Phrack RU issue 016

Русская версия Phrack, выпуск 016. Полный текст статей с кодом и таблицами.

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

Материалы выпуска: Вступление к Phrack #16; Информация Bellcore; Руководство хакера по PRIMOS; Взлом глобальной телекоммуникационной сети; Законы, регулирующие мошенничество с кредитными картами; Прослушивание телефонных линий; Чтение отчётов Trans-Union: урок по терминологии; Phrack World News, часть 1; История о федералах на XXXXXXX BBS; Побег BBS Безумного Телефонщика в дружественную иностранную державу; Shadow Hawk снова арестован; Phrack World News, часть 5.

Больше крутых материалов в моём телеграм канале @grogrigs

Вступление к Phrack #16

Автор: Elric of Imrryr

Приветствуем вас в Phrack #16. Мы немного задержались, но зато номер вышел объёмнее, чем когда-либо. Думаем, этот выпуск окажется для вас очень интересным. Наслаждайтесь и получайте удовольствие.

Elric of Imrryr — редактор

Содержание номера

Phrack World News

Приём материалов

Статьи для публикации в Phrack принимаются на следующих BBS:

* — на этих системах вы получите ответ быстрее всего.

Информация Bellcore

Автор: The Mad Phone-man

Итак, вы вскрыли большую телефонную коробку на стене и смотрите на кучу бирок с цифрами и буквами. Где линия модема? Где линия 1-800 WATS? Где сигнальная линия? У Bell существует специальный набор кодов, позволяющий определить, что именно перед вами. Это те же коды, которые монтажник получает в центре коммутации, чтобы настроить линию, проверить её и убедиться, что она соответствует заказу клиента. Ниже приведены некоторые выдержки из справочника Bellcore.

Для начала рассмотрим гипотетический номер линии, с которым я знаком:

```
64FDDV 123456
```

Формат серийного номера

```
-----------------------------------------------------------------
     Префикс +  код услуги + модификатор + серийный номер +
разряды:  1,2        3,4          5,6        7,8,9,10,11,12     продолжение
-------------------------------------------------------------------------

     Суффикс +  номер цепи, присвоенный АТС +   сегмент
разряды: 13,14,15           16,17,18,19          20,21,22
-------------------------------------------------------------------------
```

Самое важное — 3-й и 6-й разряды.

Коды услуг — внутризоновые и межзоновые блоки 1–26

```
AA — Аналоговая абонентская линия пакетной передачи
AB — Транк пакетной коммутации
AD — Оператор (attendant)
AF — Коммерческое аудио, постоянный режим
AI — Автоматическое определение исходящего набора
AL — Альтернативные услуги
AM — Пакет, линия внесетевого доступа
AN — Служба объявлений
AO — Международное/заморское аудио (постоянный режим)
AP — Коммерческое аудио (неполный режим)
AT — Международное/заморское аудио (неполный режим)
AU — Autoscript
BA — Защитная сигнализация (CD)
BL — Звонок и световая сигнализация
BS — Управление сиреной
CA — SSN-доступ
CB — OCC-аудиоканалы
CC — OCC-цифровой канал средней скорости
CE — SSN-абонентская линия
CF — OCC-специальный канал
CG — OCC-телеграфный канал
CH — OCC-цифровой канал высокой скорости
CI — Транк идентификатора концентратора
CJ — OCC-управляющий канал
CK — OCC-заморский соединительный канал широкополосный
CL — Линия АТС Centrex
CM — OCC-видеоканал
CN — SSN-сетевой транк
CO — OCC-заморский соединительный канал
```

CP — Сигнальное звено идентификатора концентратора
CR — OCC-резервный канал
CS — Канальная служба
CT — SSN-связной транк
CV — OCC-канал телефонного качества
CW — OCC-канал по проводной паре
CZ — OCC-канал доступа
DA — Цифровая передача данных, внесетевое удлинение
DB — HSSDS, абонентская линия 1,5 Мбит/с
DF — HSSDS, узел-узел 1,5 Мбит/с
DG — HSSDS, узел-земная станция 1,5 Мбит/с
DH — Цифровая служба
DI — Прямой входящий набор
DJ — Цифровой транк
DK — Канал передачи данных
DL — Линия диктофона
DO — Прямой исходящий набор
DP — Цифровые данные — 2,4 кбит/с
DQ — Цифровые данные — 4,8 кбит/с
DR — Цифровые данные — 9,6 кбит/с
DW — Цифровые данные — 56 кбит/с
DY — Цифровая служба (менее 1 Мбит/с)
EA — Коммутируемый доступ
EB — Транк оконечной АТС ENFIA II
EC — Транзитный транк ENFIA II
EE — Комбинированный доступ
EF — Канал входа — телефонного качества
EG — Телеграф тип 2
EL — Линия экстренной связи
EM — Транк центра экстренной связи
EN — Канал доступа к коммутационной сети АТС
EP — Канал входа — программного качества
EQ — Только оборудование (назначение только сети)
ES — Служба удлинения — телефонного качества
ET — Канал входа — телеграфного качества
EU — Служба удлинения — телеграфного качества
EV — Улучшенный транк экстренной связи
EW — Внесетевой эквивалент услуг MTS/WATS
FD — Выделенная линия — данные
FG — Спектр группа-супергруппа
FR — Диспетчерская связь пожарной службы
FT — Транк иностороннего обмена
FW — Широкополосный канал
FV — Канал телефонного качества
FX — Иностоящий обмен
HP — Не-DDS цифровые данные 2,4 кбит/с
HQ — Не-DDS цифровые данные 4,8 кбит/с
HR — Не-DDS цифровые данные 9,6 кбит/с
HW — Не-DDS цифровые данные 56 кбит/с
IT — Межтранзитный связной транк
LA — Локальный канал передачи данных
LL — Терминальная линия дальней связи
LS — Местная служба
LT — Терминальный транк дальней связи
MA — Транк доступа к сотовой сети, двусторонний
MT — Музыка по проводам
NA — Звено CSACC (EPSCS)
NC — Звено CNCC (EPSCS)
ND — Сетевая линия данных
OI — Абонентская линия внешней внутренней связи
ON — Внесетевая линия доступа
OP — Внешнее удлинение
OS — Абонентская линия внешней АТС
PA — Защитная сигнализация (АС)
PC — Коммутируемая цифровая линия доступа
PG — Пейджинг
PL — Выделенная линия — голос
PM — Защитный мониторинг
PR — Защитная релейная связь — телефонного качества
PS — Резервный канал, смонтированный MSC
PV — Защитная релейная связь — телеграфного качества

PW — Защитная релейная связь — сигнального качества
PX — Абонентская линия АТС
PZ — Цепь, смонтированная MSC
QU — Асинхронная линия пакетного доступа
QS — Синхронная линия пакетного доступа
RA — Удалённый оператор
RT — Радиоканал наземной линии
SA — Спутниковый транк
SG — Сигнал управления/дистанционного измерения — сигнального качества
SL — Секретарская линия
SM — Выборка
SN — Оконечное устройство специального доступа
SQ — Только оборудование — абонентское
SS — Dataphone select-a-station
TA — Транзитный связной транк
TC — Управление/дистанционное измерение — телеграфного качества
TF — Телефото/факс
TK — Местный транк АТС
TL — Нетранзитный связной транк
TR — Транк пульта оператора или автоматического распределителя вызовов (ACD)
TT — Канал телетайпа
TU — Линия пульта оператора или ACD
TX — Выделенный канал
VF — Коммерческое телевидение (полный режим)
VH — Коммерческое телевидение (неполный режим)
VM — Управление/дистанционное измерение — голосового качества
VO — Международное заморское телевидение
VR — Некоммерческое телевидение (7003, 7004)
WC — Специальный транк 800-й поверхностный
WD — Специальный транк WATS (исходящий)
WI — Транк 800-й поверхностный
WO — Линия WATS (исходящая)
WS — Транк WATS (исходящий)
WX — Линия службы 800
WY — Транк WATS (двусторонний)
WZ — Линия WATS (двусторонняя)
ZA — Сигнальные цепи
ZC — Цепи вызова и переговоров
ZE — Цепи аварийного коммутирования
ZF — Цепи заказов, каналы
ZM — Цепи измерения и регистрации
ZP — Испытательная цепь, центр обслуживания объектов связи
ZQ — Цепи контроля качества и управления
ZS — Цепи коммутации, управления и передачи
ZT — Испытательные цепи центральной АТС
ZV — Цепи заказов, обслуживание

Коды услуг для доступа в зоне LATA

HC — Высокая ёмкость 1,544 Мбит/с
HD — Высокая ёмкость 3,152 Мбит/с
HE — Высокая ёмкость 6,312 Мбит/с
HF — Высокая ёмкость 6,312
HG — Высокая ёмкость 274,176 Мбит/с
HS — Высокая ёмкость субскоростная
LB — Голос — некоммутируемая линия
LC — Голос — коммутируемая линия
LD — Голос — коммутируемый транк
LE — Голос и тон — радиоканал наземной линии
LF — Данные низкоскоростные
LG — Базовые данные
LH — Голос и данные — транк доступа к сети PSN
LJ — Голос и данные — доступ SSN
LK — Голос и данные — межмашинный транк SSN
LN — Удлинение данных, канал данных телефонного качества
LP — Телефото/факс
LQ — Голосовой канал, индивидуальный
LR — Защитная релейная связь — голосового качества

```
LZ — Выделенный канал
MQ — Металлический, индивидуальный
NQ — Телеграфный, индивидуальный
NT — Защитная сигнализация — металлическая
NU — Защитная сигнализация
NV — Защитная релейная связь/телеграфного качества
NW — Канал телеграфного качества — 75 бод
NY — Канал телеграфного качества — 150 бод
PE — Программное аудио, 200–3500 Гц
PF — Программное аудио, 100–5000 Гц
PJ — Программное аудио, 50–8000 Гц
PK — Программное аудио, 50–15000 Гц
PQ — Программный канал, индивидуальный
SB — Коммутируемый доступ — стандартный
SD — Коммутируемый доступ — улучшенный
SE — Специальный доступ WATS — стандартный
SF — Специальный доступ WATS — улучшенный
SJ — Ограниченная коммутируемая линия доступа
TQ — Телевизионный канал, индивидуальный
TV — Телеканал односторонний, аудио 15 кГц
TW — Телеканал односторонний, аудио 5 кГц
WB — Широкополосный цифровой, 19,2 кбит/с
WE — Широкополосный цифровой, 50 кбит/с
WF — Широкополосный цифровой, 230,4 кбит/с
WH — Широкополосный цифровой, 56 кбит/с
WJ — Широкополосный аналоговый, 60–108 кГц
WL — Широкополосный аналоговый, 312–552 кГц
WN — Широкополосный аналоговый, 10 Гц–20 кГц
WP — Широкополосный аналоговый, 29–44 кГц
WR — Широкополосный аналоговый, 564–3064 кГц
XA — Выделенный цифровой, 2,4 кбит/с
XB — Выделенный цифровой, 4,8 кбит/с
XG — Выделенный цифровой, 9,6 кбит/с
XH — Выделенный цифровой, 56 кбит/с
```

Модификатор: позиция 5

Последние два важных разряда — 5-й и 6-й — расшифровываются следующим образом.

ВНУТРИШТАТНЫЙ	МЕЖШТАТНЫЙ	
A	B	Альтернативные данные и не-данные
C		Услуга под управлением клиента
D	E	Данные
N	L	Операция без данных
P		Предлагается только по внутренней тарифной сетке RPL
S	T	Одновременные данные и не-данные
F		Доля оператора межстанционной связи менее 50%
	G	Доля межштатного оператора более 50%

Модификатор: позиция 6

```
============================================================
```

Позиция 6 — модификаторный символ

ТИП УСЛУГИ		Внутризоновая LATA
ВСЕ КРОМЕ ПРАВИТ. США		ПРАВИТЕЛЬСТВО США
T	M	Цепь: клиент BOC — клиент BOC, все средства предоставлены TELCO
C	P	Цепь: BOC/BOC, часть средств или оборудования предоставлена TELCO
A	J	Цепь: BOC/BOC, всё электрически подключённое оборудование клиентское
L	F	Цепь заканчивается на объекте клиента оператора межстанционной связи
Z		Официальная корпоративная служба
		Межзоновая (Interlata)
S	S	Цепь заканчивается в точке подключения (POT) оператора межстанционной связи
V	V	Цепь заканчивается на интерфейсе оператора радиосвязи (RCC)
Z		Официальная корпоративная служба
		Коридорная
Y	X	Коридорная цепь
		Международная
K	H	Цепь имеет минимум два окончания в разных странах
		Оператор межстанционной связи
Y	X	Транспортная цепь между терминалами оператора межстанционной связи

Таким образом, `64FDDV` — это выделенная линия данных, оканчивающаяся у оператора радиосвязи (RCC). Аналогичным образом можно расшифровать любой другой номер.

Надеюсь, эта информация принесёт вам столько же пользы, сколько мне доставило её нахождение.

-=- The Mad Phone-man =-

Руководство хакера по PRIMOS

Автор: Cosmos Kid

```
  ========================================
  ====    Cosmos Kid Presents...      ====
  ====   A Hacker's Guide To:  PRIMOS   ====
  ====             Part I              ====
  ====    (c) 1987 by Cosmos Kid     ====
  ========================================
```

Примечание автора

Этот файл — первый из двух, посвящённых системе PRIMOS и принципам её работы. Второй файл вскоре поступит в оборот, так что непременно найдите его на каком-нибудь хорошем BBS.

Предисловие

Этот файл написан таким образом, чтобы быть полезным как новичкам, так и опытным пользователям PRIMOS, хотя в первую очередь он рассчитан именно на начинающих. Вопреки расхожему мнению, PRIMOS может оказаться весьма мощной системой, если пользоваться ею правильно. В этом файле я изложил ряд самых базовых команд и их применение, а также некоторые команды, уже не такие простые.

Вход в систему PRIMOS

Систему PRIMOS проще всего узнать по её нестандартным приглашениям командной строки: `OK,` и `ER!`. Однако сразу после подключения вы их не увидите. Сначала система должна представиться, например:

```
Primenet V2.3
-or-
Primecom Network
```

После этого система ожидает от вас ввода — предпочтительно команды `LOGIN`. Затем система попросит вас ввести идентификатор пользователя и пароль в целях безопасности. Процесс входа в PRIMOS выглядит следующим образом:

```
CONNECT
Primenet V 2.3   (система)
LOGIN<CR>        (вы)
User id?         (система)
AA1234           (вы)
Password?        (система)
KILLME           (вы)
OK,              (система)
```

Перед приглашением `OK,` система выведет своё приветственное сообщение. Обратите внимание: если после подключения вы не введёте `LOGIN`, большинство других команд будут проигнорированы, а система ответит:

```
Please Login
ER!
```

Выход из системы PRIMOS

Если PRIMOS вам наскучит, в любой момент можно ввести `LOGOFF`, чтобы покинуть систему. На некоторых системах реализована функция тайм-аута: если вы не вводите ничего в течение заданного промежутка времени, система автоматически выйдет из вашей учётной записи, сообщив что-нибудь вроде:

```
Maximum Inactive Time Limit Exceeded
```

Системные приглашения

Как уже говорилось, в PRIMOS используются приглашения `ER!` и `OK,`. Приглашение `OK,` означает, что последняя команда выполнена успешно и система ожидает следующей. Приглашение `ER!` означает, что при вводе последней команды допущена ошибка; как правило, ему предшествует сообщение об ошибке.

Специальные символы

Некоторые терминалы поддерживают встроенные специальные функции:

CONTROL-H — удаляет последний введённый символ.

Прочие специальные символы

RETURN — клавиша ввода сигнализирует PRIMOS о том, что вы закончили набирать команду и готовы к её обработке.

BREAK / CONTROL-P — останавливает всё, что в данный момент обрабатывается в памяти, и возвращает управление PRIMOS вам. Чтобы перезапустить процесс, введите:

```
START
```

(можно сократить до `S`).

CONTROL-S — приостанавливает прокрутку вывода на терминале для просмотра.

CONTROL-Q — возобновляет прокрутку вывода на терминале.

ТОЧКА С ЗАПЯТОЙ `;` — логический символ конца строки. Точка с запятой позволяет вводить несколько команд в одной строке.

Получение справки

Получить информацию о доступных командах PRIMOS в интерактивном режиме можно с помощью команды `HELP`. Система справки работает по ключевым словам: вся информация хранится под ключевыми словами, отражающими содержимое справочных файлов. Это схоже с VAX. Ввод одной лишь команды `HELP` открывает подсистему справки и выводит информационную страницу. На следующей странице будет представлен список тем и их ключевых слов, включая такие темы, как PRIME, RAP, MAIL и DOC. Введя ключевое слово MAIL, вы получите сведения о почтовой подсистеме, доступной пользователям. Введите `PRIME`, чтобы получить информацию обо всех командах PRIMOS, или, например, `COPY` — чтобы узнать об этой конкретной теме.

Имя файла или поддиректории может содержать до 32 символов. Имя файла может включать любые из перечисленных ниже символов, при единственном ограничении: первый символ имени не может быть цифрой. Обратите внимание: пробелы НИГДЕ не допускаются:

```
A-Z .....буквы алфавита
0-9 .....цифры
&   .....амперсанд
#   .....решётка
$   .....знак доллара
-   .....дефис/минус
*   .....звёздочка
.   .....точка
/   .....косая черта
```

Соглашения об именовании

Ограничений на имена файлов совсем немного. Тем не менее следует учитывать, что многие компиляторы и команды на PRIME будут делать определённые допущения, если вы придерживаетесь установленных правил. Суффиксы имён файлов помогают идентифицировать их содержимое применительно к языку, на котором написан исходный код. Например, если вы написали программу на PL/1 и назвали файл с исходным кодом `PROG1.PL1`, компоновщик SEG возьмёт бинарный файл, подключит все указанные вами бинарные библиотеки и создаст файл `PROG1.SEG`, содержащий бинарный код, необходимый для выполнения программы. Некоторые распространённые суффиксы имён файлов: F77, PAS, COBOL, PL1G, BASIC, FTN, CC, SPIT (файлы с исходным кодом). Все они обозначают отдельные языки программирования и относятся к более продвинутому программированию на PRIMOS (например, FTN = Fortran).

```
BIN  — бинарный код, созданный компилятором
LIST — листинг программы, созданный компилятором
SEG  — скомпонованный бинарный код, созданный SEG
```

Некоторые файлы, не использующие стандартные суффиксы, вместо этого применяют префиксы для обозначения содержимого. Распространённые префиксы:

```
B  — бинарный код, созданный компилятором
L  — листинг исходной программы
C  — командные файлы
$  — временные рабочие файлы (например, T$0000)
#  — файлы SEG
```

PRIMOS располагает рядом команд для управления файлами и доступа к их содержимому. Эти команды позволяют просматривать содержимое файлов и директорий, а также копировать, добавлять, удалять, редактировать и распечатывать файлы. Заглавные буквы в описании каждой команды соответствуют допустимому сокращению. Список аргументов должен быть заключён в круглые скобки.

`Close arg` — закрывает файл, указанный в `arg`. `Arg` может быть списком номеров файловых модулей PRIMOS или словом `ALL`, которое закрывает все открытые файлы и модули.

`LIMITS` — выводит информацию об учётной записи: данные о выделенных и использованных ресурсах, о том, кто предоставил доступ, и срок действия.

`Edit Access` — редактирует права доступа к указанным директориям и файлам.

`CName arg1 arg2` — изменяет имя `arg1` на `arg2`. Аргументами могут быть файлы или директории.

`LD` — команда просмотра директории (List Directory) поддерживает несколько аргументов, позволяющих задать формат вывода и критерии отбора записей.

`Attach arg` — позволяет подключиться к директории `arg` с правами доступа, указанными в её списке управления доступом (ACL).

`DOWN` — позволяет перейти вниз в поддиректорию (sub-ufd). Необязательный аргумент `arg` указывает, в какую именно поддиректорию следует перейти.

`UP` — позволяет перейти вверх в директорию более высокого уровня (ufd). Необязательный аргумент `arg` указывает, в какую именно.

`WHERE` — показывает текущую точку подключения к директории и ваши права доступа.

`CREATE arg` — создаёт новую поддиректорию с именем, указанным в `arg`.

`COPY arg1 arg2` — копирует файл или директорию, указанные в `arg1`, в файл с именем, указанным в `arg2`. Оба аргумента могут быть именами файлов.

Для печати используется команда `SPOOL`, имеющая следующий формат:

```
SPOOL filename -AT destination
```

где `filename` — имя файла, который нужно распечатать, а `destination` — имя принтера. Например, чтобы распечатать файл `HACK.FTN` на принтере `LIB`, введите:

```
SPOOL HACK.FTN -AT LIB
```

PRIMOS выведет информацию о том, что указанный файл поставлен в очередь, и укажет его размер в записях PRIMOS. Чтобы просмотреть очередь печати, введите:

```
SPOOL -LIST
```

PRIMOS выведет список всех файлов, ожидающих печати на принтерах вашей системы, с указанием имени файла, имени учётной записи пользователя, поставившего файл в очередь, времени постановки в очередь, размера файла в записях PRIMOS и имени принтера.

Смена пароля учётной записи

Чтобы сменить пароль вновь приобретённой учётной записи, используйте команду `CPW` (Change PassWord). Введите текущий пароль в командной строке и нажмите RETURN. PRIMOS попросит вас ввести новый пароль и подтвердить его. Например, чтобы сменить пароль `JOE` на `SCHMOE`, введите:

```
OK,           (система)
CPW JOE       (вы)
New Password? (система)
```

Сохранить копию сеанса работы с терминалом можно с помощью команды `COMO` (COMmand Output). После ввода:

```
COMO filename
```

всё, что вводится или отображается на вашем терминале, записывается в файл с именем, указанным в командной строке. Если файл с таким именем уже существует, он будет ЗАМЕНЁН БЕЗ КАКОГО-ЛИБО ПРЕДУПРЕЖДЕНИЯ! Завершив запись нужного фрагмента сеанса, введите:

```
COMO -End
```

Это остановит запись и закроет файл COMO. Затем вы можете распечатать его с помощью команды `SPOOL`, как описано выше.

Заключение

На этом первый файл о PRIMOS завершён. Помните: этот файл написан прежде всего для начинающих, и некоторые разделы могли показаться вам СКУЧНЫМИ! Тем не менее он намеренно написан подробно, чтобы ПОЛНОСТЬЮ ПОЗНАКОМИТЬ новичков с PRIMOS. Вторая часть будет посвящена нескольким языкам программирования на PRIMOS и ряду других команд.

Послесловие автора

Я хотел бы поблагодарить следующих людей за помощь в написании этого файла:

AMADEUS (старожил, который уже ДАВНО УШЁЛ!)
The University Of Kentucky
State University Of New York (SUNY) Primenet

И многих других…

Вопросы, угрозы и предложения можно направлять мне — меня можно найти на следующих BBS:

```
The Freeworld ][.........301-668-7657
Digital Logic............305-395-6906
The Executive Inn........915-581-5146
OSUNY BBS................914-725-4060
```

-=*< Cosmos Kid >*=-

Взлом глобальной телекоммуникационной сети

Автор: The Kurgan

Составлено 10/5/87

Различия в процедурах работы с сетью

Глобальная телекоммуникационная сеть (GTN) — это международная сеть передачи данных Citibank, которая обеспечивает клиентам и сотрудникам Citicorp доступ к компьютеризированным службам банка по всему миру.

Существует два различных порядка входа в систему: Тип A и Тип B. Все пользователи, кроме некоторых в США, обязаны использовать Тип B. (Для пользователей из США: тип процедуры входа определяется тем, на какой номер вы звоните и какой приветственный баннер получаете.) Приветственные баннеры выглядят следующим образом:

```
ТИП A:
WELCOME TO CITIBANK. PLEASE SIGN ON.
XXXXXXXX

@
PASSWORD =

@

ТИП B:
PLEASE ENTER YOUR ID:-1->
PLEASE ENTER YOUR PASSWORD:-2->

CITICORP (CITY NAME). KEY GHELP FOR HELP.
  XXX.XXX
 PLEASE SELECT SERVICE REQUIRED.-3->
```

Команды пользователя Типа A

Пользовательские команды — это инструкции или сведения, которые вы передаёте в сеть для выполнения. Доступные команды перечислены ниже.

Действие пользователя	Назначение
@ (CR)	Переход в командный режим — режим, в котором можно приостановить активный сеанс и запросить у сети информацию либо выйти из службы. (Примечание: этот символ также служит приглашением сети; см. сообщения Типа A.)
BYE (CR)	Выход из службы из командного режима.

Continue (CR)	Возврат в приложение из командного режима (снятие паузы).
D (CR)	Выход из службы из командного режима.
ID	Идентификация пользователя в сети (начало процедуры входа): введите ID, затем пробел и назначенный вам сетевой идентификатор (обычно 5 или 6 символов).
Status (CR)	Вывод сетевого адреса (только из приглашения @). Этот адрес необходим при «сообщении о проблеме».

Сообщения Типа A

Сеть выводит на экран разнообразные сообщения, требующие ввода команды или несущие информацию.

На экране	Пояснение
@	Приглашение сети — запрос сетевого идентификатора.
BAD PASSWORD	Сеть не принимает ваш пароль.
<address> BUSY	Адрес занят, попробуйте позднее.
WELCOME TO CITIBANK. PLEASE SIGN ON. XXX.XXX	Приветственный баннер сети. Вторая строка содержит адрес для сообщения о «проблемах».
<address> ILLEGAL	Введён несуществующий адрес.
<address> CONNECTED	Соединение установлено.
DISCONNECTED	Соединение разорвано.
NOT CONNECTED	В данный момент вы не подключены ни к одной службе.
NUI REQUIRED	Введите свой сетевой идентификатор пользователя.
PASSWORD =	Запрос назначенного вам пароля.
STILL CONNECTED	Вы по-прежнему подключены к используемой службе.

?	Сеть не распознала введённую вами команду.

Команды и сообщения Типа B

Поскольку процедура Типа B используется при коммутируемых подключениях к GTN, для управления сетью требуется меньше команд. Существует только одна команда Типа B: Break + CR позволяет сохранить соединение с одной службой и одновременно подключиться к другой.

```
"PLEASE ENTER YOUR ID:-1->"
```

Процедуры входа в систему

Существует два типа процедур входа: Тип A и Тип B.

Тип A

Проще всего войти в систему с процедурой Типа A через Telenet. Наберите номер местного порта Telenet. Получив приглашение `@`, введите адрес службы Типа A (приводится далее в статье) и следуйте дальнейшим инструкциям.

Тип B

Наберите номер телефона GTN и дважды нажмите Return. Вы увидите:

```
"PLEASE ENTER YOUR PASSWORD:-2->"
```

Введите сетевой идентификатор и нажмите Return.

Затем появится:

Страна / Город	Номер	Стандарт
Канада, Торонто	416-947-2992	1200 Baud V.22 Modem Standard
США, Лос-Анджелес	213-629-4025	300/1200 Baud U.S.A. Modem Standard
США, Джерси-Сити	201-798-8500	
США, Нью-Йорк	212-269-1274	
США, Нью-Йорк	212-809-1164	

Введите сетевой пароль и нажмите Return.

Наконец вы увидите приветственный баннер `CITICORP (city name)`, после чего система предложит выбрать нужную службу. Введите адрес и нажмите Return. (Список адресов приведён

ниже.)

Устранение неполадок

Если у вас возникнут какие-либо проблемы, персонал Citicorp с удовольствием поможет своим «сотрудникам» с любыми вопросами. Достаточно прикинуться работником Citibank — и вам расскажут многое. Это проверено неоднократно. Нередко при попытке входа в систему, допустив ошибку в пароле, вы получаете номер телефона для получения помощи. Позвоните туда и скажите, что забыли пароль или что-то в этом роде. Обычно это срабатывает, поскольку от вас не ждут обмана. Если у вас есть вопросы по самой сети, звоните по номеру 305-975-5223 — это Центр технических операций (TOC) в Помпано, Флорида.

Коммутируемые подключения

Следующий список коммутируемых номеров предназначен для Северной Америки. Существуют и другие, но они вряд ли кому-нибудь потребуются. Напоминаю: коммутируемые подключения требуют процедуры входа Типа B. Тип A доступен в системах, подключаемых через Telenet.

Страна / Город	Номер	Стандарт
Канада, Торонто	416-947-2992	1200 Baud V.22 Modem Standard
США, Лос-Анджелес	213-629-4025	300/1200 Baud U.S.A. Modem Standard
США, Джерси-Сити	201-798-8500	
США, Нью-Йорк	212-269-1274	
США, Нью-Йорк	212-809-1164	

Адреса служб

Ниже приведён весьма краткий список лишь некоторых из сотен адресов служб. В одном из следующих выпусков будет опубликован полный список.

```
CONNECT 1200
TELENET
216 13.41

TERMINAL=VT100

@2240003300

223 90331E CONNECTED
ENTER TYPE NUMBER OR RETURN
```

```
  TYPE B IS BEEHIVE DM20
  TYPE 1 IS DEC VT100
  TYPE A IS DEC VT100 ADV VIDEO
  TYPE 5 IS DEC VT52
  TYPE C IS CIFER 2684
  TYPE 3 IS LSI ADM 3A
  TYPE L IS LSI ADM 31
  TYPE I IS IBM 3101
  TYPE H IS HP 2621
  TYPE P IS PERKIN ELMER 1200
  TYPE K IS PRINTER KEYBOARD
  TYPE M IS MAI BASIC 4
  TYPE T IS TELEVIDEO 9XX
  TYPE V IS VOLKER CRAIG 4404
  TYPE S IS SORD MICRO WITH CBMP
  RELEASE BSC9.5 - 06JUN85
  FOR 300 BAUD KEY ! AND CARRIAGE RETURN
  CONFIG.□K1.1-I11H-R-C-B128
  ENTER TYPE NUMBER OR RETURN K

  CONNECTED TO CITIBANK PARIS - CBP1 ,PORT 5
```

Пример процедуры входа

Ниже приведён буферизованный текст сеанса входа в CITIBANKING PARIS через Telenet.

Пользуйтесь этой информацией с умом — и помните: в конечном счёте победит технология.

Законы, регулирующие мошенничество с кредитными картами

Автор: Tom Brokaw

19 сентября 1987 года

Написано эксклюзивно для Phrack Magazine

(Совместный выпуск Tom Brokaw / Disk Jockey Law File)

Введение

В этой статье я попытаюсь объяснить законы, касающиеся незаконного использования кредитных карт. Будет рассмотрена позиция законодательства штата Мичиган в отношении злоупотреблений кредитными картами и их определения.

Определение

Раздел 157 законодательства штата Мичиган определяет кредитную карту как «любой инструмент или устройство, которое продаётся, выпускается или иным образом распространяется коммерческой организацией, указанной на нём, для получения товаров, имущества, услуг или чего-либо ценного». Держатель кредитной карты определяется как: 1) «лицо или организация, запросившие кредитную карту и в пользу которых впоследствии выпущена кредитная карта», либо 2) «лицо или организация, которым была выпущена кредитная карта и которые используют её независимо от того, был ли запрос на выпуск сделан или нет». Иными словами, если компании или физическому лицу выдана карта и они начали ею пользоваться, они автоматически принимают все законы и условия, связанные с ней.

Кража, изъятие, удержание или сокрытие

Законодательство штата Мичиган устанавливает, что незаконно «красть, заведомо брать или изымать кредитную карту у держателя карты». Также незаконно «скрывать кредитную карту без согласия её держателя». Обратите внимание: здесь ничего не говорится о копирках или номерах, полученных с BBS. Однако я полагаю, что это может быть квалифицировано как часть законов, регулирующих доступ к счёту человека без ведома держателя карты, как описано выше.

Владение с намерением распространить или продать

Закон устанавливает, что незаконно владеть кредитной картой или контролировать её, а также получать её, если намерение состоит в распространении или продаже карты. Также незаконно

передавать, распространять или продавать кредитную карту, зная, что такое владение, контроль или получение осуществляется без согласия держателя карты, — виновный признаётся совершившим **тяжкое преступление (felony)**. Снова обратите внимание: здесь прямо ничего не говорится о владении копирками или номерами. Также чётко не прописано, что именно считается «распространением» или «владением», поэтому мы можем лишь предполагать. Сказано лишь то, что владение физической картой (пластиком) является незаконным.

Мошенничество, подделка, существенное изменение, фальсификация

Тем не менее, само по себе владение копиркой или номером кредитной карты может и не считаться явно незаконным. Однако мошенничество в отношении держателя кредитной карты **однозначно незаконно**. Законодательство Мичигана устанавливает, что любое лицо, которое с умыслом на мошенничество, подделку, существенное изменение или фальсификацию кредитной карты, признаётся виновным в тяжком преступлении.

Использование отозванной или аннулированной карты с умыслом на мошенничество

Данное положение устанавливает, что «любое лицо, которое заведомо и с умыслом на мошенничество, с целью получения товаров, имущества или услуг или чего-либо ценного, использует кредитную карту, отозванную или аннулированную либо заявленную украденной эмитентом или получателем, и которому было направлено уведомление об аннулировании заказным или заверенным письмом либо иным способом личного вручения, подлежит штрафу в размере не более $1 000 и лишению свободы на срок не более одного года, либо и тому, и другому». Однако в законе чётко не указано, является ли это тяжким преступлением, проступком или гражданским нарушением. По моим предположениям, это будет зависеть от суммы и способа, посредством которых было совершено мошенничество. Как правило, если сумма не превышает $100 — это проступок, если свыше $100 — тяжкое преступление. Видимо, законодатели считают, что граждане должны знать об этом сами.

Дело «Народ штата Мичиган против Андерсона» (владение)

4 апреля 1980 года некий Х. Андерсон попытался купить пару брюк в магазине Danny's Fashion Shops в районе Детройта. Когда он подошёл к кассиру расплатиться, тот спросил, есть ли у него разрешение пользоваться кредитной картой. Андерсон ответил: «Нет, я выиграл её вчера ночью в карточной игре». По его словам, он мог купить товаров на $50, чтобы погасить долг. При этом он полагал, что карта действительна и не является краденой. Однако выяснилось, что карта была украдена, хотя Андерсон об этом не знал. Впоследствии он предстал перед судом и признал себя виновным в попытке незаконного владения чужой кредитной картой с умыслом на её распространение или продажу. На слушаниях по признанию вины г-н Андерсон заявил, что кредитная карта, которую он пытался использовать, была получена им в счёт уплаты карточного долга, и он полагал, что передавший её человек является её законным владельцем. Суд первой инстанции принял его признание вины. Однако во время вынесения приговора Андерсон отрицал

какой-либо преступный умысел. Он обжаловал решение, указав, что суд ошибочно принял его признание вины на основании недостаточных фактических данных. В связи с этим суд первой инстанции не должен был выносить обвинительный приговор по статье о попытке незаконного владения, и обвинения были сняты.

Дело «Народ штата Мичиган против Уилли Докери»

23 июня 1977 года Уилли Докери попытался купить бензин на заправочной станции Sears, используя краденую кредитную карту. Работник станции заметил, что фотография на водительских правах была наклеена поверх оригинальной, и вызвал полицию. Докери заявил, что нашёл кредитную карту и права на перекрёстке в городе Флинт. Он признал, что сознательно использовал кредитную карту и водительские права без согласия владельца, однако утверждал, что купил на карту только бензин. Выяснилось, что кредитная карта и права были похищены у человека, чей продуктовый магазин был ограблен. Докери заявил, что ничего не знал о краже и предыдущих операциях по карте на общую сумму $1 373,21. Он признал, что сам наклеил свою фотографию на водительские права. Однако суд вновь допустил ошибку: следствие представило доказательства того, что у обвиняемого имелись судимости за тяжкие преступления, начиная с шестнадцатилетнего возраста, и суд сделал вывод о его виновности на основании предыдущих правонарушений. Впоследствии судья констатировал, что вынесенный приговор не может устоять в данном суде, и дело было передано в другой суд.

Заключение

Я надеюсь, что смог дать вам более глубокое понимание законодательства, регулирующего незаконные аспекты использования кредитных карт. Вся приведённая информация взята из «Свода законов штата Мичиган с комментариями» (Michigan Compiled Laws Annotated), том 754, разделы 157a–s, а также из «Сборника апелляционных решений штата Мичиган» (Michigan Appeals Report).

В следующем файле я расскажу о законах, касающихся мошенничества с чеками.

— Tom Brokaw

Прослушивание телефонных линий

Голос или данные

Ради удовольствия, денег и паролей

Или как надолго угодить за решётку.

Автор: Agent Steal, 08/87

В этом файле рассматривается:

• Необходимое оборудование
• Где его купить
• Как подключить
• Как читать записанные данные

Но и это ещё не всё:

• Как я нашёл узел Tymnet
• Как я туда попал

Оборудование

Первое, что вам понадобится — аудиокассетный магнитофон. То, что вы будете записывать — голос или данные — представлено в аналоговом аудиоформате. В дальнейшем речь пойдёт преимущественно о записи данных. Большинство стандартных кассетных магнитофонов вполне подойдут. Однако их ограничение — один час записи на сторону, что в ряде ситуаций создаёт неудобства. Можно использовать катушечный магнитофон. Его минусы — габариты и необходимость питания от сети. Кроме того, некоторые катушечники лишены разъёма дистанционного управления, который нужен для запуска и остановки записи в момент использования линии, — хотя это не всегда критично. Подробнее — далее. Два типа магнитофонов, которые я не рекомендую для записи данных: микрокассетные диктофоны и стандартные кассетники, модифицированные для записи продолжительностью 8–10 часов. Скорость лентопротяжного механизма у них слишком нестабильна. Следующий необходимый элемент — устройство, которое Radio Shack продаёт под названием «Telephone recording control», артикул 43-236, цена $24.95. См. стр. 153 каталога Radio Shack 1987 года.

Как подключить

Блок управления записью с телефона (TRC) имеет три провода.

#1 — провод с модульным телефонным разъёмом. Срежьте его и замените на крокодиловые зажимы.

#2 — аудиопровод с миниатюрным телефонным джеком (не телефонным в смысле RJ). Подключается к входу микрофонного уровня магнитофона.

#3 — аудиопровод с субминиатюрным телефонным джеком. Подключается к разъёму «REM» или дистанционного управления магнитофона.

Теперь остаётся лишь найти телефонную линию, подсоединить крокодиловые зажимы, включить магнитофон и вернуться позже. Как только трубка снимается, магнитофон запускается. Всё просто.

Чтение данных

Это самая трудоёмкая часть. Разные модемы и программы ведут себя по-разному, но есть общие принципы. Модем подключается как обычно — к телефонной линии и компьютеру. Затем вывод динамика кассетного плеера подключается напрямую к телефонной линии. Снимите трубку и наберите старший номер петли, чтобы на линии не было лишних шумов, мешающих данным. После этого переведите модем в режим ответа и нажмите «Воспроизведение». Лента должна стоять в начале записанного звонка — чтобы увидеть начало входа в систему. За один раз можно прослушивать только одну сторону сеанса связи. В режиме originate вы видите то, что передавал хост, включая эхо терминала. Пароль, разумеется, будет отражаться в виде `#######`, однако переключившись в режим answer, вы увидите именно то, что вводил терминал. Разберётесь, когда увидите. Возможные проблемы — фон и мусорные символы на экране. Попробуйте подключить выход динамика к микрофону телефонной трубки. Используйте согласующий трансформатор 1:1 между входом плеера и аудиовыходом TRC. Эти проблемы, как правило, возникают при использовании оборудования с питанием от сети: общая земля такого оборудования создаёт помехи с телефонной землёй, работающей от постоянного тока.

Я несколько колебался, прежде чем написать этот файл, — мне так и не удалось прочитать ни одну из записей данных на скорости 1200 бод. Я консультировался с инженерами и техниками, в том числе с одним из разработчиков модемов. Все они сошлись во мнении, что это В ПРИНЦИПЕ возможно, но объяснить мою неудачу никто не смог. Думаю, проблема в моём дешёвом модеме. Один из техников сказал, что мне нужен модем с цепью фазовой коррекции, которая встречается в большинстве дорогих модемов на 2400 бод. Ну, когда-нибудь найду пятьсот долларов на улице и потрачу их именно на это! Ха! На самом деле у меня есть план — но это уже другой файл...

Стоит упомянуть один способ чтения данных на 1200 бод. Теоретически он должен работать, хотя сам я его не пробовал.

Любой полностью Hayes-совместимый модем поддерживает команду, отключающую несущую и переводящую в режим мониторинга линии. Команда — `ATS10`. Затем нужно выбрать режим answer или originate в зависимости от того, чью сторону вы хотите прослушать. Можно написать программу, записывающую первые 300 или около того символов и сохраняющую их на диск — это позволит работать в автоматическом режиме без присутствия оператора.

Насколько я безбашенный

ПАРОЛЕЙ — ЗАВАЛИСЬ!

После многочисленных звонков в несколько офисов Bell я нашёл тот, который обслуживал счёт Tymnet. Вот примерная стенограмма:

```
Оп:  Pacific Bell, отдел приоритетных заказов клиентов. Чем могу помочь?
Я:   Доброе утро, это Миллер из Tymnet Inc. Нас интересует расширение услуг
     в нашем офисе в городе X.
Оп:  С удовольствием помогу, мистер Миллер.
Я:   Мне нужно узнать, сколько линий у нас входит в ротари и есть ли
     свободные пары в магистрали. Мы рассматриваем добавление десяти
     дополнительных линий в ротари и, возможно, подключение FX-сервиса.
Оп:  Хорошо... На какой номер оформлен счёт?
Я:   xxx-xxx-xxxx (номер местного узла)
Оп:  Минуту... Хорошо, так-то и так-то...
```

В общем, идею вы поняли. После нескольких незначительных уточняющих вопросов я попросил её назвать адрес. Без проблем, она даже не колебалась. Конечно, всего этого можно было избежать, если бы служба CN/A в моём районе выдавала адреса, — но они дают только списки абонентов. Облачившись в лучший телефонистский наряд — кепку Pac*Bell, рабочий пояс с инструментами и измерительную трубку — я отправился туда. Обычное офисное здание, там даже магазин компьютеров был. Побродив по нему, я нашёл то, что искал: массивная стальная дверь с кодовым замком. Снова к телефону. Разыскав номер, по которому можно было дозвониться до сервисных техников, я позвонил и поговорил с их менеджером.

```
Мен: Алло, это Джо Болван.
Я:   Привет, это Миллер (мне нравится это имя) из Pacific Bell. Я сейчас
     у вашего узла в городе X, у нас проблема — ищем утечку газа в одном
     из магистральных кабелей. Кажется, наш магистральный кабель теряет
     давление прямо в вашем помещении.
Мен: Не уверен...
Я:   Могли бы вы прислать кого-нибудь или просто сказать мне код входа?
Мен: Конечно, код 1234.
Я:   Спасибо, если что — дам знать.
```

Я помчался домой, взял стерео-видеомагнитофон и купил ещё один TRC в Trash Shack. Подключил видеомагнитофон к первым двум входящим линиям ротари: каждая пошла на свой канал (левый и правый). Поскольку поток звонков был более-менее постоянным, останавливать запись между ними не требовалось — я просто оставлял его работать. Возвращался на следующий день, чтобы сменить кассету. Видеомагнитофон спрятал под поднятым полом на случай, если кто-то из техников придёт на обслуживание. Эти узлы — небольшие компьютерные комнаты с кондиционерами и фальшполом. Модемы и коммутационное оборудование пакетной сети смонтированы в стойках за стеклом. Большинство узлов при этом не обслуживается постоянным персоналом. Что мне удалось получить? Многие сеансы шли на 1200 бод, так что содержимое я так и не узнал — хотя записи всё ещё хранятся на плёнке. Значительную часть трафика в Tymnet и Telenet составляют маленькие терминалы для проверки кредитных карт, выходящие на Visa или Amex: транзакция длится около 30 секунд, и на моих плёнках таких — сотни. Остальное:

• Easylink
• CompuServe
• Quantumlink
• 3Mmail
• PeopleLink
• Homebanking
• USPS
• Chrysler parts order
• Yamaha
• Ford
• Dow Jones

...и ещё несколько разных систем, не представляющих особого интереса. Уверен, если бы я проявил больше настойчивости, нашлось бы что-то поинтереснее. Я провёл несколько месяцев, пытаясь разобраться с проблемой 1200 бод. Когда я вернулся туда снова — код уже сменили. Почему? Разбираться не стал. Убрался подобру-поздорову. Я рассказал кое-кому, кто, как потом выяснилось, не заслуживал доверия. Что ж. Лучше перестраховаться.

Если нужно со мной связаться — попробуйте мою VMS по номеру 415-338-7000, ящик 8130. Правда, неизвестно, надолго ли. Ну и, конечно, всегда есть P-80 systems по номеру 304-744-2253 — там, наверное, навсегда. Спасибо Scan Man, кто бы ты ни был. Также читайте мой файл о разводке местных телефонных петель — он поможет понять, как найти нужную линию. Называться он должен `Telcowiring.Txt`.

<<< AGENT STEAL >>>

Чтение отчётов Trans-Union: урок по терминологии

Автор: The Disk Jockey

(Материал группы 2af)

Этот файл посвящается всем фрикам и хакерам, арестованным летом 1987 года — пожалуй, одного из самых разрушительных лет для нашего сообщества.

Предисловие

Trans-Union — кредитное бюро, схожее с CBI, TRW или Chilton, однако предлагающее более конкурентные тарифы и всё активнее используемое различными агентствами кредитных проверок.

Вход в систему

Позвоните на один из коммутируемых номеров Trans Union по параметрам 300, E, 7, 1, Half Duplex. Один из таких номеров — 314-XXX-XXXX. После подключения нажмите Ctrl-S. Система ответит `GO` и будет ждать ввода учётных данных: номера счёта, пароля и режима, например: `S F1111,111,H,T`. Затем система сообщит, к какой базе данных вы подключены — для ваших целей это, как правило, не имеет значения. Чтобы получить отчёт, введите:

```
P JONES,JIM* 2600,STREET,CHICAGO,IL,60604** <Ctrl-S>
```

Здесь: Jim Jones — имя субъекта, 2600 — номер дома, STREET — название улицы, Chicago — город, IL — штат, 60604 — почтовый индекс.

Отчёт

Отчёт будет выглядеть несколько необычно, с обилием нотаций. Пример записи по карте Visa:

```
SUB NAME/ACCT#  SUB#     OPEND  HICR DTRP/TERM BAL/MAX.DEL PAY.PAT   MOP

CITIBANK         B453411  3/87  $1000  9/87A    $0    12111     R01
4128XXXXXXXXX             $1500        5/87     $120
```

Расшифровка: Citibank — банк-эмитент; B453411 — код подписчика; 3/87 — дата открытия счёта; HICR — максимальная сумма, потраченная по карте; 9/87 — дата последнего обновления отчёта (обычно ежемесячно при активном использовании); $1000 — кредитный лимит; $0 — текущий баланс; 12111 — история платежей, где 1 = оплата в течение 30 дней, 2 = оплата в течение 60 дней; R01 означает «возобновляемый» (Revolving) счёт — держатель может вносить частичные платежи вместо полного погашения долга; 4128-etc — номер счёта (номер карты); $1500 — кредитный лимит по карте; 5/87 — дата последней просрочки; $120 — сумма просроченного платежа.

Ниже приведён список терминов, которые помогут лучше идентифицировать и понимать отчёты.

Коды ECOA: идентификаторы запросов и счетов

Код	Значение
I	Индивидуальный счёт для единоличного использования заявителем
C	Совместная договорная ответственность супругов
A	Авторизованный пользователь общего счёта
P	Участник использования счёта, не являющийся ни C, ни A
S	Поручитель, не являющийся супругом
M	Основной должник по счёту с привлечением поручителя
T	Отношения со счётом прекращены
U	Не обозначено
N	Запрос от супруга, не являющегося заявителем

Коды замечаний и споров FCBA

U	Не обозначено
N	Запрос от супруга, не являющегося заявителем

Тип счёта

Код	Значение
O	Открытый счёт (30 или 90 дней)
R	Возобновляемый или опционный счёт (открытый)
I	Рассрочка (фиксированное число платежей)

M	Ипотека
C	Чековый кредит (кредитная линия в банке)

Обычный порядок платежей

Код	Значение
00	Слишком новый для оценки; одобрен, но не используется или не оценён
01	Платит (или платил) в течение 30 дней с момента выставления счёта; соблюдает условия
02	Платит более чем через 30 дней, но не более чем через 60 дней
03	Платит более чем через 60 дней, но не более чем через 90 дней
04	Платит более чем через 90 дней, но не более чем через 120 дней
05	Платит через 120 дней и более
07	Вносит платежи по плану выплат под контролем суда или аналогичному соглашению
08	Изъятие имущества
8A	Добровольное изъятие
8D	Принудительное изъятие по решению суда
8R	Имущество выкуплено после изъятия
09	Безнадёжный долг; передан в коллекторское агентство; судебный иск; решение суда; уклонение
9B	Передан в коллекторское агентство
UR	Без оценки
UC	Не классифицирован

Классификация видов бизнеса

Код	Значение
A	Автомобильная отрасль
B	Банки
C	Одежда
D	Универмаги и магазины разнообразных товаров
F	Финансы
G	Продукты питания
H	Товары для дома
I	Страхование
J	Ювелирные изделия и фотоаппараты
K	Подрядчики
L	Лесоматериалы и строительные материалы
M	Медицина и здравоохранение
N	Национальные кредитные карты
O	Нефтяные и национальные кредитные карты
P	Персональные услуги (кроме медицинских)
Q	Торговля по почте
R	Недвижимость и предприятия общественного питания
S	Спортивные товары
T	Товары для сельского хозяйства и садоводства
U	Коммунальные услуги и топливо
V	Государственный сектор
W	Оптовая торговля
X	Реклама
Y	Коллекторские службы

Z	Прочее

Тип рассрочного кредита

AF	Бытовая техника / мебель
AP	Самолёт
AU	Автомобиль
BT	Лодка
CA	Трейлер-дом
CL	Кредитная линия
CM	Совместный заёмщик
CO	Консолидация долгов
EQ	Оборудование
FH	Кредит по программе FHA
FS	Финансовая ведомость
HI	Улучшение жилья
IN	Страхование
LE	Аренда (лизинг)
MB	Мобильный дом
MC	Прочее
MT	Моторхоум
PI	План улучшения имущества
PL	Личный кредит
RE	Недвижимость
ST	Студенческий кредит
SV	Сберегательные облигации, акции и т.п.
US	Необеспеченный кредит

VA	Кредит для ветеранов

Коды дат

C	Дата закрытия
F	Изъятие / списание
M	Дальнейшие обновления прекращены
P	Оплачено
R	Внесённые данные
S	Дата последней продажи
V	Дата подтверждения

Индикатор подтверждения занятости

R	Внесено, но не подтверждено
S	Медленный ответ
T	Уволен
V	Подтверждено
X	Нет ответа

Надеюсь, это поможет. Все, кто работал с Trans-Union, безусловно оценят эту шпаргалку — коды результатов порой весьма трудно расшифровать.

— The Disk Jockey

Phrack World News, часть 1

Автор: Shooting Shark

Из San Francisco Chronicle от 16 сентября, стр. A19:

НЕМЕЦКИЕ ХАКЕРЫ ВЗЛОМАЛИ СЕТЬ NASA (выдержки)

Бонн

Группа западногерманских компьютерных любителей проникла в международную компьютерную сеть Национального управления по аэронавтике и исследованию космического пространства и свободно копалась в данных не менее трёх месяцев, прежде чем была обнаружена — об этом сообщили вчера энтузиасты и пользователи сети.

Организация из Гамбурга под названием Chaos Computer Club, выступившая от имени анонимной группы, осуществившей взлом, заявила, что незваным гостям удалось установить «троянского коня» и получить доступ к 135 компьютерам европейской сети.

«Троянский конь» — термин, обозначающий постоянно действующую программу, которая позволяет компьютерным любителям [в отличие от профессионалов?], или «хакерам», использовать пароль для обхода всех защитных процедур системы и получить доступ ко всем данным на целевом компьютере.

[На самом деле подобная программа называется «бэкдор» или «люк». Группа вполне могла *использовать* троянского коня, чтобы создать бэкдор, однако сам по себе это, по всей видимости, не был троянский конь. Троянский конь — это программа, которая, помимо ожидаемой функции, выполняет некие скрытые от пользователя вредоносные действия. Смотрите Phrack xx-x, «Unix Trojan Horses», где описано, как создать троянского коня, в свою очередь создающего люк в чужую учётную запись.]

Взломанная сеть NASA называется Space Physics Analysis Network [ого!] и предназначена главным образом для предоставления авторизованным учёным и организациям доступа к данным NASA. Систему безопасности сети поставила американская компания Digital Equipment Corp. [Наверное, DECNET. Поделом им.] Пользователи сообщили, что сеть широко применяется учёными в США, Великобритании, Западной Германии, Японии и пяти других странах и не содержит засекреченных сведений.

Представитель Chaos Club Bay Холланд отрицал, что какие-либо данные были изменены. По его словам, это противоречило бы «хакерской этике».

В репортажах западногерманского телевидения сообщалось, что компьютерное пиратство карается в Западной Германии лишением свободы сроком до трёх лет. Правительство пока не сообщило, какие меры намерено предпринять.

Chaos Club явно расценивает свой взлом как крупный успех. Холланд, которому позвонили по телефону в Гамбурге, назвал произошедшее «наиболее успешным применением троянского коня» из всех ему известных; клуб также разослал обширное телексное сообщение в новостные организации.

В нём говорилось, что «троянский конь» был обнаружен пользователем в августе, после чего группа взломщиков решила предать дело огласке, поскольку «почувствовала, что вступает на опасную территорию промышленного шпионажа, экономических преступлений, противостояния

Востока и Запада... а также законных интересов безопасности высокотехнологичных учреждений».

Еженедельный журнал Stern опубликовал интервью с несколькими анонимными любителями, которые показали, как именно получали доступ к сети. Один из них описал своё волнение, когда впервые увидел на экране: «Welcome to the NASA headquarters VAX installation».

По данным Chaos, любители обнаружили уязвимость в системах Digital VAX версий 4.4 и 4.5 и воспользовались ею для установки своего «троянского коня».

[Выдержки набраны Shooting Shark. Комментарии — его же.]

История о федералах на XXXXXXX BBS

Автор: The Mad Phone Man

[Примечание редактора: Некоторые данные в статье намеренно скрыты (XXXXX) по просьбе автора]

Однажды днём я вернулся домой вместе с другом и сразу почувствовал: что-то не так, едва зашёл в комнату с компьютером. На борде появился «Новый пользователь»... и язык, которым он писал, был... скажем так, «устрашающим»...

«Хочу, чтобы вы все знали: я из оперативной группы OCC, и мы знаем, кто вы такие... скоро мы устроим небольшую встречу и "побеседуем" с каждым из вас.»

Хм... лузер? Захожу в режим чата: «Эй, чувак, что происходит?» — спрашиваю.
«Твой номер, придурок», — отвечает он.

Ну и способ заходить на борду, скажу я вам...

«Слушай, ты знаешь, я с тобой разговаривал и знаю, кто ты.»
«О да?.. И кто же я?»

Он мешкает и говорит: «Ну... ты же раньше работал в Sprint, не так ли?»

Я отвечаю: «Нет, ты меня с кем-то спутал. Я учусь в старшей школе, одиннадцатый класс.»

«Вот как?.. Больно умные слова для школьника», — говорит он.

«Ну, на всякий случай сообщаю: английскому у нас теперь учат всерьёз...»

Он говорит: «Ты действительно хочешь знать, в какой LD-компании я работаю?»

Я говорю: «Нет, но если тебе от этого полегчает — скажи.»

Он называет MCI. (Уф! Я ими не пользуюсь.) «Что ж, не повезло тебе, придурок — я сам плачу за звонки и MCI не использую.» Его это явно ставит в тупик.

Я желаю ему всего наихудшего; он просит оставить его угрожающий пост на моём борде, после чего мы вешаем трубки.

Теперь я наполовину парализован... хм... Проверяю его анкету: оставил номер с кодом 303... Денвер... Хватаю трубку, звоню. Это телефонная компания Stromberg. Бинго — он у меня в руках.

Лезу в файлы пользователей — нахожу пользователя под ником «Cocheese» оттуда. Провёл с ним голосовую верификацию; он сказал, что работает в небольшой телко под названием Stromberg. Теперь я на его след напал.

Чуть позже на той же неделе я нахожусь в офисе телефонной компании в ближайшем крупном городе. Случайно вижу папку с надписью «Конфиденциально. Табельные номера сотрудников AT&T». Листаю — и вот он: некий R.F. Stromberg работает в одном из офисов AT&T в Денвере, но перекрёстной ссылки на конкретный отдел нет. (Верный признак того, что он занимается безопасностью.) Не желая уступать этому лузеру, я набираю NCIC и делаю групповой запрос по водительским правам на его имя. Бинго. Номер прав, список машин в собственности, номер социального страхования — а перекрёстная ссылка по файлам водительских прав выдаёт жену, двух детей и зарегистрированную на него лодку.

Я так ему и не перезвонил, но если у меня когда-нибудь возникнут с ним проблемы — я нанесу небольшой визит в Колорадо...

Побег BBS Безумного Телефонщика в дружественную иностранную державу

Автор: The Mad Phone-Man

[Примечание редактора: некоторые имена в статье изменены для защиты автора]

Зная, что копы конфискуют компьютер при обыске, я всерьёз обеспокоился потерей крупных вложений в мой IBM. Я решил, что есть способ получше... Переехать! Но куда? Где безопасно от PhBI? В старые времена, чтобы избежать призыва, люди бежали в Канаду — почему бы не эмигрировать туда же со своей доской? Правда, стоимость аренды линии там весьма высокая — надо поискать, что предлагают в других местах.

Как-то раз днём я работаю в местной больнице (той, для которой делаю телекоммуникационные работы) и спрашиваю менеджера по связи, есть ли у них каналы в Канаду. Он говорит — да, мол, есть межмедицинский канал через 23-гигагерцовый микроволновый линк в город прямо через границу. Прошу показать оборудование. ВОТ ЭТО ДА! Мечта становится явью: стоит D4-банк (Rockwell), а в нём всего четыре карты каналов. Будучи «хорошим» парнем, я предлагаю ему обслуживание этого оборудования в обмен на разрешение добавить ещё один канал — он соглашается. Интрига нарастает.

У меня есть вспомогательный офис для одного бизнеса неподалёку от больницы, на другой стороне границы. Я быстро звоню в добрый старый Bell Canada и прошу провести двухпроводную линию из аппаратной к моему офису. Остаётся только раздобыть пару карт для вставки в мультиплексор, чтобы выйти в эфир.

Двухпроводная карта E&M стоит около 319 долларов, и нужны две штуки. Обзваниваю поставщиков по штату — нахожу одну неисправную в Рочестере. В тот же день отправляюсь туда на мотоцикле. Карта у меня — единственная неисправность, которую удаётся найти, это плохой регулятор напряжения. Заезжаю в офис Rockwell в пригороде Рочестера, обмениваю карту, а заодно покупаю вторую (да, на свою карточку) — и еду домой. К 9 вечера того же дня канал поднят, и мы в эфире.

Результат: очень хорошая линия, без шумов, при желании её можно переделать под другую карту за скромную плату и расширить полосу пропускания. Вот так и получилось, что доска переехала в «дружественную иностранную державу».

The Mad Phone-Man

Shadow Hawk снова арестован

Автор: Phrack World News, часть 4

Как многие из вас знают, Shadow Hawk (он же Shadow Hawk 1) пережил обыск в своём доме — агенты ФБР, Секретной службы и Следственного управления по уголовным делам Министерства обороны провели его 4 сентября и изъяли часть имущества. Мы не будем перепечатывать статью из Washington Post — она доступна из других источников. Вместо этого — краткое изложение.

В начале июля SH купил AT&T 3B1 («Unix PC») с диском на 67 МБ за смешные $525. За Sys V 3.5 он доплатил ещё $200, однако остался недоволен большей частью прилагаемого программного обеспечения (в частности, ему досталась версия uucp 1.1).

Когда федералы вышли на него, он скачивал программное обеспечение (в виде исходных кодов на C) с различных систем AT&T. По имеющимся сведениям, среди них были инсталляции Bell Labs в Нейпервилле (штат Иллинойс) и Мюррей-Хилл (штат Нью-Джерси). Прокуроры также утверждали, что он получил доступ к системам AT&T (и скачал с них ПО) на объекте НАТО в Берлингтоне (Северная Каролина) и на авиабазе Робинс в Джорджии. AT&T заявила, что он похитил программного обеспечения на $1 миллион. Часть из него — невыпущенные разработки, изъятые с систем Bell Labs, которым представители Bell Labs присвоили гипотетические ценники. Агенты конфисковали его 3B1, два Atari ST, находившихся в его комнате, и несколько дискет.

SH — 17 лет, и по всей видимости дело будет рассматриваться в соответствии с нормами о несовершеннолетних. На момент написания этого материала ему либо грозило федеральное уголовное преследование за «компьютерное хищение», либо дело могло быть ограничено преследованием по законодательству штата Иллинойс.

Адвокат SH, Карен Плант, была процитирована следующим образом: SH «категорически отрицает, что делал что-либо недозволенное», и что у него «не было абсолютно никаких злых умыслов в плане хищения имущества». Как уже говорилось, он просто собирал программное обеспечение для своего нового Unix PC. Когда я связался с г-жой Плант 25 сентября, она сообщила, что понятия не имеет, будет ли федеральный прокурор возбуждать дело и когда. С Карен Плант можно связаться по телефону (312) 263-1355. Её адрес: 134 North LaSalle, #306, Chicago, Illinois.

Из письма SH от 9 июля

```
So you see, I'm screwed. Oh yeah, even worse! In my infinite (wisdom
|| stupidity, take your pick 8-)) I set up a local AT&T owned 7300 to call me
up and send me their uucp files (my uucp works ok for receive) and guess what.
I don't think I've to elaborate further on THAT one... (holding my breath, so
to type)
□□□□(_>Sh<_
```

Перевод: Итак, как видите — я влип. О да, и это ещё не всё! В своей бесконечной (мудрости || глупости — выбирайте сами 8-)) я настроил местный AT&T 7300 так, чтобы он звонил мне и присылал свои uucp-файлы (мой uucp нормально принимает) — и угадайте, что вышло. Думаю, не стоит расписывать ЭТОТ момент подробнее... (затаив дыхание, так сказать)

Phrack World News, часть 5

Автор: Tribune Staff Writer (набрал $muggler)

«Телефонные компании по всей стране хотят узнать номер похитителя монетных ящиков»

Из Tribune — четверг, 5 ноября 1987 г.

САН-ФРАНЦИСКО — Семь телефонных компаний по всей стране, включая Pacific Bell, настолько измотаны одним похитителем монетных ящиков, что объявили вознаграждение в размере 25 000 долларов за его поимку.

По словам представителей телефонных компаний, он чрезвычайно ловок — единственный известный в стране подозреваемый, способный с относительной лёгкостью вскрывать замки монетных ящиков в телефонных будках.

Считается, что он несёт ответственность за кражи сотен тысяч долларов из монетных ящиков в районе залива и Сакраменто за текущий год.

Власти установили личность подозреваемого: Джеймс Кларк (James Clark), 47 лет, из Пенинсулы, штат Огайо, — механик и инструментальщик, которому предположительно приписываются кражи из монетных ящиков ещё в 24 штатах.

Другие компании, участвующие в выплате вознаграждения: Ohio Bell, Southern Bell, South Carolina Bell, South Central Bell, Southwestern Bell, Bell Telephone of Pennsylvania и U.S. West.

По имеющимся данным, Кларк промышлял у таксофонов вблизи автострад и других крупных магистралей. Его внешность: рост около 175 см, волосы до плеч каштанового цвета, очки в золотой оправе. Предполагается, что он передвигается на новом микроавтобусе Chevrolet Astro тёмно-синего металлика.

Недавно он находился в Аризоне, однако, по имеющимся сведениям, вернулся в Калифорнию.