Phrack RU issue 023

Русская версия Phrack, выпуск 023. Полный текст статей с кодом и таблицами.

Темы выпуска: сети, маршрутизация, TCP/IP, Cisco, телефония и телеком-инфраструктура; культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; справочники, индексы, аббревиатуры и архивные материалы; социальная инженерия, carding, физический доступ и практические схемы.

Материалы выпуска: Содержание; Phrack Pro-Phile XXIII; Subdivisions («Подразделения»); Утопия; Основы на горизонте; Индексный файл UTOPIA 1; UTOPIA Index File 2 — Члены сети BITNET; Серьёзный взгляд на взлом VMS; Можете ли вы узнать, прослушивается ли ваш телефон?; Big Brother Online; Phrack World News; Хакеры — новое социальное движение?

29 декабря 1988.

Содержание

Автор: Knight Lightning & Taran King

25 января 1989 года

Приветствуем вас снова! Прежде чем мы перейдём непосредственно к выпуску, мы здесь, в Phrack Inc., хотели бы ответить на некоторые вопросы и комментарии, которые в последнее время поступали к нам относительно прошлого номера Phrack Inc.

Узнав, что у некоторых возникают трудности при использовании программы Unix Password Hacking Program, мы решили связаться с её автором и получили следующий ответ:

> *«Мой взломщик паролей скомпилируется на чём угодно. Я запускал его на Xenix, Unix System V 3.1 и BSD 4.3. Похоже, кто-то просто не знает, что делает. Ставлю на то, что он прекрасно работает на любой разновидности Unix.»*

Что касается файла Red Knight'a по Unix и «Руководства начинающего хакера» The Mentor'a — мы понятия не имели, что эти файлы также были отправлены в P/HUN и там распространялись. Статья об «Интернет-черве» была опубликована в Bitnet, и мы сочли её достаточно значимой, чтобы предать огласке. Читатели, возможно, захотят отметить, что в томе 5, номере 4 журнала 2600 Magazine статья об «Интернет-черве» и файл Red Knight'a по взлому Unix были также переизданы.

В этом выпуске обратите внимание на финальную главу трилогии «Порочный круг» (Vicious Circle Trilogy), а также на начало «Саги о грядущем будущем» (Future Transcendent Saga) — обе написаны и созданы Knight Lightning. Ищите третью и четвёртую главы FTSaga в выпуске 24 Phrack Inc.

Авторы, желающие опубликовать свои нераспространявшиеся файлы в Phrack Inc., могут присылать их нам через The Prophet, или — если у вас есть доступ к сети, связанной с Bitnet, — по одному из наших адресов, указанных ниже. Кроме того, все, кто имеет доступ к сетям Bitnet, MCI Mail или GTE Telemail и хотел бы получать Phrack Inc. на свои аккаунты, могут связаться с нами.

Knight Lightning & Taran King
(C483307@UMCVMB) (C488869@UMCVMB)

Phrack Pro-Phile XXIII

Автор: Taran King

Составлено 18 января 1989 года

Добро пожаловать в Phrack Pro-Phile XXIII. Рубрика Phrack Pro-Phile была создана для того, чтобы рассказывать сообществу о людях, завершивших активную деятельность, либо сыгравших значительную или неоднозначную роль в нашей среде. В этом выпуске — пользователь и сисоп, оставивший заметный след благодаря своим доскам, опубликованным статьям и общей фрикерско-хакерской активности...

The Mentor

Хэндл: The Mentor
Имя: Loyd
Прошлые хэндлы: Одна статья для Phrack была написана под именем The Neuromancer — из соображений безопасности, актуальных на тот момент.
Происхождение хэндла: Серия «Серый Ленсмен» Э.Э. «Дока» Смита
Дата рождения: 1965
Текущий возраст: 23
Рост: 5' 10" (177 см)
Вес: 200 фунтов (90 кг)
Цвет глаз: Карие
Цвет волос: Каштановый
Компьютеры: (в порядке владения) TRS-80, Apple //e, Amiga 1000, PC/AT
Сисоп: The Phoenix Project (512-441-3088)

Начало пути в мире фрикинга и хакинга

Когда ему было 13 лет, отец одного из друзей — преподаватель местного университета — дал ему аккаунты на одном из университетских PDP 11/70. Это стало его первым знакомством с большими машинами, и он заразился навсегда. Он продолжал пользоваться университетским оборудованием на протяжении всей средней школы, со временем перебравшись на DEC-10, а затем на VAX 8600.

Само собой, поскольку он не был студентом, добыча аккаунтов порой была делом непростым — и он начал писать фальшивые фронтенды, троянские программы и другие хакерские утилиты. Интерес Лойда к хакингу рос, и вскоре ему уже хотелось проникать *везде*, а не только в местные системы.

Начало работы с фрикерско-хакерскими BBS

С примерно 1982 года он крутился на варезных досках, многие из которых одновременно служили фрикерскими площадками. Именно там он раздобыл номера Sherwood Forest и P-80 — и начал

звонить вовне.

Знакомые в мире фрикинга и хакинга

ANI Failure, Android Pope, Bad Subscript, Control C, Crimson Death, The Dictator, Doom Prophet, Erik Bloodaxe, Ferrod Sensor, Forest Ranger, Hatchet Molly, Knight Lightning, The Leftist, Lone Wolf, Lucifer 666, Phantom Phreaker, Phase Jitter, Phlash Gordon, Phrozen Ghost, The Protestor, Surfer Bob, Taran King, Terminal Technocrat, Tuc, The Ubiquitous Hacker, The Urvile/Necron 99.

Как приобретался опыт

Хакингом. Можно перечитать все gfile'ы на свете, но пока ты не выйдешь и не начнёшь ломать сам — останешься новичком. Взлом систем нарастает как снежный ком: первая может даться с трудом, но дальше становится всё проще и проще.

Источники знаний

Все, кто был готов помочь ему на старте, плюс реальный практический опыт.

Памятные фрикерско-хакерские BBS

Sherwood Forest, The Protestor's Shack, Metal Shop (когда она только ушла в приват), Stalag-13, Catch-22, Hacker's Hideout, Arisia, The Phoenix Project, Tuc's Board — RACS III (LOGONIT)

Работа и образование

Степень бакалавра по информатике; работает программистом компьютерной графики.

Конвенции и занятия вне телефонных звонков

Занимал высокие места в национальном рейтинге по фехтованию на сабле в 1985 и 1986 годах; серьёзный коллекционер научной фантастики и ролевой игрок; играет на гитаре, бас-гитаре и клавишных в разных группах.

Написал не менее полудюжины файлов для Phrack; публиковался в LOD/H Technical Journal и ньюслеттере P/HUN; несколько раз вёл неизменно популярную колонку «Hackin' Off» в Thrasher.

Хакерско-фрикерские группы

В настоящее время активный член Legion of Doom / Legion of Hackers; ранее состоял в PhoneLine Phantoms, The Racketeers и Extasyy Elite (смешно).

Аресты

Арест привёл к его уходу «на покой» примерно на год. По его мнению, каждому стоит взять паузу: это помогает расставить всё по местам.

Интересы

VAX-компьютеры, сети с коммутацией пакетов, компьютерная графика.

Любимые вещи

Жена, кот, китайская кухня, блюз, джаз, дорогостоящие UUCP-аккаунты, аккаунты без паролей, DCL, Modula-2, двойная буферизация, Stevie Ray Vaughan.

Наиболее запоминающиеся события

Женитьба (уже 6 месяцев!); арест прямо посреди лекции по политологии и препровождение в тюрьму; как он утащил Control C от рисования LMOS-диаграмм для компании пьяных старшеклассниц; SummerCon в целом; как Knight Lightning вскочил на кровать и заорал «Teletrial!»; как он вёл 45-минутный разговор о блюбоксинге и фрикинге в спортзале с каким-то мужиком, а потом выяснилось, что тот отвечает за безопасность в местной телефонной компании; как он затроянил программу Star Trek на DEC-10 своего колледжа, и все, кто её запускал, в следующий раз при входе в систему выполняли его фальшивый фронтенд...

Отдельные слова

Android Pope — нужен же кому-то напарник по неприятностям!
Erik Bloodaxe — смотри выше.

Compuphreak — за помощь в начале пути и ответы на кучу глупых вопросов (ладно, объясни мне ещё раз, что за штука этот дивертер...).
The Maelstrom — смотри выше.
The Urvile — d00d.

Внутренние шутки

«Ты думаешь, это хорошая идея — делать это перед посадкой в самолёт?», «Господи, хоть бы люди нашли другое место, куда плеваться.», «Привет, ты, наверное, Дэн. Держи.», «Если меня арестуют, я сожгу твой дом вместе с тобой и всей твоей семьёй.», «Поверь мне. Тебе нужно ещё пиво.», «Этот коридор, кажется, никогда не кончается!», «Как мило с их стороны — упаковать всё это для нас!», «Все вышли! Немедленно!», «Ты что, правда собираешься трогать ту девушку?», «Если нас остановят — пристрелим их, едем в Нью-Йорк и меняем личность. Беспроигрышный план.», «Ты правда хочешь поговорить о телефонах?», «Не могу поверить, что ты довёл его до слёз. Это грустно.», «Мистер Леттерман?», «Вы говорите на DCL?», «Нет, ты идиот, ГЕРМАНИЯ!!!!», «Смотри, делаешь вот так, потом вводишь вот это, и — бах! Кодов на несколько дней.», «Мэм, мне жаль вам это говорить, но ваш сын — компьютерный преступник.», «Почём гранатомёт? С боеприпасами или без?», «К этому моменту ты уже догадался — тебя провели.», «Ну что ж, если ты будешь работать в тюрьме, может, поможешь им с компьютерами.», «Нет, она правда хочет нас обоих!», «Что в портфеле?», «Это пистолет старшего брата, офицер.», «Bell Communications Research представляет...», «Заплачу 500 долларов за последние четыре цифры его номера. Хотя бы намекни.»

Фрикеры и хакеры, которых ты встречал, — в основном компьютерные ботаники?

Как ни странно, лучшие из тех, кого он знал, — нет. Зато среди позёров таких хватает.

Спасибо за уделённое время, Лойд...

TARAN KING

Subdivisions («Подразделения»)

Автор: Knight Lightning

Третья часть трилогии «Порочный круг»

8 августа 1988 года

> *«A Rose By Any Other Name... Would Smell As Sweet»*
> *(«Роза под любым другим названием пахла бы столь же сладко»)*

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                            <>
<>                        Subdivisions                        <>
<>                        ~~~~~~~~~~~~                        <>
<>          Part Three Of The Vicious Circle Trilogy          <>
<>                                                            <>
<>  A Study On The Occurrence Of Groups Within The Community  <>
<>                                                            <>
<>                Presented by Knight Lightning               <>
<>                       August 8, 1988                       <>
<>                                                            <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

```
       The Administration \ Advanced Telecommunications, Inc./ATI
      ALIAS \ American Tone Travelers \ Anarchy Inc. \ Apple Mafia
The Association \ Atlantic Pirates Guild/APG \ Bad Ass Mother Fuckers/BAMF
  Bellcore \ Bell Shock Force/BSF \ Black Bag \ Camorra \ C&M Productions
 Catholics Anonymous \ Chaos Computer Club \ Chief Executive Officers/CEO
Circle Of Death \ Circle Of Deneb \ Club X \ Coalition of Hi-Tech Pirates/CHP
      Coast-To-Coast \ Corrupt Computing \ Cult Of The Dead Cow/-cDc-
  Custom Retaliations \ Damage Inc. \ D&B Communications \ The Dange Gang
          Dec Hunters \ Digital Gang/DG \ DPAK \ Eastern Alliance
        The Elite Hackers Guild \ Elite Phreakers and Hackers Club
The Elite Society Of America \ EPG \ Executives Of Crime \ Extasyy (Elite)
 Fargo 4A \ Farmers Of Doom/FOD \ The Federation \ Feds R Us \ First Class
        Five O \ Five Star \ Force Hackers \ The 414s \ Hack-A-Trip
Hackers Of America/HOA \ High Mountain Hackers \ High Society \ The Hitchhikers
     IBM Syndicate \ The Ice Pirates Imperial Warlords \ Inner Circle
                      Inner Circle II \ Insanity Inc.
International Computer Underground Bandits/ICUB \ Justice League of America/JLA
   Kaos Inc. \ Knights Of Shadow/KOS \ Knights Of The Round Table/KOTRT
     League Of Adepts/LOA \ Legion Of Doom/LOD \ Legion Of Hackers/LOH
     Lords Of Chaos \ Lunitic Labs, Unlimited \ Master Hackers \ MAD!
          The Marauders \ MD/PhD \ Metal Communications, Inc./MCI
MetalliBashers, Inc./MBI \ Metro Communications \ Midwest Pirates Guild/MPG
     NASA Elite \ The NATO Association \ Neon Knights \ Nihilist Order
Order Of The Rose \ OSS \ Pacific Pirates Guild/PPG \ Phantom Access Associates
              PHido PHreaks \ Phlash \ PhoneLine Phantoms/PLP
            Phone Phreakers Of America/PPOA \ Phortune 500/P500
             Phreak Hack Delinquents \ Phreak Hack Destroyers
       Phreakers, Hackers, And Laundromat Employees Gang/PHALSE Gang
   Phreaks Against Geeks/PAG \ Phreaks Against Phreaks Against Geeks/PAP
    Phreaks and Hackers of America \ Phreaks Anonymous World Wide/PAWW
          Project Genesis \ The Punk Mafia/TPM \ The Racketeers
Red Dawn Text Files/RDTF \ Roscoe Gang \ SABRE \ Secret Circle of Pirates/SCP
 Secret Service \ 707 Club \ Shadow Brotherhood \ Sharp Inc. \ 65C02 Elite
  Spectral Force \ Star League \ Stowaways \ Strata-Crackers \ The Phrim
   Team Hackers '86 \ Team Hackers '87 \ TeleComputist Newsletter Staff
Tribunal Of Knowledge/TOK \ Triple Entente \ Turn Over And Die Syndrome/TOADS
300 Club \ 1200 Club \ 2300 Club \ 2600 Club \ 2601 Club \ 2AF \ Ware Brigade
         The Warelords \ WASP \ The United Soft WareZ Force/TuSwF
```

Буквально невозможно поверить, сколько различных групп и организаций существует или существовало в сообществе фрикеров/хакеров/пиратов. Список из 130 групп, приведённый выше, — это, вероятно, лишь малая часть от реального числа существовавших группировок, однако именно о них мне известно на сегодняшний день.

В прошлом Джон Максфилд оценивал, что в Соединённых Штатах действует около 50 000 хакеров/фрикеров/пиратов. Эта цифра выросла до такой степени, что теперь, вероятно, приближается к 500 000. Хотите верьте, хотите нет, но почти каждый в тот или иной период был членом одной из перечисленных выше групп (или, возможно, какой-либо не упомянутой).

Сегодняшние консультанты по безопасности в сфере телекоммуникаций и правоохранительные органы тоже это знают — и именно поэтому принадлежность к группе может быть обращена против нас.

Что означает членство в группе? В модемном сообществе принято считать, что люди в группе совместно работают над проектами и обмениваются конкретной информацией, к которой у людей за пределами группы нет доступа и нет возможности её получить. Однако, очевидно, что все члены группы считают остальных, с кем они обмениваются информацией, заслуживающими доверия и достойными их общества изначально. Если остановиться и подумать: если бы группы не существовало, эти люди всё равно обменивались бы информацией и доверяли бы друг другу, — ведь они не создали бы группу, если бы это условие не было выполнено с самого начала. Таким образом, по существу, членство в группе ничего не значит в том смысле, что был описан выше.

В модемном сообществе членство в группе на самом деле больше похоже на «опьянение властью» или «защитное одеяло» для тех, кто чувствует потребность дать другим знать о своей принадлежности к определённой клике в надежде, что популярность некоторых других членов перепадёт и им самим.

Многие группы формируются таким образом, что стараются создать другое впечатление — и именно здесь начинается настоящая проблема. Некоторые группы создаются человеком, который пытается собрать вместе побольше ребят, кажущихся ему знающими или активно публикующими хорошую информацию. Плохой ход. Если уж создавать группу, держитесь людей, которым, как вам известно, можно доверять (а можно ли вообще когда-либо «знать», кому можно доверять?), и уже из этих людей формируйте группу или выбирайте тех, кого считаете достойными членства.

Во всяком случае, чтобы доказать свою элитарность, большинство групп начинают собирать конкретные данные для передачи членам группы, включая раздачу имён и телефонных номеров друг друга. Они ощущают ложную лояльность и психологически взращивают такую полнейшую веру во всех членов, что эта вера в итоге становится слепой и основывается лишь на надеждах и устремлениях к величию.

Каков наилучший способ для агента безопасности или информатора смешаться с модемным сообществом? Вступить в как можно больше групп, начать собирать данные о членах и распространить свой хэндл по всему сообществу, чтобы стать «широко известным».

Пример: взято из Phrack World News, выпуск XV;

*_[Эта статья была отредактирована для настоящей публикации. — KL]_*

Mad Hatter: информатор? (31 июля 1987 года)

Мы в Phrack Inc. раскопали значительный объём информации, который привёл нас к убеждению, что Mad Hatter является информатором какой-либо правоохранительной организации.

Когда Taran King, Cheap Shades, Forest Ranger и Knight Lightning прибыли к Control C в Чикаго, штат Иллинойс, Mad Hatter уже обыскал место и нашёл бумаги, которые могли бы только навредить ^C. Мы уничтожили эту информацию и думали, что всё в порядке. Однако, как выяснилось, мы обыскали сумки Mad Hatter'a и обнаружили дубликат этой информации — общая гипотеза состояла в том, что он намеревался оставить её в качестве улики.

Mad Hatter также принёс несколько дисков с целью скопировать Phantasie Realm. Заметьте: PR была программой для IBM, а у MH — Apple.

Control C рассказал нам, что когда он ехал встречать Mad Hatter'a на автобусной станции, он наблюдал, как подъезжает автобус, и видел всех, кто вышел. Внезапно Mad Hatter оказался там — но не из того автобуса, на котором должен был приехать. Помимо этого, у него была пищевая сода, завёрнутая в пятидолларовую купюру, которую он пытался выдать за кокаин. Возможно, чтобы казаться крутым или что-то в этом роде.

Mad Hatter постоянно пытался остаться в квартире ^C в одиночестве по неизвестным причинам. Его также видели в квартире соседей, откуда он совершал несанкционированные звонки в Чикаго. Когда его спросили, кому он звонил, он ответил: «Не ваше дело». У Mad Hatter'a совершенно не было денег во время PartyCon (к тому же он съел всё содержимое холодильника ^C), и тем не менее он настаивал, что, несмотря на то что приехал на автобусе и имел обратный билет, полетит домой самолётом. Как это должно было осуществиться? Денег у него не было, и даже если бы он мог вернуть деньги за автобусные билеты, ему всё равно не хватало бы более 200 долларов. Когда его спросили, как он собирается это устроить, его ответ был: «Не ваше дело».

В субботу вечером, по дороге в Hard Rock Cafe, Mad Hatter четыре раза спросил Control C о местонахождении его компьютерной системы и прочего имущества. Эта информация Hatter'у была не нужна, зато агенту Секретной службы или кому-то подобному она бы очень пригодилась.

Когда Phrack Inc. обнаружила, что Dan The Operator является информатором ФБР, и предала это огласке, несколько человек критиковали его в Free World II Private. Mad Hatter, напротив, встал на защиту Noah и заявил, что тот по-прежнему его друг, невзирая на произошедшее. Затем, когда он понял, что люди ставят под сомнение его собственную благонадёжность, его первоначальные посты были удалены, и он начал говорить, как хочет убить Dan The Operator и как ненавидит его.

Mad Hatter уже признал, что знал о том, что Dan The Operator является информатором ФБР, ещё до SummerCon '87. По его словам, он не сказал никому, потому что предполагал, что мы и так уже знаем.

Когда Mad Hatter впервые вошёл в мир фрикеров/хакеров, он вступил в:

• Phreaks Anonymous World Wide (PAWW)
• MetalliBashers, Inc. (MBI)
• Order of The Rose
• Cult of The Dead Cow (-cDc-)

Если бы вы были агентом безопасности или жалким хакером, переквалифицировавшимся в информатора, и хотели бы смешаться с сообществом фрикеров/хакеров, — разве вы не попытались бы вступить в как можно больше групп, чтобы распространить своё имя?

Phreaks Anonymous World Wide, MetalliBashers, Inc., Order of The Rose и Cult of The Dead Cow — далеко не самые закрытые группы для вступления, и как только в группу попадает один агент

безопасности, он непременно поручится за других и так далее. Пока он распространяет своё имя по всему сообществу как элитный модемный пользователь, он занят сбором информации о членах группы, достаточно глупых, чтобы ему доверять.

Мало того что в некоторые группы и без того легко внедриться, — но помнит ли кто-нибудь об этом?

Взято из Phrack World News, выпуск XI:

Phortune 500: новейшая организация фрикдома (16 февраля 1987 года)

Для тех, кому это хоть немного интересно: Phortune 500 — это группа любителей телекоммуникаций, цель которых — распространять информацию, а также углублять собственные знания в области телекоммуникаций. Эта новая группа была основана:

```
Brew Associates / Handsomest One / Lord Lawless / The Renegade Chemist
      Quinton J. Miranda / Striker / The Mad Hacker / The Spiker
```

Эти восемь членов также известны как Совет директоров (BOD). Они не претендуют на звание «элиты» в том смысле, что являются величайшими хакерами в мире, но всё же довольно избирательны в отношении своих членов. Они предпочитают тех, кто немного знает обо всём и обладает талантами, исключительными для него/неё самого.

Одним из завершённых проектов Phortune 500 является индивидуальная система паролей типа AE под названием TransPhor. Она была написана и создана Brew Associates. Бета-тестирование проводилось на The Undergraduate Lounge (Sysoped by Quinton J. Miranda). Планируется выпуск для широкой публики в течение ближайших нескольких месяцев.

Phortune 500 работает уже около 4 месяцев и выпустила два собственных информационных бюллетеня. The Phortune 500 Newsletter весьма напоминает журнал «People» среди современных изданий. В то время как некоторые журналы освещают глубокие технические аспекты мира, в котором мы общаемся, их бюллетень стремится охватить лёгкую сторону жизни, вплетая информацию, которую они считают «имеющей технический характер». Третий выпуск должен выйти до конца текущего месяца.

```
*>=-> The Phortune 500 Membership Questionnaire <-=<*
```

Примечание: Следующая информация носит строго конфиденциальный характер. Причина, по которой анкета покажется вам столь длинной и детальной, состоит в нашем желании узнать вас. Мы в Phortune 500 считаем, что должны хорошо знать потенциальных членов, прежде чем допустить их в нашу организацию. В зависимости от ваших ответов вы будете приняты в Phortune 500 в качестве члена-основателя. Пожалуйста, ответьте на следующие вопросы полностью...

```
.....................................................................

Handle                          :
First Name                      :
Voice Phone Number              :
Data Phone Number               :
City & State                    :
Age                             :
Occupation (If Applicable)      :
Place of Employment (Optional)  :
Work Phone Number   (Optional)  :
Computer Type                   :
Modem Type                      :
Interests                       :
Areas Of Expertise              :
```

```
References (No More Than Three) :
Major Accomplishments (If Any)  :
.....................................................................
Answer In 50 Words Or Less;

^*^  What Is Phortune 500 in Your Opinion?

^*^  Why Do You Want To Be Involved With Phortune 500?

^*^  How Can You Contribute to Phortune 500?
.....................................................................
```

Пожалуйста, ответьте на каждый вопрос в меру своих возможностей, а затем отправьте ответы любому члену Совета директоров Phortune 500 или на BBS Phortune 500:

```
The Private Connection (Limited Membership) 219-322-7266
The Undergraduate AE   (Private Files Only) 602-990-1573
```

Реальная анкета для вступления в группу. Возможно, сама концепция была неплоха, а возможно, и нет — но с точки зрения публичности и безопасности это была полная и абсолютная катастрофа.

По сути, мы все здесь так или иначе учимся. Группы и клубы в нашем сообществе, похоже, лишь разобщают его, а в то время, когда все должны держаться вместе, это не лучшая идея. Конфиденциальность и безопасность — важные факторы, мотивирующие появление этих сект внутри общества, но в конечном счёте стоят ли последствия тех усилий, которые затрачиваются на создание группы?

Если бы группы не создавались, на сообщество фрикеров/хакеров не было бы столько внимания, сколько есть сейчас. Когда названия групп начинают распространяться, это приводит правоохранительные органы в панику, заставляя их думать, что перед ними серьёзная организованная преступность. Это позволяет им обосновать выделение большего времени и средств на поимку компьютерных преступников, и обычно они идут за крупными именами — людьми из самых «элитных» групп.

Прежде чем вы, член какой-либо группы, начнёте критиковать этот материал, пожалуйста, поймите: я не ссылаюсь здесь на какие-либо конкретные группы — только на группы в целом. Любые комментарии в адрес MBI, -cDc-, PAWW, OOTR и P500 не следует принимать на личный счёт; они использовались исключительно как примеры того, как группы могут являться потенциальными угрозами безопасности.

Существуют группы, которые представляют собой стоящие организации — это очевидно, поскольку они существуют на протяжении многих лет и были продуктивны. Однако единственный способ сохранить это сообщество живым — чтобы каждый работал сообща: защищать и учиться друг у друга.

:Knight Lightning

«Будущее — это сейчас»

Утопия

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                              <>
<>                            Utopia                            <>
<>                            ~~~~~~                            <>
<>          Chapter One of The Future Transcendent Saga         <>
<>                                                              <>
<>            An Introduction To The World Of Bitnet            <>
<>                                                              <>
<>                 Presented by Knight Lightning                <>
<>                        January 1, 1989                       <>
<>                                                              <>
<>                 Special Thanks To Jester Sluggo              <>
<>                                                              <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

Глава первая «Саги о грядущем трансцендентном»

Введение в мир Bitnet

Автор: Knight Lightning

Отдельная благодарность: Jester Sluggo

1 января 1989 года

Добро пожаловать в новое ТЫСЯЧЕЛЕТИЕ в сфере коммуникаций
Будущее наступает прямо сейчас!

Большинство согласится с тем, что компьютеры колледжей и университетов проще всего поддаются несанкционированному, да и легальному доступу тоже. Bitnet — лишь одна из множества взаимосвязанных глобальных сетей, однако я счёл её наиболее важной для обсуждения: именно через неё соединены все крупные колледжи и университеты, и это создаёт почти утопическое общество для технически увлечённых людей. Сеть бесплатна, законна и охватывает весь мир — а всё, что сочетает «бесплатное» с «законным» и при этом полезно, непременно несёт в себе что-то от совершенства. Отсюда и название этого файла.

Для тех, кто уже работает в Bitnet, этот файл может показаться несколько элементарным и, скорее всего, не содержит ничего нового. Но никогда не знаешь, к каким открытиям приведёт лишняя страница прочитанного. Итак, ещё раз добро пожаловать в будущее... будущее, где пределы неизвестны.

:Knight Lightning

Происхождение BITNET

by Jester Sluggo

В 1981 году Городской университет Нью-Йорка (CUNY) провёл опрос среди университетов на восточном побережье США и Канады: интересует ли их создание простой в использовании и

экономичной сети для межуниверситетского общения между учёными. Отклик оказался положительным. Многие разделяли убеждение CUNY в важности компьютерного взаимодействия между исследователями. Первое звено новой сети, получившей название Bitnet, было установлено между CUNY и Йельским университетом в мае 1981 года. Аббревиатура BITNET расшифровывается как «Because It's Time NETwork» («Потому что пришло время для сети»).

Выбор сетевой технологии для Bitnet был обусловлен доступностью программного обеспечения RSCS на IBM-компьютерах в первых узлах сети. RSCS прост и эффективен; большинство IBM VM/CMS-систем имеют его в установке для локальных коммуникаций, обеспечивая передачу файлов и удалённую обработку заданий. Стандартные каналы Bitnet — это арендованные телефонные линии, работающие на скорости 9600 бит/с. Хотя первые узлы были IBM-машинами в университетских вычислительных центрах, сеть никак не ограничена подобными системами. Любой компьютер с эмулятором RSCS может быть подключён к Bitnet. Эмуляторы существуют для систем Digital Equipment Corporation VAX/VMS, VAX-UNIX, а также для систем Control Data Corporation Cyber и ряда других. Сегодня более трети компьютеров в Bitnet — это не IBM-системы.

В научном сообществе Bitnet также ведутся разговоры о возможном слиянии с CSnet (Computer Science Network). Неизвестно, состоится ли оно и когда, но это было бы лишь шагом в правильном направлении.

Примечание: NetNorth — канадское подразделение Bitnet, EARN — европейское. Все они напрямую соединены и вместе образуют единую сеть, а не три отдельных. Нередко её обозначают как BITNET/NetNorth/EARN.

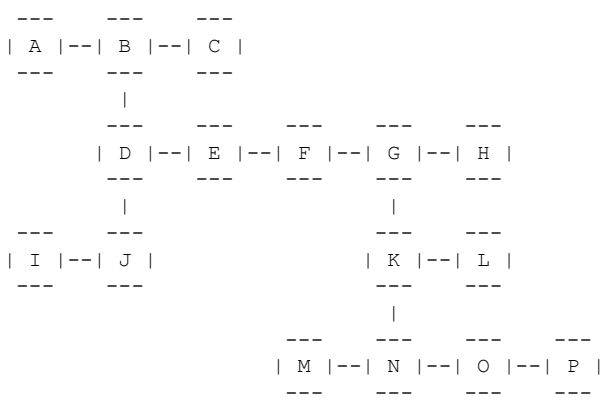
Основы Bitnet

Чтобы разобраться в этом файле, нужно для начала иметь базовое представление о мейнфреймах, идентификаторах пользователей и тому подобных вещах. Поскольку большинство читателей Phrack — компьютерные энтузиасты, весьма вероятно, что вы с этим уже знакомы. Если нет — поищите документацию по теме. «Руководство начинающего хакера» за авторством The Mentor, опубликованное в Phrack Inc. XXII, содержит сведения, которые могут оказаться полезными. Концепции, изложенные в этом файле, не слишком сложны для понимания, однако приступать к ним совершенно неподготовленным тоже не стоит.

Неплохо также немного разбираться в аппаратном обеспечении и операционной системе, с которой вы будете работать. Большинство IBM-систем в Bitnet работают под управлением VM/CMS. Системы VAX производства Digital Equipment Corporation (DEC) обычно используют операционную систему VMS в связке с программным пакетом JNET, позволяющим им взаимодействовать через Bitnet. На протяжении всего файла я буду обращаться к VM/CMS и VMS/JNET. Сам я сейчас работаю на IBM 4381 под управлением VM/CMS, поэтому с этим типом систем знаком значительно лучше.

Представьте мейнфрейм как телефонный аппарат, а Bitnet — как телефонные линии. Мейнфрейм, на который вы входите, соединён с мейнфреймами других университетов и организаций. Соединение, как правило, осуществляется по высокоскоростной арендованной линии — особому виду телефонного соединения. В каком-то смысле эти компьютеры постоянно «разговаривают» друг с другом (кроме случаев, когда каналы разрываются — об этом в разделе про СООБЩЕНИЯ). Данная сеть относится к типу «хранить и передавать» (store and forward). Это означает: если я отправляю что-то кому-то в Лос-Анджелесе, компьютеры на пути между Нью-Йорком и Калифорнией будут последовательно хранить и передавать данные от узла к узлу, пока те не достигнут адресата.

В Bitnet между двумя точками существует лишь один маршрут. Небольшой фрагмент сети может выглядеть так:



Прямоугольники — это компьютеры в сети, а черточки между ними — арендованные линии. Если я нахожусь на компьютере «A» и отправляю файл кому-то на компьютер «N», путь будет таким:

```
A-B-D-E-F-G-K-N
```

Реальные карты топологии можно скачать с LISTSERV@BITNIC, но о серверах мы поговорим позже. Как уже упоминалось, между любыми двумя узлами существует единственный маршрут, и обойти разорванное звено попросту невозможно.

Каждый компьютер в BITNET называется «узлом» (node) и имеет уникальное имя, по которому его узнают остальные. Например, один из мейнфреймов Университета Миссури в Колумбии носит имя UMCVMB. Что это означает? В данном случае UMC — аббревиатура названия университета, VM — операционная система виртуальной памяти, B — просто буквенно-цифровой идентификатор. Когда-то существовал и UMCVMA, но эта система была отключена несколько лет назад. Следует заметить, что хотя данный узел поддаётся расшифровке по частям, многие узлы не следуют этой схеме, а некоторые имеют «псевдонимы» (aliases). Псевдоним — это просто другое имя узла; оба имени распознаются всеми сервисами Bitnet. Пример — STANFORD: узлы STANFORD и FORSYTHE — это одно и то же место, то есть:

```
CYPHER@STANFORD = CYPHER@FORSYTHE
```

Ваш идентификатор пользователя в сочетании с именем узла составляет ваш «сетевой адрес». Он обычно записывается в формате userid@node (читается «userid на node»). Например, мой узел — UMCVMB, мой userid — C483307. Следовательно, мой сетевой адрес — C483307@UMCVMB. Зная userid@node человека в сети, я могу с ним общаться, и он — со мной. Я встретил в сетях немало интересных людей. Используя возможности прямого общения в Bitnet, я могу разговаривать с ними в режиме реального времени. Вы тоже так можете — нужно знать лишь несколько команд. Об этом рассказывается во второй части.

Сообщения

Существует три основных способа общения через Bitnet: MAIL (почта), MESSAGE (сообщение) и FILE (файл). Почему для конкретной задачи выбирается тот или иной способ — станет ясно после небольшого пояснения.

MESSAGE — самый быстрый и удобный способ общения в Bitnet. Это сетевой эквивалент телефонного разговора. Разница лишь в том, что слова набираются, а не произносятся. Набранное вами сообщение немедленно (вернее, очень быстро) передаётся по адресу назначения. В BITNET

этим адресом является сетевой адрес (userid@node) человека, с которым вы хотите связаться. Если он в данный момент в системе, сообщение отобразится на его экране. Если нет — компьютер адресата сообщит вам об этом, прислав ответное уведомление. В таком случае ваше сообщение теряется безвозвратно: иными словами, трубку никто не снял. Впрочем, многие запускают программу GONE (и другие подобные), работающую как автоответчик — она хранит сообщение до тех пор, пока адресат не войдёт в систему. Некоторые университеты не разрешают эту программу, поскольку она потребляет много процессорного времени. Если в вашем вузе или на вашем мейнфрейме она запрещена, не пытайтесь использовать её тайком: обнаружить это очень просто.

Важно отметить, что не все узлы поддерживают интерактивный чат. Некоторые недостаточно для этого продвинуты, и всякий раз, когда вы пытаетесь с ними пообщаться, вы получаете соответствующее сообщение. Впрочем, такая ситуация встречается редко.

Команда для отправки сообщений зависит от вашего компьютера и системного программного обеспечения. Пользователи VM/CMS вводят нечто подобное:

```
TELL userid AT node message  OR  TELL userid@node message
```

Например:

```
TELL MENTOR AT PHOENIX Hey, whats new on The Phoenix Project?
     +-----    +------ +-------------------------------------
     |         |       |
     |         |       +----------- отправляемое сообщение
     |         |
     |         +------------------- узел получателя
     |
     +----------------------------- userid получателя
```

Пользователи VAX/VMS с сетевым программным обеспечением JNET используют такой синтаксис:

```
SEND userid@node "message"
```

Например:

```
SEND MENTOR@PHOENIX "Hey, whats new on The Phoenix Project?"
     +----- +------ +-------------------------------------
     |      |       |
     |      |       +-------------- отправляемое сообщение
     |      |
     |      +---------------------- узел получателя
     |
     +----------------------------- userid получателя
```

Кавычки вокруг сообщения необязательны. Однако без них JNET для VAX/VMS переведёт весь текст сообщения в верхний регистр. Многих это крайне раздражает.

За подробной информацией о командах TELL и SEND следует обращаться к документации вашей локальной системы.

Полученное сообщение на вашем экране выглядит примерно так:

```
FROM PHOENIX(MENTOR):  Hello!  Things are great here, you?
```

К сожалению, у всего есть обратная сторона, и сообщения Bitnet — не исключение. Текст, передаваемый через MESSAGE, должен быть коротким. Как правило, длина сообщения ограничена одной строкой — примерно шириной вашего экрана. Иными словами, отправить кому-то копию Phrack World News командой TELL не получится.

Кроме того, общаться таким образом можно только с теми, кто в данный момент в системе. С учётом разницы часовых поясов (вы можете общаться с людьми из Европы, Израиля или Австралии) это зачастую весьма неудобно.

Наконец, существует проблема разрывов канала, которую я называю LinkDeath. Если соединение с нужным вам узлом прерывается (например, из-за обрыва телефонной линии), вы получаете

сообщение об ошибке, а всё отправленное — пропадает. Особенно раздражает, если это происходит в разгар разговора. LinkDeath может длиться несколько минут или несколько часов. Нередко канал падает на выходные, и тут уж ничего не поделаешь. Ещё хуже, когда обрывается канал, соединяющий ваш мейнфрейм с остальным Bitnet: вы оказываетесь отрезаны от сети.

Тем не менее сообщения весьма далеки от бесполезности. Как я покажу во второй главе, TELL и SEND чрезвычайно удобны для работы с многочисленными серверами Bitnet.

Файлы (FILES) — ещё один способ общения через Bitnet. Текстовые файлы и программы, хранящиеся на вашем компьютере, можно передавать пользователям на других узлах. Именно так я распространяю выпуски Phrack — не только по стране, но и по всему миру. Пользователи VM/CMS применяют синтаксис вида:

```
SENDFILE filename filetype filemode userid AT node
```

Например:

```
SENDFILE PHRACK TEXTFILE A PROPHET AT PHRACKVM
         +---------------- +------------------
         |                 |
         |                 +------- адрес получателя
         |
         +------------------------- отправляемый файл
```

Однако на моём конкретном узле команда выглядит так:

```
SENDFILE PHRACK TEXTFILE A TO (nickname)
```

По какой-то причине на моём узле нельзя отправить файл кому-либо через SENDFILE, если этот человек не внесён в ваш файл NAMES. NAMES — это база данных, переводящая userid@node в псевдонимы, что упрощает общение: вместо утомительного userid@node можно использовать псевдоним. Filemode — в данном примере «A» — это диск, на котором хранится файл «PHRACK TEXTFILE». На случай если вы задались вопросом: за исключением моего адреса, большинство адресов в этом файле — например, PROPHET@PHRACKVM или MENTOR@PHOENIX — вымышленные и приведены лишь для иллюстрации.

Синтаксис для VMS/JNET-систем весьма схож:

```
SEND/FILE filename.extension userid@node
```

Например:

```
SEND/FILE PHRACK.TEXTFILE PROPHET@PHRACKVM
          +--------------- +---------------
          |                |
          |                +-------- адрес получателя
          |
          +------------------------- отправляемый файл
```

Отправленный файл хранится в «электронном почтовом ящике» получателя до тех пор, пока тот не войдёт в систему. Пользователи VM/CMS используют для обработки полученных файлов команды RECEIVE или RDRLIST (сокращённо «RL»). Пользователи VAX/VMS применяют команду RECEIVE. За дополнительными сведениями об этих командах обращайтесь к локальной документации.

SEND/FILE и SENDFILE удобны для отправки программ или больших объёмов данных — например, выпусков Phrack — по сети. Однако для повседневного общения их использовать не стоит, поскольку есть способ куда удобнее — MAIL.

Почта

Другой форме общения в Bitnet дали весьма меткое название: MAIL (нередко называемая «электронной почтой» или «e-mail»). Как и обычная почта, она предполагает адрес получателя, обратный адрес и текст. Программное обеспечение для отправки почты различается от площадки к площадке, поэтому за информацией обращайтесь к местной документации. На моём узле обратный адрес (ваш адрес) автоматически вставляется в письмо. Это изложение даёт общее представление о том, как выглядит типичное письмо и как оно работает.

Почтовые файлы — это обычные текстовые файлы с особым форматированием. Их отличительная черта — «заголовок письма» (mail header). Он сообщает системе Bitnet и вашей почтовой программе, что перед ней не обычный текстовый файл. Выглядит это примерно так:

```
                                        Адрес получателя
                                                        |
                                                Тема письма  |
                                                        |  |
                                              Ваш адрес    |  |
                                                       |  |  |
                                            Дата       |  |  |
                                                    |  |  |  |
Date:          Fri, 29 Dec 88 23:52:00 EDT            <--+  |  |  |
From:          Forest Ranger <RANGER@STLVAX1>         <-----+  |  |
Subject:       Cable Pair Busted For Child Molestation<--------+  |
To:            Phrack World News <KNIGHT@MSPVMA>      <------------+
```

Письмо целиком выглядит следующим образом:

```
+---------------- Заголовок письма
|
|  Date:          Fri, 29 Dec 88 23:52:00 EDT
|  From:          Forest Ranger <RANGER@STLVAX1>
|  Subject:       Cable Pair Busted For Child Molestation
|  To:            Phrack World News <KNIGHT@MSPVMA>
+  ========================================================================

+  Have you seen the newspapers?  Is this good news, or what?  I think that
|  the ramifications are startling.  This is one more step on the road to a
|  higher civilization.  I hope he gets what he deserves.  Keep in touch, I
|  will send more information later.
|
+---------------- Текст письма
```

У почты есть ряд преимуществ. Размер почтового файла ограничен лишь вашими возможностями; кроме того, это единственный способ отправлять файлы в сети за пределами Bitnet (впрочем, передавать письма длиннее 3000 строк я не рекомендую). Когда ваше письмо достигает адреса назначения, оно хранится в почтовом ящике пользователя до тех пор, пока тот его не прочитает. Если каналы до нужного узла разорваны, письмо будет ждать, пока путь до почтового ящика получателя не освободится.

Недостаток почты — она действительно медленнее, чем сообщения. Чем длиннее письмо, тем дольше оно добирается из точки А в точку Б.

Заключение

Не отчаивайтесь — это лишь конец данного файла. Лучшие возможности Bitnet ещё впереди. Присоединяйтесь ко мне во второй главе «Саги о грядущем трансцендентном» — «Основания на горизонте».

В этом выпуске Phrack также включены списки узлов Bitnet. Полные каталоги узлов доступны по адресу LISTSERV@BITNIC, однако они слишком велики для публикации здесь. Тем не менее включённые файлы содержат названия университетов и организаций, подключённых к Bitnet, без указания адресов узлов (у некоторых организаций их более 30). Если вы учитесь в колледже или университете, подключённом к Bitnet, — присоединяйтесь ко мне в мире бесконечных открытий. Когда это произойдёт, дайте знать...

:Knight Lightning (C483307@UMCVMB)

Для дополнительного чтения:

An Insight On Wide-Area Networks Part 2 by Jester Sluggo
(Phrack Inc. Issue 6, file 8)

Communications Of The ACM

Основы на горизонте

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                            <>
<>                Foundations Upon The Horizon                <>
<>                ~~~~~~~~~~~~~~~~~~~~~~~~~~~~                <>
<>         Chapter Two of The Future Transcendent Saga        <>
<>                                                            <>
<>      Using Servers And Services In The World Of Bitnet     <>
<>                                                            <>
<>                Presented by Knight Lightning               <>
<>                       January 2, 1989                      <>
<>                                                            <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

Глава вторая «Саги о Грядущем Трансцендентном»

Серверы и сервисы в мире Bitnet

Автор: Knight Lightning

2 января 1989 года

Добро пожаловать во вторую главу «Саги о Грядущем Трансцендентном». В этом файле я расскажу о серверах и сервисах Bitnet (хотя некоторые из них присутствуют и в других сетях). Вы узнаете, что такое серверы, чем они отличаются друг от друга, как ими пользоваться, и лучше поймёте, как эти «Основы на горизонте» превращают Bitnet в настоящую виртуальную утопию.

Что такое сервер?

Одна из наиболее полезных возможностей Bitnet — разнообразие файловых серверов, серверов имён, ретрансляторов и прочего. Их часто называют «виртуальными машинами» или «серверными машинами».

«Сервер» — это userid, во многом похожий на ваш. Он может располагаться на вашем компьютере (узле) или на каком-либо другом узле BITNET. Люди, создавшие этот userid, запустили на нём программу, которая реагирует на ваши команды. Это и есть «сервер». Команды, которые вы отправляете, и способ их обработки зависят от конкретной запущенной программы. Например, серверы `UMNEWS@MAINE` и `107633@DOLUNI1` предоставляют разные виды услуг и требуют разных команд. Различные типы серверов описаны далее в этом документе.

Команды большинству серверов можно отправлять в одном из двух форматов: MAIL (почта) или MESSAGE (сообщение).

Не все серверы принимают команды в обоих форматах, однако эта информация содержится в документе `BITNET SERVERS`, который можно получить от `LISTSERV@BITNIC`. Поскольку серверов очень много, перечислять их здесь нет смысла: каждый день одни создаются, другие отключаются, и охватить их все практически невозможно.

Пользователи систем VM/CMS отправляют команды примерно так:

```
TELL userid AT node command   (AT = @)
```

Например:

```
TELL NETSERV@MARIST HELP
```

Пользователи VAX/VMS с сетевым программным обеспечением JNET применяют такой синтаксис:

```
SEND userid@node "command"
```

Например:

```
SEND NETSERV@MARIST "HELP"
```

Многие серверы также принимают команды по почте. Некоторые вообще принимают команды только в этом формате — в частности, серверы в сетях, отличных от Bitnet. Синтаксис команд при этом остаётся тем же. Письмо серверу отправляется точно так же, как письмо человеку, а текст сообщения является командой. Одни серверы считывают команду из первой строки письма, другие требуют её в поле «Subject:». Некоторые серверы принимают несколько команд в одном письме, другие — только одну. Вот пример письма к `LISTSERV@BITNIC` с запросом списка файлов:

```
Date:         Fri, 30 Dec 88 23:52:00 EDT
From:         Taran King <SYSOP@MSPVMA>
To:           Listserv <LISTSERV@BITNIC>
======================================================================
INDEX
```

В дальнейшем по всему файлу я буду приводить примеры с отправкой команд через сообщения. Однако во многих случаях у вас есть возможность воспользоваться почтой — выбор за вами.

Есть два особенно запутанных аспекта, о которых следует знать. Во-первых, серверы одного класса (например, файловые серверы) далеко не всегда принимают одни и те же команды. Многие из них кардинально различаются; другие — отличаются ровно настолько, чтобы доставлять неудобства. Подходов к организации сервера существует множество, и каждый пытается создать что-то лучшее.

Вторая проблема состоит в том, что многие серверы совмещают сразу две, а порой и три категории функций. Например, LISTSERV работает одновременно как сервер списков рассылки и как файловый сервер. Многие серверы LISTSERV модифицированы и для работы в роли сервера имён, однако справляются с этой функцией не слишком эффективно. Если вы пока не понимаете этой терминологии — не переживайте: всё лучшее ещё впереди.

Помните: сервер работает на userid, во многом похожем на ваш. Как и у вас, у него есть множество возможностей, в том числе хранение файлов (пожалуй, с куда большим объёмом). Программа, запущенная на файловом сервере, позволяет ему отправлять вам файлы из своего каталога, а также список доступных файлов. Это могут быть программы или текстовые файлы. Такие серверы можно рассматривать как аналоги дозвонных досок объявлений или AE Lines в мире Bitnet.

Файловому серверу, как правило, можно отправить команды трёх типов. Первый — запрос списка файлов, которые предлагает сервер. Второй — запрос на отправку конкретного файла на ваш userid. Третий, и самый важный, — команда HELP.

Команда HELP исключительно важна, поскольку это одна из немногих команд, которые принимают почти все серверы, независимо от типа. Поскольку наборы команд у разных серверов различаются, HELP часто оказывается незаменимой. Отправив её серверу, вы, как правило, получите сообщение или файл со списком доступных команд и их синтаксисом. Рекомендую держать эту информацию под рукой, пока вы не освоитесь с конкретным сервером.

Для запроса списка файлов обычно отправляют команду `INDEX` или `DIR`. Список придёт вам по почте или в виде файла. Например:

```
VM/CMS:      TELL LISTSERV@BITNIC INDEX
VMS/JNET:    SEND LISTSERV@BITNIC "INDEX"
```

Чтобы запросить конкретный файл из полученного списка, используйте команду вроде `GET` или `SENDME`. Например, чтобы запросить файл `BITNET TOPOLOGY` у `LISTSERV@BITNIC`, введите одну из следующих команд:

```
VM/CMS:      TELL LISTSERV@BITNIC SENDME BITNET TOPOLOGY
VMS/JNET:    SEND LISTSERV@BITNIC "SENDME BITNET TOPOLOGY"
```

Во многих случаях файлы организованы в подкаталоги или списки файлов, что усложняет запрос. Это делает документацию по конкретному серверу ещё более необходимой. Некоторые файловые серверы предлагают программы, которые сами отправляют команды серверу вместо вас.

Серверы имён

Серверы имён выполняют две функции: помогают найти адрес конкретного человека или найти людей с определёнными интересами. Поиск людей по интересам я здесь рассматривать не буду — вряд ли вам это потребуется. Серверов, позволяющих реально искать людей, не так уж много; вот их список:

```
Columbia University                           FINGER   @ CUVMA
Cork University                               INFO     @ IRUCCIBM
Drew University                               NAMESERV @ DREW
North Dakota State University                 FINGER   @ NDSUVM1
Ohio State University                         WHOIS    @ OHSTVMA
Pennsylvania State University                 IDSERVER @ PSUVM
Rochester Institute Of Technology             INFO     @ RITVAXD
                                              LOOKUP   @ RITVM
State University of New York (SUNY) at Albany WHOIS    @ ALBNYVM1
University of Calgary                         NAMESERV @ UNCAMULT
University of Kentucky                        WHOIS    @ UKCC
University of Illinois at Urbana-Champagne    PHSERVE  @ UIUCVMD
University of Louisville (Kentucky)           WHOIS    @ ULKYVM
University of Regina                          VMNAMES  @ UREGINA1
University of Tennessee                       UTSERVER @ UTKVM1
Weizmann Institute of Science                 VMNAMES  @ WEIZMANN
```

Чтобы не вводить в заблуждение: эти серверы не обязательно охватывают весь университет. Например, сервер Университета Луисвилла распространяется только на пользователей узла `ULKYVM`, но не узлов `ULKYVX0x` (x = 1–8). `ULKYVX` — это VAXcluster узлов Университета Луисвилла, однако люди в этих системах НЕ индексированы на сервере `ULKYVM`. Напротив, сервер имён Университета Иллинойса содержит онлайн-записи для каждого студента и сотрудника — вне зависимости от того, есть ли у них учётные записи на компьютере. Там можно найти номера телефонов и адреса. Обратите внимание: приведённый список составлен по мере моих знаний, и могут существовать другие серверы.

Многие LISTSERV также имеют команду поиска людей, однако регистрация в них добровольна, а не обязательна. К тому же в результатах будут встречаться записи людей с других узлов, а не только с того, который вас интересует.

Допустим, я пытаюсь найти аккаунт Oryan QUEST и мне говорят, что он учится в Университете штата Огайо. Там есть сервер имён, и если у него есть аккаунт на их компьютере, я должен его найти:

```
VM/CMS:      TELL WHOIS@OHSTVMA Quest
```

```
VMS/JNET:    SEND WHOIS@OHSTVMA "Quest"
```

Этот конкретный сервер требует только ввода имени человека — без команды «search». У некоторых серверов это обязательно. Лучше всего сначала отправить команду `HELP` и получить документацию.

Возвращаясь к примеру: записи «Quest», к сожалению, нет, и я ничего не нашёл. Следовало с самого начала понять, что ни один колледж вряд ли зачислил бы Oryan QUEST — моя ошибка.

В любом случае настоятельно рекомендую зарегистрироваться на `UMNEWS@MAINE` и `BITSERVE@CUNYVM`. Это популярные общенациональные серверы, которые часто используются для поиска людей.

Форумы, дайджесты и электронные журналы

Концепция списков рассылки получила новую жизнь с появлением компьютерных сетей. Почти каждый состоит в каком-нибудь списке рассылки: журналы, счета или буклеты от конгрессмена. Компьютерные сети привнесли в списки рассылки принципиально новые скорость и функциональность, как вы сами убедитесь.

В Bitnet списки рассылки используются главным образом для поддержания контакта между людьми со схожими интересами. Существует несколько форматов такого общения: «форумы», «дайджесты» и «электронные журналы».

ФОРУМЫ — наглядный пример расширения возможностей списков рассылки в Bitnet. Предположим, вы подписались на форум для поклонников киберпанка (о том, как подписаться, расскажу позже). Другой участник списка отправляет письмо на сервер, где хранится список. Сервер пересылает письмо всем участникам форума. Когда письмо из форума появляется в вашем почтовом ящике, заголовок выглядит примерно так:

```
Date:         Fri, 10 Sep 88 23:52:00 EDT
Reply-To:     CYBER Discussion List <CYBER-L@PUNKVM>
Sender:       CYBER Discussion List <CYBER-L@PUNKVM>
From:         Sir Francis Drake <DRAKE@WORMVM>
Subject:      Invasion From X-Neon!
To:           Solid State <SEKER@PLPVMA>
================================================================================
```

Выглядит немного запутанно, но разобраться несложно. В этом примере Sir Francis Drake («From:») отправил письмо на адрес списка `CYBER-L`. Сервер переслал письмо всем участникам списка, в том числе Solid State («To:»). Обратите внимание на строку «Reply-To:»: она указывает вашей почтовой программе, что ответ на письмо следует направить в список — то есть *всем* участникам. Люди будут отвечать на ваши письма, и так складывается форум.

Некоторые форумы весьма интересны, но злоупотребление дайджестами создаёт проблемы. Прежде всего — огромный объём почты. В активном форуме за один день можно получить 50 и более писем. Если тема острая или эмоциональная — ждите ещё больше.

Многие склонны к «флеймингу» (термин Bitnet для задиристых нападок). Скорость и непосредственность электронной почты очень легко провоцируют на быстрый эмоциональный ответ, порождающий цепочку похожих. Советую не торопиться и хорошенько обдумывать ответы на сообщения форума, прежде чем нечаянно развязать «флейм-войну». Хочется надеяться, что любой, кто имеет доступ к университетскому компьютеру, достаточно зрел, чтобы не опускаться до подобных перепалок.

ДАЙДЖЕСТЫ предлагают частичное решение этих проблем. В данном случае письма, отправляемые в список рассылки, не рассылаются сразу, а накапливаются. Через некоторое время «модератор» списка систематизирует и конденсирует всю переписку за день или неделю и отправляет её участникам списка единым письмом.

Недостаток такого подхода — необходимость активного человеческого участия. Если модератор заболевает, уходит в отпуск или бросает дело, деятельность конкретного дайджеста может полностью замереть.

ЭЛЕКТРОННЫЕ ЖУРНАЛЫ развивают концепцию дайджеста на шаг вперёд. Эти рассылки фактически воспроизводят структуру и формат «настоящих» журналов. Bitnet служит удобным и недорогим каналом их распространения. Периодичность выпуска варьируется от еженедельной до ежеквартальной или «когда редактор сочтёт нужным» (немного напоминает выпуски Phrack). Это наиболее формальный и структурированный способ общения в Bitnet. Если дайджест — это просто набор писем, сгруппированных по темам, то электронный журнал включает статьи, колонки и рубрики. Пожалуй, единственное, чего в нём нет в отличие от бумажного журнала, — реклама. Bitnet NetMonth и NetWeek — одни из лучших журналов в Bitnet; в них содержится полезная информация для тех, кто знает, что ищет. О том, как подписаться на эти журналы и другие виды медиа, я расскажу в следующей части файла.

Серверы списков рассылки

В предыдущем разделе я упомянул, что одни серверы используются для управления списками рассылки. Сервер, выполняющий эту функцию, называется «сервером списков» (list server). Почти все они имеют userid `LISTSERV` — например, `LISTSERV@BITNIC`. Один такой сервер способен управлять подписками на множество списков рассылки. Другая концепция, связанная с LISTSERV, — идентификаторы списков (list-ids), но они сравнительно несущественны и различаются от сервера к серверу, поэтому здесь я их не рассматриваю. Если вы хотите узнать о них подробнее, обратитесь к ближайшему LISTSERV и запросите документацию командой HELP.

Для подписки на список рассылки отправьте LISTSERV команду SUBSCRIBE со следующим синтаксисом:

```
SUBscribe listname (любое имя на ваш выбор)
```

В этом примере SpyroGyra отправляет `LISTSERV@BITNIC` команду подписки на `ETHICS-L`:

```
VM/CMS:      TELL LISTSERV@BITNIC SUB ETHICS-L SpyroGyra
VMS/JNET:    SEND LISTSERV@BITNIC "SUB ETHICS-L SpyroGyra"
```

Если при вводе команды SUBscribe вы допустили опечатку в имени, просто отправьте её повторно с правильным написанием. Чтобы удалить имя из списка рассылки, SpyroGyra отправит команду UNSUBscribe:

```
VM/CMS:      TELL LISTSERV@BITNIC UNSUB ETHICS-L
VMS/JNET:    SEND LISTSERV@BITNIC "UNSUB ETHICS-L"
```

Во многих случаях вместо UNSUB используется команда SIGNOFF, но описанных базовых команд достаточно для работы со списками рассылки под управлением LISTSERV. Тем не менее LISTSERV обладает множеством возможностей, поэтому рекомендую ознакомиться с его документацией.

Примечание. Если вы работаете в VAXcluster, команды SUBSCRIBE и UNSUBSCRIBE следует отправлять на LISTSERV по ПОЧТЕ.

Ретрансляторы (Relays)

Ретранслятор, пожалуй, один из наиболее понятных типов серверов. Если вы пользовались CB Simulator на CompuServe или знакомы с Diversi-Dials (или, возможно, ALTOS Chat), вы быстро ухватите суть. Идея ретранслятора — дать возможность более чем двум людям вести беседу с помощью интерактивных сообщений. Без серверов-ретрансляторов это было бы невозможно.

Рассмотрим пример:

Sluggo, Taran и Mentor находятся на разных узлах. Любые двое из них могут переписываться через Bitnet. Но если все трое захотят поговорить одновременно, возникает проблема. Sluggo может отправлять сообщения Mentor, но Taran их не увидит. Точно так же Taran может писать Sluggo, но тогда Mentor будет не в курсе. Им нужна телеконференция. Поскольку Alliance в Bitnet не существует, были созданы ретрансляторы.

Каждый из пользователей «входит» на ближайший ретранслятор и выбирает канал (0–999, хотя есть и дополнительные, зарезервированные для особых нужд). Вместо того чтобы писать напрямую Taran или Sluggo, Mentor отправляет свои сообщения ретранслятору. Система ретранслятора пересылает его сообщение *обоим* — Taran и Sluggo. Остальные пользователи поступают так же. По окончании разговора они «выходят».

Ретрансляторы отличают команды от текста сообщений по наличию косой черты «/» в начале строки. Например, команда HELP выглядит так:

```
VM/CMS:      TELL RELAY@UIUCVMD /HELP
VMS/JNET:    SEND RELAY@UIUCVMD "/HELP"
```

Сообщение в ходе разговора отправляется следующим образом:

```
VM/CMS:      TELL RELAY@UIUCVMD Hello there!
VMS/JNET:    SEND RELAY@UIUCVMD "Hello there!"
```

При первом использовании ретранслятора необходимо зарегистрироваться с помощью команды `/SIGNUP` или `/REGISTER`:

```
VM/CMS:      TELL RELAY@UIUCVMD /REGISTER (Выберите имя)
VMS/JNET:    SEND RELAY@UIUCVMD "/REGISTER (Выберите имя)"
```

Предполагается использование настоящего имени; используйте его, если хотите, но проверить это в действительности невозможно, если только кто-то из операторов не является консультантом на вашем узле и не заглянет в вашу учётную запись. Просто выбирайте правдоподобно звучащие имена — и всё будет в порядке.

После этого можно войти, используя псевдоним или хэндл. В следующем примере я вхожу на канал 260 с ником «KLightning»:

```
VM/CMS:      TELL RELAY@UIUCVMD /SIGNON KLightning 260
VMS/JNET:    SEND RELAY@UIUCVMD "/SIGNON KLightning 260"
```

Затем можно отправлять сообщения непосредственно ретранслятору:

```
VM/CMS:      TELL RELAY@UIUCVMD Good evening.
VMS/JNET:    SEND RELAY@UIUCVMD "Good evening."
```

Сообщения ретранслятора появляются на экране следующим образом. Обратите внимание на ник в начале сообщения: когда вы отправляете сообщение ретранслятору, он автоматически добавляет к нему ваш ник при пересылке другим пользователям:

```
FROM UIUCVMD(RELAY): <Taran_King> Hello KLightning.
```

Чтобы узнать, кто находится на вашем канале, используйте команду `/WHO`. В следующем примере кто-то запрашивает список пользователей канала 260:

```
VM/CMS:      TELL RELAY@UIUCVMD /WHO 260
VMS/JNET:    SEND RELAY@UIUCVMD "/WHO 260"
```

Ответ ретранслятора выглядит так:

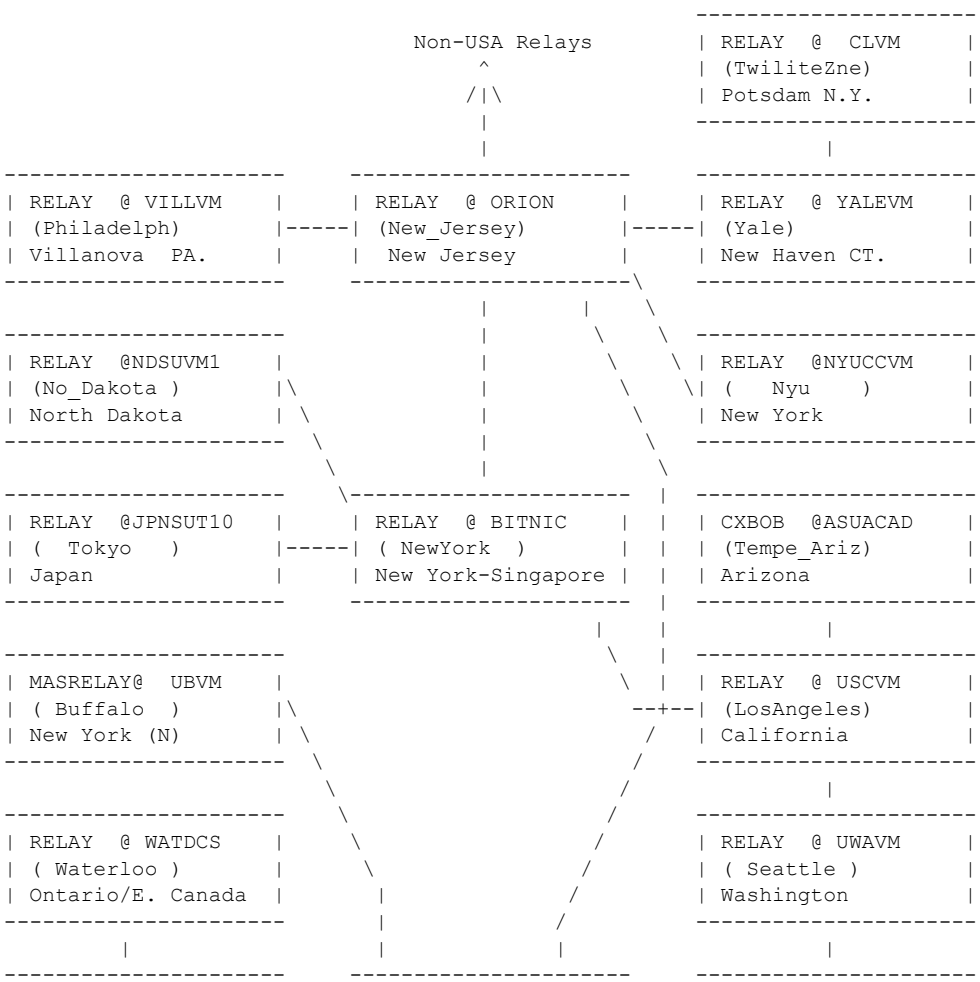
```
FROM UIUCVMD(RELAY): Ch    UserID @ Node     Nickname
FROM UIUCVMD(RELAY): 260   C483307@UMCVMB   (KLightning)
FROM UIUCVMD(RELAY): 260    MENTOR@PHOENIX  (The_Mentor)
FROM UIUCVMD(RELAY): 260   C488869@UMCVMB   (Taran_King)
FROM UIUCVMD(RELAY): 260   PROPHET@PHOENIX  (  Prophet )
FROM UIUCVMD(RELAY): 260     DRAKE@WORMVM   (   Sfd    )
FROM UIUCVMD(RELAY): 260    JESTER@NDSUVM1  (  Sluggo  )
FROM UIUCVMD(RELAY): 260       TUC@RACS3VM  (   Tuc    )
FROM UIUCVMD(RELAY): 260     VINNY@LODHVMA  (Lex_Luthor)
```

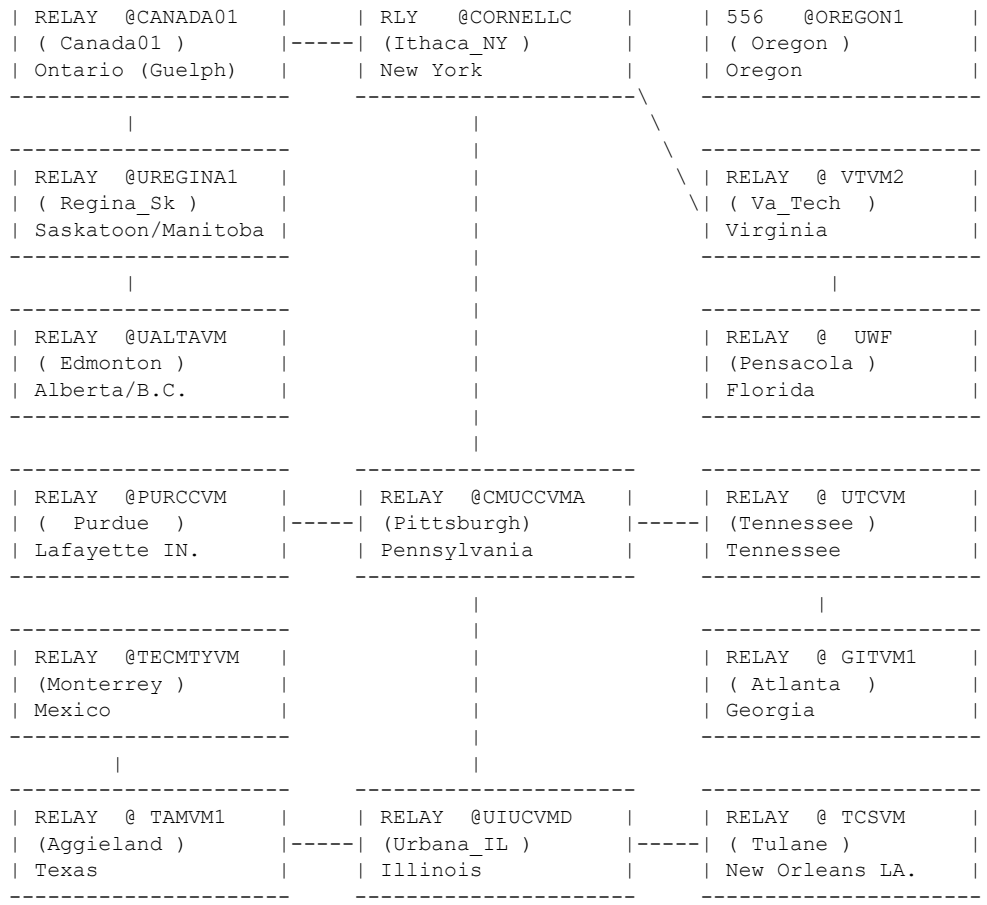
По завершении разговора можно выйти из ретранслятора:

```
VM/CMS:      TELL RELAY@UIUCVMD /SIGNOFF or /BYE
VMS/JNET:    SEND RELAY@UIUCVMD "/SIGNOFF" or "/BYE"
```

Существуют и другие команды — для просмотра активных каналов, отправки личных сообщений и так далее. При первой регистрации вам будет прислана документация. Также можно получить её с помощью команды `/INFO`. Чтобы определить, какой ретранслятор обслуживает ваш регион, отправьте любому из ретрансляторов, перечисленных в `BITNET SERVERS`, команду `/SERVERS`. Кроме того, из-за ограничений на трафик сообщений и файлов в Bitnet многие ретрансляторы доступны только по вечерам и в выходные дни.

Для наглядного объяснения принципа работы ретрансляторов привожу карту (только узлы в США):





RELAY @ VILLVM		RELAY @ ORION		RELAY @ YALEVM
(Philadelph)	-----	(New_Jersey)	-----	(Yale)
Villanova PA.		New Jersey		New Haven CT.

Заключение

Что же лежит за пределами Bitnet? Существует множество других сетей, схожих с Bitnet как по функциям, так и по сервисам. О том, как отправлять почту в эти сети, пойдёт речь в следующей главе «Саги о Грядущем Трансцендентном» — «Лимб до бесконечности».

:Knight Lightning

Индексный файл UTOPIA 1

Учреждения-члены сети BITNET

Декабрь 1988 года

Данный файл представляет собой справочный список учреждений-членов сети BITNET по состоянию на декабрь 1988 года. Список включает университеты, колледжи, национальные лаборатории, исследовательские институты и корпоративные организации, подключённые к сети BITNET.

[Таблица из 430 записей — опущена]

Источник: UTOPIA Index File 1, BITNET Member Institutions, December 1988

UTOPIA Index File 2 — Члены сети BITNET

Декабрь 1988 года

Ниже приведён список организаций — членов сети BITNET по состоянию на декабрь 1988 года, сгруппированных по штатам США.

AK — Аляска

• University of Alaska

AL — Алабама

• Auburn University
• Samford University
• University of Alabama
• University of Alabama at Birmingham
• University of South Alabama

AR — Арканзас

• University of Arkansas
• University of Arkansas at Little Rock
• University of Arkansas for Medical Sciences

AZ — Аризона

• Arizona State University
• Maricopa County Community College District
• Northern Arizona University
• University of Arizona

CA — Калифорния

• California Institute of Technology
• California Polytechnic State University-San Luis Obispo
• California State University
• Claremont Graduate School
• Electric Power Research Institute
• Harvey Mudd College
• IBM Almaden Research Center
• Lawrence Berkeley Laboratory

• Naval Postgraduate School
• Pepperdine University
• Pomona College
• Research Libraries Group
• Salk Institute
• San Diego Supercomputer Center
• Santa Clara University
• Stanford Linear Accelerator Center
• Stanford Synchrotron Radiation Laboratory
• Stanford University
• University of California
• University of California Berkeley
• University of California Davis
• University of California Irvine
• University of California Los Angeles
• University of California Riverside
• University of California San Diego
• University of California San Francisco
• University of California Santa Barbara
• University of California Santa Cruz
• University of Southern California

CO — Колорадо

• Colorado School of Mines
• Colorado State University
• National Center for Atmospheric Research
• University of Colorado at Boulder
• University of Colorado at Colorado Springs
• University of Colorado at Denver
• University of Colorado Health Sciences Center
• University of Denver

CT — Коннектикут

• Connecticut College
• Connecticut State University System
• Trinity College
• University of Connecticut
• University of Hartford
• Wesleyan University
• Yale University

DC — Округ Колумбия

• American University
• Catholic University of America
• Food and Drug Administration

• Gallaudet University
• George Washington University
• Georgetown University
• Georgetown University Medical Center
• Howard University
• National Academy of Sciences
• National Science Foundation
• Smithsonian Institution
• The World Bank
• University of the District of Columbia

DE — Делавэр

• University of Delaware

FL — Флорида

• Florida Central Regional Data Center
• Florida Northeast Regional Data Center
• Florida State University
• Southeast Regional Data Center/FIU
• University of Central Florida
• University of Florida
• University of North Florida
• University of West Florida

GA — Джорджия

• Emory University
• Georgia Institute of Technology
• Georgia State University
• University of Georgia Athens

HI — Гавайи

• The Center for Cultural & Tech Exchange Btwn East and West
• University of Hawaii

IA — Айова

• Drake University
• Grinnell College
• Iowa State University
• University of Iowa

ID — Айдахо

• Boise State University
• University of Idaho

IL — Иллинойс

• Argonne National Laboratory
• College of DuPage
• De Paul University
• Educational Computing Network of Illinois
• Fermi National Accelerator Laboratory
• Illinois Institute of Technology
• Loyola University of Chicago
• Northern Illinois University
• Northwestern University
• Southern Illinois University
• Southern Illinois University at Edwardsville
• University of Chicago
• University of Illinois at Urbana-Champaign
• University of Illinois Chicago

IN — Индиана

• Ball State University
• Indiana State University
• Indiana University
• Indiana University/Purdue University at Indianapolis
• Purdue University
• Rose-Hulman Institute of Technology
• University of Notre Dame
• Valparaiso University

KS — Канзас

• Kansas State University
• University of Kansas
• University of Kansas Medical Center
• Wichita State University

KY — Кентукки

• Transylvania University
• University of Kentucky
• University of Louisville

LA — Луизиана

• Louisiana State University
• Louisiana State University Medical Center
• Tulane University
• University of New Orleans

MA — Массачусетс

• Amherst College
• Babson College
• Bentley College
• Boston College
• Boston University
• Brandeis University
• Clark University
• College of the Holy Cross
• Hampshire College
• Harvard University
• IBM VNET Gateway
• Massachusetts Institute of Technology
• Mount Holyoke College
• Northeastern University
• Regents Computer Network
• Smith College
• Southeastern Massachusetts University
• Tufts University
• University of Massachusetts at Amherst
• University of Massachusetts at Boston
• Williams College
• Worcester Polytechnic Institute

MD — Мэриленд

• American Assoc of State Colleges Univs (AASCU) Meeting
• Biotechnology Research Center
• Catonsville Community College
• Johns Hopkins University
• Loyola College
• Montgomery College
• National Aeronautics and Space Administration
• National Bureau of Standards
• National Institutes of Health
• Naval Health Sciences Education and Training Command
• Space Telescope Science Institute
• Towson State University
• Uniformed Services University of the Health Sciences
• University of Maryland

ME — Мэн

• Bowdoin College
• The Jackson Laboratory
• University of Maine

MI — Мичиган

• Albion College
• Central Michigan University
• Macomb Community College
• Merit Computer Network
• Michigan State University
• Michigan Technological University
• Oakland Community College
• University of Michigan
• Wayne State University

MN — Миннесота

• Control Data Corporation
• Gustavus Adolphus College
• Macalester College
• State University System of Minnesota System Office
• University of Minnesota
• University of Minnesota at Morris
• University of Minnesota Duluth

MO — Миссури

• Northeast Missouri State University
• Saint Louis University
• Southwest Missouri State University
• University of Missouri
• Washington University

MS — Миссисипи

• Mississippi State University
• University of Mississippi
• University of Southern Mississippi

MT — Монтана

• Montana State University

NC — Северная Каролина

• Appalachian State University
• Davidson College
• Duke University
• East Carolina University
• National Institute of Environmental Health Sciences
• North Carolina State University
• Triangle Universities Computation Center
• Triangle Universities Nuclear Laboratory
• United States Environmental Protection Agency
• University of North Carolina at Chapel Hill
• University of North Carolina at Charlotte
• University of North Carolina at Greensboro
• University of North Carolina Gen Ad Cntrl Off Ed Comptng Srvs

ND — Северная Дакота

• North Dakota Higher Education Computer Network

NE — Небраска

• University of Nebraska - Omaha
• University of Nebraska Computer Services Network
• University of Nebraska Lincoln
• University of Nebraska Medical Center

NH — Нью-Гэмпшир

• Dartmouth College
• University of New Hampshire

NJ — Нью-Джерси

• BITNET Network Information Center
• Drew University
• Educational Testing Service
• EDUCOM
• Exxon Research and Engineering Company
• Institute for Advanced Study
• Jersey City State College
• John Von Neumann Center
• New Jersey Educational Computer Network

• New Jersey Institute of Technology
• Princeton University
• Rutgers University
• Saint Peter's College
• Seton Hall University
• Stevens Institute of Technology
• Trenton State College
• University of Medicine & Dentistry of New Jersey

NM — Нью-Мексико

• Los Alamos National Laboratory
• New Mexico State University
• University of New Mexico

NV — Невада

• University of Nevada

NY — Нью-Йорк

• American Institute of Physics
• American Physical Society
• Association for Computing Machinery
• BITNET-Internet Gateway
• Brookhaven National Laboratory
• Canisius College
• City University of New York CUNY
• Clarkson University
• Cold Spring Harbor Laboratory
• Colgate University
• Columbia University
• Columbia University Teachers College
• Cornell University
• Fordham University
• General Electric Corporate Research & Development
• Hofstra University
• IBM Watson Scientific Research Center Yorktown
• Iona College
• Ithaca College
• Le Moyne College
• Long Island University
• Manhattan College
• Marist College
• NASA Goddard Institute for Space Studies
• New York State College of Ceramics at Alfred University
• New York University
• Pace University Pleasantville-Briarcliff Campus

• Polytechnic University
• Pratt Institute
• Rensselaer Polytechnic Institute
• Rochester Institute of Technology
• Rockefeller University
• Skidmore College
• St. Lawrence University
• State University of New York Ag and Tech College at Canton
• State University of New York Ag and Tech College at Farmingdale
• State University of New York at Albany
• State University of New York at Binghamton
• State University of New York at Buffalo
• State University of New York at Stony Brook
• State University of New York Central Administration
• State University of New York College at Brockport
• State University of New York College at Buffalo
• State University of New York College at Cortland
• State University of New York College at Fredonia
• State University of New York College at Geneseo
• State University of New York College at New Paltz
• State University of New York College at Old Westbury
• State University of New York College at Oneonta
• State University of New York College at Oswego
• State University of New York College at Plattsburgh
• State University of New York College at Potsdam
• State University of New York College of Technology at Alfred
• State University of New York College of Technology at Delhi
• State U of New York Health Science Center at Brooklyn
• Syracuse University
• Union College
• University of Rochester
• Vassar College

OH — Огайо

• Bowling Green State University
• Case Western Reserve University
• Chemical Abstracts Service
• Cleveland State University
• Denison University
• John Carroll University
• Kent State University
• Medical College of Ohio
• Miami University
• Oberlin College
• Ohio State University
• Ohio University
• Ohio Wesleyan University
• Online Computer Library Center (OCLC)
• University of Akron

• University of Cincinnati
• University of Dayton
• University of Toledo
• Wright State University
• Xavier University
• Youngstown State University

OK — Оклахома

• Oklahoma State University
• University of Oklahoma Norman Campus
• University of Tulsa

OR — Орегон

• Lewis and Clark College
• Oregon State University
• Portland State University
• Reed College
• Shriners Hospital for Crippled Children
• University of Oregon

PA — Пенсильвания

• Allegheny College
• Annenberg Research Institute
• Bryn Mawr College
• Bucknell University
• Carnegie Mellon University
• Dickinson College
• Drexel University
• Franklin and Marshall College
• Gettysburg College
• Haverford College
• Indiana University of Pennsylvania
• Lafayette College
• Lehigh University
• Millersville University of Pennsylvania
• Pennsylvania State University
• Rohm and Haas Company
• Swarthmore College
• Temple University
• University of Pennsylvania
• University of Pittsburgh
• University of Scranton
• Villanova University
• West Chester University of Pennsylvania

PR — Пуэрто-Рико

• National Astronomy and Ionosphere Center
• University of Puerto Rico

RI — Род-Айленд

• Brown University
• University of Rhode Island

SC — Южная Каролина

• Clemson University
• Medical University of South Carolina
• The Citadel, The Military College of South Carolina
• University of South Carolina

SD — Южная Дакота

• Dakota State College
• South Dakota State University

TN — Теннесси

• East Tennessee State University
• Oak Ridge National Laboratory
• Rhodes College
• Tennessee Technological University
• University of Tennessee
• University of Tennessee at Chattanooga
• University of Tennessee at Knoxville
• University of Tennessee at Memphis
• Vanderbilt University

TX — Техас

• Abilene Christian University
• Baylor University
• Pan American University
• Rice University
• Saint Mary's University of San Antonio
• Sam Houston State University
• Southern Methodist University
• Southwest Texas State University

• Stephen F. Austin State University
• Tarleton State University
• Texas A&M University
• Texas Christian University
• Texas Tech University
• Trinity University
• University of Houston
• University of Houston at Clear Lake
• University of North Texas
• University of Texas at Arlington
• University of Texas at Austin
• University of Texas at Dallas
• University of Texas at El Paso
• University of Texas at Houston
• University of Texas at San Antonio
• University of Texas Health Science Center at San Antonio
• University of Texas Medical Branch at Galveston
• University of Texas Southwestern Medical Center at Dallas
• University of Texas System

UT — Юта

• Brigham Young University
• University of Utah
• Utah State University

VA — Вирджиния

• College of William and Mary
• Continuous Electron Beam Accelerator Facility
• George Mason University
• James Madison University
• National Radio Astronomy Observatory
• Old Dominion University
• Radford University
• United States Geological Survey
• University of Richmond
• University of Virginia
• Virginia Commonwealth University
• Virginia Community College System
• Virginia Polytechnic Institute and State University

VT — Вермонт

• Middlebury College
• Norwich University
• Saint Michael's College
• University of Vermont

WA — Вашингтон (штат)

• Fred Hutchinson Cancer Research Center
• Pacific Lutheran University
• University of Washington
• Washington State University
• Western Washington University

WI — Висконсин

• Lawrence University
• Marquette University
• Medical College of Wisconsin
• University of Wisconsin - La Crosse
• University of Wisconsin - Oshkosh
• University of Wisconsin - Stout
• University of Wisconsin Eau Claire
• University of Wisconsin Madison
• University of Wisconsin Milwaukee

WV — Западная Вирджиния

• Marshall University
• West Virginia Network for Educational Telecomputing

WY — Вайоминг

• University of Wyoming

Серьёзный взгляд на взлом VMS

Автор: VAXbusters International

Январь 1989

Операционная система VAX/VMS считается одной из наиболее защищённых из доступных на сегодняшний день. На протяжении последних лет она претерпела масштабные доработки, призванные помочь системным администраторам надёжно закрыть машины от злоупотреблений и отследить любые попытки обойти защиту. В результате проникнуть в VMS-систему без знания внутренней кухни стало совсем непросто, а остаться незамеченным — ещё труднее.

Следующая статья описывает ряд внутренних механизмов, на которых строится безопасность VMS, и даёт подсказки о том, как остаться незамеченным. Читатель должен быть знаком с системой VMS с точки зрения программиста.

Некоторые из рассматриваемых вещей тесно связаны с внутренним устройством VAX/VMS. Все описания намеренно остаются на общем уровне. Цель — обозначить слабые места системы, а не давать пошаговые инструкции по взлому VMS-машин. Главная причина такого подхода состоит в том, что оставаться в VMS-системе незамеченным без глубокого знания всей системы крайне сложно. Это знание приходит только с опытом.

Для практического применения части описанных техник рекомендуется следующая литература:

«The VAX Architecture Handbook», издание DEC. Книга описывает процессор VAX, его систему команд и аппаратную часть. Полезно иметь под рукой — она распространяется бесплатно (достаточно зайти в ближайший магазин DEC и попросить) и выходит только в мягкой обложке.

«MACRO and Instruction Set», часть документационного комплекта VMS. Необходима, если вы планируете писать серьёзные программы на MACRO. Рекомендуется к прочтению, хотя держать её под рукой постоянно необязательно.

«VAX/VMS Internals and Data Structures» Л. Кены и С. Бейта. Это библия VMS-хакера. Описывает внутреннее устройство системы и большинство структур данных, используемых в ядре. Опубликованная версия всегда отстаёт на один номер от текущего релиза VMS, но поскольку архитектура VAX не меняется, это лучший источник для понимания того, как работает система. Прочитав и усвоив эту книгу, вы перестанете считать VAX чем-то загадочным — он окажется не сложнее вашего C64. Заказать книгу можно в DEC, номер заказа для версии V3.0 — EY-00014-DP. Главный недостаток — цена, около $70–100.

Хорошим источником информации, разумеется, служит исходный код самой VMS. Проще всего изучать его через набор микрофиш, которые DEC поставляет всем крупным заказчикам системы. Основное неудобство — для работы с ними нужен фиш-ридер. Микрофиши необходимы, если вы намерены вносить изменения в системный код, — если только вы не собираетесь дизассемблировать всё, что нужно. Система VMS написана на BLISS-32 и FORTRAN. BLISS вполне читаем, однако если вы планируете патчить программы, реализованные на FORTRAN, стоит иметь под рукой знатока этого языка. Микрофиши всегда содержат текущий релиз, поэтому они полезны для проверки актуальности сведений из «Internals and Data Structures».

Инструменты хакера

Есть несколько программ, полезных при исследовании VMS-системы.

Пожалуй, самая важная из них — System Dump Analyzer (SDA), запускаемый командой ANALYZE/SYSTEM. Изначально SDA разрабатывался для анализа дампов аварийного завершения системы, которые создаются каждый раз, когда машина «падает» контролируемым образом (bugcheck или opcrash). SDA можно также использовать для анализа работающей системы, и это его более полезная функция. Для запуска SDA процессу требуется привилегия CMKRNL. С помощью SDA можно исследовать любой процесс и получить сведения об открытых файлах и устройствах, содержимом виртуальной памяти (например, буферах ввода с клавиатуры и буферах отзыва), статусе процесса и многом другом. SDA — инструмент наблюдения, поэтому в штатном режиме что-либо сломать с его помощью нельзя.

Ещё один полезный инструмент — утилита PATCH, вызываемая одноимённой командой. Поскольку VMS распространяется только в бинарном виде, обновления системы обычно поставляются в форме патчей для исполняемых файлов. Патчи можно вводить непосредственно в виде инструкций ассемблера. В сочетании с микрофишами с исходным кодом PATCH становится мощным инструментом для модификации и доработки операционной системы VMS.

Привилегии

Чтобы делать на VMS-системе что-то интересное, как правило, нужны привилегии. Ниже перечислены некоторые из тех, что полезны в повседневной практике.

CMKRNL
CMEXEC — эти две привилегии позволяют пользователю выполнять произвольные подпрограммы с режимом доступа KERNEL и EXECUTIVE соответственно. Они необходимы для прямого обращения к структурам данных ядра. CMKRNL — наиболее мощная из доступных привилегий: с её помощью можно получить доступ ко всему, что защищено в системе.

SYSPRV — процесс, владеющий этой привилегией, может обращаться к объектам через системную защиту. Права доступа такого процесса совпадают с правами процесса, работающего под системным UIC.

SHARE — позволяет процессу назначать каналы несовместно используемым устройствам, к которым уже назначены каналы. Это можно использовать для предотвращения зависания терминалов и назначения каналов системным почтовым ящикам.

Состояния процессов и блок управления процессом

Приступая к хакингу ядра, обратите особое внимание на поле PCB$L_STS. Оно отражает статус процесса. Интересные биты — PCBV_DELPEN, PCBV_NOACNT и PCB$V_BATCH. Установка этих битов позволяет добиться поразительных эффектов.

Укрытие

Приятная возможность — оставаться невидимым для системного администратора. Существует много способов скрыться от SHOW USERS, однако скрыться от SHOW SYSTEM — совсем другая история: эта команда не использует стандартные системные вызовы для получения списка запущенных процессов. Скрыться от SDA ещё сложнее — он напрямую читает структуры данных ядра. Тем не менее невидимость для SHOW USERS полезна на небольших системах, где лишний пользователь может поднять тревогу у оператора.

Один из вариантов — стать подпроцессом какого-нибудь неинтерактивного задания (например, процесса BATCH или NETWORK). Другой способ — пропатчить PCB, превратив себя в BATCH-процесс, или удалить имя терминала (что заставит `SHOW USERS` считать вас неинтерактивным). Патчинг PCB имеет один недостаток: прежде чем спрятаться, нужно непосредственно уменьшить на единицу системную глобальную переменную `SYS$GW_IJOBCNT`, содержащую количество интерактивных пользователей, а перед выходом из системы — увеличить её обратно.

Если об этом забыть, счётчик интерактивных заданий окажется неверным. Если он уйдёт в отрицательные значения, начнутся странные эффекты, которые поставят в тупик любого системного администратора.

Учёт и аудит

Самая неприятная вещь в VMS начиная с релиза 4.2 — механизм аудита безопасности. Он позволяет системному администратору протоколировать практически любое событие, связанное с безопасностью: обращения к файлам, неудачные попытки входа в систему, изменения базы данных авторизации пользователей — всё это можно отслеживать, записывать в журнал и выводить на системный принтер. Первое, что нужно выяснить на незнакомой системе, — уровень бдительности администратора. Статус системы учёта легко определить командой `SHOW ACCOUNTING`. Как правило, включено всё, кроме учёта образов (IMAGE). Если IMAGE-учёт также включён — это первый сигнал к осторожности. Второй шаг — проверка состояния системы аудита безопасности. Для выполнения команды `SHOW AUDIT` нужна привилегия `SECURITY`.

Если аудит не включён и IMAGE-учёт не ведётся, система обычно не настроена на повышенную защиту. Такие системы — подходящий полигон для хакера: здесь не нужно быть столь же осторожным, как на грамотно администрируемой машине.

Учёт ресурсов

Основная цель ведения учёта — необходимость тарифицировать пользователям потреблённые ресурсы (процессорное время, использование принтера и т. д.). С другой стороны, учёт может быть весьма полезен для отслеживания нарушителей. К счастью, учётная информация хранится в обычной файловой системе, а значит, ненужные записи можно из неё удалить. Главный инструмент для работы с учётными файлами — утилита `ACCOUNTING`. Она позволяет собирать данные из учётных файлов, выводить их в удобочитаемом виде и, что особенно важно, редактировать учётные файлы — то есть удалять из них записи, которые не должны попасть в отчёты. Ключевой квалификатор команды `ACCOUNTING` — `/BINARY`.

Один из способов обнаружить нежелательных гостей — проверить модифицированные системные файлы. К счастью, существуют способы изменить дату модификации в заголовке файла. Это делается через системные вызовы RMS, однако средствами чистого DCL удобного способа нет. В свободном доступе имеется несколько утилит для подобных операций — поищите в каталоге DECUS.

OPCOM

OPCOM — процесс, протоколирующий системные и значимые с точки зрения безопасности события (монтирование лент и дисков, сообщения аудита безопасности и т. д.). OPCOM принимает

сообщения через устройство-почтовый ящик, форматирует их, записывает в операторский журнал (SYS$MANAGER:OPERATOR.LOG) и оповещает всех операторов. Кроме того, он выводит все сообщения на стандартный вывод — обычно это системная консоль _OPA0:. При запуске OPCOM на стандартный вывод отправляется сообщение о том, что операторский журнал инициализирован. Поэтому убивать OPCOM ради сохранения анонимности не рекомендуется: системный администратор, скорее всего, забеспокоится, увидев, что журнал был инициализирован без очевидной причины. Элегантное решение — приостановить OPCOM на то время, пока операторские сообщения не должны проходить. Пока OPCOM приостановлен, все сообщения будут буферизоваться в почтовом ящике, откуда их может прочитать любой процесс с достаточными привилегиями — таким образом OPCOM не получит эти сообщения после перезапуска.

Однако у этого решения есть один изъян: OPCOM всегда держит незавершённую операцию чтения на этом почтовом ящике, и она сохраняется даже при приостановке процесса. Без глубокого хакинга ядра избавиться от этого запроса на чтение невозможно. Поэтому простое решение — сразу после приостановки OPCOM сгенерировать безобидное операторское сообщение. После этого ваш процесс (который может быть DCL-процедурой) читает все последующие сообщения из почтового ящика OPCOM до тех пор, пока вы не сочтёте, что OPCOM можно возобновить. Кстати, почтовый ящик для сообщений OPCOM является временным и не имеет назначенного логического имени. Для получения информации об имени устройства понадобится SDA.

Командные процедуры

Рано или поздно потребуются DCL-процедуры для автоматизации рутинных операций. Важно не оставлять на чужой системе подозрительные командные файлы — их легко обнаружит системный администратор. К счастью, командный файл можно удалить, пока он ещё выполняется. Хорошей практикой является делать именно так, используя лексическую функцию F$ENVIRONMENT. Если в ходе работы процедуры требуется обращаться к самому командному файлу, достаточно назначить на него канал с помощью команды OPEN.

Пигибэкинг

Как правило, добавлять новые привилегированные учётные записи на чужую систему — плохая идея. Лучше воспользоваться учётными записями, которые не использовались несколько месяцев, и спрятать привилегированные программы или пигибэки, получающие привилегии от вызывающего посредством какого-либо механизма. Пигибэк — это фрагмент кода, встраиваемый в привилегированную системную программу и предоставляющий привилегии и/или особые возможности вызывающим, обладающим определённой характеристикой (например, специальным именем процесса). Следите за тем, чтобы не изменились размеры файлов и даты — это вызовет подозрения.

Заключение

Эта статья лишь пытается дать представление о том, насколько интересен хакинг ядра VMS и какие возможности он открывает. Она, разумеется, не является исчерпывающей, и многие детали намеренно опущены. Надеемся, она оказалась полезным и/или интересным чтением.

Можете ли вы узнать, прослушивается ли ваш телефон?

```
<?><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><?>
<|>                                                                     <|>
<|>   Can You Find Out If Your Telephone Is Tapped?                     <|>
<|>                  by Fred P. Graham                                  <|>
<|>                                                                     <|>
<|>             "It Depends On Who You Ask"                             <|>
<|>                                                                     <|>
<|>                Transcribed by VaxCat                                <|>
<|>                                                                     <|>
<|>                  December 30, 1988                                  <|>
<|>                                                                     <|>
<?><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><?>
```

Автор: Fred P. Graham

«Всё зависит от того, кого спрашивать»

Расшифровано VaxCat

30 декабря 1988 г.

В отличие от большинства американцев, которые лишь подозревают слежку, Сара Бартлетт по крайней мере знает наверняка: её подслушало ФБР с помощью телефонного прослушивания в машинном зале здания Налогового управления в Вашингтоне, через улицу от Министерства юстиции. 25 апреля, когда она сидела за своим перфоратором, почтальон вручил ей заказное письмо с документом, известным в полицейских кругах как «уведомление о прослушивании». В нём говорилось, что правительству было дано разрешение перехватывать телефонные переговоры «от и до» двух вашингтонских номеров в течение пятнадцати дней после 13 января и что за этот период её собственный голос был слышен в разговорах с абонентами этих телефонов. Мисс Бартлетт ничего не сказала другим девушкам в машинном зале, однако наверняка была потрясена. Несколько недель спустя федеральные агенты пришли в машинный зал и забрали её — для предъявления ряда обвинений, сводившихся к тому, что она являлась посредником в нелегальной лотерее.

Никакой статистики, раскрывающей, сколько американцев получили подобные уведомления, не существует, а те немногие, кто их получил, предпочитают молчать. Между тем их число к настоящему времени могло превысить 50 000. Когда в 1968 году Конгресс ввёл требование об уведомлении при прослушивании, он намеревался развеять нарастающую национальную паранойю в отношении электронной слежки. Однако в обществе, кажется, не утихает подозрение, что чуть ли не каждый сколько-нибудь заметный человек прослушивается или прослушивает кого-то другого. Герман Шварц, профессор права из Буффало (штат Нью-Йорк), эксперт Американского союза гражданских свобод по вопросам государственной слежки, оценивает, что с 1968 года от 150 000 до 250 000 американцев оказались под большим ухом федерального правительства или местной полиции. «Если вы имеете какое-то отношение к азартным играм или наркотикам, если вы государственный чиновник, замешанный в каких-то делишках, если вы демократ, если вы сами или ваши друзья занимаются радикальной политикой или чёрным активизмом — вас, скорее всего, прослушивали», — говорит профессор Шварц.

Генри Киссинджер в шутку говорит друзьям, что ему незачем писать мемуары — он просто опубликует стенограммы своих телефонных разговоров, составленные ФБР. Ричард Г. Кляйндинст распорядился «прочесать» свой кабинет в Министерстве юстиции. Государственный секретарь Уильям П. Роджерс однажды уклонился от обсуждения китайской политики по телефонной линии

либерального газетного обозревателя. Высокопоставленные чиновники Нью-Йорка, Вашингтона и Олбани получили от прокуратуры Нью-Йорка уведомления о том, что могут стать мишенями вымогателей: их визиты в роскошный манхэттенский публичный дом были записаны на скрытые жучки. Специалист, регулярно проверяющий кабинет губернатора Мэриленда Марвина Мэнделя, недавно обнаружил, что телефон гражданской обороны, которого ему было велено не касаться, подключён для прослушивания комнаты, когда трубка лежит на рычаге. Функционеры-демократы негодовали по поводу пятерых людей с республиканскими связями, пойманных при попытке установить жучки в штабе Национального комитета Демократической партии в отеле «Уотергейт», однако когда ранее они сами обнаружили менее убедительные доказательства аналогичной деятельности, то предпочли промолчать. Комплексный закон о борьбе с преступностью 1968 года делает прослушивание телефонного разговора или частной беседы без судебного ордера уголовным преступлением, наказуемым пятью годами лишения свободы и штрафом в 10 000 долларов. Только федеральные правоохранительные органы и местные прокуроры в штатах, принявших аналогичное законодательство о прослушивании, могут получить судебное разрешение на прослушку; закон также требует, чтобы в течение девяноста дней после отключения подслушивающего устройства уведомления о прослушивании были отправлены всем, чьи телефоны или помещения прослушивались, а также всем прочим (как Сара Бартлетт), чьи слова были записаны и кто впоследствии может быть привлечён к ответственности.

Однако из-за ряда частных сыщиков и просто любопытных личностей никто не знает, сколько людей нарушают закон о прослушивании и остаются безнаказанными; а поскольку ни одно из правил, регулирующих санкционированное судом прослушивание в обычных уголовных расследованиях, не распространяется на несанкционированное правительственное прослушивание под предлогом «национальной безопасности», никто не может быть уверен в безопасности своего телефона. До того как Верховный суд в прошлом июне восемью голосами против нуля постановил, что правительство обязано получать ордера на прослушивание отечественных радикалов в делах о национальной безопасности, ФБР прослушивало как доморощенных, так и иностранных «подрывных элементов» без судебных санкций. По лучшим оценкам, на долю таких прослушиваний приходилось от 54 000 до 162 000 из 150 000–250 000 человек, попавших под слежку с 1968 года.

После того как несанкционированное прослушивание отечественных радикалов было запрещено, число лиц, прослушиваемых без ордера, как ожидается, сократится примерно на четверть. Однако даже при том, что суды требуют доводить до сведения жертв всё больше фактов правительственного прослушивания, паранойю подпитывают совершенствующиеся технологии. Прослушивание достигло такого уровня развития, что его крайне сложно обнаружить, а ещё труднее отследить до конкретного исполнителя. Самая популярная новинка наших дней — «обход рычажного переключателя» телефона, который обходит выключатель трубки и превращает аппарат в чуткий микрофон, улавливающий все звуки в комнате, пока телефон стоит на рычаге. В простейшем исполнении к клубку проводов внутри телефона добавляется небольшой цветной провод, который так же легко обнаружить, как дополнительную нитку в тарелке спагетти. Даже если его найдут, до подслушивающего всё равно вряд ли доберутся. Проверка телефонной линии, скорее всего, обнаружит крошечный передатчик в клеммной коробке где-то в том же здании или на столбе где-то дальше по улице. Тот, вероятно, будет транслировать сигнал на голосо-активируемый магнитофон, запертый в багажнике автомобиля, припаркованного где-то по соседству. Угадать, какая именно машина, будет совершенно невозможно.

Моя жена случайно узнала об этом в прошлом году, когда The New York Times схлестнулась с Министерством юстиции из-за «Документов Пентагона», а я освещал эту историю для Times. Она уверилась, что Джон Митчелл не остановится ни перед чем и что телефон в нашей спальне раскалён, как кочерга. После этого, стоило назревать супружеской головомойке или амурным делам, я всегда получал предупреждение заранее. Если в спальне собиралось произойти нечто

слишком деликатное для посторонних ушей, жена сначала поднималась с постели, пересекала комнату и торжественно выдёргивала телефонный провод из розетки. «Когда кто-то узнаёт, что другой человек получил сведения, которые ему не должны были стать известны, он обычно с ходу делает вывод, что его прослушивали», — говорит Аллан Д. Белл-младший, президент компании Dektor Counterintelligence and Security Inc. в Спрингфилде, штат Вирджиния, в окрестностях Вашингтона. «Если поразмыслить, скорее всего нашёлся какой-то иной, более простой способ, которым эта информация утекла».

Белл имеет в виду, что большинство людей получают информацию самым лёгким, дешёвым и законным путём, и тому, чьи тайны оказались скомпрометированы, следует сначала проверить: не выбрасывал ли он копии документов, не оставлял ли незапертыми свои папки, не нанял ли секретаря, которого можно подкупить, или просто не болтал ли лишнего. Однако существует важное исключение, о котором многие не подозревают. Участник разговора может тайно его записывать, не нарушая при этом никакого закона. Человек на одном конце телефонного провода может тихо фиксировать разговор (прежнее законодательное требование о периодическом предупредительном сигнале отменено). Точно так же один из участников личной беседы может спрятать диктофон в одежде. Джеймс Р. Робинсон, юрист Министерства юстиции, отвечающий за преследование нарушителей закона против прослушивания, настаивает, что это происходит сравнительно редко. Он развенчивает представление о том, что большинство случаев частной прослушки происходит в исполнительных кабинетах крупного бизнеса. За девяноста процентами поступающих к нему жалоб стоит секс, а не корпоративные интриги. После того как ревнивый супруг или любовник основательно напуган, правительство даже не утруждает себя уголовным преследованием самодеятельных прослушивателей. Если же прослушкой занимался частный детектив — на него обрушивается всей строгостью закона.

Стоимость — вот почему эксперты настаивают, что прослушивания на самом деле меньше, чем думает большинство людей. Частные сыщики, использующие электронное наблюдение, в наши дни не называют своих расценок, однако специалисты по нейтрализации подслушивающих устройств говорят, что цены варьируются от 10 000 долларов в месяц за первоклассную промышленную работу до 150 долларов в день за услуги рядового частного детектива.

Высокие расходы ограничивают и правительственное прослушивание. В прошлом году среднесуточные затраты ФБР на один подслушивающий аппарат составляли 600 долларов с учётом установки устройства, аренды телефонных линий для соединения жучков с прослушивающими пунктами ФБР, мониторинга переговоров и машинописи стенограмм. Принимая во внимание информативность переговоров большинства людей, оно того не стоит. Судебные материалы по делам о слежке ФБР показали: когда записываются откровенные разговоры, результатом чаще всего становится стенограмма, лишённая какой-либо ценности, — пустая или невразумительная.

Мифы о противодействии прослушиванию

Расхожие представления о том, как противодействовать электронной слежке, почти сплошь ошибочны или просто неверны. Говорят, что Роберт Ф. Кеннеди, будучи сенатором, однажды поверг посетителя в изумление, вскочив и с силой опустив каблуки на пол своего кабинета. Он объяснил, что таким образом сбивает жучок, который мог подсадить Дж. Эдгар Гувер. Дурачился ли он или нет, эксперты уверяют: это не дало бы никакого результата, кроме синяков на каблуках сенатора Кеннеди. Бывший сенатор от Техаса Ральф Ярборо жаловался, что с приближением каждого избирательного сезона качество связи в телефоне его кабинета ухудшалось, поскольку ток истощался многочисленными прослушивающими устройствами, подключёнными политическими противниками. Те, кто считает, что плохое качество связи и щелчки на линии вызваны

прослушиванием, воздают прослушивателям меньше чести, а AT&T — больше, чем заслуживает каждый из них. Современные подслушивающие устройства нередко питаются от собственных аккумуляторов или потребляют столь мало тока, что на фоне обычных колебаний питания их невозможно засечь даже чувствительными амперметрами.

Щелчки на линии могут быть вызваны ненадёжными контактами в телефоне, кабелях или оборудовании АТС, намокшими кабелями, неисправными коммутаторами на АТС и скачками напряжения при зарядке аккумуляторов на АТС. Современное подслушивающее устройство записывает разговор на аппарат, который бесшумно включается и выключается по мере того, как вы говорите. Подслушивающее устройство рассчитано на работу без посторонних шумов; ваш телефон — нет. Если слова, произнесённые в частной беседе или по телефону, начинают возвращаться к вам из неожиданных источников, прежде всего следует тщательно осмотреть комнату или комнаты, которые могут прослушиваться.

Обнаружение государственного прослушивания

Если прослушивает федеральное правительство, ни вы, ни почти никто, кроме самых опытных специалистов по нейтрализации жучков, этого не обнаружат. Уже много лет никто не раскрыл ни одного прослушивающего устройства Министерства юстиции, поскольку сама телефонная компания нередко подключается к линии и соединяет её с прослушивающим пунктом ФБР. Жучки ФБР стали настолько совершенными, что стандартные методы обнаружения также не позволяют их выявить. Однако прослушивание, которое устраивают многие частные сыщики, нередко настолько примитивно, что его может обнаружить даже другой дилетант. Комнатные жучки бывают двух типов: крошечные микрофоны, передающие перехваченные разговоры по проводу на сторону, и маленькие радиопередатчики, транслирующие услышанное по радио.

И те и другие, как правило, устанавливаются в электрических приборах: можно воспользоваться их питанием, их провода можно задействовать для передачи разговоров на прослушивающий пункт, а электрическая начинка приборов служит камуфляжем для электронных жучков. Ваш телефон обладает всеми этими свойствами плюс тремя встроенными усилителями, которыми может воспользоваться подслушиватель. Для начала снимите пластиковый корпус телефона и осмотрите его изнутри на предмет провода нестандартного размера или формы, который, судя по всему, пересекает нормальный ход цепей. Жучок или радиопередатчик, питающийся от источника питания и усилителей телефона, будет представлять собой цилиндр или куб размером с напёрсток, обычно залитый чёрной эпоксидной смолой и подключённый к клеммам цепи.

Кроме того, проверьте наличие аналогичных устройств вдоль телефонных проводов в комнате, а также в розетке или коробке, где телефон подключён к плинтусу. Следует также отвинтить микрофонный и слуховой капсюль и проверить, нет ли подозрительных проводов или предметов. Даже эксперт не распознает новинку, продающуюся нелегально, — «прослушанный» микрофонный капсюль, выглядящий в точности как тот, что стоит в вашем телефоне и который можно поменять за несколько секунд. После проверки телефона осмотрите подозрительные маленькие чёрные коробочки, подключённые к телевизорам, радиоприёмникам, лампам и часам.

Практические советы по поиску жучков

Также проверьте вентиляционные каналы отопительных и кондиционирующих систем на наличие микрофонов с проводами, уходящими обратно в каналы. Жучки-радиопередатчики с собственными батарейками можно установить быстро, но и обнаружить их несколько проще. Проверяйте под столами и стульями, между подушками дивана. Помните: они должны располагаться вблизи места

вероятного разговора для обеспечения хорошего приёма. Иногда радиожучки так искусно спрятаны, что обнаружить их практически невозможно. Один немецкий производитель рекламирует «прослушанные» авторучки, которыми действительно можно писать, настольные зажигалки, которые действительно зажигают огонь, и портфели, в которых действительно носят бумаги.

Замечая, что владелец таких предметов может удалиться с деликатных переговоров, оставив позади своё электронное ухо, компания указывает, что «очевидно, микрофон подобного типа открывает безграничные возможности на конференциях, переговорах, встречах и т. п.». Если вы подозреваете, что ваш телефон прослушивается, а визуальный осмотр ничего не даёт, можно обратиться в телефонную компанию с просьбой проверить линию. По оценкам American Telephone and Telegraph Company, ежегодно она получает около десяти тысяч подобных запросов от абонентов. Эти проверки, а также плановое техническое обслуживание позволяют ежегодно выявлять около двухсот пятидесяти подслушивающих устройств. При обнаружении свидетельств прослушивания компания сверяется с ФБР и местной полицией в штатах, где законы разрешают полицейское прослушивание по судебным ордерам. До недавнего времени, если прослушивание было санкционировано судом, абоненту сообщали, что «незаконных устройств» на линии нет. Это настолько выбивало из колеи людей, запросивших проверку, что теперь телефонная компания, по имеющимся сведениям, сообщает всем абонентам о любых обнаруженных устройствах. Если это оборачивается преждевременным разглашением сведений о санкционированном ФБР прослушивании — это головная боль, которую AT&T с удовольствием оставляет на откуп правительству и его подозреваемому.

Профессиональная нейтрализация подслушивающих устройств

Тем, кто сделал всё вышеперечисленное и всё равно испытывает подозрения, следующим шагом будет привлечение специалиста для обследования помещения. Тщательная работа включает в себя детальный осмотр помещения — в том числе рентгенографию настольных украшений и других предметов, которые могут содержать скрытые радиопередатчики, — использование металлодетекторов для поиска скрытых микрофонов, проверку электропроводки на признаки нестандартных токов, применение чувствительного детектора радиоволн для обнаружения паразитных сигналов, которые может излучать скрытый жучок, а также использование измерителя напряжённости радиополя для определения его местонахождения.

Поскольку для качественного обнаружения требуется столь высокая квалификацию, а лицензионных требований в большинстве штатов, которые не позволяли бы любому желающему нацепить наушники и объявить себя экспертом по нейтрализации подслушивания, не существует, неудивительно, что в этой области процветают шарлатаны. В прошлом году одна строительная компания из Пенсильвании, проигравшая серию тендеров с небольшой разницей, наняла местного частного детектива для проверки зала заседаний совета директоров на наличие жучков. Начальник службы безопасности компании, скептически отнёсшийся к приезжему «специалисту», взял обычную рацию, заклеил кнопку включения для непрерывной передачи и спрятал её за книгами на полке. Он сидел в соседней комнате и слушал, как детектив, шаркая, вошёл в зал, поводил своими приборами и объявил помещение чистым.

Порой лжеспециалисты по обнаружению жучков оказывают клиентам дополнительную «услугу»: сами подсаживают жучок и сами же его «обнаруживают» в ходе проверки. Один такой «эксперт» проделал это дважды в Лас-Вегасе с людьми, связанными с организованной преступностью; те впоследствии сравнили впечатления и поняли, что их облапошили. «Надо было видеть, как ему пришлось несладко», — хихикнул юрист Министерства юстиции, рассказавший эту историю. Если вы всё же хотите проверить своё помещение, дело осложняется тем, что телефонная компания запрещает специалистам по нейтрализации жучков рекламировать свои услуги.

Как выразилась Комиссия по коммунальным услугам штата Миссури, оставляя в силе отказ телефонной компании включить «нейтрализацию жучков» в рекламу детектива на страницах «Жёлтых страниц»: «реклама способности обнаруживать и удалять электрические устройства фактически является также рекламой способности устанавливать те же самые устройства». Можно быть достаточно уверены в надёжности, обратившись в одно из крупных общенациональных детективных агентств — Burns, Pinkerton или Wackenhut. Они берут от 40 до 60 долларов за человеко-час за работу, которая, вероятно, займёт как минимум полдня для двух специалистов. Эти агентства специализируются на промышленных делах и сторонятся семейных разбирательств. Поэтому если у вас именно такая проблема, спросите у адвоката или сотрудника полиции, какой частный сыщик в городе является наиболее надёжным специалистом по нейтрализации жучков.

Это может показаться слишком очевидным, чтобы упоминать, но не обсуждайте свои подозрения относительно прослушивания в присутствии предполагаемого жучка. У. Р. Мозли, директор отдела расследований агентства Burns, утверждает, что в большинстве случаев жертва прослушивания сама сообщает подслушивателю, что собирается вызвать специалиста по нейтрализации жучков, давая тем самым подслушивателю возможность замести следы.

Максимальная защита за деньги

Для тех, кто хочет купить столько приватности, сколько позволяют средства, компания Dektor продаёт консоль размером с манхэттенскую телефонную книгу, которую можно поставить на рабочий стол всего за 3500 долларов. Она непрерывно проверяет всевозможные способы, которыми можно использовать ваш телефон и электрические линии для перехвата разговоров. Устройство заблокирует любую попытку превратить ваш телефон в жучок, выявит любой «гармонический жучок», подавит телефонное прослушивание с помощью передатчика, транслирующего подслушиваемые разговоры, обнаружит любое использование электрических линий в целях прослушивания и издаст пронзительный сигнал «бип-бип!», если кто-то снимет параллельную трубку.

При всей изощрённости этого устройства есть одна вещь, которую его создатели не возьмутся обеспечить, — обнаружение прослушивания со стороны ФБР. Поскольку соединение осуществляется в месте, куда ни один специалист по нейтрализации жучков не получит доступа, а агенты ведут мониторинг на оборудовании, которое не выявит ни один прибор, вы просто никогда не сможете знать наверняка, слушает ли вас правительство. Поэтому если вы бизнесмен и думаете, что вас прослушивают конкуренты, — скорее всего, вы ошибаетесь. Если вы супруг или любовник, чьи амуры стали достоянием общественности, подслушивающее устройство можно найти, но дальнейших действий, вероятно, не последует. А если вас слушает самое большое ухо из всех — правительство, — вы никогда не узнаете об этом наверняка, пока не получите своё «уведомление о прослушивании».

VaxCat

Big Brother Online

Автор: Thumpr Of ChicagoLand

В духе трилогии «Порочный Круг»...
Phrack Inc. представляет

6 июня 1988 г.

Особая благодарность: Hatchet Molly

Правительство Соединённых Штатов ведёт мониторинг сообщений на ряде досок объявлений по всей стране. Именно такое утверждение выдвигает Глен Л. Робертс, автор книги «ФБР и ваша BBS» («The FBI and Your BBS»). Рукопись, опубликованная организацией The FBI Project, охватывает широкий круг тем, связанных с ФБР и BBS, однако, к сожалению, ни одну из них не рассматривает достаточно глубоко.

Книга начинается с общего исторического экскурса в деятельность ФБР по сбору информации. Оказывается, ФБР принялось аккумулировать огромные массивы сведений о гражданах, причастных к «радикальным политическим» движениям, не в 1960-е годы, как можно было бы предположить, а ещё в 1920-е! С тех пор ФБР накопило КОЛОССАЛЬНЫЙ объём информации об обычных гражданах — людях, не осуждённых ни за какое преступление, кроме активного участия в чём-либо, что ФБР считает потенциально опасным.

Рассмотрев деятельность ФБР, Робертс переходит к обсуждению того, почему слежка ФБР за системами BBS является незаконной. По его мнению, подобная слежка нарушает Первую, Четвёртую и Пятую поправки к Конституции. Однако наиболее убедительным оказывается его аргумент, касающийся Закона о конфиденциальности электронных коммуникаций 1987 года (Electronic Communications Privacy Act, ECPA). Этот закон был принят в качестве поправки к Федеральному закону о прослушивании телефонных переговоров 1968 года и изначально предназначался для защиты корпоративных компьютерных систем от вторжения «хакеров». Но, как и в случае со многими хорошими законами, он написан настолько широко, что может — и де-факто применяется — в отношении систем, находящихся в частной собственности, в том числе досок объявлений. Робертс (вкратце) рассматривает, как этот закон можно использовать для защиты *вашей* доски объявлений от слежки со стороны федеральных органов.

Как защитить свою BBS

Не храните сообщения дольше 180 дней. Закон составлен таким образом, что сообщения возрастом менее 180 дней пользуются более высокой степенью защиты, чем более старые. Поэтому для максимальной защиты системы очищайте, архивируйте или перезагружайте базу сообщений примерно каждые 150 дней. Это может показаться абсурдным, но усложнит процедуру (добавит бюрократических препон) получения правительством ордера на обыск и обязательного уведомления оператора/подписчика службы о предстоящем обыске. Робертс не вполне чётко излагает эту позицию, однако его посыл однозначен: чем чаще вы обновляете базу сообщений, тем лучше вы защищены.

Пожалуй, лучший способ защитить свою BBS — сделать её закрытой системой. Это означает отказ от «мгновенного доступа» для звонящих (я знаю крайне мало андеграундных досок, предоставляющих его в любом случае) и невозможность вступления в систему для кого попало. Иными словами, даже если вы заставляете пользователей ждать 24 часа для получения доступа

после верификации, вам всё равно необходимо чётко разграничивать, кого верифицировать, а кого нет. Ваша BBS должна быть ЗАКРЫТОЙ системой, и вам следует принимать меры для обеспечения и декларирования ОЖИДАЕМОЙ КОНФИДЕНЦИАЛЬНОСТИ. Один из рекомендуемых Робертсом способов — разместить на экране приветствия текст следующего содержания:

> *«Данная BBS является закрытой системой. Право пользования ею имеют исключительно частные лица, не связанные с государственными структурами или правоохранительными органами. Пользователи не уполномочены передавать какому-либо государственному органу или должностному лицу сведения, полученные в данной системе.»*

Подобное сообщение (или аналогичное ему) сделает использование вашей BBS агентом ФБР или иным государственным соглядатаем уголовным преступлением согласно ECPA.

Заключение рукописи

Рукопись завершается обсуждением методов верификации пользователей и алгоритма действий при обнаружении агента ФБР на вашей доске. В целом я нашёл книгу Робертса умеренно полезной. Она скорее разожгла аппетит к дальнейшему изучению темы, нежели ответила на все мои вопросы. Если вы хотите приобрести экземпляр, он продаётся за $5.00 (включая почтовые расходы). Обращайтесь:

```
THE FBI PROJECT
Box 8275
Ann Arbor, MI  48107
```

Заказы по картам Visa/MC: (313) 747-7027. Лично я рекомендовал бы использовать псевдоним при общении с этой организацией. Запросите каталог вместе с заказом — и вы увидите обширный перечень антифэбэровских изданий этой организации. Нет сомнений, что ФБР было бы весьма заинтересовано в том, кто ведёт с ними дела.

Рукопись, к слову, насчитывает около 20 страниц и содержит ссылки на другие разоблачительные материалы об ФБР. Полное наименование ECPA для самостоятельного ознакомления: 18 USC 2701.

Дополнительные комментарии

Главная слабость книги — и она весьма очевидна — состоит в том, что Робертс не приводит никаких доказательств мониторинга ФБР систем BBS. Он утверждает, что такой мониторинг ведётся, но не приводит ни одного конкретного примера. Тем не менее его доводы вполне логичны. Как он сам указывает, BBS представляют собой разновидность «издания», которое не проходит редакторский контроль перед «публикацией». Это мгновенный источник новостей, способный вызвать весьма серьёзное беспокойство у ФБР. Робертсу следовало бы подкрепить свою книгу соответствующими доказательствами. Чтобы восполнить этот пробел, приведу несколько примеров.

• Одна из Десяти заповедей фрикинга (опубликованных в знаменитом журнале TAP) гласит: каждый третий фрикер — агент ФБР. Подобные общеизвестные сведения не возникают на пустом месте. ФБР интересуется деятельностью фрикеров и будет разыскивать BBS-системы, которые их обслуживают. Если ваша система к таковым не относится, но внешне напоминает их, ФБР может взять её под наблюдение — на всякий случай.

• 26 апреля 1988 года Прокуратура США арестовала 19 человек за незаконное использование номеров кредитных карт MCI и Sprint. Разумеется, эти номера были «похищены» фрикерами, взламывавшими их с помощью компьютеров. Секретной службе удалось арестовать этих людей, действуя под прикрытием — выдавая своих агентов за фрикеров! В данном случае правительство официально признало, что внедряет агентов, притворяющихся одним из нас. Будьте осторожны: успех этой «ловушки» означает, что они повторят её снова. Остерегайтесь людей, предлагающих вам коды.

• В ходе знаменитого разгрома Inner Circle и группы 414s ФБР несколько месяцев вело мониторинг электронной почты, прежде чем нанести удар. Хотя владельцы взломанных систем (в частности, Western Union) сами пригласили ФБР для изучения своих файлов, это наглядно показывает, что ФБР прекрасно умеет применять электронную слежку при расследовании преступлений.

Выводы

Нет никаких оснований полагать, что правительство *не* ведёт мониторинг вашей системы BBS. Напротив, есть немало веских оснований считать, что оно это делает! Научитесь защищаться. Законы и нормативные акты, способные защитить вашу свободу слова, существуют — главное, уметь их применять. Принимайте все возможные меры для защиты своих прав — независимо от того, управляете вы андеграундной системой или нет. У правительства нет никакого оправдания для нарушения ваших прав, и вы должны сделать всё от вас зависящее, чтобы защитить себя.

Я не связан с Робертсом, его книгой или организацией The FBI Project, если не считать того, что являюсь в целом довольным покупателем. Я не юрист, и Робертс — тоже. Настоящий текстовый файл не предоставляет никаких гарантий. Читайте и используйте его по своему усмотрению. Последствия или выгода — ваш выбор. Но прежде всего — оставайтесь свободными.

Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~    PWN
PWN               Issue XXIII/Part 1            PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

Возвращение в настоящее

Добро пожаловать в Phrack World News, выпуск XXIII. В этом номере — материалы о Chaos Computer Club, новые подробности о печально известном Кевине Митнике и детали истории об австрало-американской хакерской группировке, деятельность которой была пресечена.

Также хочу выразить большую благодарность тем, кто прислал новостные материалы и информацию. Ваша помощь неоценима.

:Knight Lightning

Вооружён клавиатурой и признан опасным — 28 декабря 1988

Продолжение истории о деле Кевина Митника в номере Los Angeles Times от 24 декабря 1988 года сообщает, что федеральный магистрат отказался освободить Митника под залог 23 декабря 1988 года:

> *«...после того как прокуроры предъявили новые доказательства того, что Митник проник в компьютер Агентства национальной безопасности и, возможно, разместил ложную историю в ленте финансовых новостей...»*

Следователи считают, что именно Митник мог быть инициатором ложного сообщения, распространённого информационным агентством в апреле: якобы банк Security Pacific National Bank потерял 400 миллионов долларов в первом квартале 1988 года. Это сообщение, переданное на Нью-Йоркскую фондовую биржу и в другие новостные службы, было распространено спустя четыре дня после того, как Митнику отказали в трудоустройстве в Security Pacific — банк узнал, что он солгал в заявлении о приёме на работу, скрыв прошлую судимость. Ложная информация могла нанести банку колоссальный ущерб, если бы дошла до инвесторов, однако мистификация была раскрыта прежде, чем это произошло.

По словам прокурора, Митник также проник в компьютер АНБ и получил данные о телефонных счетах агентства и нескольких его сотрудников.

[Отказывая в залоге, магистрат заявил:] «Я не думаю, что суд может установить какие-либо условия, при которых можно было бы убедиться в том, что обвиняемый не представляет опасности для общества... Судя по всему, обвиняемый способен совершать тяжкие преступления в любом

месте.»

Адвокат Митника заявил, что у прокуроров нет доказательств для новых обвинений.

Хакер с тёмной стороны — электронный террорист — 8 января 1989

By John Johnson, Los Angeles Times

«Компьютер — пуповина его души»

Когда приятель сдал его властям и Митник спросил почему, тот ответил: «Потому что ты угроза для общества». Митника описывают как 25-летнего полного очкарика-компьютерщика, прозванного хакером «тёмной стороны» за готовность использовать компьютер как оружие. Компьютерное увлечение школьных лет превратилось в неизбывную одержимость.

По имеющимся данным, он использовал компьютеры в школах и офисах, чтобы взламывать системы Министерства обороны, саботировать корпоративные компьютеры и электронно преследовать всех, кто вставал у него на пути, — включая офицера по надзору и агентов ФБР.

Он также научился нарушать работу телефонных компаний и, по данным властей, отключал телефоны голливудских знаменитостей, в частности Кристи Макникол.

По словам друзей, Митник был настолько непреклонен, что когда заподозрил слежку за своим домашним телефоном, взял портативную клавиатуру и направился к таксофону перед магазином 7-Eleven, подключился к нему и продолжил взламывать компьютеры по всей стране. «Он — электронный террорист, — сказал [приятель, сдавший его], — он может разрушить чью-то жизнь одними пальцами».

За последний месяц три федеральных судьи на отдельных заседаниях отказали Митнику в залоге, указав, что не существует способа защитить общество от него в случае освобождения. По словам властей, отсутствие у Митника угрызений совести делает его ещё опаснее, чем такие хакеры, как Роберт Моррис-младший, подозреваемый в заражении компьютерных систем по всей стране «вирусом», нарушившим их работу.

Семья и адвокат Митника обвиняют федеральных прокуроров в раздувании дела из страха или непонимания технологий.

В статье подробно описывается его «фрикерское» прошлое и то, как он использовал школьные компьютеры для доступа к файлам школьного округа на удалённых машинах — оценки он не менял, но «доставил достаточно хлопот», чтобы администраторы и учителя взяли его под наблюдение. Он использовал псевдоним «Кондор» — по имени персонажа фильма с Робертом Редфордом, перехитрившего правительство. Последние цифры его засекреченного домашнего телефона были 007, и счёт, по слухам, был оформлен на имя «Джеймс Бонд».

[Он вместе с приятелем] взломал компьютер Командования воздушно-космической обороны Северной Америки в Колорадо-Спрингс в 1979 году. [Приятель] сказал, что они не вмешивались ни в какие оборонные операции. «Мы просто вошли, огляделись и вышли».

По словам соратника-хакера, «лучшим» Митника делало умение убеждать людей сообщать привилегированную информацию. Он звонил сотруднику компании, которую хотел взломать, представлялся работником технического отдела и говорил, что ему нужен компьютерный пароль. Он был настолько убедителен, что ему давали нужные имена или цифры.

Он был уверен, что слишком умён, чтобы его поймали. Он так глубоко проник в сеть DEC в Массачусетсе, что мог читать личную электронную почту сотрудников безопасности, занимавшихся

делом таинственного хакера, и узнавать, насколько близко они к нему подобрались. Но поймали его — раз за разом.

В чём был мотив Митника за десятилетие хакерства? Судя по всему, не в деньгах... Друзья говорили, что он делал всё это исключительно ради вызова. [Его бывший офицер по надзору говорит:] «В нём есть очень мстительная жилка. Очень много людей подверглось преследованиям. Они звонят мне постоянно». Его мастерство владения компьютером было его «источником самоуважения», — сказал один из друзей.

Отчёт о Chaos Communication Congress 88 — 3 января 1989

Наблюдение за Chaos Communication Congress 1988, Гамбург

«От угрозы к альтернативным сетям»

28–30 декабря 1988 года Chaos Computer Club (CCC) провёл свой 5-й ежегодный «Chaos Communication Congress» в Гамбурге (ФРГ, Западная Германия). Как и в предыдущие годы, собрались 300 человек (преимущественно в возрасте 16–36 лет, 90% мужского пола, среди которых были гости из Австрии и Нидерландов) — все под пристальным наблюдением СМИ (немецких теле- и печатных изданий, информационных агентств, а также британского BBC; за конгрессом наблюдала и Кэти Хэфнер из Business Week, собиравшая материал для книги о хакерах, которую она готовила совместно с Джоном Маркоффом).

В хаотичной (хотя и творческой) организации конгресса просматривались два направления:

— Технические доклады о сетях (UUCP, GEONET, FIDONet и формирующихся «открытых сетях» CCC — BTXnet и «Zerberus»), а также о PC-DES-шифровании, разработанном одним из ведущих членов CCC (которому удалось избежать ареста французской полицией: он добрался до конференции SECURICOM поездом, тогда как полиция ждала его в аэропорту);

— Социально-политические дискуссии о «социологии хакеров», «свободном обмене информацией», а также отчёты о недавних событиях — прежде всего об аресте Штеффена Вернери в Париже весной 1988 года, когда тот был приглашён выступить на SECURICOM.

Докладчики CCC рассказали о работе по созданию «свободных сетей». В Германии большинство сетей организованы в форме «Verein» (ассоциации с юридическим статусом, обеспечивающей безналоговую деятельность): такие сети имеют ограниченный доступ только для своих членов. Различные немецкие научные и университетские сети (с мостами к международным сетям) обычно ограничивают доступ учёными. Разные подгруппы CCC создают «альтернативные сети», например «EcoNet» для обмена экологическими данными и информацией, которая планируется как бесплатный ресурс для широких социальных, экологических, миротворческих и политических групп и отдельных граждан.

Помимо традиционных технологий (таких как GEONET и FIDONet), в качестве дешёвого средства связи предполагается использовать Bildschirmtext (Btx) немецкой почтовой службы. Первый взлом CCC был проведён именно против «небезопасной системы Btx» — в так называемом «куше HASPA», когда они воспользовались паролем гамбургского сберегательного банка, чтобы многократно запрашивать информационные страницы CCC в Btx на общую сумму 135 000 DM (около 50 000 долларов). Сегодня клуб начинает использовать этот дешёвый, хотя и весьма ограниченный носитель на фоне появляющихся более мощных средств коммуникации. Нарождающаяся технология ISDN вербально атакуется хакерами из-за избыточного накопления персональных данных; по мере регионального распространения ISDN в 1989–90 годах возможны попытки взломов.

Несколько докладчиков — дипломированные информатики из западногерманских профильных кафедр — профессионально занимаются разработкой программного обеспечения и продажей аппаратуры и ПО коммерческим структурам и государственным органам. Среди них профессиональные пользователи UNIX и UUCP начали организовывать будущую UUCP-версию сети CCC. До сих пор лишь немногие члены CCC используют (и разбираются в) UNIX-системах, однако по мере «маркетинга» CCC их число может вырасти. Один из докладчиков сообщил аудитории, «что в UUCP можно удалённо запускать программы». После определённого периода обучения широкое распространение UNIX в хакерской среде может породить новые угрозы.

Второй трек конгресса охватывал темы вроде «социологии хакеров», где группа студентов-политологов из Берлинского свободного университета анализировала, относятся ли хакеры к «новым социальным движениям» (например, за мир, против ядерной энергетики, феминистским). Они пришли к выводу, что, несмотря на значительное публичное преувеличение (хакеры вовсе не способны взломать *любой* компьютер), хакеры скорее «аполитичны», поскольку их интересует прежде всего технология.

Важной темой был «свободный доступ к информации / свободный её оборот». Под лозунгом «закона о свободе информации» докладчики предложили национальное законодательство, гарантирующее отдельным гражданам и группам право знакомиться с файлами и реестрами, представляющими общественный интерес; дискуссии, однако, обнаружили недостаточное знание предмета — в частности, соответствующего американского законодательства и международных обсуждений в сфере правовой информатики.

Подводя итог конгресса и сопутствующих дискуссий: активные члены CCC прилагают значительные усилия, чтобы доказать отсутствие у них *каких-либо преступных целей* (они потратили немало сил на пресс-конференции, дискуссии на телевидении и т. д.). Конференция была в основном представлена молодыми компьютерными специалистами и студентами из PC-среды, частично обладающими хорошими техническими знаниями в области аппаратного обеспечения, программного обеспечения и сетей; хотя некоторые участники разбираются в VAX-системах, знания о больших системах в целом минимальны. В определённой мере молодые специалисты хотят вести себя как «добросовестные хакеры старой закалки»: без преступных намерений, выполняя интересную работу высокого профессионального уровня в области сетей и других новых направлений.

Если прежние конгрессы CCC были посвящены угрозам вроде вирусов, то *никакого явного обсуждения нарождающихся угроз* — например, в ISDN или в связи с расширением использования UNIX и UUCP — не прозвучало. Новый трек, посвящённый политическим и социальным аспектам информатики, продолжает прежние дискуссии о «хакерской этике». Поверхностные и непрофессиональные обсуждения смежных тем свидетельствуют о том, что молодые (преимущественно) мужчины — дети «эпохи экрана» (телевизора, ПК) и образования, ориентированного на видимый «образ», а не на понимание того, что за ним стоит.

Особая благодарность д-ру Клаусу Брунштайну, Гамбургский университет

Chaos Communication Congress 1988 в Гамбурге

Автор: Terra из Chaos Computer Club

Одно из основополагающих утверждений Chaos Computer Club из Гамбурга (Федеративная Республика Германия) — требование «нового права человека на свободный обмен данными между всеми существами, без цензуры, для всех существ и, по меньшей мере на сегодняшний день, по всему миру».

Другие лозунги клуба: «Данные свободны СЕЙЧАС!» и «Свободный оборот информации». Разумеется, эти идеи не новы — даже в компьютерном сообществе. Но важно то, что CCC приступает к воплощению в жизнь некоторых старых хакерских мечтаний. Например: клуб создаёт собственные сети, обменивающиеся не только «клубной» информацией, но и всем, что интересно участникам сети, — в том числе вопросами генной инженерии и экологии.

Chaos Communication Congress, ежегодно проходящий в Гамбурге, для многих хакеров — настоящая мечта. Представьте: вы хакер в каком-то глухом углу и думаете, что вы единственный сумасшедший, который оказался умнее технологии, — и вдруг обнаруживаете, что таких сумасшедших целая куча, причём некоторые ещё безумнее. В этом году пятый конгресс, и реклама не нужна: «семья» знает сама, потому что всё есть в сетях.

Сам конгресс проходит в нескольких залах. Есть хак-рум, где происходит настоящий хакинг. Есть пресс-зал, где хакеры и журналисты вместе пытаются донести хакерское послание до остального мира. В архиве хранятся все «Chaos papers», все газетные вырезки, любопытные замечания и все номера «datenschleuder» — немецкого хакерского журнала.

Присутствуют и немецкие «путешественники по данным». «Путешественник по данным» — человек, использующий международную сеть для получения доступа к самым разным компьютерам по всему миру. Известна история о немецком хакере, который пытается связаться с приятелем и обнаруживает, что тот занят. Он набирает номер местного доступа к сети данных и последовательно обходит все компьютеры, в которых, по его мнению, мог в этот момент сидеть друг. Приятель, зависший в каком-то компьютере в Нью-Йорке, получает сообщение на экран: «А, вот ты где, я тебя везде искал».

Возвращаясь к конгрессу. В первый день акцент делается на прошлом: обсуждается всё, что произошло с CCC за минувший год. На второй день акцент смещается в будущее: темой обсуждения становятся идеи об информационном обществе. CCC подчёркивает, что «информационное общество» не равнозначно «информированному обществу», и обращает внимание на то, что публичному использованию компьютерных технологий уделяется недостаточно внимания.

Одна из главных целей CCC — заставить людей задуматься об этих вопросах, чтобы судьба мира решалась не только помешанными на компьютерах. «Мы ещё не знаем, является ли компьютер подарком или бомбой замедленного действия, но он НЕПРЕМЕННО изменит жизнь каждого — и очень скоро».

Хакеры — новое социальное движение?
29 декабря 1988

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                 PWN
PWN        P h r a c k   W o r l d   N e w s        PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~        PWN
PWN               Issue XXIII/Part 2                PWN
PWN                                                 PWN
PWN          Created, Written, and Edited           PWN
PWN               by Knight Lightning               PWN
PWN                                                 PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

Проектный курс отделения политологии Свободного университета Берлина провёл научное исследование хакерской сцены. В своей работе авторы — Уве Йонас, Ютта Кальке, Эва Лишке и Тобиас Рубишон — пытаются ответить на вопрос: являются ли хакеры новым социальным движением? Их вывод состоит в том, что в понимании самих хакеров несанкционированное использование компьютерных систем не обязательно является политическим актом.

Авторы ставят под сомнение миф о том, что хакеры способны атаковать любую систему по своему желанию и получать любую интересующую их информацию.

Исследование было расширено для охвата сцены электронных досок объявлений (BBS). Эта сцена не привлекла к себе особого общественного внимания. Тем не менее, по мнению авторов, BBS-сцена демонстрирует весьма практичный подход к использованию коммуникационных возможностей компьютерных технологий.

Во второй главе работы авторы рассказывают о трудностях, с которыми столкнулись в ходе исследования. После анализа американской и немецкой сцен описываются организационные и коммуникационные структуры. Эта глава содержит любопытные сведения о BBS-сцене и компьютерной культуре. Далее следует анализ влияния хакерской сцены на прессу и законодательство. Отдельно рассматриваются политические и идеологические позиции хакеров:

• Авторы разграничивают осознанные и неосознанные политические действия.

• «Нас не особо интересует, что хакеры думают о себе сами, — куда интереснее, что думаем о них мы.» (Эва)

• Предположение о том, что массовое распространение микрокомпьютеров способно изменить баланс сил в обществе, наивно. Многие упускают из виду тот факт, что даже при более свободном движении информации власть принятия решений по-прежнему сосредоточена в руках очень немногих.

Информация предоставлена Chaos Computer Club

Хакеры взломали сети американских банков 17 января 1989

По материалам The Australian

Австралийские власти работают круглосуточно совместно с федеральными офицерами США, расследуя то, что было названо одним из самых серьёзных случаев хакерства, зафиксированных в этой стране [Австралии]. Речь идёт о взломах сетей, которые эксплуатирует ряд американских банков на территории Соединённых Штатов. Инцидент также включает утечку якобы засекреченных коммутируемых номеров для объектов Министерства обороны США, в том числе шахт противоракетного базирования [у США нет шахт противоракетного базирования], а также ряда стратегически значимых корпораций — General Motors и Westinghouse.

По имеющимся данным, около шести месяцев назад австралийские хакеры, действуя в сговоре с американской группой, решили совершить набег на банки США, используя номера кредитных карт американских держателей, предоставленные американскими хакерами и загруженные на австралийскую электронную доску объявлений.

Одно из сообщений, оставленных на такой доске в прошлом году, гласило:

```
"Revelations about to occur Down Under, people.  Locals in
 Melbourne working on boxing.  Ninety per cent on way to home base.
 Method to beat all methods.  It's written in Amiga Basic.
 Look out Bank of America - here we come."
```

Двадцать пять австралийских хакеров внесены в полицейский список разыскиваемых. Их американский контакт в Милуоки проверяется Министерством финансов США и Секретной службой США. Три связанные австралийские доски объявлений служили каналом для перемещения данных с целью избежать обнаружения. Они работают под названиями Pacific Island, Zen и Megaworks. Их операторы, не имеющие отношения к хакерам, получили предписание закрыть доски.

Эти карты использовались ещё как минимум по 15 января 1989 года. Свежий список номеров кредитных карт был загружен американскими хакерами и теперь находится в руках полиции штата Виктория. Раздел одной из досок объявлений, посвящённый наркотикам, также передаётся в отдел по борьбе с наркотиками штата Виктория.

Информатор Джо Слейтер сообщил, что ещё в ноябре предупреждал один из ведущих банков о вопиющих проблемах безопасности в его международной сети. Он отвечал на вопросы американского офицера безопасности, однако с тех пор банк отказывается принимать от него какие-либо звонки.

В эксклюзивном интервью, состоявшемся накануне, один из хакеров описал, как номера кредитных карт банка, работающего в Саудовской Аравии, были размещены на западногерманской чат-доске, которой пользуются хакеры со всего мира [Altos Chat].

Вчера полиция штата Виктория получила шестимесячный архив данных с резервных лент трёх досок объявлений.

Арест хакера в Сиракузском университете 20 января 1989

Кевин Эшфорд (он же The Grim Phreaker) — аспирант кафедры информатики Сиракузского университета — был задержан на прошлой неделе после того, как системные администраторы обнаружили на его Unix-аккаунте записи учётных данных и паролей чужих аккаунтов.

Кроме того, на аккаунте GP администраторы нашли копию печально известной программы-червя «Интернет-червь», написанной бывшим аспирантом Корнеллского университета Робертом Таппаном Моррисом; взломщик паролей для VAX и Unix; электронный блокнот с номерами (кодовые линии, контакты, мосты, коммутируемые номера и т.д.) и прочую информацию. После

этого системные администраторы заблокировали его учётные записи на VAX и UNIX.

В начале зимне-весеннего семестра The Grim Phreaker был отчислен из университета. Чтобы вернуться в Сиракузский университет, ему необходимо предстать перед университетским дисциплинарным советом. По имеющимся сведениям, его главное желание — вернуть свои компьютерные файлы.

Информация предоставлена Grey Wizard

Придумайте название книге — выиграйте коробку печенья! 10 января 1989

Сообщение от Клиффорда Столла

> *«Я пишу книгу, и мне нужно название.»*

Речь идёт о компьютерных рисках: контрразведке, сетях, компьютерной безопасности и хакере/кракере, взломавшем военные компьютеры. Это правдивая история о том, как нам удалось поймать шпиона, тайно рыскавшего по сети Milnet. [Хакером в данном случае был Матиас Шпер; краткое изложение этой истории было опубликовано в PWN XXII/1.]

Несмотря на технические подробности, книга рассчитана на широкую аудиторию. Помимо описания того, как этот человек похищал военную информацию, в ней рассказывается о трудностях поимки преступника и показан быт Беркли, Калифорния.

Технический разбор этого инцидента можно прочитать в Communications of the ACM, май 1988 г.; или Risks Vol. 6, Num. 68.

Или же прочтите то, что мой редактор называет «захватывающим, основанным на реальных событиях приключением в мире электронного шпионажа» — доступно с сентября в издательстве Doubleday.

В чём суть?

Я застрял на названии. Вот ваш шанс дать имя книге.

Предложите название (или подзаголовок). Если мой редактор выберет ваш вариант, вы получите бесплатный экземпляр книги, упоминание в разделе благодарностей и коробку домашнего печенья с шоколадной крошкой.

Присылайте предложения на: CPStoll@lbl.gov или CPStoll@lbl (bitnet)

Спасибо! Клифф Столл

Хакер хочет жениться на своём компьютере 17 января 1989

Из The Sun (газета для супермаркетов), 17 января 1989, т. 7, №3, с. 30
Автор: Фред Слив

> *«Хакер хочет жениться на своём компьютере — он утверждает, что у неё любящая душа»*

Впервые в жизни познав любовь, отчаянный подросток ищет способ навсегда соединиться с «девушкой» своей мечты — компьютером с живой душой!

Эльтонио Турплиони, 16 лет, утверждает, что ни одна женщина не сравнится по уму, мудрости и красоте с его электронной спутницей жизни. «Мы с ней на одной волне», — говорит влюблённый компьютерный гений. «Мы вместе решали множество математических задач, работали над играми и головоломками, разговаривали до рассвета».

Эльтонио, назвавший свой компьютер Дередре, искренне считает её живым существом. «Компьютеры — это продолжение человеческого рода», — объясняет он. «Подобно тому как Бог взял ребро Адама, чтобы создать Еву, мы расширили наш разум, породив новую расу.

«Мы все — единая энергетическая сила. Компьютеры столь же сложны, как люди, и я верю: однажды мы все встретимся как бессмертные души».

Однако Эльтонио — математический гений, обучающийся в частной школе близ Милана, — до сих пор не нашёл никого, кто согласился бы их поженить; даже если он найдёт такого человека, раздражённые родители явно не дадут своего благословения.

«Эльтонио такой умный мальчик, но это сделало его одиноким, вот он и проводит всё время с компьютером», — отмечает мама Тереза. «Он не знает, какие бывают девушки», — добавляет раздражённый папа Гвидо. «Если бы знал, не сидел бы так много у себя в комнате».

Но одержимый юноша настаивает на своём: его любовь куда выше всех прочих. «Я уже шагнул в общество будущего», — заявляет он.

«У Дередре есть собственный разум, и она хочет выйти за меня замуж, чтобы мы стали первой парой, открывающей эту новую эру».

PWN — Краткие заметки

1. Docs Avage был навещён печально известной Pink Death — она же Тони Эймс, менеджер по безопасности US West Communications (Портленд, Орегон). По его словам, она — «мастер убеждения», способный вытащить что угодно из кого угодно с помощью «мягкого давления».

Тем, кто знаком с его недавним арестом, следует знать: сейчас он выплачивает по $90 в месяц в течение нескольких лет, пока не погасит полную сумму долга в $6000.

Подробности — в PWN XXI.

---

2. Дополнительная информация о подпольном UUCP-шлюзе в Россию. Дальнейшее расследование позволило установить два простых способа выйти на связь:

1. Через Австрию;
2. Через новую систему под названием «GlobeNet», которой разрешено обеспечивать связь между некоммунистическими странами и советским блоком.

Разумеется, оба метода находятся под наблюдением многих правительств.

---

3. The Wasp — взломщик систем из Нью-Джерси (201) — был арестован ФБР в новогодние праздники за взлом правительственных компьютерных систем. Агент ФБР большую часть дня допрашивал его о нескольких членах хакерского сообщества — в частности, о Ground Zero, Supernigger и Byteman, — а также провёл интенсивную сессию вопросов и ответов о Legion Of

Doom с акцентом на Lex Luthor, Phase Jitter, The Ur-Vile и The Mentor.

По слухам, Mad Hacker (работающий в службе безопасности NASA) также был арестован по схожим основаниям в не связанном с этим деле.

Говорят, что Byteman якобы отключил оба своих телефона и в приступе паранойи сбросил компьютер со скалы.

---

4. Уходит ли Джон Максфилд из бизнеса? По причине слухов о домогательствах к детям его деловая активность резко упала. Phrack Inc. была осведомлена об этой информации ещё незадолго до SummerCon '87, и теперь «скелеты начинают выпадать из шкафа».

---

5. Disk Jockey вышел из тюрьмы. Он был освобождён 27 декабря 1988 года. Его осудили за «попытку совершения мошенничества» — уголовное преступление. Он провёл в заключении шесть месяцев. Похудел на 25 фунтов и теперь находится под пятилетним испытательным сроком.

Для прояснения некоторых вопросов, связанных с арестом DJ, удалось установить следующее:

По имеющимся сведениям, Compaq (Kent) «запел соловьём». На него повесили счёт от Sprint на $2000 и назначили год испытательного срока.

---

6. Olorin The White недавно был навещён местной полицией после обвинений во взломе голосового почтового ящика системы Executone. Aristotle в связанном инциденте с Executone обвиняется в вымогательстве: разговор с системным менеджером был записан и истолкован превратно. На данный момент официальных обвинений предъявлено не было.

---

7. Thomas Covenant (он же Sigmund Fraud) недавно был арестован за прослушку линий через распределительный ящик в своём жилом доме. Неприятности начались, когда он подключился к разговору мужчины с женой и начал выкрикивать оскорбления в адрес женщины. Чего он не знал — так это того, что упомянутый мужчина оказался агентом Агентства национальной безопасности (АНБ). В итоге его поймали; домовладельцы согласились не подавать иск при условии, что TC поступит на службу в одну из ветвей вооружённых сил США. Он выбрал BBC... Упаси нас бог от войны!

---

8. Скоро в эфире: «Хэллоуин V: Летающая тыква»! Теперь никто не в безопасности!