: The Pearly Gates, AT&T Phone Center, Blottoland (пусть я попал туда лишь в последней фазе её существования) и Bean Dial — плюс все обычные, на которых сидел каждый и его брат.

Сейчас я учусь в Университете штата Северная Дакота на специальности «компьютерная инженерия». Работаю в McDonald's — жарю котлеты.

Сожаления

Жалею, что вообще бросил мир фрикерства. Меня разочаровали все эти мелкие нерды с компьютерами и модемами, которые думали, что они фрики только потому, что какой-то болван из их окружения дал им код.

Любимое

Девушки: Те, у которых очень большой... э... Мозг! Вот именно! Знаете, они выпячивают из бюстгальтера... Э... то есть их интеллект так и выпирает!! Ага, именно!

Люди: Мне нравится почти любой, кому есть что интересное и значимое сказать (ну и девушки с большой ****)

Музыка: Музыка 70-х — Led Zeppelin и большинство хэви-метал групп. Могу слушать и топ-40, лишь бы там не было Уитни, Джексона, Дж. Майкла или им подобной дряни.

Самые памятные моменты

Тот раз, когда мы с другом из Айдахо позвонили одному местному парню, который ДУМАЛ, что он фрик. Я говорил с ним по одной линии, а МАЙК — по другой, с межгорода, убеждая его, что служба безопасности AT&T реально повязала его. Я никогда в жизни не слышал, чтобы кто-то звучал так испуганно! ХАХАХ

Два года в составе команды по американскому футболу своей старшей школы — вместо обычных 0–1 года.

Люди, которых стоит упомянуть

• Lord Kahz
• Cookie Cruncher
• Android Base — за то, что указал верное направление
• Simon Templar — за то, что взял это направление и показал, что с ним делать

Всем остальным, кто так или иначе помогал мне — с вопросами или чем-то ещё... Спасибо.

Внутренняя шутка

Для Kahz: «Эй, ММ, давай позвоним Мари!»

Серьёзный раздел

Я думаю, что те, кто злоупотребляет кредитными картами, — идиоты. Это не приносит ничего, кроме вреда нам всем: один человек получает выгоду, а многие страдают. Например, сисопы досок, где неизбежно ПОЙМАННЫЙ идиот выкладывал номера своих CC.

Хотя Скотт никогда не встречал хакеров лично, по некоторым телефонным разговорам он считает, что там попадаются отдельные чудаки.

Спасибо за уделённое время, Скотт.

— Taran King

Тени прошлого в будущем

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                            <>
<>                  Shadows Of A Future Past                  <>
<>                  ~~~~~~~~~~~~~~~~~~~~~~~~                  <>
<>           Part One Of The Vicious Circle Trilogy           <>
<>                                                            <>
<>        A New Indepth Look At A Re-Occurring Problem        <>
<>                    by Knight Lightning                     <>
<>                                                            <>
<>                       August 6, 1988                       <>
<>                                                            <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

Автор: Knight Lightning

6 августа 1988 г.

Часть первая трилогии «Порочный круг»

Новый глубокий взгляд на повторяющуюся проблему

В чём проблема?

Судьба всего модемного сообщества в значительной мере держится на фундаменте компьютерных досок объявлений (BBS). Эти пространства для обмена информацией превратились в центры обучения и распространения самых разных сведений для тысяч хакеров по всей территории Соединённых Штатов и по всему миру.

Однако сегодняшние консультанты по безопасности и правоохранительные органы тоже стали умнее, чем когда-либо прежде, и они знают, куда бить, чтобы нанести максимальный ущерб. Идея создать BBS специально для поимки хакеров была неслыханной вплоть до инцидента с Phoenix Phortress в 1986 году. Создание этой системы позволило сержанту Дэну Паскуале из полицейского департамента Фримонта проникнуть сквозь незримый барьер, отделяющий сообщество фрикеров и хакеров от остального мира.

Настоящий файл призван показать масштабы этой проблемы внутри сообщества и, возможно, поможет читателям найти способы защитить себя от многочисленных «венериных мухоловок», с которыми им предстоит столкнуться. Материалы, представленные здесь, — специально отредактированные перепечатки из прошлых выпусков Phrack World News.

Доказательства — незримые истины таятся в тенях нашего прошлого и будущего

Ниже приведён отрывок из Phrack World News, выпуск III:

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Phoenix Phortress: семеро попались в сети

5 марта 1986 года были арестованы следующие семь фрикеров — в ходе того, что вошло в историю как первая «подставная» операция по компьютерным преступлениям:

```
Captain Hacker \ Doctor Bob \ Lasertech \ The Adventurer
       The Highwayman \ The Punisher \ The Warden
```

Многие из них или другие участники Phoenix Phortress состояли в следующих группах:

```
High Mountain Hackers \ Kaos Inc. \ Shadow Brotherhood \ The Nihilist Order
```

Из семерых: троим было по 15 лет, двоим — по 16, одному — 17, одному — 19.

Им были предъявлены обвинения:

• несколько правонарушений (мисдиминоров);
• торговля похищенными кодами доступа к услугам дальней связи;
• торговля похищенными номерами кредитных карт;
• хранение похищенного имущества;
• хранение холодного оружия (оружие боевых искусств);
• заказ товаров по почте с оплатой похищенными кредитными картами;
• сбыт похищенного имущества;
• звонки за рубеж за счёт чужих телефонных номеров.

Среди других фрикерских досок, упомянутых в деле:

• **Bank Vault** (преимущественно номера кредитных карт и советы по мошенничеству с ними)
• **Phreakers Phortress** (преимущественно коды для фрикинга и прочая информация)

После того как ранним утром в среду по семи адресам во Фримонте, где молодые люди жили с родителями, были проведены обыски, полиция изъяла оборудование на сумму не менее 12 000 долларов: компьютеры, модемы, мониторы, дискеты и руководства с информацией от инструкций по изготовлению бомб до кодов доступа к корпоративным компьютерам финансовых компаний Merrill Lynch и Dean Witter.

Сисопом Phoenix Phortress был The Revenger — предположительно некий Уолли Ричардс, 25-летний житель Хейворда, который «немного фрикил на востоке» в Нью-Джерси. Телефонный номер он оформил на имя Эл Дэвис. На самом же деле им был сержант Дэниел Паскуале из полицейского департамента Фримонта.

Представляя свою доску другим пользователям, он называл её «новейшей, крутейшей фрикерской доской в округе».

Паскуале рассказал, что идея подставной операции пришла к нему после того, как 16-летний подросток, арестованный прошлым летом за хранение краденого, «сдал их всех. Он рассказал нам всё об их делах».

Паскуале использовал компьютер Apple //e и оборудование полицейского департамента, а коды доступа и информацию предоставили восемь корпораций, в том числе Wells Fargo Bank, Sprint и MCI.

По его словам, доска приняла более 2500 звонков примерно от 130 постоянных пользователей со всей страны. Первое дело полиция начала разрабатывать через три дня после запуска доски.

> *«Мы оформили скрытый телефонный номер на имя Эл Дэвис, — рассказывал Паскуале. — За шесть дней эти ребята выложили имя на доску. Мне бы пришлось получать ордер на обыск, чтобы добыть такую информацию».*

Аресты состоялись после пятимесячного расследования, которое вёл Дэн Паскуале.

Инцидент с Phoenix Phortress привёл к аресту всего семи хакеров. Однако одновременно он позволил правоохранительным органам собрать сведения более чем о сотне других хакеров, об

обсуждавшихся системах, обо всей переписке по электронной почте на доске — и, по всей видимости, дал им информацию о сотнях других хакеров, досок и всего прочего.

Ниже приведён отрывок из Phrack World News, выпуск VII:

Maxfield снова наносит удар — 20 августа 1986 г.

Многие из вас, вероятно, помнят систему под названием «THE BOARD» в зоне NPA 313 (Детройт). Номер был 313-592-4143, а пароль для новых пользователей — `HEL-N555,ELITE,3` (затем Enter). Система была несколько необычной, поскольку работала на компьютере HP2000.

20 августа 1986 года на THE BOARD начали появляться следующие сообщения:

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

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

                      300/1200 baud - 24 hours.

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


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

Greetings:

You are now on THE BOARD, a "sting" BBS operated by MIKE WENDLAND of the
WDIV-TV I-Team.  The purpose?  To demonstrate and document the extent of
criminal and potentially illegal hacking and telephone fraud activity by the
so-called "hacking community."

Thanks for your cooperation.  In the past month and a half, we've received all
sorts of information from you implicating many of you to credit card fraud,
telephone billing fraud, vandalism, and possible break-ins to government or
public safety computers.  And the beauty of this is we have your posts, your
E-Mail and--- most importantly ---your REAL names and addresses.

What are we going to do with it?  Stay tuned to News 4.  I plan a special
series of reports about our experiences with THE BOARD, which saw users check
in from coast-to-coast and Canada, users ranging in age from 12 to 48.  For our
regular users, I have been known as High Tech, among other ID's.  John Maxfield
of Boardscan served as our consultant and provided the HP2000 that this "sting"
ran on.  Through call forwarding and other conveniences made possible by
telephone technology, the BBS operated remotely here in the Detroit area.

When will our reports be ready?  In a few weeks.  We now will be contacting
many of you directly, talking with law enforcement and security agents from
credit card companies and the telephone services.

It should be a hell of a series.  Thanks for your help.  And don't bother
trying any harassment.  Remember, we've got YOUR real names.

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


Board:   General Information & BBS's
```

```
Message: 42
Title:   BOARDSCAN
To:      ALL
From:    THE REAPER

This is John Maxfield of Boardscan.  Welcome!  Please address all letter bombs
to Mike Wendland at WDIV-TV Detroit.  This board was his idea.

The Reaper (a.k.a. Cable Pair)

--------------------------------------------------------------------------------
```

Джон Maxfield в целом был чрезвычайно горд своей работой с THE BOARD и говорил, что многие из тех, чьи голоса он идентифицировал, должны были сразу его узнать. По словам Maxfield, единственная цель этой подставной доски — показать «что сейчас происходит в сообществе фрикеров и хакеров». Он заявил, что никаких правовых последствий не будет, и вдобавок операция хорошо «пополнила его досье» на многих людей!

[Репортажи для WDIV-TV 4 появились в Phrack World News, выпуск IX.]

Вот классический пример того, как люди не учатся на чужих ошибках. В какой-то момент до этого инцидента номер THE BOARD был опубликован, вокруг доски поднялся ажиотаж, и она в итоге заманила хакеров, словно мух в паутину — из которой ничего не подозревавшие пользователи уже не выбрались.

Вот о чём я и пытаюсь сказать: сегодняшний фрикер/хакер должен научиться думать о безопасности. Что даёт кому бы то ни было основания доверять человеку только потому, что тот запустил доску объявлений? Именно эта слепая вера и погубит многих хакеров, пока они не поумнеют и не начнут внимательнее следить за тем, что делают. Безопасность прежде всего — ставки в этой игре намного выше, чем неделя без телевизора: стоит телефонному номеру хакера попасть не в те руки, и правоохранители или такие организации, как Ассоциация по противодействию телекоммуникационному мошенничеству (CFCA), смогут узнать о вас всё. Я знаю это, потому что сам видел их картотеки, — и их база данных по хакерам невероятно обширна и точна... это просто поразительно.

Ниже приведён отрывок из Phrack World News, выпуск XIV:

Metalland South: фрикерская BBS или MetaliFEDS Inc.? — 2 июня 1987 г.

BBS Metalland South по номеру 404-327-2327 была когда-то довольно известной доской, где обитали многие уважаемые члены сообщества хакеров и фрикеров. Первоначально её вели двое ребят из Metal Communications, Inc., хотя это не был клубный сайт MCI. Сисопом числился Iron Man, сосисопом — Black Lord. Недавно автору стало известно, что MLS сменила руководство, политику и, возможно, саму концепцию — а именно превратилась в ловушку.

Где-то в сентябре-октябре 1986 года Iron Man удалил со своей системы все подфорумы, посвящённые хакингу и фрикингу, а также все G-файлы. По всей видимости, он опасался ареста. В последний раз, когда этот репортёр разговаривал с ним, Iron Man говорил, что намерен вернуть хак/фрик-разделы на место. Вскоре после этого разговора номер сменился (прежний был 404-576-5166).

Некто, использующий псевдоним The Caretaker, стал сосисопом, а Iron Man перестал отвечать на обратную связь. Всем занимался The Caretaker [далее — TC]. TC не допускал никаких хак/фрик-разделов, но обещал их открыть, если пользователи согласятся пройти СТРОГУЮ верификацию.

Строгая верификация на MLS включала:

```
^*^  Ваше настоящее имя
^*^  Ваш адрес
^*^  Ваш голосовой телефонный номер
^*^  Конверт с обратным адресом (в котором вам вышлют номер аккаунта и пароль)
```

Последствия очевидны. Доска или сисоп попадается, а затем договаривается передать доску какой-то компании или ведомству. Чтобы гарантированно получить нужных людей, вас заставляют предоставить все эти сведения, а пароль вам могут выдать только по почте — тем самым гарантируя: если под этим аккаунтом будет что-то незаконное опубликовано, ответственность несёте вы, и никаких «но».

Существовало ещё немало доказательств того, что Metalland South была ловушкой или подставной доской, а общая аура таинственности вокруг этой системы делала любой звонок туда бессмысленным риском.

Никогда и ни при каких обстоятельствах не сообщайте сисопу свой адрес, чтобы он выслал вам пароль по почте. Подобная информация совершенно не нужна — она способна лишь причинить вам серьёзный вред и не даст сисопу ничего, что не обернулось бы против вас.

Ещё один случай, связанный с досками объявлений, описан в PWN, выпуск V: речь идёт об обнаружении в Texacе очередной хакерской ловушки под названием The Tunnel. И не забудем о P-80 от TMC, которую вёл Scan Man, — именно она привела к задержанию Shawn of Phreakers Quest (известного также как Capt. Caveman).

Однако не обманывайте себя, полагая, что доски объявлений — единственное место, где вас могут поджидать неприятности. Обычные системы, с которыми вы привыкли работать, не менее опасны, если проявлять беспечность. Druidic Death и Celtic Phrost убедились в этом на собственном горьком опыте на Unix-системе MIT, едва не угодив в ловушку последовательного вовлечения, которая обоих бы погубила.

Ниже приведён отрывок из Phrack World News, выпуск XI:

MIT Unix: жертва или агрессор? — 23 января — 2 февраля 1987 г.

Была ли система MIT невинной жертвой хакерского произвола — или просто очередной ловушкой для поимки хакеров с поличным?

Всё началось вот так...

[Некоторые посты слегка отредактированы для соответствия теме]

```
------------------------------------------------------------------------------
MIT
Name: Druidic Death
Date: 12:49 am  Mon Jan 20, 1986

Lately I've been messing around on MIT's VAX in there Physics Department.

Recently some one else got on there and did some damage to files.  However MIT
told me that they'll still trust us to call them.  The number is:

617-253-XXXX

We have to agree to the following or we will be kicked off, they will create a
"hacker" account for us.

<1>  Use only GUEST, RODNEY, and GAMES.  No other accounts until the hacker one
     is made.  There are no passwords on these accounts.
<2>  Make sure we log off properly.  Control-D.  This is a UNIX system.
<3>  Not to call between 9 AM and 5 PM Eastern Standard Time.  This is to avoid
```

tying up the system.
<4> Leave mail to GEORGE only with UNIX questions (or C). And leave our handles so he'll know who we are.

Unix
Name: Celtic Phrost
Date: 4:16 pm Mon Jan 20, 1986

Thanks Death for the MIT computer, I've been working on getting into them for weeks. Here's another you can play around with:

617/258-XXXX login:GUEST

Or use a WHO command at the logon to see other accounts, it has been a long time since I played with that system, so I am unsure if the GUEST account still works, but if you use the WHO command you should see the GUEST account needed for applying for your own account.

-Phrost

Unix
Name: Celtic Phrost
Date: 5:35 pm Mon Jan 20, 1986

Ok, sorry, but I just remembered the application account, its: OPEN
Gawd, I am glad I got that off my chest!

-(A relieved)Celtic Phrost.

Also on that MIT computer Death listed, some other default accounts are:

LONG MIKE GREG NEIL DAN

Get the rest yourself, and please people, LEAVE THEM UNPASSWORDED!

MIT
Name: Druidic Death 12
Date: 1:16 am Fri Jan 23, 1987

MIT is pretty cool. If you haven't called yet, try it out. Just PLEASE make sure you follow the little rules they asked us about! If someone doesn't do something right the sysop leaves the gripe mail to me. Check out my directory under the guest account just type "cd Dru". Read the first file.

MIT
Name: Ctrl C
Date: 12:56 pm Sat Jan 24, 1987

MIT Un-Passworded Unix Accounts: 617-253-XXXX

ALEX BILL GAMES DAVE GUEST DAN GREG MIKE LONG NEIL TOM TED
BRIAN RODNEY VRET GENTILE ROCKY SPIKE KEVIN KRIS TIM

And PLEASE don't change the Passwords....

-=>Ctrl C<=-

MIT Again
Name: Druidic Death
Date: 1:00 pm Wed Jan 28, 1987

Ok people, MIT is pissed, someone hasn't been keeping the bargain and they aren't too thrilled about it. There were only three things they asked us to do, and they were reasonable too. All they wanted was for us to not compromise the security much more than we had already, logoff properly, not leave any processes going, and call only during non-business hours, and we would be able to use the GUEST accounts as much as we like.
Someone got real nice and added themselves to the "daemon" group which is

superusers only, the name was "celtic". Gee, I wonder who that could have been? I'm not pissed at anyone, but I'd like to keep on using MIT's computers, and they'd love for us to be on, but they're getting paranoid. Whoever is calling besides me, be cool ok? They even gave me a voice phone to chat with their sysops with. How often do you see this happen?

A little perturbed but not pissed...

DRU'

Tsk, Celtic.
Name: Evil Jay
Date: 9:39 am Thu Jan 29, 1987

Well, personally I don't know why anyone would want to be a superuser on the system in question. Once you've been on once, there is really nothing that interesting to look at...but anyway.

-EJ

In trouble again...
Name: Celtic Phrost
Date: 2:35 pm Fri Jan 30, 1987

...I was framed!! I did not add myself to any "daemon" group on any MIT UNIX. I did call once, and I must admit I did hang up without logging off, but this was due to a faulty program that would NOT allow me to break out of it, no matter what I tried. I am sure that I didn't cause any damage by that.

-Phrost

Major Problems
Name: Druidic Death
Date: 12:20 pm Sat Jan 31, 1987

OK, major stuff going down. Some unidentified individual logged into the Physics Dept's PDP11/34 at 617-253-XXXX and was drastically violating the "agreement" we had reached. I was the one that made the "deal" with them. And they even gave me a voice line to talk to them with.

Well, one day I called the other Physics computer, the office AT and discovered that someone created an account in the superuser DAEMON group called "celtic". Well, I was contacted by Brian through a chat and he told me to call him. Then he proceeded to nicely inform me that "due to unauthorized abuse of the system, the deal is off".

He was cool about it and said he wished he didn't have to do that. Then I called George, the guy that made the deal and he said that someone who said he was "Celtic Phrost" went on to the system and deleted nearly a year's worth of artificial intelligence data from the nuclear fission research base.

Needless to say I was shocked. I said that he can't believe that it was one of us, that as far as I knew everyone was keeping the deal. Then he (quite pissed off) said that he wanted all of our names so he can report us to the FBI. He called us fags, and all sorts of stuff, he was VERY!! [underline twice] PISSED! I don't blame him. Actually I'm not blaming Celtic Phrost, it very easily could have been a frame up.

But another thing is George thinks that Celtic Phrost and Druidic Death are one and the same, in other words, he thinks that *I* stabbed him in the back. Basically he just doesn't understand the way the hacker community operates.

Well, the deal is off, they plan to prosecute whoever they can catch. Since George is my best friend's brother I have not only lost a friend, but I'm likely to see some legal problems soon. Also, I can forget about doing my graduate work at MIT. Whoever did this damage to them, I hope you're happy. You really messed things up real nice for a lot of people.

Celtic, I don't have any reason to believe you messed with them. I also have no reason to think you didn't. I'm not making an accusation against you, but WHOEVER did this, deserves to be shot as far as I'm concerned. Until this data

was lost, they were on the verge of harnessing a laser-lithium produced form of nuclear fission that would have been more efficient than using the standard hydrogen. Well, back to the drawing board now.

I realize that it's hard to believe that they would have data like this on this system. But they were quite stupid in many other areas too. Leaving the superuser account with no password?? Think about it.

It's also possible that they were exaggerating. But regardless, damage seems to have been done.

MIT
Name: Phreakenstein
Date: 1:31 am Sun Feb 01, 1987

Heck! I dunno, but whoever it was, I think, should let himself (the s00per K-rad elyte d00d he is) be known.

I wasn't on MIT, but it was pretty dumb of MIT to even let Hackers on. I wouldn't really worry though, they did let you on, and all you have to prove is that you had no reason to do it.
----Phreak

I wonder...
Name: Ax Murderer 15
Date: 6:43 pm Sun Feb 01, 1987

I highly doubt that is was someone on this system. Since this is an elite board, I think all the users are pretty decent and know right and wrong things to do. Could be that one of the users on this system called another system and gave it out!??

Ax Murderer

It was stupid
Name: Druidic Death 12
Date: 9:21 pm Sun Feb 01, 1987

It seems to me, or, what I gathered, they felt that there were going to be hackers on the system to begin with and that this way they could keep themselves basically safe.

I doubt that it was Celtic Phrost, I don't think he'd be an asshole like that. But I can't say. When I posted, I was pretty pissed about the whole deal. I've calmed down now. Psychic Warlord said something to me voice the other day that made me stop and think. What if this was a set up right from the start? I mean, MIT won't give me specifics on just what supposedly happened, Celtic Phrost denies everything, and the biggest part of it is what George said to me.

"We can forgive you for what you did to us if you'll promise to go straight and never do this again and just tell us who all of your friends are that are on the system".

I didn't pay much attention to that remark at first, now I'm beginning to wonder...

I, of course, didn't narc on anyone. (Who do I know??? hehe)

DRU'

Comments...
Name: Delta-Master
Date: 7:15 am Mon Feb 02, 1987

It wouldn't surprise me if it was some kind of setup, it's been done before.

Delta-Master

[All posts in this article were taken from ShadowSpawn.]

- -

Решение

Что ещё тут добавить? Всё выглядит так, будто подставная операция действительно имела место, и это, вероятно, было не первый раз — и не последний. Так как же защитить себя?

Что касается досок объявлений: существует неписаное правило, гласящее, что хорошим сисопом может быть только тот, кто сам был хорошим пользователем. Если сисоп некой таинственной доски — человек, которого вы ни разу не встречали прежде, я бы туда не звонил. Но даже если это кто-то давно известный, рекомендации от того, кому вы доверяете, — необходимость. В конечном счёте всё сводится к надёжности информации и конкретных людей.

Когда имеешь дело с системами наподобие MIT Unix, помните: если что-то выглядит слишком хорошо, чтобы быть правдой, значит, скорее всего, вам что-то не договаривают. Кто в здравом уме раздаст свободные аккаунты в важной системе с деликатной информацией группе хакеров? Это безумие.

Надеюсь, этот файл послужит свежим и информативным взглядом на старую игру. Лично для меня: даже если время, потраченное на написание этой статьи, поможет или убережёт хотя бы одного фрикера/хакера — я считаю свою работу выполненной.

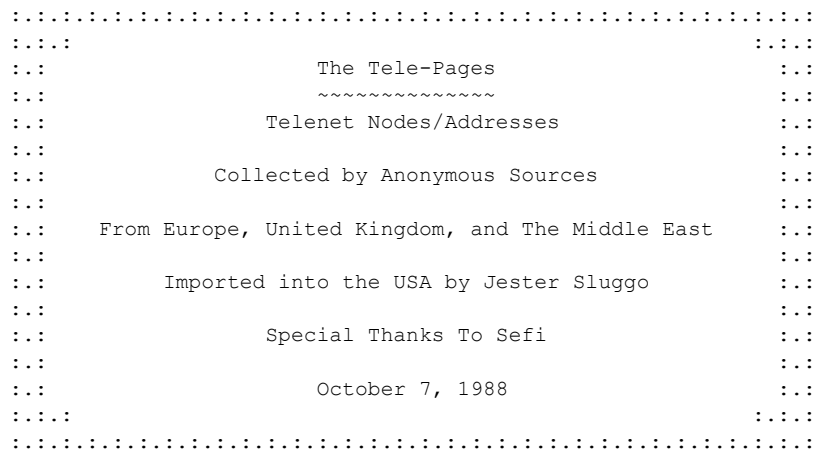
:Knight Lightning

```
                           "The Future Is Forever"

                             The Phoenix Project

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

The Tele-Pages



Автор: Jester Sluggo (при участии анонимных источников; особая благодарность — Sefi)

Этот файл содержит список узлов/адресов сети Telenet, которые используются при подключении за пределами США/Канады (например, из Великобритании, Европы или с Ближнего Востока). Огромная признательность замечательным людям, работавшим над этим бесчисленное количество месяцев. — Sluggo !!

`(* = Пароли, удалённые из данной публикации. — KL)`

Основная таблица узлов

[Таблица из 57 записей — опущена]

Колонки: Name | Number | Ext. | User Name | Password | KN | DN | NO | Test | Land

---

Дополнительные NUA по странам

Неклассифицированные записи (CTR)

[Таблица из 7 записей — опущена]

AUS — Австралия

[Таблица из 6 записей — опущена]

CH — Швейцария

[Таблица из 8 записей — опущена]

D — Западная Германия

[Таблица из 66 записей — опущена]

F — Франция

[Таблица из 5 записей — опущена]

GB — Великобритания

[Таблица из 70 записей — опущена]

I — Италия

[Таблица из 1 записи — опущена]

IRL — Ирландия

[Таблица из 4 записей — опущена]

N — Норвегия

[Таблица из 1 записи — опущена]

NL — Нидерланды

[Таблица из 1 записи — опущена]

S — Швеция

[Таблица из 3 записей — опущена]

SF — Финляндия

[Таблица из 2 записей — опущена]

USA — США

[Таблица из 408 записей — опущена]

— J. Sluggo

Спутниковая связь

Автор: Scott Holiday

11 июля 1988 г.

Системы спутниковой связи используют микроволновые терминалы на спутниках и наземных земных станциях для организации высоконадёжных и высокопропускных каналов связи. Коммуникационные спутники размещены на геосинхронных орбитах примерно в 22 000 миль над поверхностью Земли. Благодаря этому скорость вращения спутника совпадает со скоростью вращения Земли, и спутник кажется неподвижным относительно наземных станций. Для покрытия всего земного шара достаточно трёх равномерно распределённых спутников.

Микроволновые терминалы спутника принимают сигналы от земной станции и ретранслируют их на другой частоте на другую земную станцию. Из-за больших расстояний путь сигнала «туда и обратно» занимает около половины секунды. Это явление называется задержкой распространения. Задержка распространения на обычной наземной телефонной линии составляет около 1 миллисекунды (мс) на каждые 100 миль.

Каждый микроволновый терминал на спутнике, называемый репитером или транспондером, включает приёмник для восходящих (uplink) передач и передатчик для нисходящих (downlink) передач. Для восходящих и нисходящих передач выделены отдельные полосы частот в диапазоне 1,5–30 ГГц (1,5 ГГц равно 1 500 000 000 Гц, или 1,5 миллиарда герц). Типичные рабочие частоты коммуникационных спутников: 4–6 ГГц для INTELSAT 5 и 12–14 ГГц для Anik-B — канадского спутника.

Каждый спутниковый транспондер, как правило, имеет двенадцать каналов по 36 МГц, которые могут использоваться для передачи голоса, данных или телевизионных сигналов. Ранние коммуникационные спутники имели от 12 до 20 транспондеров, более поздние — до 27 и более. INTELSAT 5, например, располагает в общей сложности 27 и более транспондерами, обеспечивающими 24 500 каналов передачи данных/голоса, одним транспондером с двумя телевизионными каналами по 17,5 МГц и одним транспондером SPADE на 800 каналов. SPADE (Single carrier per channel, Pulse code modulation, multiple Access, Demand assignment — одна несущая на канал, импульсно-кодовая модуляция, множественный доступ, динамическое распределение) представляет собой цифровую телефонную службу, резервирующую пул каналов спутника для использования на основе динамического распределения по запросу. Каналы SPADE могут активироваться по требованию между разными странами и использоваться на необходимые сроки — короткие или длительные.

Задержка распространения

Приблизительная четвертьсекундная задержка распространения в одну сторону при спутниковой связи влияет как на голосовую телефонию, так и на передачу данных. Пользователи голосовых каналов через спутниковые линии сталкиваются с двумя неприятными особенностями: задержкой речи и эхом. Для снижения эха до приемлемого уровня устанавливаются подавители эха. При передаче данных задержка распространения порождает более серьёзные проблемы. Линейные протоколы и схемы обнаружения/исправления ошибок резко замедляются из-за четвертьсекундной задержки. Выполнение требований к времени отклика пользователя может оказаться затруднительным вследствие накопленного эффекта этих задержек.

Для обеспечения соединения и улучшения работы наземных коммуникационных терминалов, изначально не рассчитанных на задержку распространения в спутниковых системах, существуют блоки компенсации спутниковой задержки. По одному такому блоку требуется на каждой конечной точке. Блоки переформатируют данные в более крупные эффективные блоки передачи, что позволяет реже отправлять запросы на повторную передачу. Это сокращает количество переключений направления на линии, каждое из которых занимает около четверти секунды при передаче данных от терминала или компьютера назначения или к нему. Один из применяемых методов обнаружения и исправления ошибок, называемый GO-BACK-N, требует повторной передачи всех блоков данных, хранящихся в буфере передачи, начиная с того, в котором обнаружена ошибка. Более эффективный метод — повторная передача только блока с ошибкой, однако он требует более сложной логики в оборудовании на каждом конце.

Подключение к земным станциям

Большинство пользователей не могут позволить себе спутниковую земную станцию, поэтому для подключения к ближайшей земной станции требуется наземная линия (которая, как говорят, обеспечивает 65 000 бит/с для арендованной линии). Из-за огромного расстояния, которое сигнал проходит в космосе, относительно небольшое расстояние между двумя пользователями на Земле становится несущественным и фактически не влияет на стоимость эксплуатации. В целом это экономически нецелесообразно. Особенно это справедливо для высокоёмких широкополосных приложений. Несмотря на то что эксплуатационные расходы не зависят от расстояния, спутниковые компании могут по-прежнему взимать более высокую плату за большие расстояния, ориентируясь на конкуренцию с наземными линиями.

Внеатмосферные проблемы

Внеатмосферная часть спутниковой связи позволяет обойти проблемы, связанные с обрывами телефонных линий и т. п., однако у неё есть собственный специфический набор проблем. Поскольку спутниковая связь использует высокочастотную микроволновую радиопередачу, необходимо тщательное планирование во избежание помех между спутником и другими микроволновыми системами. Затмения Солнца, а также Луны, могут создавать трудности, поскольку прерывают подачу энергии для солнечных батарей спутника. Для решения большинства этих проблем используются резервные аккумуляторы, однако наиболее серьёзная проблема возникает, когда Солнце оказывается прямо позади спутника и становится источником недопустимого уровня шума. Это происходит 10 раз в год примерно по 10 минут каждый раз. Для обеспечения бесперебойного обслуживания земная станция должна иметь вторую антенну-тарелку на небольшом расстоянии от первой, либо единственная тарелка должна иметь доступ к другому спутнику.

Доступ к спутнику

Существуют три метода, с помощью которых несколько пользователей (земных станций) могут получать доступ к спутнику. Первый — множественный доступ с частотным разделением (FDMA), при котором общая полоса пропускания делится на отдельные частотные каналы, назначаемые пользователям. Каждый пользователь получает канал, который может простаивать, если у этого пользователя нет трафика. Множественный доступ с временным разделением (TDMA) предоставляет каждому пользователю определённый временной слот или несколько временных слотов. Здесь каналы являются общими, но часть слотов может простаивать, если у пользователя

нет трафика. При множественном доступе с кодовым разделением (CDMA) каждый пользователь может в любое время использовать всю полосу пропускания, применяя уникальный код для идентификации своего трафика. Разумеется, между тремя методами существуют компромиссы; они касаются частоты ошибок, размера блоков, пропускной способности, помехоустойчивости и стоимости.

Преимущества

• Спутниковые линии исключительно хорошо подходят для широкополосных приложений, таких как голосовая связь, телевидение и видеотелефония, а качество передачи остаётся высоким.
• Спутниковые линии, как правило, дешевле для всех видов передачи голоса и данных — будь то коммутируемые или арендованные линии большой протяжённости. Это особенно справедливо для зарубежных передач: нет подводных кабелей, которые могли бы создавать проблемы с обслуживанием.

Недостатки

• Задержка распространения около четверти секунды в одну сторону требует от участников голосового разговора небольшой паузы перед ответом, чтобы убедиться, что собеседник закончил говорить. Для передачи данных задержка распространения оказывает более серьёзное влияние, которое усиливается при высоких скоростях, полудуплексном режиме работы, малых блоках данных и опросе (polling). Блоки компенсации спутниковой задержки, процессоры переднего плана, мультиплексоры и другие устройства были разработаны для обхода этих проблем, однако полностью устранить потерю половины секунды в суммарном времени отклика интерактивных приложений невозможно.
• Некоторые из используемых сегодня модемов не были рассчитаны на длительную задержку при первоначальном установлении соединения через спутник, что может приводить к потере соединения. Это может вызывать раздражение, когда оператор связи выбирает спутниковые линии для обычных коммутируемых вызовов — например, в 55 процентах всех вызовов из определённого города в периоды пиковой нагрузки.

Заключение

Спутниковая связь — очень интересная тема для изучения. Возможно, нынешние и будущие хакеры в области спутников и любительского радио когда-нибудь запустят доску объявлений (Bulletin Board) на базе спутника WESTSTAR — кто знает, может, такая уже существует? *(Хитрая усмешка)*

— Scott Holiday

Организации, обеспечивающие работу телекоммуникационных сетей: Центр управления сетью

Автор: Knight Lightning & Taran King

9 августа 1988 года

Введение в управление сетью — Southwestern Bell Telephone Company

Современные телекоммуникационные сети, опирающиеся на прямой ввод данных от абонентов и на коммутацию с программным управлением (обычным и с хранимой программой), в целом весьма надёжны и позволяют предоставлять недорогие услуги связи всем желающим. Поскольку такие сети рассчитаны исходя из вероятности того, что не все абоненты одновременно нуждаются в обслуживании, они спроектированы и оснащены так, чтобы обеспечивать приемлемый уровень сервиса при нормальной нагрузке трафика. Когда потребности абонентов или сбои оборудования приводят к отклонению от расчётных параметров, либо когда интенсивность вызовов превышает норму, современные сети могут переполняться, и пропускная способность сети снижается.

> *Управление сетью обеспечивает средства для повышения производительности сети в подобных нештатных ситуациях.*

Цели и задачи

Цель Центра управления сетью (NMC) — осуществлять непрерывный мониторинг и контроль, необходимые для поддержания сети на оптимальном уровне производительности. Это охватывает внутризоновые (Intra-Lata) сети Bell Operating Company (BOC), а также межузловые линии и каналы.

Задача NMC — удовлетворять потребности и ожидания абонентов и рынка и одновременно максимизировать доходы от предоставления сетевых услуг.

Хотя NMC не может гарантировать абоненту определённый уровень сервиса, он способен обеспечить наиболее эффективное использование существующих сетевых ресурсов в любых ситуациях. Это выражается в:

• увеличении числа завершённых вызовов;
• более высокой отдаче от капитальных вложений в сеть;
• улучшении качества обслуживания абонентов;
• защите критически важных служб, таких как 911, в нештатных сетевых ситуациях;
• обеспечении равного доступа;
• поддержке национальной безопасности и готовности к чрезвычайным ситуациям.

NMC располагает возможностью изменять или перестраивать коммутационную сеть практически в режиме реального времени. Это достигается посредством управляющих воздействий на коммутационные машины. Управляющие сообщения от NMC обрабатываются коммутационными машинами: они либо расширяют ёмкость сети за счёт задействования простаивающего оборудования и каналов, либо ограничивают сеть, отказывая в доступе трафику с низкой вероятностью завершения вызова, — тем самым освобождая оборудование и каналы для трафика с высокой вероятностью завершения.

Принципы и обязанности в области эксплуатации

При выполнении своих целей и задач NMC руководствуется стандартными принципами, применимыми к коммутационным технологиям и архитектуре сети. Все управляющие воздействия на сеть, как правило, основаны как минимум на одном из этих принципов.

Предотвращение перегрузки коммутатора

Большое число безуспешных попыток соединения в коммутационной машине, вызванное перегрузкой трафика или неисправностью оборудования, может превысить расчётную ёмкость системы. Если не принять мер, перегрузка может распространиться на другие подключённые коммутационные системы. Средства управления сетью позволяют устранять безуспешные попытки соединения с перегруженной машиной, предотвращая перегрузку коммутатора и её распространение на соседние системы.

Использование всех доступных каналов

Коммутационная сеть рассчитана и оснащена с учётом потребностей в телефонных переговорах в типичный рабочий день. Сосредоточенные перегрузки (вызванные штормами, праздниками, наводнениями и гражданскими беспорядками) нередко приводят к резкому росту интенсивности вызовов, на которую сеть не рассчитана. Такая аномалия может также возникать из-за отказов линий и сбоев коммутационных систем. В подобных случаях одни группы каналов оказываются сильно перегружены, тогда как другие практически простаивают. Во многих таких ситуациях можно активировать переадресацию трафика средствами управления сетью, чтобы использовать временно незадействованные ресурсы сети и тем самым завершить вызовы, которые иначе были бы заблокированы.

Поддержание всех каналов занятыми полезными сообщениями

Сообщение — это завершённый вызов. Поскольку сеть, как правило, ограничена ёмкостью каналов, важно оптимизировать соотношение сообщений (приносящих доход) и не-сообщений (не приносящих дохода) в любой группе каналов. Когда в сети возникают необычные или нештатные условия, приводящие к росту числа вызовов с коротким временем удержания (не-сообщения: сигнал «занято», сигнал повторного набора, записанное объявление, «мёртвый» эфир), количество завершённых вызовов снижается, поскольку не-сообщения занимают бóльшую долю системных ресурсов. Средства управления сетью предназначены для сокращения трафика не-сообщений и увеличения числа завершённых вызовов, что повышает удовлетворённость абонентов и увеличивает доходы отрасли.

Приоритет однозвенных соединений

В сетях, рассчитанных на автоматическую альтернативную маршрутизацию вызовов, наиболее эффективное использование доступных каналов достигается при нагрузке трафика на уровне расчётных значений или ниже. При превышении расчётной нагрузки большее число вызовов идёт по альтернативным маршрутам и для завершения вызова требуется более одного канала. В условиях перегрузки использование нескольких каналов для одного вызова случается всё чаще, и вероятность того, что многозвенный вызов заблокирует другие попытки соединения, резко возрастает. Поэтому в ряде случаев необходимо применять средства управления сетью для ограничения альтернативной маршрутизации, чтобы дать трафику первого маршрута разумный шанс завершить больше вызовов, чем было бы завершено в противном случае.

Ответственность Центра управления сетью весьма широка и затрагивает многие рабочие группы и организации как внутри Southwestern Bell Telephone Company, так и в других телефонных компаниях и среди абонентов.

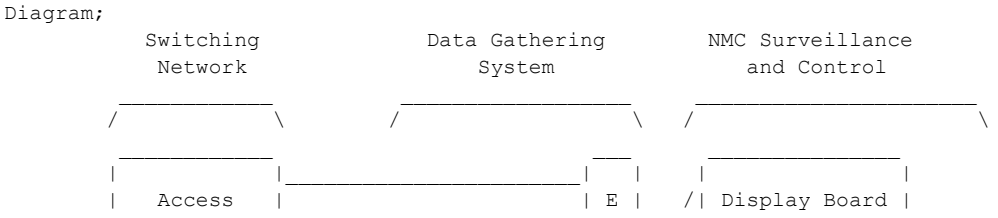
NMC обеспечивает:

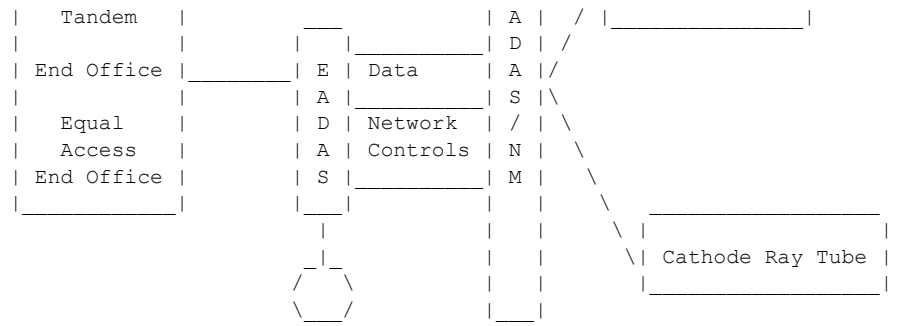
• мониторинг коммутационной сети и управление ею в режиме реального времени;
• выявление нештатных сетевых ситуаций;
• централизованный источник информации для высшего руководства, межузловых операторов (IC), независимых компаний и других BOC;
• координацию вопросов национальной безопасности и готовности к чрезвычайным ситуациям.

Система в целом: схема

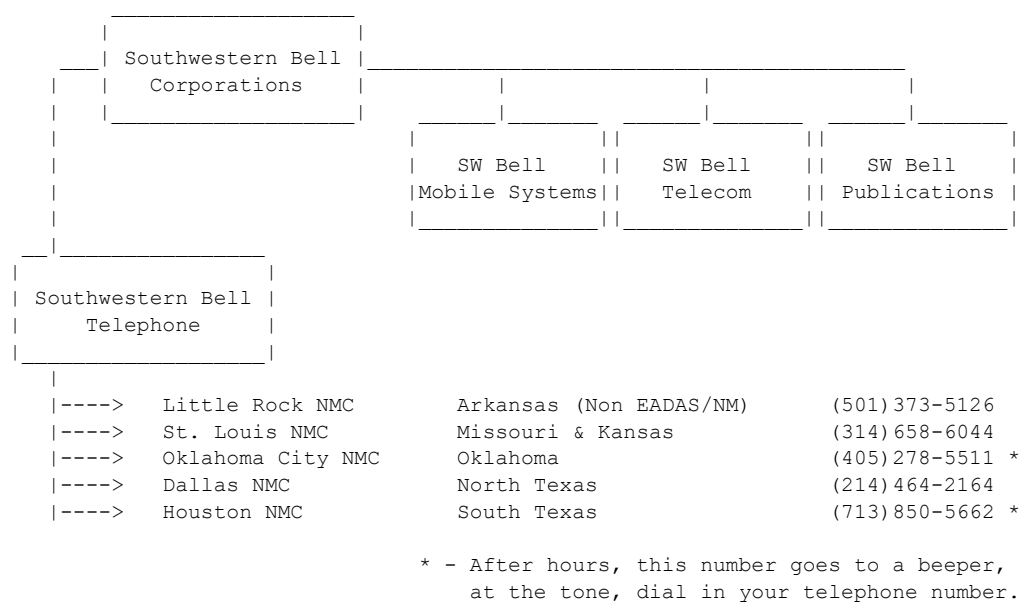
Система управления сетью состоит из трёх основных компонентов: собственно коммутационной сети, системы сбора данных и системы наблюдения и управления (NMC).

NMC управляется действиями абонентов в коммутационной сети, которые регистрируются и отображаются через систему EADAS/NM (Engineering Administration Data Acquisition System for Network Management — система сбора административно-инженерных данных для управления сетью). Управляющие воздействия на сеть направляются с терминала CRT в коммутационную сеть через ту же систему.





Центры управления сетью Southwestern Bell Telephone Company



Little Rock NMC	Arkansas (Non EADAS/NM)	(501)373-5126
St. Louis NMC	Missouri & Kansas	(314)658-6044
Oklahoma City NMC	Oklahoma	(405)278-5511 *
Dallas NMC	North Texas	(214)464-2164
Houston NMC	South Texas	(713)850-5662 *

* - After hours, this number goes to a beeper,
at the tone, dial in your telephone number.

Заключение

Управление сетью — термин, описывающий совокупность действий, направленных на улучшение прохождения сетевого трафика и качества обслуживания абонентов в тех случаях, когда нештатные условия (нетипичные профили трафика или отказы оборудования) могут привести к перегруженной и неэффективной сети. Эти действия включают применение средств управления сетью там и тогда, где и когда это необходимо, а также планирование мер по минимизации последствий сетевых перегрузок.

Управление сетью основано на использовании данных о группах каналов и коммутационных системах, получаемых практически в режиме реального времени, а также на возможности реализовывать необходимые управляющие воздействия посредством системы EADAS/NM.

Управление сетью направлено на завершение максимально возможного числа вызовов внутри внутризоновой (Intra-Lata) сети и на обеспечение равного обращения с трафиком, поступающим ко всем межузловым операторам и от них.

«Будущее вечно»

Неопубликованные номера

Наблюдения за Illinois Bell

Автор: Patrick Townson, The Portal System (TM)

Особая благодарность: Hatchet Molly

Все примеры в этой статье относятся к телефонной компании Illinois Bell Telephone Company, которая обслуживает столичный район Чикаго и значительную часть остального штата Иллинойс.

Существует три типа телефонных номеров, которые не фигурируют в печатном и общедоступном справочнике:

1. Слишком новые, чтобы попасть в список
2. Не включённые в список (Non-listed)
3. Неопубликованные (Non-published)

Третья категория номеров, отсутствующих в телефонной книге и недоступных через Справочную службу, — это неопубликованные номера. Неопубликованные номера **не** выдаются на уровне Справочной службы (DA, Directory Assistance). Запросы о таких номерах, вводимые в терминал DA, просто возвращают сообщение: «По просьбе абонента номер не занесён в наши записи; номер является неопубликованным».

Так кто же всё-таки хранит записи о неопубликованных номерах? В Коммерческом отделе нет удобного способа их получить, поскольку сотрудники опираются на фактический номер телефона при запросе записи для обсуждения лицевого счёта. После того как заявка на обслуживание обработана, номер и связанное с ним имя становятся недоступны рядовому сотруднику в центральном офисе.

На протяжении нескольких лет существовала небольшая группа, известная как «Бюро неопубликованных номеров» (NonPub Number Bureau), располагавшаяся в то время в Хинсдейле, штат Иллинойс. Разумеется, телефонный номер самого этого Бюро тоже был неопубликованным и был доступен лишь определённым сотрудникам Illinois Bell, которым был предоставлен «допуск по принципу необходимости знать». Теперь, когда все записи глубоко компьютеризированы, хранители неопубликованных номеров рассредоточены по разным телефонным офисам.

Процедура доступа к неопубликованному номеру

Когда у сотрудника телефонной компании возникает конкретная необходимость получить неопубликованный номер абонента, вступают в силу определённые меры безопасности. Прежде всего, лишь ничтожно малый процент сотрудников телефонной компании вообще имеет «допуск по принципу необходимости знать»; в их числе — старшие операторы-руководители (GCO, Group Chief Operators), отдельные руководящие сотрудники центральных офисов, некоторые сотрудники отдела казначейства/бухгалтерии, а также, разумеется, представители службы безопасности как Illinois Bell, так и различных операторов дальней связи — AT&T, US Sprint и MCI.

Гипотетический пример

Рассмотрим гипотетическую ситуацию. Ваша мать тяжело заболела и находится при смерти. Ваш брат не может до вас дозвониться и сообщить об этом, потому что у вас неопубликованный номер. Получив отказ в Справочной службе — просто потому, что там этого номера нет, — он просит позвать супервизора и объясняет ситуацию. Он сообщает своё имя и номер телефона, и супервизор говорит, что перезвонит позднее. Супервизор не уточняет, действительно ли имеет место чрезвычайная ситуация — а ведь только это является единственным законным основанием для нарушения режима безопасности. Супервизор может, если он добросовестно выполняет свою работу, прямо спросить у звонящего: «Вы заявляете, что это чрезвычайная ситуация?»

Имейте в виду: закон в штате Иллинойс и во многих других штатах гласит, что если человек утверждает о существовании чрезвычайной ситуации с целью повлиять на использование (или прекращение использования) телефона, тогда как на самом деле никакой чрезвычайной ситуации нет, он совершает уголовный проступок (misdemeanor). Вы отвечаете: «Да, это чрезвычайная ситуация, и мне нужно срочно связаться с братом/сестрой/и т. д.» Супервизор затем переговорит со своим руководителем, который обычно занимает должность главного оператора (Chief Operator) данного объекта.

Главный оператор позвонит в службу неопубликованных номеров, представится и **оставит свой обратный номер**. Сотрудники этой службы перезвонят, чтобы удостовериться в источнике звонка, и лишь после этого предоставят информацию о телефонном номере вашего брата. Это проще, если вы знаете **точное** написание имени в записях и **точный** адрес; если окажется, что неопубликованный номер есть у нескольких человек с одинаковой фамилией, вам могут ответить, что не в состоянии определить, кого именно вы ищете.

Затем сотрудник службы неопубликованных номеров позвонит абоненту с неопубликованным номером и объяснит, что произошло: «Такой-то обратился к одному из наших операторов с просьбой помочь выйти с вами на связь. Звонящий утверждает, что речь идёт о семейной чрезвычайной ситуации, требующей вашего немедленного внимания. Можем ли мы сообщить ему/ей ваш номер, или вы предпочтёте сами ему/ей перезвонить?»

В зависимости от ответа номер либо передаётся главному оператору, либо сообщается, что абонент с неопубликованным номером уведомлён. Если абонент соглашается передать номер, главный оператор перезвонит вам, спросит, кто **вы** такой — а не назовёт того, с кем хочет поговорить, — и, удостоверившись в вашей личности, сообщит искомый номер либо сообщит, что ваш брат получил сообщение от сотрудника офиса и сказал, что свяжется с вами.

Меры защиты от несанкционированного доступа

Прежде чем сотрудники службы неопубликованных номеров вообще станут с вами разговаривать, ваш «обратный номер» должен быть в их списке авторизованных номеров для данных целей. Клерк Коммерческого отдела не может, например, выдать себя за главного оператора — просто потому, что служба неопубликованных номеров скажет: «Номер, на который вы просите нас перезвонить, отсутствует в нашем списке. Сообщите своему руководителю, что именно вы ищете, и пусть он нам позвонит…»

Другие экстренные запросы неопубликованных номеров могут быть связаны с крупным пожаром в каком-либо предприятии среди ночи, когда необходимо оповестить владельцев компании по месту жительства, или с ситуацией, когда полиция обнаружила заблудившегося ребёнка, который слишком мал, чтобы знать неопубликованный номер родителей.

Служба рассматривает и неэкстренные запросы, но только при условии их определённой значимости и при отсутствии признаков легкомысленности. Например: вы только что приехали в город и разыскиваете давнего друга, у которого неопубликованный номер; или вы составляете список приглашений на пятидесятилетний юбилей вашего школьного выпуска и обнаруживаете, что номер одного из одноклассников неопубликован. В разумных пределах служба передаёт ваш запрос нужному лицу и предоставляет ему самому решить, перезванивать или нет. Но при этом вы всегда оставляете свой номер, и в своё время кто-нибудь перезвонит и сообщит, что было сказано или сделано.

Вы бы удивились — а может, и нет — тому количеству уловок и историй, которые люди рассказывают телефонной компании, чтобы получить неопубликованные номера чужих абонентов. К счастью, Bell придаёт большое значение своим усилиям по защите конфиденциальности подписчиков.

— РТ

Блокировка междугородных звонков

Автор: Jim Schmickley

Краткое содержание

В этом файле описывается «блокировка», которую одна междугородная телефонная компания применяет к доступу через свою сеть к определённым номерам — в особенности к номерам BBS. Блокировка осуществляется крайне произвольно, а компания с высокомерием заявляет, что операторы BBS и все, кто пользуется компьютерным модемом, являются «хакерами».

Компания на самом деле не хочет обсуждать сложившуюся ситуацию, однако, судя по всему, произошло следующее. Некие «лица или лицо», личность которых так и не была установлена, получили один или несколько «действующих» номеров счетов для международных звонков и впоследствии воспользовались ими один или несколько раз для мошеннических звонков на законную компьютерную доску объявлений (BBS). Когда компания обнаружила мошеннические списания, она «заблокировала» линию, не потрудившись провести расследование или связаться с оператором BBS за помощью. Более того — компания не удосужилась даже установить имя системного оператора.

Долгодистанционный перевозчик хотел бы представить инцидент, послуживший поводом для описанных в этой статье действий, как единичный случай, не связанный ни с чем другим. Однако с этим вопросом глубоко переплетены важнейшие принципы свободного и ничем не ограниченного общения и индивидуальных прав. И остаётся навязчивый вопрос: «Если одна компания дальней связи вмешивается в переговоры своих клиентов почти что по прихоти, не вмешиваются ли и другие такие компании в право американцев на свободу "электронного слова"?»

Призыв к действию

Ваши отклики и протесты необходимы прямо сейчас, чтобы опровергнуть утверждение компании о том, что «никто не пострадал от их действий по блокировке, потому что никто не жаловался». Разумеется, долгое время никто не жаловался, потому что блокировка линии была произведена так, что вплоть до апреля 1988 года никто не понял, что вообще происходит.

Пожалуйста, прочитайте эту статью и составьте собственное мнение. Затем напишите в организации, указанные в конце статьи; настаивайте на том, что ваше право звонить на любой номер по вашему выбору не должно ущемляться произвольным решением какого-то бюрократа в телефонной компании, которому до прав его клиентов нет никакого дела. Протестуйте в самых жёстких выражениях. И помните: права, которые вы отстоите, БУДУТ ВАШИМИ СОБСТВЕННЫМИ!

Место действия

Teleconnect — компания дальней связи и телефонного директ-маркетинга со штаб-квартирой в Сидар-Рапидс, Айова. Компании около восьми лет; её абонентская база в сегменте дальней связи

насчитывает примерно 200 000 клиентов. Teleconnect только что завершила первичное публичное размещение акций и в настоящее время (август 1988 года) участвует в слиянии, которое сделает её четвёртым по величине в стране оператором дальней связи. Это очень быстро растущая компания: свой впечатляющий рост она достигла за счёт предложения услуг дальней связи по тарифам, которые, по её собственным заявлениям, на 15–30% ниже тарифов AT&T.

Когда Teleconnect начинала работу в сфере телефонной коммутации, лишь немногие АТС были оборудованы для «равного доступа», поэтому компания создала сеть местных номеров доступа (по сути — просто нелистинговые местные УПАТС — частные автоматические телефонные станции) и присвоила каждому клиенту шестизначный номер счёта. Позднее ко всем номерам счетов была добавлена седьмая «защитная» цифра. Сейчас Teleconnect предлагает прямой набор с «равным доступом» на большинстве АТС, однако прежняя система номеров доступа и кодов счетов по-прежнему действует для тех АТС, которые «равного доступа» ещё не получили. Эта система по-прежнему очень удобна для клиентов, которые звонят из офиса или других мест, отличных от дома.

Обнаружение «блокировки»

В начале апреля 1988 года один знакомый упомянул, что Teleconnect «блокирует» определённые телефонные линии, на которых обнаруживает компьютерный тон. В частности, он не мог дозвониться до BBS «Stock Exchange» Курта Кила в Уотерлу, Айова. Это звучало как что-то, во что мне определённо стоит разобраться, и я попробовал позвонить на BBS Курта.

Контакт с Teleconnect

Teleconnect не пропустила мой звонок. Вместо этого я услышал записанное голосовое сообщение о том, что это — местный звонок из моего места нахождения. При второй попытке — то же самое. По крайней мере, они были последовательны.

Я позвонил своему представителю Teleconnect и спросил, в чём проблема. Выслушав объяснение, она предположила, что это, должно быть, местный звонок. Я объяснил, что звонок на расстояние в 70 миль из Сидар-Рапидс до Уотерлу вряд ли можно считать местным. Она разобралась в ситуации и сообщила мне, что линия «заблокирована». Я спросил почему, и она «предположила, что по просьбе абонента». После того как я объяснил, что это утверждение не имеет смысла, она признала, что на самом деле не знает. Итак — к её начальнику.

Руководитель первого уровня подтвердил, что линия «заблокирована службой безопасности Teleconnect», однако не могла или не хотела объяснить почему. Затем она бросила вызов: «А зачем вам звонить на этот номер?» Это был неверный вопрос раздражённому клиенту, и дама быстро обнаружила, что подобная информация не является её делом. Далее — к её начальнику...

Руководитель второго уровня отказалась раскрывать рядовому клиенту какую-либо ценную информацию, однако предложила, что до любого заблокированного Teleconnect номера можно дозвониться через AT&T или Northwestern Bell, набрав 10288-1. На вопрос о том, почему Teleconnect — компания, долгие годы продвигавшая свои услуги дальней связи как более дешёвую альтернативу AT&T — теперь рекомендует клиентам пользоваться AT&T, у дамы ответа не нашлось.

Затем меня известили, что за дополнительной информацией следует обращаться к Дэну Роджерсу, вице-президенту Teleconnect по работе с клиентами. Это звучало обнадёживающе: «Соедините меня с ним, пожалуйста». И тут: «Мне жаль, но господин Роджерс сейчас в командировке и вернётся только на следующей неделе». «На следующей неделе?» — «Но он регулярно звонит в офис. Возможно, он сможет перезвонить вам раньше». Господин Роджерс действительно перезвонил мне в тот же день из Вашингтона, округ Колумбия, где он вместе с «людьми из службы безопасности» Teleconnect участвовал в конференции по телефонной безопасности.

Teleconnect отвечает — но не вполне

Дэн Роджерс начал разговор так: «Я просто пресс-секретарь; я не разбираюсь во всех технических деталях. Наша служба безопасности блокирует этот номер, потому что в прошлом с ним были проблемы». Я возразил, что обвинение в «проблемах» не имеет смысла, поскольку номер принадлежит компьютерной доске объявлений, которую ведёт уважаемый предприниматель — Курт Кил.

Господин Роджерс сказал, что я только что сообщил Teleconnect новую информацию: они не могли установить, чей номер блокируют. «Наши люди — профессионалы, но не настолько. Northwestern Bell не предоставляет нам информацию об абонентах». И когда в следующий понедельник он вернётся в офис, то попросит людей из службы безопасности проверить, можно ли снять блокировку.

В следующий понедельник из Teleconnect позвонила другая женщина и сообщила, что они проверили линию и снимают с неё блокировку. Она добавила, что за четыре года это был первый случай, когда кто-то попросил разблокировать линию. Я предположил, что, скорее всего, не последний.

В последующем телефонном разговоре Дэн Роджерс подтвердил, что блокировка с линии Курта Кила снята, но предупредил, что линия будет заблокирована снова «при возникновении любых новых проблем». Затем последовало краткое, ни к чему не приведшее обсуждение права Teleconnect на подобные действия. Я добавил, что то обстоятельство, что «служба безопасности» Teleconnect не смогла установить личность оператора заблокированной доски, просто не укладывается в голове — похоже, «люди из службы безопасности» не слишком компетентны. Тут господин Роджерс признал, что каждый раз, когда сотрудники службы безопасности пытались позвонить на этот номер, им отвечал сигнал «занято» (и, хотя господин Роджерс этого не признал, они просто «махнули рукой» и произвольно заблокировали линию). Ах да, голосовое сообщение «Это местный звонок...» было, по словам Дэна Роджерса, вовсе не призвано кого-либо обманывать. Просто в оборудовании Teleconnect было лишь ограниченное число записей, и именно эту они выбрали для заблокированных линий.

Начало бумажной переписки

Было очевидно, что Teleconnect не намерена уделять серьёзного внимания телефонным звонкам рядовых клиентов. 22 апреля Бен Блэксток, практикующий адвокат и бывалый системный оператор, написал господину Роджерсу письмо с призывом разрешить клиентам Teleconnect звонить на любые номера по их выбору. Бен поставил под сомнение право Teleconnect блокировать звонки и предположил, что подобные действия несут в себе явные черты «большого брата». Он также указал, что «нельзя наказывать невиновных, добираясь до того, кто, по-видимому, создаёт

Teleconnect трудности».

Кейси Д. Мэйон, старший вице-президент и главный юрисконсульт Teleconnect, ответила на письмо Бена Блэкстока 28 апреля. Этот ответ стал началом, казалось бы, нескончаемого потока расплывчатых общих обвинений со стороны Teleconnect в адрес «хакеров» и «компьютерных досок объявлений». Teleconnect настаивала на наличии у неё полномочий блокировать доступ к телефонным линиям и сослалась на 18 USC 2511(2)(a)(i) как на пример подобных полномочий. Позиция Teleconnect была изложена в письме следующим образом:

> *«Наконец, просим принять к сведению, что компания готова "разблокировать" линию, чтобы убедиться в том, прекратился ли незаконный взлом. Однако в случае возобновления кражи услуг дальней связи Teleconnect посредством данной доски объявлений мы, разумеется, снова заблокируем доступ через сеть Teleconnect и воспользуемся предоставленными нам федеральным законом полномочиями для установления личности хакера или хакеров».*

Перчатка подобрана

Господин Блэксток проверил указанный раздел Кодекса США и обнаружил, что он относится исключительно к «перехвату» переговоров, но не имеет никакого отношения к «блокировке». Он высказал мне своё мнение, а также написал ответное письмо Кейси Мэйон, оспаривая её толкование данного раздела федерального закона.

В своём письме Бен отметил: «Либо Teleconnect предоставляет услуги связи без дискриминации, либо нет». Он добавил, что «мягко говоря, расстроится», если обнаружит, что Teleconnect блокирует доступ к его BBS. Господин Блэксток завершил письмо предложением о сотрудничестве с Teleconnect в получении декларативного судебного решения относительно её «права» блокировать телефонный номер из-за действий третьего лица. По сей день Teleconnect никак не отреагировала на это предложение.

13 мая я отправил собственный ответ Кейси Мэйон, опровергнув все аргументы её письма по существу. Я отметил, что даже я, не будучи юристом, знаю разницу между «перехватом» и «блокировкой», а если Teleconnect не знает, она может проконсультироваться у любого футбольного болельщика. Мое письмо заканчивалось следующим образом:

> *«Поскольку политика "блокировки", проводимая Teleconnect, является непродуманной, безрассудно произвольной, антипотребительской и сомнительной с точки зрения законности, её необходимо немедленно исправить. Прошу сообщить мне, каким образом Teleconnect пересматривает данную политику, чтобы гарантировать мне и всем остальным законным абонентам беспрепятственный доступ к любым номерам дальней связи по нашему выбору».*

3 июня Кейси Мэйон ответила. Неудивительно — она отмахнулась от всех моих доводов. Кроме того, она выдвинула первое из масштабных обобщений с полным уклонением от конкретики, что впоследствии мы стали воспринимать как фирменный стиль Teleconnect. Один абзац хорошо суммирует письмо Кейси Мэйон:

> *«При всём уважении к времени и мысли, очевидно вложенным в ваше письмо, я не разделяю вашего вывода о том, что усилия Teleconnect по пресечению кражи её услуг каким-либо образом неуместны. На протяжении всей истории индустрия операторов межрегиональной связи страдала от действий лиц, проявляющих незаурядную изобретательность в краже услуг дальней связи. Случаи, когда оператор*

межрегиональной связи теряет до 500 000 долларов в месяц вследствие краж, не являются редкостью. Как вы понимаете, подобные потери в течение определённого периода времени могут привести компанию к банкротству».

Эскалация

К этому моменту было совершенно очевидно, что Teleconnect будет упорствовать до тех пор, пока какая-либо третья сторона — предпочтительно регулирующий орган — не убедит компанию в ошибочности её пути. Соответственно, я собрал документы и добавил жалобу, адресованную Комиссии по коммунальному хозяйству Айовы. В жалобе просто указывалось, что Teleconnect следует обязать ввести надлежащие защитные меры, чтобы «невинные третьи лица» более не страдали от произвольной политики «блокировки» Teleconnect.

Моя жалоба была датирована 7 июля 1988 года, а Комиссия по коммунальному хозяйству Айовы ответила 13 июля 1988 года. В ответе говорилось, что Teleconnect обязана ответить на мою жалобу до 2 августа 1988 года, после чего Комиссия предложит вариант урегулирования. Если предложенное урегулирование окажется неудовлетворительным, я смогу запросить повторное рассмотрение жалобы. Если и этот результат окажется неудовлетворительным, можно будет потребовать проведения официального слушания.

После подачи жалобы я также направил копию документов конгрессмену Тому Тауке. Господин Тауке представляет Второй избирательный округ Айовы, включающий Сидар-Рапидс, а также является членом Подкомитета Палаты представителей по телекоммуникациям. Впоследствии у меня состоялась личная беседа с господином Тауке, а также дополнительная переписка по данному вопросу. Похоже, у него есть глубокий и искренний интерес к проблеме, однако по моей просьбе он пока остаётся лишь заинтересованным наблюдателем. Мы надеемся, что Комиссия по коммунальному хозяйству Айовы предложит приемлемое урегулирование без привлечения дополнительной помощи.

Ответ без ответа

«Ответ» Teleconnect в Комиссию по коммунальному хозяйству Айовы был подан 29 июля 1988 года. Как и ожидалось, он представлял собой нагромождение расплывчатых обобщений и бездоказательных утверждений. Тем не менее в нём содержался один новый и шокирующий факт: BBS Курта Кила была заблокирована на десять месяцев — с 6 июня 1987 по середину апреля 1988 года. (Здесь следует отметить, что клиенты Teleconnect понятия не имели, что компания блокирует часть их звонков. Мы просто думали, что звонки не проходят из-за технических проблем у Teleconnect).

Teleconnect уклонялась от включения в своё письмо какой-либо конкретной или хотя бы уместной информации. Однако компания предложила шепнуть кое-что на ухо сотрудникам Комиссии: «Teleconnect готова поделиться подробной информацией по данному конкретному делу и по теме взлома в целом с сотрудниками Комиссии — так же, как ранее делала это с различными федеральными и местными правоохранительными органами, включая Секретную службу США. Teleconnect, однако, с уважением просит Комиссию согласиться сохранить такую информацию в конфиденциальности, поскольку иное повлечёт публичное раскрытие сведений о ведущихся расследованиях уголовных преступлений и о методах, с помощью которых операторы межрегиональной связи, включая Teleconnect, выявляют подобные кражи».

Никто, по всей видимости, не поставил вопрос о том, не нарушит ли подобная «конфиденциальная» встреча Закон Айовы об открытых заседаниях. Никто, по всей видимости, не задался вопросом, почему за десять месяцев «текущего расследования» Teleconnect так и не смогла установить имя лица, чью линию она блокировала. Разумеется, всё, что они делали, было оправдано, ведь, по их собственным словам, «Teleconnect понесла значительные финансовые потери в результате кражи услуг дальней связи посредством компьютерного взлома с использованием компьютерной доски объявлений, доступной по данному номеру».

Самым гнусным утверждением Teleconnect было: «Нередко хакер вводит похищенный авторизационный код на компьютерных досках объявлений, позволяя другим красть услуги дальней связи с помощью этого кода». Но никакого вреда от блокировки номера BBS причинено не было, ведь «за десять месяцев, в течение которых номер был заблокирован, Teleconnect не получала жалоб ни от кого, кто заявил бы о своём праве на данный номер». То обстоятельство, что у Курта Кила не было никакой возможности узнать о блокировке его линии, возможно, и объясняет, почему он не жаловался.

Было также указано, что у меня вообще нет права на жалобу, поскольку «прежде всего и главным образом, господин Шмикли не является абонентом данного номера». Это верно — я просто давний клиент Teleconnect, которому было отказано в обслуживании из-за предполагаемых действий неизвестного третьего лица.

Затем Teleconnect обрушила на сотрудников Комиссии копию семистраничной статьи из журнала Business Week под заголовком «Насколько защищён ваш компьютер?». Эта статья не имела никакого отношения к краже услуг дальней связи, за исключением отрывка из врезки о западногерманском клубе хакеров. В статье сообщалось, что «в 1984 году Chaos обнаружил дыру в безопасности системы видеотекс, которую строил немецкий телефонный регулятор Deutsche Bundespost. Когда ведомство проигнорировало предупреждения клуба о том, что сообщения в частных электронных почтовых ящиках клиентов не защищены, члены Chaos решили доказать свою правоту. Они вошли в компьютеры Hamburger Sparkasse, сберегательного банка, и запрограммировали их на тысячи звонков через видеотекс на штаб-квартиру Chaos на одни выходные. Уже через два дня банк задолжал Bundespost 75 000 долларов за телефонные переговоры».

Решение со штампом в руках

Сотрудники Комиссии по коммунальному хозяйству Айовы ответили на мою жалобу письмом 19 августа 1988 года. Они, по всей видимости, приняли расплывчатые инсинуации Teleconnect без какой-либо проверки: «Принимая во внимание незаконные действия, которые, по имеющимся сведениям, осуществлялись с номера (319) 236-0834, блокировка представляется обоснованной. Вместе с тем мы полагаем, что Комиссия должна получать уведомление вскоре после введения блокировки, а также разрешение на её продление на любой срок».

Тем не менее было также отмечено: «Кодекс штата Айова, раздел 476.20(1) (1987), гласит: "Коммунальное предприятие не должно, за исключением чрезвычайных случаев, прекращать, сокращать или ухудшать обслуживание какой-либо территории или её части, за исключением случаев неоплаты счёта или нарушения правил и положений, без предварительного получения разрешения Комиссии"». В письме далее уточнялось: «Хотя Кодекс Айовы допускает толкование, сотрудникам представляется, что "чрезвычайность" относится к сравнительно короткому сроку...».

Оценка доказательств

Поскольку было очевидно, что сотрудники Комиссии не поставили под сомнение и не проверили ни одно из утверждений Teleconnect, их ответ был совершенно ошеломляющим. Соответственно, 22 августа я подал ходатайство о пересмотре.

В ходатайстве о пересмотре было поднято три вопроса:

1. Оценка сотрудников должна была быть сосредоточена на отказе в обслуживании мне и бесчисленному множеству других клиентов Teleconnect из числа её 200 000 абонентов, а не только на блокировке входящих звонков на одну BBS.

2. Сотрудники приняли все утверждения Teleconnect как факт, хотя в их подтверждение не было представлено ни единого доказательства.

3. По словам самой цитаты сотрудников, похоже, что Teleconnect непрерывно нарушала Кодекс штата Айова, раздел 476.20(1) (1987) на протяжении десяти месяцев, а возможно, и четырёх лет.

Поскольку Teleconnect взвалила на сотрудников семистраничную нерелевантную журнальную статью, представлялось справедливым предложить им теперь двухстраничный совершенно уместный материал. Это была статья «О вашем компьютере — доски объявлений» из июньского номера журнала «Changing Times» за 1988 год. В этой прекрасной статье девять BBS были названы «хорошим местом для начала». В числе девяти перечисленных BBS был «Stock Exchange» Курта Кила, Уотерлу, Айова (319-236-0834). Даже гениям из Teleconnect должно быть под силу понять, что эта BBS, рекомендованная национальным журналом, — именно та, которую они блокировали на протяжении десяти месяцев.

А тем временем...

Вы теперь в курсе всей истории целиком. Сейчас мы распространяем информацию, чтобы все заинтересованные люди могли связаться с властями Айовы — и те поняли, что данное дело гораздо шире, чем блокировка одной BBS. ВЫ можете помочь.

Прочитайте приведённое ниже уведомление и ДЕЙСТВУЙТЕ. Если вы являетесь клиентом Teleconnect, крайне важно, чтобы вы написали в указанные в уведомлении инстанции. Если вы не являетесь клиентом Teleconnect, но заинтересованы в сохранении своего права на свободное общение, вы также можете помочь делу, написав в эти инстанции. Пожалуйста, пишите прямо сейчас! Пока не стало слишком поздно!

- -

T E L E C O N N E C T C U S T O M E R S
= =

Клиентам Teleconnect

Если вы пользуетесь услугами дальней связи Teleconnect, вам необходимо знать об их политике «блокировки»:

Teleconnect «набрасывается» на звонящих на доски объявлений и другие «компьютерные номера», блокируя доступ законных абонентов к определённым телефонным номерам, на которые поступали

звонки с мошеннически использованными кодами Teleconnect. Именно так была «заблокирована» BBS «Stock Exchange» Курта Кила в Уотерлу. Представители Teleconnect дали понять, что и другие «компьютерные номера» в прошлом подвергались аналогичным мерам, и компания «вправе» продолжать подобные действия в будущем.

Помимо попрания индивидуальных прав, гарантированных Биллем о правах Конституции США, это произвольное действие лишь «наказывает невиновных» — клиентов Teleconnect и операторов досок объявлений, — совершенно ничего не делая для того, чтобы установить, наказать или получить возмещение от виновных. Венцом абсурда является то, что Teleconnect, рекламирующая значительную экономию по сравнению с тарифами AT&T на дальнюю связь, теперь предлагает жалующимся клиентам дозваниваться на заблокированный номер через AT&T.

Пожалуйста, напишите в Teleconnect. Объясните, как долго вы являетесь клиентом, что ваш модем генерирует значительную часть дохода, который они с вас получают, и что вы категорически возражаете против того, чтобы компания произвольно решала, на какие номера вам можно или нельзя звонить. Поставьте под сомнение их «право» вводить политику «блокировки» и настаивайте на её изменении. Направляйте протесты по адресу:

```
Teleconnect Company
Mr. Dan Rogers, Vice President for Customer Service
500 Second Avenue, S.E.
Cedar Rapids, Iowa  52401
```

Жалоба, поданная в Комиссию по коммунальному хозяйству Айовы, была первоначально рассмотрена в пользу Teleconnect. Ходатайство о пересмотре подано, и СЕЙЧАС настало время для ВАС написать письма властям штата Айова. Пожалуйста, пишите СЕЙЧАС:

```
Mr. Gerald W. Winter, Supervisor, Consumer Services
Iowa State Utilities Board
Lucas State Office Building
Des Moines, Iowa  50319
```

И также:

```
Mr. James Maret
Office of the Consumer Advocate
Lucas State Office Building
Des Moines, Iowa  50319
```

Пишите сейчас. Права, которые вы отстоите, БУДУТ ВАШИМИ СОБСТВЕННЫМИ.

После подачи ходатайства о пересмотре моей жалобы я получил ответ от Комиссии по коммунальному хозяйству штата Айова, в котором, в частности, говорилось:

> *«Благодарим вас за письмо от 22 августа 1988 года с дополнительными комментариями относительно вашей жалобы на блокировку доступа к определённым телефонным номерам со стороны Teleconnect.*
> *В целях надлежащего изучения вопросов, поднятых в жалобе, мы направляем ваши комментарии в компанию и запрашиваем ответ до 15 сентября 1988 года».*

Ещё раз подчеркну: это очень важный вопрос. Если говорить просто: имеет ли ЛЮБАЯ телефонная компания право «блокировать» (то есть отказывать в соединении) ЛЮБОЙ номер на основании бездоказательных, непроверенных обвинений в «телефонном мошенничестве» — особенно когда предполагаемое мошенничество совершено третьей стороной без ведома вызываемой стороны? Применительно к данному конкретному случаю вопрос звучит так: может ли оператор дальней связи отказаться обслуживать звонки на BBS исключительно потому, что некий неизвестный мошенник совершал мошеннически оплаченные звонки на эту BBS? Кстати, когда будете писать, пожалуйста, указывайте номер дела C-88-161.

Если у вас есть какая-либо дополнительная информация, которая может оказаться полезной в этой борьбе, пожалуйста, сообщите мне.

Вы можете написать мне по почте США:

```
Jim Schmickley
7441 Commune Court, N.E.
Cedar Rapids, Iowa  52402
```

(См. «On The Edge Of Forever» в PWN XXI/1 — обновление по данному вопросу. — KL)

Шоу Эда Шварца на радио WGN 720 AM

```
PWN PWN PWN PWN PWN PWN PWN Special Edition PWN PWN PWN PWN PWN PWN
PWN                                                             PWN
PWN                      Phrack World News                      PWN
PWN                  Special Edition Issue Two                  PWN
PWN                                                             PWN
PWN               Created, Written, and Edited                  PWN
PWN                    by Knight Lightning                      PWN
PWN                                                             PWN
PWN              Special Thanks To Hatchet Molly                PWN
PWN                                                             PWN
PWN PWN PWN PWN PWN PWN PWN Special Edition PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

27–28 сентября 1988 года

Расшифровка: Hatchet Molly

Приветствуем вас. В этом специальном выпуске Phrack World News представлены сокращённые стенограммы шоу Эда Шварца — ночного ток-шоу, которое выходит в эфир на радиостанции WGN 720 AM в Чикаго, штат Иллинойс.

Стенограммы, опубликованные здесь в Phrack, были отредактированы для настоящей публикации. В основном я решил опустить посторонние разговоры, а также любые комментарии и обсуждения, не относящиеся к тематике Phrack World News. Помимо этого, я несколько отредактировал речь, чтобы сделать её более удобочитаемой — задача, прямо скажем, непростая. Тем не менее полную неотредактированную версию этой передачи можно найти на The Phoenix Project (512)441-3088, сисоп — The Mentor.

:Knight Lightning

Действующие лица

```
A  = Anna (самопровозглашённый телефонный фрикер из Канзас-Сити, штат Миссури)
AA = Sergeant Abagail Abraham (Полиция штата Иллинойс; отдел компьютерных преступлений)
B  = Bob (оператор доски объявлений BBS)
BG = Bob Gates (менеджер по корпоративной безопасности Ameritech)
CM = Chuck Moran (директор по внутренним делам; Ameritech Applied Technologies)
D  = Dan (студент компьютерного факультета Технического института DeVry в Чикаго, IL)
ES = Edward Schwartz (ведущий)
EZ = Ed Zahdi (исследователь из THE READER, местного издания в Чикаго)
G  = Gordon (Hatchet Molly, аспирант Северного университета Иллинойса)
JM = John F. Maxfield (наш знаменитый друг из BoardScan в Детройте, штат Мичиган)
K  = Kevin (сисоп BBS)
L  = Louis (слушатель)
P  = Penny (пострадавший)
R  = Robert (законопослушный хакер)
R  = Ray (бывший пират программного обеспечения)
S  = ?? (инженер-консультант)
```

Также упоминаются, но не участвуют в шоу: SHADOW HAWK из Чикаго, штат Иллинойс, недавно арестованный за хищение программного обеспечения у AT&T, и TOM TCIMPIDIS, известный сисоп, арестованный за то, что на его легальной доске объявлений без его ведома оказались номера карточек AT&T.

Стенограмма

ES: Двенадцать минут после начала часа. Час, разумеется, одиннадцатый. По ночам и ранним утром происходит огромное количество деловых операций. Говоря о деловых операциях, я имею в виду компьютерные операции всех видов — от перфоратора до табулятора, всё что угодно.

Мы уже сделали два выпуска с Эдом Захди, исследователем из THE READER (еженедельной газеты), из колонки «straight dope». Эд Захди занимается исследованиями, и в двух его появлениях (два пятничных вечера) за последний год или около того он получил множество телефонных звонков — о компьютерном хакерстве, о людях, у которых телефоны таинственно звонят среди ночи — или практически в любое время суток, но постоянно, — и когда они берут трубку, на линии никого нет.

Когда Эд Захди был у нас в последний раз, нас завалили звонки от людей, которые утверждали:

• что существуют всевозможные телемаркетинговые организации, обзванивающие телефоны;
• что телефонная компания тестирует телефоны без ведома абонента;
• что телефонная сеть проверяется каждый день и телефон у всех звонит один раз или на полуударе, и никого никогда нет.

Меня поразило количество и характер поступивших звонков. Мы позвонили в телефонную компанию и попросили содействия, и сегодня вечером у нас в гостях не только г-н Эд Захди из THE READER, но и г-н Чак Моран, директор по внутренним делам Ameritech Applied Technologies. Также у нас г-н Боб Гейтс, менеджер по корпоративной безопасности Ameritech.

Мы разберёмся во всём этом: злоупотребляют ли люди телефонными сетями или нет, прощупывают ли компьютерные хакеры телефонные номера с помощью компьютеров, можно ли в самом деле запрограммировать компьютер так, чтобы он случайным образом звонил на каждый телефон в городе.

Если вы занимаетесь компьютерами — оставайтесь с нами. Мы также поговорим о некоторых мерах, которые телефонная компания и другие смежные предприятия принимают, чтобы не отставать от компьютерных хакеров.

JC: Звучит интересно.

ES: Вы готовы к этому? Бюро уголовных расследований полиции штата Иллинойс располагает подразделением по компьютерному мошенничеству.

JC: Угу.

ES: И знаете, чем они любят заниматься?

JC: Чем?

ES: Сажать компьютерных хакеров за решётку. Сегодня ночью хакеры у нас разбегутся кто куда! Хотя, пожалуй, правильнее сказать «набирать со скоростью ветра», а?

JC: Наверное! (смеётся)

ES: Потому что они не бегают — большинство из них просиживают штаны на диване.

JC: Совершенно верно!

ES: Рад видеть вас здесь, Эд.

EZ: Рад быть здесь, Эд. В рубрике «straight dope» мы занимаемся самыми разными вопросами. Один из них — вопрос о «звонках-призраках». Люди слышали их преимущественно ночью.

ES: На домашнем телефоне?

EZ: На домашнем телефоне. Человек сидит дома, телефон звонит — полным звонком, или целым звонком, а то и двумя. Берёт трубку — никого. Я слышал об этом раньше. Думал, это какая-то причуда телефона, купленного в K-Mart или ещё где-нибудь.

За вечер мы получили легко дюжину звонков от людей с одинаковым опытом. И это всегда, как ни странно, происходило в одно и то же время ночи, или в один и тот же день недели в одно и то же время ночи, и это было довольно жутковато.

Нам позвонила одна женщина, с которой я с тех пор неоднократно разговаривал. Она работала оператором телефонного центра и у неё были целые ряды телефонов. Группы телефонов звенели один раз в определённое время ночи, на следующий день в определённое время ночи звенела другая группа, а на следующей неделе или в следующий раз когда бы то ни было — закономерность повторялась, но никого на линии не было. Мы решили, что этому должно быть очевидное объяснение. Тогдашние предположения сводились к тому, что это какая-то программа тестирования телефонной компании для проверки магистральных линий или чего-то в этом роде.

Я позвонил в телефонную компанию — Illinois Bell, в CenTel, в Bell Labs, в подобные места — и спросил, знают ли они что-нибудь об этом. Поинтересовался, есть ли программа тестирования, и если нет, то какое объяснение они могут предложить. Они ответили «нет», никакой программы тестирования не существует, они понятия не имеют. Были некоторые предположения — возможно, причиной служит какой-то компьютерный сервис обзвона, — но никакой ясной идеи у них не было. Поэтому несколько месяцев назад мы снова вернулись к этому вопросу.

ES: Нас снова завалили звонки.

EZ: Я попросил женщину по имени Пэт — оператора телефонного центра — позвонить мне. Она перезвонила и вызвалась помочь: предложила использовать её телефонную систему в качестве подопытного кролика и посмотреть, сможет ли телефонная компания каким-то образом установить источник этих «звонков-призраков». Среди прочего она отметила, что во время пожара в Хинсдейле, пока Хинсдейлский коммутатор не работал после пожара, «звонки-призраки» прекратились.

ES: Ааа!

EZ: После ремонта звонки возобновились, но стали более нерегулярными, тогда как раньше приходили как по часам в определённое время ночи.

ES: Угу.

EZ: Теперь одни и те же группы телефонов звонили в данный день, но в предсказуемое время. Отклонение составляло около часа. Поэтому я хотел договориться с Пэт и с телефонной компанией, встретиться у неё и посмотреть, что удастся выяснить. К сожалению, она заболела — тяжёлая инфекция, — и долго не работала.

ES: Угу.

EZ: Она только недавно вышла на работу, я разговаривал с ней сегодня. Наш план таков: я заеду к ней в четверг, сам всё посмотрю, а потом, скорее всего, позвоню вашему другу Кену Венту из Illinois Bell.

ES: Начальник службы безопасности.

EZ: Посмотрим, что удастся узнать, и постараемся уложиться в скромный бюджет — ресурсов у нас немного. Проблема в том, что соединение длится долю секунды, и я не уверен, что за столь короткое время можно произвести трассировку. Мне не вполне ясно, насколько это вообще возможно.

ES: Когда вы были у нас несколько недель назад в пятничный вечер, выяснился ещё один аспект. Известно, что телемаркетеры, разыскивая людей, звонят на номера, которых у них нет.

EZ: Нам поступила действительно интересная информация. Было две основные версии, о которых, думаю, стоит рассказать. Первая — это делают компьютерные хакеры. Одна из вещей, которые хакеры делают, — программируют свои компьютеры, используя модемы для поиска других компьютеров. Найдя компьютер, они улавливают характерный тон, который сигнализирует другому компьютеру, что тот достиг ещё одного компьютера. Если компьютер не найден, можно отключиться очень быстро — до того как соединение фактически установлено и звонок записан на счёт. Таким образом, всё это делается фактически бесплатно. Они делают это регулярно, пытаясь найти новые местонахождения компьютеров.

ES: Понятно.

EZ: Это была одна версия. Её слабое место — зачем повторять попытку звонить на данный номер снова и снова? Очевидно, если компьютера нет там во вторник, его там не будет и в пятницу днём. Зачем пробовать снова каждую неделю? В этом была одна проблема. Вторая версия, которую нам представили, — телемаркетинговые фирмы делают это, чтобы поддерживать свои базы в актуальном состоянии. Они хотят знать, используются ли данные номера.

ES: Ведь люди переезжают и меняют номера.

EZ: Верно, поэтому они быстро набирают номер и вешают трубку раньше, чем вы успеваете ответить. По крайней мере, они могут определить, работает ли линия. По всей видимости, это даёт им некоторую полезную информацию. Таковы были две основные версии, и существовали их различные разработки, о которых мы, наверное, ещё услышим сегодня вечером. Проблема, как я уже сказал, в том, что по-прежнему неясно, какую именно пользу это регулярное обращение — еженедельное или по иному расписанию — приносит тому, кто это делает.

ES: Здесь есть несколько очень важных аспектов. Во-первых, вчера утром у нас выступал человек, который, судя по всему, подал иски против компаний, занимающихся телемаркетингом, за то, что те беспокоят его. Он намерен создать прецедент: если вас беспокоят дома телемаркетеры, вы можете подать на них в суд и взыскать ущерб. Обычно суммы невелики, но достаточны, чтобы они задумались. И он пытается научить других людей, как судиться с телемаркетерами.

(Рекламная пауза, затем повторные представления)

CM: Спасибо, Эд. Рады быть здесь.

ES: Рад иметь вас здесь. Ameritech Applied Technologies — это подразделение Ameritech, телефонной компании, верно?

CM: Верно. Мы — дочерняя компания Ameritech, которая занимается потребностями в информационных технологиях семьи Ameritech, включая Illinois Bell.

ES: Чем вы занимаетесь и за что отвечаете?

CM: Я отвечаю за компьютерную безопасность компаний Ameritech. Кроме того, занимаюсь аудитом Ameritech Applied Technologies, физической безопасностью нашей компании. Что-то в этом роде.

ES: Серьёзная работа!

CM: Да. Мы регулярно, постоянно сталкиваемся с хакерами.

ES: Рад видеть вас сегодня вечером, Чак. Также хочу представить г-на Боба Гейтса, менеджера по корпоративной безопасности Ameritech Applied Technologies.

BG: Доброе утро.

ES: И вам доброе утро. Боб ранее был полицейским. Сколько лет вы работаете в корпоративной безопасности Ameritech, Боб?

BG: С момента разделения — в январе 1984 года. Это намного более специализированная сфера, и вы имеете дело с одним конкретным аспектом всего сценария.

ES: Ваши слушатели правы? Вы звоните людям в разное время дня и ночи? Существуют ли «звонки-призраки»? Есть ли люди, которые балуются этим? Это телефонная компания или кто-то другой? Что происходит?

CM: Я в телефонном бизнесе 22 года.

ES: Это директор по внутренним делам Ameritech Applied Technologies, г-н Моран, прошу вас.

CM: В годы работы в Illinois Bell мы нередко получали подобные жалобы. Мы неизменно пытались выяснить причину, и кое-что из того, что мы обнаружили, — это хакеры! Они любят сканировать префиксы в поисках компьютерного тона. Хотят найти компьютер для общения, поэтому звонят на телефон. Их компьютер звонит вашему.

ES: Это можно делать из спальни тринадцатилетнего фрикера, верно? Или любого другого, если уж на то пошло.

CM: Если у него достаточно развитое компьютерное мышление, он может делать это во сне. Запрограммирует свой ПК, чтобы тот использовал модем для набора вашего номера.

ES: Большинство компьютерных взломов и несанкционированного использования компьютеров происходит в нерабочее время? То есть это не деловые люди в дневное время, верно? Это примерно соответствует вашему описанию типичного хакера?

CM: Людям всё равно нужно жить, кормить себя, ходить в школу или на занятия. Поэтому, поскольку хакерство — хобби, им занимаются в свободное время. Как правило, это вечера, выходные и отпуска.

ES: Мне кажется, я хочу установить, что большинство компьютерных злоупотреблений происходит скорее из частных домов, чем из деловых офисов.

CM: Нет. Исследования показывают, что 80% компьютерных злоупотреблений совершают люди в бизнесе, и они злоупотребляют своей собственной компанией. Однако это не заставит звонить ваш телефон. Люди, использующие сеть для звонков в поисках компьютеров, — это те, кого мы обычно называем хакерами. Они составляют 15–25% всех компьютерных злоупотреблений в мире.

ES: Насколько Ameritech и другие технологические и телефонные компании по всей стране озабочены всем этим?

CM: Как и любой бизнес, Ameritech в значительной степени зависит от информационных систем для выживания. Поэтому нас беспокоят все риски, связанные с использованием компьютеров.

ES: Вы оба смотрели фильм «Военные игры» с Мэттью Бродериком?

CM и BG: Да.

ES: Хотя сюжет довольно экстравагантный, теория работоспособна, верно?

BG: Природная пытливость молодого ума, потребность исследовать.

ES: Мы слышали истории о компьютерных хакерах, которые проникали в компьютеры правительственных учреждений, средних школ, колледжей и университетов. Они меняли оценки, добавляли и удаляли данные из баз, делали всевозможные вещи.

Записи о заработной плате изменялись, и теперь у нас есть такое явление, как компьютерный вирус. Получил обвинительный приговор человек, который буквально уничтожил компьютерную программу через два дня после ухода из компании. По всей видимости, это то, что очень беспокоит

компьютерных специалистов.

Придём ли мы в конечном счёте к огромному числу людей, которых называют «компьютерной полицией»? Чтобы взять всё это под контроль — это то, что нам нужно?

BG: Думаю, компьютерная безопасность — это просто естественное продолжение использования компьютеров, гарантия того, что они используются в защищённом режиме. Что они не подвергаются взлому и злоупотреблениям. Для этого нужно приложить определённые усилия для защиты компьютерной системы.

ES: Готовы ли правоохранительные органы к тому, чтобы справляться с преступлениями, над которыми вы работаете, которые расследуете и с которыми пытаетесь справляться?

BG: В правоохранительных органах есть эксперты. Но им приходится расследовать всё, что происходит. Поэтому для частных компаний приоритетным делом становится взять на себя обязательство самостоятельно разбираться с этим, чтобы защитить свои системы, и привлекать правоохранительные органы при необходимости.

ES: Не кажется ли вам, что многие люди просто наивно оставляли компьютерные системы без защиты?

BG: Да. Говоря о правоохранительных органах, в нашей нынешней системе уголовного правосудия я знаю, что в штатах, с которыми мы работаем, и в федеральных агентствах, с которыми мне приходилось иметь дело, часть проблемы состоит в том, чтобы найти прокурора, судью и присяжных, которые понимают, что такое компьютерное преступление. Потому что они не владеют компьютерной грамотностью.

ES: Что ж, кража информации и кража времени — это преступления. Как насчёт историй о хакерах, взламывающих компьютеры в ядерных лабораториях, таких как Ливерморская национальная лаборатория имени Лоуренса в Калифорнии? Там ведут исследования в области ядерного оружия и бог знает чего ещё. Подумайте о потенциале подобного поведения — это пугает.

BG: Вот почему компьютерная безопасность стала горячей специальностью.

EZ: Я по-прежнему пытаюсь сосредоточиться на своей непосредственной проблеме — на вопросе о «звонках-призраках». Из того, что вы говорите, я делаю вывод, что эти звонки — преимущественно дело рук хакеров.

CM: Думаю, это вполне правдоподобная причина.

EZ: Вопрос, который люди задают по этому поводу, конечно, состоит в следующем: можно понять, что это происходит время от времени, но почему всё время на регулярной основе?

CM: Хакер сканирует префиксы и настраивает свой автодозвонщик на поиск компьютерных тонов. Он может найти несколько номеров и сообщить двум-трём друзьям. Те двое-трое расскажут ещё двум-трём. Они увидят эти номера и затем снова просканируют весь блок из тысячи номеров.

EZ: Я всё равно не совсем понимаю, почему «звонки-призраки» происходят в строго одно и то же время.

CM: На этот вопрос я ответить не могу.

ES: Я объяснил бы это тем, что время, скорее всего, приблизительное. Большинство часов у людей неточны, как и их память. Однако если большинство хакеров учится в средней школе, они, вероятно, ложатся спать примерно в одно и то же время каждый вечер и настраивают свои автодозвонщики работать, пока они спят, — поэтому и звонят на одни и те же номера примерно в одно и то же время каждую ночь.

Правда ли, что они могут запрограммировать эти компьютеры выполнять свою работу без формирования каких-либо биллинговых данных? И как им это удаётся? Или это область, которой

нам лучше не касаться — не хочу ставить вас в неловкое положение.

BG: Вы говорите о телефонном мошенничестве — это, строго говоря, не моя область компетенции. Телефонное мошенничество существует, но я не специалист по нему.

CM: Предполагается, что биллинг включается через долю секунды после того, как трубка снята, — это и позволяет им уходить от ответственности.

BG: Спросите Кена.

ES: Кен расскажет вам вещи, о которых вы никогда не сможете говорить по радио или писать, боюсь. Мы перейдём к некоторым другим аспектам всего этого. Соответствуют ли наказания, предусмотренные для хакеров, тяжести преступления? То есть мы ловим многих из них? Их наказывают? И соответствует ли наказание преступлению?

CM: Хакеры, которых обычно ловят, — несовершеннолетние. Это означает, что максимум, что можно сделать, — это держать их под стражей до 21 года и конфисковать компьютерное оборудование. Прокуратура США по Северному округу Иллинойса действительно возбудила дело о правонарушении несовершеннолетнего против хакера, использовавшего псевдоним SHADOW HAWK. Это попало на первую страницу Chicago Tribune.

ES: Что он сделал? Можете рассказать?

CM: По данным Tribune, он похитил программное обеспечение у AT&T.

ES: Это доказывает, что, как бы умны ни были некоторые хакеры, некоторых из них всё же ловят — а может, и многих. Так что, как бы они ни старались обойти систему, вы, судя по всему, работаете изнутри системы, чтобы сорвать их планы и поймать их.

CM: Именно.

ES: Если их не преследовать в судебном порядке, когда поймают, — это ничего не будет значить. Означает ли это, что различные телефонные компании и их дочерние структуры весьма серьёзно настроены на привлечение к ответственности тех, кого удаётся поймать? Таков путь в будущее?

CM: Каждое дело индивидуально. Уголовное преследование — всегда один из вариантов.

ES: Мы немного опоздали с решением этой проблемы — лет на несколько?

BG: Законы, как правило, успевают за потребностью. Нужно сначала выявить проблему, чтобы по-настоящему её решить.

ES: Благодаря нашим сегодняшним гостям нам удалось договориться о разговоре с детективом-сержантом полиции штата Иллинойс, который работает по делам о компьютерном мошенничестве, — сержантом Абагейл Абрахам.

AA: Доброе утро. Рада быть здесь.

ES: Вы слушали радио до нашего звонка?

AA: Я была прикована к радиоприёмнику, да.

ES: Хорошо. Ваше подразделение называется «Отдел компьютерных преступлений»?

AA: Именно.

ES: Как давно вы существуете?

AA: С февраля 1986 года.

ES: Видимо, была потребность. Достаточно ли у нас законов штата или соответствующих статей, чтобы вы могли делать свою работу?

AA: Думаю, да. На момент создания отдела законы были весьма несовершенны. Большинство компьютерных преступлений было уголовными проступками вплоть до нескольких месяцев спустя, когда генеральный прокурор провёл слушания, в которых мы участвовали, и в результате был принят закон.

ES: Сержант, лучше ли это решается на уровне штата, чем на федеральном? Господа из Ameritech упоминали, что прокуратура США недавно возбудила уголовное преследование здесь, в Северном Иллинойсе. Будет ли их ведомство продолжать такую работу, или вы видите её на уровне штата?

AA: Думаю, это зависит от характера дела. Одни дела, вероятно, лучше рассматриваются на федеральном уровне, другие — на местном. При работе с федеральными агентствами юрисдикция по делам о компьютерном мошенничестве разделена между ФБР и Секретной службой. Таким образом, то, какое агентство возьмёт дело, зависит от его характера. Но многие дела не подходят для федерального участия.

ES: Допустим, студент изменил оценку в школьной компьютерной системе. Это будет скорее дело штата, чем федеральное, полагаю?

AA: Конечно, скорее всего, это дело штата. У нас был подобный случай.

ES: Если бы вам удалось разработать такое дело и собрать доказательства, вы бы получили обвинительный приговор? Наши гости говорили, что суды не обязательно разбираются во всём этом. Когда вы приходите в суд штата с таким делом, понимают ли судьи и/или присяжные, о чём идёт речь?

AA: Ни одно из наших дел не дошло до суда присяжных. Собственно, ни одно не дошло даже до разбирательства без присяжных, потому что, как и подавляющее большинство дел в системе, они завершаются сделкой о признании вины.

ES: Они признают себя виновными?

AA: У нас стопроцентная раскрываемость.

ES: Правда!

AA: Наш успех основан на очень хорошем взаимодействии с прокуратурами штата. С передачей дел у нас не было никаких проблем.

ES: Ваши данные настолько хороши, что к моменту, когда вы производите арест, им никак не выкрутиться. Вы застигаете их с поличным.

AA: Да, с этим проблем не было.

ES: Какие наказания вы добиваетесь, сержант?

AA: Во всех наших делах стопроцентная раскрываемость, но окончательных решений было не так много. Они находятся на разных стадиях, потому что закон ещё очень новый.

ES: Полагаю, вы продолжите упорно работать и сажать всё больше людей за решётку.

AA: Да, это растущая отрасль.

ES: Директор Марголис поддерживает то, что вы делаете?

AA: Думаю, да. Наш отдел был создан при прежнем директоре, Цегале, но директор Марголис очень поддерживает наши усилия, и я подозреваю, что со временем его поддержка только усилится.

ES: Знают ли жертвы компьютерных преступлений, куда сообщать? Если вы ведёте бизнес и ваш компьютер был взломан или с ним что-то сделали, знает ли среднестатистический владелец компьютера, куда сообщать?

AA: Нет. Вот это действительно простой вопрос!

BG: Я бы знал, но только потому, что работаю в этой отрасли. Однако средний мелкий предприниматель, вероятно, был бы несколько в растерянности.

AA: Он может даже не понять, что это преступление.

BG: Совершенно верно, и к счастью, у Иллинойса хватило дальновидности создать такое подразделение, как у сержанта.

ES: Допустим, есть компания среднего размера, использующая компьютеры. Придумаю компанию. Меня зовут г-н Х, у меня неплохое агентство недвижимости в Чикаго. У меня около дюжины сотрудников, и пару лет назад мы перешли на компьютеры для ведения учёта объектов, бухгалтерии, записей о клиентах и всех контактах. Данных накопилось много. Мы обмениваемся информацией с другими агентствами недвижимости, используем модемы, телефонные линии и компьютерную связь. Поскольку часть работы ведётся, когда офис закрыт, мы оставляем систему подключённой. Вчера утром я пришёл на работу и обнаружил, что кто-то проник в наш компьютер и стёр все наши данные, или часть из них, или что-то изменил. Я стал жертвой преступления. Должен ли я взять трубку и позвонить в полицию штата Иллинойс?

AA: Конечно.

ES: Вы приедете и проведёте расследование?

AA: Конечно.

ES: Хорошо.

AA: Есть несколько способов, которыми дело может попасть к нам. Один — вы как пострадавший напрямую обращаетесь к нам. Другой — обратиться в местную полицию и надеяться, что та позвонит нам.

ES: Вот ключевое слово — «надеяться». Знают ли чикагская полиция, полиция Уилметта, полиция Джолиета достаточно, чтобы передавать эти дела вам?

AA: Не знаю насчёт Джолиета, но Чикаго и Уилметт — точно знают. Для всех полицейских, которые сейчас нас слушают, добавлю: если нам передадут дело, мы разберёмся с ним любым из возможных способов. Если местное агентство передаёт его нам и не хочет заниматься им, потому что у самих дел по горло, — мы возьмём дело. Если они хотят просто совместной работы или чтобы мы сопровождали их на одном-двух допросах для перевода того, что говорит потерпевший, — мы рады и так. Работы у нас сейчас достаточно, чтобы не забирать дела целиком. Мы рады работать с любым агентством.

CM: Думаю, стоит заметить, что мы сосредоточились на преступлении, совершаемом по телефону. Компьютерное преступление совершается дистанционно, и жертва не знает преступника.

AA: Это правда.

CM: Большинство дел, вероятно, вообще не связано с телефонами. Они касаются собственных сотрудников компаний, которые, по сути, совершают растрату с помощью компьютеров. Либо переводят деньги по компьютеру на собственные счета, либо как-то иначе играют с книгами учёта, и работодатель может долго не замечать, пока какой-то аудит не выявит, что преступление вообще имело место.

AA: Вы правы. Подобных случаев немало. В таких делах, когда виновен кто-то внутри компании, часто случается, что компания предпочитает не привлекать полицию, а вместо этого принимает дисциплинарные меры или увольняет человека. Их аргумент, как правило, — нежелание огласки. Мы не гонимся за заголовками, если только наша жертва сама не заинтересована в этом. Мы не стремимся афишировать дела и позорить жертву. Просто информация об этом поступает нечасто.

EZ: Однажды я разговаривал с консультантом по компьютерам, который сказал, что чем выше человек стоит в компании и чем более он причастен к чему-то подобному, тем меньше вероятность не только того, что он когда-либо окажется за решёткой, но и что ему вообще будет назначено какое-либо наказание. Мне рассказали об одном конкретном случае — вице-президент банка, я думаю, похитил колоссальную сумму, счёт шёл на миллионы. Его обнаружили спустя какое-то время, но раскрывать, что один из доверенных сотрудников оказался мошенником, не хотели. Поэтому устроили ему прощальный банкет.

ES: Ха-ха-ха-ха!

EZ: Проводили его из компании с почестями.

AA: Мне нравится...

EZ: Консультант сказал, что присутствовал на этом и это было самое лицемерное, что он когда-либо видел. Но они пойдут на это ради того, чтобы избежать негативной огласки.

ES: Верю.

AA: Конечно, если вы высоко стоите в организации и контролируете её, то можете контролировать различные процедуры таким образом, что вас с меньшей вероятностью поймают. И вы, вероятно, распоряжаетесь достаточным количеством денег, чтобы придумывать творческие способы присвоения с меньшим возникновением подозрений. Не знаю почему, но чем больше вы берёте, тем меньше вероятность, что вас привлекут к ответственности.

ES: Люди восхищаются такими преступлениями.

(Рекламная пауза, затем повторные представления)

ES: Хочу приветствовать нового участника нашего вечера — г-на Джона Максфилда. Джон Максфилд владеет консалтинговой компанией по корпоративной безопасности. Джон, вы здесь?

JM: Да, доброе утро.

ES: Доброе утро. Вы, насколько я понимаю, за пределами Чикаго — достаточно близко, чтобы слышать нашу программу?

JM: К сожалению, я несколько восточнее вас, и с прослушиванием по радио возникли сложности, так что последние несколько минут я слушаю по телефону.

ES: Мы обсудили здесь всевозможные данные. Вы с сержантом раньше разговаривали?

JM: Не думаю. Возможно, я разговаривал с кем-то из полиции штата Иллинойс около года назад, но это был не сержант.

ES: Сержант Абрахам, вы всё ещё здесь?

AA: Да, я здесь.

ES: Полагаю, Джон, вы знакомы с Чаком Мораном и Бобом Гейтсом.

JM: Да, я знаком с Бобом Гейтсом.

ES: Чем занимается частная компания по компьютерной безопасности?

JM: Мы занимаемся делами, которые, пожалуй, не попадают в заголовки. Моя роль — скорее консультирование клиентов о том, как защитить свои системы, ознакомление их с рисками и характером угроз, с которыми они сталкиваются.

ES: Мы говорили ранее о фильме «Военные игры», с которым вы наверняка знакомы. Мои гости немного рассказали нам о том, что происходит. Подозреваю, что проблема компьютерного хакерства и связанных с ним форм поведения весьма серьёзна, не правда ли?

JM: Да, это безусловно растущая проблема. «Военные игры» вынесли на широкую публику то, что долгие годы происходило очень тихо за кулисами. И конечно, в результате «Военных игр» хакерская активность, думаю, возросла, потому что многие хакеры вдруг осознали, что это, пожалуй, то, чем стоит заниматься ради известности.

ES: У меня есть вопрос, на который, возможно, и нет ответа. Почему законное использование компьютера не удовлетворяет его пользователя или владельца? Иными словами, зачем взламывать? Зачем нарушать закон? Зачем обходиться дорогой ценой для людей? Ведь с компьютером можно делать столько увлекательных вещей, не нарушая закона. Почему так много людей занимается этим антисоциальным, антибизнесовым поведением?

JM: Это сложный вопрос. Можно спросить: «Почему существуют преступники?» — ведь достаточно возможностей для законного заработка. Что касается хакеров, большинство из них — искатели острых ощущений. Они, как правило, не те, кто будет хорошим специалистом по компьютерам, они умеют лишь причинять вред. Они что-то вроде аналога вандалов. Некоторые очень умны, но глубоко заблуждаются. Им дали неправильное направление. Трудно сделать обобщение или составить стереотип, потому что они охватывают широкий спектр. На одном конце спектра — много молодых ребят, подростков. И в основном это мальчики — среди хакеров очень мало женщин.

ES: Правда?

JM: Да, это интересный феномен. Я бы сказал, что на десять тысяч мальчиков приходится, пожалуй, одна девочка. Но так или иначе, на одном конце спектра — дети, которые просто носятся где попало. Они толком ничего не умеют, но когда им что-то удаётся, причиняют большой ущерб — уже одним своим количеством. На другом конце спектра — профессиональный преступник, избравший совершение преступлений по телефонной линии. Вместо того чтобы грабить людей с оружием, он грабит банки по телефону. Спектр очень широк, и навесить на него ярлык крайне сложно. Но большинство хакеров начинают потому, что в этом есть азарт — что-то вроде острого ощущения от того, что надул телефонную компанию, взломал банковский компьютер и уничтожил данные. Присутствует своеобразное упоение властью.

ES: Итак, вы стараетесь консультировать клиентов, как избежать этого, прежде чем оно случится. Большинство из них всё же обращаются к вам, уже пострадав, или люди достаточно умны, чтобы вкладывать средства заранее?

JM: Безопасность в деловом мире, к сожалению, обычно отходит на второй план, потому что не генерирует прибыли, не приносит дохода. Это расходы. Если вас беспокоят грабители и вы живёте в большом городе, вам приходится тратить лишние деньги на замки и сигнализацию. Это неудобно — нужно открывать дверь тремя разными ключами, откидывать все эти засовы, выключать и снова включать сигнализацию, уходя. Так что безопасность обычно откладывается на потом. И конечно, когда корпорацию всё же взломали, данные повредили, украли или уничтожили, — денег не жалеют, лишь бы это не повторилось.

ES: Нам говорили, что не существует помещения, которое невозможно обокрасть, нет человека, сколь бы важным он ни был, которого невозможно устранить. Можно ли надёжно защитить компьютер или компьютерную систему? То есть можно ли научить кого-то защитить систему так, что хакер просто не сможет до неё добраться?

JM: Откровенно говоря, вы правы. Думаю, единственный по-настоящему защищённый компьютер — это тот, который отключён от сети. Или если сменить все пароли и не записывать их, так что никто не сможет войти. Как и при любой другой форме защиты: если нацепить на двери и окна достаточно замков и решёток, взломщик уйдёт туда, где добраться легче. То же самое в компьютерной безопасности. Вы можете защитить свою систему от всего, кроме действительно серьёзной и организованной атаки. Очевидно, что в промышленности есть определённые сегменты, которые являются мишенями: банки, очевидно, — мишень, ведь там деньги.

ES: Если компьютеры столь мощны и умны, нельзя ли сказать компьютеру: «Компьютер, защити себя»?

JM: Компьютер в действительности вполне способен защищать себя, единственная проблема — он не разумен. И ему, в сущности, всё равно, взломают его или нет. В системе нет человека, если угодно. Поэтому нужно, чтобы где-то был человек, который просматривает исключительные отчёты, которые генерирует компьютер, и замечает: «Что за входы в систему в два часа ночи? Эти учётные записи не должны быть активны в это время суток». Можно запрограммировать компьютер делать часть этого, но всё равно нужен человек-аудитор, который время от времени тщательно проверяет работу системы — просто чтобы убедиться, что компьютер защищает то, что должен защищать.

ES: Джон, как называется ваша компания?

JM: Моя компания называется BoardScan, мы находимся в Детройте, штат Мичиган.

ES: У нас есть звонки. Первой выйдет на связь молодая женщина по имени Пенни. Пенни, вы здесь?

P: Да, Эд. Как вы?

ES: Хорошо. Вам нравится программа?

P: Да! Я жертва!

ES: Жертва! Расскажите, как это случилось.

P: Мы въехали около трёх месяцев назад. Два телефона у нас с дисковым набором, и один — дешёвый тональный, который переключается с тонального на импульсный. Когда кто-то набирает номер с одного из дисковых телефонов, этот дешёвый телефон пищит в ответ. Меня это не сильно беспокоит, потому что у меня маленькие дети и я знаю, кто пользуется телефоном. Но когда в 22:38 мои дети уже спят, а я сижу в гостиной, мой маленький тональный телефон пищит. Дважды.

JM: О, думаю, я могу это объяснить. Значит, он просто пищит...

P: Дважды!

JM: И это происходит каждую ночь примерно в одно время?

P: Почти, да.

JM: Что ж, в каждой телефонной станции есть автоматический сканер, который работает ночью и тестирует линии.

ES: О нет! Подождите!

P: Постойте! Они говорили, что этого не бывает! Нет-нет-нет.

ES: Телефонная компания, значит. Это единственное, что все, с кем мы разговаривали в телефонной отрасли, отрицали!

EZ: Мы, э-э, да...

ES: Давайте, Эд! Перехватывайте, перехватывайте!

EZ: Мы разговаривали с рядом сотрудников телефонной компании, и первоначальная идея состояла в том, что телефонная компания проводит какое-то тестирование. Но сотрудники компании, с которыми мы разговаривали, сказали «нет». Тестирование происходит только тогда, когда в ходе обычного телефонного звонка устанавливается реальное соединение. Это часть текущей программы тестирования. Дополнительного тестирования, однако, нет, заявили они. Но в Мичигане это работает по-другому?

JM: Не знаю. Знаю, что у меня есть телефон с маленьким зуммером, который «тик-ток» примерно в 1:30 ночи каждую ночь. И если вы подключены к одной из старых электромеханических станций, то, осмелюсь утверждать, там есть сканер, который проверяет все линии ночью. И он останавливается на каждой линии примерно на полсекунды — ровно достаточно, чтобы телефон пикнул дважды. Уверен, что именно в этом объяснение. Я достаточно компетентен — до работы в области компьютерной безопасности я занимался установкой телефонных станций.

P: Хорошо. У меня есть домашний компьютер — Commodore. Модема нет. Можно ли каким-то образом с его помощью это проверить?

JM: Не вижу, что общего имеет модем с тем, что телефонная компания тестирует вашу линию в 22:30. Не понимаю связи.

P: Что могло бы подтвердить это? Могла ли я убедиться, что меня используют для тестирования, или что мою линию сканирует какой-то компьютер в другом месте?

JM: Нет. Если вас сканирует хакер, вы получите настоящий звонок, а не просто короткий сигнал.

EZ: Пенни, где вы живёте?

P: Оклон.

EZ: Готовы ли вы поучаствовать в небольшом эксперименте?

P: Конечно, это происходит довольно регулярно.

EZ: Хорошо. Это происходит каждую ночь или только иногда?

P: 6 ночей из 10. Чаще, чем 50 на 50. Сегодня вечером это было, кстати.

EZ: Хорошо, договорились.

P: И вчера вечером тоже было!

ES: Пенни, мы запишем ваше имя и номер, и Эд свяжется с вами днём и немного поработает над этим, хорошо?

P: Звучит хорошо.

ES: Спасибо, Пенни. Подождите минуту.

P: Спасибо.

ES: Видите ли, г-н Максфилд говорит нам кое-что, что все наши источники отрицали. Нам говорят, что не существует случайного тестирования телефонной сети — ни местной телефонной компанией, ни AT&T, и они спрашивают нас: «А зачем?» Нет в этом нужды, нет причины. Позвольте спросить наших гостей в студии из Ameritech. Кто-нибудь из вас слышал о чём-то подобном? Это то, что кто-нибудь из вас может прокомментировать? Я понимаю, что вы компьютерщики, но как насчёт этого?

CM: Я знаю, с кем вы разговаривали в службе безопасности Illinois Bell. Исторически, когда-то они проводили тестирование, но прекратили это ещё в то время, когда я работал в Illinois Bell.

ES: Значит, это было несколько лет назад.

CM: Да.

EZ: Это распространялось только на электромеханические системы?

CM: Все офисы, где я работал, были электромеханическими, так что — да.

JM: Что ж, не знаю. Это было бы моим первым предположением, потому что когда я был на электромеханической станции здесь, в Детройте, так и происходило каждую ночь.

ES: Это другая телефонная компания.

JM: Знаю, но оборудование то же самое. На двух электронных коммутационных системах линия тестируется каждый раз при совершении звонка. Так что такого сканера там нет. Думаю, загадка разрешилась бы, просто проверив, из какого оборудования обслуживается её линия.

EZ: Нам и в голову не приходило, что это может иметь значение.

(Рекламная пауза, затем повторные представления)

ES: У меня звонок дальней связи из Миссури. Анна, вы здесь?

A: Да.

ES: Из какого города в Миссури?

A: Из Канзас-Сити.

ES: И вы слушаете нас сегодня вечером?

A: Да.

ES: Хорошо. Мой продюсер сообщает, что когда вы позвонили, то представились компьютерным хакером. Это верно?

A: Я — женщина-телефонный фрикер и компьютерный хакер. Да.

ES: Одна из немногих, потому что, судя по всему, этим в основном занимаются мужчины.

A: Угу.

ES: Анна, говорите погромче. Сколько вам лет?

A: 27.

ES: Двадцать семь лет. У вас есть работа?

A: Нет.

ES: Нет?!

A: Нет. У меня много свободного времени.

ES: И вы — компьютерный хакер. По определению, что вы делаете со своим компьютером, что делает вас хакером?

A: Ну, я перебираю коды, которые жители и компании используют у US Sprint и других компаний. Я совершила переговоры примерно на пятнадцать тысяч долларов бесплатной межгородской связи.

ES: Вы сейчас звоните бесплатно?

A: Да. Я не плачу за этот звонок.

ES: Ваш компьютер позволил вам совершить незаконный международный звонок?

A: Через компьютер я получаю коды, а затем набираю их с тонального телефона.

ES: Сержант, мне следует разговаривать с ней, ведь она прямо сейчас совершает преступление? Я становлюсь соучастником? Нет, подождите... Нет. У меня на линии полицейский... Сержант?

AA: Да.

ES: Как думаете? Продолжать ли нам?

AA: Мне было бы очень интересно узнать, чем она оправдывает своё поведение.

ES: Что скажете на это, Анна?

A: У меня много свободного времени и очень мало денег, а я люблю общаться с друзьями. Хочу кое-что предложить компаниям и жителям, у которых могут быть коды удалённого доступа: сделайте их сложными, не лёгкими, а то хакеры — ну, первое, что они пробуют, — это 1-2-3-4 и

тому подобное.

ES: Позвольте задать вам вопрос, Анна. Вы считаете, что хакерство даётся вам сравнительно легко?

A: Да.

ES: Значит, вы говорите, что компьютерные специалисты мира недостаточно стараются, чтобы не пустить вас?

A: Нет, недостаточно. Я бы предложила телефонным компаниям, которые используют коды удалённого доступа, делать эти коды более сложными.

ES: Когда мы сталкиваемся с такими людьми, как Анна, которые, очевидно, обладают интуитивным талантом и добиваются успеха, почему бы не нанять таких людей и не использовать их знания?

AA: Нет!

ES: Нет?

JM: Нет. Я тоже должен сказать нет.

A: Почему нет?

JM: Нужно понимать техническую сторону вопроса. Умение взламывать коды не означает, что вы знаете, как изменить систему так, чтобы коды больше нельзя было взломать.

AA: Существует представление, что все эти люди — вундеркинды, и я не думаю, что это так.

ES: Вы вундеркинд, Анна?

A: Нет. Я не всегда использую компьютер для поиска кодов. У меня много друзей, и я немного занимаюсь хакингом сама, существует много разных методов. Вы выясняете, сколько цифр в кодах, и тому подобное, так что это требует некоторого ума. Если только не полагаться на друзей — тогда ум и не нужен.

ES: Вы разве не понимаете, что то, что вы делаете, незаконно? Это даже не принимается в расчёт?

A: Конечно, понимаю! Да.

ES: То, что вы делаете, кому-то другому в конечном счёте приходится оплачивать. Вас это не беспокоит? Я имею в виду, что если бы вы стали жертвой вора или грабителя, вы бы, наверное, вызвали полицию и кричали бы, пока что-нибудь не сделают. И всё же вы и тысячи таких же людей, как вы, ничтоже сумняшеся совершают кражи и мошенничество по проводам и бог знает что ещё. И то, что жертва находится не в той же комнате, что и вы, вас нисколько не беспокоит.

A: Я физически никому не причинила вреда, и в основном я имела дело с компаниями.

ES: Это делает происходящее допустимым? Компании состоят из людей. Иногда они принадлежат частным владельцам, иногда — акционерам, но компании — это люди. Значит, вы причиняете вред людям.

CM: Не знаю, через какой сервис она выходит на связь, но нужно помнить, что прямо сейчас это обходится компании денег, и они вынуждены перекладывать эти затраты на своих законных клиентов.

A: Разве они не просто списывают это как налоговый вычет?

BG: Нет.

JM: Некоторые небольшие компании дальней связи, некоторые из тех, кто перепродаёт услуги AT&T или Sprint, — некоторые из этих небольших компаний были доведены до банкротства такими людьми, как Анна.

A: Ну, я знаю человека, который обанкротил одну из них.

AA: Не понимаю, чем это может кого-то радовать.

A: Я и не горжусь тем, что знаю этого человека.

AA: Почему вы гордитесь тем, что делаете сами? Ведь вы делаете то же самое, только, пожалуй, в меньшем масштабе.

A: Я не имею дела с мелкими компаниями.

AA: Значит, вы и многие подобные вам обходитесь крупным компаниям в огромные суммы. Именно вы — причина того, что такая компания, как Sprint, не получает прибыли и фактически может обанкротиться или вынуждена сокращать сотрудников и лишать людей работы.

A: Они не получают прибыли?

JM: Sprint работает почти в убыток с самого начала.

CM: Или просто повышают базовые тарифы, что делает телефонную связь менее доступной.

EZ: Моя компания дальней связи — All-Net, которая за прошлый год трижды меняла коды доступа. Главным образом из-за хакеров, и, думаю, она никогда не была прибыльной.

CM: Что неудобно для вас как клиента.

EZ: Конечно.

ES: Думаю, меня больше всего беспокоит в ситуации с Анной то, что она совершает преступления буквально каждый день и даже не признаёт этого морально предосудительным.

JM: Да, вы нащупали суть проблемы. Эти телефонные фрикеры и хакеры действительно не считают себя преступниками. Преступление здесь полностью анонимно — это так же просто, как набрать на телефоне чужие цифры. И жертвы нет как таковой. Хакер или телефонный фрикер зачастую даже не знает жертву, на чей счёт записывает звонок.

ES: Как грабитель, который грабит днём, когда никого нет дома, — он не видит лиц своих жертв, и это очень обезличенное преступление. Анна, как бы вы себя почувствовали, если однажды в дверь постучали и это оказались ФБР или Секретная служба, которые наконец вас выследили, а прокурор США по Канзас-Сити решил возбудить против вас дело, у него веские доказательства, и вы оказываетесь в тюрьме? Как бы вы себя почувствовали?

A: Изначально мой интерес к этому хобби возник потому, что кто-то завладел моей карточкой AT&T и накрутил телефонный счёт на несколько тысяч долларов. Я заинтересовалась, чтобы разобраться, что происходит. У меня были контакты с Секретной службой и ФБР, и они ничего не предприняли против человека, который причинил мне вред. Абсолютно ничего.

AA: Это не отвечает на вопрос.

ES: Что произойдёт, если они снова придут и арестуют вас? Как бы вы себя почувствовали, оказавшись в тюрьме?

A: Ну, такова судьба.

ES: Вы замужем или одна?

A: Одна.

ES: Знает ли ваша семья о вашей деятельности?

A: Да.

ES: Как они отреагировали бы на ваш арест?

A: Полагаю, они больше не получали бы бесплатной межгородской связи.

ES: Они тоже этим пользуются?!

A: Они просят меня звонить для них.

ES: Знаете, что меня беспокоит. Вы не производите впечатления глупого человека, но представляете такой уровень безнравственности, который меня глубоко тревожит. Действительно. Думаю, вы воплощаете определённый образ мышления, который морально обанкротился. Я не пытаюсь вас обидеть, но вы меня оскорбляете!

A: Ну, спасибо за внимание и за то, что дали мне слово. Я хотела дать некоторым из вас знать, что мы существуем. Поосторожнее с нами. Делайте коды удалённого доступа посложнее...

BG: Чтобы сделать вызов более трудным для вас?

A: Возможно, для некоторых из нас. Но также и для тех хакеров, у которых нет ни интеллекта, ни нужных знакомств, ни компьютеров, ни чего-то ещё, чем они пользуются.

BG: Или свободного времени.

A: Верно. Свободного времени. Вот именно.

ES: Как вы платите за жильё, Анна? Или живёте с родителями?

A: Я живу с родителями.

ES: О... понятно.

AA: Почему не потратить это время на что-то созидательное или полезное для общества?

A: Ну, я ходила и подавала заявку на работу в US Sprint. Меня не взяли.

AA: Правильно сделали!

EZ: Удивительно ли это?!

ES: Анна, вы часто слушаете нашу программу? Кажется, вы раньше не звонили?

A: Нет.

ES: Иногда слушаете?

A: Да. Я только что узнала от друга, что она выйдет в эфир.

ES: Хорошо. Послушайте, Анна. Небольшой подарок всем новым звонящим. У меня есть замечательные футболки WGN. Если вы дадите моему продюсеру своё имя и адрес, мы вышлем вам одну. Ладно?

A: Ладно.

ES: Мы вернёмся через минуту. *(Щелчок!)* Она положила трубку. Честно говоря, мне казалось, что на секунду мы её поймали.

AA: Браво!

JM: Она бросила трубку?

ES: Как только мы перешли на её линию, чтобы взять адрес и выслать приз, она повесила трубку.

JM: Да, нисколько не удивлён.

ES: Я не хочу враждовать с этой женщиной, но меня действительно тревожит её нравственный дефицит. У меня на линии ещё один человек, называющий себя хакером. Дэн, вы здесь?

D: Да.

ES: Вы хакер?

D: Нет. Я студент компьютерного факультета.

ES: О, хорошо.

D: Хотел бы спросить ваших специалистов по безопасности: какие виды управления рисками существуют применительно к получению несанкционированного доступа к корпоративным компьютерным системам?

BG: Вы спрашиваете, что мы делаем, чтобы не пускать несанкционированных лиц. Ответить на это — значит раскрыть все карты.

AA: К тому же на это ушло бы дня два.

JM: Думаю, можно ответить в общих чертах. Мы говорим, видимо, о телефонном удалённом доступе к компьютерам.

BG: Думаю, он спрашивает в общем смысле. Просто о компьютерах. Полагаю, подробно говорить об этом было бы неуместно. В открытом доступе достаточно литературы. Вы студент компьютерного факультета — читайте её, и там найдёте ответ.

EZ: Просто для примера: я знаю, что применительно не столько к компьютерам, сколько к злоупотреблению кредитными картами дальней связи, All-Net, с которой я работаю, сделала номера длиннее — это самое простое, что можно сделать. Найти рабочий номер становится сложнее.

JM: При защите компьютеров первый рубеж обороны — пароль. Очевидно, не стоит использовать тривиальные пароли. Это первый рубеж. Затем добавляются другие меры: обратный дозвон, шифрование и различные другие методы, которые исключат любого, кто просто предпринимает случайную попытку доступа, — она не пройдёт.

ES: Дэн, где вы учитесь?

D: Прямо напротив WGN — в Институте DeVry.

ES: Каковы ваши ощущения, когда вы слышите о чём-то подобном — вы только что слышали Анну. Что вы думаете о том, что она делает?

D: Я не очень знаком с хакерами.

ES: Разве вас не беспокоит то, что крадут? Это вас задевает? Незаконность, аморальность?

D: Я считаю это крайне неэтичным, потому что у многих компаний оборудование стоимостью в миллиарды долларов.

ES: Вы сами этим не занимаетесь?

D: Нет, совершенно верно.

ES: Рад это слышать. Спасибо за звонок, Дэн.

D: Пожалуйста.

ES: Луис, вы здесь?

L: Да, я здесь.

ES: Хорошо, вы на связи со всей нашей группой, Луис.

L: Большое спасибо. Я слышал историю об одном хакере, который проник в компьютерную систему, скажем, крупной нефтяной компании. Без имён. Там установили систему безопасности, которая автоматически отслеживает звонок до места его источника. И этот болван позвонил из своего дома. Дня через два-три на его пороге появились агенты ФБР.

AA: Я не знакома с этим делом, но это вполне реально.

JM: Такое случается довольно часто. Человек вроде Анны, например, может воспользоваться услугой дальней связи, подписанной на сервис идентификации входящего номера от оператора-источника. Когда выставляется мошеннический счёт, номер, с которого сделан звонок, там тоже фигурирует, и восстановить цепочку в обратном направлении совсем несложно.

L: Они просто поставили что-то вроде ловушки на линию.

JM: В некоторых системах ловушка уже есть. Это просто часть системы, а не специальная ловушка.

ES: Есть способы поймать людей, и хакеры любят играть на вероятностях. Ладно, Луис, спасибо.

L: Надеюсь, это отобьёт желание у многих, кто подумывает о подобном.

ES: Надеюсь, хорошее замечание. Спасибо за звонок.

L: Большое спасибо.

ES: У нас звонок. Алло, Боб!

B: Хотел бы сделать несколько замечаний по поводу законодательства о компьютерах. Я живу в Оклоне, там самые современные станции Illinois Bell. Мой сын живёт в этом районе, и я знаю, что там предлагаются функции, доступные только на новых коммутаторах. Я знаком с компьютерами ещё со времён до того, как Apple и IBM продавали ПК, — у меня дома было несколько штук.

ES: Угу.

B: Первый модем я купил примерно в 1978 году. Считаю себя в некотором роде хакером, но никогда по-настоящему не пытался войти в чужую систему — не потому что считал это незаконным, а просто потому, что ничего интересного для меня там не было. Что касается компьютеров: если я сижу дома и набираю случайные номера в некоторых штатах — это незаконно. Это незаконно, если этим занимается ваш четырнадцатилетний ребёнок дома за компьютером, но не незаконно, если вы используете компьютеризированную телефонную систему для генерации потенциальных покупателей.

ES: Это мы называем телемаркетингом.

B: Телемаркетинг — это, по существу, то, из-за чего некоторым хакерам досаждают, и в ряде штатов это теперь незаконно. Я случайно подключался к системам, к которым не собирался подключаться.

CM: Но вы же не стали продолжать, правда?

B: Нет, никогда. Я никогда не использовал компьютер для кражи услуг. Я не собираюсь защищать тех, кто использует компьютер как инструмент кражи услуг у телекоммуникационной компании. Однако есть определённые компьютерные законы, которые никогда не должны были принимать. Случай в Калифорнии два-три года назад: у человека была доска объявлений, кто-то разместил на ней коды доступа. У него автоматическая машина, отвечающая на его телефонный звонок. Телефонная линия оформлена на его имя. Секретная служба пришла и конфисковала его оборудование. Это неправильно — случилось из-за кражи услуг третьими лицами.

BG: Думаю, такое обоснование чрезмерно упрощает ситуацию.

B: Вопрос по существу в следующем: несу ли я ответственность за то, что вы говорите, когда я беру трубку?

BG: Нет, думаю, вопрос в том, несёт ли оператор доски объявлений ответственность за то, что на ней размещено.

B: Но это буквально лишено смысла. Если мне позвонит телемаркетер, несу ли я ответственность за всё, что он скажет после того, как я возьму трубку?

BG: Доска объявлений служит для дальнейшего распространения информации. Когда кто-то что-то размещает — в данном случае код — доска объявлений служит для дальнейшего распространения этой информации.

JM: Полагаю, вы имеете в виду дело Тома Тсимпидиса — я хорошо с ним знаком. Оно выглядело не совсем так, как вы описали. Украденная карточка AT&T была размещена анонимно. И буквально через минуту после того, как анонимный участник разместил карточку AT&T, сам Том Тсимпидис — сисоп, оператор доски объявлений — был в сети и разместил другие сообщения. Так что были основания предполагать, что анонимный пользователь и был оператором системы. Возникло и ещё одно осложнение: украденная карточка AT&T принадлежала бывшему работодателю оператора. В конечном счёте доказательств для обвинения не хватило, и всё тихо прекратилось. Но это поставило интересные вопросы об ответственности оператора системы: г-н Тсимпидис утверждал, что не знал о коде, однако лог его оборудования показывал, что он был в сети.

B: Продолжим логику. Допустим, к его телефону был подключён автоответчик, и мы знаем, что он прослушивал автоответчик. Допустим, кто-то оставил ему голосовое сообщение с полдюжиной украденных номеров кредитных карт. Действия правоохранительных органов были бы теми же?

JM: Нет... нет, вы...

B: Думаю, нужно посмотреть на ситуацию, при которой со временем возник излишний страх перед частью хакеров. Телефонные фрикеры пугают меня в определённой мере. На моих счетах US Sprint и All-Net появлялись фиктивные звонки — но в счёте AT&T такого никогда не было. Вижу, что это серьёзная проблема, телефонные фрикеры меня пугают, и я понимаю, что реальная проблема в том, что, судя по всему, никто не сверяет каждый звонок и даже не читает счета за дальнюю связь.

AA: Если у меня на телефоне есть автоответчик и кто-то позвонил и оставил мне информацию, использование которой было бы незаконным, а я либо стёрла эту информацию, либо сообщила о том человеке — у меня нет намерения ею пользоваться, и я не могу представить себе ни одного правоохранителя, который предпринял бы какие-то действия, ни прокурора, который взял бы это дело.

ES: Иными словами, если человек создаёт компьютерную доску объявлений специально для обмена информацией, которую он не должен иметь, и другие люди размещают информацию, которую не должны иметь, — думаю, нет никаких сомнений в том, каковы их намерения и что они нарушают закон.

Сержант, если бы вы взялись за кого-то вроде Анны за то, что она призналась: она украла на 15 000 долларов дальней связи, — вам удалось бы провести расследование, собрать доказательства и арестовать её. Какое наказание она могла бы получить?

AA: Очень сложный вопрос, потому что это зависит от её предыдущей судимости. У большинства хакеров нет истории преступлений. В случае Анны преступление квалифицировалось бы как фелония четвёртого класса, что, вероятно, вылилось бы в простое условное осуждение за фелонию.

ES: Она призналась в краже 15 000 долларов!

AA: Уверена, что её оценка резко занижена. Если она распространяет коды, то в определённой мере несёт ответственность и за использование этих кодов другими.

ES: Можно ли обвинить её в сговоре?

AA: Конечно!

ES: Она создала непрерывное преступное предприятие.

AA: Снова зависит от того, будете ли вы преследовать её на федеральном уровне или на уровне штата. Здесь она могла бы столкнуться с фелонией третьего или второго класса в зависимости от суммы похищенного.

ES: Суть в том, что если наказание не соответствует преступлению, оно не остановит преступников.

AA: Нужно помнить, что это люди, которые не прошли через систему уголовного правосудия. Даже провести их в ИВС округа Кук на выходные — это не то, что я бы желала повторить.

ES: Многие из них производят довольно высокомерное впечатление.

(Рекламная пауза и повторные представления)

ES: У нас появился новый интересный телефонный закон — глава 38 Уголовного кодекса Иллинойса. Теперь человека можно преследовать, арестовать и осудить за беспокойство кого-либо, даже если тот не ответил на звонок. Теперь просто позвонить кому-то — уже нарушение закона, это харассмент.

JM: Добавлю, раз уж мы говорим о харассменте по телефону: хакеры меня не очень любят, и я получаю примерно по одной угрозе убийством в неделю от хакеров.

ES: Правда?

JM: О да. И время от времени я выясняю, кто это был, перезваниваю ему — и это немного их встряхивает.

ES: Здесь был один журналист, которого хакер изводил звонками в нашем новостном отделе. У хакера был компьютер, который звонил на телефон как ненормальный. Я не знал об этом. В конце концов журналист спросил, что я могу посоветовать. Я сделал один звонок, служба безопасности Illinois Bell сделала что должна была, затем подключилась чикагская полиция. Однажды ночью, пока я был в эфире, офицеры поехали к этому парню домой, постучали в дверь, и мальчик был потрясён! Он оказался торговым представителем крупного журнала и, судя по всему, работал дома, держа часть их оборудования у себя, включая быстрый дозвонщик. К нему пришли двое детективов прямо в дверь, а он только что положил трубку. Все данные у нас есть. И теперь вопрос: что с ним делать? Суд? Арест? Идти к его начальнику? Я вернулся к журналисту в нашей редакции и спросил, что он хочет с этим делать.

JM: И что он сказал?

ES: Написать сочинение на 500 слов о том, почему он больше никогда так не сделает.

JM: Ха-ха! У нас был один четырнадцатилетний хакер, который вёл аккаунты на досках объявлений и публиковал сообщения о том, как делать самодельные взрывные устройства, различные яды, коды дальней связи, компьютерные пароли и тому подобное. На досках объявлений он представал как Чингисхан или Иосиф Сталин. Сплошные матерные слова. Но при личной встрече это был очень кроткий, тихий, воспитанный подросток. Однако стоило ему сесть за клавиатуру — личность как будто менялась. Что делать с четырнадцатилетним? Он слишком мал, чтобы проходить через серьёзное уголовное преследование. Его наказание состояло в том, что он должен был читать вслух родителям все сообщения, которые публиковал на досках, — со всем матом. И это его исправило... хахаха.

В большинстве дел, которые я вёл, реальное лишение свободы — редкость. Думаю, самый длительный срок, которого я был участником, — около 30 дней. Кажется, в Вирджинии был один случай — 90 дней. Не стоит обязательно сажать этих людей, потому что в камере они познакомятся с настоящими уголовниками и научат их всем своим трюкам.

ES: Не приведи господь. Возьмём быстрый звонок от Гордона. Алло, Гордон, откуда вы?

G: Алло, я звоню из ДеКалба, штат Иллинойс.

ES: У вас есть вопрос к нашей группе — прошу вас.

G: Да. Я аспирант по криминологии здесь, в Северном университете Иллинойса, и занимаюсь полевыми исследованиями, связанными с теми типами людей, о которых вы говорите сегодня вечером. Я слышал много терминов, летавших туда-сюда — «фрикеры», «хакеры» и тому подобное. Хотел бы услышать от участников группы, как они определяют эти виды деятельности, проводят ли они между ними различия, и во-вторых — может ли кто-нибудь добавить понимание того, сколько именно людей сейчас активно занимаются такими вещами.

JM: Могу ответить на это, поскольку одна из моих специализаций — идентификация и сбор данных о количестве преступников. На первый вопрос: компьютерный хакер — это тот, кто концентрируется главным образом на взломе компьютерных систем. Телефонный фрикер — это тот, кто, как Анна сегодня вечером, просто бесплатно совершает звонки дальней связи. Проблема в том, что их невозможно по-настоящему разделить. Хакеру нужно знать приёмы телефонного фрикера, чтобы взламывать компьютеры в других штатах или странах. Телефонному фрикеру, в свою очередь, возможно, нужна компьютерная помощь для получения украденных кодов. Их трудно разделить. Можно называть их фрикерами, можно — хакерами, а можно просто — преступниками.

Что касается количества — это сложный вопрос: где провести черту? Считать ли телефонным фрикером того, кто за год наговаривает на пятнадцать тысяч долларов, а тот, кто наговаривает на 14 900 — уже нет? Проблема в том, что традиция «обдирать» телефонную компанию существует с самого начала. Телефонные фрикеры существуют двадцать пять или тридцать лет. С тех пор как появилась дальняя связь.

BG: Телефонная компания — не единственная под осадой.

JM: Хакеров тысячи. Я бы сказал, только в штате Иллинойс несколько тысяч активных компьютерных хакеров.

G: Эти хакеры — активные? Можно ли сказать, что большинство из них общаются через системы досок объявлений и голосовые почтовые ящики, или это преимущественно одиночная деятельность?

JM: Есть несколько хакеров-одиночек. Собственно, в начале хакерства, 25–30 лет назад, это была одиночная деятельность. Доски объявлений изменили всё. Теперь хакеры по-настоящему в одиночку уже не действуют.

AA: Стоит добавить об этом криминальном элементе — хакерах и фрикерах: мой опыт показывает, что у нас было очень мало «чистых» компьютерных мошенничеств. Некоторые занимались только многоуровневым сбытом кодов, что выливается в огромные суммы, но очень часто мы обнаруживали, что хакеры причастны и к другим вещам. Например, к мошенничеству с кредитными картами. При обысках мы находили значительное количество незаконных веществ, оружие, другие улики других преступлений. Наверное, легко 50% наших обысков выявляют что-то помимо компьютерного мошенничества. Думаю, это интересный момент, который стоит иметь в виду.

ES: Очень важное замечание.

(Рекламная пауза и повторные представления)

R: Алло. Хотел бы позвонить и прояснить кое-что о компьютерных хакерах. Я хакер, но не преступник.

ES: Ну, мы сами разберёмся, Бобби.

R: Думаю, разберётесь. Говорю это потому, что вы смешиваете понятия. «Хакер» — это термин, который можно применить или сравнить примерно с «радиолюбителем». Это компьютерный энтузиаст, который занимается этим у себя дома или получает доступ к легальным сервисам по всей стране и платит за свои услуги, — он хакер. Есть много безответственных людей, в основном

подростков, которые весьма впечатлены мощью этих машин, увлекаются и совершают уголовные действия. Они случайно являются хакерами, но они ещё и преступники. Вот в чём разница.

CM: Думаю, это справедливое замечание. Думаю, изначально слово «хакер» было очень положительным термином, и по каким-то причинам оно приобрело некоторые негативные коннотации.

R: Да, и это несправедливо, потому что я знаю легионы людей, которые являются хакерами.

JM: Я считаю себя хакером, но точно не компьютерным преступником *(по крайней мере, не компьютерным)*. Моё дело — ловить преступных хакеров. Если вернуться к 1983 году, когда хакеры впервые попали в заголовки газет, — это была банда Milwaukee 414, они называли себя хакерами. И сразу же хорошее слово «хакер», означавшее того, кто способен делать удивительные вещи с компьютером, превратилось в обозначение того, кто способен делать преступные вещи с компьютером.

ES: Помню, несколько лет назад была арестована группа преступников, придумавших устройство под названием «чёрный ящик», которое они использовали для уклонения от оплаты международных переговоров. Это было началом компьютерного злоупотребления? Это было компьютерное устройство?

JM: Есть несколько ящиков: чёрный, синий, красный, серебряный и так далее. Должен признаться, что когда я был подростком — более тридцати лет назад, — компьютеров для игры ещё не было, зато существовала эта замечательная телефонная сеть Bell System. Я был одним из первых изобретателей устройства, известного как чёрный ящик, и другого устройства, известного как синий ящик *(ага, конечно, вы их изобрели)*. В те времена телефонная сеть была устроена так, что ею можно было манипулировать с помощью очень простых тоновых сигналов.

Чёрный ящик, по существу, позволяет получать все входящие звонки бесплатно для звонящего. Иными словами, если кто-то звонит вам с автомата — монеты ему возвращаются, а если кто-то набирает вас напрямую из другого города — счёт ему не приходит.

Синий ящик был несколько более коварен. Он позволяет фактически перехватить международные линии и звонить прямо куда угодно в мире. Я занялся этим из чистого любопытства как настоящий хакер — обнаружил, что подобное возможно, и рассказал другу на телефонной компании о том, что могу сделать с их схемами. Тот, конечно, сдал меня в службу безопасности.

Это так и не получило огласки, но передо мной сейчас лежит устройство, которое воспроизводит некоторые из тех тонов. Можно назвать его синим ящиком. Полагаю, это законное тестовое оборудование, но посмотрим, сработает ли. *(Бееееп!)*

ES: Прошло громко и чисто.

JM: Синий ящик сегодня устарел, по-настоящему не работает. Есть несколько схем, которые всё ещё используют такие сигналы, но 25–30 лет назад именно так делали бесплатные звонки. Не было ни Sprint, ни MCI, которые можно было бы обирать.

S: Сейчас я инженер-консультант, но в прошлом был руководителем службы связи в трёх компаниях из Fortune 500. Одной из причин, по которой меня наняли, была необходимость остановить определённую активность звонков дальней связи, которая обошлась той компании свыше полутора миллиона долларов за 27 месяцев. Мы нашли человека, который это делал, и он получил условный срок шесть месяцев. Затем мы обратились в гражданский суд с иском к нему.

ES: Нам нужно начать обращаться с этими преступниками как с преступниками. Условные сроки недопустимы. Реальный тюремный срок — абсолютно обязателен. К сожалению, — и думаю, сержант, вы, вероятно, согласитесь со мной, — должно быть очень обидно тратить столько часов на преследование людей и даже когда они признают себя виновными — видеть, как легко порой они отделываются.

AA: О, конечно.

S: Сколько человек в вашем отделе здесь, в штате, сержант?

AA: Вы разговариваете с 50% отдела.

(Рекламная пауза и повторные представления)

ES: Ладно, Рэй, прошу вас.

R: Вы не поверите, как давно я пытаюсь до вас дозвониться. С 14 лет каждый раз, когда я звонил, линия была занята.

ES: И сколько вам сегодня вечером?

R: 18.

ES: Четыре года?! О чём вы думаете?

R: Я раньше пиратил игры, когда был моложе. Да, в 14 лет. То есть папа только что купил мне компьютер и модем, и я был в полном восторге. Люди всегда жалуются на это, но четырнадцатилетнему это сделать так легко — не думаете ли вы, что стоило бы немного усложнить задачу?

ES: Да, но, Рэй, угнать машину тоже легко. Если сосед оставил машину на подъездной дорожке с ключами в замке зажигания, это даёт вам право её взять?

R: Я знаю, что поступал неправильно, но вернуть уже невозможно. Это просто глупо — когда взрослеешь, начинаешь чувствовать вину за прошлое.

ES: Что именно вы делали?

R: Я звонил в определённые места, взламывал их и забирал игры себе.

BG: Это было для вас скорее развлечением?

R: Это занимало меня, и это было так легко, что я начал думать, что, может, это нарочно сделали лёгким — ради рекламы.

JM: Есть, пожалуй, разница: когда вы копируете компьютерную программу, её не отличить от оригинала, тогда как копия кассеты или пластинки звучит несколько иначе.

CM: Когда тебе 14, это что-то новое, верно?

R: Это давало мне огромный заряд.

CM: Думаю, вы делали кое-что для своего эго, и это давало вам ощущение власти.

ES: Ладно, Рэй.

R: Пока.

ES: Программа мне очень понравилась, но время вышло. Джон, хочу поблагодарить вас за то, что не ложились спать. У меня чувство, что мы продолжим делать радио, потому что вы — интересный человек.

JM: Спасибо. Было интересно общаться. Кстати, думаю, знаю, кто такая Анна, но сохраним это в тайне от слушателей.

ES: О. Тогда почему бы просто не рассказать ФБР?

JM: Секретной службе — да.

ES: Верно. И хочу поблагодарить всех за участие в сегодняшнем шоу.

Все: Было очень приятно. Давайте повторим это когда-нибудь.

Phrack Inc.

Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN The Legacy...                         ...Lives On PWN
PWN                 Phrack World News                 PWN
PWN                    Issue XXI/1                    PWN
PWN                                                   PWN
PWN           Created by Knight Lightning             PWN
PWN                                                   PWN
PWN              Written and Edited by                PWN
PWN          Knight Lightning and Epsilon             PWN
PWN                                                   PWN
PWN The Future...                      ...Is Forever PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning и Epsilon

На краю вечности — 4 ноября 1988 г.

Приветствуем вас в выпуске XXI Phrack World News! Как большинство из вас уже заметили, Taran King и я вернулись всерьёз и надолго, и традиция Phrack Inc. продолжается. 17 ноября 1988 года Phrack Inc. исполняется три года, и мы как никогда гордимся своими усилиями по выпуску лучшего из возможных журналов.

Однако в одиночку нам не справиться. Мы оба с Taran King вернулись к полностью законопослушному образу жизни и не можем позволить себе роскошь звонить на BBS или поддерживать контакт со всеми людьми, с которыми хотели бы общаться.

Epsilon очень помогает нам, выступая в роли собирателя материалов для Phrack и ряда новостных статей. Пожалуйста, если у вас есть файл для Phrack Inc. или статья для PWN — свяжитесь с ним или оставьте письмо The Mentor. Кстати, у The Phoenix Project новый номер: (512) 441-3088. Обязательно позвоните.

Статья о Pacific Bell в этом выпуске может содержать информацию, которую некоторые из вас уже видели. Тем не менее PWN — это место, где подобная информация архивируется для последующего обращения и помогает сохранять важные события в определённой последовательности, что полезно для всех.

В этом выпуске Phrack представлена Вторая специальная презентация Phrack World News — сокращённая версия радиошоу WGN, посвящённого хакерам, в которой участвовал John Maxfield.

Относительно статьи о Teleconnect Long Distance: Hatchet Molly сообщает, что теперь Teleconnect «помечает» подозрительные BBS, и если для звонка на одну из них используется карточка Teleconnect, её номер аннулируется, а в течение трёх дней клиенту по почте высылается новая карточка. Какая замечательная корпоративная политика.

В ближайшие месяцы я работаю над материалом о хакерах за рубежом — главным образом о Chaos Computer Club, с которым у меня завязываются крепкие связи, а также о других хакерских явлениях в Европе и других частях света.

На январь/февраль запланирована серия файлов о глобальных сетях: Bitnet и, возможно, ARPAnet, MILInet, NSFnet, IBM VNET, CCnet, UUCP, CSnet, SPAN, JANet, JUNet и так далее. Основной акцент будет сделан на Bitnet, второй по значимости — на UUCP и остальных сетях.

Надеемся, этот выпуск вам понравится, и помните: «The Future Is Forever».

:Knight Lightning

Pacific Bell настроена серьёзно — 6 октября 1988 г.

Следующая информация изначально появилась в WORM Newsletter, издании Sir Francis Drake. Представленная здесь серия служебных записок демонстрирует участникам современного хакерского сообщества в полной мере понять силы, которые действуют против них. Записки отредактированы для данной публикации. —KL

Кому: Roland Donaldson — **3 августа 1987 г.**
Тема: Несанкционированный удалённый доступ к компьютерам

Сан-Франциско, 29 июля 1987 г.
Дела №: 86-883, 87-497

T. M. CASSANI, директор — Electronic Operations:

Electronic Operations недавно расследовала два дела с участием ряда опытных хакеров, умело незаконно проникавших в компьютеры государственного и частного секторов. Среди жертв этих хакеров оказались Pacific Bell, а также другие местные операторы телефонной связи и провайдеры дальней связи.

Ниже приводится краткое изложение двух дел (87-497 и 86-883), каждое из которых демонстрирует слабые места в системах удалённого коммутируемого доступа Pacific Bell.

Дело № 87-497

14 мая 1987 года Electronic Operations получила судебный ордер, предписывающий Pacific Bell установить ловушки на телефонные номера компании «Santa Cruz Operations». Ордер был выдан с целью установить номер телефона, с которого некое лицо незаконно проникало в компьютер Santa Cruz Operations и похищало информацию.

28 мая 1987 года один и тот же телефонный номер пять раз был зафиксирован при попытке незаконного входа в компьютер Santa Cruz Operations. Исходящий номер — 805-PRE-SUFF, зарегистрированный на имя Jane Doe, 8731 W. Cresthill Drive, кв. 404, Thousand Oaks, Калифорния.

3 июня 1987 года по адресу 8731 W. Cresthill Drive, кв. 404, Thousand Oaks, Калифорния, был произведён обыск. Жильцы квартиры, которых не оказалось дома, были установлены: Jane Doe, программист General Telephone, и Kevin Hacker, известный хакер. В квартире были обнаружены три компьютера, многочисленные дискеты и ряд руководств по компьютерным системам General Telephone.

Kevin Hacker несколько лет назад был арестован за взлом компьютеров Pacific Bell, UCLA и Hughes Aircraft Company; на момент ареста он был несовершеннолетним. Впоследствии Kevin Hacker был снова арестован за взлом базы данных Santa Cruz Operations.

Изъятые дискеты выявили причастность Mitnick к компрометации UNIX-операционных систем Pacific Bell и других баз данных. На дисках было задокументировано следующее:

• Взлом Hacker'ом всех компьютеров SCC/ESAC в Южной Калифорнии. В файлах хранились имена, логины, пароли и домашние телефонные номера сотрудников ESAC Северной и Южной

Калифорнии.
• Номера дозвона и идентификаторы схем для компьютеров SCC и Data Kit.
• Команды для тестирования и захвата тестовых транковых линий и каналов.
• Команды и логины для COSMOS wire centers Северной и Южной Калифорнии.
• Команды для прослушивания линий и захвата dial tone.
• Ссылки на случаи выдачи себя за агентов безопасности Южной Калифорнии и сотрудников ESAC с целью получения информации.
• Команды для установки терминирующих и инициирующих ловушек.
• Адреса объектов Pacific Bell и коды электронных дверных замков для следующих центральных офисов Южной Калифорнии: ELSG12, LSAN06, LSAN12, LSAN15, LSAN23, LSAN56, AVLN11, HLWD01, HWTH01, IGWD01, LOMT11 и SNPD01.
• Внутренняя электронная почта с описанием новых процедур логина/пароля и мер защиты.
• Рабочий файл UNIX-взломщика шифрования. В случае успеха эта программа могла бы вскрыть любую UNIX-систему по желанию.

Дело № 86-883

14 ноября 1986 года Electronic Operations получила ордер, предписывающий Pacific Bell устанавливать ловушки на звонки к компьютеру Стэнфордского университета. Этот компьютер незаконно использовался для доступа к другим крупным компьютерным системам по всей стране.

Звонки к компьютеру Стэнфорда маршрутизировались через нескольких операторов связи и через многочисленные штаты. Путём комбинации ловушек, трассировок и анализа информации, опубликованной на Стэнфордском компьютере, по всей территории Соединённых Штатов было установлено несколько подозреваемых.

Группа хакеров, незаконно получивших доступ к Стэнфордской компьютерной системе, была известна под названием «Legion of Doom». Последующее расследование показало, что Legion of Doom несёт ответственность за:

• Использование высокопроизводительных мейнфреймов Стэнфордского университета для атаки и взлома мини-компьютеров ESAC/SCC с помощью файла взломщика паролей UNIX. Файлы паролей затем хранились на Стэнфордских системах для использования другими членами Legion of Doom. Логины и пароли для каждого местного оператора, а также мини-компьютеров AT&T SCC/ESAC находились в хранилище.
• Использование Legion of Doom компьютеров Стэнфорда для проникновения в компьютеры других учреждений и частных подрядчиков. Некоторые компьютеры подрядчиков использовались для исследований в области национальной обороны.

21 июля 1987 года в трёх штатах по местам проживания членов Legion of Doom было проведено восемь обысков. Три из них прошли в Калифорнии. Steve Dougherty, старший следователь Electronic Operations, сопровождал агентов Секретной службы при проведении обыска по адресу 2605 Trousdale Drive, Burlingame, Калифорния — по месту жительства Stan QUEST, шестнадцатилетнего члена Legion of Doom.
(Поправка — Oryan QUEST никогда не был членом Legion of Doom. —KL)

Dougherty допросил QUEST, который при доступе к компьютерам использовал псевдоним «O'Ryan Quest» (Oryan QUEST). В ходе допроса QUEST признал следующее:

• Проникновение в центральные офисы (Burlingame, San Mateo, San Bruno, Millbrae) под видом курьера Federal Express. Цель визитов — разведка обстановки в центральных офисах: поиск компьютерных терминалов с телефонами, расположения коммутаторов и стоек, имён техников, а

также материалов, связанных с работой центрального офиса. QUEST также утверждал, что побывал в административном офисе AT&T на Folsom Street в Сан-Франциско.
• Телефонная связь QUEST дважды отключалась за неуплату, и оба раза он восстанавливал её, выдавая себя за представителя службы.
• Обучение тестированию схем и транков с помощью компьютера с использованием процедур тестирования ROTL и CAROT.
• Члены Legion of Doom нередко получали доступ к тестовым транкам, чтобы из интереса прослушивать линии друг друга.
• В ряде случаев QUEST публиковал номер телефона-автомата для доступа к своей BBS Digital IDS, а затем обращался к COSMOS wire center в Millbrae и добавлял переадресацию вызовов на этот автомат. Он активировал переадресацию на свой домашний номер, скрывая таким образом своё местонахождение.
• QUEST выдавал себя за сотрудника, имеющего право пользоваться Data Kit, и добивался его включения. Закончив, он перезванивал и просил отключить Data Kit.
• QUEST также пользовался своими знаниями, чтобы отключать и блокировать телефонные услуги неприятных ему людей. Кроме того, он добавлял к их линиям несколько дополнительных платных опций, увеличивая тем самым их счета.
• С помощью тестовых транков и компьютера было очень легко захватить чужой dial tone и записать звонки на чужой счёт. QUEST не признал, что записывал на кого-либо звонки на номера 976, однако знал о других, кто это делал.
• При атаке на компьютерную систему Legion of Doom отводил себе пять минут на выполнение взлома. Если за это время добиться успеха не удавалось, они переходили к следующей системе. Legion of Doom удавалось взломать компьютер менее чем за пять минут примерно в 90% случаев.
• QUEST выдавал себя за сотрудников, чтобы получать закрытые телефонные номера. Ему удалось получить закрытый номер основателя Apple Computer Стива Возняка и членов рок-группы The Beastie Boys.
• QUEST рассказал Dougherty об одном нью-йоркском члене Legion of Doom — «Bill from Arnoc» (Bill From RNOC), который самостоятельно устанавливал ловушки в Нью-Йорке. Bill from Arnoc (Bill From RNOC) помогал QUEST устанавливать ловушки в Pacific Bell.

(Ну и ну, Стэн, ты забыл упомянуть о нелегальном переходе границы. —KL)

Анализ вещественных доказательств, изъятых у QUEST, в целом подтверждает все его показания.

Выводы

Из вышеизложенных двух дел можно сделать ряд важных выводов относительно будущих проблем компьютерной безопасности.

• Число людей, способных проникнуть в операционные системы Pacific Bell, растёт.
• Хакеры совершенствуют методы своих атак.
• Коммутируемые порты всегда будут привлекательной целью для хакерского проникновения.
• Даже коммутируемые порты с обратным вызовом и модемами с ручным управлением могут быть скомпрометированы.
• Хакер может вывести центральный офис из строя, перегрузив мини-компьютер SCC путём некорректной установки ловушек или расстановки ловушек на нескольких группах DID multi-trunk, например группах MCI или Sprint.
• Террористические или организованные преступные группировки могут использовать эти подпольные компьютерные технологии против Pacific Bell или в собственных интересах.
• Проприетарные базы данных Pacific Bell, такие как PTT ESAC или PB2 ESAC, могут быть скомпрометированы.

• Достоверность счетов за услуги связи была поставлена под сомнение в результате доступа к CEBS (Computerized Electronic Billing System) и останется таковой. Клиент может оспорить крупные звонки с прямым набором, заявив, что его телефон был задействован хакером.

(Oryan QUEST — невероятно болтлив и готов подставить кого угодно, лишь бы избавиться от комплекса неполноценности нелегального эмигранта без грин-карты. За исключением истории с Dan The Operator/Maxfield, я не видел такого массового самопризнания в вине. И что ещё хуже — QUEST, по всей видимости, сам выдумал большую часть этих историй, чтобы казаться крутым хакером. —KL)

Рекомендации

Информация, полученная в ходе вышеуказанных расследований, должна быть доведена до сведения лиц, ответственных за целостность наших компьютерных систем. Кроме того, необходимо установить и поддерживать постоянное деловое партнёрство между службой безопасности и подразделениями, отвечающими за защиту компьютерных систем, для своевременного и эффективного решения будущих проблем компьютерной безопасности.

JOHN E. VENN
Руководитель — Electronic Operations

Особая благодарность Sir Francis Drake

Он совсем вышел из-под контроля — PostCon'88

> *«Я бы УНИЧТОЖАЛ всё подряд, потому что мы вытаскиваем из мусорных баков столько информации, что это просто НЕРЕАЛЬНО...»*
> *— Control C*

На протяжении последних нескольких месяцев вокруг таинственных обстоятельств, связанных с Michigan Bell и Control C, велось немало споров. Чтобы расставить всё по местам, ^C передал мне все подробности произошедшего.

Незадолго до отъезда из Чикаго, где ^C учился, он незаконно получил доступ к системе AOL, принадлежащей Michigan Bell. Системный оператор прервал его сеанс, и ^C безуспешно пытался выдать себя за легитимного пользователя. Когда это не удалось, он повесил трубку и не придал случившемуся особого значения. Вернувшись домой в Детройт, он обнаружил у себя сообщение с просьбой связаться с сисопом системы AOL. Он позвонил, и они вместе с представителями безопасности Michigan Bell встретились за обедом. Чтобы избежать уголовного преследования, Control C был вынужден раскрыть всю имевшуюся у него информацию о той системе и объяснить, как ему удалось туда проникнуть. Поскольку он сотрудничал, его отпустили без дальнейших последствий. К сожалению, вскоре Control C снова попался — на этот раз за проникновение в свой местный центральный офис, и теперь ему так легко отделаться не удалось. Он был вынужден согласиться на участие в телевизионном ток-шоу и создание плаката (процитированного в начале статьи) для Michigan Bell. Оба материала были распространены по всей стране, чтобы наглядно продемонстрировать хакерский образ мышления и напомнить о необходимости уничтожать важные документы перед выбрасыванием.

В ходе допроса, проведённого службой безопасности Michigan Bell, Control C был показан список недавно задержанных хакеров в ходе общенационального рейда 21 июля 1987 года. В этом списке числился Sir Francis Drake — именно так и появился слух о том, что SFD был арестован в прошлом году. Однако ни Control C, ни Michigan Bell не знали, что когда Mark Gerardo был задержан в прошлом году, его приняли за SFD и ввели в базу данных под ошибочным именем.

Информация предоставлена Control C

С небольшой помощью в разгадке путаницы с SFD от меня и Taran King

:Knight Lightning

Кошмар Северной Дакоты — 10 сентября 1988 г.

> *«За кражу документов Kracking Crue игра для Docs Avage окончена»*

В марте 1987 года члены Kracking Crue из Северной Дакоты (Docs Avage и SpyroGyra, известный также как Ractor) обнаружили местный экстендер и смогли подобрать к нему код. Оба жили в кампусе Государственного университета Северной Дакоты и могли безнаказанно злоупотреблять кодом, поскольку телефонная система Dimension, установленная в кампусе, обеспечивала им высокую степень анонимности.

Они использовали этот код до конца всего учебного года, и ничто не мешало им делать это. Из-за отсутствия мер безопасности DA и SG начали полагать, что код будет в безопасности при использовании из любого места. Учебный год закончился, члены Crue разъехались по домам. В конце концов они обнаружили номер 1-800 для того провайдера дальней связи, которым злоупотребляли, и снова начали им пользоваться. Однако вскоре им предстояло убедиться, что они вовсе не так защищены, как думали.

Провайдер LD всё это время следил за кодом, но не мог поймать Crue с поличным из-за системы Dimension в кампусе NDSU. Docs Avage начал пользоваться кодом из своей квартиры, чтобы звонить SpyroGyra и ещё нескольким людям, — и компания поставила на его линию прослушку и вела записи всех его звонков.

Словами самого Docs Avage:

> *«27 июля 1988 года я вернулся в свою квартиру после выходных у родителей. Меня несколько удивило, что на парковке стоят три лишних машины, одна из которых — Dodge Diplomat.*
> *Войдя в квартиру, я обнаружил двух детективов, двух телефонных чиновников и двух "компьютерных экспертов", с упоением разбиравших мой Apple и всю периферию. Один из моих соседей был в наручниках и сидел на стуле, второго держали под неусыпным наблюдением на кухне. Меня спросили, кто я такой, и зачитали мои права. Я согласился сотрудничать. Меня поймали на дозвоне.*
> *Том самом дозвоне, который я взломал несколько месяцев назад и которым злоупотреблял с избытком (ладно, признаю — я перегнул палку с этой штукой). В своей квартире я наговорил с его помощью примерно на 1000 долларов. Я звонил через него и раньше, но не в таких масштабах.*
> *Я был полностью готов сотрудничать и поговорил с несколькими представителями телефонных служб безопасности, в том числе из AT&T и U.S. Sprint (у меня была распечатка 4 кодов Sprint — никогда ими не пользовался, просто хранил). Сотрудники безопасности — настоящие специалисты по психологическому давлению, и должен признать, что запугать меня им удалось весьма неплохо. Тем не менее я понимал, что*

они просто играют на нервах, поэтому всё обошлось не так страшно, как могло.
Мой сосед был обвинён в том же преступлении, что и я, — краже услуг связи, фелония класса C (макс. 5 лет / 5000 долларов). При этом его единственная причастность к делу заключалась в том, что телефонный счёт был оформлен на его имя. Обвинения с него сняли.
Почти через два месяца ожидания настал день вынесения приговора. Я признал себя виновным в рамках сделки, которую мой адвокат заключил с прокуратурой. Приговор включал возмещение ущерба (сумма ещё не определена). Телефонная компания изо всех сил старается повесить на меня крупный счёт за услуги, моя причастность к которым не доказана; счёт может достигать 5000 долларов (чёрт возьми, если я столько заплачу), плюс весьма занятная оговорка под названием Deferment of Imposition. По сути, я остаюсь на испытательном сроке до полного погашения реституции, после чего смогу пройти слушания, доказать отсутствие рецидива, и тогда судимость не будет внесена в мою запись. Пока же — ежемесячные выплаты под надзором пробационного офицера. Само собой разумеется, я, Docs Avage, ушёл на пенсию — по крайней мере настолько, насколько это возможно при моём положении.»

Docs сказал, что уже какое-то время подумывал уйти, и этот инцидент стал последней каплей. Он также добавил, что его спрашивали о Jester Sluggo, Phrack Inc. и Legion of Doom. Он ничего не знал.

Информация предоставлена Docs Avage и SpyroGyra

Phrack World News

```
  PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
  PWN The Legacy...                         ...Lives On PWN
  PWN                 Phrack World News                 PWN
  PWN                    Issue XXI/2                    PWN
  PWN                                                   PWN
  PWN            Created by Knight Lightning            PWN
  PWN                                                   PWN
  PWN               Written and Edited by               PWN
  PWN           Knight Lightning and Epsilon            PWN
  PWN                                                   PWN
  PWN The Future...                       ...Is Forever PWN
  PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Авторы: Knight Lightning и Epsilon

Программисту предъявлено обвинение в «заражении» компьютеров

24 мая 1988 г.

Форт-Уэрт, Техас (AP) — 39-летнему программисту предъявлены уголовные обвинения в заражении компьютеров своего бывшего работодателя электронным «вирусом»; в случае признания виновным ему грозит до 10 лет лишения свободы.

Дональду Джину Бёрлесону предъявлено обвинение в «противоправном доступе к компьютеру»; он находится на свободе под залогом в 3 000 долларов в ожидании суда, назначенного на 11 июля.

Полиция квалифицировала электронное вмешательство как «массовое уничтожение» более 168 000 записей о торговых комиссионных выплатах сотрудникам.

По словам Дэвиса Маккауна, начальника отдела по экономическим преступлениям окружной прокуратуры округа Таррант, Бёрлесон, по всей видимости, стал первым человеком, которому предъявлено обвинение по государственному закону о компьютерном саботаже, вступившему в силу 1 сентября 1985 года — примерно за три недели до предполагаемого инцидента.

Начался отбор присяжных на первом процессе по делу о вирусе

6 сентября 1988 г.

Из Washington Post (7 сентября 1988 г.), стр. C-1

Форт-Уэрт, Техас (AP) — Сегодня начался отбор присяжных на уголовный процесс над 40-летним программистом, обвиняемым в том, что он с помощью компьютерного «вируса» уничтожил тысячи записей на своём бывшем месте работы. Ожидается, что процесс продлится около двух недель.

Дональду Г. Бёрлесону в случае обвинительного приговора грозит до 10 лет заключения и штраф в размере 5 000 долларов — это первый подобный процесс в компьютерной индустрии. Бёрлесон был обвинён в краже со взломом и противоправном доступе к компьютеру в связи с причинением ущерба компьютерной системе брокерской фирмы, сообщила Нелл Гаррисон, секретарь уголовного суда штата в Форт-Уэрте. Через своего адвоката Джека Бича Бёрлесон отрицает

обвинения, но отказался от дополнительных комментариев.

По гражданскому иску против Бёрлесона фирма уже получила 12 000 долларов. По словам Гаррисон, на сегодня были запланированы предварительные слушания, за которыми последовал отбор присяжных.

Бёрлесону вменяется внедрение компьютерной программы, известной как вирус, в компьютерную систему компании USPA&IRA Co. через два дня после своего увольнения. Вирус — это компьютерная программа, нередко скрытая в внешне обычном программном обеспечении, которая даёт компьютеру команду изменить или уничтожить информацию в заданное время либо после определённой последовательности команд. По утверждению руководства USPA, Бёрлесон однажды ночью проник в офис компании и внедрил в компьютерные записи вирус, который должен был ежемесячно стирать данные о торговых комиссионных. Вирус был обнаружен через два дня, к тому моменту он уже уничтожил 168 000 записей.

White Lightning высказывается

28 июля 1988 г.

White Lightning ранее был, по всей видимости, обвинён в том, что он является осведомителем службы безопасности Sprint в отношении сведений, касающихся The Disk Jockey и Compaq.

Он оставил следующее сообщение в голосовой системе Phrack:

> *«Да, это White Lightning. Я хотел бы сделать официальное заявление для Phrack Magazine. Что касается того, что случилось с The Disk Jockey, — чёрт, я понятия не имею, ладно? Я появляюсь в бридже, пропадал две недели, появляюсь в пятницу вечером, и, блин, этот парень Laser из 206-го говорит, что я его сдал, — я ничего об этом не знаю, ладно? Что касается Compaq из 219-го, Кент, я просто прошу тебя — твоя информация неверна.. [В голосовой системе Phrack есть сигнал, предупреждающий, что у вас осталось 10 секунд.] Что это за чёрт?! Алло?! Кто это?!»*

Сообщение для White Lightning от Phrack Inc.:

> *Если вы захотите изложить свою версию событий более чётко, мы с удовольствием вас выслушаем. Уверены, что это будет интересно всем. Спасибо.*

Информация предоставлена White Lightning

AT&T; объединяется с GTE

1 августа 1988 г.

AT&T усиливает усилия по наращиванию доходов от телекоммуникационного оборудования, приобретая бизнес телефонных коммутаторов GTE. AT&T станет ведущим поставщиком оборудования для телефонных компаний GTE, которые являются основным источником дохода коммутационного бизнеса, приносящего 500 миллионов долларов в год.

AT&T получит долю в 49% в новой компании, которая объединит производственные мощности GTE по выпуску коммутаторов в Иллинойсе и научно-исследовательский центр в Финиксе, Аризона. GTE, в чьём бизнесе занято 5 000 человек, рассчитывает на техническую экспертизу AT&T для поддержки своей базы телефонных коммутационных систем. Кроме того, GTE стремится выйти из

бизнеса телефонного оборудования. Главная задача AT&T — сделать коммутаторы способными справляться с масштабными требованиями по передаче голоса и компьютерных данных, которые прогнозируют телефонные компании GTE на следующие 15 лет.

Ни один из партнёров не раскрыл финансовых условий совместного предприятия. Однако к 1993 году AT&T будет владеть 80% компании, а к 2003 году — 100%. Структура управления пока не определена. GTE в последние годы совершала аналогичные сделки, которые в итоге приводили к передаче полного управленческого контроля и собственности партнёрам. В числе таких сделок — соглашение с западногерманской Siemens в области продуктов для передачи данных и второе — с японской Fujitsu в области офисных телефонных систем.

Информация предоставлена журналом Business Week

Есть ли в зале доктор?

1 августа 1988 г.

Всё началось, когда я встретил его в бридже в Техасе. Никто по-настоящему не понимает, зачем он это сделал и почему выбрал именно этот псевдоним. Судя по всему, у него есть неплохие знания, и добиться высокой известности ему не составило бы большого труда. Если только за этим не кроется нечто большее.

Doc Holiday/Scott из 713 — САМОЗВАНЕЦ!

Он довольно убедительно притворялся настоящим Doc Holiday. Он тщательно изучил всё о нём, включая подробности недавнего ареста за злоупотребление COSMOS, и придумал обрамляющую историю, объясняющую, как и почему он теперь Скотт, а не Робби, и как его семья переехала из Теннесси в Техас. Большинство участников сообщества фриков и хакеров поверило этой истории, и он продолжал бы оставаться неразоблачённым, если бы не вернулись некоторые люди, исчезнувшие прошлой осенью: Knight Lightning и Taran King. Услышав о некоем Doc Holiday из 713-го, они уже подозревали, что он ненастоящий, и после разговора с ним убедились: это не тот Doc Holiday. Чтобы поставить смешную точку в этом фарсе, они выждали, пока смогут связаться с настоящим Doc Holiday и посвятить его в разоблачение.

Как бывает по воле судьбы, настоящий Doc Holiday был в отпуске и оказался в Сент-Луисе на выходных, сразу после SummerCon '88. Все трое встретились, заставили Scott Holiday продолжать наговаривать на себя, а затем предоставили НАСТОЯЩЕМУ Doc Holiday возможность представиться и насладиться победой.

Scott Holiday поначалу был потрясён и попытался объяснить, что у него были веские причины так поступить, но к телефону подошла его мать, и ему пришлось уйти.

После этого инцидента я поговорил с ним голосом, и он объяснил мне, что ему нравилось всё это, и назвал это «самой крутой аферой», которую он когда-либо провернул, — хотя можно поспорить, что по-настоящему провернуть её ему не удалось. Поскольку Scott весьма искусен в социальной инженерии, ему не составило особого труда убедить (за неимением лучшего слова) людей, незнакомых с настоящим Doc Holiday. Однако столкнувшись с лучшими из лучших, он с треском провалился.

Смысл публикации этого инцидента — задокументировать, что людей легко можно обмануть, и что обман среди телефонных фриков не ограничивается только телефонными компаниями. Помните: люди не обязательно те, за кого себя выдают, и в этом заключается величайшая истина.

Информация предоставлена Epsilon

Особая благодарность Knight Lightning и Taran King за разоблачение.

Канада аннулирует The Underlord

3 августа 1988 г.

«Я всё равно хакерствую!»

The Underlord проснулся 11 февраля 1988 года в 7:30 утра от звонка в дверь. Несколько мгновений спустя его мать вошла в комнату и сообщила, что его ждут трое мужчин. Выражение её лица было довольно растерянным. Он набросил одежду и сбежал вниз, чтобы встретить свою судьбу лицом к лицу. «Толстяк» предъявил ему ордер на обыск и сообщил, что он арестован по 7 статьям обвинения. Всё было конфисковано.

The Underlord был препровождён в машину (его мать шла следом) и доставлен в полицейский участок. Ему что-то говорили про камеры по всему участку, но ему было всё равно, потому что, как он сам сказал: «Я всё равно не собирался никого убивать». Оттуда его отвели в небольшую комнату, где он слышал, как полицейские возятся с его компьютером, телефоном и лентами, которые они конфисковали.

Ему пришлось просидеть там в одиночестве четыре часа, пока отец не отвёз его домой и не показал ему бумаги.

> *«Мне сказали, что мне предъявлены четыре обвинения в "краже средств телекоммуникации" (это реальный закон в Канаде) и три обвинения в хулиганстве».*

По его словам, обвинения в хулиганстве были связаны с тем, что он звонил на экстренный номер 911 (хотя он утверждал, что делал это через АТС) и говорил непристойности вместе с другом по трёхстороннему звонку.

Примерно через шесть месяцев, 16 июня 1988 года, The Underlord наконец получил всё обратно и явился в суд. Он должен был заплатить 750 долларов в общей сложности и отбыть восемь месяцев испытательного срока. При этом в его деле значились только три обвинения в хулиганстве.

Он объяснил, что в Канаде, если правительство хочет взыскать штраф, оно сначала должно доказать, что у человека достаточно средств для его уплаты. UL таких средств не имел, и власти согласились снять обвинения, если он заплатит 750 долларов.

Информация предоставлена The Underlord 416 через The Phoenix Project

---

Группа подростков-хакеров набрала огромный телефонный счёт

7 октября 1988 г.

Автор: Роберт Мейси (Associated Press)

Лас-Вегас, Невада — Десять подростков-хакеров, возможно, наговорили телефонных звонков на сумму до 650 000 долларов, обманув компьютеры телефонной компании; их родители могут быть привлечены к ответственности за оплату счёта, сообщили представители властей.

Том Спёрлок, старший оперативный агент отделения Секретной службы в Лас-Вегасе, сообщил, что подростки применяли Blue Boxing — технику, позволявшую им общаться с другими хакерами по всей Европе.

Подростки не были задержаны и не были привлечены к ответственности, однако их компьютеры были изъяты. Спёрлок сказал, что решение о взыскании ущерба будет за AT&T после получения окончательных подсчётов.

Вирус поразил Unix в Bell Labs

13 мая 1988 г.

В пятницу 13-го разрушительный вирус поразил Bell Labs в Мюррей-Хилл. Первые сообщения от выживших свидетельствуют о том, что разрушения оказались весьма масштабными, хотя и ограничились рабочими станциями Sun. По слухам, вирус был внедрён недовольным сотрудником Sun в ядро Sun Unix. Реальный объём потерянных данных неизвестен, как и политика Murray Hill в отношении частоты резервного копирования дисков.

Перевод материала из журнала 2600

Осень 1988 г.

Следующий текст появился на странице 46 журнала 2600 Magazine, том 5, номер 3. Он был на немецком языке, и я позволил себе попросить приятеля — члена Chaos Computer Club в Германии — перевести его для PWN.

«Хакер» снова на свободе

Один из руководителей гамбургского CCC, С. Вернери, был освобождён из парижской тюрьмы. 26-летний мужчина прибыл вчера в гамбургский аэропорт (когда именно — в статье даты не было). Он заявил, что обвинения против него всё ещё расследуются. После допроса судьёй он был освобождён под залог, однако обязан явиться в Париж по первому требованию.

:Knight Lightning

Краткие новости

1. ВАЖНО! Новый каталог Telecom Library! 1-800-Library. Бесплатно, 125 книг и другое.

2. The Teleconnect Dictionary: глоссарий телекоммуникационных аббревиатур, терминов и жаргона. Не просто определения — мини-эссе. $9.95 — 1-800-LIBRARY.

3. Демонстрационные номера Microlog — компания Microlog из Ирвайна, Калифорния, производит оборудование для голосового ответа. Номера для демонстрации:

• Microlog — (800)562-2822
• Служба иммиграции и натурализации — (800)777-7770
• Посольство Канады — (202)785-1431
• Управление по личному составу — (202)653-8468
• Консульство Австралии — (202)797-3161

4. Наиточнейшее время в мире: (303)499-7111. Синхронизировано с атомными часами Национального бюро стандартов в Боулдере, Колорадо.

5. Подать в суд на Почтовую службу США? Удачи.
Если Почтовая служба США потеряет посылку, отправленную экспресс-почтой, вы не сможете взыскать убытки так, как это можно сделать с другими курьерскими службами.
Причина: правительство США обладает иммунитетом от судебных исков, за исключением случаев, когда само на это соглашается. Почтовая служба сохранила этот иммунитет.

6. Объявляется о запуске новой электронной почтовой службы Sub-Etha. Она принадлежит и управляется Компьютерным клубом Ольденбурга, Западная Германия.

Номер телефона: (0441/777397), 300 бод, N/8/1