# The Complete History of Hacking

Maybe not the **complete** history but a valid attempt. A complete hacker history will never be obtainable since so much of the history is fragmented, unfounded and unreported.This will not be a complete list but a work in progress.

## 1960s

[1960 Nov] Telephone calls are switched for the first time by computer.

[1963] Dartmouth College, located in Hanover, New Hampshire, incorporates the introduction to the use of computers as a regular part of the Liberal Arts program.

[1963] ASCII (American Standard Code for Information Interchange) is created, permitting machines from different manufacturers to exchange data. ASCII consists of 128 unique strings of ones and zeros.

[1964] There are approximately 18,200 computer systems in the United States. Over 70% of those computers were manufactured by International Business Machines (IBM).

[1964] Thomas Kurtz and John Kemeny created BASIC (Beginner's All-Purpose Symbolic Instruction Code), an easy-to-learn programming language, for their students at Dartmouth College.

[1967] The Advanced Research Projects Agency (ARPA) work with U.S. computer experts to form a network of Interface Message Processors (IMPS). The computers would act as gateways to mainframes at a variety of institutions in the United States and provide a major part of what would become the Internet in the years ahead.

[1969] The Advanced Research Projects Agency (ARPA) originates ARPANET, a service designed to provide efficient ways to communicate for scientists. A Cambridge, Massachusetts consulting firm, Bolt Beranek and Newman, who won a ARPA contract to design and build a network of Interface Message Processors (IMPS) the year prior, ships (Sept) the first unit to UCLA and ships (Oct) the second unit to Stanford Research Institute. IMPS act as gateways to mainframes at a variety of institutions in the United States. Within a few days of delivery, the machine at UCLA and Stanford link up for the first time and ARPANET is founded. Later the network expands to four nodes. The first four nodes (networks) consisted of the, University of California Los Angeles, University of California Santa Barbara, University of Utah and the Stanford Research Institute. This system would evolve to be known as the Internet or the Information Super Highway.

[1969] Intel makes the announcement of a much larger RAM chip. It boasts of a 1KB capacity.

[1969] Ken L. Thompson, Dennis M. Ritchie and others start working on the UNIX operating system at Bell Labs (later AT&T). UNIX was designed with the goal of allowing several users to access the computer simultaneously.

[1969] The first computer hackers emerge at MIT. They borrow their name from a term to describe members of a model train group at the school who "hack" the electric trains, tracks, and switches to make them perform faster and differently. A few of the members transfer their curiosity and rigging skills to the new mainframe computing systems being studied and developed on campus.

[1969] Joe Engressia ('The Whistler', 'Joybubbles' and 'High Rise Joe') considered the father of phreaking. Joe, who is blind, was a mathematics student at USF in the late 1960s when he discovered that he could whistle into a pay telephone the precise pitch --the 2600-cycle note, close to a high A-- that would trip phone circuits and allow him to make long-distance calls at no cost.

## 1970s

[1970] An estimated 100,000 computer systems are in use in the United States.

[1970] Digital Equipment Corporation (DEC) introduces the famous PDP-11, which is considered to be one of the best designed minicomputers ever, and many of the machines are still used today. Some of the best computer hackers in the world cut their teeth on -11's.

[1971] The first personal computer, the Kenback, is advertised in the September issue of Scientific American.

[1971] John Draper ('Cap'n Crunch') learns that a toy whistle given away inside Cap'n Crunch cereal generates a 2600-hertz signal, the same high-pitched tone that accesses AT&T's long-distance switching system. Draper builds a blue box that, when used in conjunction with the whistle and sounded into a phone receiver, allows phreakers to make free calls.

[1971] Esquire magazine publishes Secrets of the Little Blue Box with instructions for making a blue box, and wire fraud in the United States escalates. Among the perpetrators: college kids Steve Wozniak and Steve Jobs, future founders of Apple Computer, who launch a home industry making and selling blue boxes.

[1971] First e-mail program written by Ray Tomlinson and used on ARPANET which now has 64 nodes. Tomlinson of Bolt Beranek and Newman, contracted by the Advanced Research Projects Agency (ARPA) to create the ARPANET, selects the @ symbol to separate user names in e-mail as the first e-mail messages are sent between computers.

[1972 May] John Draper arrested for phone phreaking and sentenced to four months in California's Lompoc prison.

[1973] Intel's chairman, Gordon Moore, publicly reveals the prophecy that the number of transistors on a microchip will double every year and a half. Moore's Law will hold true for more than twenty years.

[1975] About 13,000 cash dispensing Automatic Teller Machines (ATM) are installed.

[1975] Atari, Inc.'s home version of PONG begins selling at 900 Sears and Roebuck stores under the Sears' Telegames brand.

[1975 Aug] William Henry Gates, III (Bill Gates) and Paul Allen found Microsoft.

[1976] David R. Boggs and Robert M. Metcalfe invent Ethernet at Xerox in Palo Alto, California.

[1976 Apr] Stephen Wozniak, Steven Paul Jobs and Ron Wayne sign an agreement that founds Apple Computer on April 1.

[1977 Aug 3] The TRS-80 ('Trash-80') Model I offered to the public and becomes the first desktop computer.

[1977 Dec] The Atari 2600 is selling for $199.95 and includes one game and two controllers.

[1978] Bill Joy produces first Berkeley Software Distribution (BSD) of UNIX.

[1978] There are an estimated 5,000 desktop computers in use within the United States.

[1978] Kevin David Mitnick ('Condor') meets phone phreak Lewis De Payne ('Roscoe') of Roscoe gang while harassing a HAM radio operator on the air in Southern California.

[1979] The C Programming Language by Brian W. Kernighan and Dennis M. Ritchie is published.

[1979 Jun] The Apple II+ with 48K RAM and a new "auto-start" ROM is introduced by Apple Computer for $1,195.

## 1980s

[1980] There is an estimated 350,000 computer terminals "networked" with larger "host" computers.

[1980] Nintendo, Ltd. releases Donkey Kong as a coin-operated arcade game.

[1980] Usenet is born, networking UNIX machines over slow phone lines. Usenet eventually overruns ARPANET as the virtual bulletin board of choice for the emerging hacker nation.

[1980 Dec] Roscoe Gang, including Kevin Mitnick, invade computer system at US Leasing.

[1981] Kenji Urada, 37, becomes the first reported death caused by a robot. A self-propelled robotic cart crushed him as he was trying to repair it in a Japanese factory. :-)

[1981] Commodore Business Machines starts shipping the VIC-20 home computer. It features a 6502 microprocessor, 8 colors and a 61-key keyboard. Screen columns are limited to 22 characters. The product is manufactured in West Germany and sells in the U.S. for just under $300.

[1981 Jul] Microsoft acquires complete rights to Seattle Computer Product's DOS and names it MS-DOS.

[1981] Ian Murphy ('Captain Zap') was the first hacker to be tried and convicted as a felon. Murphy broke into AT&T's computers and changed the internal clocks that metered billing rates. People were getting late-night discount rates when they called at midday.

[1981 May 23] Kevin Mitnick, 17, is arrested for stealing computer manuals from Pacific Bell's switching center in Los Angeles, California. He will be prosecuted as a juvenile and sentenced to probation.

[1981 May 28] First mention of Microsoft on Usenet.

[1982] There are an estimated 3 million computer terminals "networked" with larger "host" computers. Also, there are an estimated number of 5 million desktop computers in use within the United States. More than 100 companies make personal computers.

[1982] Sun Microsystems, Inc. is founded by four 27-year-old men; Andreas von Bechtolsheim, Vinod Khosla, Scott McNealy and Bill Joy.

[1982] As hacker culture begins to erode, losing some of its brightest minds to commercial PC and software start-ups, Richard Stallman starts to develop a free clone of UNIX, written in C, that he calls GNU (for Gnu's Not Unix).

[1982] Lewis De Payne ('Roscoe') pleas guilty to conspiracy and fraud. Sentence: 150 days in jail. Accomplice gets

thirty. Mitnick gets ninety day diagnostic study by juvenile justice system, plus a year probation.

[1982] Kevin Mitnick cracks Pacific Telephone system and TRW; destroys data.

[1982] William Gibson coins term "cyberspace."

[1982] '414 Gang' phreakers raided. '414 Private' BBS was where the '414 Gang' would exchange information while breaking into systems of Sloan-Kettering Cancer Center and Los Alamos military computers.

[1982 Aug] Commodore ships the Commodore 64 computer and enters more than one million homes during this first year. The C-64 was the first home computer with a standard 64K RAM. With an suggested retail price of $595, it was considered a huge value. It included a keyboard, CPU, graphics and sound chips.

[1982 Sep 19] Scott E. Fahlman typed the first on-line smiley, :-)

[1983] The Internet is formed when ARPANET is split into military and civilian sections.

[1983] The movie WarGames is released, Matthew Broderick plays a computer whiz kid who inadvertently initiates the countdown to World War III.

[1983] Plovernet BBS (Bulletin Board System) was a powerful East Coast pirate board that operated in both New York and Florida. Owned and operated by teenage hacker 'Quasi Moto', Plovernet attracted five hundred eager users in 1983. Eric Corley ('Emmanuel Goldstein') was one-time co-sysop of Plovernet, along with 'Lex Luthor', who would later found the phreaker/hacker group, Legion of Doom.

[1983 Sep 22] Kevin Poulsen ('Dark Dante') and Ron Austin are arrested for breaking into the ARPANET. At 17 Poulsen is not prosecuted and Austin receives 3 years probation.

[1983 Sep 27] Richard Stallman makes the first Usenet announcement about GNU.

[1983 Nov 12] First mention of Microsoft Windows on Usenet.

[1984] Andrew Tanenbaum writes the first version of Minix, a UNIX intended for educational purposes. Minix later gave Linus Torvalds the inspiration to start writing Linux.

[1984] The University of California at Berkeley released version 4.2BSD which included a complete implementation of the TCP/IP networking protocols. Systems based on this and later BSD releases provided a multi-vendor networking capability based on Ethernet networking.

[1984] Bill Landreth ('The Cracker') is convicted of breaking into some of the most secure computer systems in the United States, including GTE Telemail's electronic mail network, where he peeped at NASA Department of Defense computer correspondence. In 1987 Bill violated his probation and was back in jail finishing his sentence. Bill also authored an interesting read titled 'Out of the Inner Circle'.

[1984] Legion of Doom formed. Legion of Doom, a hacker group which operated in the United States in the late 1980's. The group's wide ranging activities included diversion of telephone networks, copying proprietary information from companies and distributing hacking tutorials. Members included: 'Lex Luther' (founder), 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 RNOC', 'Carrier Culprit', 'Master of Impact', 'Phantom Phreaker', 'Doom Prophet', 'Thomas Covenant', 'Phase Jitter', 'Prime Suspect', 'Skinny Puppy' and 'Professor Falken'.

[1984] 2600: The Hacker Quarterly founded by Eric Corley ('Emmanuel Goldstein').

[1984 Jun 19] The X Window System is released by Robert W. Scheifler.

[1985] Hacker 'zine Phrack is first published by Craig Neidorf ('Knight Lightning') and Randy Tischler ('Taran King').

[1985 May 24] Date of incorporation under original founding name, Quantum Computer Services (America Online).

[1986] The Congress passes Computer Fraud and Abuse Act. The law, however, does not cover juveniles.

[1986] The german hacker group, Chaos Computer Club, hacked information about the german Nuclear Power Program from government computers during the Chernobyl crisis.

[1986 Jan 8] Legion of Doom/H member Loyd Blankenship ('The Mentor') is arrested around this time. He publishes a now-famous treatise that comes to be known as the Hacker's Manifesto.

[1986 Feb 26] The Phoenix Fortress BBS issues warrants for the arrest and confiscation of the equpment of 7 local users in Fremont, CA. The Sysop turns out to be a local law enforcement agent and the Phoenix Fortress created to catch hackers and software pirates.

[1986 Sep 1] An unknown suspect or group of suspects using the code name Pink Floyd repeatedly accessed the UNIX and Portia computer systems at Stanford University without authorization. Damage was estimated at $10,000.

[1986 Aug] In August, while following up a 75 cent accounting error in the computer logs at the Lawrence Berkeley Lab at the University of California, Berkeley, network manager Clifford Stoll uncovers evidence of hackers at work. A year-

long investigation results in the arrest of the five german hackers responsible.

[1987 Sep 14] It's disclosed publicly that young german computer hackers calling themselves the Data Travellers, managed to break into NASA network computers and other world-wide top secret computer installations.

[1987 Nov 23] Chaos Computer Club hacks NASA's SPAN network.

[1987 Dec] Kevin Mitnick invades systems at Santa Cruz Operation. Mitnick sentenced to probabtion for stealing software from SCO, after he cooperates by telling SCO engineers how he got into their systems.

[1988 Jun] The U.S. Secret Service (USSS) secretly videotapes the SummerCon hacker convention.

[1988 Nov 2] Robert T. Morris, Jr., a graduate student at Cornell University and son of a chief scientist at a division of the National Security Agency (NSA), launches a self-replicating worm on the government's ARPANET (precursor to the Internet) to test its effect on UNIX systems. The worm gets out of hand and spreads to some 6,000 networked computers, clogging government and university systems. Morris is dismissed from Cornell, sentenced to three years probation and fined $10,000.

[1988 Nov 3] First mention of the Morris worm on Usenet.

[1988 Dec] Legion of Doom hacker Robert Riggs ('The Prophet') cracks BellSouth AIMSX computer network and downloads E911 document (describes how the 911 emergency phone system works). Riggs sends a copy to Phrack editor Craig Neidorf ('Knight Lightning'). Both Craig and Robert are raided by Federal authorities and later indicted. The indictment said the "computerized text file" was worth $79,449, and a BellSouth security official testified at trial it was worth $24,639. The trial began on July 23, 1990 but the proceedings unexpectedly ended when the government asked the court to dismiss all the charges when it was discovered that the public could call a toll-free number and purchase the same E911 document for less than $20.

[1988 Dec 16] 25-year-old computer hacker Kevin Mitnick is held without bail on charges that include stealing $1 million in software from DEC (Digital Equipment Corporation), including VMS source code, and causing that firm $4 million in damages.

[1989] 22-year-old computer hacker and ex-LOD member Corey Lindsly ('Mark Tabas') pleaded guilty to felony charges relating to using a computer to access US West's system illegally, which resulted in five years probation. [see also 1995 Feb. 'Phonemasters']

[1989] At the Cern laboratory for research in high-energy physics in Geneva, Tim Berners-Lee and Robert Cailliau develop the protocols that will become the world wide web.

[1989 Jan 23] Herbert Zinn ('Shadowhawk'), a high school dropout, was the first to be convicted (as a juvenile) under the Computer Fraud and Abuse Act of 1986. Zinn was 16 when he managed to break into AT&T and Department of Defense systems. He was convicted on January 23, 1989, of destroying $174,000 worth of files, copying programs valued at millions of dollars, and publishing passwords and instructions on how to violate computer security systems. Zinn was sentenced to nine months in prison and fined $10,000.

[1989 May] A task force in Chicago raids and arrests an alleged computer hacker known as 'Kyrie'.

[1989 Jun] An underground group of hackers known as the NuPrometheus League distributes proprietary software illegally obtained from Apple Computer.

[1989 Jul 21] Known as the "Atlanta Three" case, 3 members of the LOD/H (Legion of Doom) where charged with hacking into Bell South's Telephone (including 911) Networks - possessing proprietary BellSouth software and information, unauthorized intrusion, illegal possession of phone credit card numbers with intent to defraud, and conspiracy. The three hackers where: Franklin Darden ('The Leftist'), Adam Grant ('The Urvile' and 'Necron 99'), Robert Riggs ('The Prophet').

[1989 Jun 22] 'Fry Guy', a 16-year-old in Elmwood, Indiana cracks into McDonald's mainframe on the Sprint Telenet system. One act involved the young hacker altering phone switches so that calls to a Florida county probation department would ring at a New York phone-sex line answered by "Tina." On September 14 1990, he was sentenced to forty-four months probation and four hundred hours community service.

---

## 1990s

---

[1990] Electronic Frontier Foundation is formed by Mitch Kapor and John Perry Barlow in part to defend the rights of those investigated for alleged computer hacking.

[1990] Kevin Poulsen's now-infamous incident with KIIS-FM in Los Angeles. In 1990 the station ran the "Win a Porsche by Friday" contest, with a $50,000 Porsche given to the 102nd caller. Kevin and his associates, stationed at their computers, seized control of the station's 25 telephone lines, blocking out all calls but their own. Then he dialed the 102nd call -- and later collected his Porsche 944.

[1990 Jan 15] AT&T's long-distance telephone switching system crashed. During the nine long hours of frantic effort that it took to restore service, some seventy million telephone calls went uncompleted. Hackers where first suspected of causing the crash but later AT&T engineers discovered the "culprit" was a bug in AT&T's own software.

[1990 Jan 18] Chicago task force raids an alleged computer hacker Craig Neidorf ('Knight Lightning') in St. Louis.

[1990 Feb] U.S. Secret Service raid an alleged computer hacker Len Rose ('Terminus') in Maryland. Len somehow got his hands on System V 3.2 AT&T Unix Source Code, including the source login.c

[1990 Feb 21] Chicago Task Force raids the home of Robert Izenberg, an alleged computer hacker in Austin.

[1990 Mar 1] Chicago task force raids Steve Jackson Games, Inc. Reportedly, workers Loyd Blankenship ('The Mentor') and Chris Goggans ('Erik Bloodaxe'), had ties to a hacker group (LOD) that the Justice Department was investigating. Finding a rulebook to a game called G.U.R.P.S. CYBERPUNK, raiders interpreted the findings as a tutorial on computer hacking and proceeded to seize equipment and documents found at the site. Steve Jackson Games, Inc. prevailed in an ensuing legal battle, however their equipment was never returned in its entirety.

[1990 May 7] May 7 through Wednesday, May 9, the United States Secret Service and the Arizona Organized Crime and Racketeering Bureau implement Operation Sundevil computer hacker raids in Cincinnati, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose and San Francisco.

[1990 Mar 7] A 24 year-old Denver man, Richard G. Wittman Jr., has admitted breaking into a NASA computer system. In a plea bargain, Wittman plead guilty to a single count of altering information - a password inside a federal computer.

[1990 Apr] Between April 1990 and May 1991, computer hackers from the Netherlands penetrated 34 DOD sites. At many of the sites, the hackers had access to unclassified, sensitive information on such topics as military personnel--personnel performance reports, travel information, and personnel reductions; logistics--descriptions of the type and quantity of equipment being moved; and weapons systems development data.

[1990 May] At least four British clearing banks are being blackmailed by a mysterious group of computer hackers who have broken into their central computer systems. The hackers demanded substantial sums of money in return for showing the banks how their systems where penetrated. One computer expert described their level of expertise and knowledge of the clearing bank computer systems as "truly frightening".

[1991] The Internet, having been established to link the military and educational institutions banned access to businesses. That ban is lifted this year.

[1991] Rumors circulate about the Michelangelo virus, a program expected to crash computers on March 6, 1992, the artist's 517th birthday. Doomsday passes without much incident.

[1991 Feb] DOS version of AOL released.

[1991 Apr 11] Kevin Poulsen ('Dark Dante') arrested for breaking into Pacific Bell phone systems.

[1991 Jul] Justin Petersen ('Agent Steal' and 'Eric Heinz') arrested for breaking into TRW, stealing credit cards.

[1991 Aug 6] Tim Berners-Lee's Usenet announcement of the World Wide Web project.

[1991 Sep] Justin Petersen released from prison to help FBI track hacker Kevin Mitnick.

[1991 Sep 17] Linus Torvalds publicly releases Linux version 0.01. While a computer science student at the University of Helsinki Linus created the Linux operating. Linus originally named his operating system Freax.

[1991 Oct 5] Linus Torvalds decides to announce the availability of a free minix-like kernel called Linux on Usenet.

[1992] Masters of Deception (MOD) phone phreakers busted via wiretaps.

[1992] Morty Rosenfeld convicted after hacking into TRW, stealing credit card numbers and selling credit reports.

[1992 Jan 29] Minix creator, Andy Tanenbaum, posts the infamous LINUX is obsolete newsgroup posting on comp.os.minix. Later, Linux creator Linus Torvalds quickly responds to the posting.

[1992 Nov] Kevin Mitnick cracks into California Department of Motor Vehicles.

[1993 Mar 1] Microsoft releases Windows NT.

[1993 Jun] Slackware, by Patrick Volkerding, becomes the first commercial standalone distribution of Linux.

[1993 Jul 9] The first Def Con hacking conference takes place in Las Vegas. The conference is meant to be a one-time party to say good-bye to BBSs (now replaced by the Web), but the gathering is so popular it becomes an annual event.

[1993 Aug] Justin Petersen arrested for stealing computer access equipment.

[1993 Oct 28] Randal Schwartz uses Crack at Intel to crack passwords, later found guilty under an Oregon computer crime law, and sentenced.

[1993 Dec] FreeBSD version 1.0 is released.

[1994] Red Hat is founded.

[1994] Linux 1.0 is released.

[1994 Jan 12] Mark Abene ('Phiber Optik') starts his one year sentence. As a founding member of the Masters of Deception, Mark inspired thousands of teenagers around the country to "study" the internal workings of our nation's phone system. A federal judge attempted to "send a message" to other hackers by sentencing Mark to a year in federal prison, but the message got garbled: Hundreds of well-wishers attended a welcome-home party in Mark's honor at a Manhattan Club. Soon after, New York magazine dubbed him one of the city's 100 smartest people. Other MOD

members: Elias Ladopoulos ('Acid Phreak'), Paul Stira ('Scorpion'), John Lee ('Corrupt'), Allen Wilson ('Wing'), 'The Seeker', 'HAC', 'Red Knight', 'Lord Micro' and Julio Fernandez ('Outlaw').

[1994 Mar 23] 16-year-old music student Richard Pryce ('Datastream Cowboy') is arrested and charged with breaking into hundreds of computers including those at the Griffiths Air Force base, NASA and the Korean Atomic Research Institute. The Times of London reported that knowing he was about to be arrested, Richard "curled up on the floor and cried." Pryce later pled guilty to 12 hacking offenses and fined $1,800. Later, Matthew Bevan ('Kuji'), mentor to Pryce was finally tracked down and arrested. The charges against Bevan were later dropped and now he works as a computer security consultant.

[1994 Jun 13] Vladimir Levin, a 23-year-old, led a Russian hacker group in the first publicly revealed international bank robbery over a network. Stealing around 10 million dollars from Citibank, which claims to have recovered all but $400,000 of the money. Levin was later caught and sentenced to 3 years in prison.

[1994 Aug] Justin Petersen electronically steals $150k from Heller Financial.

[1994 Sep] Netcom's (bought by MindSpring, MindSpring then bought by Earthlink) credit card database was on-line and accessible to the unauthorized.

[1994 Dec 25] Kevin Mitnick (supposedly) cracks into Tsutomu Shimomura's computers. Mitnick was first suspected of hacking into Tsutomu's computers in 1994 but an unknown Israeli hacker (friend to Mitnick) was later suspected. The Israeli hacker was thought to be looking for the Oki cell phone disassembler written by Shimomura and wanted by Mitnick.

[1995 Jan 27] Kevin Mitnick cracks into the Well; puts Shimomura's files and Netcom (bought by MindSpring, MindSpring then bought by Earthlink) credit card numbers there.

[1995 Feb] Ex-LOD member, Corey Lindsly ('Mark Tabas') was the major ringleader in a computer hacker organization, known as the 'Phonemasters', whose ultimate goal was to own the telecommunications infrastructure from coast-to-coast. The group penetrated the systems of AT&T, British Telecom., GTE, MCI WorldCom, Sprint, Southwestern Bell and systems owned by state and federal governmental agencies, to include the National Crime Information Center (NCIC) computer. They broke into credit-reporting databases belonging to Equifax Inc. and TRW Inc. They entered Nexis/Lexis databases and systems of Dun & Bradstreet. They had access to portions of the national power grid, air-traffic-control systems and had hacked their way into a digital cache of unpublished phone numbers at the White House. A federal court granted the FBI permission to use the first ever "data tap" to monitor the hacker's activities. These hackers organized their assaults on the computers through teleconferencing and utilized the encryption program PGP to hide the data which they traded with each other. On Sep. 16 1999 Corey Lindsly, age 32, of Portland, Oregon, was sentenced to forty-one months imprisonment and ordered to pay $10,000 to the victim corporations. Other 'Phonemasters' members: John Bosanac ('Gatsby') from San Diego, Calvin Cantrell ('Zibby') and Brian Jaynes both located in Dallas, Rudy Lombardi ('Bro') in Canada, Thomas Gurtler in Ohio. Calvin Cantrell, age 30, of Grand Prairie, Texas, was sentenced to two years imprisonment and ordered to pay $10,000 to the victim corporations. John Bosanac got 18 months.

[1995 Feb 15] Kevin Mitnick arrested and charged with obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions; and stealing, copying, and misappropriating proprietary computer software from Motorola, Fujitsu, Nokia, Sun, Novell, and NEC. Mitnick was also in possession of 20,000 credit card numbers.

[1995 Mar 18] SATAN (Security Administrator Tool for Analyzing Networks) security tool released to the Internet by Dan Farmer and Wietse Venema. The release stirs huge debate about security auditing tools being given to the public.

[1995 May 5] Chris Lamprecht ('Minor Threat') becomes 1st person banned from Internet. Chris was sentenced for a number of crimes to which he pled guilty. The crimes involved the theft and sale of Southwestern Bell circuit boards. In the early 1990s Chris wrote a program called ToneLoc (Tone Locator), a phone dialing program modeled on the program Matthew Broderick used in the movie WarGames to find open modem lines in telephone exchanges.

[1995 Aug 16] French student Damien Doligez cracks 40-bit RC4 encryption. The challenge presented the encrypted data of a Netscape session, using the default exportable mode, 40-bit RC4 encryption. Doligez broke the code in eight days using 112 workstations.

[1995 Sep 11] 22-year-old Golle Cushing ('Alpha Bits') arrested for selling credit card and cell phone info.

[1995 Sep 17] Ian Goldberg and David Wagner broke the pseudo-random number generator of Netscape Navigator 1.1. They get the session key in a few hours on a single workstation.

[1995 Nov 15] On November 15, Christopher Pile becomes the first person to be jailed for writing and distributing a computer virus. Pile, who called himself the 'Black Baron', was sentenced to 18 months in jail.

[1996] The internet now has over 16 million hosts and is growing rapidly.

[1996] Icanet, a company that designed Internet sites for public schools, was threatened by an extortionist in Germany. The deal: If Icanet agreed to buy his computer security program for $30,000, the hacker would not devastate the company's computers. In April, Andy Hendrata, a 27-year-old Indonesian computer science student in Germany, was convicted of computer sabotage and attempted extortion. He received a one-year suspended sentence and was fined $1,500.

[1996] The U.S. General Accounting Office reports that hackers attempted to break into Defense Department computer files some 250,000 times in 1995 alone. About 65 percent of the attempts were successful, according to the report.

[1996 Mar 6] United Press International (UPI) reveals that a hacker called 'u4ea' and also known as 'el8ite', 'eliteone',

'el8' and 'b1ff' on-line has been threatening to crash systems at the Boston Herald newspaper and several Internet Service providers in the Boston, Massachusetts area. Reports indicate that the hacker may have covertly entered up to 100 Internet sites and desytroyed files on many of them. An investigation is initiated by the NYPD Computer Crimes section.

[1996 Apr 4] According to prosecutors, 19-year-old Christopher Schanot of St. Louis, Missouri, hacked into national computer networks, military computers, and the TRW and Sprint credit reporting service.

[1996 Apr 5] 19-year-old Christopher Schanot ('N00gz') a St. Louis honor student indicted in Philadelphia for computer fraud, illegal wiretapping, unauthorized access to many corporate and government computers including Southwestern Bell, BELLCORE, Sprint, and SRI.

[1996 Apr 19] Hackers break into the NYPD's phone system and change the taped message that greeted callers. The new message said, "officers are too busy eating doughnuts and drinking coffee to answer the phones." It directed callers to dial 119 in an emergency.

[1996 Jul 5] First known Excel virus, called Laroux is found.

[1996 Jul 31] Tim Lloyd plants software time bomb at Omega Engineering in NJ; First federal computer sabotage case. The software time bomb destroyed the company's computer network and the global manufacturer's ability to manufacture in the summer of 1996. The attack caused the company $12 million in losses and cost 80 employees their jobs. Lloyd received 41 months in jail. He also was ordered to pay more than $2 million in restitution.

[1996 Aug 22] Eric Jenott, a Fort Bragg, NC paratrooper is accused of hacking U.S. Army systems and furnishing passwords to a citizen of communist China. Eric's attorney says the Fort Bragg soldier is just a computer hacker who tested the strength of a supposedly impenetrable computer system, found a weakness and then told his superiors about it. Eric was later cleared of the spy charges, but found guilty of damaging government property and computer fraud.

[1996 Sep] Johan Helsingius closes penet.fi. Penet.fi, the world's most popular anonymous remailer, was raided by the Finnish police in 1995 after the Church of Scientology complained that a penet.fi customer was posting the church's secrets on the Net. Helsingius closed the remailer after a Finnish court ruled he must reveal the customer's real e-mail address.

[1996 Sep 6] DoS attack against Panix.com, a New York-based ISP. An attacker used a single computer to send thousands of copies of a simple message that computers use to start a two-way dialog. The Panix machines receiving the messages had to allocate so much computer capacity to handle the dialogs that they used up their resources and were disabled.

[1996 Sep 25] Kevin Mitnick indicted for damaging computers at USC. Mitnick was charged with 14 counts of wire fraud, arising from his alleged theft of proprietary software from manufacturers. The charges also accuse him of damaging USC's computers and "stealing and compiling" numerous electronic files containing passwords.

[1997] AOHell is released, a freeware application that allows a burgeoning community of unskilled hackers -- or script kiddies -- to wreak havoc on America Online (AOL).

[1997 Jan 28] Ian Goldberg, a University of California-Berkeley graduate student, took on RSA Data Security's challenge and cracked the 40-bit code by linking together 250 idle workstations that allowed him to test 100 billion possible "keys" per hour. In three and a half hours Goldberg had decoded the message, which read, "This is why you should use a longer key."

[1997 Feb 5] Members of the Chaos Computer Club, the infamous hacking elite of Germany, demonstrated an ActiveX hacking program that allowed them to access copies of Quicken, the accounting software package from Intuit, and transfer money between bank accounts, without needing to enter the normal password security systems of Quicken.

[1997 Mar 10] Hacker named 'Jester' has the first federal charges brought against a juvenile for a computer crime. 'Jester' cuts off the FAA tower at Worcester Airport and sentenced to paying restitution to the telephone company and complete 250 hours of community service.

[1997 Apr 21] A hacker named 'Joka' managed to trick America Online to briefly shut down a site run by the Texas branch of the Ku Klux Klan, forcing the AOL to act, for security reasons, after it had declined to do so in response to widespread criticism that the site contains offensive material.

[1997 May 23] Carlos Felipe Salgado, Jr., 36, who used the on-line name 'Smak', allegedly inserted a sniffer program that gathered the credit information from a dozen companies selling products over the Internet. Carlos gathered 100,000 credit card numbers along with enough information to use them, said the FBI.

[1997 Jun] Netcom (bought by MindSpring, MindSpring then bought by Earthlink) voice-mail hacked by 'Mr Nobody'. The 15-year-old intruder claimed he has been inside Netcom's voice-mail for two years. There, he cracked into numerous mailboxes via his telephone key pad and used the system to break into third-party telephone switches to make long-distance calls.

[1997 Oct 31] Eugene Kashpureff arrested for redirecting the NSI web page to his Alternic web site. Kashpureff designed a corruption of the software system that allows Internet-linked computers to communicate with each other. By exploiting a weakness in that software, Kashpureff hijacked Internet users attempting to reach the web site for InterNIC, his chief commercial competitor, to his AlterNIC web site, impeding those users' ability to register web site domain names or to review InterNIC's popular "electronic directory" for existing domain names.

[1997 Dec] Julio Ardita ('El Griton') a 21 year old Argentinean was sentenced to a three-year probation for hacking into computer systems belonging to Harvard, NASA, Los Alamos National Laboratory and the Naval Command, Control and Ocean Surveillance Center.

[1997 Dec 8] www.yahoo.com is defaced by 'pantz' and 'h4gis'.

[1998] Two hackers, Hao Jinglong and Hao Jingwen (twin brothers) are sentenced to death by a court in China for breaking into a bank computer network and stealing 720,000 yuan ($87,000). The Yangzhou Intermediate People's Court in eastern Jiangsu province of China rejected an appeal of Hao Jingwen and upholding a death sentence against him. Jingwen and his brother, Hao Jinglong, hacked into the Industrial and Commercial Bank of China computers and shifted 720,000 yuan ($87,000) into accounts they had set up under phoney names. In September of 1998, they withdrew 260,000 yuan ($31,400) of those funds. Hao Jinglong's original sentence to death was suspended in return for his testimony.

[1998 Jan 1] Mark Abene ('Phiber Optik'), a security expert, launched a command to check a client's password files—and ended up broadcasting the instruction to thousands of computers worldwide. Many of the computers obligingly sent him their password files. Abene explained that the command was the result of a misconfigured system, and that he had no intention of generating a flood of password files into his mailbox.

[1998 Jan 16] Tallahassee Freenet hacked. TFN was attacked by a person or persons whose intent was clearly to destroy all of the files on the system. Before the attacks were stopped by bringing the system offline, thousands of user home directories, many system files, and all of the user spool mail had been deleted.

[1998 Feb 25] MIT Plasma & Fusion Center (PSFC) and DoD computers hacked by Ehud Tenebaum ('Analyzer'). The MIT computer was running an old version of Linux, the vulnerability which facilitated intrusion. After gaining access to an account, the hackers took advantage of other security holes and installed a packet-sniffer. The hackers were able to collect user names and passwords to computers outside the network.

[1998 Feb. 26] Solar Sunrise, a series of attacks targeting Pentagon computers, leads to the establishment of round-the-clock, online guard duty at major military computer sites.

[1998 Feb 27] The 56-bit DES-II-1 challenge by RSA Data Security was completed by a massively distributed array of computers coordinating their brute-force attacks via the distributed.net "organization." The cleartext message read, "Many hands make light work." The participants collectively examined 6.3 x 10^16 keys—fully 90 percent of the entire keyspace—in about 40 days.

[1998 Mar 3] Santa Rosa Internet Service Provider NetDex rehacked by Ehud Tenebaum ('Analyzer'), in retaliation over the arrest of his two U.S. hacker friends ('Cloverdale Two').

[1998 Mar 18] Ehud Tenebaum ('The Analyzer'), an Israeli teen-ager is arrested in Israel. During heightened tensions in the Persian Gulf, hackers touch off a string of break-ins to unclassified Pentagon computers and steal software programs. Officials suspect him of working in concert with American teens to break into Pentagon computers. Then-U.S. Deputy Defense Secretary John Hamre calls it "the most organized and systematic attack" on U.S. military systems to date. An investigation points to two American teens. A 19-year-old Israeli hacker who calls himself 'The Analyzer' (Ehud Tenebaum) is eventually identified as their ringleader and arrested. Israeli Prime Minister Benjamin Netanyahu calls Tenebaum "damn good ... and very dangerous." The attacks exploited a well-known vulnerability in the Solaris operating system for which a patch had been available for months. Today Tenebaum is chief technology officer of a computer consulting firm.

[1998 Mar 20] Two teenagers hack T-Online, the online service run by Germany's national telephone company, and steal information about hundreds of bank accounts. The two 16-year-old hackers bragged about their exploits, calling Deutsche Telekom's security for the online service "absolutely primitive".

[1998 Apr] Shawn Hillis, 26, of Orlando, Florida, a former employee of NASA contractor Lockheed Martin Corp., pled guilty in Federal district court to using a NASA workstation at the Kennedy Space Center to gain unauthorized access to computer networks of several Orlando businesses.

[1998 Apr 20] An Alabama juvenile hacker launches an e-mail bomb attack consisting of 14,000 e-mail messages across a NASA network against another person using network systems in a commercial domain. The youth was later ordered to probationary conditions for 12 months.

[1998 Apr 22] The MoD criminal hacker group (Masters of Downloading, not to be confused with the 1980's group Masters of Deception) claimed to have broken into a number of military networks, including the DISN (Defense Information Systems Network); and the DEM (DISN Equipment Manager), which controls the military's global positioning satellites (GPSs).

[1998 May] Members from the Boston hacker group, L0pht (now @stake), testify before the U.S. Senate about Internet vulnerabilities.

[1998 May 30] A criminal hacker used the sheer size of AOL's technical support (6,000 people) to social engineer his way into the ACLU's web site. The attacker repeatedly phoned AOL until he found a support technician foolish enough to grant access to the targeted web site, which was wiped out as a result of the attack.

[1998 Jun 30] Former Coast Guard employee, Shakunla DeviSingla, entered a personnel database she had helped design. DeviSingla used her experience and a former co-worker's password and other identification to delete data. Her action required 115 employees and 1800 hours to recover the deleted information

[1998 Jul 31] During Def Con 6 The Cult of the Dead Cow (cDc) release Back Orifice (BO), a tool for analyzing and compromising Windows security.

[1998 Sep 13] Hackers deface The New York Times (www.nytimes.com) web site, renaming it HFG (Hacking for Girls). The hackers express anger at the arrest and imprisonment of Kevin Mitnick, the subject of the book 'Takedown' co-authored by Times reporter John Markoff. In early November, two members of HFG told Forbes magazine that they initiated the attack because they were bored and couldn't agree on a video to watch.

[1998 Sep 17] Aaron Blosser a contract programmer and self-described "math geek" harnessed over 2,500 U S West computers by installing a program that would utilize their idle time to find very large prime numbers. Their combined computational power in theory surpassed that of most supercomputers. Blosser enlisted 2,585 computers to work at various times during the day and night and quickly ran up 10.63 years of computer processing time in his search for a new prime number. "I've worked on this (math) problem for a long time," said Blosser. "When I started working at U S West, all that computational power was just too tempting for me."

[1998 Oct 1] Hackers calling themselves the Electronic Disruption Theater allege the Pentagon used illegal offensive information warfare techniques (DDoS attack)-- a charge DoD officials deny-- to thwart the group's recent computer attack.

[1998 Nov] The 'Cloverdale Two' sentenced to 3 years probation, the two Cloverdale, California teens ('Makaveli' and 'Too Short') hacked dozens of computer systems, including ones run by the Pentagon. It was later discovered that the infamous Israeli hacker, Ehud Tenebaum ('Analyzer') was the mastermind and mentor to the teens.

[1999 Feb 1] Canadian teen charged in Smurf attack of Sympatico ISP. Smurf attacks are when a malicious Internet user fools hundreds or thousands of systems into sending traffic to one location, flooding the location with pings. The attack was eventually traced to the teen's home.

[1999 Feb 15] 15-year-old from Vienna hacks into Clemson University's system and tries breaking into NASA.

[1999 Mar 18] Jay Satiro, an 18-year-old high school dropout was charged with computer tampering after hacking into the internal computers of America Online and altering some programs. Jay pled guilty and was sentenced to one year in jail and five years without a home PC.

[1999 Mar 26] Melissa virus affects 100,000 email users and caused $80 million in damages; written by David Smith a 29-year-old New Jersey computer programmer. The virus known as Melissa, was named after a Florida stripper.

[1999 Apr] Ikenna Iffih, age 28, of Boston, Massachusetts, was charged with using his home computer to illegally gain access to a number of computers, including those controlled by NASA and an agency of the U.S. Department of Defense, where, among other things, he allegedly intercepted login names and passwords, and intentionally caused delays and damage in communications. On November 17, 2000, he was sentenced to 6 months home detention, placed on supervised release for 48 months, and ordered to pay $5,000 in restitution.

[1999 Apr 26] CIH virus released by Chen Ing-Hou, the creator of the CIH virus, that takes his initials. This was the first known virus to target the flash BIOS.

[1999 May] The Napster peer-to-peer MP3 file-sharing system, used mainly to copy and swap unencrypted files of songs for free, begins to gain popularity, primarily on college campuses where students have easy access to high-speed Internet connections. It was created by Northeastern University students Shawn Fanning and Sean Parker, age 19 and 20, respectively. Before being shut down on July 2, 2001, Napster, had attracted 85 million registered users downloading as many as 3 billion songs a month.

[1999 May 11] Whitehouse.gov defaced by Global Hell.

[1999 Jul 10] Back Orifice 2000 released at Def Con 7.

[1999 Aug 30] Microsoft Corporation shuts down its Hotmail operation for approximately two hours. The shut down comes after receiving confirmed reports that hackers breached some of their servers by entering Hotmail accounts through third-party Internet providers without using passwords.

[1999 Aug 19] ABC news web site defaced by United Loan Gunmen.

[1999 Sep 5] C-Span web site defaced by United Loan Gunmen.

[1999 Sep 13] Drudge Report web site defaced by United Loan Gunmen

[1999 Sep 23] Nasdaq and American Stock Exchange web sites defaced by United Loan Gunmen.

[1999 Nov] 15-year-old Norwegian, Jon Johansen, one of the three founding members of MoRE (Masters of Reverse Engineering), the trio of programmers who created a huge stir in the DVD marketplace by releasing DeCSS, a program used to crack the Content Scrambling System (CSS) encryption used to protect every DVD movie on the market. On Jan. 24, 2000 authorities in Norway raid Johansen's house and take computer equipment.

## 2000s

[2000 Jan 15] 19-year-old Raphael Gray ('Curador') steals over 23,000 credit card numbers from 8 small companies. Raphael styled himself as a "saint of e-commerce", as he hacked into U.S., British and Canadian companies during a "crusade" to expose holes in Internet security and who used computer billionaire Bill Gates' credit card details to send him Viagra.

[2000 Feb 7] 16-year-old Canadian hacker nicknamed 'Mafiaboy', carried out his distributed denial-of-service (DDoS) spree using attack tools available on the Internet that let him launch a remotely coordinated blitz of 1-gigabits-per-second flood of IP packet requests from "zombie" servers which knocked Yahoo off-line for over 3 hours. After pleding guilty 'Mafiaboy' was sentenced on Sep. 12 2001 to eight months in a youth detention center.

[2000 Feb 9] Two days later the DDoS attacks continued, this time hitting eBay, Amazon, Buy.com, ZDNet, CNN,

E*Trade and MSN.

[2000 May] GAO (General Accounting Office) auditors were able to gain access to sensitive personal information from the Department of Defense (DOD) through a file that was publicly available over the Internet. The auditors tapped into this file without valid user authentication and gained access to employee's Social Security numbers, addresses and pay information.

[2000 May 15] Love Bug virus sent from Philippines; AMA computer college. Michael Buen & Onel de Guzman are suspected of writing the virus.

[2000 Jun 1] Qualcomm in San Diego hacked by University of Wisconsin-Madison student Jerome Heckenkamp ('MagicFX').

[2000 Jun 15] An Information Technology consultant breached the security of British internet service provider Redhotant to expose security lapses. He managed to obtain the names, addresses, passwords and credit card details of more than 24,000 people, including military scientists, government officials, and top company executives just to show it could be done. The hacker said breaching the site's security was "child's play".

[2000 Jul 18] AOL, based in Vienna, Virginia, confirmed that records for more than 500 so-called screen names of its customers had been hacked. Those records typically contain information such as a customer's name, address and the credit card number used to open the account.

[2000 Jul 7] Utilities firm Powergen located in the UK was forced to ask thousands of its customers to cancel credit cards after a web site blunder left a database of card details exposed.

[2000 Jul 24] Andrew Miffleton ('Daphtpunk'), age 25, of Arlington, Texas was sentenced in federal court to 21 months imprisonment and ordered to pay a $3,000.00 fine. Miffleton associated himself with a group known as "the Darkside Hackers", who were interested in using unauthorized access devices to fraudulently obtain cellular telephone service through cloned cellular telephones or long distance telephone service through stolen calling card numbers.

[2000 Aug 17] United States District Judge Lewis Kaplan in New York bars Eric Corley ('Emmanuel Goldstein'), publisher of 2600 magazine, from republishing software hacks that circumvent DVD industry encryptions. The code would enable movies to be more readily copied and exchanged as data files on the Internet.

[2000 Sep 5] A 21-year-old New Rochelle, New York man was sentenced to four months in prison for breaking into two computers owned by NASA's Jet Propulsion Laboratory in 1998 and using one to host Internet chat rooms devoted to hacking, prosecutors said. Raymond Torricelli ('rolex') was a member of the hacking group '#conflict' which used their computers to electronically alter the results of the annual MTV Movie Awards. Additionally, over 76,000 discrete passwords were found on Raymond's personal computer.

[2000 Sep 6] Patrick W. Gregory ('MostHateD'), age 20, pled guilty for his role as a founding member of a hacking ring called GlobalHell and is sentenced to 26 months imprisonment, three years supervised release, and was ordered to pay $154,529.86 in restitution. GlobalHell is said to have caused at least $1.5 million in damages to various U.S. corporations and government entities, including the White House and the U.S. Army. Gregory, a high school dropout who has said he wants to start his own computer security business, admits in a plea agreement to stealing telephone conferencing services from AT&T, MCI, and Latitude Communications and holding conference calls between 1997 and May 1999 with other hackers around the country.

[2000 Sep 26] Jason Diekman ('Shadow Knight', 'Dark Lord') arrested after Federal agents discovered evidence on Diekman's computers indicating that he intercepted usernames and passwords from universities, including Harvard University. In a statement he made to investigators, Diekman admitted that he had hacked into "hundreds, maybe thousands" of computers, including systems at JPL, Stanford, Harvard, Cornell University, the California State University at Fullerton, and University of California campuses in Los Angeles and San Diego. On February 4, 2002, Diekman was sentenced to 21 months in federal prison, three years supervised release, restricted use of the computer and over $87,000 in restitution.

[2000 Oct] Microsoft admits that its corporate network has been hacked and source code for future Windows products has been seen. Hacker suspeted to be from St Petersburg.

[2000 Oct 10] FBI lure 2 Russian hackers to their arrest in Seattle, after it was determined that Alexei Ivanov, 20, and Vasiliy Gorshkov, 25, spent two years victimizing American businesses. The FBI established a bogus computer security firm that they named, fittingly enough, Invita. They leased office space in downtown Seattle and immediately called Ivanov in Russia about possible employment as a hacker. The FBI communicated with Gorshkov and Ivanov, by e-mail and telephone during the summer and fall of 2000. The men agreed to a face-to-face meeting and on Nov. 10, Gorshkov and Ivanov flew to Seattle and went directly to a two-hour "job interview" with undercover FBI agents who were posing as Invita staff. The Russians were asked to further demonstrate their hacking skills on an IBM Thinkpad provided by the agents. The hackers happily complied and communicated with their home server back in Chelyabinsk, unaware that the laptop they were using was running a "sniffer" program that recorded their every keystroke. The FBI agents' descriptions of the meeting portray Ivanov and Gorshkov as not only blissfully ignorant of their impending arrest, but also somewhat cocky about their hacking skills. At one point in the meeting, as Gorshkov glibly detailed how he and Ivanov extorted money from a U.S. Internet service provider after hacking into its servers, he told the room of undercover agents that "the FBI could not get them in Russia."

[2000 Oct 28] After 9 million hack attempts security web site AntiOnline is defaced by Australian hacker 'ron1n' ('n1nor'). AntiOnline was deemed "unhackable" by the sites owner, John Vranesevich, but a poorly coded cgi script(s) written by Vranesevich led to the hack.

[2000 Nov 7] A 19-year-old Dutch hacker named 'Dimitri' broke in to Microsoft's internal web servers with intentions to show the company its vulnerability due to not installing their own patches.

[2000 Dec 13] More than 55,000 numbers were stolen from Creditcards.com, which processes credit transactions for

online companies. About 25,000 of them were posted online when an extortion payment was not made.

[2000 Dec 24] Exigent International, a U.S. government contractor, acknowledged that one or more cyberthieves broke into a restricted federal computer system and stole the company's proprietary code for controlling satellite systems. The software, known as OS/COMET, allows ground-control personnel to communicate and send commands to satellites and rockets. The U.S. Air Force has plans to use the OS/COMET software to control the NAVSTAR Global Positioning System from its Colorado Springs Monitor Station, which is part of the Air Force Space Command.

[2001 Feb 1] Hackers invade World Economic Forum. The compromised data included credit card numbers, personal cell phone numbers and information concerning passports and travel arrangements for a number of government and business leaders. Among the notable victims whose personal information was pilfered were Microsoft chairman Bill Gates, Palestinian Authority chairman Yasser Arafat, U.N. Secretary-General Kofi Annan, former U.S. Secretary of State Madeline Albright and former Israeli Prime Minister Shimon Peres.

[2001 Feb 12] Anna Kournikova virus released by 20-year-old Dutchman Jan de Wit ('OnTheFly') who was later arrested and sentenced to 150 hours of community service.

[2001 Mar 1] FBI reports that 40 e-commerce sites located in 20 U.S. states were cracked by eastern Europe hackers, have stolen more than one million credit card numbers from U.S. e-commerce and banking websites.

[2001 Mar 7] Jesus Oquendo ('Sil'), age 27, of Queens, New York was convicted and sentenced to 27 months in Manhattan federal court on charges of computer hacking and electronic eavesdropping of victim company Five Partners Asset Management LLC ("Five Partners"), a venture capital company based in Manhattan. Oquendo left the victim a taunting message on its network: "Hello, I have just hacked into your system. Have a nice day."

[2001 May 1] Chinese and U.S. hackers attack each other because of the U.S. spy plane that had to make an emergency landing in China after the U.S. plane collides with and kills Chinese fighter pilot Wang Wei.

[2001 May 4] Gibson Security Research Corp came under attack (DDOS) and taken off-line by a 13-year-old hacker, at first due to a mistaken belief that Steve Gibson had called him a name, then simply because it was fun.

[2001 May 11] Solaris/IIS worm infects Solaris boxes up to version 7, and then scans for IIS machines susceptible to the folder traversal vulnerability and then replaces the default web page.

[2001 May 15] Hackers attack University of Washington and put file sharing program on its computers.

[2001 May 17] 'Fluffy Bunny' hacker group hacks Apache.org and SourceForge.net.

[2002 May 21] Max Butler ('Max Vision' and 'The Equalizer') was sentenced to 18 months in prison for launching an Internet worm that crawled through hundreds of military and defense contractor computers over a few days in 1998. Max Butler also lived three lives for five years. As 'Max Vision', he was an incredibly skilled hacker and security expert who boasted that he'd never met a computer system he couldn't crack. As 'The Equalizer', he was an FBI informant, reporting on the activities of other hackers. As Max Butler, he was a family man in Santa Clara, California who ran a Silicon Valley security firm. At Max Vision Network Security, he specialized in running "penetration tests," attempting to break into corporate networks to prove that their security wasn't as good as it could be.

[2001 Jun 9] Los Angeles Times newspaper reports that hackers attacked a computer system that controls much of the flow of electricity across California's power grid for seventeen days or more during the state's worse days of the power crisis. According to the Times, the discover was ade on Friday, May 11 and that it was determined that attackes began as early as Wednesday, April 25. The attack appears to have primarily by an individual associated to China's Guangdong province and routed through China Telecom. The 17-day intrusion into the networks running California's leading electric power grid has caused considerable concern among state and federal bureaucrats.

[2001 Jun 15] Christine Gunhus, the wife of an U.S. senator, pleads no contest to charges of using a pseudonym to send e-mail messages that disparaged her husband's Democratic rival.

[2001 Jun 20] U.S. security company ZixIt reported that a database holding details of customers' credit cards had been hacked.

[2001 Jul 12] Notorious hacker group World of Hell managed to deface 679 web sites in just one minute.

[2001 Jul 17] Code Red worm is released. The worm exploits vulnerabilities in the Microsoft Internet Information Server IIS. The worm got its name from "Code Red" Mountain Dew which was used to stay awake by the hackers that disassembled the exploit.

[2001 Jul 16] 27-year old Russian programmer Dmitry Sklyarov arrested at Def Con 9 for creating a program to copy Adobe electronic books. He was charged with violating the 1998 Digital Millennium Copyright Act. Demitry was later released, as part of the agreement, Sklyarov will testify for the government in the case that remains against ElcomSoft, the company that sells the copying software.

[2001 Aug 21] Washington-based Riggs bank has its Visa customer database stolen by hackers.

[2001 Sep 18] Nimda worm (admin backwards) starts to spread, infecting Microsoft IIS servers that are open to known software vulnerabilities.

[2001 Nov 20] Hackers access Playboy.com's credit card data. The hacking group 'ingreslock 1524' claim responsibility.

[2001 Nov 20] 25 church web sites hacked by Hacking for Satan group.

[2001 Dec 8] Federal prosecutors accuse one time Los Alamos National Laboratory employee Jerome Heckenkamp of breaking into Qualcomm and other corporate computer systems while he was a student. Heckenkamp, they say called

himself 'MagicFX'. When school police asked for the password for his personal computer. Court records say Heckenkamp chuckled when he gave it up. "Hackme," he told them. Jerome is also suspected of hacking into a half-dozen other companies, including eBay Inc. and E*Trade Inc., over a nine-month period.

[2001 Nov 26] 2 former Cisco accountants sentenced to 34 months for breaking into company computers and stealing stock.

[2002 Feb 25] A 17-year-old female hacker, from Belgium, calling herself 'Gigabyte' takes credit for writing the first-ever virus, called 'Sharpei', written in Microsoft's newest programming language C# (C sharp).

[2002 Jul 11] Hackers broke into USA Today's web site and replaced several of the newspaper's legitimate news stories with phony articles. Israeli hackers were suspeted.

[2002 Jul 25] Princeton University admissions officials gained unauthorized access to a web site at rival Yale University containing personal information about applicants to the Ivy League school, according to officials at both institutions.

[2002 Jul 30] Copies of OpenSSH are trojaned. OpenSSH is a popular, free version of the SSH (Secure Shell) communications suite and is used as a secure replacement for protocols such as Telnet, Rlogin, Rsh, and Ftp. The main openBSD (ftp.openbsd.org) mirror was compromised, after developers noticed that the checksum of the package had changed.

[2002 Aug 2] Italian police arrest 14 suspected hackers who are accused of thousands of computer intrusions, including attacks on the U.S. Army and Navy and the National Aeronautics and Space Administration. They were all members of two hacking groups, called Mentor and Reservoir Dogs.

[2002 Aug 17] Federal law enforcement authorities searched the computers of a San Diego security firm that used the Internet to access government and military computers without authorization over the summer. Investigators from the FBI, the Army and NASA visited the offices of ForensicTec Solutions Inc. seeking details about how the company gained access to computers at Fort Hood in Texas and at the Energy Department, NASA and other government facilities. The searches began hours after it was reported that ForensicTec consultants used free software to identify vulnerable computers and then peruse hundreds of confidential files containing military procedures, e-mail, Social Security numbers and financial data, according to records maintained by the company. While ForensicTec officials said they wanted to help the government and "get some positive exposure for themselves," authorities are pursuing the matter as a criminal case.

[2002 Aug 28] The Recording Industry Association of America's (RIAA) web site is defaced, and copyrighted mp3s are uploaded to the server. The RIAA along with the Motion Picture Association of America (MPAA), has won many critics online in its quest to shut down popular file-trading networks such as Napster.

[2002 Sep 20] Samir Rana ('Torner') a 21 year-old London hacker is arrested following a year-long investigation into the creation of the Linux rootkit program called Tornkit and on suspicion of being a member of the infamous hacker group Fluffy Bunny. It was later reporter that Rana owned the pink stuffed toy depicted in website defacements by Fluffy Bunny.

[2002 Sep 23] A UK hacker received an 18-month prison sentence for corporate sabotage. Stephen Carey, a 28-year-old computer engineer from Eastbourne, Sussex, is sentenced to 18 months for hacking into a firm's database and modifying information.

[2002 Oct 4] Hacker Vasily Gorshkov, 27, of Chelyabinsk, Russia, is sentenced to three years in prison for convictions on 20 counts of conspiracy, fraud and related computer crimes. Gorshkov is also ordered to pay restitution of nearly $700,000 for losses he caused to Speakeasy Network of Seattle, and the online credit card payment company PayPal.

[2002 Oct 8] CERT (Computer Emergency Response Team) advisory is released detailing the discovery of a back door (trojan horse) found in the source code files of Sendmail 8.12.6.

[2002 Oct 16] Microsoft admits to being hacked. The security breach took place on a server that hosts Microsoft's Windows beta community, which allows more than 20,000 Windows users a chance to test software that is still in development.

[2002 Oct 21] A distributed denial-of-service (Dee-Dos) attack, lasting one hour, sent a barrage of data at the 13 domain-name service root servers. The attack was in the form of an ICMP flood, which was blocked by many of the root servers, preventing any real loss of network performance.

[2002 Nov 12] Gary McKinnon ('Solo'), 36, of London, an unemployed British sysadmin was indicted for what US authorities describe as the "biggest hack of military computers ever detected". From February 2001 until March 2002, McKinnon allegedly exploited poorly-secured Windows systems to attack 92 networks run by NASA, the Pentagon and 12 other military installation scattered over 14 states. Private sector businesses were also affected by the alleged attacks, which caused an estimated $900,000 in damage overall. Prosecutors said that McKinnon "stole passwords, deleted files, monitored traffic and shut down computer networks on military bases from Pearl Harbour to Connecticut".

[2002 Nov 22] Lisa Chen, a 52-year-old Taiwanese woman who pleaded no contest in one of the largest software piracy cases in the U.S. was sentenced to nine years in prison, one of the longest sentences ever for a case involving software piracy. Chen was arrested along with three associates in November 2001 after local sheriffs seized hundreds of thousands of copies of pirated software worth more than $75 million, software that Chen smuggled from Taiwan.

[2002 Dec 17] A jury acquitted ElcomSoft, Russian software company, of criminal copyright charges related to selling a program that can crack antipiracy protections on electronic books. The case against ElcomSoft is considered a crucial test of the criminal provisions of the Digital Millennium Copyright Act (DMCA), a controversial law designed to extend copyright protections into the digital age.

[2003 Jan 21] Computer hacker Kevin Mitnick is goes online for the first time in nearly a decade. He was captured in a raid and sent to jail for almost five years for computer crimes against companies including Sun Microsystems and

Motorola. The prison term was followed by another three and a half years of restrictions regarding Mitnick's access to computers and the Internet.

[2003 Jan 21] Simon Vallor, 22, a British Web designer was sentenced to two years in prison for writing one of the world's most destructive viruses which wiped out computers worldwide. Vallor was the author of 3 viruses -- "Gokar," "Redesi," and "Admirer" -- "Gokar" spread the most widely and was at one point ranked as the third most prevalent virus of all time.

[2003 Feb 6] Douglas Boudreau, 21, allegedly installed keystroke monitoring software on more than 100 computers at Boston College and then watched as thousands of people sent e-mail, downloaded files and banked online. He was later indicted on charges he placed software on dozens of computers that allowed him to secretly monitor what people were typing, and then stole around $2,000 using information he gleaned.

[2003 Feb 7] Two hackers who broke into Riverside County, Calif., court computers and electronically dismissed a variety of pending cases plead guilty to the crime. Both William Grace, 22, and Brandon Wilson, 28, were sentenced to nine years in jail after pleading guilty to 72 counts of illegally entering a computer system and editing data, along with seven counts of conspiracy to commit extortion

[2003 Feb 10] Twice in the past two weeks, online vandals--like the ones who tagged many Web sites with "Free Kevin!" graffiti during Mitnick's time in prison--broke into the Web server of the former hacker's security start-up, Defensive Thinking.

[2003 Feb 18] It's reported that a hacker ("unauthorized intruder") gained access to some 8 million credit card account numbers —including Visa, MasterCard and American Express —by breaching the security of a company that processes transactions for merchants, the card companies said.

[2003 Mar 7] Online attackers stole information on more than 55,000 students and faculty from insecure database servers at the University of Texas at Austin.

[2003 Apr 29] New Scotland Yard said Wednesday they arrested 24-year-old Lynn Htun at a London convention center, the site of InfoSecurity Europe 2003. Law enforcement and Internet security professionals said they believe Htun is the mastermind of the “Fluffi Bunni” hacking exploits, hacking into sites ranging from those of McDonalds Corp to Internet security specialists SANS Institute and Symantec Corp’s virus detection group SecurityFocus.

[2003 Jun 12] Web designer John Racine II, 24, admitted diverting traffic and e-mails from al-Jazeera's Arabic Web site to a site he had designed called "Let Freedom Ring" and bearing the U.S. flag. John carried out this attack on the al-Jazeera Web site during the Iraq war because the Arab satellite TV network had shown pictures of dead and captured American soldiers.

[2003 Jul 6] Internet experts brace for hacker contest. The assault is being billed as a contest to see who can deface 6,000 Web sites in six hours. The widely publicised hacking contest which encouraged vandals to deface websites ended without causing serious trouble.