Dynamic Chiropractic

NEWS / PROFESSION

A Brief History of Computer Hacking

Michael Devitt

Computer hackers have existed almost as long as computers In fact, "hackers" have been in existence for more than a century. In 1878, just two years after the telephone was invented by Alexander Graham Bell, a group of teenage boys hired to run the switchboards were kicked off of a telephone system in New York. The reason? The boys were more interested in knowing how the phone system worked than in making proper connections and directing calls to the correct place. In essence, they were trying to "hack" the system to see how it worked.

Originally, "hacker" did not carry the negative connotations now associated with the term. In the late 1950s and early 1960s, computers were much different than the desktop or laptop systems most people are familiar with. In those days, most companies and universities used mainframe computers: giant, slow-moving hunks of metal locked away in temperature-controlled glass cages. It cost thousands of dollars to maintain and operate those machines, and programmers had to fight for access time.

Because of the time and money involved, computer programmers began looking for ways to get the most out of the machines. The best and brightest of those programmers created what they called "hacks" - shortcuts that would modify and improve the performance of a computer's operating system or applications and allow more tasks to be completed in a shorter time.

Not until the early 1980s did the word "hacker" earn disdain, when people like Kevin Mitnick, Kevin Poulsen and Vladimir Levin (more on them later) began using computers and the internet for their own questionable gains. Still, for all the negative things hackers have done, I believe they provide a necessary (and even valuable) service, which I'll elaborate on after a brief timeline of some of the high points (or low points, depending on how you look at it) in the history of computer hacking

Computer Hacking: A Timeline

1971: Computer hobbyist John Draper discovers that a toy whistle included in a box of children's cereal reproduces exactly the 2600-hertz audio tone needed to open a telephone line and begin making free long-distance calls. He adopts the moniker "Captain Crunch," after the cereal and is arrested dozens of times in the next few years for phone tampering.

1975: Two members of the Homebrew Computer Club of California begin making "blue boxes," devices based on Draper's discovery that generate different tones to help people hack into the phone system. Their names? Steve Wozniak and Steve Jobs, who would later go on to found a company called Apple Computers in 1977.

1983: The movie "War Games," starring Matthew Broderick, is released in theaters. Broderick plays a teenage hacker who taps into a Pentagon supercomputer nicknamed "WOPR" and nearly starts World War III. (WOPR is a spoof of NORAD's old central computer processing system, which had the acronym "BURGR.")

In one of the first high-profile cases against computer hackers, the FBI arrests six teenagers from

Milwaukee known as the "414s," named after the city's area code. They are accused of breaking into more than 60 computer networks, including those of Memorial Sloan-Kettering Cancer Center and Los Alamos National Laboratory. One hacker gets immunity for his testimony; the others are given probation.

1984: Eric Corley begins publishing an underground magazine called *2600: The Hacker Quarterly,* which quickly becomes a clearinghouse for telephone and computer hacking. The following year, a pair of journalists from St. Louis begin publishing Phrack, an electronic magazine that provides hacking information.

The Comprehensive Crime Control Act is passed, which gives the Secret Service jurisdiction over cases of credit card and computer fraud.

1986: Congress passes the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, which makes it a crime to break into computer systems. In typical congressional fashion, the law doesn't apply to those individuals largely responsible for computer crimes - juveniles.

1987: Herbert Zinn, a 17-year-old high-school dropout who lives with his parents in Chicago and goes by the nickname of "Shadow Hawk," is arrested and admits to breaking into AT&T's computer network after bragging about it on an electronic bulletin board. Federal authorities say the teenager - who did most of his hacking from a computer in his bedroom - was only a few steps away from tapping into the company's central telephone switching system, which could have brought most of the nation's telephone networks and communications systems to a standstill.

Brain, the first known MS-DOS computer virus, is released on the internet. The program itself is mostly harmless; users whose computers are infected with the virus find a small file added to their hard drive containing an unencrypted text message giving contact information for a "Brain Computer Services" in Pakistan.

1988: Robert Morris, a 22-year-old graduate student from Cornell University releases a self-replicating virus on the Internet designed to exploit security holes in UNIX systems. The virus eventually infects more than 6,000 systems - roughly one-tenth of the Internet's computers at the time - and virtually shuts down the entire network for two days.

Morris is arrested for releasing the virus and is sentenced to three years probation, 400 hours of community service and a $10,000 fine. Despite the online havoc he wreaks, he's more than absolved by the Internet community; he later forms a startup internet company, Viaweb, which is bought in 1998 for approximately $49 million.

As a result of the Morris virus, the federal government forms the Computer Emergency Response Team. Based at Carnegie Mellon University in Pittsburgh, its mission is to investigate attacks on computer networks.

1989: Five West German computer users are arrested on espionage charges after an administrator at UC Berkeley detects and tracks their intrusions into U.S. government and university computer systems. The hackers are charged with selling information and software to the KGB; three are convicted and sentenced to prison terms, but none of the hackers ever spends any time behind bars.

In a separate incident, a hacker who goes by the name of "The Mentor" publishes a now-famous treatise on hacking, *The Conscience of a Hacker.* The work ends with the line: "You may stop this individual, but you can't stop us all."

1990: Four members of a band of hackers from the Southeastern United States affectionately known as the "Legion of Doom" are arrested for stealing the technical specifications for BellSouth's 911 emergency telephone network. The hackers are accused of lifting login accounts, passwords and connect addresses for its computer networks, information that could "potentially disrupt or halt 911 service in the United States," according to a subsequent indictment. Three of the hackers are found guilty and given prison sentences ranging from 14 to 21 months; they are also ordered to pay BellSouth nearly a quarter of a million dollars in damages.

The Secret Service, in conjunction with Arizona's organized crime unit, unveils Operation Sundevil, a nationwide project designed to hunt down computer hackers. They eventually seize computer equipment in 14 cities, including Tucson, Miami and Los Angeles.

The Electronic Frontier Foundation is created, with the primary goal of defending the rights of people accused of computer hacking.

1991: The General Accounting Office reveals that during the Gulf War, a group of Dutch teenagers broke into a Defense Department computer network and gained access to "sensitive" information on war operations, including data on military personnel, the amount of military equipment being sent to the Persian Gulf, and the development of certain weapons systems.

1993: After hackers break into AT&T's computer networks and bring long-distance telephone service to a halt on Martin Luther King Jr. Day, the Secret Service initiates a national crackdown on computer hackers, arresting members of a group titled "Masters of Deception" in New York, and other hackers in St. Louis and Austin, Texas. The members all plead guilty of computer crimes and conspiracy.

Twenty-eight-year-old Kevin Poulsen, who was already facing charges for stealing military documents and disrupting telecommunications services, is charged along with two other hackers, of using computers to rig promotional contests at three Los Angeles radio stations. In a rather ingenious scheme, Poulsen and his cohorts use computers to seize control of incoming phone lines at the radio stations and make sure that only their calls get through. The three hackers wind up "winning" two Porsches, $20,000 in cash and two trips to Hawaii before being caught.

1994: Two hackers (known as "Data Stream" and "Kuji") break into several hundred computer systems, including NASA and the Korean Atomic Research Institute. After a lengthy manhunt, detectives from Scotland Yard finally corral "Data Stream," a 16-year-old boy who curls up in the fetal position and cries when captured.

A temporary worker at British Telecom breaks into a computer network that contains a number of highly sensitive telephone numbers, including those of the Queen, Prime Minister John Major, and several top-secret military installations, all of which are then posted live on the internet.

1995: Russian hacker Vladimir Levin is arrested in Britain after allegedly using his laptop computer to break into Citibank's computer network and transfer funds to various accounts around the world. Levin is eventually extradited to the U.S., where he is sentenced to three years in prison and order to pay Citibank $240,000. The exact amount of money stolen by Levin remains unknown; estimates range between $3.7-$10 million.

Legendary computer hacker Kevin Mitnick is arrested in Raleigh, North Carolina and accused of a number of security violations, such as copying computer software, breaking into various networks and stealing private information, including 20,000 valid credit card numbers. He spends four years in jail without a trial, then pleads guilty to seven counts in March 1999 before finally being released on parole in January 2000. Mitnick had previously been convicted of stealing software and long distance telephone codes from two telecommunications companies in 1989.

1996: The General Accounting Office release a report that states that hackers attempted to break into Defense Department files more than 250,000 times in 1995 alone; about 65 percent of the attempts were successful.

In August, hackers defame the U.S. Department of Justice website, adding swastikas, obscenities and a picture of Adolf Hitler to the site and renaming it the "Department of Injustice." The following month, a group called the Swedish Hackers Association breaks into the CIA's website, altering the front page's look and changing the organization's name to the "Central Stupidity Agency."

1997: The hacking program "AOHell" is released, aimed at wreaking havoc for users of America Online. For days, the AOL network is brought to a virtual standstill, as hundreds of thousands of users find their mailboxes flooded with multiple-megabyte e-mail messages and their chat rooms disabled or disrupted with "spam" messages.

1998: The Symantec AntiVirus Research Center, a leader in security and antivirus software, reports that 30,000 computer viruses are circulating "in the wild" on the internet.

For the first time, federal prosecutors charge a juvenile with computer hacking after a boy shuts down the Bell Atlantic airport communications system in Worcester, Massachusetts. The boy's attack interrupts communications between airplanes and the control tower at Worcester Airport for more than six hours, but no accidents occur. The boy, whose name and exact age are not released, pleads guilty and is sentenced to two years probation, 250 hours of community service, and is ordered to repay Bell Atlantic $5,000.

Members of a hacking group called the Masters of Downloading claim to have broken into a Pentagon network and stolen software that allows them to control a military satellite system. They threaten to sell the software to terrorists. The Pentagon denies that the software is classified or that it would allow the hackers to control their satellites, but later admits that a less-secure network containing "sensitive" information had been compromised.

Deputy Defense Secretary John Hamre announces that hackers have carried "the most organized and systematic attack the Pentagon has seen to date" by breaking into unclassified computer networks, then viewing and altering payroll and personnel data at dozens of federal agencies. Two teenagers from Cloverdale, California are originally implicated. Three weeks later, authorities arrest an Israeli teenager known as "The Analyzer," who claims to have taught the two Californians how to conduct the attacks.

Two hackers are sentenced to death by a court in China for breaking into a banks computer network and stealing 260,000 yuan ($31,400).

U.S. Attorney General Janet Reno announces the creation of the National Infrastructure Protection Center, an organization designed to protect the nation's telecommunications, technology and transportation systems from hackers.

In May, members of "L0pht," a well-known hacker group, testify before Congress. They cite serious security weaknesses in many of the government's computer networks; one member claims that if the group wanted to, it could shut down the entire internet in half an hour.

Two "internet terrorists" defame the New York Times website, renaming it "Hackers for Girls" and expressing anger at the arrest of Kevin Mitnick, who was the subject of a book written by a reporter at the *Times.*

The hackers group Legion of the Underground (LoU) breaks into China's human rights website in October and replaces the front page with a message asking consumers and businesses to boycott all Chinese goods and services. A few months later, LoU issues a statement declaring a "cyber war" on Iraq and China calling for "the complete destruction of all computer systems" in those countries.

1999: In March, a hacker by the name of MagicFX breaks into the popular online auction site E-Bay, destroying the site's front page. According to the company, the attack was so severe that MagicFX was able to change auction prices, post fake items for sale, and divert traffic to other sites.

Throughout May and June, dozens of government and consumer sites, including those of the U.S. Senate, the White House and the U.S. Army, fall prey to cyber attacks. In each case, the hackers defame the site's front page with arcane messages that are quickly erased.

In November, a Norwegian hacker group, MoRE (Masters of Reverse Engineering), cracks a key to decoding copy-protected DVDs. The group creates a DVD decoder program, which is widely distributed for free on the internet.

2000: The Symantec AntiVirus Research Center estimates that one new computer virus "enters the wild" every hour of every day.

In a 72-hour period in early February, more than a dozen of the internet's most popular websites, including Yahoo, Buy.com, Amazon.com, E-Bay, CNN.com, eTrade and ZDNet, are hacked via "denial of service" attacks that overloaded the sites' servers with an overwhelming number of information requests.

The "I Love You" virus debuts on the Internet in May, appearing first in the Philippines, then spreading across the globe in a matter of hours. It causes an estimated $10 billion of damage globally in lost files and computer downtime before a solution is found.

The trade publication *Computer Economics* estimates that computer viruses will cost companies a total of $17 billion worldwide in ruined or lost data and lost production time.

A study released by PC Data in the summer reveals an alarming trend: although most people have some type of antivirus software on their personal computer, almost 45 percent of those who log onto the Internet regularly still don't have that software engaged, even if it's installed. In effect, this leaves nearly half of all home computer users exposed and vulnerable to attack from a virus.

In October, in what many people see as a fit of poetic justice, software giant Microsoft admits to having its computer network infiltrated by a hacker (or hackers) from Russia. According to company statements, the hacker(s) used a trojan horse program to create a surreptitious e-mail account and were able to access the source code of an as-yet-unnamed Microsoft product still being developed. Microsoft security experts later admit they were able to track the movements of the hacker(s) throughout their network but were unable to actually catch them in the act.

2001: In early May, groups of Chinese hackers infiltrate several U.S. government sites, including those of the White House, the Central Intelligence Agency, and the Department of Health and Human Services. The attacks are believed to be a form of retaliation for an incident involving a U.S. spy plane earlier in the year.

Also in early May, Microsoft websites in the U.S., Great Britain, Mexico and Saudi Arabia are temporarily disrupted by distributed denial-of-service (DDOS) attacks.

Don't Hate the Hacker

Having just read this timeline, I'm sure that few (if any) of you probably feel sorry for computer hackers. I can't blame you. Like hundreds of companies, *Dynamic Chiropractic* fell victim to the "I Love You" virus late last year; in fact, I was the one who accidentally opened the file containing the virus. As a result, our company's e-mail system was shut down for two days, and it took the better part of a week before every computer in the office was declared virus-free.

Because of that virus, our company has instituted a policy whereby every computer in the office automatically receives the latest virus updates weekly, and every file sent to *DC* via e-mail is scanned for viruses before it is opened. Those policies weren't in place before the virus attacked; we've now taken steps to insure such an accident doesn't happen again.

Personally, I think hackers play a necessary role in the advancement of technology; in fact, they've been a major influence on modern society long before computers were invented. Most of our greatest inventions were created by people who broke into existing technologies, examined how they worked, and looked for ways to improve or expand those technologies. In effect, the Kevin Poulsens and Vladimir Levins of today are providing the same type of service that people like Bell, Marconi and Thomas Edison did a century ago.

I also think hackers serve a useful purpose in that they make companies take action and be responsible for their laziness and lack of organization. Last year, CNN reported that more than 100 federal computer systems were compromised by hackers. They were so successful because many federal system operators failed to download and apply a software patch from Microsoft, even though it had been available on line - for free - for more than a year.

If a 15 year old breaks into the Wells Fargo banking system, for instance, who should we be more angry with: the teenager who expolits a problem and takes down the network for an hour, or the multibillion dollar corporation that failed to have the proper security systems installed in the first place, left vast amounts of personal data exposed, and could have caused financial ruin for thousands of customers? It's not an easy question to answer.

Computer crime exists, and these crimes rake in millions of dollars a year. In the grand scheme of things, though, I think the price is well worth it. The fact is that computer hacking, as much as people hate to admit it, is an integral part of the internet. By exposing flaws in other people's systems and forcing companies to be responsible, hackers do something most of us would like to do, but can't: they make the internet a safer, more secure place for everyone. I may not agree with their methods, but I respect what they do, and I'm thankful they're around.

Michael Devitt, BA
Huntington Beach, California
mdevitt@mpamedia.com

JUNE 2001