Reference: cyber history

A brief history of cybersecurity

https://cybersecurityguide.org/resources/cybersecurity-101/

The 1970s

Cyber attacks span back through history to the 1970s. In 1971, Digital Equipment Corporation's DEC PDP-10 mainframe computers working on the TENEX operating system started displaying the message, "I'm the creeper, catch me if you can!" Dubbed Creeper, this worm spread using the ARPANET, a forerunner to the Internet. It was created by Bob Thomas and was designed only to see if the concept was possible. Creeper laid the groundwork for viruses to come.

In response to the Creeper virus, Ray Tomlinson created Reaper. Reaper was the first antivirus software and was designed to move across the ARPANET and delete the self-replicating Creeper worm.

The 1980s

In September of 1983, the first cybersecurity patent was granted. Massachusetts Institute of Technology (MIT) was awarded this patent for a "cryptographic communications system and method." It introduced the Rivest-Shamir-Adleman (RSA) algorithm. RSA is one of the first public-key cryptosystems and is widely used for secure data transmission.

In 1986 the Computer Fraud and Abuse Act (CFAA) was enacted to address hacking. It has been amended several times over the years to cover a broad range of conduct. The CFAA prohibits intentionally accessing a computer without prior authorization but fails to define what that means.

Also in 1986, Lawrence Berkeley National Laboratory systems manager Clifford Stoll learned that someone was hacking into the lab's computer system. This discovery was made when Stoll tried to correct a 75-cent accounting error. Using a honeypot, Stoll determined that the lead hacker is Markus Hess, who had been selling information exfiltrated from hacked computers to the KGB. Hess and his accomplices were arrested by German authorities and convicted of selling stolen data to the Soviet Union. They only received suspended jail sentences.

In 1988 a Cornell University graduate student named Robert Morris released several dozen lines of code, which replicated wildly and spread to thousands of computers worldwide. The Morris Worm

crashed about 10 percent of the 60,000 computers then linked to the Internet. Morris became the first person convicted by a jury under the CFAA.

The 1990s

Cybersecurity systems, as we think of them today, really started to become popular in the early 1990s. Antivirus (AV) software was the first mass-produced cyber protection application on the cyber landscape. They appeared in the late 1980s, but the masses did not convert to the idea that they were necessary for several years.

These first antivirus systems, initially called AV scanners, were simple in functionality. They essentially scanned all the compiled code on a given system. They tested them against a database of known malicious signatures. The thinking was that as new viruses were discovered, these databases would be updated to watch for the new malware.

Researchers soon found out, however, that staying ahead of the bad guys was no easy task. The number of malware samples to check against grew from tens of thousands in the early 90s to millions of new samples each year, twenty years later. It is estimated that by 2014, as many as 500,000 unique malware samples were being produced every day.

These early software applications were resource-intensive and tended to bog down their host system. They also frustrated users with too many false-positive results.

Secure Sockets Layer (SSL) internet protocol is the security protocol that allows people to do simple things like purchase items online securely. Netscape released SSL 1.0 in 1994. After improvements, SSL became the core of the language for safely using the web, known as the Hypertext Transfer Protocol (HTTP).

In 1999, Kevin Mitnick pleaded guilty to four counts of wire fraud, two counts of computer fraud, and one count of illegally intercepting a wire communication. As the self-proclaimed world's most famous hacker, he was sentenced to 46 months in prison plus 22 months for violating the terms of his supervised release sentence for computer fraud.

In his 2002 book entitled *The Art of Deception*, Mitnick asserts that he compromised computers only by using user names and passwords that he gained by social engineering. He maintains he did not use software programs or hacking tools for cracking passwords or otherwise exploiting computer or phone security.

In 1998, Microsoft Windows 98 was released, and this ushered in a whole new level of accessibility for the novice computer user. This increase in computer usage paved the way for software security systems to become common. Many new releases, updates, and patches soon followed. Security vendors discovered the vast market for security products intended for home users.

The 2000s

In 2003, the first universally known hacker group, Anonymous, emerged on the scene. This group can be defined as a decentralized online community acting anonymously in a semi-coordinated manner, usually toward loosely self-agreed goals.

Over the years, dozens of people have been arrested for involvement in Anonymous cyberattacks around the world. Support of the group's actions and effectiveness varies widely. Advocates have called the group freedom fighters and digital Robin Hoods.

In contrast, critics have described them as a cyber lynch mob or cyber terrorists. In 2012, Time Magazine called Anonymous one of the 100 most influential people in the world.

In recent years, however, Anonymous's media exposure has declined, and they have largely vanished from the popular culture's lexicon.

The late 2000s brought a whole new level of cyberattacks. Bad actors had developed an appetite for stolen credit cards. The years 2005 to 2007 were plagued by an ever-increasing frequency of data breaches.

To stem the flow of stolen data, governments around the world began to implement regulatory solutions. In the US, regulations required that authorities be notified when a breach was discovered and that funds be set aside to compensate victims.

The 2010s

The increased regulation of the 2000s proved to be too little, too late. The sophistication of hackers spiked as the profits seemed limitless.

Even nation-sanctioned bad actors with access to enormous funding could be observed battling for cyber-turf and waring over such prizes as online betting or gaming sites.

This decade saw the appearance and rise of Endpoint Protection and Response systems (EPR). The systems replaced the legacy AV systems by including the same basic functionality but are radically improved and enhanced.

Instead of relying on a static signature to identify viruses, EPR scan for malware families. Malware samples follow a progression or mutation and so they can effectively be recognized as belonging to certain families even when no known malware signatures are detected.

Notable cybersecurity attacks

Each year brings with it a new spate of cyberattacks. Some reported by the victims in compliance with ever-stiffening government regulations and some uncovered by Security analysts. Largely because of their news value, the size of reported high-profile attacks is undoubtedly trending upward.

Some attacks catch the publics' attention because of the name recognition of the victim. In contrast, others swindle large segments of the general population. Below are a few of the more notable cyberattacks over the last decade-plus.

Learn more about cyber phishing attacks

Adobe

Adobe released information in October 2013 about the massive hacking of its IT infrastructure. Personal information of 2.9 million accounts was stolen.

Exfiltrated information included logins, passwords, names, and credit card numbers with expiration dates.

Another file discovered on the Internet later brought the number of accounts affected by the attack to 150 million. To access this information, the hackers took advantage of a security breach related to security practices around passwords.

Adult Friend Finder

In 2015, this dating site was attacked for the first time.

The information revealed included pseudonyms, dates of birth, postal codes, IP addresses, and sexual preferences of 4 million accounts.

This stolen data was made public on a forum only accessible on Tor. Malicious actors obtained these files; however, no banking data had been hijacked.

The following year, Adult Friend Finder faced a new attack, even more severe than the first one. This time more than 400 million files were exposed.

The stolen information was less sensitive, but in total, 20 years of personal information were taken.

Alteryx

This marketing analytics firm left an unsecured database online that publicly exposed sensitive information for about 123 million U.S. households.

The information included 248 fields of data for each home, ranging from addresses and income to ethnicity and personal interests.

Details included contact information, mortgage ownership, financial histories, and whether a household contained a pet enthusiast. Names were not included.

Equifax

Equifax, an American credit company, revealed, six weeks after the fact, that it had suffered a cyberattack over the course of several months.

Detected in July of 2017, it contained personal data such as names, birthdates, social security numbers, and driver's license numbers.

It also exposed 200,000 credit card numbers. Victims included 143 million American, Canadian, and British customers.

ILOVEYOU Virus

ILOVEYOU, sometimes referred to as Love Bug or Love Letter for you, is a computer worm that infected over ten million personal computers on and after May 2000.

It started circulating as an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.

Marriott

Personally identifiable information from up to 500 million guests at the Marriott-owned Starwood hotel group was compromised, beginning in 2014.

The rift was first detected in September 2018.

Data exfiltrated includes payment information, names, mailing addresses, phone numbers, email addresses, passport numbers, and even details about the Starwood Preferred Guest (SPG) account.

NotPeta Malware

Petya is a class of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows-based systems.

It infects the master boot record and executes a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin to regain access to the system.

Variants of Petya were first seen in March 2016, which propagated via infected email attachments. In June 2017, a new variant of Petya was used for a global cyberattack targeting Ukraine.

The new variant spreads via the EternalBlue exploit, which was used earlier in the year by the WannaCry ransomware.

Kaspersky Lab referred to this latest version as NotPetya to distinguish it from the 2016 variants, due to these differences in operation. Although it claims to be ransomware, this variant was modified so that it is unable to revert its own changes and release the hard drive.

Sony

Sony's PlayStation Network (PSN) was attacked in April 2011. This attack leaked the personal data of 77 million users. The banking information of tens of thousands of players was compromised.

After the intrusion discovery, PSN, as well as Sony Online Entertainment and Qriocity, were closed for one month. Unfortunately, in November 2014, a subsidiary, Sony Pictures Entertainment, was attacked by malware.

The "Guardians of Peace" stole 100 terabytes of data, including large quantities of confidential information such as film scripts, compromising emails, and personal data of 47,000 employees.

Target

Target, the second-largest U.S. discount retail chain, was the victim of a massive cyberattack in December 2013.

Data was hijacked between November 27 and December 15 of that year. The information taken included bank card records of 40 million customers and personal data of another 70 million customers.

TJ Maxx

In March of 2007, TJX Companies (parent of TJ Maxx) confirmed with the Securities and Exchange Commission that it had been attacked.

A network intrusion carried out on its systems resulted in the loss of 45.7 million consumer records, making it the most significant such breach on record at that time.

WannaCry Ransomware Attack

The WannaCry ransomware attack was a May 2017 worldwide cyber-event.

This attack employed the WannaCry ransomware cryptoworm which targeted devices running the Microsoft Windows operating system. It encrypted data and demanded ransom payments.

It propagated through EternalBlue; an exploit developed by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers a few months before the attack.

Yahoo

In 2014, Yahoo announced it had suffered a cyberattack that affected 500 million user accounts, constituting the most extensive hacking of individual data directed against a single company to that date.

Names, dates of birth, telephone numbers, and passwords were taken. It is now thought that as many as 3 billion user accounts may have been affected by this attack.

Migrated from Apple Server Wiki. Original page ID: m105P5

Revision #2
Created 2026-09-29 16:00:04 UTC by Admin
Updated 2026-09-29 16:23:14 UTC by Admin