Phrack RU issue 017

Русская версия Phrack, выпуск 017. Полный текст статей с кодом и таблицами.

Темы выпуска: культура Phrack, новости сцены, loopback, prophile и хакерские манифесты.

Материалы выпуска: Введение в Phrack XVII; Отчёт Dun & Bradstreet об AT&T; Отчёт Dun & Bradstreet о компании Pacific Telesis; Взрывчатые вещества на основе триодида азота; Как взломать CDC Cyber; Как взломать HP 2000; Доступ к государственным компьютерам; Безопасность модемов с обратным дозвоном; Перехват компьютерных данных — проще простого; Phrack World News, часть 1; «Облава на незаконных хакеров»; Phrack World News, Часть 3.

Введение в Phrack XVII

Автор: Shooting Shark

07 апреля 1988 года

Прошло немало времени, но мы вернулись. После двух успешных выпусков под новым редакторством Таран Кинг сообщил нам, что во время каникул сможет собрать Phrack Seventeen. Его планы вскоре изменились, и Семнадцатый номер снова стал нашей ответственностью. Прокрастинация взяла своё, при компиляции файлов возникли некоторые трудности, но в итоге мы справились — и вот он перед вами.

В этом выпуске немало хорошего материала, и нам повезло: вклад в PWN внесли несколько источников, что превратило номер в настоящий коллективный труд. Поскольку The Mad Chemist и Sir Francis Drake, как и я сам, переходят к другим делам, редакторство Phrack Inc. может смениться с выходом Phrack Eighteen. Вне зависимости от того, в каком направлении двинется издание, я знаю, что участия в создании следующего выпуска принимать не буду, — поэтому хочу сейчас отметить: моя причастность к журналу — сначала в качестве автора, а затем приглашённого редактора — была в удовольствие. Phrack продолжит существование — я уверен — ещё как минимум семнадцать выпусков и по-прежнему будет главным памятником жизнеспособности хакерской культуры.

— Shooting Shark
Приглашённый редактор

Содержание Phrack XVII

17.7	Доступ к правительственным компьютерам	The Sorceress	9K
17.8	Безопасность модемов с обратным дозвоном	Elric of Imrryr	11K
17.9	Перехват данных без лишних усилий	Elric of Imrryr	4K
17.10	PWN17.1 Обновление по делу об аресте	Sir Francis Drake	3K
17.11	PWN17.2 «Незаконная» волна преследований хакеров	The $muggler	5K
17.12	PWN17.3 Крекеры обманывают Bell	The Sorceress	8K

Отчёт Dun & Bradstreet об AT&T;

Автор: Elric of Imrryr

Кредитное досье AT&T, получено из базы Dun & Bradstreet пользователем Elric of Imrryr.

```
% = % = % = % = % = % = % = %
=                           =
%   P h r a c k   X V I I   %
=                           =
% = % = % = % = % = % = % = %

      Phrack  Seventeen
        07 April 1988

File 2 of 12 : Dun & Bradstreet Report on AT&T
```

Финансовые записи Dun & Bradstreet

Copyright (C) 1987, Dun & Bradstreet Credit Service

Наименование и адрес:

```
AMERICAN TELEPHONE AND TELEGRAPH          Торговое наименование:
550 Madison Ave                           AT & T
NEW YORK, NY 10022

Телефон: 212-605-5300

Номер DUNS: 00-698-0080

Вид деятельности: УСЛУГИ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИЙ (TELE)

Основной код SIC: 4811
Дополнительные коды SIC: 4821 3661 3357 3573 5999

Год основания: 1885             (31.12.86)  КОМБИНИРОВАННЫЙ ФИНАНСОВЫЙ ГОД
Всего сотрудников:   317 000    Продажи:        34 087 000 000
Сотрудников здесь:     1 800    Чистые активы:  14 462 000 000

Компания является ПУБЛИЧНОЙ
```

Финансовая отчётность за 31.12.86 (комбинированный финансовый год)

(Цифры в тысячах долларов)

Финансовые показатели

[Таблица из 15 записей — опущена]

Коэффициенты — отраслевые квартили

[Таблица из 12 записей — опущена]

Отраслевые нормы рассчитаны по 469 компаниям с активами свыше 5 млн долларов.

Финансовая отчётность за 31.12.85 (комбинированный финансовый год)

(Цифры в тысячах долларов)

Финансовые показатели

[Таблица из 15 записей — опущена]

Коэффициенты — отраслевые квартили

[Таблица из 12 записей — опущена]

Отраслевые нормы рассчитаны по 605 компаниям с активами свыше 5 млн долларов.

Финансовая отчётность за 31.12.84 (комбинированный финансовый год)

(Цифры в тысячах долларов)

Финансовые показатели

[Таблица из 15 записей — опущена]

Коэффициенты — отраслевые квартили

[Таблица из 12 записей — опущена]

Отраслевые нормы рассчитаны по 504 компаниям с активами свыше 5 млн долларов.

КОНЕЦ ДОКУМЕНТА

История компании

(Данные на 20.04.87)

Руководство:

• JAMES E. OLSON — Председатель совета директоров, Главный исполнительный директор
• ROBERT E. ALLEN — Президент, Главный операционный директор
• RANDALL L. TOBIAS — Заместитель председателя совета директоров
• CHARLES MARSHALL — Заместитель председателя совета директоров
• MORRIS TANENBAUM — Заместитель председателя совета директоров
• S. LAWRENCE PRENDERGAST — Вице-президент, Казначей
• C. PERRY COLWELL — Вице-президент, Контролёр

Члены совета директоров: Howard H. Baker Jr, James H. Evans, Peter F. Haas, Philip M. Hawley, Edward G. Jefferson, Belton K. Johnson, Juanita M. Kreps, Donald S. Perkins, Henry B. Schacht, Michael I. Sovern, Donald F. McHenry, Rawleigh Warner Jr, Joseph D. Williams и Thomas H. Wyman.

Компания зарегистрирована в штате Нью-Йорк 3 марта 1885 года.

Уставный капитал состоит из 1 200 000 000 обыкновенных акций номинальной стоимостью 1 доллар и 100 000 000 привилегированных акций номинальной стоимостью 1 доллар.

По состоянию на 28 февраля 1987 года в обращении находилось 1 071 904 000 обыкновенных акций; по состоянию на 31 декабря 1986 года привилегированные акции в обращении состояли из погашаемых привилегированных акций: 8 500 000 акций с дивидендом 3,64 долл., объявленная стоимость 50 долл.; 8 800 000 акций с дивидендом 3,74 долл., объявленная стоимость 50 долл.; 25 500 акций с дивидендом 77,50 долл., объявленная стоимость 1 000 долл.

Компания начала деятельность в 1885 году.

Обыкновенные акции компании котируются на Нью-Йоркской, Бостонской, Средне-Западной, Филадельфийской и Тихоокеанской фондовых биржах под тикером «ATT». По состоянию на 31 декабря 1986 года насчитывалось 2 782 102 держателя обыкновенных акций. По состоянию на 1 января 1986 года должностные лица и члены совета директоров в совокупности владели менее чем 1% акций в обращении, остальное принадлежало широкой публике.

Биографии руководителей:

OLSON, 1925 г.р. В 1950 году окончил Университет Северной Дакоты (BSC). Также учился в Университете Пенсильвании. 1943–1946 гг. — Военно-воздушные силы армии США. 1960–1970 гг. — Northwestern Bell Telephone Co, вице-президент — генеральный директор. 1970–1974 гг. — Indiana Bell Telephone Co, президент. 1974–1977 гг. — Illinois Bell Telephone Co, президент. С 1977 г. — AT&T; 1979 г. — заместитель председателя СД; июнь 1985 г. — президент; 1986 г. — председатель СД.

MARSHALL, 1929 г.р., женат. В 1951 году окончил Университет Иллинойса (BS); также учился в Университете Брэдли. С 1953 г. по настоящее время — AT&T: 1980 г. — помощник казначея, 1976 г. — вице-президент–казначей, 1985 г. — исполнительный вице-президент, 1986 г. — заместитель председателя СД.

TANENBAUM, 1928 г.р., женат. В 1949 году окончил Университет Джонса Хопкинса (BA, химия). В 1950 году — Принстонский университет (MA, химия). В 1952 году — PhD по физической химии. С 1952 г. по настоящее время — AT&T, различные должности; 1985 г. — исполнительный вице-президент; 1986 г. — заместитель председателя СД.

PRENDERGAST, 1941 г.р., женат. В 1963 году окончил Университет Брауна (BA). В 1969 году — Нью-Йоркский университет (MBA). 1963–1973 гг. — Western Electric Company; с 1973 г. по настоящее время — AT&T: 1980 г. — помощник казначея, 1984 г. — вице-президент–казначей.

COLWELL, 1927 г.р. Обучался в Институте технологий AT&T. 1945–1947 гг. — армия США. С 1948 г. работает в AT&T и её дочерних структурах на различных должностях. 1984 г. — вице-президент и контролёр AT&T Technologies Inc (дочерняя компания); с 1985 г. по настоящее время — вице-президент–контролёр.

ALLEN, 1935 г.р., женат. В 1957 году окончил Колледж Вабаш (BA). Занимал различные руководящие должности в бывших дочерних структурах Bell Operating и AT&T. Назначен на нынешнюю должность в 1986 году.

TOBIAS, 1943 г.р. В 1964 году окончил Университет Индианы (BS, маркетинг). Занимал различные управленческие и руководящие должности в бывших дочерних структурах Bell Operating и AT&T. Избран на нынешнюю должность в 1986 году.

Прочие должностные лица: James R. Billingsley, Sr V Pres Federal Regulation; Michael Brunner, Ex V Pres Federal Systems; Harold Burlingame, Sr V Pres Public Relations and Employee Information; Vittorio Cassoni, Sr V Pres Data Systems Division; Richard Holbrook, Sr V Pres Business Sales; Robert Kavner, Sr V Pres & CFO; Gerald Lowrie, Sr V Pres Public Affairs; John Nemecek, Ex V Pres Components &

Electronic Systems; John O'Neill, Ex V Pres National Systems Products; Alfred Partoll, Sr V Pres External Affairs; John Segall, Sr V Pres Corporate Strategy & Development; Alexander Stack, Sr V Pres Communications Systems; Paul Villiere, Ex V Pres Network Systems Marketing and Customer Operations; John Zegler, Sr V Pres and General Counsel; Lydell Christensen, Corp V Pres and Secretary.

Члены совета директоров:

• MCHENRY — исследовательский профессор, Джорджтаунский университет.
• BAKER JR — партнёр, Vinson & Elkins и Baker, Worthington, Crossley, Stansberry & Woolf, адвокаты.
• EVANS — бывший председатель Union Pacific Corporation.
• HAAS — председатель Levi Strauss & Company.
• HAWLEY — председатель Carter Hawley Hale Stores Inc.
• JEFFERSON — бывший председатель E.I. du Pont de Nemours and Company.
• JOHNSON — частный инвестор и владелец ранчо Chaparrosa.
• KREPS — бывший министр торговли США.
• PERKINS — бывший председатель Jewel Companies Inc.
• SCHACHT — председатель Cummins Engine Company Inc.
• SOVERN — президент Колумбийского университета.
• WARNER JR — бывший председатель Mobil Corporation.
• WILLIAMS — председатель Warner Lambert Company.
• WYMAN — бывший председатель CBS Inc.

В результате антимонопольного иска, предъявленного Министерством юстиции США к American Telephone and Telegraph Company (AT&T), компания в январе 1982 года согласилась на разукрупнение своих активов. В августе 1982 года Федеральный окружной суд округа Колумбия вынес согласительный декрет, обязавший AT&T провести отчуждение части операций.

Затронутые операции включали местную телефонную связь, функции доступа к местным сетям, услуги печатных справочников и услуги сотовой радиосвязи. AT&T сохранила за собой AT&T Communications Inc, AT&T Technologies Inc, Bell Telephone Laboratories Incorporated, AT&T Information Systems Inc, AT&T International Inc, а также те подразделения 22 дочерних телефонных компаний системы Bell, которые производили новое оборудование для помещений клиентов. Согласительный декрет с поправками был одобрен AT&T, Министерством юстиции США и утверждён Верховным судом США в феврале 1983 года. В декабре 1982 года AT&T представила план реорганизации, определявший порядок соблюдения требований о разукрупнении. В августе 1983 года суд утвердил этот план.

Разукрупнение, завершённое 1 января 1984 года, было осуществлено путём реорганизации 22 основных дочерних телефонных компаний системы AT&T Bell под управлением 7 новых региональных холдинговых компаний. Каждый держатель обыкновенных акций AT&T по состоянию на 10 декабря 1983 года получил по 1 акции каждой из вновь созданных корпораций на каждые 10 обыкновенных акций AT&T. Держатели сохранили также своё владение акциями AT&T.

Компания имеет долевое участие в ряде совместных предприятий:

1. Владеет 22% голосующих акций компании Ing C. Olivetti & C., S.p.A. (Милан, Италия), совместно с которой разрабатывает и продаёт продукты для автоматизации офиса в Европе.
2. Владеет 50% в совместном предприятии с голландской N. V. Philips Company, созданном для производства и сбыта систем коммутации и передачи данных в Европе и других регионах.
3. Владеет 44% в совместном предприятии с южнокорейской Goldstar Group, которое производит коммутационное оборудование и распространяет семейство компьютеров 3B в Корее.

Компания также владеет акциями других организаций. Помимо совместных предприятий, межкорпоративные отношения включали периодическое предоставление авансов со стороны компании.

Описание деятельности

(Данные на 20.04.87)

Через дочерние структуры компания предоставляет услуги дальней телефонной связи внутри штатов, между штатами и на международном уровне, а также услуги транспортировки информации. В широкую линейку голосовых и дата-услуг входят: местная и дальняя связь, широкополосные телекоммуникационные услуги (WATS), служба 800, служба 900 «Dial It» и цифровые голосовые и дата-сервисы с низкой, средней и высокой скоростью, известные под маркой Accunet Digital Services. Компания также производит телефонное оборудование и аппаратуру, телефонные провода и кабели, компьютеры для телекоммуникационных систем и общего назначения; продаёт и сдаёт в аренду телефонное оборудование; ведёт исследования и разработки в области информационных и телекоммуникационных технологий.

Деятельность компании подпадает под юрисдикцию Федеральной комиссии по связи (FCC) в части тарифов, линий, услуг и иных вопросов межштатной и международной связи.

Условия оплаты: нетто 30 дней, наличный расчёт и договоры с поэтапными платежами и окончательным расчётом по завершении работ.

Дочерняя компания AT&T Communications Inc обеспечивает дальней связью между штатами и внутри штатов 80 миллионов частных абонентов и 7 миллионов предприятий. Клиентами являются предприятия самых разных отраслей, государственные органы, физические лица и другие категории. Деятельность не носит сезонного характера.

Сотрудники: 317 000 человек, включая руководящий персонал; 1 800 человек — в данном офисе.

Объекты: Компания владеет помещениями в многоэтажном стальном здании, находящемся в хорошем состоянии. Помещения в порядке.

Местоположение: Центральный деловой район на главной улице.

Филиалы: Дочерние структуры компании эксплуатируют 19 крупных производственных предприятий, расположенных по всей территории США, общей площадью 26,2 млн кв. футов, из которых 1,49 млн кв. футов — арендованные площади. Функционируют 7 региональных центров и 24 центра дистрибуции. Кроме того, существуют многочисленные внутренние и зарубежные представительства.

Дочерние компании: По состоянию на 31 декабря 1986 года у компании имелось большое число дочерних структур, выполняющих описанные выше функции. Неконсолидированная финансовая дочерняя компания AT&T Credit Corporation обеспечивает финансирование клиентов через программы лизинга и рассрочки и выкупает у дочерних структур AT&T права на дебиторскую задолженность по долгосрочным сервисным соглашениям. Межкорпоративные отношения включают периодическое предоставление авансов материнской компанией дочерним структурам и расчёты по сервисным операциям. Список основных дочерних компаний по состоянию на 31 декабря 1986 года хранится в офисе Dun & Bradstreet в г. Миллберн, штат Нью-Джерси.

Банки-партнёры: Chemical Bank, 277 Park Ave; Marine Midland Bank, 140 Broadway; Chase Manhattan Bank, 1 Chase Manhattan Plaza.

Сводная финансовая отчётность за 31.12.86 (комбинированный финансовый год)

(Цифры в тысячах долларов)

[Таблица из 10 записей — опущена]

Коэффициенты — отраслевые квартили

[Таблица из 7 записей — опущена]

Отраслевые нормы рассчитаны по 469 компаниям с активами свыше 5 млн долларов.

End_of_File.

Отчёт Dun & Bradstreet о компании Pacific Telesis

Автор: Elric of Imrryr

Кредитное досье Pacific Telesis, получено из Dun & Bradstreet пользователем Elric of Imrryr.

Наименование и адрес

```
  PACIFIC TELESIS GROUP (INC)
  140 New Montgomery St
  SAN FRANCISCO, CA 94105

  Телефон: 415-882-8000

  Номер DUNS: 10-346-0846

  Вид деятельности: УСЛУГИ СВЯЗИ

  Основной код SIC: 4811
  Дополнительные коды SIC: 2741 5063 5732 6159

  Год основания: 1906             (31.12.86)  КОМБИНИРОВАННЫЙ ФИНАНСОВЫЙ ГОД
  Всего сотрудников:    74 937    Выручка:          8 977 300 000
  Сотрудников здесь:     2 000    Чистые активы:    7 753 300 000

  Компания является ПУБЛИЧНОЙ
```

Финансовая отчётность — 31.12.86, комбинированный финансовый год

(Показатели указаны в ТЫСЯЧАХ)

[Таблица финансовых показателей и коэффициентов за 1986 год — 469 компаний-ориентиров с активами свыше 5 млн долл. — опущена]

Финансовая отчётность — 31.12.85, комбинированный финансовый год

(Показатели указаны в ТЫСЯЧАХ)

[Таблица финансовых показателей и коэффициентов за 1985 год — 605 компаний-ориентиров с активами свыше 5 млн долл. — опущена]

Финансовая отчётность — 31.12.84, комбинированный финансовый год

(Показатели указаны в ТЫСЯЧАХ)

[Таблица финансовых показателей и коэффициентов за 1984 год — 504 компании-ориентира с активами свыше 5 млн долл. — опущена]

КОНЕЦ ДОКУМЕНТА

Наименование и адрес (повтор)

История компании

Дата справки: 01.09.87

Руководящий состав:

• DONALD E GUINN — председатель совета директоров, президент
• THEODORE J SAENGER — вице-председатель, президент группы
• SAM L GINN — вице-председатель
• JOHN E HULSE — вице-председатель, финансовый директор
• ROBERT V R DALENBERG — исполнительный вице-президент, генеральный советник, секретарь
• BENTON W DIAL — исполнительный вице-президент по управлению персоналом
• ARTHUR C LATNO JR — исполнительный вице-президент
• THOMAS G CROSS — вице-президент, казначей
• FRANK V SPILLER — вице-президент, главный бухгалтер

Совет директоров: перечисленные выше сотрудники, отмеченные знаком (+), а также Norman Barker Jr, William P Clark, William K Coblentz, Myron Du Bain, Herman E Gallegos, James R Harvey, Ivan J Houston, Leslie L Luttgens, E L Mc Neely, S Donley Ritchey, William French Smith и Mary S Metz.

Компания зарегистрирована в штате Невада 26 октября 1983 года. Уставный капитал состоит из 505 000 000 обыкновенных акций номинальной стоимостью $0,10 каждая.

Акционерный капитал в обращении: по состоянию на 31 декабря 1986 года — 215 274 878 обыкновенных акций с объявленной стоимостью $21,5 млн плюс дополнительный оплаченный капитал в размере $5 068,5 млн.

Акции свободно обращаются на Нью-Йоркской, Тихоокеанской и Среднезападной фондовых биржах. По состоянию на 1 февраля 1987 года насчитывалось 1 170 161 акционер по обыкновенным акциям. Должностные лица и директора в совокупности владеют менее чем 1% акций. Ни одна другая организация не владела более чем 5% находившихся в обращении обыкновенных акций.

В 1987 году поправкой к уставу разрешённый уставный капитал был увеличен до 1 100 000 000 акций. Помимо этого, компания объявила дробление акций в соотношении два к одному в форме выплаты дивидендов акциями в размере 100%, вступившее в силу 25 марта 1987 года.

Предыстория: Компания основана в 1906 году как корпорация штата Калифорния. Pacific Telephone & Telegraph Company образована 31 декабря 1906 года. До реорганизации контрольный пакет акций принадлежал American Telephone & Telegraph Co (AT&T), Нью-Йорк, штат Нью-Йорк.

Реорганизация (Divestiture): Согласно решению Федерального окружного суда округа Колумбия, компания AT&T выделила из состава своих 22 дочерних телефонных компаний, находившихся в

полной собственности (включая Pacific Telephone & Telegraph Company), подразделения местной телефонной связи, операторской деятельности, доступа к сети и продажи рекламы в телефонных справочниках. AT&T сохранила за собой бывшую межштатную организацию AT&T Long Lines, а также те части дочерних компаний, которые осуществляют межстанционные услуги связи и оборудование на территории клиента. Для реализации реорганизации была создана настоящая региональная холдинговая компания, принявшая на себя соответствующие операции и активы Pacific Telephone & Telegraph Company и её дочерней структуры Bell Telephone Company of Nevada. Акции образованной компании были распределены среди акционеров AT&T, сохранивших также свои акции AT&T. Реорганизация завершена 1 января 1984 года.

Последние события: В июне 1986 года компания завершила приобретение Communications Industries Inc (Даллас, штат Техас).

В декабре 1986 года полностью принадлежащая компании дочерняя структура Pac Tel Cellular Inc of Michigan подписала соглашение о покупке пяти объектов сотовой связи за $316 млн плюс ряд условных платежей. Пять указанных систем работают под брендом Cellular One. Сделка подлежит одобрению со стороны регуляторов и суда, а также окончательной правовой проверке.

Биографии руководителей

GUINN — родился в 1932 году, женат. В 1954 году получил степень бакалавра гражданского строительства в Орегонском государственном университете. 1954–1960 — работал в The Pacific Telephone & Telegraph Company, Сан-Франциско, Калифорния. 1960–1964 — вице-президент Pacific Northwest Bell Telephone Co, Сиэтл, Вашингтон. 1964–1970 — AT&T. 1970–1976 — Pacific Northwest Bell. 1976–1980 — вице-президент по сетевым услугам AT&T. 1980 — председатель и главный исполнительный директор The Pacific Telephone & Telegraph Company. 1984 — председатель, президент и главный исполнительный директор Pacific Telesis Group.

SAENGER — родился в 1928 году, женат. В 1951 году получил степень бакалавра в Калифорнийском университете. 1946–1947 — служба в армии США. 1951–1952 — секретарь и управляющий Молодёжной торговой палаты Окленда. 1950–1970 — различные должности в The Pacific Telephone & Telegraph Company. 1970–1971 — директор по операциям трафика для сетевого управления в Нью-Йорке (AT&T). 1971 — вернулся в The Pacific Telephone & Telegraph Company. 1974 — вице-президент. 1977 — президент. 1984 — вице-председатель и президент Pacific Bell в составе Pacific Telesis Group.

GINN — родился в 1937 году, женат. В 1959 году окончил Обернский университет. В 1969 году получил степень магистра в Стэнфордском университете. 1959–1960 — капитан корпуса связи армии США. 1960 — поступил в AT&T Long Lines. 1977 — вице-президент по персоналу AT&T Long Lines. 1978 — исполнительный вице-президент по сети в The Pacific Telephone & Telegraph Company. 1983 — вице-председатель. 1984 — вице-председатель и президент группы PacTel Companies в Pacific Telesis Group.

HULSE — родился в 1933 году, женат. В 1955 году получил степень бакалавра в Университете Южной Дакоты. 1956–1958 — служба в армии США. 1958 — поступил в Northwestern Bell Telephone Co. 1980 — исполнительный вице-президент и финансовый директор The Pacific Telephone & Telegraph Company. 1983 — вице-председатель. 1984 — вице-председатель и финансовый директор Pacific Telesis Group.

LATNO — родился в 1929 году, женат. Получил степень бакалавра в Университете Санта-Клары. 1952 — поступил в Pacific Telephone & Telegraph Co. 1972 — вице-президент по регуляторным вопросам. 1975 — исполнительный вице-президент по внешним связям. 1984 — исполнительный

вице-президент по внешним связям в Pacific Telesis Group.

DALENBERG — родился в 1930 году, женат. Окончил юридический факультет и высшую школу бизнеса Чикагского университета. В 1956 году допущен к адвокатской практике в штате Иллинойс, в 1973-м — в штате Калифорния. 1957–1967 — частная юридическая практика в Чикаго, Иллинойс. 1967–1972 — главный юрисконсульт Illinois Bell. 1972–1975 — главный юрисконсульт The Pacific Telephone & Telegraph Company. 1975 — заместитель генерального советника. 1976 — вице-президент, секретарь, генеральный советник. 1984 — исполнительный вице-президент и генеральный советник-секретарь Pacific Telesis Group.

CROSS — вице-президент и казначей, а также вице-президент Pacific Bell.

DIAL — родился в 1929 году, женат. В 1951 году получил степень бакалавра в Уиттиерском колледже. В 1961 году получил степень магистра в Калифорнийском государственном университете. 1951–1953 — служба в армии США. 1954 — поступил в The Pacific Telephone & Telegraph Company. 1973 — вице-президент по региональному персоналу и операционному обслуживанию Южной Калифорнии. 1976 — вице-президент по работе с клиентами в Лос-Анджелесе. 1977 — вице-президент по корпоративному планированию. 1980 — вице-президент по управлению персоналом. 1984 — исполнительный вице-президент по управлению персоналом в Pacific Telesis Group.

SPILLER — родился в 1931 году, женат. В 1953 году получил степень бакалавра в Калифорнийском университете, Сан-Франциско. 1954–1956 — служба в армии США в звании второго лейтенанта. 1953 — поступил в The Pacific Telephone & Telegraph Company. 1977 — помощник главного бухгалтера. 1981 — помощник вице-президента по финансовому управлению. 1981 — вице-президент и главный бухгалтер. 1984 — вице-президент и главный бухгалтер Pacific Telesis Group.

Прочие члены совета директоров

• **BARKER** — почётный председатель First Interstate Bank Ltd.
• **CLARK** — советник юридической фирмы Rogers & Wells.
• **COBLENTZ** — старший партнёр Coblentz, Cahen, Mc Cabe & Breyer, Attorneys, Сан-Франциско, Калифорния.
• **DU BAIN** — председатель SRI International.
• **GALLEGOS** — консультант по управлению.
• **HARVEY** — председатель и главный исполнительный директор Transamerica Corporation, Сан-Франциско, Калифорния.
• **HOUSTON** — председатель и главный исполнительный директор Golden State Mutual Life Insurance Co.
• **LUTTGENS** — общественный деятель.
• **MC NEELY** — председатель и главный исполнительный директор Oak Industries, Inc, Сан-Диего, Калифорния.
• **RITCHEY** — почётный председатель Lucky Stores Inc.
• **SMITH** — партнёр Gibson, Dunn & Crutcher, Attorneys.
• **METZ** — президент Mills College.

Операционная деятельность

Дата справки: 01.09.87

Pacific Telesis Group является региональной холдинговой компанией, ведущей деятельность через дочерние структуры.

Две крупнейшие дочерние компании — Pacific Bell и Nevada Bell — предоставляют широкий спектр услуг связи в Калифорнии и Неваде, включая местную и международную телефонную связь, доступ к сети и рекламу в телефонных справочниках; в совокупности они обеспечили свыше 90% совокупных доходов за 1986 год.

Прочие дочерние структуры (перечислены ниже) занимаются издательством справочников, сотовой мобильной связью и сопутствующими услугами, оптовой торговлей телекоммуникационным оборудованием, интегрированными системами и прочими услугами, розничной продажей средств связи и расходных материалов, финансированием продуктов аффилированных клиентов, девелопментом и консалтингом. Конкретные доли данных направлений недоступны, однако в совокупности они составляют около 10%.

Условия оплаты — нетто 30 дней. Число клиентских счетов превышает 11 000 000. Компания работает как с частными лицами, так и с коммерческими организациями. География деятельности: весь мир.

Сотрудники: 74 937, включая должностных лиц. На данном объекте занято 2 000 человек. Данные по состоянию на 31 декабря 1986 года на консолидированной основе.

Недвижимость: Компания владеет более чем 500 000 кв. футов площадей в 20-этажном здании из бетона и стали в хорошем состоянии. Помещения ухоженные.

Местоположение: Деловой центр города, боковая улица.

Филиалы: Компания располагает несколькими вспомогательными административными офисами в Сан-Франциско, однако основная часть операционных подразделений функционирует в рамках дочерних компаний — прежде всего Pacific Bell и Nevada Bell в соответствующих штатах.

Дочерние компании

Все перечисленные ниже основные операционные дочерние структуры находятся в полной собственности компании — прямой или косвенной. Телефонные дочерние структуры обеспечивают свыше 90% операционных результатов.

1. **Pacific Bell (Inc)**, Сан-Франциско, Калифорния. Образована в 1906 году как корпорация штата Калифорния. Приобретена в 1984 году в рамках реорганизации AT&T. Крупнейшая дочерняя структура компании. Предоставляет услуги связи на территории обслуживания в Калифорнии.

2. **Nevada Bell (Inc)**, Рено, Невада. Зарегистрирована в 1913 году. Выделена из состава Pacific Bell в 1984 году путём передачи акций в ходе реорганизации. Предоставляет услуги связи в штате Невада.

3. **Pac Tel Cellular Inc**, Техас. Переименованная дочерняя структура, ранее называвшаяся Communications Industries Inc. Приобретена в 1986 году. Осуществляет продвижение услуг сотовой связи и пейджинга. В свою очередь имеет ряд основных дочерних структур:
• (a) **Gen Com Incorporated** — предоставляет услуги персонального пейджинга.
• (b) **Multicom Incorporated** — реализует услуги пейджинга.

4. **Pac Tel Personal Communications** — создана для консолидации всех операций компании в области сотовой связи и пейджинга. Является головной структурой для:

• (c) **Pac Tel Cellular** — обеспечивает сотовую деятельность компании.
• (d) **Pac Tel Mobile Services** — создана для сдачи в аренду и продажи пользовательского оборудования сотовой связи и пейджинга, а также для перепродажи услуг сотовой связи; в настоящее время в основном неактивна.

5. **Pac Tel Corporation**, Сан-Франциско, Калифорния — начала работу в январе 1986 года как прямая дочерняя холдинговая структура. Владеет акциями следующих компаний:
• (e) **Pac Tel Communications Companies** — управляет двумя основными подразделениями: Pac Tel Info Systems и Pac Tel Spectrum Services.
• (f) **Pac Tel Finance** — предоставляет лизинговые финансовые услуги.
• (g) **Pac Tel Properties** — осуществляет операции с недвижимостью; стоимость активов на 31 декабря 1986 года составляла около $140 млн.
• (h) **Pac Tel Publishing** — в настоящее время неактивна.
• (i) **Pacific Telesis International** — управляет телекоммуникационным бизнесом в Великобритании, Японии, Южной Корее, Испании и Таиланде.

6. **Pac Tel Capital Resources**, Сан-Франциско, Калифорния — обеспечивает финансирование посредством размещения долговых ценных бумаг.

Внутригрупповые отношения: Включают общее руководство, внутригрупповые услуги, операции с товарно-материальными запасами и оборудованием, займы и авансы. Кроме того, долговые обязательства Pac Tel Capital Resources обеспечены соглашением о поддержке со стороны материнской компании, безусловно гарантирующей погашение долга без права регресса к акциям или активам телефонных дочерних структур или каким-либо долям участия в них.

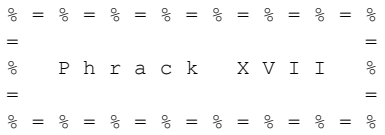
```
08-27(1Z2   /27)         29709                   052678678   H
ANALYST: Dan Quinn
```

Сводная финансовая отчётность — 31.12.86, комбинированный финансовый год

(Показатели указаны в ТЫСЯЧАХ)

[Таблица сводных финансовых показателей и коэффициентов за 1986 год — 469 компаний-ориентиров с активами свыше 5 млн долл. — опущена]

Взрывчатые вещества на основе триодида азота



Phrack Seventeen
07 April 1988

Автор: Signal Sustain

Введение

Это взрывчатое вещество — настоящий проигрышный вариант. Оно невероятно нестабильно, опасно в изготовлении, опасно в работе, и особой пользы от него тоже нет. Связка хлопушек-«кошек» стоит куда больше. По крайней мере, антлионов ими взрывать можно.

NI-3 — это, по сути, соединение, которое можно легко получить, смешав кристаллы йода и аммиак. Образующийся осадок чрезвычайно мощный и крайне нестабильный. В мокром виде он относительно стабилен (хотя доверять этому не стоит), а в сухом — абсолютно неустойчив. В сухом состоянии его способно инициировать что угодно: вибрация, ветер, солнце, муха, севшая на него. Это одно из наиболее нестабильных взрывчатых веществ, с которыми вообще приходится иметь дело.

Однако его легко сделать. Любой может зайти в магазин химических реактивов, купить бутылочку йода, а в супермаркете — чистый аммиак. Смешайте — и готово. (Подробнее об этом ниже.)

Итак, некоторые из вас всё равно попробуют это сделать, и я могу с таким же успехом поделиться советами из личного опыта. (Я убедился, что это провальная затея, попробовав самому.)

Работайте с малыми порциями

Для начала сделайте совсем небольшую пробную партию. Когда поймёте, насколько мощно это вещество, сами всё осознаете. При работе с кристаллами йода (именно кристаллами — йод является металлом, галогеном, а в твёрдом виде представляет собой кристаллы; то, что продают в аптеках как «йод», это примерно 3% йода в куче растворителей, и для данной цели не подходит) берите не более 1/4 чайной ложки, а лучше и того меньше. Четверть чайной ложки этого вещества — это один чертовски мощный взрыв; когда оно сработало у меня во дворе, дребезжали окна в радиусе целого квартала.

Поэтому, если вы прислушаетесь ко мне, используйте 1/4 ч.л. Причина в нестабильности соединения. Если вы смешаете две чайных ложки, и это рванёт в руке, прощайтесь с рукой по самое запястье. Ведро такого вещества, вероятно, снесёт любой дом. Но при 1/4 чайной ложки у вас есть шанс сохранить пальцы. Поскольку я знаю, что вы не собираетесь работать с этим дистанционными инструментами, держите количество минимальным. Вещество настолько нестабильно, что лучше перестраховаться.

Примечание: При работе с NI3 старайтесь держать его дистанционными инструментами — например, пинцетом. Но если вам всё же нужно взять его руками, прижмите большой палец к указательному и держите ёмкость только остальными пальцами. Не берите колбу обычным образом — пальцы с одной стороны, большой палец с другой. Так, если произойдёт взрыв, противопоставляемый большой палец у вас, возможно, останется — а это уже что-то.

Соединение значительно стабильнее во влажном состоянии, но определённой стабильности в нём нет. Именно поэтому производители взрывчатых веществ им не пользуются: даже небольшая вероятность случайного взрыва слишком опасна. (Они и так периодически теряют заводы по производству динамита — вот почему те полностью автоматизированы.) Но когда это вещество высыхает — берегитесь. Хайнлайн говорит: «Достаточно сурово взглянуть, и оно сработает», — и он не шутит. Ветер, вибрация, дыхание рядом — что угодно его инициирует. (Кстати, процесс из фантастического романа Хайнлайна «Свободное владение Фарнхэм» тоже не работает — жидкий йод для этого не годится. Необходимы именно кристаллы.)

Не храните его

Особую опасность представляет попытка хранить это вещество. Допустим, вы поместили его в стакан. Через день вокруг края жидкости образуется корка, которая высыхает. Вы берёте стакан — бабах! — корка срабатывает, а жидкость взлетает от удара. Ваши пальцы приземляются на газоне соседа. Если вы это делаете, принимайте все меры, чтобы вещество оставалось влажным. Как минимум закупорьте пробирку, чтобы не допустить испарения.

Приготовление

Всё ещё хотите попробовать? Ладно. Купите кристаллы йода в магазине химических реактивов. Если спросят зачем — скажите, что нужно очищать воду в походе; вас, конечно, поучат насчёт более удобных альтернатив (галазон), но кристаллы всё равно продадут. Или скажите честно, что вас попросили сыграть роль «мистера Волшебника», — скорее всего, тоже дадут. Хранение йода не является незаконным.

Покупайте как можно меньше. Вам нужно немного, а после одного эксперимента вещество становится бесполезным. Ориентируйтесь на 1/4 чайной ложки.

Во-вторых, купите в магазине ПРОЗРАЧНЫЙ аммиак БЕЗ МЫЛЬНЫХ ДОБАВОК — например, для бытовой уборки (НО БЕЗ ПЕНЫ! Она всё портит, NI-3 не получится).

В-третьих, налейте аммиак в миску. Фу! Приятный запах.

В-четвёртых, добавьте 1/4 ч.л. или меньше кристаллов йода. Учтите: эти кристаллы, похожие на растворимый кофе, разрушают металлы, поэтому поберегите столовые приборы. По возможности используйте пластиковую посуду (миску, ложку). Кристаллы также оставляют долговременные пятна йода на руках, а это весьма компрометирует, если произошёл взрыв NI-3 и ищут виновных. Пожалуйста, надевайте резиновые перчатки и выбрасывайте их после использования.

Кристаллы немного рассредоточатся. При необходимости слегка перемешайте. Будьте крайне осторожны: не оставляйте раствор на ложке, где он может высохнуть. Поверьте, сработает. (Проверено на собственном опыте.)

Дайте кристаллам разойтись и пошипеть — они это сделают. Затем, примерно через час, на дне прозрачного аммиака останется красновато-коричневая липкая масса. Вязкая, как грязь, трудно поддаётся работе. Это и есть NI-3.

Пока она влажная — относительно безопасна. (НЕ ДОПУСКАЙТЕ ОБРАЗОВАНИЯ КОРКИ ПО КРАЮ ЖИДКОСТИ!)

Применение

Теперь давайте сразу же используем эту дрянь и НЕ пытайтесь её хранить.

Вынесите её на улицу в безопасное место. В моей школе кто-то однажды рассыпал совсем крошечные кусочки (буквально отдельные кристаллики) в коридоре. Эффект хороший — словно подкладываешь пистон под чужой башмак, когда вещество высыхает. Для этого тоже нужно намного меньше 1/4 ч.л.

Рассыпьте на солнце и дайте высохнуть. НЕ ТРОГАЙТЕ. Если вдруг услышите резкий ЩЕЛЧОК — это значит, ветра оказалось достаточно, чтобы инициировать взрыв, или оно сработало само по себе. Такое тоже бывает.

Вещество должно полностью высохнуть, чтобы достичь максимальной нестабильности, при которой срабатывает от сурового взгляда. Разумеется, верхние кристаллы высыхают первыми — будьте начеку. Любой резкий удар инициирует взрыв, мокрое вещество или сухое.

Пока ждёте высыхания, СОЖГИТЕ пластиковую посуду, в которой всё делали. В процессе горения услышите лёгкие потрескивания — это подсыхающий остаток раствора срабатывает в пламени.

Часа через два бросайте в NI-3 камни с дальнего расстояния, и увидите взрывы. После каждого — фиолетовый дым. Звук резкий, как удар хлыста, не перепутаете.

В общем. Как я и говорил, большинство людей делают это, потому что компоненты легкодоступны. Сделают, потом думают: и что с этим делать? — и рассыпают крохотные кристаллики в коридоре. Бах-бах-бах. И больше никогда не делают, потому что пальцы на руке даются один раз, и большинство хочет их сохранить.

Или помещают NI-3 ещё в «жидкой» форме в дверные замки и ждут, пока высохнет. Следующий, кто вставит ключ, получит большой сюрприз.

(Именно поэтому большинство учителей химии в школах держат кристаллы йода под замком.)

Как избавиться от NI-3

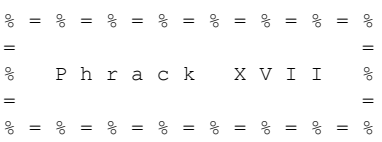
Если смыть кристаллы NI-3 в кухонную раковину, останется только ждать, пока они высохнут и сработают. Они прилипнут к трубам (это свойство галогенов). Я слышал, как трубы трещали и щёлкали несколько дней после того, как кто-то так сделал. Рекомендую выбросить всю массу на пустырь и постараться инициировать взрыв, чтобы никто другой случайно не пострадал.

Если решитесь — удачи, и имейте в виду: вы были предупреждены.

-- Signal Sustain

Как взломать CDC Cyber

Автор: Grey Sorcerer



Phrack Seventeen
07 April 1988

File 5 of 12 : How to Hack Cyber Systems

Содержание

Я пропущу всё то, что есть в ваших справочных руководствах CDC — что такое локальный файл и всё в таком духе. Если вы уже готовы взламывать систему, вы это и так знаете; если нет — сначала разберитесь с основами, иначе многое из написанного ниже будет непонятно. По-моему, слишком много файлов «как взломать» — это просто короткие пересказы пользовательских руководств (которые вам в любом случае стоит достать при серьёзной попытке проникновения, иначе пропустите массу возможностей), без каких-либо реальных советов по взлому системы.

---

1. Общие советы по взлому

Не попадайтесь. Используйте удалённые дозвоны, если это возможно, и никогда, никогда не пользуйтесь номером пользователя, который можно связать с вами. Никогда не используйте один и тот же номер пользователя дважды. Помните: на типичном сайте Cyber — миллион номеров пользователей, и за каждым не уследишь. Растворитесь в толпе. И как только обстановка накаляется — залягте на дно.

Магнитные ленты — великолепная вещь. Они вмещают около 60 Мб, а с новыми накопителями — и того больше. Здесь можно спрятать много всего в офлайне, например дампы системы для изучения. Купите несколько качественных лент — мне больше всего нравятся Black Watch, которые

продаёт мой сайт, — запишите на первые несколько записей что-нибудь невинное: данные, учебную программу или что угодно, а потом уже прячьте ценное. Так вы пройдёте поверхностную проверку. Помните: обычный сайт хранит ТЫСЯЧИ лент, и проверять каждую у них нет ни времени, ни сил.

Одна вещь насчёт Cyber — они ведут журнал аудита, называемый «port log», для всех обращений к PPU и CPU. Обычно его никто не смотрит. Но помните: ***всё***, что вы делаете, записывается — если у кого-то хватит ума и упорства (в конечном счёте исходящих от вас) это найти. Поэтому не делайте глупостей вроде: поработал под своим номером, вышел, тут же вошёл под другим и сдампил систему. Они УЗНАЮТ.

Не оставляйте следов.

Запомните также первое правило хвастовства: ваши друзья вас сдадут.

И второе: если все узнают трюк с повышением приоритета, вы все снова окажетесь на одном уровне, не так ли? А если вы покажете это всего двум друзьям, считайте: они покажут ещё двум, те — ещё четырём...

Так что наслаждайтесь шуткой сами и держите её при себе.

---

2. Развлечения с карточным перфоратором

Да, как ни невероятно, сайты CDC всё ещё используют перфокарты. Это вполне соответствует общему подходу CDC к жизни: «На дворе 1960-е».

Первое, что стоит сделать, — вытряхнуть из лотка перфоратора все маленькие кружочки-пробивки и в какой-нибудь шумный вечер бросить их кому-нибудь в волосы. Гарантирую: эти маленькие гады застрянут там на полгода — вытащить их невозможно. Статическое электричество или что-то в этом роде заставляет их держаться, как вши. Даже душ не помогает.

Следующее — понаблюдайте, как ваша местная установка обращается с колодами перфокарт. Обычно это выглядит так. Операторам нравятся задания на перфокартах, потому что их можно поставить в очередь с ультранизким приоритетом, заставив бедолаг-пользователей ждать, пока операторы гоняют своего «сборщика плакатов» или Star Trek с высоким приоритетом. Так что обычно вы засовываете колоду в ридер, идёте в комнату для распечаток, и через вечность получаете свой листинг.

Кроме того, сразу много людей одновременно суют свои колоды в карт-ридер.

Если есть возможность, пробейте карту со сплошными отверстиями — все позиции пробиты. Это, как известно, может повесить PPU карт-ридера и уронить систему. Ха-ха. К тому же это почти наверняка заклинит ридер. Если хотите посмотреть, как оператор лёжа на спине пытается пинцетом вытащить кусочки карты из ридера — вот ваш шанс.

Далее, структура задания на карточной колоде открывает массу возможностей для веселья. Обычно она выглядит так:

```
   JOB card:  имя задания (первые 4 символа)
   User Card: номер пользователя и пароль -- зависит от сайта
EOR card: пробиты 7-8-9
   Ваше пакетное задание (например, скомпилировать эту программу на Fortran): FTN.
   LGO. (означает: запустить скомпилированную программу)
EOR card: пробиты 7-8-9
   Исходный код программы на Fortran
EOR card: пробиты 7-8-9
   Данные для вашей программы на Fortran
EOF card: пробиты 6-7-8-9. Означает: конец колоды.
```

Это абсолютно типично для начального курса Fortran.

На обычном мэйнфрейм-сайте колоды накапливаются в лотке у стола оператора. Потом, когда у него дойдут руки, оператор карт-ридера берёт штук пятьдесят колод, складывает их все подряд и прогоняет через ридер. Затем кладёт их обратно в лоток и возвращается к своему Penthouse.

---

3. Как легко получить новый номер пользователя

Попробуйте вот что для смеха — сделайте своё пакетное задание таким:

```
JOB card:  имя задания (первые 4 символа)
User Card: номер пользователя и пароль -- зависит от сайта
EOR card:  пробиты 7-8-9
COPYEI INPUT,filename:  копирует всё после метки EOR в файл filename этого аккаунта
EOR Card:  пробиты 7-8-9.
```

Только НЕ кладите карту EOF в конец своего задания.

Большой сюрприз для следующего в очереди: его целая колода перфокарт — вместе, разумеется, с его номером пользователя и паролем — будет скопирована в ваш аккаунт. Это происходит потому, что последняя карта ВАШЕЙ колоды — это конец записи, который сигнализирует: дальше идут данные программы, а «данными» и является колода следующего человека — вплоть до его EOF-карты. COPYEI при этом позаботится о том, чтобы пропустить надоедливые метки записей.

Думаю, дальше вы и сами догадаетесь — несложно.

---

4. Взлом через Telex и пакетная архитектура CDC

Когда CDC добавляла разделение времени к машинам Cyber, изначально спроектированным под пакетную обработку перфокарт, она создала два типа доступа: Batch и Telex. Batch — это, как правило, колода перфокарт, которая запускается тогда, когда оператор соизволит. Внутри системы она получает ультранизкий приоритет и выполняется урывками. Это «пачка» задач с началом и концом.

Telex — другое дело. Это система разделения времени, поддерживающая до, скажем, 60 терминалов. Зависит от системы: чем больше RAM, чем больше области свопинга (если повезло с этим), тем больше терминалов можно поддерживать, прежде чем вся система начнёт ползти улиткой.

Telex реализован как странный «пакетный» файл, в котором система не знает ни сколько ей придётся сделать, ни где это закончится, — и просто выполняет команды по мере их ввода. Настоящий костыль.

Поскольку люди за CRT ожидают хоть какой-то реакции, им дают более высокий приоритет. Это приводит к «Telex thrashing» на сильно загруженных системах CDC: только пользователи Telex успевают хоть что-то сделать, и они сидят и дерутся за ресурсы машины.

Бедолаги с колодами перфокарт никогда не пробиваются в машину, потому что все приоритеты и CPU захвачены пользователями Telex. (Поэтому НЕ используйте перфокарты.)

Ещё один хороший совет: если вы ВЫНУЖДЕНЫ использовать перфокарты, наберите свою программу на CRT и сбросьте её на автоматический перфоратор. Это куда удобнее, чем

исправлять опечатки на картах...

Работая в Telex, вы являетесь частью одного из нескольких «заданий» внутри системы. Как правило, там есть «TELEX», что-то для управления построчным принтером, что-то для управления карт-ридером, драйверы магнитных лент (называемые «MAGNET») и, может быть, ещё несколько. В Cyber ограниченное пространство — ни за что не поверите: 128K 60-битных слов, — поэтому ограничено и число заданий, которые туда влезают. CDC вложила все силы в «планировщик заданий», чтобы выжать максимум из того, что было.

Вы можете выполнить команду статуса, чтобы увидеть все запущенные задания — это познавательно.

Так вот, машины CDC изначально проектировались для выполнения карточных заданий с большим объёмом работы с магнитными лентами — например, для IRS. Поэтому там никто не задумывался о том, что задание может «прерваться» — как при нажатии BREAK на CRT, — потому что карточные задания не могут. Это открывает прекрасные возможности.

Например:

---

5. Как получить копию всей системы

К примеру. Перейдите в режим BATCH из Telex и запустите компиляцию Fortran. Пока она идёт, нажмите BREAK. Вы получите запрос подтверждения «Continue?». Скажите нет, вы хотите остановиться.

Теперь посмотрите список своих локальных файлов. Ой-ой, там появился новый БОЛЬШОЙ файл. На самом деле это копия ВСЕЙ системы, на которой вы работаете: PPU-код, CPU-код, ВСЕ компиляторы, всё-всё! Изучите этот локальный файл — вы найдёте там все потроха, приятель, готовые к изучению.

Конечно, вы же уже настроились сбросить это на ленту или диск в удобное время?

Это работает потому, что люди в CDC никогда не думали, что компиляцию Fortran можно прервать, — они полагали, что она всегда будет запускаться с карт. Поэтому они оставляли системные файлы локальными для задания до конца компиляции. Прервите компиляцию — и они останутся локальными.

Предупреждение: когда вы делаете ЧТО УГОДНО, копия вашего текущего пакетного процесса появляется на консоли оператора. Обычно операторы читают Penthouse и им всё равно, к тому же изображение мелькает так быстро, что его трудно разглядеть. Но если вы копируете всю систему, это занимает какое-то время, и они получают подробный отчёт о том, что копируется. («Эй, почему этот %^&$^ на терминале 29 копирует PPU-код?») Меня однажды так накрыли; я прикинулся шлангом, и они меня отпустили. («Я думал, это файл данных моей программы».)

---

6. Оставаться «загруженным» с помощью BREAK

Когда люди в CDC проектировали планировщик заданий, они создали несколько «очередей».

Вот они:

1. **Входная очередь (Input Queue).** Ваше задание ещё даже не попало внутрь. Оно стоит снаружи, на диске, в ожидании.

2. **Очередь выполнения (Executing Queue).** Ваше задание сейчас находится в памяти и выполняется, хотя другие задания в памяти тоже конкурируют за машину. По крайней мере вы уже в памяти.
3. **Очередь выгрузки по времени/событию (Timed/Event Rollout Queue).** Ваше задание ждёт чего-то — обычно магнитной ленты. Может также ждать наступления определённого времени. Да, это означает, что можно поставить в систему задание с отложенным эффектом. Ха-ха. В данный момент вы на диске.
4. **Очередь выгрузки (Rollout Queue).** Ваше задание ждёт своей очереди на выполнение. Сейчас вы простаиваете на диске.

Итак, допустим, у вас большая компиляция на Pascal. Во-первых, ВСЕГДА РАБОТАЙТЕ ИЗ TELEX (то есть с CRT). Никогда не используйте карты. С картами вы автоматически окажетесь в хвосте приоритетной очереди, потому что CPU не обязан возвращаться к вам быстро. У кого из нас есть время терять?

Итак, запустите компиляцию. Затем с другой машины выполните STATUS своего задания. Обычно вас оставляют внутри CPU (EXECUTE) на 10 секунд, за которые вы делите реальный CPU примерно с 10–16 другими заданиями. Потом вас выгружают (ROLLOUT) — и вы попали; нужно ждать, пока ваш приоритет снова не вырастет достаточно, чтобы продолжить выполнение задания. На сильно загруженной системе это может занять несколько минут.

(Все задания имеют заданный уровень приоритета, который обычно растёт каждые 10 секунд или около того, пока они не начнут выполняться.)

Итак, сделайте вот что. Нажмите BREAK, а на запрос «Continue?» ответьте да. Что произошло? Telex был вынужден «загрузить ваше задание» для обработки BREAK! Таким образом вы получаете ещё 10 бесплатных секунд CPU — за которые можно сделать немало.

Если нажимать BREAK — Y каждые 10 секунд во время по-настоящему большого задания, оно выполнится как на крыльях. Все остальные, конечно, будут сидеть и пялиться в свои экраны, ничего не делая, потому что компьютер занят вами.

Если вы учитесь в университете, где стоит Cyber, — вот как сдавать домашние задания на высокой скорости.

---

7. Библиотека макросов

На типичном сайте CDC вам не дадут доступа к «библиотеке макросов». Это набор вызовов CPU для выполнения различных операций: открытие файлов, команды каталога и тому подобное. Они будут слишком напуганы «каким-то хакером». Реальность такова: тупоголовые у власти не хотят ни с кем делиться НИКАКОЙ властью. С библиотекой макросов, дающей доступ к ассемблеру, вы не можете сделать намного больше, чем с пакетными командами... за исключением того, что следов остаётся куда меньше. Им придётся ОЧЕНЬ постараться, чтобы найти, что делала ваша программа, если вы используете вызовы макросов: нужно лезть в PPU port logs — это поиск иголки в стоге сена, в отличие от логов пакетных файлов, которые читаются сразу.

Не переживайте. Найдите кого-нибудь в Arizona State или Minnesota U., кто не откажет, и попросите прислать ленту с библиотеками. Получите столько кода, сколько захотите смотреть. Кстати, там есть отличная лента с плакатами — просто распечатайте их на построчном принтере. Печатается долго, но оно того стоит. (Там есть все классические: человек на луне, разные плейметы, Спок и т.д. Некоторые шириной в 7 листов!)

С библиотекой макросов можно делать много крутых вещей.

Лучшее — это демон-сканер. У всех номеров пользователей CDC есть управление доступом к отдельным файлам для других пользователей: приватный (никакого доступа для других), полуприватный (другие могут читать, но создаётся запись) или публичный (кто угодно может работать с вашими файлами, без записи). Вам нужна программа (несложная на Fortran), которая перебирает номера пользователей, выполняя команды каталога. Если что-то находит — проверяет, что это не полуприватное (чтобы не создавалась запись), и копирует к себе.

Найдёте самые невероятные вещи, гарантирую. Попробуйте понаблюдать, как какой-нибудь системщик входит в систему, подсмотреть цифры его номера пользователя, а потом просканировать вариации, начинающиеся с этого номера. Например, если он SYS1234 — просканируйте все номера, начинающиеся с SYS (от sysaaaa до sys9999).

Поскольку всё это внутри программы на Fortran, единственная запись — кроме труднопросматриваемых PPU-логов — это «Запустить программу Fortran» («LGO.») в пакетном дейфайле. Если вы не даёте перегруженным системщикам повода подозревать, что обычная студенческая компиляция на Fortran — это что-то из ряда вон, они никогда не будут проверять: объём данных в PPU-логах ОГРОМЕН.

Зато добычу можно взять отличную.

Есть целая крутая библиотека вызываемых из Fortran процедур, делающих почти всё, что угодно делать пакетной командой, — в Minnesota library. Пора заводить друзей в Миннесоте — например, через UseNet. Они охотно рассылают ленты.

Как правило, находятся старые файлы, которые какой-нибудь системщик однажды открыл в публичный доступ (чтобы приятель мог скопировать), а потом забыл. Я вот так набрал всякого разного. Прелесть в том, что я просто объяснял: мои программы на Fortran зависли в бесконечных циклах — это объясняло многосекундное время выполнения CPU. Поскольку никакой доступной записи о том, чем я занимался, не было, мне верили. К тому же, сколько пользователей-идиотов и правда застревают в циклах? Много. Растворяйтесь в толпе. Так я достал Chess 4.2 — чемпионскую шахматную программу — и много чего ещё. Например, всю библиотеку игр, закрытую для обычных пользователей, но не для системщиков.

Ещё раз: они *могут* вас отследить, если вы ведёте себя назойливо (будет довольно очевидно, что вы делаете, если в вашем PPU port log обнаружится `CAT: SYSAAAA`, `CAT: SYSAAAB`, `CAT: SYSAAAC` и т.д.) — поэтому делайте это под чужим номером пользователя.

---

8. Проверки статуса RJE

Многие тупоголовые установки CDC — впрочем, это не сужает круг — имеют станции удалённого ввода заданий (RJE). Как правило, в университетах их поручают какому-нибудь бедному студенту за гроши.

Что забавно: эти RJE могут запрашивать статус заданий в системе, и система при этом встаёт как вкопанная — запрос получает наивысший приоритет.

Так что если хотите немного разжечь возмущение, просто сидите у своего RJE и делайте запросы статуса снова и снова. Система будет ещё медленнее обычного.

---

9. Червь

Предупреждение: это довольно радикально. Это выходит за рамки простой самозащиты ради получения нужного приоритета для домашних заданий или невинного исследования системы — здесь речь идёт о том, чтобы уронить всю машину.

И это работает.

Вы можете отправлять пакетные задания в систему так же, как если бы прогоняли их через карт-ридер, — с помощью команды SUBMIT. Вы создаёте файл данных, затем выполняете `SUBMIT datafile`. Оно работает отдельно от вас.

Итак, создадим файл данных с именем WORM. Это пакетный файл. Он выглядит так:

```
JOB
USER,blah (что угодно -- номер пользователя, который вы хотите уничтожить)
GET,WORM; получить копию WORM
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
SUBMIT,WORM.; отправить в систему
  (16 раз)
(конец файла)
```

Теперь вы выполняете `SUBMIT WORM`. Что происходит? Worm создаёт 16 копий себя и отправляет их. Те, в свою очередь, создают 16 копий каждая (итого уже 256) и отправляют их. Следующий проход — 4096. Потом 65536. Потом...

Если вы настоящий профессионал, укажите в своей «карточке задания» запрос высокого приоритета. Как? Сообщите системе, что вам нужно очень мало памяти и очень мало времени CPU (что правда — SUBMIT почти ничего не требует). Планировщик «втискивает» маленькие задания между всеми большими, которые все любят гонять, и даёт ультраприоритет по-настоящему крошечным заданиям.

В итоге система отправляет себя в смерть. Рано или поздно входная очередь переполняется — места ограничены — и система рассыпается.

Это особенно жестокая вещь для системы, потому что если парень за консолью (а он обязательно будет) попытается обычный запуск, в входной очереди останутся копии WORM. Первая из них вырвется на волю — и система падает снова. При удаче система будет падать и подниматься несколько часов, пока какой-нибудь достаточно сообразительный человек не доберётся до консоли оператора и не выполнит холодный старт.

Если у вас целый зал с компьютерными занудами — все с резинками в хвостиках, усердно гоняющие компиляции на Pascal и C, — ждёт хорошее зрелище. Только что принтеры печатали — слышалось «вжик-вжик» по бумаге. Следующую секунду, после вашего запуска, они замолкнут. И будут стоять молча. Если всё сделано правильно, никто не сможет даже получить статус. Ха, ха.

Чем быстрее CPU, тем быстрее он загонит себя в могилу.

CDC утверждает, что существует ограничение на количество заданий, которые один номер пользователя может иметь в системе. Как обычно, они всё испортили, и этого ограничения не существует. Да и всё равно систему убивает переполнение входной очереди, а до неё можно

добраться в обход проверки числа заданий.

Имейте в виду: ***всё***, что находится в этом пакетном файле, будет повторено десятки тысяч раз на консоли оператора, пока маленькие задания несутся мимо тысячами. Поэтому не забудьте добавить приятные сообщения, например:

```
job,blah
user,blah
* eat me!
get,worm
submit,worm .. и т.д.
```

Теперь тысячи маленьких «eat me!» будут прокручиваться по консоли так быстро, как успевает печатать консольный PPU.

Как правило, в этот момент у оператора кровяное давление вышибет уши.

Будьте уверены: они перевернут небо и землю, чтобы найти вас. Это включает прошлые дейфайлы, логи пользователей и всё прочее. Так что будьте чисты. Помните: «Месть — блюдо, которое подают холодным». Если вы на них злитесь, и они это знают, подождите годик-другой, пока они не начнут чесать головы, недоумевая, кто же ненавидит их настолько.

И ещё: убедитесь, что не роняете что-то действительно важное, что делает кто-то другой, ладно? Например, никаких медицинских баз данных.

Теперь, для по-настоящему изящного прикосновения, отправьте задание с отложенным запуском по времени/событию (timed/event job). Оно «блокирует» задание на некоторое время, до наступления указанного момента. Потом, когда вы будете далеко-далеко, с отличным алиби, задание запустится, система рассыплется, а вы чисты. Если выполнить выгрузку по времени/событию через вызов макроса из программы на Fortran, это даже не попадёт в лог.

(Помните, что системщики в конечном счёте поймут, что вы сделали — в своих маленьких умах. Хотя на это у них может уйти год-другой.)

---

10. Метод Checkpoint/Restart для повышения привилегий

Лучшее — напоследок.

Программисты CDC создали две утилиты — CheckPoint и Restart — главным образом потому, что их компьютеры то и дело падали, не успев ничего доделать. CheckPoint делает ПОЛНУЮ копию того, над чем вы работаете: все локальные файлы, всю память и т.д. — в файл, обычно на магнитную ленту. Затем Restart «перезапускает» с этой точки.

Так что при запуске 12-часового вычислительного задания вы расставляете контрольные точки по ходу дела, и если CDC падает, можно перезапуститься с последнего CKP. Это как резервная копия жёсткого диска на ленте. Таким образом теряются только данные, обработанные между последней контрольной точкой и моментом сбоя, а не все 12 часов. Это действительно важно для заданий, занимающих несколько дней — спросите в вашем местном отделении IRS за подробностями.

Так вот, что чертовски смешно: если внимательно посмотреть на файл, который генерирует Checkpoint, вы обнаружите там копию ваших пользовательских проверок — данных, которые рассказывают системе всё о вас, — вместе с пользовательскими файлами, памятью и т.д. Придётся немного покопаться в шестнадцатеричном представлении, чтобы найти нужные числа, но они прекрасно совпадут с тем, что отображает команда просмотра ваших пользовательских проверок.

Итак, выполните `CKP` — это создаст CKP-файл. Затем напишите небольшую программу на FORTRAN, которая отредактирует проверки внутри этого файла. Затем выполните RESTART из него. Поздравляю. Вы сделали себя сами. Можете делать всё, что хотите: установить свой уровень приоритета на максимум, захватить построчный принтер как личный, выкинуть другие задания из системы (элегантнее установить их приоритет в ноль, чтобы они никогда не выполнялись) и так далее. Вы — оператор.

Вот теперь действительно стоит быть мастером CDC и знать всевозможные тёмные, коварные вещи. Я бы держал под рукой список номеров пользователей с файлами, которые хочется сделать публичными, чтобы пойти и зазапить их (superzap), а потом изучать с других входов.

Здесь есть некоторые подводные камни — например, CKP нужно запускать как часть пакетного файла из Telex. Но теперь, зная, что люди в CDC сделали так, что RESTART меняет ваши пользовательские проверки, вы найдёте способ обойти их.

В каком-то смысле это логично. Если вы пытаетесь перезапустить задание, вам нужны тот же приоритет, та же память и тот же доступ, что были при первом запуске.

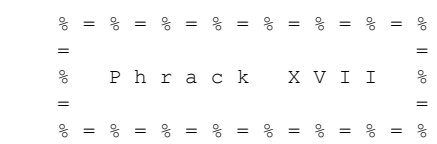
Заключение

Вот они — секреты взлома Cyber.

Они собраны за несколько лет в университете с одной машиной CDC, которую я обозначу лишь как расположенную где-то на востоке. Когда я уходил, всё это работало; возможно, CDC закрыла часть дыр, но сомневаюсь. Они не очень быстры в обновлении операционной системы.

** Grey Sorcerer

Как взломать HP 2000



Phrack Seventeen
07 April 1988

File 6 of 12 : How to Hack HP2000's

Автор: Grey Sorcerer

Итак, вы уже прочли базовые руководства по HP-2000 и ориентируетесь в системе. Повторять всё это я не стану.

Я обнаружил два-три приёма, которые позволяют обходить защиту HP 2000.

1. Прерывание HELLO-программы

При входе в систему на номере пользователя Z999 запускается файл HELLO. Зачастую именно он используется для отказа в доступе. Хотите войти? Это всего лишь программа на BASIC, и её можно прервать через BREAK — однако, как правило, первым делом она отключает прерывания функцией BRK(0). Тем не менее, если войти вот так:

```
HELLO-D345,PASS (return) (break)
```

И нажать Break почти сразу после Return, в большинстве случаев HELLO-программа прервётся, и вы окажетесь внутри свободно.

Если удастся создать «плохой файл» — а это требует определённых усилий — то при любой попытке выполнить CSAVE этого файла (компиляция и сохранение) система мгновенно уйдёт в жёсткий сбой.

Самая опасная дыра в защите HP 2000 — метод «двух терминалов». Чтобы понять принцип его работы, нужно разобраться с буферами. Когда вы открываете файл командой OPEN или ASSIGN (это одно и то же), система считывает первые 256 байт файла. Когда нужно больше — подгружается следующие 256 байт. Данные поступают с диска порциями фиксированного размера и хранятся в «буферах».

Итак. Запишите на диск кучу мусора — программы, данные, всё что угодно. Когда номер пользователя заполнится, удалите всё это. Эффект: сырые перемешанные данные остаются на диске.

Выберите момент, когда система максимально загружена, и действуйте:

Шаг 1. На терминале №1 запустите программу, которая в цикле как можно быстрее проверяет наличие файла через оператор ASSIGN. Как только файл обнаружен, программа переходит в самый конец файла и читает его в обратном направлении, запись за записью, в поисках данных. Найдя данные, она сообщает об этом и останавливается на приглашении ввода. Программа работает.

Шаг 2. На терминале №2 создайте очень большой файл с данными: `OPEN-FILE, 3000` или аналогичной командой.

Происходит следующее: команда терминала №2 начинает обнулять секторы файла, начиная с его начала. Но она успевает пройти лишь часть пути, прежде чем процессор требуется другой задаче — и терминал №2 вытесняется. Обнуление на мгновение прекращается. В это время терминал №1 получает управление, обнаруживает файл и читает до его конца. Что там находится? Старый мусор с диска. (Который, кстати, может оказаться крайне интересным — знаете ли вы, что HP использует специальный маркер для обозначения конца буфера? Вы, вполне возможно, только что получили буфер, глубина которого равна объёму системной памяти, и если проявить смекалку, можно читать или записывать данные в любое место памяти. Если такое получилось — сохраните это: на вес золота.)

Но вернёмся к делу.

Шаг 3. Терминал №2 завершает OPEN. Теперь он удаляет файл. В результате у терминала №1 остаётся буфер, полный данных, готовых к записи обратно на диск — в то место, где этот файл располагался раньше.

Шаг 4. Терминал №2 сохраняет набор программных файлов — столько, сколько нужно, чтобы заполнить область, освобождённую удалённым большим файлом.

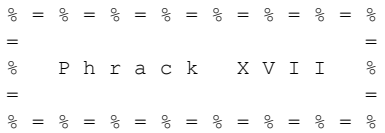
Шаг 5. Вы отпускаете терминал №1 с приглашения ввода, и он записывает свой буфер на диск. Это немедленно перезаписывает одну из только что сохранённых программ. Результат: «плохая программа». HP хранит программы в токенизированном виде с проверкой синтаксиса; «плохая программа» — это та, у которой нарушена структура токенов. Поскольку HP считает: раз программа есть на диске, значит, она прошла синтаксическую проверку и заведомо корректна — система попадает в серьёзную ловушку. Для быстрого эффекта просто выполните CSAVE: система попытается полускомпилировать испорченный код и рухнет.

Что делать дальше

На самом деле, куда более изящное применение всего этого — использовать «бездонный буфер» для изучения системы и изменения того, что вам не нравится. Например, пароль к A000? Напишите немного кода на HP, осмотрите память, получайте удовольствие. Это осуществимо.

Grey Sorcerer

Доступ к государственным компьютерам



Phrack Seventeen
07 April 1988

(ЛЕГАЛЬНО!)

Автор: The Sorceress (The Far Side 415/471-1138)

Комментарий: Я наткнулась на эту статью в журнале Computer Shopper (сентябрь 1987 года), где говорилось о том, что граждане имеют право на доступ к государственным компьютерам, поскольку оплачивают их из своих налогов. С тех пор я сама неоднократно побывала на этих системах вместе с друзьями, и базы данных оказались переполнены доступной информацией. Одно предупреждение: как правило, для получения доступа необходимо позвонить сисопу, назвать своё настоящее имя, адрес и прочие данные. Они перезванивают и проверяют вашу личность. И ещё одно предостережение: вывод BBS из строя является уголовным преступлением, поэтому с этими системами лучше не шутить — они принадлежат государству.

Национальное бюро стандартов

Электронный информационный обмен для микрокомпьютеров

Sysop: Ted Landberg & Lisa Carnahan
Голос: 301-975-3359
Данные: 301-948-5717 — 300/1200/2400 бод

Эта BBS работает под управлением Института компьютерных наук и технологий, входящего в состав одной из четырёх технических организаций Национального бюро стандартов. На борде также размещена информация о приобретении, управлении, безопасности и использовании микрокомпьютеров.

Бюро переписи населения

Центр микрокомпьютеров и офисных технологий, комн. 1065 FB-3, Вашингтон, округ Колумбия (Сьютланд, штат Мэриленд)

Sysop: Nevins Frankel
Голос: 301-763-4494
Данные: 301-763-4576 — 300/1200 бод

Цель этой BBS — предоставить пользователям доступ к следующему: бюллетени и каталоги центра микрокомпьютеров и офисных технологий Бюро переписи, оценки программного и аппаратного обеспечения, инвентаризация аппаратного и программного обеспечения, библиотека компьютерного клуба Бюро переписи, программное обеспечение в открытом доступе и т.д.

Бюро переписи населения

Центр микрокомпьютеров и офисных технологий, отдел кадров, Вашингтон, округ Колумбия

Голос: 301-763-4494
Данные: 301-763-4574 — 300/1200/2400 бод

Эта BBS предназначена для отображения вакансий Бюро переписи — от начального уровня до высшего руководства.

Министерство торговли

Управление заместителя министра по экономическим вопросам, Управление экономического анализа, Экономический информационный стенд

Sysop: Ken Rogers
Голос: 202-377-0433
Данные: 202-377-3870 — 300/1200 бод

Ещё одна хорошо организованная BBS с подробными новостями об агентствах по экономическим вопросам Министерства торговли, включая актуальные пресс-релизы и аннотации докладов.

COE BBS

Управление кадров и силовых структур, штаб-квартира Инженерного корпуса армии США, 20 Massachusetts Ave. NW, Вашингтон, округ Колумбия

Sysop: Rich Courney
Голос: 202-272-1646
Данные: 202-272-1514 — 300/1200/2400 бод

База данных файлов оказалась одной из крупнейших из всех, что мне доводилось видеть. В директории 70 находятся программы для проектирования каменных кладок и подпорных стен на основе Lotus Symphony.

Администрация общих служб

Информационно-ресурсный сервисный центр

Данные: 202-535-8054 — 300 бод

Данные: 202-535-7661 — 1200 бод

Информационно-ресурсный сервисный центр AOC предоставляет информацию о контрактах, расписаниях, политике и программах. Особый интерес представлял еженедельный дополнительный список отстранённых, приостановленных и лишённых права участия подрядчиков.

Бюджетно-финансовый борд Управления иммиграционной и натурализационной службы

НЕ ЗВОНИТЕ НА ЭТУ BBS В РАБОЧЕЕ ВРЕМЯ.

Sysop: Mike Arnold
Данные: 202-787-3460 — 300/1200/2400 бод

Система предназначена для обмена информацией, связанной с бюджетным и финансовым управлением в федеральном правительстве. Это «рабочая» система для сотрудников Иммиграционной и натурализационной службы.

Компьютерная информационная служба «Новости морской авиации» (NANci)

При поддержке журнала Naval Aviation News, корп. 159E, приложение Военно-морского двора, Вашингтон, округ Колумбия 20374

Sysop: Commander Howard Wheeler
Голос: 202-475-4407
Данные: 202-475-1973 — 300/1200 бод

Доступна с 17:00 до 8:00 в будние дни, с 17:00 пятницы до 8:00 понедельника.

Крупная BBS с обширным объёмом информации и программ на военно-морскую тематику. NANci адресована тем, кто интересуется историями, фактами и историческими сведениями о военно-морской авиации.

Федеральная национальная ипотечная ассоциация

Sysop: Ken Goosens
Данные: 202-537-7475
202-537-7945 — 300/1200 бод

Эта BBS находится в переходном состоянии. Кен Госсенс будет управлять новой BBS по номеру 703-979-6360. Возможно, BBS станет закрытой площадкой под руководством нового сисопа. У этой BBS была / есть одна из крупнейших коллекций файлов для скачивания.

Всемирный банк

Отдел информационных технологий и инфраструктуры, подразделение офисных систем, Вашингтон, округ Колумбия

Sysop: Ashok Daswani
Голос: 202-473-2237
Данные: 202-676-0920 — 300/1200 бод

По сути, это BBS для обмена программным обеспечением, однако содержит и прочую информацию об использовании микрокомпьютеров и программного обеспечения, поддерживаемого Всемирным банком. Также поддерживается актуальная информация об объявлениях IBM.

Национальное управление по исследованию океана и атмосферы (NOAA)

Национальный метеорологический центр

Для входа на эту BBS необходимо получить пароль у сисопа.

Sysop: Vernon Patterson
Голос: 301-763-8071
Данные: 301-899-0825 — 300 бод
301-899-0830 — 1200 бод

Одна из наиболее полезных из доступных онлайн баз данных. С её помощью можно получить доступ к метеорологическим данным, собранным в 6000 точках по всему миру. Также возможно отображение грубых, но информативных графических карт США с указанием температур, осадков и прогнозов.

Национальная метеорологическая служба, Министерство торговли США

BBS для пользователей восточного побережья морского прогноза

Для входа на эту BBS необходимо получить пароль у сисопа.

Sysop: Ross Laporte
Голос: 301-899-3296
Данные: 301-454-8700 — 300 бод

Используйте эту BBS для получения информации о морской погоде и навигационных данных о прибрежных водных путях, включая предупреждения о тропических штормах.

NARDAC

Военно-морской региональный центр автоматизации данных, Норфолк, штат Виргиния, 23511-6497

Sysop: Jerry Dew
Голос: 804-445-4298
Данные: 804-445-1627 — 300 и 1200 бод

Базовая утилитарная система, разработанная для удовлетворения информационных потребностей NARDAC. В файловом разделе этой BBS доступен журнал Министерства обороны CHIPS. Также имеются статьи о ВМФ и IBM.

Управление по делам ветеранов

Информационно-технологическая доска объявлений

Данные: 202-376-2184 — 300/1200 бод

Содержимое этой BBS охватывает широкий спектр: от списков вакансий до информации о компьютерной безопасности.

Министерство энергетики

Управление гражданского обращения с радиоактивными отходами, Infolink

Sysop: Bruce Birnbaum
Голос: 202-586-9707
Данные: 202-586-9359 — 300/1200 бод

Эта BBS содержит пресс-релизы, информационные листки, справочные материалы, парламентские вопросы и ответы, речи и показания Управления по гражданскому обращению с радиоактивными отходами.

Несколько BBS из исходной статьи я намеренно не включила — либо шансы попасть на них были невелики, либо они получили отрицательные отзывы. Большинство из перечисленных, судя по всему, располагают обширными информационными файлами для скачивания и изучения. В статье содержалось очень серьёзное предостережение против взлома и вывода из строя этих систем — они управляются государством и добровольными сисопами. Раз уж вы можете зайти на них законно — почему бы этим не воспользоваться?

— The Sorceress

Безопасность модемов с обратным дозвоном

Автор: David I. Emery

В статье ` пользователь gnu@hoptoad.UUCP` пишет:

> *Вот два сообщения, которые я сохранил по данной теме...*
>
> *[Полагаю, что итоговой статьёй в той дискуссии была статья Lauren Weinstein, vortex!lauren; возможно, у него есть копия.]*

Ниже следует оригинальная статья, положившая начало той дискуссии. Не знаю, можно ли считать её «итоговой», поскольку, насколько я помню, мы с Lauren оба публиковали дополнительные комментарии.

— Dave

**** СТАТЬЯ ****

Всё более популярный метод защиты коммутируемых портов от хакеров и прочих злоумышленников — режим обратного дозвона (dial back): легитимный пользователь инициирует звонок на нужную ему систему, вводит свой идентификатор пользователя и, возможно, пароль, после чего отключается и ждёт, пока система сама перезвонит ему на заранее согласованный номер. Предполагается, что злоумышленник не сможет указать номер обратного дозвона (который тщательно защищён), а значит, даже угадав пару имя пользователя/пароль, он не проникнет в систему — при подключении к системе он не может сделать ничего значимого, кроме как ввести эти данные. Если пара окажется верной, в худшем случае, как считается, произойдёт ложный звонок какому-то легитимному пользователю, что не нанесёт вреда и даже может спровоцировать расследование в области безопасности.

Многие организации рассчитывают на режим обратного дозвона модема как на основную защиту от проникновения через коммутируемые порты, ошибочно полагая, что злоумышленник никак не сможет подключиться к обратному звонку модема, не имея прямого доступа к прослушиваемой линии. Увы, это предположение не всегда верно — недостатки в конструкции модемов и устройстве телефонных сетей, к сожалению, вполне позволяют хитрому злоумышленнику перехватить обратный звонок и обмануть модем, заставив его думать, что он дозвонился до легитимного пользователя.

Проблемные области следующие.

Центральные телефонные узлы с управлением на стороне вызывающего абонента

Многие старые коммутаторы центральных телефонных узлов реализуют управление на стороне вызывающего абонента: разрыв соединения между звонящим и вызываемым абонентом находится исключительно под контролем инициирующего телефона. Это означает, что если злоумышленник просто не положит трубку после ввода имени пользователя и пароля легитимного пользователя, модем окажется не в состоянии разорвать соединение.

Практически все модемы в подобной ситуации просто перейдут в положение «на рычаге» и не заметят, что соединение не разорвано. Если та же линия используется и для входящих, и для исходящих звонков, когда модем перейдёт к дозвону легитимного пользователя, он может не

обнаружить (стандартного электрического способа это определить не существует), что злоумышленник по-прежнему подключён к линии. Это означает, что модем может попытаться набрать номер, а затем ждать тонального сигнала ответа от удалённого модема. Если злоумышленник любезно подаст этот сигнал со своего модема, услышав, как модем системы завершил набор, он сможет установить соединение и проникнуть в систему. Разумеется, некоторые модемы оснащены детекторами тонального сигнала и сигнала обратного вызова и действительно ожидают тонального сигнала перед набором и сигнала обратного вызова после набора — однако обмануть их с помощью записи тонального сигнала (или микросхемы-генератора тонального сигнала) труда не составит.

Попытка совершить исходящий звонок на звонящую линию

Некоторые модемы настолько «туги на ухо», что снимают трубку на звонящей линии и пытаются совершить с неё исходящий звонок. Этот факт может быть использован злоумышленником для обхода защиты обратного дозвона даже на коммутаторах с совместным управлением или управлением со стороны вызываемого абонента. Злоумышленнику достаточно дозвониться на линию исходящих звонков (что сработает даже если это отдельная линия, лишь бы злоумышленник смог раздобыть её номер) именно в тот момент, когда модем собирается совершить исходящий вызов. Далее применяется та же техника: ждать завершения набора, а затем подать сигнал ответа — и, конечно, техника подачи тонального сигнала модему, который его ожидает, здесь тоже работает.

Звонок на линию исходящих звонков окажется особенно эффективным в случаях, когда управляющее модемом программное обеспечение либо отключает автоответ в промежутке между входящим и обратным звонком (позволяя линии звонить без каких-либо действий), либо разрешает модему принимать звонки (автоответ включён), не проверяя при этом, занята ли линия в момент попытки совершить исходящий звонок.

Окно звонка

Даже тщательно написанное программное обеспечение может быть обмануто проблемой «окна звонка». Многие центральные телефонные узлы фактически соединят входящий звонок с линией, если та снимет трубку в момент поступления звонка — даже без предварительной подачи сигнала вызова с частотой 20 Гц. Сигнал вызова на многих телефонных коммутаторах подаётся асинхронно каждые 6 секунд на каждую линию с непринятым входящим звонком; таким образом, если входящий звонок достигает линии сразу после окончания периода сигнала вызова, а линия «провидчески» снимает трубку, она может так и не получить сигнала вызова.

Это означает, что модем, снимающий трубку для исходящего звонка в тот самый момент, когда злоумышленник дозванивается, может не зафиксировать сигнала вызова и, следовательно, не иметь возможности понять, что подключён к входящему звонку, а не к исходящей схеме коммутатора. И даже если коммутатор всегда подаёт сигнал вызова перед соединением входящего звонка, большинство модемов имеют «окно» непосредственно при снятии трубки для инициирования вызова, в течение которого они игнорируют переходные процессы (в том числе сигнал вызова) — полагая, что те порождены самим процессом снятия трубки. [Автор знает, что некоторые коммутаторы инвертируют полярность напряжения на линии в режиме ответа, чтобы отличить его от режима инициирования, однако поскольку это далеко не повсеместная практика, мало какие модемы используют эту информацию.]

Итоги

Таким образом, невозможно с какой-либо уверенностью утверждать, что когда модем снимает трубку и пытается совершить исходящий звонок на линии, способной принимать входящие звонки, он действительно подключён к коммутатору и совершает исходящий вызов. А поскольку злоумышленнику сравнительно легко обмануть схему обнаружения тональных сигналов в модеме, заставив её «считать», что она слышит тональный сигнал, сигнал обратного вызова и т. д., вплоть до момента, когда злоумышленник подаёт сигнал ответа, подключается и проникает в систему, — безопасность не должна опираться на подобный режим обратного дозвона.

Рекомендации

Обратный дозвон с использованием той же линии, по которой поступил входящий звонок, не очень безопасен и не может быть сделан полностью безопасным с помощью обычных модемов. Применение случайных (псевдослучайных) временных задержек между входящим и обратным звонком в сочетании с разрешением модему принимать звонки в период ожидания (с механизмом распознавания того, что принятый звонок не является инициированным исходящим — например, путём проверки режима модема: инициирующий или отвечающий) существенно сократит это окно уязвимости, однако полностью устранить его невозможно.

Очевидно, что при подключении к старому коммутатору с управлением на стороне вызывающего абонента использование одной и той же линии для входящих и исходящих звонков вовсе небезопасно. Это легко проверить экспериментально, так что избежать подобных ситуаций вполне возможно.

Обратный дозвон с использованием отдельной линии (или линии и модема) для исходящих звонков значительно надёжнее — при условии, что либо линия исходящих звонков «стерильна» (злоумышленнику непросто связать её с целевой системой), либо она является односторонней и не может принимать входящие звонки вообще. К сожалению, последнее решение в большинстве организаций значительно предпочтительнее первого, поскольку длительное сокрытие номера телефона линий исходящих звонков сопряжено со значительным риском. Автор не пытался заказать телефонную линию только для исходящих звонков, поэтому ему не известно, какие дополнительные тарифы могут быть установлены за эту услугу и доступна ли она вообще.

Последнее предупреждение

В прошлом в некоторых регионах можно было получить доступ к тестовым и верификационным транкам телефонных компаний с помощью MF-тонов так называемых «синих ящиков» (blue boxes). Эти тестовые транки подключаются к специальным портам на телефонных коммутаторах, позволяя установить тестовое соединение с линией, которое не разрывается при повешенной трубке. Такие тестовые соединения можно было использовать для обмана модема исходящих звонков — даже на выделенной линии только для исходящих звонков (поскольку телефонная компания нуждается в способе тестирования, она, как правило, обеспечивает к ней тестовые подключения, даже если клиент не может принимать звонки).

Доступ к верификационным и тестовым портам и транкам был ужесточён (они представляют собой нечто вроде «прослушивания по звонку», так что достать их должно быть очень непросто), однако, как и в любой системе, всегда существует опасность, что кто-то — по глупости или невежеству, а не по злому умыслу — предоставит злоумышленнику доступ к одному из них.

Дополнительные комментарии

После публикации этой статьи несколько человек предложили использовать линии ATC, которые могут совершать исходящие звонки, но не могут принимать входящие, либо линии WATS только для исходящих звонков, на которые также нельзя дозвониться. Также несколько человек предложили использовать переадресацию вызовов — перенаправлять входящие звонки на линию исходящих звонков в службу безопасности. [Это может плохо работать в зонах обслуживания некоторых коммутаторов ESS, которые в любом случае один раз звонят на номер, с которого переадресуются звонки, — на случай если кто-то забыл отменить переадресацию. Переадресация также подвержена случайной отмене при перезагрузке программного обеспечения коммутатора.]

После публикации я фактически попытался измерить, насколько широко «окно» входящего вызова для модемов, используемых нами для дозвона в CRDS. Оказалось, что для модемов US Robotics Courier со скоростью 2400 бод оно составляет не менее 2–3 секунд. Я обнаружил, что могу вполне уверенно обходить защиту обратного дозвона на той же линии за несколько десятков попыток, какие бы трюки с таймингом и мониторингом состояния модема в программном обеспечении авторизации при обратном дозвоне я ни применял. В итоге я пришёл к выводу, что без перепрограммирования микроконтроллера модема для более умного контроля состояния линии на уровне программы авторизации (getty) мало что можно сделать для обеспечения сколько-нибудь значимой безопасности при обратном дозвоне по той же линии.

Поскольку для взлома обычно требовалось несколько попыток, определённое незначительное улучшение безопасности можно обеспечить, строго ограничив количество неудачных обратных вызовов на одного пользователя в день: тогда хакеру, располагающему лишь несколькими паролями, пришлось бы предпринимать попытки на протяжении значительного периода времени.

Следует отметить, что обратный дозвон по выделенной линии только для исходящих звонков является в какой-то мере надёжным.

```
David I. Emery    Charles River Data Systems   617-626-1102
983 Concord St., Framingham, MA 01701.
uucp: decvax!frog!die
```

```
David I. Emery   Charles River Data Systems
983 Concord St., Framingham, MA 01701 (617) 626-1102 uucp: decvax!frog!die
```

Перехват компьютерных данных — проще простого

Автор: Ric Blackmon, sysop FED BBS

Получено: Elric of Imrryr & Lunatic Labs UnLtd

Примечание от Elric: Этот файл написан сисопом борды для специалистов по компьютерной безопасности (работавшей на CoCo). Насколько мне известно, борда больше не существует — хакеры слишком часто её крашили... (хехе).

Введение

На протяжении нескольких лет я принимал определённую дезинформацию за технически достоверную и не занимался этим вопросом должным образом. Несколько болванов скармливали мне болванские байки: мол, прослушка прерывает передачу компьютерных данных; данные якобы можно уловить как радиочастотное излучение, но это лишь масса неразборчивого сигнала, порождённого движением данных между регистрами; необходимо быть «в синхроне» с отправляющим компьютером; прочитать данные без точного совпадения скорости, чётности и битового паттерна невозможно; наконец, принять сигнал способен лишь компьютер той же марки и модели. Всё это — обычная чепуха.

На самом деле перехватить компьютерные данные проще, чем телефонный разговор. Техника и оборудование практически те же, однако компьютерная линия будет точнее (оба компьютера применяют процедуры коррекции ошибок) и чище (цифровые передачи дают более чёткие сигналы, чем аналоговые).

Технические основы

Прежде всего следует понимать: почти все передачи данных ведутся открытым текстом в формате ASCII. Линии, несущие иные битовые группы или зашифрованные тексты, встречаются крайне редко.

Сигнал присутствует на зелёном и красном проводах телефонной линии («tip» и «ring»). Данные, скорее всего, передаются как асинхронные последовательные данные на скорости 300 бод. По мере того как 1200 бод входит в моду, можно ожидать всё более широкого использования повышенной скорости передачи.

Наконец, не нужно беспокоиться о протоколе или даже о скорости передачи (бодах) вплоть до того момента, пока не получена записанная копия передачи.

Практический эксперимент

В ходе простого эксперимента запись передачи данных была сделана на самый дешёвый кассетный магнитофон путём подключения к зелёному и красному проводам за модемом. Затем запись воспроизводилась в модем так, словно это была оригинальная передача. В этот момент,

при необходимости, настройки протокола на приёмном терминале можно было изменить в соответствии с записью. Никаких регулировок не потребовалось — на несанкционированный экран поступил чёткий, безошибочный документ, а принтер выдал его аккуратную твёрдую копию.

Сообщение было успешно захвачено. Однако если бы это был перехват, а не простое прослушивание, его можно было бы изменить с помощью обычного текстового редактора в любых целях и вернуть в линию.

Почему данные ценнее голоса

Если бы меня интересовала информация, исходящая от конкретной компании, ведомства или офиса, я счёл бы перехват передачи данных куда более продуктивным, нежели прослушивание голосовых переговоров, — и даже более ценным, чем получение бумажных документов.

- **Значимая и важная информация сосредоточена в передаче данных в большей концентрации.**
- **Значимую и важную информацию легче обнаружить в передачах данных, чем в массивах файлов или телефонных переговорах.**
- **Переданные данные считаются достоверными, а при обнаружении подделки вину легко свалить на оборудование.**
- **Законы, касающиеся прослушивания несекретных и нефинансовых компьютерных данных, либо крайне несовершенны, либо откровенно бессмысленны.**

Вывод

Смысл всего вышесказанного в том, что благоразумный руководитель должен шифровать все передачи данных. Пакеты шифрования стоят дёшево (программа DES сейчас продаётся за 30 долларов) и просты в использовании.

Phrack World News, часть 1

Автор: Sir Francis Drake

01.02.1988

Обновление по арестам

Все, кого Секретная служба задержала в прошлом июле, в сентябре получили запросы с предложением «поговорить». Никто, кроме Solid State, больше не слышал от SS ничего. Solid State был осуждён и получил год условно плюс обязательные общественные работы. Остальные — Ninja NYC, Bill из RNOC, Oryan QUEST и другие — по-прежнему ждут решения. Ходят слухи, что Oryan QUEST активно сотрудничал с федералами, но насколько это соответствует действительности — неизвестно. Ниже — короткое интервью с Oryan QUEST. Помните, что у QUEST есть привычка врать.

PHRACK: Ты слышал от SS в сентябре? Похоже, все остальные слышали.

QUEST: Нет. Я не слышал от них ничего с момента ареста. Может, они про меня забыли.

P: Что думает твой адвокат о твоём деле?

Q: Говорит — не высовываться. Говорит, проблем нет из-за моего возраста.

P: Что думают родители?

Q: Они были реально злые около недели, потом успокоились. Я думаю, родители понимали, что я уже достаточно пережил... мне было по-настоящему хреново.

P: Планируешь продолжать заниматься телекомом — легально или нет?

Q: Эм, хочу звонить на борды... я понимаю, почему сисоп может не дать мне доступ, но... думаю поднять борд, закрытый, просто чтобы оставаться на связи, знаешь? Было весело, и я просто не хочу снова попасться.

P: Напоследок слова мудрости?

Q: Что бы кто ни говорил — я *ЭЛИТА*. Нет, не пиши это.

P: Пишу.

Q: Нет, я не хочу, чтобы люди думали, что я придурок.

P: Ну...

Q: Сам придурок.

— Совсем другая тема: Taran King, как некоторые из вас знают, был арестован и в скором времени напишет для Phrack файл о том, что произошло.

Медиа

Главной медийной темой стали пугающие истории о компьютерных вирусах, кульминацией которых стала полностраничная статья в Newsweek, написанная добрым старым Sandza с коллегами. John Markoff из San Francisco Examiner публиковал статьи о вирусах, взломе голосовой почты, а также материал, который вскоре должен выйти, — об июльских арестах (с фокусом на Oryan QUEST). Небольшой инсайд: возможно, он переходит в New York Times или San Jose Mercury.

В мире фрик-медиа дела идут под гору. Помимо PHRACK (у которого был плохой период, но, будем надеяться, мы вернулись всерьёз и надолго), есть 2600 и Syndicate Report. Syndicate Report закрыт, хотя их система голосовой почты иногда работает. 2600 превратился из ежемесячного журнала в ежеквартальный из-за финансовых потерь. Один труп и двое раненых.

Разное

Taran King и Knight Lightning весело проводят время в своём братстве в Университете Миссури. Их средние баллы — примерно 2,1 и 2,7 соответственно. Phantom Phreaker и Doom Prophet играют в панк/метал-группе. Lex Luthor жив и пишет длинные статьи для 2600. Sir Francis Drake продался и написал фрик-статьи для Thrasher. Jester Sluggo снова стал слегка активен.

Заключение

Всё меньше людей занимается фрикингом, мир в плачевном состоянии, а я иду спать. Слава Эрис.

sfd

«Облава на незаконных хакеров»

Автор: Al Simmons, редактор CCN

Из California Computer News, октябрь 1987 года

Хакеры, будьте осторожны!

Службы телефонной безопасности, местная полиция и Секретная служба усиливают давление на незаконный хакинг — электронное воровство, которое обходится компаниям дальней связи и их клиентам в миллионы долларов ежегодно. По данным правительственных источников, совокупные потери от компьютерного мошенничества всех видов в США сейчас составляют от 3 до 5 миллиардов долларов в год.

«Прокуратура Сан-Франциско добивается первого обвинительного приговора взрослому хакеру»

(Спустя примерно 18 лет — давно пора!)

Окружной прокурор Сан-Франциско Арло Смит недавно объявил о первом уголовном осуждении взрослого компьютерного хакера в Верховном суде Сан-Франциско.

В докладе, опубликованном 31 августа, прокуратура Сан-Франциско назвала имя обвиняемого: Стив Ссех (Steve Cseh), 25 лет, житель Сан-Франциско, который ранее в том же месяце признал себя виновным в уголовном преступлении — «получении телефонных услуг с мошеннической целью» (фрикинг) с помощью компьютера.

Судья Верховного суда Лоренс Кей (Laurence Kay) приговорил Ксека к трём годам условного срока и обязал его отработать 120 часов на общественных работах.

С учётом того, что Ксех в полной мере возместил ущерб U.S. Sprint — компании-жертве, — судья Кей понизил квалификацию деяния до административного правонарушения.

Тем не менее, по настоянию прокурора суд обязал Сцеха передать его компьютер и модем компании U.S. Sprint в счёт частичного покрытия расходов на выявление краж. (Это серьёзные деньги!)

По словам окружного прокурора Арло Смита, группа следователей из U.S. Sprint и Pac Tel (гестапо) несколько недель работала в начале этого года, чтобы обнаружить хакерскую активность и отследить её до телефонной линии Сцеха.

Дело было связано с использованием компьютера и специального программного обеспечения для незаконного получения учётных данных зарегистрированных пользователей с целью совершения звонков на дальние расстояния.

Звонки Сцеха прослушивались в течение трёх недель в марте прошлого года. После того как активность была отслежена до его телефонной линии, сотрудники службы безопасности телефонной компании (штурмовики гестапо) смогли получить законное разрешение — в соответствии с федеральным законом о телефонной связи — на мониторинг источника и продолжительности незаконных звонков.

Впоследствии следователи совместно с инспектором Джорджем Уолшем (George Walsh) из отдела по борьбе с мошенничеством полиции Сан-Франциско получили ордер на обыск по месту жительства Сцеха. Среди изъятых улик — компьютерное оборудование, программа автодозвона и блокноты с кодами и телефонными номерами, — сообщил помощник окружного прокурора Джерри Коулман (Jerry Coleman), который вёл это дело.

U.S. Sprint первоначально заявил о потерях более чем в 300 000 долларов в результате использования их кодов за последние два года; однако в ходе расследования удалось доказать лишь конкретные потери на меньшую сумму, отслеживаемые до Сцеха за трёхнедельный период мониторинга.

«Вероятно, другие пользователи компьютеров по всей стране также имели доступ к взломанным кодам Sprint благодаря их распространению на нелегальных компьютерных досках объявлений», — добавил Коулман. (С каких это пор BBS стали незаконными, господин Коулман?)

«Сакраментские следователи разоблачили группу электронных воров на Тахо»

Тем временем на южном берегу озера Тахо агенты Секретной службы и следователи телефонной компании арестовали Томаса Гулда Элворда (Thomas Gould Alvord), ликвидировав группу по электронному воровству, предположительно наделавшую несанкционированных звонков более чем на 2 миллиона долларов.

Согласно материалу Sacramento Bee, подготовленному журналистами Тедом Беллом (Ted Bell) и Джимом Льюисом (Jim Lewis), 37-летний Элворд был арестован 9 сентября по пяти уголовным статьям за компьютерный взлом кодов доступа к дальней связи пяти частных телефонных компаний.

По данным аффидавита, поданного в окружной суд Сакраменто, Элворд использовал автоматический дозвонщик с запрограммированными формулами подбора, что позволяло ему находить номера кредитных карт дальней связи, которыми пользовались клиенты частных телефонных компаний.

В аффидавите, составленном Уильямом С. Грейнджером (William S. Granger), специальным агентом Секретной службы, указана Пола Хейес (Paula Hayes), следователь компании Tel-America из Солт-Лейк-Сити, — именно она, работая под прикрытием, в конечном счёте положила конец незаконной деятельности «South Shore Electronic Co.» Элворда. Хейес под видом покупателя приобретала у него коды доступа.

Аффидавит агента Грейнджера фиксирует потери U.S. Sprint в размере 340 000 долларов, однако представитель Sprint Дженей Коттрелл (Jenay Cottrell) заявил, что эта цифра «может существенно вырасти», — сообщает Sacramento Bee.

По имеющимся данным, ежемесячный счёт одной брокерской компании в Pacific Bell планомерно рос с 3 000 долларов в апреле до 72 000 долларов в августе. Коды дальней связи этой фирмы, по словам следователей, процитированных Bee, входили в число тех, что были отслежены до телефонов Элворда.

По имеющимся сведениям, Элворд взламывал коды доступа Sprint, Pacific Bell и других компаний и продавал их дальнобойщикам по 60 долларов в месяц. Компаниям, совершавшим международные звонки, и крупным предприятиям он выставлял счёт от 120 до 300 долларов в месяц за услуги дальней связи своей «South Shore Electronics Co.»

>From The $muggler

Phrack World News, Часть 3

Автор: Sorceress (набор текста), под редакцией $muggler
(Источник: San Francisco Chronicle)

```
  +---------------------------------------------------------------------------+
  -[ PHRACK XVII ]---------------------------------------------------------

                   "The Code Crackers are Cheating Ma Bell"
            Typed by the Sorceress from the San Francisco Chronicle
                            Edited by the $muggler

              The Far Side.........................(415)471-1138
              Underground Communications, Inc.......(415)770-0140

  +---------------------------------------------------------------------------+
```

В калифорнийских тюрьмах заключённые используют «код», чтобы бесплатно звонить по телефону — договариваясь обо всём на свете: от поставок оружия до визитов бабушки.

В студенческом общежитии в Теннесси студенты используют этот код, чтобы открыть линию дальней связи на таксофоне и говорить бесплатно двенадцать часов подряд.

Где-то в телефонной будке на Среднем Западе мафиози использует код для анонимных звонков, по которым из Южной Америки в Соединённые Штаты доставляется партия наркотиков.

Код — это на самом деле миллионы различных персональных идентификационных номеров, выданных телефонными компаниями страны. Мошеннический доступ с помощью этих кодов превратился в общенациональную эпидемию, которая обходится американским телефонным компаниям более чем в 500 миллионов долларов в год.

В конечном счёте большая часть этих убытков перекладывается на потребителей в виде повышения тарифов, говорят аналитики.

Коды безопасности варьируются от многозначных кодов доступа, применяемых клиентами альтернативных компаний дальней связи, до номеров «calling card», выдаваемых компанией American Telephone & Telegraph и 22 местными телефонными компаниями, такими как Pacific Bell.

Большая часть потерь происходит по вине компьютерных хакеров, заявила Рене Данн, представитель U.S. Sprint — третьей по величине компании дальней связи.

Эти технические умельцы — нередко смышлёные, хотя и нелюдимые подростки — настраивают свои компьютеры для дозвона на местный номер доступа одной из альтернативных компаний дальней связи, например MCI или U.S. Sprint. Когда телефон отвечает, обычный клиент вводит секретный персональный код — как правило, пятизначный, — который разрешает ему совершить звонок.

Хакеры, однако, разработали компьютерные программы, которые непрерывно перебирают комбинации чисел, пока не находят нужную, — совсем как взломщик сейфа, прислушивающийся к характерному щелчку штифтов и дисков.

После этого хакер — известный в отрасли как «крэкер», потому что он «взломал» код — получает полный доступ к телефонной линии этого клиента.

Клиент не понимает, что произошло, пока в конце месяца не получает огромный счёт. К тому времени его номер доступа и персональный код уже вывешены на тысячах электронных досок объявлений по всей стране, доступных любому, у кого есть компьютер, телефон и модем —

устройство, позволяющее компьютеру общаться по телефонным линиям.

«Это определённо серьёзная проблема», — сказал один эксперт по телефонной безопасности, пожелавший остаться неизвестным. «Я видел один счёт с суммой 98 000 долларов за месяц».

Один житель Беркли борется с телефонными мошенниками с прошлой осени, когда в его счёте MCI обнаружились около 100 долларов за звонки, которых он не совершал.

Хотя MCI заверила его, что проблема будет решена, последний счёт составил 11 страниц и включал переговоры на дальние расстояния на 563,40 доллара. Среди этих звонков:

• Двухчасовой звонок в Хайаттсвилл, штат Мэриленд, 22 января. Женщина, взявшая трубку, сказала, что понятия не имеет, кто звонил к ней домой.

• Многократные звонки в общежитие Калифорнийского университета в Лос-Анджелесе. Студентка, ответившая на звонок, сказала, что не знает, кто 39 минут разговаривал с ней или её соседкой по комнате вскоре после полуночи 23 января.

• Звонки в комнаты общежитий Университета штата Вашингтон в Пуллмане и Университета Колорадо в Боулдере. Ответившие там мужчины заявили, что не знают, кто им звонил и ничего не знают о похищенных кодах дальней связи.

Клиент из Беркли, попросивший не называть его имени, сказал, что исчерпал терпение и отказался от своего аккаунта MCI.

Телефонные компании преследуют хакеров и прочих мошенников методами, пытаясь угнаться за технологическим монстром, связанным триллионами миль телефонных линий.

Компании иногда следят за телефонными счетами клиентов. Если счёт, в среднем составлявший 40–50 долларов в месяц, вдруг резко вырастает до нескольких сотен долларов, причём звонки явно совершались из разных концов страны в один и тот же день, телефонная компания помечает счёт и пытается отследить источник.

ФБР проводит собственные проверки электронных досок объявлений в поисках похищенных кодов. Телефонные компании время от времени выходят на эти доски и публикуют сообщения с предупреждением о том, что ордера на арест не заставят себя ждать, если мошенничество не прекратится. Уважаемые доски объявлений сами предупреждают телефонных хакеров и просят держаться подальше.

Уже готовится несколько уголовных дел, сообщила Жоселин Калиа, менеджер по борьбе с мошенничеством в U.S. Sprint.

Если следователи не спешат рассказывать о своих методах, то подполье проявляет не меньшую осторожность. «Если у них (компаний) есть эффективные методы предотвращения, то почему всё это до сих пор продолжается?» — задаётся вопросом один компьютерный эксперт, ветеран хакерства, утверждающий, что перешёл на легальную сторону около десяти лет назад.

Этот эксперт, представившийся только как Dr. Strange, сказал, что был частью первоначальной группы электронных умельцев начала 1970-х, разработавших «синие ящики» — сложные устройства, имитирующие тоны телефона и позволявшие первым хакерам взламывать бесплатную систему 800 и звонить по всему миру бесплатно.

Новые хакеры, досаждающие телефонным компаниям, — это просто следствие того, что «технология сменилась с синих ящиков на компьютеры», сказал Dr. Strange. По мере того как «телефонная компания повышает ставки... задача становится всё интереснее», добавил он.

Двойственное отношение к огромным и во многом безликим телефонным компаниям облегчает многим людям самооправдание своего мошенничества. Одна женщина из юго-западного штата, получившая код авторизации от своего друга, сообщила через посредника, что никогда не воспринимала телефонное мошенничество как «нравственную проблему». «Я не злоупотребляю

этим», — сказала женщина о своей новоприобретённой телефонной привилегии. «Я не говорю долго — никогда больше часа подряд — и не раздаю код друзьям». Кроме того, добавила она, счета за звонки, которые она совершала по всей территории Соединённых Штатов последние шесть недель, приходят «в крупную корпорацию, которой я была недовольна. Это не так, будто счета получает какой-то конкретный человек».

Есть, однако, одно место, где телефонные компании, пожалуй, держат верх в постоянной войне с хакерами и мошенниками.

В некоторых тюрьмах, сообщил представитель MCI, «мы обнаружили, что можем использовать давление сообщества. Допустим, мы ограничиваем доступ к телефонам или вовсе их убираем, а среди заключённых есть немало тех, кто телефоном не злоупотреблял. Тогда до них доходит информация о том, кто именно из заключённых стал причиной изъятия телефонов. Как только (личность нарушителя) становится известна, думаю, беспокоиться не о чем», — сказал представитель. «В тюрьмах тоже есть своя система правосудия».

Phrack World News — регулярная рубрика Phrack, посвящённая новостям из мира хакерства и телекоммуникаций.