Hacking History

G. Filosofi 2019

Km ha strong ability to remember telephone numbers
Eric Heinz was a phony. The real name eas Joseph Wernle

1865

- US Secret Service (USSS) founded

1876

- Alexander Graham Bell invents telephone

1939

- "Futurian" science-fiction group raided by Secret Service

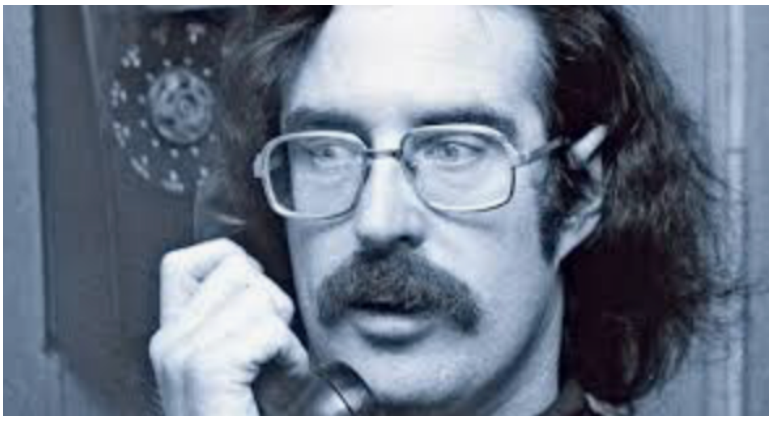
1971

- Yippie phone phreaks start YIPL/TAP magazine
- October. Esquire Magazine publishes a story called "Secrets of the Little Blue Box" by Ron Rosenbaum. This article featured Engressia and John Draper work, synonymising their names with *phreaking*. Phone phreaking got its start in the late 1950s, but its golden age was the late 1960s and early 1970s.

1972

- RAMPARTS magazine seized in blue-box rip-off scandal
- John Draper (aka *Captain Crunch*) is arrested on charges of toll fraud, for which he was sentenced to 5 years probation. Draper said “I don't do that. I don't do that anymore at all. And if I do it, I do it for one reason and one reason only. I’m learning about a system. The phone company is a System. A computer is a System, do you understand? If I do what I do, it is only to explore a system. Computers, systems, that's my bag. The phone company is nothing but a computer.” Steve Wozniak and Draper met to compare techniques for building blue boxes. Wozniak and Steve Jobs later set up a small

business selling blue boxes. In 1976 and 1978, Draper will serve 2 prison sentences for phone fraud. During a third period of incarceration in 1979, he will write *EasyWriter*, the first word processor for the Apple II

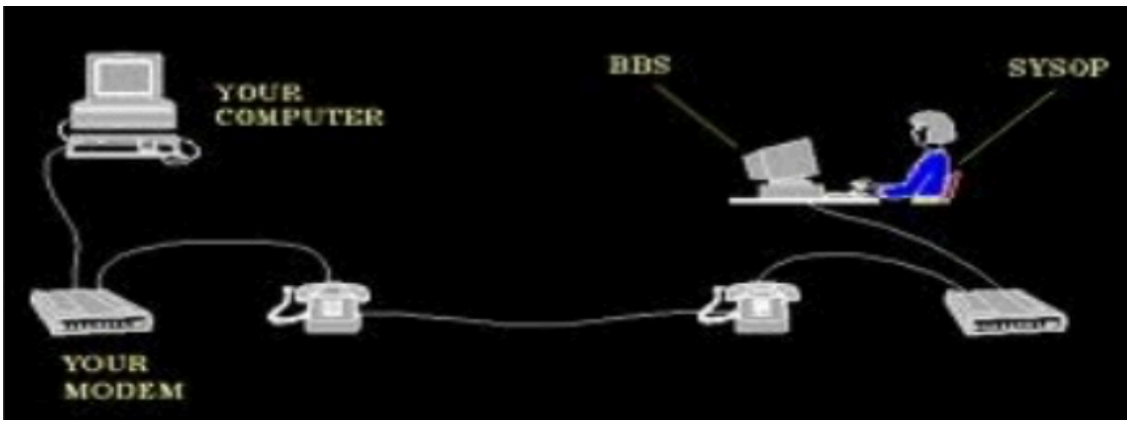


1977

- RSA (Ron Rivest, Adi Shamir, Leonard Adleman)

1978

- Ward Christenson and Randy Suess create first PC BBS (Bulletin Board System). Computer BBSs are personal computers that have been equipped with a telephone modem and special software. Users can connect with a BBS by dialing, with their own computer and modem, the phone number to which the BBS is connected. After "logging in" by supplying a valid user name and password, the user can leave messages to other users of the system. These messages are not private and anyone calling the BBS can freely read and respond to them.



1979

- Kevin Mitnick, then 16, gains unauthorised access to Ark, the computer network of DEC's RSTS/E OS dev team. He used just the modem dial-up number for Ark a friend gave him as a challenge to allow him into a circle of computer hackers. Once obtained the credentials from Kevin, they download the OS's source code, then betray Kevin giving Ark his name. For such a crime Kevin will be charged and convicted in 1988. Mitnick was born in Van Nuys (CA) in 1963 and grew up in the suburbs of LA (the San Fernando Valley). At age 12, Mitnick used social engineering and dumpster diving to bypass the punch card system used in the bus system. Later on he joined a small group of local hackers. His computer escapades began in high school, where he learned to break into the LA Unified School District's main computers. Social engineering will be his method of choice to obtain informations. In late 70s and early 80s Kevin couldn't afford a computer at home. Thereby he is continually in search of a remote computer access, either from university campuses or private businesses. it's a kind of addiction. His

preferred target was a DEC PDP-11 microcomputers running RSTS/E OS. For example, in 1980, December, Mitnick runs into Micah, a kid son of a researcher at Bloodstock Research center. Kevin breaks into their network using his account. The breaching is spotted by the company and signalled to FBI. In 1981 Mitnick and his friend Lewis De Payne were phreaking and hacking partners with no interests other than enjoying learning computer tricks. One day Mitnick obtains admin password to US Leasing's computer network by social engineering and shares this information with Lewis. Lewis's girlfriend Susan Thunder in some way obtains the credentials and repeatedly sneaks into the system, damaging files and leaving lots of clues linking to Kevin. She did it for an unclear act of revenge.
Mitnick took his nickname (*Condor*) from a movie starring Robert Redford as a man on the run from the government (Three Days of the Condor)
Mitnick was overweight due to his love for junk food.

1980

- Ian Murphy (aka *Captain Zap*) and 3 friends break into AT&T's computer system and shift the metering clocks around, so the system charged peak rates at off-peak hours and vice versa.

1981

- September. Chaos Computer Club (CCC), which will be the Europe's largest association of ethic hackers, is founded in Berlin. At the beginning they are a dozen members like Karl Coch (aka *Hagbard*), Hans Huebner (aka *Pengo*) and his friends Dirk Bresinski and Peter Carl. The pseudonym Hagbard comes from a series of science fiction novels, *The Illuminati*, where Hagbard is the leader of a small band of anarchists.
- After 18 months of investigations, *Captain Zap* is arrested. He is first person ever arrested for a computer crime
- Kevin Mitnick (aka *Condor*), age 18, breaks in the North American Air Defense Command computer in Colorado Springs. After that he breaks into the corporate offices of Pacific Bell and obtains computer manuals, and software, on the COSMOS and MicroPort computer systems. Because of his young age, he will avoid sentencing this time

1982

- William Gibson coins term *cyberspace*
- Elk Cloner, a 15-year-old high school student, writes as a joke one of the first known microcomputer viruses that spread "in the wild", i.e., outside the computer system or laboratory in which it was written. It attached itself to the Apple II's operating system DOS 3.3 and spread by floppy disk
- The *414s*, a group of hackers, break into dozens of high-profile computer systems, including ones at Los Alamos National Laboratory, Sloan-Kettering Cancer Center, and Security Pacific Bank
- *Captain Zap* is convicted with 1000 hours of community service and 2 and half years probation

1983

- AT&T is dismantled in pieces: AT&T Communications, AT&T Industries, Bell Communications Research

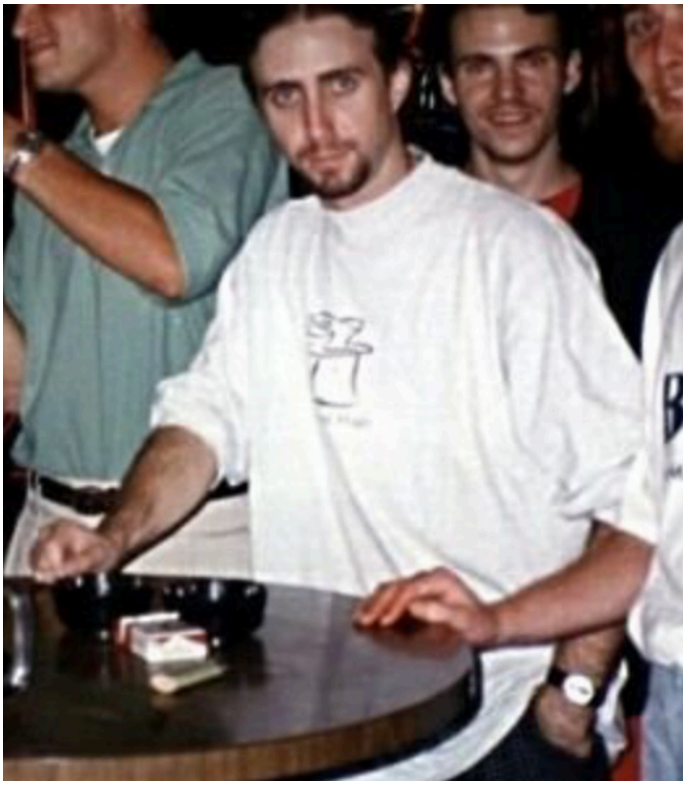
Divided into
A long-distance company controlled by A&t
7 regional siblings
Bell Communications Research (the Bell Labs)

The Baby Bells got together and funded Bellcore, aimed to develop new standards of the future. Bellcore is also responsible of security

- June 3. The 414s break-in Memorial Sloan-Kettering Center computer system in Manhattan doing $1500 worth of damage by deleting billing records. The 414s have been identified by the FBI as 6 teenagers from Milwaukee, ranged in age from 16 to 22, who met through an IBM sponsored organization called the Explorer Scouts. There, they did early coding and became friends. The group named themselves after their telephone area code, 414. They are described as "Young, male, intelligent, highly motivated and energetic". Gerald Wondra, 22, was the first visited by the FBI. Wondra lived with his mother in West Allis, a Milwaukee suburb. Wondra said he was "curious, he was just having fun". Neal Patrick, 22, a student at Rufus King High School, claims his only motivation is the challenge of getting into places he was not supposed to, and remaining there undetected. The systems they broke into were exclusively running DEC's VMS and RSTS operating systems. They used inexpensive PC, analog modems, and simple hacking techniques, such as using common or default passwords published in DEC's manufacturer guides to log in to various timeshare systems. While there was some damage to company files and property from the incidents, no laws were yet in place. Most of the members of the 414s were not prosecuted, in various agreements to stop their activities and pay restitutions. Wondra and another defendant were charged with “making harassing phone calls”. On September 26, Neal Patrick testifies before the US House of Representatives about the dangers of computer hacking. Congressman Dan Glickman calls for an investigation and new laws about computer hacking.

1984

- US Congress passes Comprehensive Crime Control Act giving USSS jurisdiction over credit card fraud and computer fraud. It contains 6 bills concerning computer crime.
- Legion of Doom (LOD) is founded by *Lex Luthor*, after a rift with his previous group, the Knights of Shadow (KOS). LOD will be strongly influential until early 2000. They considered themselves not causing any direct harm to the phone systems and computer networks they took over. Still, many members will be raided and prosecuted for causing alleged damage to systems. Early LOD members were: Chris Goggans (aka *Erik Bloodaxe*), Mark Abene (aka *Phiber Optik*), Lex Luthor, Karl Marx, Mark Tabas, Agrajag the Prolonged, King Blotto, Blue Archer, EBA, The Dragyn, Unknown Soldier. Many others joined and leaved along the way, like Mark Tabas, Karl Marx, Automatic Jack, Bill From RNOC, Lord Digital, The Mentor, Doctor Who, Dead Lord, Terminus.



- 2600 Hacker Quarterly magazine founded
- Whole Earth Software Catalog published
- The CCC draw public attention to the security flaws of the German Bildschirmtext computer network by causing it to debit DM 134K in a Hamburg bank in favour of the club. The money was returned the next day in front of the press.
- Cult of the Dead Cow (cDc) is founded in *Lubbock*, Texas. Notable members are *Grandmaster Rattè*, *Franken Gibe*, *Sir Dystic*, *Sid Vicious*.

1985

- First police "sting" BBS is established
- Kevin Mitnick and his friend Lenny DiCicco break-in Dockmaster, a computer system owned by NSA. From late 1985 through much of 1986, they hack SCCS (Switching Control Center System): they can trace lines, create and delete phone numbers, set up trap-and-traces, the access their logs, giving them an intense feeling of power, a power, Mitnick said, he never made any use of
- Whole Earth 'Lectronic Link computer conference (WELL) goes on-line. It is a BBS based in the SF Bay Area and attracts some of the best minds of the communications revolution
- *Knight Lightning* get start *Phrack*, one of the first electronic magazine focused on hacking and phreaking

1986

- Computer Fraud and Abuse Act passed
- Electronic Communications Privacy Act passed
- Mitnick, now 23, lives with his girlfriend Bonny Vitiello. Kevin has been ousted by two companies he got hired as soon as they figure out his past of hacker. FBI raids Bonny's apartment
- August. The young astronomer Cliff Stall intercepts a German hacker breaking into his computer at Lawrence Berkeley Laboratory, and connecting through Milnet to the Air Force Space Division network. That's the incipit of his bestseller titled The Cuckoo's Egg. After 10 months of investigations it turned out the hacker is Markus Hess, 25, living and working in downtown Hannover. Markus is in touch with CCC where Hagbard and Pengo routinely break into US computer networks but military. Hess didn't mind the warning Hagbard had issued to CCC members, "Never penetrate a military computer". The group will sell to Soviet KGB printouts, phon and passwords collected by Hess for $18000 and cocaine for Hagbard's habit

1987

- Chicago prosecutors form Computer Fraud and Abuse Task Force (???)
- John Perry Barlow buys a modem and login to the WELL BBS. He describes the new generation of computer-connected communities as a network of small towns where people work together, share information, creating a collective consciousness
- June, 29. West German police raids Markus Hess's apartment. On March 2, 1989, German authorities will charge with espionage Markus Hess and CCC members Hagbard, Pengo, Peter Carl, Dirk Bresinski.
- June. Kevin Mitnick and Bonnie Vitiello get married

1988

- July. Secret Service covertly videotapes "SummerCon" hacker convention
- September. *Prophet* cracks BellSouth AIMSX computer network and downloads E911 Document to his own computer and to Jolnet
- September. AT&T Corporate Information Security informed of *Prophet's* action

- October. Bellcore Security informed of *Prophet's* action
- Kevin Mitnick is convicted in LA for stealing computer programs and breaking into corporate networks. He received a one-year sentence. Mitnick will violate the terms of his probation (supervised release). He fled, becoming a fugitive for two and a half years. During this period he will hack into Pacific Bell voicemail and other systems. After 4 months at Lompoc, Mitnick discover that Bonnie was leaving him for his best friend Lewis De Payne. Mitnick was betrayed by Lewis but eventually they continued to be hacking partners. Mitnick goes to Las Vegas living with his mother and stop hacking for a while. Mitnick's Social Engineering ability magically makes some EEPROM loaded with a special firmware landing into his hands. Those chips will allow him to change the number of his Novatell PTR-825 cell phone. Now Mitnick could make phone calls that couldn't be traced back to him
- Graduate student at Cornell University Robert Morris releases the Morris worm. It is considered the first worm in history

1989

- January. *Prophet* uploads E911 Document to *Knight Lightning*
- *January 9. Time magazine reports that ".. putting a phone in Mitnick's hands is like giving a gun to a hit man."*
- February 25. *Knight Lightning* publishes E911 Document in *Phrack* electronic newsletter
- May. Chicago Task Force raids and arrests *Kyrie*
- June. *NuPrometheus League* distributes Apple Computer proprietary software
- June 13. Florida probation office crossed with phone-sex line in switching-station stunt
- Mitnick, now 26, with a friend named Lenny DiCicco steal highly secret software programs and manuals from DEC. Mitnick and DiCicco are arrested. DiCicco turned his friend in to authorities. "He's an electronic terrorist", he said. Mitnick served a year in prison and was placed on probation. He will fled in late 1992. Harriet Rosetto, the director of the rehabilitation facility Mitnick was ordered to regularly attend, said "hacking gives Kevin a sense of self-esteem that he doesn't get in the real world, there was no greed or sabotage involved... He's like a big kid playing Dungeons and Dragons".
- June. Master of Deception (MOD) is founded in NYC by Elias Ladopoulos (aka *Acid Phreak*), Paul William Stira (aka *Scorpion)*, *HAC* (?). Later on Mark Abene (aka *Phiber Optik*), got kicked out of the LOD, is brought on board.
  Scorpion, 15, equipped with a C64, mastered at the art of cracking games. He wrote what is known as a *wardialing* (or *War Games dialer*$, a program to let his modem to scan toll-free 800-prefix numbers sequentially in search of new BBSs (he created one called *Beyond the Limit*). He stumbled, and eventually breaks into, a Northern Telecom DMS 100 (Digital Multiplex Switch).
  Phiber Optik owned a TRS-80. Well skilled in Social Engineering, he knew everything about the architecture of the NYNEX Packet Switched Network.
  ??? got a C128. He is brought into the group by solving a challenge Acid Phreak issued to him, to figure out AP's real identity with only the number 555-ACID as a clue.
  As of August 1, 1990, there will be 14 members: *Acid Phreak*, *Scorpion*, *HAC*, *The Wing*, *Supernigger*, *Nynex Phreak*, *Phiber Optik*, *Crazy Eddie*, *Seeker*, *ZOD*, *Outlaw*, *Corrupt*, *The Plague*, *Red Knight*.

Supernigger was very good in Social Engineering. He could call the woman in the business office “Lady, I’m 20 feet up on tge pole”, and she gives him whatever information he wants. He was able to introduce in a corporate conference bridge, where a dozen of people would speak about quarterly earnings.
Allen Wilson (aka *The Wing*) was a kid living in Pennsylvania. He claimed to be a Unix specialist, owner of a 80386 IBM compatible computer. *Acid Phreak* knew him on a chat on the Altos BBS.
ZOD was also a Unix hacker.
John Lee (aka *Corrupt*), black, “VAX king” for the friends, knows more about VAX computers from DEC. He joined a street gang called *Decepticons*.
Julio Fernandez (aka *Outlaw*), 15, from Bronx.
MOD was never a textfile "how-to" group. It was always based on a brotherhood type deal and everything done is secretive and has a purpose behind it. Unlike other hacking groups they don’t love to share share informations. Like LOD, MOD was against wanton destruction of computers which had been hacked.

- NY Telephone employees Tom Kaiser and Fred Staples, of the toll-fraud dept., start to investigate unauthorised accesses to a dial Hub, a critical node of the telephone network. In November MOD got root access to *The Learning Link*, a Unix system owned by Channel 13/WNET. It was a public educational broadcasting television service for schoolteachers. One day the system crashes. Someone had erased all the files. Tom Kaiser noticed on his logs Acid Phreak had connected to the system. Secret Service gets advised. John Perry Barlow and two MOD’s members have a critical confrontation about the incident on a public electronic forum hosted by the Harper’s magazine. The debate’s topic is “Is Computer Hacking a Crime?”
- July. *Fry Guy* raided by USSS and Chicago Computer Fraud and Abuse Task Force
- July. Secret Service raids *Prophet*, *Leftist*, and *Urvile* in Georgia
- *Agent Steal* breaks into COSMOS (COmputer System for Main frame OperationS) of the Pacific Bell Telephone Company in California and intercepts the telephone lines of several local FM radio station ensuring he is the only caller who could get through during on-air contest, and thus the only winner. His winnings included $50K, several trips and two Porsches. Peterson has a couple of associates. Rumours link them to *Dark Dante* and Ronald Austin. Realizing he is pursued by the FBI, Peterson moves to Texas, where he fraudulently obtains and uses credit cards
- In an isolated forest outside of Hannover Hagbard’s charred bones are found next to a melted can of gasoline. No suicide note is found.

1990 (the year of the Hacker Crackdown)

- January 15. Crash strikes AT&T long-distance network nationwide. 50 million calls were blocked in 9 hours. The massive crash was caused by a one-line bug in the System 7

software running on AT&T's 4ESS switching stations. The bug was a break statement inside a if clause nested within a switch construct. The break was SUPPOSED to break the if clause, instead it broke the switch clause. Americans believed computer hackers had caused the crash

- January 18-19. Chicago Task Force raids Craig Neidorf (aka *Knight Lightning*) in St. Louis
- January 24. USSS and New York State Police raid *Phiber Optik*, *Acid Phreak* and *Scorpion* in NY
- February 3. Chicago Task Force raids Richard Andrews' home
- February 6. Chicago Task Force raids Richard Andrews' business
- February 6. USSS arrests *Terminus*, *Prophet*, *Leftist*, and *Urvile*
- February 9. Chicago Task Force arrests Craig Neidorf
- February 20. AT&T Security shuts down public-access "attctc" computer in Dallas
- February 21. Chicago Task Force raids Robert Izenberg in Austin
- March 1. Chicago Task Force raids Steve Jackson Games Inc., *Mentor* and *Erik Bloodaxe* in Austin
- April. John Perry Barlow is visited by a FBI agent in relation to the theft and distribution of the source code for a series of Macintosh ROMs. Barlow will recall the visit as "complicated by [the agent's] fairly complete unfamiliarity with computer technology. I realised right away that before I could demonstrate my innocence, I would first have to explain to him what guilt might be." Barlow is contacted by Mitch Kapor, who had had a similar experience. Barlow and Kapor feel that their experience is symptomatic of a "great paroxysm of governmental confusion during which everyone's liberties would become at risk".
- May 7-9. USSS and Arizona Organized Crime and Racketeering Bureau conduct "Operation Sundevil" raids in Cincinnatti, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose, San Francisco
- May. FBI interviews John Perry Barlow re NuPrometheus case
- June 1st. *Dark Dante* takes over all of the telephone lines for LA's radio station KIIS-FM to ensure he would be the 102nd caller in its car giveaway contest. It worked. He won a Porsche 944 S2

- June. John Perry Barlow and Mitch Kapor found Electronic Frontier Foundation (EFF) in response to a series of actions by law enforcement agencies that led them to conclude that the authorities were gravely uninformed about emerging forms of online communication, and that there was a need for increased protection for Internet civil liberties. EFF provides funds for legal defence in court to individuals and new technologies from what it considers abusive legal threats. EFF organizes political action and mass mailings, supports some new technologies which it believes preserve personal freedoms and online civil liberties, monitors and challenges potential legislation that it believes would infringe on personal liberties.
- Barlow publishes CRIME AND PUZZLEMENT manifesto, where he plans to create an organisation to "raise and disburse funds for education, lobbying, and litigation in the areas relating to digital speech and the extension of the Constitution into Cyberspace."
- July 24-27. Trial of Craig Neidorf
- *Omega*, member of cDc, uses the term "hacktivism" for the first time in an email to other

group members. Hacktivist's beliefs include access to information is a basic human right.
- Kevin Mitnick (aka *Condor*) is released from the rehabilitation facility and assigned a probation officer. Strange things began to happen... The probation officer's phone is suddenly disconnected, and the phone company having no record of it. A judge's credit record at TRW inc. is unexplainably altered. Records of Mitnick's arrest and conviction cannot be found on the Court's computers at Santa Cruz (CA)
- Winter. The MOD-LOD war reaches a crescendo

1991

- February. CPSR Roundtable in Washington D.C.
- February. Mark Abene (aka *Phiber Optik*) is arrested and charged with computer tampering and computer trespass in the first degree, New York state offenses. Abene, who is a minor, pleads "not guilty" to the first two offences and ultimately accepts a plea agreement to a lesser misdemeanour charge. He will be sentenced to 35 hours of community service. Mark was once a member of the hacker groups Legion of Doom and MOD. At very young age he used his computer to dial-up to BBSes and CompuServe time-sharing service. Getting through the BOCES educational program, he realised how to edit, save and reload programs on DEC minicomputers remotely. In the mid-1980s he joins to the Legion of Doom (LOD) to explore telecommunications systems, minicomputer and mainframe OSs. The eventual decline of the LOD toward the late 1980s caused Abene to join the MOD

- March 25-28. Computers, Freedom and Privacy conference in San Francisco
- April. Kevin Poulsen (aka *Dark Dante*) is arrested by FBI on charges of fraud and money laundering
- May 1. Electronic Frontier Foundation, Steve Jackson, and others file suit against members of Chicago Task Force
- May. Comsec Data Security is founded in Huston Texas by Chris (aka Erik Bloodaxe), Scott Chasin, Kenyon Shulman and Rob —. They offer security services to business companies. Time and Newsweek articles refer about the "hackers-turned-anti-hackers". The hackers community is displeased
- May 31. An hacker breaks into Southwestern Bell network through Tymnet to steal anti-hacker memos stored into the Bellcore's directory. Tom Kaiser traces the hacker's call to a AT&T long-distance trunk line toll-free 800 number in Pennsylvania, and then from subscriber number 555-1318, building 64A Kosciusko Street, Brooklyn NY. This is the home of *Corrupt* of MOD. Few days ahead another Tom Kaiser's successful trace brought to another MOD's intruder called Julio Fernandez (aka Outlaw). Corrupt, Outlaw and Phiber Optik had one objective, to get control of the switch serving Comsec's activity, like eavesdropping phone calls, etc. The password to Tymnet was provided to them by Jason Snitker (aka *Parmaster*). Tymnet was a huge network where big corporations and government agencies talk one another.
- July 1-2. Switching station phone software crash affects Washington, Los Angeles, Pittsburgh, San Francisco
- September 17. AT&T phone crash affects New York City and three airports
- Justin Tenner Petersen (aka *Agent Steal*) is arrested in Texas

1992

- January. Mitnick's brother, Adam, is found dead of a drug overdose in his car
- June. Several MOD's member are charged of 11 counts, each punishable by 5 years of jail or more, and carries up to $250k. Among counts were conspiracy, unauthorized access to switches and Tymnet, possession of long-distance calling card numbers, wire fraud. There will never be a trial. All of them will plead guilty. Paul and Eli get 6 months of jail and 6 months of home detention. John had 1 year of jail and 3 years of supervised release, plus 200 hours of community service. Julio will offer to testify against Mark. No jail for him.
- Kevin Mitnick (aka *Condor*) first meet Justin Peterson (aka Eric Heinz), an FBI informant trying to gather evidence agains him
- The L0pht hacker think tank is founded in Boston by *Brian Oblivion*, *Count Zero*, *White Knight* and *Golgo 13*. There is a link between L0pht and cDc: *White Knight* and *Count Zero*, as well as recent members *Dildog* and *Mudge*, are all members of cDc. L0phtCrack is one of the tools crafted by the group

1994

- The *Level Seven Crew*, a powerful hacktivist group during the mid to late 90's in US, is founded. Level Seven typify a group of hackers who act for reasons other than money or passion for challenges. They used their computer skills to make political statements and protest actions by government and industry. The name is derived from the Dante's Divina Commedia, where the seventh level of hell is reserved to the violent people

- The Network Crack hacking group formed
- June. Kevin Poulsen pleads guilty to 7 counts of conspiracy, fraud, and wiretapping. He is sentenced to 5 years in a federal penitentiary, as well as banned from using computers or the internet for 3 years after his release
- Motorola's Cellular Division reports that copies of their cellular control software have been taken from a breached computer system. Techniques of the break-in are typical of the Condor, whom FBI agents are still in search of by November of 1992, when he had disappeared from the face of the earth. He is suspected of having hacked into the computers of the California Dept. of Motor Vehicles, cracking an Army computer system, and gaining access to FBI records
- December 25. Tsutomu Shimomura, age 30, is a computational physicist and a brilliant computer scientist, system administrator at the San Diego Supercomputer Center (SDSC) and consultant to hundreds of corporate and government institutions, like the Air Force, NSA, FBI. On Christmas day Shimomura is in San Francisco, preparing his vacation in Sierra Nevada, where he's used to spend most of winter. On December 26, before he could leave for the mountains, he receives a call from his colleagues at the SDSC. The day before someone had broken into his home computer, which was connected to the SDSC's network via Internet. The attack had been started from a commandeered computer at Loyola University of Chicago. Using a spoofing technique the intruder masqueraded as a trusted computer. At the Center they had been able to detect the intrusion because one of Shimomura's machines routinely mailed a copy of several record-keeping files to a safe computer. This precaution led to an automatic warning to employees of the SDSC that an attack pwas under way. Shimomura immediately returned to his beach cottage near San Diego, in Solana Beach (CA), where he found that the hacker had stolen hundreds of important files from his computer. This was no random ransacking: the information would be useful to anyone interested in breaching the security of computer networks or cellular phone systems. Taunting messages for Shimomura were also left in a computer-altered voice on his personal voice mailbox at the SDSC "Damn you! My technique is the best... Don't you know who I am?... Me and my friends... We'll kill you!". Another voice said "OK boss, your kung-fu pretty good!". Those messages, as we'll say in a moment, will be the Mitnick's fatal error. At this moment Shimomura doesn't know that yet, but the hacker had stashed the stolen files, along with more than 20000 credit card accounts of Netcom, Inc. - a ISP based in San Jose - into an account at "The Well", a large internet provider for the San Francisco Bay Area. The account belongs to an online community of computer programmers called *Computers, Freedom and Privacy*. On 1995 January 27 Bruce Koball, a computer programmer in Berkeley and the account's subscriber, is contacted by "The Well" because they noticed an unusually large amount of data in the account, which was normally almost empty. Koball found Shimomura's name on some of the files. The day after Koball reads in the New York Times the story about the attack on Shimomura's computer. Koball quickly realizes that someone had broken in and filled the account's directory with Shimomura's files. Well officials calls in Shimomura. Federal authorities were also contacted when the credit card informations were discovered. Shimomura decides to track down the intruder. His motivation is part work and part revenge. The FBI's database comes up with a list of possible suspects. Kevin D. Mitnick is one of a few at the top of the list. One of Mitnick's "rules of thumb" was never to keep incriminating data on his own machine. Another clue that made Mitnick a suspect, was the cellular phone control software files, also found in the account. More specifically, it was source code software developed under a grant from the NSA worth $500k to $1M, called Berkeley Packet Filter, that can be used to control the operations of cellular telephones made by Motorola, NEC, Nokia, Novatel, Oki, Qualcomm and other manufacturers. That would be consistent with the kind of information of interest to Mitnick, who had first made his reputation by hacking into telephone networks. Shimomura began to set a trap for the prowler. Shimomura, Andrew Gross (a colleague from the SDSC), and Julia Menapace (an independent computer consultant), set up a temporary headquarters, attaching 3 laptop computers to the Well's internal network. First, the intruder's voice is posted as a sound file on the internet for all to hear... Next, a 24 hour monitoring

computer is set up to record any unusual activity at "The Well". Shimomura would patiently watch as the bandit returned again and again across the screen. The trap had worked and the bait is taken. Another altered voice mail message is left on Shimomura's mailbox mockingly saying "Ah Tsutomu, my learned disciple, I see that you put my voice on the Net... I am very disappointed my son...". Initially Shimomura set up his operation at the Well. But by February 8, concluding that the intruder was getting into the Well through Netcom, Shimomura and his team set up new monitoring stations there, in San Jose. They worked 20 hours a day, much of it at "listening stations," computers set up to sound an alarm when Mitnick's calls came through. Shimomura eventually determines that Mitnick was operating through a modem connected to a cellular telephone somewhere near Raleigh, with an approximation of 2 km. He flew to Raleigh, where he helped telephone company technicians and federal agents in using cellular-frequency scanners to locate Mitnick’s apartment.

1995

- February 15, Wednesday, 1:30 a.m., well-known computer hacker and federal fugitive Kevin Mitnick (aka *Condor*), age 31, is arrested by FBI at his apartment 202 at Players Club, near Raliegh (NC), where he was living alone under an assumed name Glenn Thomas Case, on federal offences related to a 2 and half year period of computer hacking which included computer fraud, cellular phone fraud, wire fraud, theft of thousands of data files and at least 20000 credit card numbers from computer systems around the nation. He was found with cloned cellular phones, more than 100 clone cellular phone codes, and multiple pieces of false identification. When agents knocked on the Mitnick’s door, he took about five minutes to open the door, then surrendered peacefully to FBI agents.

Mitnick had setup a communication system such complicated that made tracing the calls almost impossible even to best of experts in the field: a cellular modem was used to dial into a Sprint Cellular site on the reverse channels - these are the channels usually reserved for mobile to base communications - then he dialed into a GTE switching office and re-routed his call to Colorado where he dialed into a Netcom internet connection.
Shimomura did make the
difference in bringing him to justice.
Federal officials say Mitnick's motives always have been murky. There is no evidence yet that Mitnick had attempted to use the stolen credit card accounts for personal financial gain. Mitnick often has seemed more concerned with proving that his technical skills are better than those whose job it is to protect the computer networks he has attacked.
Shimomura was present Wednesday at Mitnick's pre-arraignment hearing at the federal

courthouse in Raleigh. At the end of the hearing, Mitnick turned to Shimomura, whom he had never met face to face, and said "Hello, Tsutomu, I respect your skills." Shimomura nodded solemnly. Although Mitnick apparently respects the man who tracked him down, Shimomura does not reciprocate. "From what I have seen, he doesn't have a whole lot of expertise," he said.

- March 28. At the Fifth Conference on *Computers, Freedom, and Privacy*, held in Burlingame (CA) Chairman Carey Heckman says "Mitnick has created a Sputnik like urgency for higher computer security"
- July 10. Kevin Mitnick (aka *Condor*) is tried on a 23 count Federal Indictment, charging him with crimes such as wire fraud, computer fraud, cellular phone fraud, and using illegal telephone access devices to divert toll costs. Already wanted for previously violating his probation, Mitnick's violations includes other charges covering 6 jurisdictions, and facing a maximum of 20 years for each of the 23 counts. Mitnick is charged with violation of 18 US Code, Section 1029 (Fraud and Related Activity in Connection With Access Devices) in violation Title 18, Section 1038 (Fraud and Related Activities in Connection with Computers)

- SSH protocol is released
- November. Justin Peterson is sentenced to 3.4 years in US federal prison and 3 years of probation, and payment of restitution of $40K

Riuscì inizialmente ad evitare il carcere collaborando come informatore dell'FBI, oltre a mettere le sue competenze al servizio dell'agenzia. Nonostante questa opportunità, Agent Steal nonriuscìatenersilontanodai guai e, dopo un nuovo periodo di latitanza, fu condannato a 41 mesi di prigione. Fu trovato morto per cause naturali nel suo appartamento, nel 2010.

1998

- May 19. The seven members of L0pht Heavy Industries, *Brian Oblivion*, *Kingpin*, *Mudge*, *Space Rogue*, *Stefan Von Neumann*, *John Tan*, *Weld Pond*) testify before a US Senate committee that they could shut down the entire Internet in 30 minutes. Their pointing out about the serious vulnerabilities of the Internet will remain largely ignored

- August 1. At DEF CON 6 the tool *Back Orifice* computer program is presented. Written by cDc member *Sir Dystic*, this is a program for controlling a computer running Microsoft Windows fremotely. The name is a pun on Microsoft BackOffice Server software. Its purpose was to demonstrate the lack of security in Windows 98
- Cheng Ing-Hau creates CIH virus aka Chernobyl. It was programmed to infect windows 95/98/Millennium on 26th of April, anniversary of Chernobyl disaster. Quando un file qualsiasi infettato veniva eseguito, il virus creava un loop infinito che mandava il pc nella schermata blu della morte la cosiddetta Blue screen of death e successivamente sovrascriveva il bios della scheda madre rendendo il pc completamente inutilizzabile

1999

- September 7. The Level Seven Crew defaces the website of the US embassy in Chinas, in regards to the 1998 US embassy bombings. vent writes "We embrace technology, we learn from it, we use it, and we exploit it. Technology is a very powerful tool, as is knowledge, but some people go beyond these boundaries, testing limits, finding new ways and ideas... we call these people hackers, and we are one of many.."
- Kevin Mitnick (aka *Condor*) is sentenced to 5 years in a federal penitentiary. Having pleaded guilty for some of the counts, he will serve 46 months in prison, 8 months of which in solitary confinement because, according to Mitnick, law enforcement official Leon Weidman convinced a judge that he had the ability to "start a nuclear holocaust by whistling into a telephone".

2000

- January 21. Kevin Mitnick (aka *Condor*) is released. In this photo Adrian Lamo, Kevin

Mitnick and Kevin Poulsen in 2001

- February 25. *vent* is raided

2002

- Kevin Mitnick publishes The Art of Deception, a book in which he states that he compromised computers solely by using informations that he gained by Social Engineering, which he defines “the casual or calculated manipulation of people to influence them to do things they would not ordinarily do”.

2003

- Anonymous is created as a leaderless internet group for those who fights for the rights for privacy. Members use to hide their face behind the mask of Guy Fawkes. The movement’s origin begins with the online image-based bulletin board 4chan. The name is inspired by the perceived anonymity under which users posts on 4chan.
- September. The Pirate Bay (TPB) is established by the Swedish anti-copyright organisation Piratbyrån (The Piracy Bureau), an organisation that encourages copying of media over copyright. TPB was first run by Gottfrid Svartholm (aka *anakata*) and Fredrik Neij (aka *TiAMO*). They maintan a huge *tracker*, a cluster of servers used to coordinate peer-to-peer file sharing through Bit Torrent.

2006

- May 31. The Pirate Bay and The Piracy Bureau are accused of "assisting in making copyrighted content available" by the Motion Picture Association of America. The website's servers in Stockholm are raided and taken away by Swedish police, leading to 3 days of downtime.
- Julian Assange, a former Australian computer hacker, founds Wikileaks.org. The website aims to provide a platform for whistleblowers to post sensitive and secret political documents while keeping their identity anonymous
- Anonymous runs DDoS attacks on PayPal, Mastercard and Visa in protest at the

companies' refusal to handle donations to the free information group WikiLeaks. Sabu actively promotes this campaign
- The penetration testing distribution BackTrack is released by Mati Ahatoni and Max Moser

2008

- January 14. A promotional video is leaked on YouTube, showing Tom Cruise touting the benefits of Scientology, a religion founded by L. Ron Hubbard in 1965. The Church of Scientology states the video is a "pirated and edited version" of a three-hour video produced for members of Scientology, and issues a copyright violation claim against YouTube. YouTube removes the video.
- January 21. Anonymous hacker collective starts "Project Chanology", aimed to destroy Scientology, accused of removing the video of Tom Cruise from YouTube, because it portrayed the church in a negative light. Anonymous strikes back by posting a video to YouTube called "Message To Scientology", in which group says they want to uncover how danger Scientology actually is, and how the removal of the Tom Cruise video violates free speech. This was followed by DDoS attacks to the cult's organization, and soon after, black faxes, prank calls, and other measures intended to disrupt the Church of Scientology's operations. In February of the focus of the protest shifted to legal methods, including nonviolent protests and an attempt to get the Internal Revenue Service to investigate the Church of Scientology's tax exempt status in the US.

- Found vulnerability in Debian implementation of OpenSSL's PRNG used for generating keys for asymmetric cryptography. The seed was made equal to the process PID, limiting the possible seeds to 0..32768

2009

- April 17. After a trial of 9 days, members of TPB Peter Sunde, Fredrik Neij, Gottfrid Svartholm, and Carl Lundström are found guilty of assistance to copyright infringement and sentenced to 1 year in prison and payment of a fine of SEK 30M. The defendants appealed the verdict and accused the judge of giving in to political pressure. The accuse will be rejected and the court will emit the sentence in 2010

2010

- January 5-8. Transgender American soldier Chelsea Manning downloads from the Afghanistan database the 400000 documents that became known as the Iraq War logs, plus 91000 documents known later as part of the Afghan War logs. She saved the material on CD.
- February 3. Chelsea Manning sends to WikiLeaks the Iraq and Afghan War logs via Tor.

- October, Wikileaks releases some 400000 accounts written by American soldiers from 2004 to 2009 revealing that the US decided to ignore cases of torture by Iraqi authorities on civilians. Chelsea Manning, un soldato transgender aveva prelevato queste informazioni, ma fu poi scoperto grazie a una segnalazione del grey hat Adrian Lamo
- March 13, Justin Petersen is found dead in his apartment in LA. While tasked with helping FBI to catch other hackers and fugitives, he had continued to commit serious crimes
- TeaMp0ison black hat group is founded by Trick. They are political activists. Their motto is “Knowledge is power”
- January 1. *The Jester* begins a campaign against the Taliban's website. On November 28, The Jester posts several tweets claiming to be responsible for the downtime WikiLeaks was experiencing. *The Jester* (aka *th3j35t3r*) is a famous grey hat hacktivist. Abandoned US Army (he served in Afghanistan) he develops a DDoS tool called XerXeS to conduct a cyberwar against islamic jihadists and fundamentalists in the name of American patriotism, and subsequently Anonymous and WikiLeaks, guilted of exposing US soldiers safety in conflict areas. *The Jester* loathed *Sabu*, leader of Anonymous. The two stood at opposite sides on nearly any given topic. During the first half of 2011, *Sabu* and *The Jester* tried repeatedly to uncover each other’s identity.

2011

- 30 May to 2 June. LulzSec hackers break into Sony Pictures Europe's website by SQL injection. They steal, and eventually publish, names, birth dates, addresses, emails, phone numbers and passwords of thousands of people who had entered contests promoted by Sony. The breach ultimately cost the company more than $600K.
- June 7th. In Manhattan FBI agents knock the door of In NY federal agents arrest Hector Xavier Monsegur (aka aka *Sabu*), 28, Puerto Rican, and arrest him who is publicly known as , . Monsegur had been implicated in dozens of illegal, high-profile hacks, not to mention multiple DDoS attacks. Sabu was the charismatic leader of Anonymous implicated in dozens of illegal, high-profile hacks, not to mention multiple DDoS attacks.. During Sabu’s reign, Anonymous gained popularity over the media. Sabu collected a smaller cadre of hacktivists from Anonymous and named it LulzSec, which became famous very quickly for a series of high-profile hacks, including like the attack of Sony Pictures. At the time Sony Pictures was running several prize giveaways as part of a marketing campaign. LulzSec used a basic SQL injection to breach the SonyPictures.com database and grabbed the usernames, passwords, and personal profiles of over one million registered users. By that moment, Sabu became number one on the FBI’s most wanted cybercriminal list. After his arrest, Monsegur is pleaded guilty to 12 charges, including 3 of conspiracy to hack into computers, 5 of hacking, 1 of hacking for fraudulent purposes, 1 of conspiracy to commit bank fraud, and 1 of aggravated identity theft.After his arrest, Ffacing a sentence of 25 to 100 years in prison, Monsegur struck a deal in which he agreed to turn over his friends from LulzSec

to the authorities. Many will serve long jail sentences and owe hundreds of thousands of dollars in restitution to the organizations they once brazenly penetrated. Many in Anonymous felt betrayed by Monsegur's cooperation with the authorities and publicly called him out. From being one of the most beloved hacktivist, Munsegur became the most loathed figure on cyberspace.

2012

- *Kim Dotcom*, founder of Megaupload, is arrested
- TeaMp0isoN disbanded following the arrests of 3 of its core members, *Trick*, *MLT* and *hex00010*. They were responsible for hacking Facebook, UN, NASA, NATO, leaking of Tony Blair address book, and defacing the official BlackBerry blog as a response to RIM, the maker of the BlackBerry, promising to co-operate with the police in the 2011 England riots.
- March 5. *The Jester* changes his Twitter account @th3j35t3r avatar to a QR code without comment or explanation. Scanning the QR code with a smartphone redirects the browser to a URL displaying an image of his signature and an embedded, hidden code that allegedly exploited a browser vulnerability (CVE-2010-1807), capable of triggering arbitrary code execution, such that the "device would silently make a TCP shell connection back to my remote server," The Jester wrote. "Like a phone call, if you like". The Jester uses this hack to track his detractors

2013

- February 12. US President Obama issues EO 13636, "Improving Critical Infrastructure Cybersecurity"
- May 20. CIA employee and contractor Edward Snowden moves from Haiti to Hong Kong, where on early days of June he will leak thousands of classified NSA documents to journalists. His disclosures reveal global surveillance programs run by the NSA with the cooperation of telco companies and European governments.
- June 21. The US Department of Justice unseals charges against Snowden of violating the Espionage Act of 1917 and theft of government property. Snowden's passport is revoked
- June 23. Snowden lands at Moscow. He is granted the right of asylum from Russia, where he lives in an undisclosed location

- October. At the Glen Park branch of the San Francisco Public Library, Ross Ulbricht (aka *Dread Pirate Roberts*) is arrested by FBI agents. He is accused of being the "mastermind" behind the Silk Road, a website in the Dark Web where he run illegal tradings and traffic of narcotics under anonymity guaranteed by Tor and bitcoin. Ulbricht was born and educated in Austin, Texas (US). By the time he graduated from Pennsylvania State University in 2009 Ulbricht developed his personal economic view. He started Silk Raod on February 2011 "as an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force".
- July 2. *The Jester* (aka th3j35t3r) takes responsibility for a series of DoS cyberattacks

against the Ecuadorean stock exchange and the country's tourism website, and promise to attack any other governments considering granting asylum to Edward Snowden, accused to be “a traitor who has jeopardized all our lives”.
- March. The penetration testing distribution Kali Linux 1.0 is released. The project to turn BackTrack into a real Debian distro had started in 2012

2014

- Sony Pictures’s internal network data are stolen by the North Corean Lazarus Group
- May 27. Hector Xavier Monsegur is freed. Thanks to his three years long “extraordinary cooperation” with the FBI, many members of LulzSec are now serving long jail sentences and owe hundreds of thousands of dollars in restitution to the organizations they once brazenly penetrated. Many in Anonymous felt betrayed by Monsegur’s cooperation with the authorities and publicly called him out. Then, from being one of the most beloved hacktivist, Munsegur became the most loathed figure on Internet. Monsegur told the court: “I’m not the same person I was three years ago. I’ve come a long way. I’ve had to do a lot of thinking and soul-searching.”

2015

- Chrysler announced that it's issuing a formal recall for 1.4 million vehicles that may be affected by a hackable software vulnerability in Chrysler's Uconnect dashboard computers.
- February. Ross Ulbricht (aka Dread Pirate Roberts) is convicted of money laundering, computer hacking, conspiracy to traffic fraudulent identity documents, and conspiracy to traffic narcotics by means of the Internet.
- AnonCoders group of hackers gets started. Using defacements, DoS attacks, database hijacking, database leaks, admin panel takeovers, social media accounts and other methods, it mainly targets political groups and anti-Islam websites. The group has vandalized sites in Israel, Europe, and the United States.ku200it
- August. Kali Linux 2.0 is published

2016

- From july a number of DDoS attacks are conducted by a botnet called Mirai. Most of the victims are IoT devices, like cameras, DVRs and routers
- Edward Snowden becomes the president of the Freedom of the Press Foundation, an organization that aims to protect journalists from hacking and government surveillance
- OurMine, a black hat hacker group based in Saudi Arabia that compromised celebrities internet accounts (mainly Twitter and Facebook), often causing cybervandalism. By 2017, victims include Wikipedia co-founder Jimmy Wales, Google CEO Sundar Pichai, Facebook co-founder Mark Zuckerberg, Sony President Shuhei Yoshida, the New York Times, Game of Thrones, Playstation, Real Madrid, CNN. In October BuzzFeed publishes an article linking OurMine to a Saudi Arabian teenager using moniker Ahmad Makki on social media. OurMine denies the allegations. The day after the article's publication, OurMine defaces BuzzFeed's website altering several posts to read "Hacked By OurMine".

2017

- August 31. *OurMine* leaves a message on the homepage of WikiLeaks: “Hi, it’s OurMine (Security Group), don’t worry we are just testing your…. blablablab, oh wait, this is not a security test! Wikileaks, remember when you challenged us to hack you?"

2018

- May, GDPR (General Data Protection Regulation)

2019

- April, Julian Assange raided by British police. The Ecuador government has revoked the political asylum
- August 8. Armis Labs discloses “URGENT/11”, 11 zero day vulnerabilities affecting since

2006 TCP/IP stack of VxWorks, the OS used by over 2 billion devices including critical industrial, medical and enterprise devices. 6 of the vulnerabilities are classified critical

Sources

J. R. Minor, The true story of Kevin Mitnick - World famous Computer Hacker (1995)
J. Meyer, L.A. Hacker to Waive Extradition, LA Times, Feb 17, 1995. p B1
J. Johnson, A Cyberspace Dragnet Snared Fugitive Hacker, LA Times, Feb 19, 1995. p A1
M. Slatalla and J.Quittner, *Masters Of Deception, The Gang That Ruled Cybersapace*, 1995
K. Mitnick, *Gost in the Wires*, 2011
K. Mitnick, *The Art of Deception*, 2002