

Historia hackingu (1960 -2003)

1960

- [1960] Listopad: Rozmowy telefoniczne są przełączane po raz pierwszy przez komputer
- [1963] Dartmouth College, w Hanover, New Hampshire, wprowadza stosowanie komputerów jako regularną część programu nauk humanistycznych. ASCII (American Standard Code for Information Interchange) zostaje stworzony, umożliwiając urządzeniom różnych producentów wymianę danych. ASCII składa się ze 128 unikalnych łańcuchów jedynek i zer.
- [1964] Istnieje około 18 200 systemów komputerowych w USA. Ponad 70% jest produkowanych przez International Business Machines (IBM). Thomas Kurtz i John Kemeny tworzą BASIC (Beginner's All-Purpose Symbolic Instruction Code), łatwy do nauczenia język programowania, dla swoich studentów w Dartmouth College
- [1967] Advanced Research Projects Agency (ARPA) współpracuje z amerykańskimi ekspertami komputerowymi tworząc sieć Interface Message Processors (IMPS). Komputery mogą działać jako bramy do komputerów typu mainframe różnych instytucji w USA i stanowi znaczną część tego co w nadchodzących latach stanie się Internetem
- [1969] Advanced Research Projects Agency (ARPA) przechodzi w ARPANET, usługi mające na celu zapewnienie efektywnych sposobów komunikowania się naukowców. Firma konsultingowa Cambridge Massachusetts, Bolt Beranek and Newman, którzy wygrali przetarg na ARPA, zaprojektowali i zbudowali sieć Interface Message processors (IMPS) w roku poprzedzającym, dostarczyli (wrzesień) pierwsze urządzenie do UCLA, i dostarczyli (październik) drugie urządzenie do Stanford Research Institute. IMPS działał jako brama do mainframe'ów w różnych instytucjach w USA. W ciągu kilku dni od dostawy, maszyny z UCLA i Stanford połączyły się po raz pierwszy i ARPANET znalazł uzasadnienie. Później sieć rozwinęła się w cztery węzły. Były to Uniwersytet Kalifornijski z Los Angeles, Uniwersytet Kalifornijski z Santa Barbara, Uniwersytet Utah i Stanford Research Institute. System ten będzie ewoluował rozwijając się pod nazwą Internet lub Super Autostrada Informacyjna.
- Intel informuje o dużo większych pamięciach RAM. Oferuje 1KB pojemności.
- Ken L. Thompson, Dennis M. Ritchie i inni zaczynają pracę nad systemem operacyjnym Unix w Bell Labs (później AT&T). UNIX był stworzony w celu dopuszczenia kilku użytkowników

do jednoczesnego dostępu do komputera.

Pierwsi hackerzy komputerowi pojawiają się na MIT. Zapożyczyli nazwę od terminu opisującego członków grupy modelującej pociągi w szkole, którzy "hackowali" pociągi elektryczne, tory i przełączniki aby uczynić je szybszymi i lepszymi. Kilku z tych członków przeniosło swoją ciekawość i umiejętności na osprzęt nowych systemów komputerowych typu mainframe, które były badane i opracowywane w kampusie

Joe Engressia ("Whistler", "Joybubbles" i "High Rise Joe"), uważany za ojca phreaking. Joe, który był niewidomy, był studentem matematyki na USF pod koniec lat sześćdziesiątych, kiedy odkrył, że dzięki gwizdaniu blisko wysokiego A (2600 Hz), uaktywniają się obwody telefonu, dzięki czemu mógł prowadzić rozmowy międzymiastowe bez ponoszenia kosztów

1970

[1970] Szacuje się, że około 100 000 systemów komputerowych pracuje w USA. Digital Equipment Corporation (DEC) wprowadził wspaniałą PDP-11, który jest uważany za jeden z najlepiej zaprojektowanych mikrokomputerów, a wiele z tych maszyn jest stosowanych do dzisiaj. Niektórzy z najlepszych hackerów ćwiczyli właśnie na "jedenastkach".

[1971] Pierwszy komputer osobisty, Kenback, ogłasza się na łamach wrześniowego wydania "Scientific American".

Joe Draper ("Cap'nCrunch") dowiaduje się, że zabawka-gwizdek, dodawana do płatków zbożowych Cap'n'Crunch generuje dźwięk o częstotliwości 2600 Hz, ten sam wysoki ton, jaki ma dostęp do międzymiastowego systemu przełączeń AT&T. Draper zbudował blue box, który, używany w połączeniu z gwizdkiem i skierowany do głośnika telefonu umożliwia phreakerom na wykonywanie bezpłatnych rozmów telefonicznych.

Magazyn "Esquire" publikuje "Secrets of the Little Blue Box" z instrukcjami dotyczącymi tworzenia blue boxa, a oszustwa kablowe narastają w USA. Wśród sprawców: dzieciaki Steve Wozniak i Steve Jobs, przyszli założyciele Apple Computer, którzy rozpoczęli domową produkcję i sprzedaż blue boxów.

Pierwszy program e-mail napisany przez Raya Tomlinsona i stosowany w ARPANET, który ma już 64 węzły. Tomlinson, Bolt Beranek i Newman, zakontraktowani przez Advanced Research Projects Agency (ARPA) do stworzenia ARPANET, wybrali znak @ do oddzielenia nazwy użytkownika w e-mailu

jakio pierwszym przesłanym między komputerami.

- [1972]** Maj: John Draper aresztowany za phreaking telefoniczny i skazany na 4 miesiące więzienia w więzieniu kalifornijskim Lompoc.
- [1973]** Prezes firmy Intel, Gordon Moore, publicznie ujawnia swoje proroctwo, że liczba tranzystorów w mikrochipach będzie podwajać się co półtora roku. Prawo Moore'a zachowuje swoją prawdziwość od ponad dwudziestu lat.
- [1975]** Zainstalowano około 13 000 bankomatów.
- Domowa wersja PONG od Atari Inc, rozpoczyna sprzedaż w 900 sklepach Sears and Roebuck, pod marką Searsa "Telegames".
- Sierpień: William Henry Gates III (Bill Gates) i Paul Allen zakładają Microsoft.
- [1976]** David R. Boggs i Robert M. Metcalfe wymyślili Ethernet w firmie Xerox w Palo Alto, Kalifornia.
- Kwiecień: Stephen Wozniak, Steven Paul Jobs i Ron Wayne podpisują porozumienie zakładające Apple Computer.
- [1977]** 3 Sierpień: Zaoferowano publicznie TRS-80 ('Trash-80') Model I, który stał się pierwszym komputerem stacjonarnym
- Grudzień: Atari 2600 w sprzedaży po 199,95\$, zawiera jedną grę i dwa kontrolery.
- [1978]** Bill Joy tworzy pierwszą wersję Berkeley Software Distribution (BSD) UNIX'a
- Oszacowano, że w USA używa się 5000 komputerów stacjonarnych.
- Kevin David Mitnick ('Condor') spotyka phreakera Lewisa De Payne ('Roscoe') z gangu Roscoe atakując operatora radia HAM w Południowej Kalifornii.
- [1979]** Został opublikowany Język ANSI C przez Briana W. Kernighana i Dennisa M. Ritchiego.
- Lipiec: Apple II+ z 48K RAM i nowym ROM'em z "auto-startem" wprowadził Apple Computer po 1 195\$
- 1980**
- [1980]** Szacuje się, że jest 350 000 terminali komputerowych "połączonych w sieć" z dużymi komputerami "hostami"

Nintendo Ltd wprowadza Donkey Kong jako grę zręcznościową w automatach do gier.

Rodzi się Usenet, sieciowe komputery UNIX tworzą sieć komputerową przez wolne łącza telefoniczne. Usenet w końcu zastępuje ARPANET jako wirtualną tablicę ogłoszeń z wyboru wschodzącego narodu hackerów.

Grudzień: Gang Roscoe, w tym Kevin Mitnick atakują system komputerowy w US Leasing

[1981] Kenji Urada, 37 lat, stał się pierwszą opisaną ofiarą robota. Samobieżny robot zgniótł go, kiedy próbował go naprawić w fabryce w Japonii.

Comodore Business Machine zaczyna sprzedawać komputer domowy VIC-20. Jest wyposażony w mikroprocesor 6502, 8 kolorów i 61 klawiszową klawiaturę. Kolumny ekranu są ograniczone do 22 znaków. Jest produkowany w Niemczech i sprzedawany w USA za niecałe 300\$.

Lipiec: Microsoft przejmuje pełne prawa do produktu DOS Seattle Computeri nazywa go MS-DOS.

Ina Murphy ("Captain Zap") był pierwszym hackerem osadzonym i skazanym jako przestępca. Murphy włamał się do komputerów AT&T i pozmieniał wewnętrzne zegary, które mierzyły stawki rozliczeniowe. Ludzie mieli stawki nocne, kiedy dzwonili w południe

23 Maj: Kevin Mitnick, 17 lat, został aresztowany za kradzież podręczników komputerowych z Pacific Bell w Los Angeles, Kalifornia. Był ściągany jako nieletni i skazany na wyrok w zawieszeniu.

28 Maj: Pierwsza wzmianka o Microsoft w Usenecie

[1982] Istnieje 3 miliony terminali komputerowych połączonych w sieć z większymi hostami komputerowymi. Oszacowano ponadto 5 milionów komputerów używanych w USA. Więcej niż 100 firm buduje komputery osobiste.

Założono Sun Microsystems przez czterech 27 latków: Andreeasa von Bechtolsheima, Vinoda Khosla, Scotta MnNealy i Billa Joya

Ponieważ kultur hackerska zaczęła erodować, utraciła niektóre najzdolniejsze umysły na rzecz komercyjnych PC i oprogramowania, start-upów. Richard Stallman zaczyna rozwijać darmowy klon UNIX, napisany w C, który nazwał GNU (Gnu's Not Unix)

Lewis De Payne ("Roscoe") przyznał się do zarzutu spisku

i oszustw. Wyrok: 150 dni więzienia. Accomplice dostaje 30. Mitnick dostaje 90 dni jako nieletni a także zawieszenie na rok.

Kevin Mitnick crackuje system Pacific Telephone i TRW, niszcząc dane.

William Gibson wprowadza termin "cyberprzestrzeń"

Zaczyna działać phreakerów "Gang 414". BBS "414 Private" to miejsce gdzie "Gang 414" wymieniał się informacjami podczas włamania do systemów Sloan-Kettering Cancer Center i komputerów wojskowych w Los Alamos.

Sierpień: Commodore wprowadziło komputer Commodore 64, który wszedł do więcej niż miliona domów podczas pierwszego roku. C-64 był pierwszym komputerem domowym ze standardowy, 64K RAM. Przy sugerowanej cenie detalicznej 595\$ uznano to za wielką wartość. Miał kalwiturę, procesor, układy grafiki i dźwięku.

19 Września: Scott E. Fahlman wpisał pierwszy uśmiezek on-line , :-).

[1983] Formuje się Internet, kiedy ARPANET jest podzielony na dział wojskowy i cywilny

Film "Gry Wojenne" wchodzi na ekrany. Matthew Broderic gra nastolatka ,któy przypadkowo zaczyna odliczanie do III wojny światowej.

Piracki Plovernet BBS (Bulletin Board System) działa na wschodnim wybrzeżu, działając w Nowym Yorku i na Florydzie. Jest własnością i jest zarządzany przez nastoletniego hackera "Quasi Moto". Plovernet przyciąga pięciuset chętnych użytkowników w 1983. Eric Corley ("Emmanuel Goldstein") był w tym samym czasie współoperatorem systemu wraz z "Lexem Luthorem", który później założył grupę phreakerów / hackerów, Legion of Doom

22 Września: Kevin Poulsen ("Dark Dante") i Ron Austin aresztowany za włamanie do sieci ARPANET. W wieku 17 lat Polsen nie jest ścigany sadownie a Austin otrzymuje 3 lata w zawieszeniu.

27 Września: Richard Stallman daje pierwszą wzmiankę o GNU na Usenecie

12 Listopad: Pierwsze wzmianki o Microsoft Windows na Usenecie

[1984] Andrew Tanenbaum napisał pierwszą wersję Minix, UNIX

przeznaczony do celów edukacyjnych. Minix natchnął Linusa Torvaldsa do napisania Linuxa.

Uniwersytet Kalifornijski w Berkeley wydał wersję 4.2 BSD, która zawierała kompletną implementację protokołów sieciowych TCP/IP. Systemy oparte na tym i późniejszym BSD dostarczały możliwości sieciowe od wielu sprzedawców w oparciu o sieć Ethernet.

Bill Landreth ("Cracker") został skazany za włamanie się do jednych z najbardziej bezpiecznych systemów komputerowych w USA, w tym sieci elektronicznej GTE Telemail Mail, gdzie w NASA znajdowała się korespondencja Departamentu Obrony. W 1987 roku Bill złamał warunki zwolnienia i wrócił do więzienia.

Powstał Legion of Doom. Legion of Doom, grupa hackerów, która działała w USA pod koniec 1980 roku. Szeroki zakres działania grupy obejmowała sieci telefoniczne, kopiowanie poufnych danych od firm i dystrybucja samouczków hackerskich. Członkowie: Lex Luther (założyciel), Chris Goggans ('Erik Bloodaxe'), Mark Abene ('Phiber Optik'), Adam Grant ('The Urvile'), Franklin Darden ('The Leftist'), Robert Riggs ('The Prophet'), Loyd Blankenship ('The Mentor'), Todd Lawrence ('The Marauder'), Scott Chasin ('Doc Holiday'), Bruce Fancher ('Death Lord'), Patrick K. Kroupa ('Lord Digital'), James Salsman ('Karl Marx'), Steven G. Steinberg ('Frank Drake'), Corey A. Lindsly ('Mark Tabas'), 'Agrajag The Prolonged', 'King Blotto', 'Blue Archer', 'The Dragyn', 'Unknown Soldier', 'Sharp Razor', 'Doctor Who', 'Paul Muad'Dib', 'Phucked Agent 04', 'X-man', 'Randy Smith', 'Steve Dahl', 'The Warlock', 'Terminal Man', 'Silver Spy', 'The Videosmith', 'Kerrang Khan', 'Gary Seven', 'Bill From RNOG', 'Carrier Culprit', 'Master of Impact', 'Phantom Phreaker', 'Doom Prophet', 'Thomas Covenant', 'Phase Jitter', 'Prime Suspect', 'Skinny Puppy' and 'Professor Falken'.

2600: Kwartalnik Hackera, założony przez Erica Corleya ('Emmanuel Goldstein')

19 Czerwiec: X Windows System stworzony przez Roberta W. Scheiflera

[1985] Zine hackerski Phrack po raz pierwszy opublikowana przez Craiga Neidorfa ("Knight Lightning") i Randy Tischlera ("Taran King")

24 Maj: Data rejestracji pod oryginalną nazwą Quantum Computer Service (America Online).

[1986] Kongres uchwała Computer Fraud and Abuse Act. Prawo jednak nie obejmuje nieletnich

Niemiecka grupa hackerska Chaos Coputer Club, złamał informacje o niemieckim programie nuklearnym z komputerów rządowych w czasie kryzysu czernobylskiego.

8 Styczeń: Członek Legion of Doom Loyd Blankenship ('The Mentor') zostaje aresztowany. Publikuje swój słynny traktat, który znany jest jako "Manifest Hackera".

26 Luty: BBS Phoenix Fortess publikuje nakazy aresztowania i konfiskaty sprzętu 7 lokalnych użytkowników w Fremont, CA. Sysop okazał się być lokalnym przedstawicielem prawa a Phoenix Fortress stworzony do wyławiania hackerów i piratów oprogramowania.

1 Września: Nieznana osoba lub nienazana grupa używająca nazwy Pink Floyd wielokrotnie uzyskała dostęp do systemów UNIX i Portia na Uniwersytecie Stanforda bez uwierzytelnienia. Szkody oszacowana na 10 000\$.

Sierpień: W sierpniu, podczas wykrycia 75 centowego błędu księgowego w komputerze na Lawrence Berkeley Lab na Uniwersytecie w Berkeley, Clifford Stoll odkrył dowody hackerów w pracy. Całoroczne śledztwo doprowadziło do aresztowania odpowiedzialnych pięciu niemieckich hackerów.

[1987]

14 Września: Ujawniono publicznie, że młodzi hackerzy niemieccy, nazywający siebie Data Travellers, włamali się do komputerów NASA i innych sieci na całym świecie do ściśle tajnych instalacji komputerowych

23 Listopad: Chaos Computer Club hackuje sieć SPAN NASA

Grudzień: Kevin Mitnick atakuje systemy Santa Cruz Operation. Mitnick skazany za kradzież oprogramowania SCO, poczym współpracuje z inżynierami SCO mówiąc im jak dostał się do ich systemu.

[1988]

Styczeń: US Secret Service potajemnie nagrywa kasetę z konwencji hackerów SummerCon.

2 Listopad: Robert T. Morris Jr, absolwent Cornell University i syn głównego naukowca w dziale w dziale Agencji Bezpieczeństwa Narodowego (NSA), uruchomił samoreplikującego się robaka w rządowej ARPANET (prekursora Internetu) w celu przetestowania jego wpływu na system UNIX. Robak wymyka się z rąk i rozprzestrzenia na około 6000 sieci komputerowych, zatykając systemy rządowe i uniwersyteckie. Morrisa zwolniono z Cornell, skazano na trzy lata w zawieszeniu i grzywnę 10 000\$.

3 Listopad: Pierwsza wzmianka o robaku Morrisa na Usenet

Grudzień: Hacker z Legion of Doom Robert Riggs ('The Prophet') włamał się na sieć komputerową BellSouth AIMSX i ściągnął dokument E911 (opisujący jak działa telefon alarmowy 911). Riggs wysłał egzemplarz do Phrack Craiga Neidorfa ('Knight Lightning'). Craig i Robert zostali schwytani przez władze federalne i skazani. Akt oskarżenia mówił, że "komputerowy plik tekstowy" był wart 79 449\$, a osoba z BellSouth zeznała, że był wart 24 639\$. Proces rozpoczął się w 23 lipca 1990, ale nioczekiwanie zakończyło się postępowanie, kiedy rzą zwrócił się do sądu o oddalenie wszystkich zarzutów, gdy okazało się, że społeczeństwo może zadzwonić pod bezpłatny numer i zakupić ten sam dokument za mniej niż 20\$.

[1989]

22 letni hacker i ex-członek LOD Corey Lindsly ("Mark Tabas") przyznał się do winy za przestępstwo nielegalne dostania się do US West, w wyniku czego dostał 5 lat nadzoru kuratorskiego.

W laboratorium CERN z zakresie badań z fizyki wysokich energii w Genewie, Tim Berners-Lee i Robert Cailliau rozwijają protokół, który stanie się World Wide Web.

23 Styczeń: Herbert Zinn ('Shadowhawk') porzucił szkołę, był pierwszym skazanym (jako nieletni) z Computer Fraud and Abuse Act z 1986 roku. Zinn miał 16 lat kiedy udało mu się włamać do AT&T i Departamentu Obrony. Został skazany 23 stycznia 1989 roku, zniszczył pliki warte 174 000\$, kopiując programy warte miliony dolarów i publikując hasła i instrukcje jak naruszać systemy bezpieczeństwa komputerowego. Zinn został skazany na 9 miesięcy więzienia i grzywnę w wysokości 10 000\$.

Maj: Grupa specjalna w Chicago aresztowała domniemanego hackera znanego jako "Kyrie".

Czerwiec: Podziemna grupa hakckerów znana jako NuPrometheus League rozprowadza własne nielegalne oprogramowanie uzyskane z Apple Computer.

21 Lipiec: Znania jako "Atlanta Three", 3 członków LOD/H (Legion of Doom) oskarżono o włamanie do Bell South Telephone Networks (w tym 911) - posiadanie oprogramowania i informacji z BellSouth, nieuprawniony dostęp, nielegalne posiadanie numerów kart kredytowych z zamiarem oszustwa i konspirację. Tych trzech hackerów to: Franklin Darden ('The Leftist'), Adam Grant ('Urvile' i 'Necron99'), Robert Riggs ('The Prophet').

22 Czerwiec: "Fry Guy" 16 latek z Elmwood w Indianie, włamał się do mainframe'a McDonalda w systemie Sprint Telnet. 14 września 1990 roku został skazany na 44 miesiące w zawieszeniu i 400 godzin prac społecznych.

1990

[1990]

Mitch Kapor i John Perry Barlow tworzą Electronic Frontier Foundation częściowo aby bronić praw tych postępowań dla domniemanego piractwa komputerowego.

Kevin Poulsen jest sprawcą niesławnego incydentu z KIIS-FM w Los Angeles. W 1990 stacja prowadziła konkurs "Wygraj Porsche w Piątek", z 50 000\$, Porsche dawane było co 102 dzwoniącemu. Kevin i jego wspólnicy, przy swoich komputerach przejęli kontrolę na 25 liniami telefonicznymi stacji, blokując wszystkie połączenia oprócz własnego. Potem wykręcił 102 połączenie i wygrał Porsche 944

15 Styczeń: Padł system telefonii międzymiastowej AT&T. W ciągu dziewięciu długich godzin szalonego wysiłku dla przywrócenia usługi, około siedemdziesięciu milionów połączeń nie zostało wykonanych. Hackerzy byli pierwszymi podejrzanymi o spowodowanie wypadku ale później inżynierowie AT&T odkryli ,że "winowajcą" był błąd własnego oprogramowania AT&T.

18 Styczeń: Siły specjalne Chicago aresztowały domniemanego hackera Craiga Neidorfa ("Knight Lightning" w St. Louis.

Luty: US Secret Service urządziły nalot na domniemanego hackera Len Rose'a ("Terminus") w Maryland. Len dostał w swoje ręce System V 3.2 AT&T Unix Source Code, wliczając w źródło login.c.

21 Luty: Siły policyjne w Chicago zrobiły nalot na dom Roberta Izenberga , domniemanego hackera w Austin

1 Marca: Siły policyjne Chicago zrobiły nalot na Steve Jackson Games, na pracowników Loyda Blankenshipa ("The Mentora") i Chrisa Goggansa ("Eryk Bloodaxe"), którzy mieli związek z grupą hackerską (LOD), którą badał Departament Sprawiedliwości. Znalaziono podręcznik do gry nazwanej G.U.R.P.S. Cyberpunk, co zostało zinterpretowane jako tutorial dotyczący piractwa komputerowego i przystąpiło do wykorzystania sprzętu i dokumentów znalezionych na miejscu.

7 Maj: Od 7 do 9 maja w USA Secret Service i Arizona Organized Crime and Racketeering Bureau przystąpiły do Operacji Sundevil przeciwko hackerom w Cincinnati, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tuscon, San Diego, San Jose i San Francisco.

7 Marzec: 24 letni Richard G. Wittman Jr, przyznał się do systemu komputerowego NASA. Wittman przyznał się do

zmodyfikowania informacji - wewnętrznego hasła komputera federalnego

Kwiecień: Między kwietniem 1990 roku a majem 1991 roku hackerzy z Holandii spenetrowali 34 stron DOD. NA wielu tych stronach mieli dostęp do poufnych danych na temat personelu wojskowego - raporty wydajności pracowników, informacje turystyczne redukcje personelu; logistyka - opis rodzaju i ilości sprzętu, systemów broni będących w rozwoju.

Maj: Co najmniej cztery banki rozliczeniowe były szantażowane przez tajemniczą grupę hackerów, którzy włamali się do centralnych systemów komputerowych. Hackerzy zażądali znacznej sumy pieniędzy w zamian za pokazanie bankom jak przeniknęli do ich systemów. Ekspert komputerowy określił ich poziom wiedzy i znajomość systemów rozliczeń bankowych jako "naprawdę przerażający".

[1991] Internet , ustanowiony w celu połączenia wojskowych i edukacyjnych instytucji, zablokował dostęp przedsiębiorstwom. Zakaz został zniesiony jeszcze tym samym roku.

Krażą pogłoski na temat wirusa Michelangelo, oczekiwany program zawiesił komputery 6 marca 1992 roku, w 517 rocznicę urodzin artysty. Doomsday przechodzi bez większych incydentów.

Luty: AOL udostępnił wersję DOS

11 Kwietnia: Kevin Poulsen ('Dark Dante') aresztowany za włamanie do systemu telefonicznego PacificBell

Lipiec: Justin Petersen ('Agent Steal' i 'Eric Heinz') aresztowany za włamanie do TRW, kradnąc karty kredytowe

6 Sierpnia: Tim Berners-Lee ogłasza w Usenecie projekt World Wide Web.

Wrzesień: Justin Petersen wychodzi z więzienia aby pomóc FBI złapać Kevina Mitnicka.

17 Wrzesień:Linus Torvalds upublicznia wersję 0.01 programu Linux. Student informatyki na Uniwersytecie Helsińskim tworzy system operacyjny Linux. Pierwotnie nazwał swój system Freax.

5 Październik: Linus Torvalds decyduje się ogłosić udostępnienie za darmo oparetego o minix jądra o nazwie Linux na Usenecie

[1992]

Masters of Deception (MOD) grupa phreakerów wpadła dzięki podsłuchowi

Morty Rosenfeld skazany po włamaniu do TRW, kradzieży numerów kart kredytowych i sprzedaży raportów kredytowych

29 Styczeń: Twórca minix, Andy Tanenbaum, umieszcza na grupie dyskusyjnej comp.os.minix posty o tym, że niesławny Linux jest przestarzały. Linus Torvalds szybko odpowiada na te posty.

Listopad: Kevin Mitnick włamuje się do California Department of Motor Vehicles

[1993]

1 Marca: Microsoft wypuszcza Windows NT

Styczeń: Slackware Patricka Volkerdinga staje się pierwszą komercyjną, samodzielnie dystrybuowaną wersją Linuksa.

9 Lipiec: Pierwsza konferencja Def Con hackerska odbywa się w Las Vegas. Konferencja ma być jednorazowym pożegnaniem z BBS'ami (zastąpionymi przez WWW), ale spotkanie jest tak popularne, że stało się wydarzeniem corocznym.

Sierpień: Justin Petersen aresztowany za kradzież wyposażenia komputerowego.

28 Październik: Randal Schwartz Intela używa Crack do łamania haseł, później skazany na podstawie prawa karnego komputerowego stanu Oregon, i skazany.

Grudzień: Wydano wersję 1.0 FreeBSD

[1994]

Założono Red Hat

Wydano Linux 1.0

12 Styczeń: Mark Abene ('Phiber Optik') rozpoczyna odsiadkę jednego roku. Jako członek - założyciel Masters of Deception, Mark zainspirował tysiące nastolatków w kraju do "badania" wewnętrznego funkcjonowania narodowego systemu telefonicznego USA. Sędzia federalny próbował "wysłać wiadomość" innym hackerom przez skazanie Marka na rok więzienia w więzieniu federalnym, ale wiadomość została przeinaczona: Setki sympatyków uczestniczyło w przyjęciu powitalnym na cześć Marka w jego domu w Manhattan Club. Wkrótce potem, New York Magazine nazwał go jednym ze 100 najbystrzejszych ludzi w mieście. Inni członkowie MOD: Elias Ladopoulos ('Acid Phreak'), Paul Stira ('Scorpion'), John Lee ('Corrupt'), Allen Wilson ('Wing'), 'The Seeker', 'HAC', 'Red Knight', 'Lord Micro'

i Julio Fernandez ('Outlaw').

23 Marzec: 16 letni student muzyki Richard Pryce ('Datastream Cowboy') został aresztowany i oskarżony o włamanie do setek komputerów, w tym te z bazy Griffiths Sił Powietrznych, NASA i koreańskiego Instytutu Badań Jądrowych. Times of London poinformował, że wiedząc o aresztowaniu, Richard "leżał skulny na podłodze i płakał". Pryce potem przyznał się do 12 włamań i ukarany grzywną 1800\$. Później, Mathew Bevan ('Kuji') mentor Pryce'a ostatecznie odnalazł Pryce'a i aresztował go. Zarzuty wobec Pryce'a zostały później wycofane a teraz pracuje jako konsultant do spraw zabezpieczeń komputerowych.

13 Czerwca: Władimir Levin, 23 latek, prowadzący rosyjską grupę hackerów, ujawnił publicznie, że okradł międzynarodowy bank przez sieć. Ukradziono około 10 milionów dolarów z Citibanku, który twierdził, że prawie wszystkie odzyskano z wyjątkiem 400 000\$. Później Levin został schwytany i skazany na 3 lata więzienia.

Sierpień: Justin Petersen elektronicznie 150 000\$ z Heller Financial

Wrzesień: Baza danych kart kredytowych Netcom (kupione przez MindSpring, potem MindSpring kupione przez Earthlink) znalazła się online i była dostępna dla nieuprawnionych osób

25 Grudzień: Kevin Mitnick (prawdopodobnie) włamuje się do komputera Tsutomu Shimomury. Mitnick był pierwszym podejrzanym o shakowanie komputera Tsutomu w 199 roku, ale nieznanym izraelski hacker (przyjaciel Mitnicka) został o to podejrzany. Izraelski hacker szukał disasemblera do telefonu komórkowego OKI zapianego przez Shimomurę i chcianego przez Mitnicka.

[1995]

27 Styczeń: Kevin Mitnick włamuje się do Well; wstawia tam pliki Shimomury i numery kart kredytowych Netcom.

Luty: Ex-członek LOD, Corey Lindsly ("Mark Tabas") był głównym przywódcą w organizacji hackerskiej "Phonemasters", której celem była własna infrastruktura telekomunikacyjna od wybrzeża do wybrzeża. Grupa przeniknęła do systemów AT&T, British Telecom, GTE, MCI WorldCom, Sprint, Southwestern Bell i systemy należące do stanowych i fedsraknych agencji rządowych, wliczając w to komputery National Crime Information Center (NCIC). Włamali się do baz danych sprawozdawczości kredytowej należącej do Equifax Inc i TRW Inc. Weszli do baz danych Nexis/Lexis i systemów Dun&Bradstreet. Mieli dostęp do części krajowego systemu elektroenergetycznego, systemów

kontroli lotów i torowali sobie drogę do cyfrowej pamięci podręcznej niepublikowanych numerów telefonicznych Białego Domu. Sąd przyznał uprawnienia FBI do pierwszego użycia "podśluchu danych" do monitorowania aktywności hackerów. Ci hackerzy zorganizowali swoje ataki na komputerach przez telekonferencję i wykorzystali program PGP do zaszyfrowania, aby ukryć dane, którymi handlowali między sobą. 16 września 1999 roku, Corey Lindsly, lat 32 z Portland, Oregon, został skazany na 41 miesięcy pozbawienia wolności i nakazał zapłacić 10000\$ ofiarom korporacyjnym. Członkowie "Phonemasters": John Bosanac ("Gatsby") z San Diego, Calvin Cantrell ("Zibby") i Brian Jaynes obaj z Dallas, Rudy Lombardi ("Bro") z Kanady, Thomas Gürtler z Ohio. Calvin Cantrell, lat 30, z Grand Prairie w Teksasie, został skazany na dwa lata pozbawienia wolności musiał zapłacić 10000\$ dla ofiar korporacyjnych. John Bosanac dostał 18 miesięcy.

15 Luty: Kevin Mitnick aresztowany i oskarżony o uzyskanie nieautoryzowanego dostępu do komputerów należących do licznych producentów oprogramowania komputerowego i systemów operacyjnych, producentów telefonów komórkowych, dostawców usług internetowych i instytucji edukacyjnych, kradzieże, kopiowanie i sprzeniewierzenie zastrzeżonego oprogramowania komputerowego firmy Motorola, Fujitsu, Nokia, Sun, Novell, NEC. Mitnick był również w posiadaniu 20 000 numerów kart kredytowych.

18 Marzec: SATAN (Security Administrator Tool for Analyzing Networks) narzędzie bezpieczeństwa udostępnione dla Internet przez Dana Farmera i Wietes Venema. Dopuszczenie go wzbudza wielką debatę na temat narzędzi audytowania bezpieczeństwa będących podanyymi do publicznej wiadomości

5 Maj: Chris Lamprecht ("Minor Threat") stał się pierwszą zakazaną osobą z Internetu. Został skazany za liczne przestępstwa, do których się przyznał. Związane były z kradzieżą i sprzedażą płytek z obwodami elektronicznymi Southwestern. Na początku lat 90. Chris napisał program o nazwie ToneLoc (Tone Locator), program wydzwaniający wzorowany na programie stosowanym przez Matthew Brodericka w filmie Gry wojenne dla znajdowania otwartych linii modemowych w centralach telefonicznych.

16 Sierpień: Francuski student Damien Doligez złamał 40 bitowy szyfr RC4

11 Wrzesień: 22 letni Golle Cushing ("Alpha Bity") został aresztowany za sprzedaż kart kredytowych i telefonów komórkowych.

17 Wrzesień: Ian Goldberg i David Wagner złamali pseudo losowy generator liczb Netscape Navigatora 1.1. Uzyskali klucz sesyjny w kilka godzin na jednej stacji roboczej.

15 Listopad: Christopher Pile został pierwszą osobą, która została skazana za pisanie i rozpowszechnianie wirusów komputerowych. Pile, który sam nazywał siebie "Black Baron" został skazany na 18 miesięcy więzienia.

[1996]

Internet ma teraz 16 milionów hostów i szybko rośnie.

Icanet, firma, która zaprojektowała strony internetowe dla szkół została zagrożona przez szantażystę w Niemczech. Transakcja: Jeśli Icanet zgodzi się kupić jego program bezpieczeństwa komputerowego za 30 000 dolarów, haker nie zniszczy komputerów firmy. W kwietniu, Andy Hendrata, 27 letni indonezyjski student informatyki został skazany za sabotaż i próbę wymuszenia. Otrzymał rok pozbawienia wolności w zawieszeniu i 1500\$ grzywny

U.S. General Accounting Office donosi, że hackerzy próbowali włamać się do plików komputerowych Departamentu Obrony 250 000 razy w samym 1995 roku. Około 65% prób było udanych, według raportu.

6 Marzec: United Press International (UPI) ujawnił, że hacker znany jako 'u4ea', 'el8lite', 'elitone' i 'blff' zagroził online systemom komputerowym gazety Boston Herald i niektórym ISP w Bostonie. Raporty wskazywały, że hacker wszedł niezauważony na serwery 100 stron i zniszczył pliki na wielu z nich. Śledztwo zostało zainicjowane przez sekcję Przestępstw Kryminalnych NYPD.

4 Kwietnia: Według prokuratury, 19 letni Christopher Schanot z St Louis, Missouri, włamał się do krajowych sieci komputerowych, komputerów wojskowych, TRW, i usług raportowania kredytów Sprint

5 Kwietnia: 19 letni Christopher Schanot ('N00gz') z St Louis oskarżony w Filadelfii o oszustwa komputerowe, nielegalne podsłuchy, nieautoryzowany dostęp do wielu korporacyjnych i rządowych komputerów w tym Southwestern Bell, Bellcore, Sprint oraz SRI

19 Kwietnia: Hackerzy włamują się do systemu telefonicznego NYPD i zmieniają nagrany komunikat witający dzwoniących. Nowa wiadomość brzmiała: 'oficerowie są zbyt zajęci jedzeniem paczków i pić kawy aby odebrać telefon'. Skierowany jest do osób dzwoniących pod 119.

5 Lipca: Pojawi się pierwszy wirus do Excela, nazwany Laroux

31 Lipca: Tim Lloyd umieszcza programową bombę czasową w Omega Engineering w NJ; Pierwszy federalny przypadek sabotażu komputerowego. Bomba czasowa zniszczyła firmową sieć komputerową i światową zdolność do produkcji latem 1996 roku. Atak spowodował straty na 12 milionów dolarów i zwolnienie 80 pracowników. Lloyd otrzymał 41 miesięcy więzienia. Został zobowiązany do zapłacenia ponad 2 milionów dolarów zadość uczynienia

22 Sierpień: Eric Jenott z Fort Bragg, spdochroniarz, jest oskarżony o włamanie do systemów armii amerykańskiej i dostarczenie haseł obywatelowi komunistycznych Chin. obrońca Erica mówił , że żołnierz z Fort Bragg jest tylko hackerem , który testował wytrzymałość rzekomo nieprzeniknionego systemu komputerowego, znalazł słabości i powiedział o nich swoim przełożonym. Eric został później oczyszczony z zarzutów o szpiegostwo, ale uznany winnym zniszczenia własności rządowej i oszustw komputerowych.

Wrzesień: Johan Helsingius zamyka penet.fi. Penet.fi, najpopularniejszy anonimowy remailer, został najechany przez fińską policję w 1995 roku, po tym jak Kościół Scjentologiczny poskarżył się , że klient penet.fi ujawnia tajemnice kościelne w Sieci. Helsingius zamknął remailer po tym jak fiński są orzekł , że musi ujawnić prawdziwy adres e-mail klienta

6 Września: Atak DoS na Panix.com, IP w Nowym Jorku, Atakujący użył jednego komputera do wysłania tysięcy kopii pojedynczej wiadomości, której używają komputery aby rozpocząć dwustrony dialog. Komputery Panix po otrzymaniu wiadomości musiały przeznaczyć tyle mocy na obsługę okien dialogowych , że wykorzystały swoje zasoby i zostały wyłączone.

25 Wrzesień: Kevin Mitnick oskarżony o uszkodzenie komputerów w USC, Mitnick został oskarżony o 14 oszustw wynikające z jego domniemanej kradzieży własnościowego oprogramowania producentów. Został również oskarżony o uszkodzenie komputerów USC i "kradzież oraz kompilację" licznych plików elektronicznych zawierających hasła.

[1997]

Powstał AOHell, darmowa aplikacja, która pozwalała rosnącej wspólnocie niewykwalifikowanych hakerów - lub script kiddies - siać spustoszenie na America Online (AOL)

28 Styczeń: Ina Goldberg student Uniwersytetu Kalifornijskiego z Berkeley podjął wyzwanie RSA Data Securityi złamał 40 bitowy kod łącząc ze sobą 250 bezczynnych stacji roboczych, co pozwoliło mu

przetestować 100 miliardów możliwych "kluczy" na godzinę. W ciągu trzech i pół godziny Goldberg zdekodował wiadomość, która brzmiała "To dlatego powinieneś używać dłuższego klucza"

5 Luty: Członkowie Chaos Computer Club, niesławna elita hackerska Niemiec, zademonstrowała program hackujący ActiveX, który pozwalał i na dostęp do kopii Quicken, oprogramowania księgowego z Intuit i przetransferowania pieniędzy między rachunkami bankowymi, bez konieczności wchodzenia do zabezpieczonego normalnym hasłem systemu bezpieczeństwa Quicken

10 Marzec: Hacker 'Jester' jest pierwszym oskarżonym przez władze federalne jako nieletni o przestępstwa komputerowe.

21 Kwiecień: Hacker 'Joka' oszukał America Online i na chwilę zaknął stronę prowadzoną przez teksański oddział Ku Klux Klanu, zmuszając AOL do działania, ze względów bezpieczeństwa.

23 Maj: Carlos Felipe Sa;lgado Jr, 36 lat, który używał nazwy "Smak" rzekomo wstawia program do sniffowania, który zbiera informacje od firm kredytowych tuzina firm sprzedających produkty przez Internet. Carlos zebrał 100 000 numerów kart wraz z dużą ilością informacji aby z nich korzystać, powiedział FBI

Czerwiec: Poczta głosowa Netcom (kupiony przez Mindspring, następnie przez Earthlink) została złamana przez 'Mr Nobody'. 15 latek twierdził, że był wewnątrz poczty głosowej Netcom przez dwa lata. Tam złamał wiele skrzynek pocztowych za pośrednictwem klawiatury swojego telefonu i używał systemu do włamania się do innych telefonów do połączeń międzystrefowych.

31 Październik: Eugene Kashpureff aresztowany za przekierowanie strony internetowej NSI do swojej strony Alternic. Kashpureff zaprojektował oprogramowanie derforumujące systemi, który umożliwiał komputerom połączonym w sieci porozumiewać się. Wykorzystując słabość tego oprogramowania, Kashpureff przechwytywał użytkowników próbujących dostać się na stronę InterNIC, jego konkurenta, na swoją stronę AlterNIC, utrudniając tym użytkownikom możliwość rejestracji nazwy domeny lub przeglądania popularnych "elektronicznych katalogów" InterNIC dla nazw istniejących domen

Grudzień: Julio Ardita ('El Griton') 21 letni Argentyńczyk został skazany na trzy lata więzienia w zawieszeniu za włamanie do systemów komputerowych

należących do Harvardu, NASN, Los Alamos National Laboratory i Dowództwa Marynarki, Contorl and Ocean Surveillnace Center

8 Grudnia: www.yahoo.com jest uszkodzony przez 'pantz' i 'h4gis'

[1998]

Dwóch hackerów (bracia bliźniacy) Hao Jinglong i Hao Jingwen zostało skazanych na śmierć przez są w Chinach za włamanie do sieci komputerowej banku i kradzież 720 000 juanów (87 000 dolarów). Ynagzhou Intermediate People's Court we wschodniej prowincji Jiangsu w Chinach odrzucił apelację Hao Jingwena i utrzymał w mocy wyrok śmierci przeciw niemu. Jingwen i jego brat , Hao Jinglong, włamał się do komputerów Industrial and Comercial Bank of China i przesunął 720 000 juanów (87 000 dolarów) na konta założone na fałszywe nazwiska. We wrześniu 1998 roku wycofał 260 000 juanów (31 400 dolarów) z tych funduszy. Wyrok śmierci na Hao Jinglonga został zawieszony w zamian za zeznania.

1 Styczeń: Mark Abene ('Phiber Optik'), ekspert ds bezpieczeństwa, uruchomił polecenie sprawdzenia plików z hasłami klienta - i zakończył nadawanie instrukcji do tysięcy komputerów na świecie. Wiele komputerów posłusznie wysłało mu swoje pliki z hasłami. Abene wyjaśnił , że polecenie było wynikiem źle skonfigurowanego systemu, i że nie miał zamiaru zalewać swojej skrzynki pocztowej plikami z hasłami

16 Styczeń: Zhackowano Tallahassee Freenet. TFN został zaatakowany przez osobę lub osoby których zamiarem było wyraźne zniszczenie wszystkich plików w systemie. Zanim ataki zostały powstrzymane, tysiące katalogów domowych użytkowników, wiele systemów plików i wszystkie przesyłki mailowe zostały usunięte.

25 Luty: Zostały zhackowane komputery MIT Plasma & Fusion Center (PSFC) i DoD przez Ehuda Tenebauma ('Analyzez'). Komputer MIT został uruchomiony w starszej wersji Linuksa, z luką w zabezpieczeniach która ułatwiła włamanie. Po uzyskaniu dostępu do konta, hacker wykorzystał inne dziury w bezpieczeństwie i zainstalował pakiet sniffera. Hacker mógł zebrać nazwy użytkowników i hasła komputerów spoza sieci.

26 Luty: Solar Sunrise, szereg ataków na komputery Pentagonu prowadzi do ustanowienia całodobowej warty na stronach głównych komputerów wojskowych

27 Luty: Wyzwanie 56 bitowy DES - II - 1 RSA Data Security został uzupełniony o znacznie rozproszoną tablicę komputerów koordynując ich ataki brute force przez

"organizację" distributed.net. Wiadomość została odczytana "Wiele pracy wykonano" Uczestnicy wspólnie zbadali 6.3×10^{16} kluczy - pełne 90% całej przestrzeni kluczy -w około 40 dni

3 Marzec: Ehud Tenebaum ponownie shackował Dostawcę Internetu z Santa Rosa, NetDex, w odwecie za zatrzymanie jego dwóch amerykańskich przyjaciół hackerów ('Cloverdale Two').

18 Marzec: Ehud Tenebaum ('Analityczny') izraelski nastolatek został aresztowany w Izraelu. Podczas napięcia w Zatoce Perskiej, hackerzy wywołali całą włamań do jawnych komputerów Pentagonu i ukradli oprogramowanie. Urzędnicy podejrzewali go o pracę w porozumieniu z amerykańskimi nastolatkami przy włamaniu do komputerów Pentagonu. Zastępca Sekretarza Obrony USA, John Hamre nazwał to "najbardziej zorganizowanym i systematycznym atakiem" na system obrony USA do tej pory. Dochodzenie doprowadziło do dwóch amerykańskich nastolatków. 19 letni hacker izraelski nazywający siebie 'The Analityczny' jest określony jako ich przywódca i aresztowany. Izraelski Premier Benajmin Natanjahu nazywa Tenebauma "cholernie dobrym ... i bardzo niebezpiecznym". Ataki wykorzystywały dobrze znane luki w zabezpieczeniach systemu operacyjnego Solaris do którego poprawki były dostępne od miesiąca.

20 Marzec: Dwóch nastolatków hackuje T-Online, usługi online prowadzone przez narodową firmę telefoniczną w Niemczech, i wykradli informacje o setkach kont bankowych. Dwóch 16 letnich hackerów chwalili się swoimi wyczynami, nazywając bezpieczeństwo Deutsche Telekom dla usług online "absolutnie prywmitycznym"

Sierpień: Shawn Hill, 26 lat, z Orlando na Florydzie, były pracownik NASA, kontrahent Lockheed Martin Corp., przyznał się w sądzie federalnym do wykorzystania stacji roboczej NASA w Centrum Lotów Kosmicznych Kennedy'ego w celu uzyskania nieautoryzowanego dostępu do sieci komputerowych kilku firm w Orlando

20 Kwiecień: W Alabamie nastoletni hacker uruchamia mailowy atak bombowy składający się z 14 000 wiadomości w sieci NASA przeciwko innej osobie używające systemu sieciowego w domenie komercyjnej.

22 Kwiecień: Grupa kryminalnych hackerów z MoD (Masters of Downloading, nie mylić z grupą Masters of Deception) twierdziła ,że włamała się licznym sieci wojskowych, w tym do DISN(Defense Information Systems Network) oraz DEM (DISN Equipment Manager), która kontroluje wojskowy GPS (Global Positioning Satellites)

Maj: Członkowie bostońskiej grupy hackerskiej L0pht (teraz @stake), składają zeznania przed Senatem USA na temat luk w Internecie

30 Maj: Hacker wykorzystujący rozległość wsparcia technicznego firmy AOL (6000 osób) wykorzystał inżynierię społeczną w drodze do witryny internetowej ACLU. Napastnik dzwonił do AOL dopóki nie znalazł technika wsparcia, który był na tyle głupi aby udzielić dostępu do strony docelowej, która została zniszczona w wyniku ataku.

30 Czerwca: Była pracownica Straży Przybrzeżnej, Shakunla DeviSingla weszła do bazy danych personelu, którą pomagał stworzyć. DeviSingla użyła swego doświadczenia i hasła dawnego współpracownika i innej identyfikacji aby usunąć dane. Jej działania wymagały 115 pracowników i 1800 godzin dla odzyskania usuniętych informacji.

31 Lipca: Podczas Def Con 6, The Cult of Dead Cow (CDC) pokazał Back Orifice (BO) narzędzie do analizowania i kompromitowania bezpieczeństwa Windows

13 Sierpień: Hackerzy zniszczyli stronę New York Times (www.nytimes.com), zmieniając jej nazwę na HFG (Hacking for Girls). Hackerzy wyrazili swój gniew przeciw zatrzymaniu i uwięzieniu Kevina Mitnicka, temtu książki 'Takedown', współautorem której był reporter Times'a, John Markoff. Na początku listopada, dwaj członkowie HFG powiedzieli magazynowi Forbes, że rozpoczęli atak ponieważ byli znudzeni i nie mogli się dogadać co do filmu do obejrzenia.

17 Wrzesień: Aaron Blosser, programista kontraktowy, sam opisujący się jako "matematyczny maniak" wykorzystał ponad 2500 komputerów US West, instalując program, który wykorzystywał ich bezczynność do znajdowania bardzo dużych liczb pierwszych. Ich połączona moc obliczeniowa teoretycznie przekroczyła moc większości superkomputerów. Blosser zaprzęgnął 2585 komputerów do pracy w różnych porach dnia i nocy i szybko przekroczył 10.63 lat czasu przetwarzania w poszukiwaniu nowej liczby pierwszej. "Pracowałem nad tym problem (matematycznym) dłużej czas" powiedział Blosser. "Kiedy zacząłem pracować w US West, cała moc obliczeniowa była zbyt kusząca dla mnie"

1 Październik: Hackerzy nazywający się Electronic Disruption Theater twierdzili, że Pentagon używał nielegalnych technik ofensywnych w wojnie informacyjnej (ataki DDoS)

Listopad: 'Cloverdale Two' skazani na 3 lata w

zawieszeniu , 'Makaveli' i 'Too Short' włamali się do kiludziesięciu systemów komputerowych, wliczając w to te w Pentagonie. Dopiero później odkryto, że mentorem dla tych nastolatków był niesławny izraelski hacker , Ehud Tenebaum ('Analyzez').

[1999]

1 Luty: Kanadyjski nastolatek dokonał ataku Smurf na ISP Sympatico. Ataki Smurf występują kiedy złośliwy użytkownik Internetu

15 Luty: 15 latek z Wiednia włamuje się do systemu Uniwersytetu Clemson i próbował się włamać do NASA

18 Marzec: Jay Satiro, 18 latek po porzuceniu szkoły został oskarżony o włamanie do wewnętrznych komputerów America Online i zmodyfikowanie pewnych programów. Jaya uznano winnym i skazano na rok więzienia i 5 lat bez komputera w domu.

26 Marzec: Wirus Melissa atakuje 100 000 użytkowników poczty i spowodował straty na 80 milionów dolarów; napisany przez Davida Smitha 29 letniego programistę z New Jersey. Wirus został nazwany na cześć striptizerki z Florydy.

Kwiecień: Ikenna Iffith, 28 latek z Bostonu, został oskarżony o użycie domowego komputera do uzyskania nielegalnego dostępu do kilku komputerów, w tym kontrolowanych przez NASA i agencję Departamentu Obrony USA, gdzie m.in rzekomo przechwycono loginy i hasła, spowodował umyślne opóźnienia i uszkodzenia w komunikacji. 17 listopada 2000 roku został skazany na 6 miesięcy aresztu domowego

26 Kwiecień: Wirus CIH wydany przez Chen Ing-Hou, twórcy wirusa, który przyjął po nim inicjały. Był to pierwszy znany wirus skierowany przeciwko flash BIOS.

Maj: Napster, system wymoany plików MP3 peer-to-peer używany głównie do kopiowania niezaszyfrowanych plików z muzyką za darmo zaczyna zdobywać popularność, głównie na uczelniach gdzie studenci mają łatwy dostęp do połączeń internetowych o dużych prędkościach. Został stworzony przez studentów Uniwersytetu Northeastern Shawna Flaminga i Seana Parkera ,19 i 20 lat,, odpowiednio. Przed zamknięciem 2 lipca 2001 roku, Napster miał 85 milionów zarejestrowanych użytkowników pobierających 3 miliardy piosenek miesięcznie

11 Maj Whitehouse.gov zniszczona przez Global Hell

10 Lipca: Pokazano Back Orifice na Def Con 7

30 Siepień: Microsoft Corporation zamyka Hotmail na około 2 godziny. Zamknięcie następuje po otrzymaniu potwierdzonego doniesienia, że hackerzy naruszyli niektóre serwery wprowadzając konta Hotmail za pośrednictwem innych dostawców Internetu bez używania haseł

19 Sierpień: Strona ABC zaatakowana przez United Loan Gunmen

5 Wrzesień: Strona C-Span zaatakowana przez United Loan Gunmen

13 Wrzesień: Strona Drudge Report zaatakowana przez United Loan Gunmen

23 Wrzesień: Strony Nasdaq i American Stock Exchange zaatakowane przez United Loan Gunmen

Listopad: 15 letni Norweg Jon Johansen, jeden z trzech założycieli MoRE (Masters of Reverse Engineering), trio programistów, którzy zrobili duże poruszenie na rynku DVD przez wydanie DeCSS, programu używanego do złamania Content Scrambling System (CSS) szyfrującego każdy film DVD na rynku. 24 stycznia 2000 roku, władze norweski weszły do domu Johansena i zabrały sprzęt komputerowy

2000

[2000] 15 Styczeń: 19 letni Raphael Gray ('Curador') kradnie ponad 23 000 numerów kartkredytowych z 8 małych firm. Raphael kreuje się na "świętego e-commerce", po tym jak włamał się do amerykańskich brytyjskich i kanadyjskich firm podczas "krucjaty" odsłaniającej luki w bezpieczeństwie internetowym i który użył numeru karty kredytowej Billa Gatesa aby wysłać mu Viagrę

7 Luty: 16 letni kanadyjski hacker o pseudonimie 'Mafiaboy' prowadzi Distributed Denial-of-Service używając narzędzi dostępnych w Internecie, które pozwalają mu uruchomić zdalną koordynację błyskawicznego 1 gigabitów na sekundę floodowania żądanych pakietów IP z serwerów "zombie", co zablokowało Yahoo! Na ponad 3 godziny. Po przyznaniu się do winy, 'Mafiaboy' został skazany 12 września 2001 roku na osiem miesięcy w ośrodku dla młodzieży

9 Luty: Dwa dni później ataki DDoS skierowane przeciwko eBay, Amazon, ZDNet, CNN, E*Trade i MSN

Maj: Audytorzy GAO (General Accounting Office) byli w stanie uzyskać dostęp do informacji osobistych Departamentu Obrony przez plik który był dostępny

publicznie w Internecie. Audytorzy użyli tego pliku bez ważnego uwierzytelnienia i uzyskali dostęp do numerów ubezpieczniaków, adresów i informacji dotyczących płac

15 Maj: Wirus Love Bug wysłany z Filipin; koledzy z AMA, Michael Buen i Onel de Guzman są podejrzani o jego napisanie

1 Czerwiec: Qualcomm w San Diego shakowane przez studenta Uniwersytetu Wisconsin - Madison, Jerome'a Heckenkampa ('MagicFX')

15 Czerwiec: Konsultant Information Technology naruszył bezpieczeństwo brytyjskiego dostawcy Internetu, Redhotant odkrywając błędy zabezpieczeń. Udało mu się uzyskać nazwiska, adresy, hasła i numery kart kredytowych ponad 24 000 osób, wliczając w to wojskowych naukowców, urzędników państwowych i wyższej kadry kierowniczej, aby pokazać, że można to zrobić. Hacker powiedziała, że naruszenie bezpieczeństwa było "dziecinna zabawa"

18 Lipiec: AOL z siedzibą w Vienna, Wirginia, potwierdził, że zapisy na ponad 500 tak zwanych nazw użytkowników jego klientów zostało zhackowanych. Zapisy te zwykle zawierają informacje takie jak imię i nazwisko, adresy i numery kart kredytowych używanych do otwarcia konta.

7 Lipiec: Firma narzędzi Powergen ulokowana w Wielkiej Brytanii zmuszona była prosić tysiące swoich klientów o anulowanie kart kredytowych po pozostawieniu błędu w bazie danych kart

24 Lipiec: Anrew Miffleton ('Daphtpunk'), wiek 25 lat, z Arlington, Teksas, został skazany w sądzie federalnym na 21 miesięcy pozbawienia wolności i nakazał zapłacenie 3 000 dolarów grzywny. Miffleton związał się z grupą znaną jako "Darkside Hackers", którzy byli zainteresowani w używaniu nieautoryzowanych dostępów do urządzeń do wyłudzenia usług telefonii komórkowej i usług międzymiastowych za pomocą skradzionych numerów kart telefonicznych.

17 Sieprpień: Sędzia Lewis Kaplan z Nowego Jorku zakazał Ericowi Corleyowi ('Emmanuel Goldstein'), wydawcy magazynu 2600, publikowania oprogramowania obchodzącego system szyfrowaniwa DVD, Kod pozwalał na łatwiesze kopiowanie i wymianę filmów w Internecie

5 Września: 21 letni mężczyzna z New Rochell, Nowy Jork został skazany na cztery miesiące więzienia za włamanie do dwóch komputerów należących do Jet Propulsion Laboratory NASA w 1998 roku i użycie jednego z nich do

wejścia na czat poświęcony hackowaniu. Raymond Torricelli ('rolex') został członkiem grypy hackerskiej '#conflict', która używała swoich komputerów do elektronicznego modyfikowania rocznych wyników MTV Movie Awards. Dodatkowo znaleziono 76 000 dyskretnych haseł na jego komputerze.

6 Września: Parick W. Gregory ('MostHateD'), lat 20, przyznał się do roli jako członka założyciela Global Hell i został skazany na 26 miesięcy więzienia, trzy lata nadzoru kuratorskiego i musiał zapłacić 154 529,86 dolarów odszkodowania. GlobalHell spowodował szkód na co najmniej 1,5 miliona dolarów w różnych firmach amerykańskich i instytucjach rządowych, w tym Biały Dom i armia amerykańska. Gregory porzucił szkołę aby założyć własną firmę zajmującą się bezpieczeństwem komputerowym, przyznał się do kradzieży telefonicznych usług konferencyjnych z AT&T, MCI i Latitude Communications i konferencji telefonicznych między 1997 a majem 1999 roku, wraz z innymi hackerami w całym kraju

26 Wrzesień: Jason Diekman ('Shadow Knight', 'Dark Lord') aresztowany przez agentów federalnych, którzy odkryli na komputerach Diekmana dowody wskazujące ,że przechwytywał nazwy użytkowników i hasła z uniwersytetów, w tym Harvardu. Diekman przyznał się ,że włamał się do "setek, może tysięcy" komputerów w tym do systemów JPL, Standforda, Harvardu, Uniwersytetu Cornell, Uniwersytetu Stanowego w Fullerton, Uniwersytetu Kalifornijskiego w Los Angeles i San Diego.4 lutego 2002 roku, Diekan został skazany na 21 miesięcy więzienia w więzieniu federalnym, trzy lata nadzoru kuratora i ponad 87 000 dolarów odszkodowania.

Październik: Microsoft przyznaje ,że jego sieci korporacyjne zostały zhackowane i przejrano kod źródłowy jego przyszłych Windowsów. Podejrzewano hackera z St. Petersburga

10 Październik: FBI przyczyniło się do aresztowania 2 rosyjskich hackerów w Seattle, po tym jak stwierdzono ,że Aleksiej Iwanow , lat 20, i Wasilij Gorszkow, lat 25, spędzili dwa lata na atakowaniu amerykańskiego bizneu. FBI ustanowiła sfałszowane firmy bezpieczeństwa komputerowego, którą nazwali, trafnie, Invita (Zaproszenie). Wynajęli przestrzeń biurową w centrum Seattle i natychmiast zaprosił Iwanowa z Rosjii do pracy jako hacker. FBI porozumiewała się z Iwanowem i Gorszkowem przez e-mail i telefon latem i jesienią 2000 roku. Zgodzili się na spotkanie twarzą w twarz i obaj polecili do Seattle udając się na dwógodzinne "rozmowy kwalifikacyjne" z tajnymi agentami FBI, udającymi pracowników Invity. Rosjanie zostali poproszeni o

zaprezentowanie swoich umiejętności hackerskich na IBM Thinkpadzie dostarczonym przez agentów. Hackerzy komunikowali się ze swoim domowym serwerem w Czelabińsku, nieświadomi, że na laptopie jakiego używali zainstalowany był program "sniffujący", który nagrywał każde naciśnięcie klawisza. Opisy agentów FBI po spotkaniu przedstawiają Iwanowa i Gorszkowa jako nie tylko błogo nieświadomych zbliżającego się aresztowania ale i zarozumiałych co do swoich umiejętności hackerskich. W pewnym momencie Gorszkow bez zająknięcia opisał szczegółowo jak on i Iwanow wymuszały pieniądze od dostawcy usług internetowych w USA po zhackowaniu jego serwerów, powiedział w pokoju z tajnymi agentami, że "FBI nie mogła ich dopaść w Rosji"

28 Październik: Po 9 milionach prób złamania zabezpieczeń strony AntiOnline, zostały złamane przez australijskiego hakera 'ronln' ('nlnor'). AntiOnline został uznany za "niełamliwy" przez właściciela strony, Johna Vranesevicha, ale słaby skrypt(y) CGI napisany przez Vranesevicha doprowadziły do włamań

7 Listopad: 19 letni holenderski hacker 'Dimitri' włamał się do wewnętrznych serwerów Microsoft z intencją pokazania firmie jej słabości ze względu na instalowanie ich własnych poprawek

13 Grudnia: Więcej niż 55 000 numerów zostało skradzionych z Creditscard.com, który przetwarza transakcje kredytowe dla firm online. Około 25000 z nich zostały umieszczone w Internecie.

24 Grudzień: Exigent International, wykonawca rządu USA przyznał, że jeden lub więcej cyberzłodziei włamał się do ograniczonego, federalnego systemu komputerowego i ukradł z firmy kod sterowania systemami satelitarnymi. Oprogramowanie to jako OS/COMET, pozwala personelowi naziemnemu komunikowanie i wysyłania poleceń do stelitów i rakiet. Siły Powietrzne USA planowały użyć oprogramowania OS/COMET do sterowania NAVSTAR Global Positioning System z Colorado Springs Monitor Station, która jest częścią Sił Powietrznych

[2001]

1 Luty: Hackerzy atakują World Economic Forum naruszając dane zawierające numery kart kredytowych osobiste numery komórek, informacje dotyczące paszportów i organizacji podróży dla wielu rządów i liderów biznesu. Wśród znanych ofiar by szef Microsoftu Bill Gates, Jaser arafat, sekretarz generalny ONZ Kofi Anan, Madeline Albright i były premier Izraela Szymon Preses

12 Luty: Wirus Anna Kournikova wydany przez 20 letniego Holendra Jana de Wit ('OnTheFly'), który został potem

aresztowany i skazany na 150 godzin prac społecznych

1 Marzec: FBI informuje , że 40 stron e-commerce znajdujących się w 20 stanach USA zostało złamanych przez hackerów z Europy Wschodniej, kradnąc więcej niż milion numerów kart kredytowych z e-commerce USA i stron bankowych

7 Marzec: Jesus Oquendo ('Sil'), 27 lat, z Queens , Nowy Jork został oskarżony i skazany na 27 miesięcy w sądzie federalnym na Manhattanie pod zarzutem piractwa komputerowego i elektronicznego podsłuchu firmy Five Partners Asset Management LLC, spółki venture capital z Manhattanu. Oquedo zostawił swojej ofierze wiadomość : "Wtaj, właśnie włamałem się do twojego systemu. Życzę miłego dnia"

1 Maj: Chińscy i amerykańscy atakują się wzajemnie po tym jak amerykański samolot szpieowski musiał dokonać awaryjnego lądowania w Chinach po zderzeniu z samolotem i zabiciem chińskiego pilota myśliwca Wang Wei

4 Maj: Gibson Research Corp Security zaatakowany przez 13 letniego hackera.

11 Maj: Robak Solaris/IIS infekuje Solarisy do wersji 7, potem skanuje komputery IIS podatne na usterki dostępu do folderu, następnie zastępuje stronę domyślną

15 Maj: Hackerzy atakują Uniwersytet Waszyngtoński i umieszczają program do wymiany plików na swoich komputerach

17 Maj: Hacker 'Fluffy Bunny' atakuje Apache.org i SourceForge.net

21 Maj: Max Butler ('Max Vision' i 'The Equalizer') zostaje skazany na 18 miesięcy więzienia za uruchomienie robaka internetowego który pełzał po setkach wojskowych i obronnych komputerów przez parę dni 1998 roku. Max Butler miał też trzy życia. Jako 'Max Vision' był niezwykle wykwalifikowanym hackerem i ekspertem ds bezpieczeństwa, który chwalił się , że nigdy nie spotkał systemu informatycznego , którego nie mógł złamać. Jako 'The Equalizer' był informatorem FBI, raportującym o działalności innych hackerów. Jako Max Butler rodzinny człowiek z Santa Clara w Kalifornii, prowadził firmę z branży zabezpieczeń w Silicon Valley. Max Vision Network Security specjalizowała się w "testach penetracyjnych", próbach włamań do sieci korporacyjnych aby udowodnić , że ich bezpieczeństwo nie jest tak dobre jak mogłoby być.

9 Czerwiec: Los Angeles Times raportuje , że hackerzy

zaatakowali system komputerowy, który kontroluje większość przepływu energii elektrycznej w Kalifornii.

15 Czerwiec: Christine Gunhus, żona senatora USA, nie przyznała się do użycia pseudonimu do wysłania wiadomości e-mail , który dyskredytował demokratycznego rywala jej męża

20 Czerwiec: Amerykańska firma ZixIt raportuje , że baza danych zawierająca szczegóły kart kredytowych klientów została zhackowana

12 Lipiec: Znana grupa hackerska World of Hell w ciągu minuty zniszczyło 679 stron internetowych.

17 Lipiec: Robak Code Rod udostępniony. Robak wykorzystywał słabości w IIS Microsoftu.

16 Lipiec: 27 letni rosyjski programista Dimitrij Skljarow aresztowany na Def Con 9 za stworzenie programu kopiującego elektroniczne książki Adobe. Został oskarżony za naruszenie Digital Millennium Copyright Act.

21 Sierpień: Z waszyngtońskiego banku Riggs skradziona baza danych Visy

18 Wrzesień: Robak Nimda (admin od tyłu) zaczyna się rozprzestrzeniać, infekując serwery Microsoft IIS, które są otwarte dka znanych luk w oprogramowaniu

20 Listopad: Hackerzy mają dostęp do danych kart kredytowych Playboy.com. Grupa hackerska 'ingreslock 1524' wzięła to na siebie.

20 Listopad: 25 stron internetowych kościołów zhackowała grupa Hacking for Satan

8 Grudnia: Prokuratorzy oskarżają pracownika Los Alamos National Laboratory Jerome'a Heckenkampa o włamanie do firmy Qualcomm i innych systemów komputerowych kiedy był studentem. Heckenkamp, jak mówili nazywał się 'MagicFX'. Kiedy policja zapytała go o hasło do komputera, zachichotał i powiedział "Hackme". Jerome jest także podejrzany o włamanie do pół tuzina innych firm takich jak eBay Inc i E*Trade Inc, w okresie 9 miesięcy.

26 Listopad: 2 byłych księgowych Cisco skazano na 34 miesięcy za włamanie do komputerów firmy i kradzieże

[2002]

25 Luty: 17 letnia hackerka z Belgii, nazywająca się "Gigabyte" pisze pierwszy wirus "Sharpei", napisany w najnowszym języku programowania Microsoft, C# (C sharp)

11 Lipiec: Hackerzy włamali się na stronę "USA Today" i zastąpili kilka wiadomości sfałszowanymi historiami. Podejrzenie padło na izraelskich hackerów.

25 Lipiec: Urzędnicy Uniwersytetu Princeton przyznali się do uzyskania nieautoryzowanego dostępu do strony internetowej Uniwersytetu Yale zawierającą dane osobowe kandydatów do szkoły Ivy League

30 Lipiec: Kopie OpenSSH są zarażone złośliwym oprogramowaniem. OpenSSH jest popularną, darmową wersją pakietu komunikacji SSH (Secure Shell) i jest używane jak bezpieczny zamiennik dla protokołów takich jak Telnet, Rlogin, Rsh i FTP. Główny mirror OpenBSD (ftp.openbsd.org) został naruszony, jak zauważono, że suma kontrolna pakietu została zmieniona.

2 Sierpnia: Włoska policja aresztuje 14 podejrzanych hackerów, którzy są oskarżeni o tysiące włamań komputerowych, w tym ataki na armię i marynarkę amerykańską oraz NASA. Wszyscy byli członkami dwóch grup hackerskich, Mentor i Reservoir Dogs

17 Sierpień: Federalne organy ścigania szukały komputerów z San Diego firm zajmujących się bezpieczeństwem, które używały Internetu dla uzyskania dostępu do rządowych i komputerów bez autoryzacji przez całe lato. Śledczy z FBI, armii i NASA odwiedzili biura ForensicTec Solutions Inc szukając informacji na temat sposobu w jaki spółka uzyskała dostęp do komputerów w Fort Hood w Teksasie i Departamencie Energetyki, NASA i innych rządowych obiektów. Poszukiwania zaczęły się godzinę po stwierdzeniu, że konsultanci ForensicTec używając darmowego oprogramowania zidentyfikowali słabości komputerów a potem przejrzyli setki poufnych plików zawierających procedury wojskowe, e-maile, numery ubezpieczeń i danych finansowych, zgodnie z ewidencją firmową. Podczas gdy urzędnicy ForensicTec powiedzieli, że chcieli pomóc rządowi.

28 Sierpień: Zniszczono stronę Recording Industry Association of America (RIAA) i wgrane na serwer pliki mp3. RIAA wraz z Motion Picture Association of America (MPAA) zostały skrytykowane za ich dążenia do zamknięcia sieci takich jak Napster.

20 Września: Samir Rana ('Toner') 21 letni hacker z Londynu, zostaje aresztowany po trwającym rok śledztwie w sprawie stworzenia programu rootkit nazwany Tornkit pod Linux i podejrzanego o przynależności do niesławnej grupy Fluffy Bunny.

23 Września: 28 letni informatyk Stephen Carey z

Eastbourne, Sussex, został skazany na 18 miesięcy więzienia za włamanie do bazy danych firm i modyfikowanie informacji

4 Października: Hacker Wasilij Gorszkow, 27 lat, z Czelabińska w Rosji został skazany na trzy lata więzienia z 20 zarzutami udziału w spisku, oszustw i przestępstw związanych z komputerami. Gorszkow jest również obciążony kosztami prawie 700 000 dolarów strat spowodowanych w Speakeasy Network of Seattle, i firmy zajmującej się obsługą płatności kart kredytowych PayPal.

8 Październik: Doradczy CERT (Computer Emergency Response Team) wydał szczegóły odkrytych tylnych drzwi (koń trojański) znaleziony w plikach kodu źródłowego Sendmail 8.12.6

16 Październik: Microsoft przyznaje się, że został zaatakowany. Naruszenie bezpieczeństwa miało miejsce na serwerze, który udostępniał społeczności Microsoft wersje beta systemu Windows, który pozwalał 20 000 użytkowników przetestować oprogramowanie będące jeszcze w fazie rozwoju.

21 Październik: Atak Distributed Denial-of-Service (Dee-DOS), trwający godzinę, wysyłał zapory danych do 13 serwerów źródłowych DNS. Atak był w postaci ICMP flood, który został zablokowany przez wiele serwerów głównych, zapobiegając rzeczywistej stracie wydajności sieci.

12 Listopad: Gary McKinnon ('Solo'), 36 letni brytyjski bezrobotny administrator systemu został oskarżony o to co władze USA opisują jako "największe włamanie do wojskowych komputerów jakie kiedykolwiek odkryto. Od lutego 2001 do marca 2001 McKinnon rzekomo wykorzystał słabo zabezpieczone systemy Windows do ataku na 92 sieci prowadzone przez NASA, Pentagon i 12 innych insatałcji wojskowych rozsianych po 14 stanach. Prywatny sektor firm również odczuł rzekome ataki, co spowodowało straty w wysokości 900 000 dolarów. Prokuratorzy stwierdzili, że McKinnon "kradł hasła, usuwał pliki, monitorował ruch i wyłączał komputery w sieci baz wojskowych od Pearl Harbour po Connecticut"

22 Listopad: Lisa Chen 52 letnia kobieta z Tajwanu nie przyznała się do jednego z największych przypadków piractwa oprogramowania w USA, została skazana na 9 lat więzienia, jeden z najdłuższych wyroków związanych z piractwem komputerowym. Chen została aresztowana wraz z trzema współpracownikami w listopadzie 2001 roku, kiedy lokalny szeryf zajął setki tysięcy kopii pirackiego oprogramowania o wartości ponad 75 milionów dolarów, oprogramowanie które Chen przemycała z Tajwanu.

17 Grudnia: Ława przysięgłych uniewinniła ElcomSoft, rosyjskiego producenta oprogramowania, od kryminalnych zarzutów związanych z naruszeniem praw autorskich przy sprzedaży programu, który mógł łamać zabezpieczenia antypirackie na książkach elektronicznych. Sprawa przeciwko ElcomSoft uważana jest za ważny sprawdzian przepisów karnych ustawy Digital Millennium Copyright Act (DMCA), kontrowersyjnej ustawy mającej na celu rozszerzenie ochrony praw autorskich w epoce cyfrowej.

[2003]

21 Styczeń: Kevin Mitnick wchodzi w tryb online po raz pierwszy od prawie dziesięciu lat. Dostał się do więzienia na prawie pięć lat za przestępstwa komputerowe przeciwko firmom takim jak Sun Microsystems i Motorola. Po więzieniu trzy i pół roku miał ograniczony dostęp do komputerów i Internetu.

21 Styczeń: Simon Vallor, 22 letni brytyjski projektant sieci został skazany na dwa lata więzienia za napisanie jednego z najabrdziej destrukcyjnych wirusów, który wymazywały komputery na całym świecie. Vallor był autorem 3 wirusów - 'Gokar', 'Redesi' i 'Admirer'.

6 Luty: Douglas Bourdeau, lat 21, rzekomo zainstalował oprogramowanie monitorujące klawiaturę na ponad 100 komputerach w Boston College na następnie obserwował jak tysiące ludzi wysyłało e-maile, ściągało pliki, i bankowało online. Został potem oskarżony o umieszczenie oprogramowania na dziesiątkach komputerów, co pozwoliło mu potajemnie moitorować to co ludzie piszą, a potem ukradł około 2000 dolarów na podstawie zebranych informacji

7 Luty: Dwóch hackerów, którzy włamali się do Riverside County w Kalifornii. Zarówno William Grace, 22 lata i Brandon Wilson, 28 lat, skazano na dziewięć lat więzienia po przyznaniu się do 72 nielegalnych wejść do systemów komputerowych i edytowania danych, wraz z siedmioma zarzutami udziału w spisku w celu popełnienia wymuszenia.

10 Luty: Dwa razy w ciągu ostatnich dwóch tygodni, wandalę online - jak ci którzy dodali do wielu sieci WWW z graffiti "Free Kevin!" podczas pobytu Mitnicka w więzieniu, włamali się do serwera sieci WWW Defensive Thinking

18 Luty: Podano wiadomości, że hacker ('nieuprawniony intruz') uzyskał dostęp do 8 milionów numerów kart kredytowych na kontach Visy, MasterCard i American Express - przez naruszenie bezpieczeństwa firmy, która przetwarzała transakcje dla kupców.

7 Marzec: Napastnicy online ukradli informacje o ponad 55

000 studentów i wykładowców z niezabezpieczonych serwerów baz danych Uniwersytetu Tekszańskiego w Austin

29 Kwietnia: New Scotland Yard poinformował w środę , że aresztowała 24 letniego Lynna Htuna w Londynie, na konwencji InfoSecurity Europe 2003. Organy ścigania i internetowe służby bezpieczeństwa powiedziały, że wierzą , że Htun jest mózgiem 'Fluffi Bunni' wykorzystującym hacking, włamując się na strony McDonalds Corp, specjalistów zabezpieczeń internetowych SANS Institute i Symantec Corp jako grupy SecurityFocus.

12 Czerwca: Projektant stron 24 letni John Racine II, przyznał , że przekierowywał ruch i e-maile ze strony arabskiej al-Jazeera na stronę którą zaprojektował i nazwał "Let Freedom Ring" i nosząca flagę amerykańską. John przeprowadził ten atak na al-Jazeerę w sieci podczas wojny w Iraku, ponieważ telewizja arabska pokazała zdjęcia zabitych i pojmanych amerykańskich żołnierzy

6 Lipiec: Internetowi eksperci przygotowują się na zawody hackerskie. Atak jest zapowiadany jako konkurs na to kto może zniszczyć 6000 stron WWW w sześć godzin. Szeroko nagłośniony konkurs zachęcający do niszczenia stron zakończył się bez poważniejszych problemów