The Evil-ution of Network Security Threats

An eBook of Hacking History

WatchGuard®

From basic DOS Trojans to debilitating ransomware

Get ready to take a trip through hacking history

Over the past 35+ years, what it means to be a hacker has changed dramatically. As a result, network security threats have evolved at a staggering pace. From small-time scams to insidious worms and massive data breaches, the industry has worked tirelessly to marshal responses each step of the way. As a result, we're all engaged in the ultimate cyber tug-of-war. But, to understand how to protect networks in the future, it's important to look at the past. What are some of those marquee hacks that forever changed the digital landscape? Take a seat and prepare yourself to experience the "Evil-ution of Network Security Threats."

1980

The era of cool

THE ERA OF TROJANS

THE ERA OF TROJANS

The awesome 80s brought us *Back to the Future*, the IBM PC, Rubik's Cube, Nintendo, and more. But, it also brought the first large-scale computer virus in history with a floppy disk infection called Elk Cloner, and closed out the decade with a not-so-awesome introduction to an early variant of ransomware – via the AIDS trojan.

The 80s threat actor

Hackers in the 80s were likely teens experimenting and exploring, with very little criminal intent. While systems were targeted, it was mainly for bragging rights (not to steal actual information). Many of these "script kiddies" relied heavily on phreaking* to gain access to the Internet and eliminate costly telecom charges. Most daydreamed about joining the elite hacker group, the Legion of Doom.

** Phreaking is a slang term coined to describe the activity of a culture of people who study, experiment with, or explore telecommunication systems, such as equipment and systems connected to public telephone networks.*

The floppy disk virus

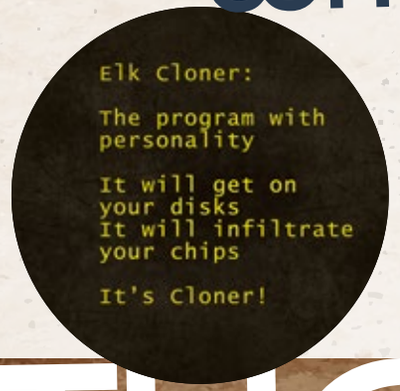
What is a floppy disk virus?

A virus is a type of malware that either replicates itself as new files in different places, or infects existing programs and files by modifying them (locally, not over a network).

In the 80s, few people connected computers to networks. Instead, floppy disks were used to carry files from computer to computer. Often, viruses could either directly infect files on a floppy disk, or users would unintentionally share a virus-infected file from their computer when moving files to a floppy disk. Thus, the floppy disk became an extremely effective delivery agent for malicious code in the 80s.

Viruses continued to evolve, leading to boot-sector floppy viruses like Brain and SCA, which hid malicious code specifically in the boot sector of a floppy disk.

Why Elk Cloner mattered



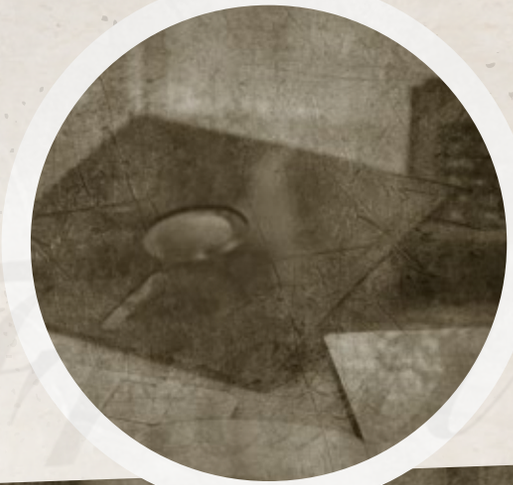
This Apple II virus was written as a joke by a 15-year-old and was attached to a game that was on a floppy disk. The fiftieth time the game was played, Elk Cloner would replace the screen with a poem. A computer infected with this virus could infect other floppy disks. This joke provided a model for other hackers to evolve floppy viruses, leading to viruses such as Brain, SCA, Stoned, and BHP.

THE AIDS TROJAN

As the 80s came to a close, this was an early view into what would later become known as modern-day ransomware. The author sent it to more than 20,000 doctors via a 5.25 floppy disk. Once inserted, an autoexec.bat script ran, renaming files and directories. Victims were instructed to send $189 USD to a PO box located in Panama. The note made it appear like the PC corporation was asking for a servicing invoice. Fortunately, the files were not truly encrypted and tools quickly emerged that could easily reverse the effects of the infection.

Industry Response

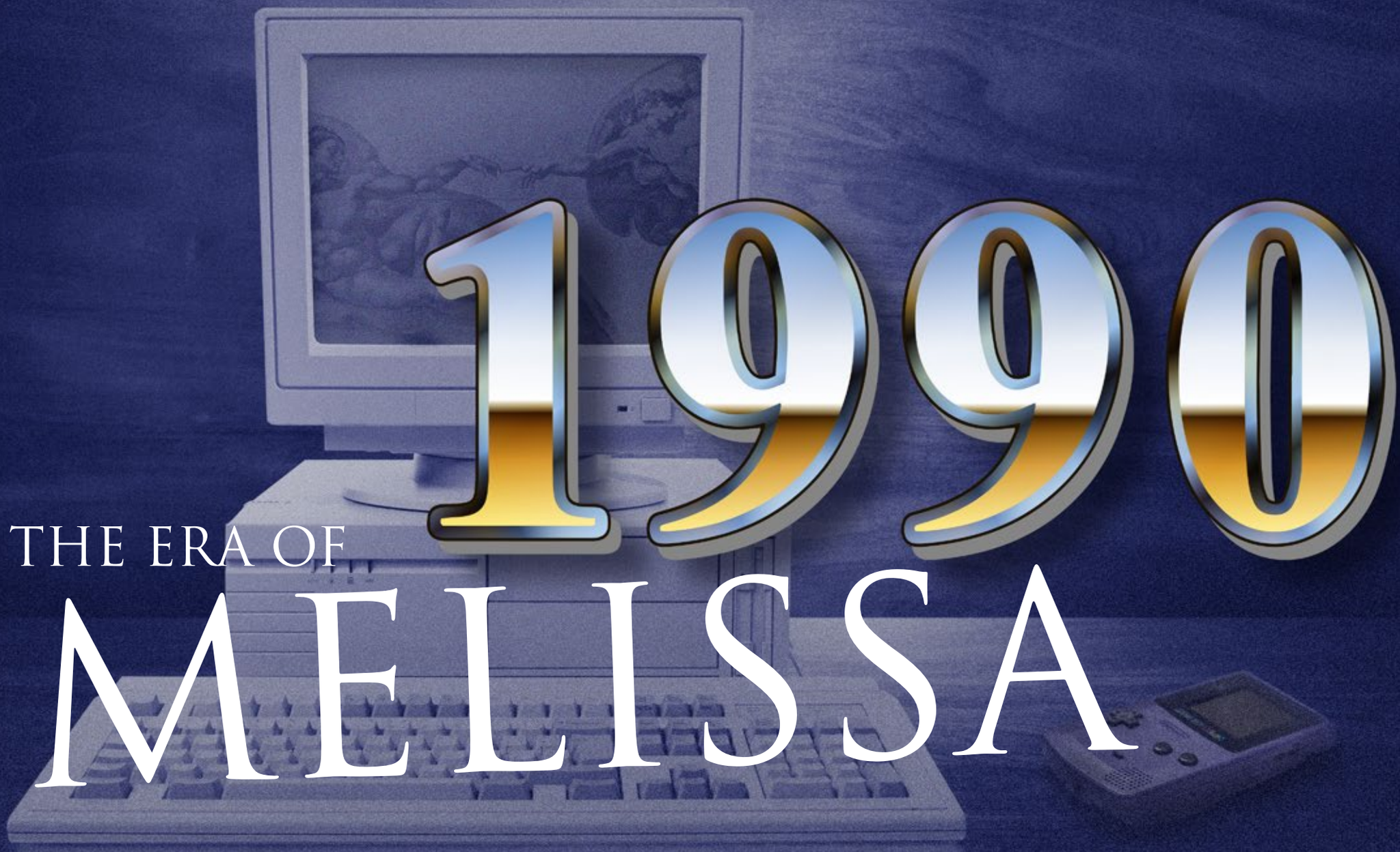
Elk Cloner did not spread widely and no real response was needed by the industry, although around this time, the U.S. Government did pass the **Computer Fraud and Abuse Act**, which aimed to protect financial and government computer systems.



OTHER NOTABLE 80s THREATS:

- The Brain Boot Sector Virus
- Vienna Virus
- Jerusalem Virus
- SCA Virus
- Ghostball

Regarding the AIDS trojan, the British anti-virus industry identified this threat and notified Scotland Yard, which arrested the author, Dr. Popp, and charged him with 11 counts of blackmail. Ultimately, he was ahead of his time on cyber extortion.



1990

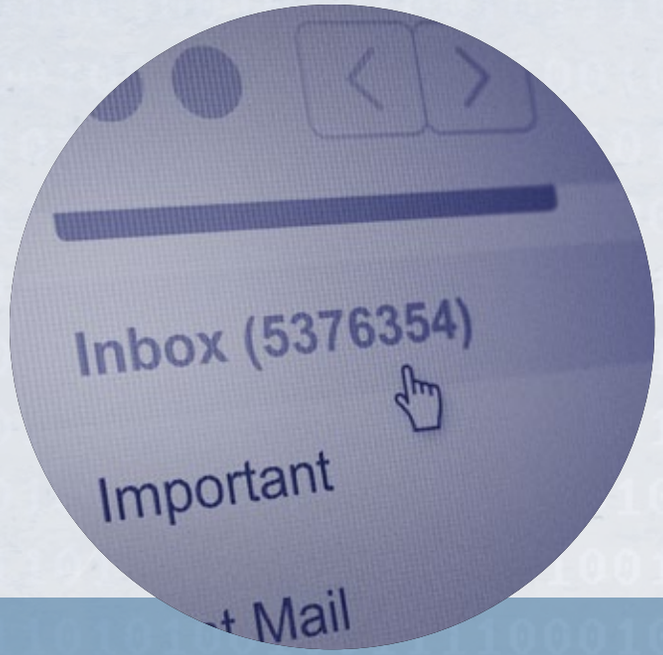
THE ERA OF MELISSA

1990 THE ERA OF MELISSA

The hits kept on rolling into the 90s. We see the first polymorphic viruses in the Chameleon family, the first macro virus called Concept is released, and the Michelangelo virus is slated to cause a digital apocalypse. But, there's no party like a 1999 party, right? Wrong. Ask Melissa, or should we say Mailissa, or Kwyjibo, or Kwejeebo? This virus shut the party down by infecting 20 percent of the world's computers.

The 90s threat actor

Hackers in the 90s began to move past experimenting with simple digital vandalism, but the majority remained non-criminal and defaced websites for sport. Some began to hijack people's servers to use as piracy servers and for file sharing, while others created chaos on AOL. Some hardcore criminal hackers began indulging in credit card theft, wire and bank fraud, and hacking government systems.



WHAT IS A MASS-MAILING MACRO VIRUS?

A macro virus uses scripting language in Office documents to infect victims. A mass-mailing macro virus, once open, spreads automatically as an email attachment. The Melissa virus was a prominent example of this virus.

WHY MELISSA MATTERED

The Melissa virus (named after the Windows registry key it created) was a macro virus that spread like wildfire as a malicious Word document attached to an email. When the victim opened the infected document, embedded macros would execute to infect the system and then automatically send the same document to the first 50 contacts in the victim's address book. It was so effective, Microsoft actually shut off incoming email temporarily. Melissa wasn't the first macro virus, but it was the first macro virus to auto-proliferate via email and it generated a high volume of network traffic. It was one of the larger viruses of its time and was a precursor to the ILOVEYOU worm of 2000.

INDUSTRY RESPONSE

With help from Monmouth Internet and some Swedish computer scientists, the FBI was able to apprehend the creator, David Smith, one week after the release of the virus, and CERT issued a fix. He was tried and sentenced to 10 years and a $5,000 fine, but only served 20 months. During that time, he worked for the government, helping them catch other hackers.

OTHER NOTABLE 90s THREATS:

- OneHalf
- Staog
- CIH Virus
- Happy99
- ExploreZip

In 1996, some computer scientists wrote a paper predicting that attackers would one day use the strong encryption available on desktop PCs to create a virus that encrypts files and holds them ransom. This was a prelude to the ransomware to come later.

WatchGuard

The Evil-ution of Network Security Threats

2000 Welcome to Y2K

The 2000s saw a dramatic increase in cyber threats. After surviving the non-disaster of Y2K, it seemed only appropriate to kick off the new millennium full of love. You may recall being one of the millions to get the ILOVEYOU email. Hopefully you didn't click that attachment while you were distracted listening to Blink 182 on your new iPod. Within 10 days, more than 50 million computers were infected and it cost the world between $5-8 billion.

The 2000s Threat Actor

Hackers in the early 2000s were on a mission to become notorious. They not only ratcheted up web defacement, but also released a large number of worms. As the decade progressed, hackers worked to monetize attacks through botnets, click-jacking and more, and in doing so, became true cyber criminals. During this period, organized crime noticed the business potential of hacking, state sponsored actors began creating powerful attacks, and Anonymous emerged.

What is a computer worm?

A computer worm is a type of malware that replicates itself by spreading automatically over a network. It is usually a stand-alone program. On the other hand, a virus is usually attached to an existing program that spreads to other file systems on a single computer.

Why ILOVEYOU mattered

ILOVEYOU was considered so dangerous, the Pentagon, CIA and British Parliament all shut down their mail systems. It is estimated to have cost the U.S. $15 billion to remove ILOVEYOU from their networks.

The ILOVEYOU worm claimed tens of millions of infections at its peak in early 2000, making it one of the most prolific malware examples in history. The worm spread as an email message with the subject “ILOVEYOU” and a malicious Visual Basic script attachment titled “LOVE-LETTER-FOR-YOU.txt.vbs.” The worm relied on the curiosity of its victims and was one of the most destructive pieces of malware during this time, overwriting many image, mp3 and document files. It was also one of the first examples of effective social engineering in malware.

industry response

Microsoft vowed to increase security with its Trustworthy Computing in response to the ILOVEYOU worm. The Philippines National Bureau of Investigation arrested two young Filipino men for the crime, but had to release them and drop all charges because there were no laws against writing malware at the time. Vendors began providing URL filtering, antivirus, VPN and early firewall technologies to help combat these types of threats.

Welcome to the Wi-Fi age

As the Sopranos ended with a 10-second fade to black in 2007, hackers turned their gaze toward TJX — better known as Marshalls, T.J. Maxx and HomeGoods. The prize? An estimated 45.6 million stolen credit and debit card numbers taken over an 18-month period. Welcome to the Wi-Fi age...and the need for wireless security. This oversight ultimately cost the company $256 million and was the first of a long run of data breaches that continues to this day.

What is a wireless hack?

Wireless hacks can occur in many different forms. A rogue access point, for example, can allow unauthorized connections to a secure network. An Evil Twin can force secure clients to unknowingly connect to and transmit sensitive data over a malicious network. An attacker can also simply sniff wireless packets right out of the air and view their contents if weak encryption is used, which was the case in the TJX Wi-Fi hack.

Why TJX mattered

Over the course of 18 months, an attacker captured wireless traffic containing financial transaction data from two Marshalls stores (owned by TJX) in Miami. The wireless traffic was encrypted using WEP, a wireless encryption standard that was considered obsolete by 2003. The attacker was able to easily crack the encryption and made off with a reported 45.6 million credit and debit card numbers, making it the largest financial data breach at the time.

industry response

Eleven people were ultimately charged with this breach. One ringleader got five years in prison and a $300,000 fine. Another got thirty years in a Turkish jail.

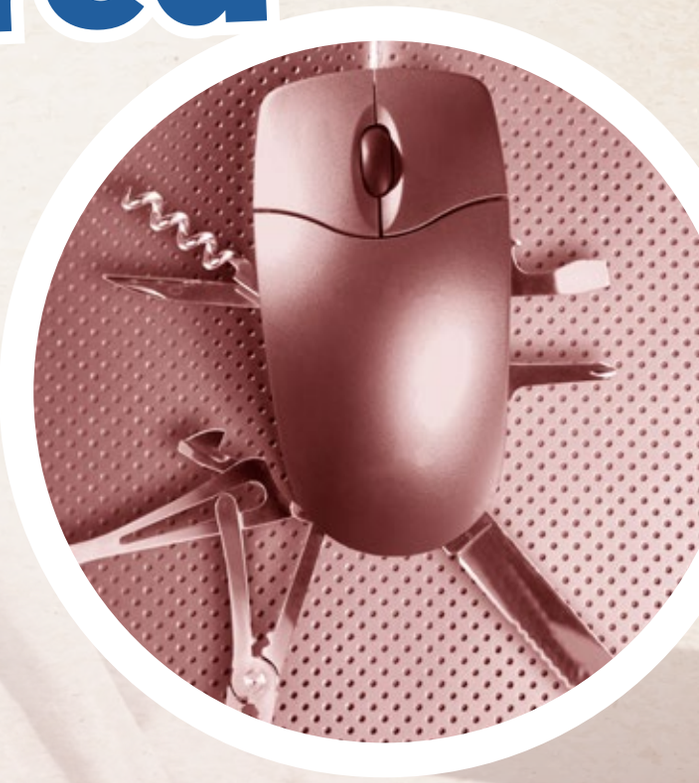
MAKE WAY for Zeus

While most of us were swarming bookstores to buy the final installment of the Harry Potter series, hackers were still trying to cash in by playing Zeus in 2007. No, not the god of sky and thunder, the malware botnet designed to steal millions of dollars from victims' bank accounts. And steal it they did, cashing in heavily to the tune of more than $12.5 million. Even scarier, this continued until 2010 when the FBI finally initiated a crackdown. Total estimated losses on the Zeus variant: $70 million.

What are botnets?

A botnet is a collection of infected clients (often called zombies) that can be controlled to carry out a coordinated attack or other actions. Botnets are responsible for many spam email campaigns, bank fraud, and distributed denial-of-service attacks. Botnets usually receive orders from a central command and control (C&C) server.

Why Zeus Mattered



The Zeus botnet was the Swiss Army Knife of malware during its reign, allowing its controllers to primarily steal banking information using browser attacks and keylogging. This botnet was also very modular and had a relatively well-programmed and organized framework. Because of that, when the source code leaked, it allowed other threat actors to easily create variants. Zeus was later used to install other malware such as CryptoLocker (and its source code was reincarnated in the form of Citadel, Game over Zeus, and eventually rolled into the SpyEye malware).

industry response

In 2010 the FBI finally took action, arresting more than 100 people in conjunction with Zeus botnets. In 2013 they arrested the alleged mastermind in Thailand, Hamza Bendelladj, or codename BX1 online.

Into the Heartland

In 2008, POS (Point of Sale) was still a nerdy acronym known mainly by those managing sales processing at retailers. But, that all changed when hackers realized they could bypass the retailer and go straight to the payment processing source. Enter the next victim, Heartland Payment Systems, which lost the magnetic strip data of more than 100 million credit cards when its POS system was targeted. When all was said and done, the company had to pay out more than $140 million in penalties and fines.

What is a POS attack?

Previous retail attacks like the TJX attack in the mid-2000s involved intercepting traffic on payment processing networks. POS attacks differ by going directly after specialized payment processing system. These attacks use sniffers to capture network communication, keyloggers to record input on the system, or more sophisticated RAM scrapers to pull payment card information directly out of the POS system's memory.

Why Heartland mattered

The Heartland data breach involved malware that was on a POS network, sniffing transaction data over an 8-month period. In the end, the number of credit card numbers lost from the data breach surpassed the earlier TJX hack by a wide margin, with an estimated 100 million card numbers acquired by the attackers. The Heartland breach demonstrated the potential massive impact of attackers targeting a payment processor directly. Rather than stealing small amounts of credit card info from individual retail companies, they could gather massive amounts of data from the company that all those retailers relied on. It also showed criminals were specifically targeting the payment processing systems themselves, which in the end, helped the industry improve these systems and led to more rigorous PCI DSS standards.

industry response

In August 2009, Albert Gonzalez was indicted in Newark, New Jersey on charges of hacking into the Heartland Payment Systems, Citibank-branded 7-Eleven ATMs and Hannaford Brothers computer systems. To help combat these types of attacks, vendors begin delivering SSL VPNs and end-to-end encryption systems.

A, B, C, D, E...

No, we're not practicing the alphabet. We are reciting the variants of the Conficker worm, otherwise known as Downup, Downadup and Kido. As 2008 came to a close, 190 countries were hit by this little devil. It was the largest known computer worm infection since Welchia in 2003, and it can still be found on computers today, making it one of the most difficult to eradicate. It uses flaws in Windows OS software and dictionary passwords to form a botnet, and employs multiple advanced malware techniques. It infected millions of computers in homes, businesses and governments around the world.

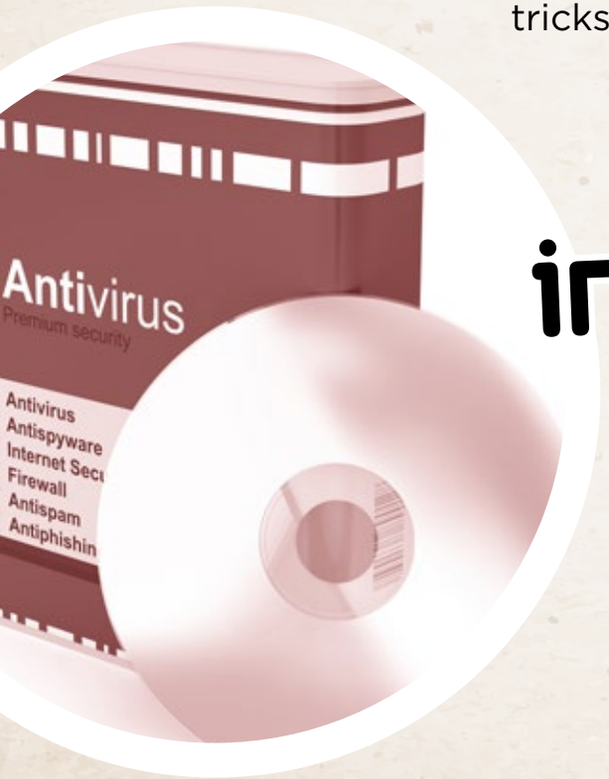
What is advanced malware?

In general, advanced malware is malware that uses relatively new techniques or mechanism to evade security controls and infect "protected" computers. Due to the endless arms race between malware authors and security companies, it is hard to precisely define specific attributes of advanced malware, simply because a new technique that was evasive and unique last year, could become ubiquitous and detectable the next year. Malware from the 2000s, for example, would disable your anti-malware services and AutoUpdate mechanisms. But today's advanced malware more commonly uses code obfuscation or "packing and crypting" to hide from signature-based antivirus solutions. More modern advanced malware also takes advantage of various "staged" loading processes, and some malware is designed to detect and evade sandboxes and virtual systems. The most advanced malware might even leverage zero day vulnerabilities.

Why Conficker mattered

Conficker was one of the most prolific computer worm infections ever created. It is still considered a top malware threat to this day. As variants have evolved over the years, they have become more effective at evading anti-malware services using tricks like selective DNS lookup blocking, process killing, and in-memory patching.

Microsoft offered a $250,000 reward for information leading to the arrest and conviction of the creator of Conficker. But the precise origin of Conficker remains unknown, although working group members stated at the 2009 Black Hat Briefings that Ukraine was the probable origin.



industry response

Microsoft announced the formation of an industry group to collaboratively counter Conficker. Apple also announced the first Apple Virus Protection product. And, the industry began offering Unified Threat Management (UTM) solutions with multi-layered network security in one appliance.

OTHER NOTABLE 2000s THREATS:

- Code Red
- SQL Slammer
- Blaster
- MyDoom

2010

When Facebook ruled, and so did cyber espionage.

2010 THE ERA OF CYBER ESPIONAGE

We started the 2010s with a bang. Even though Mark Zuckerberg was Time Magazine's Person of the Year in 2010, it's not likely Iran remained FaceBook friends with the U.S. and Israel after the malicious worm Stuxnet. Designed to sabotage Iran's nuclear program, Stuxnet targeted programmable logic controllers (PLCs) and used 4 zero day flaws across Microsoft Windows and Siemens Step7 software. Compromising the Iranian PLCs, this worm caused the centrifuges to tear themselves apart.

The 2010s Threat Actor

While mainstream hackers continued to steal data and monetize attacks, nation-states began developing red teams with the goal of stealing secrets from rival nations and conducting cyber espionage. These groups use malware customized for non-traditional computing systems and often design attacks around a very specific goal. As the public recently learned regarding the NSA leaks, governments often stockpile zero day attacks.

What is industrial system malware?

Stuxnet is an industrial system malware that is embedded in industrial system computers and controllers that quietly spreads through connected systems until it locates the specific payload target and executes.

INDUSTRY RESPONSE

Initially called Rootkit.Tmphider and discovered by the security company VirusBlokAda, the name was later changed to W32.Stuxnet by Symantec. Siemens released a removal tool for Stuxnet and recommended customers install Microsoft security updates and prohibit third-party USB flash drives. Prevention of control system security incidents is a topic that is still being addressed in both the public and the private sector. In fact, the U.S. Department of Homeland Security National Cyber Security Division (NCSD) operates a specialized computer emergency response team called the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Why Stuxnet mattered

While not the first known case of cyber warfare, it was the first discovered malware that spies on and subverts industrial systems. It was also the first malware to include four zero days, the first PLC rootkit, and the first malware to jump from Windows gear to IoT devices. It is reported that Stuxnet succeeded in temporarily infecting and disrupting nearly one fifth of Iran's nuclear centrifuges.

A bad target

Lance Armstrong wasn't the only one to let down the American people in 2013. Discount retail giant Target was hacked and 11 gigabytes of customer data that included names, emails and payment card information was stolen. The breach affected nearly 70 million customers and to date has cost the company $300 million.

How can third-party vendors impact a business?

Attackers in the Target data breach broke in using credentials provided to an external HVAC contractor (Fazio Mechanical, a refrigeration company). Because of insufficient network segregation, attackers obtained direct access to Target's POS network via partner credentials, and were able to install card-sniffing malware directly onto the POS systems.

WHY TARGET MATTERED

This was one of the first attacks that held C-level executives accountable for poor security and policies, and ultimately cost them their jobs. It also highlighted the vulnerability third-party partners can pose to an organization.

How it was done...

A phishing email duped at least one Fazio employee, allowing Citadel, a variant of the Zeus banking trojan, to be installed on Fazio computers. With Citadel in place, the attackers waited until the malware offered up Fazio Mechanical's login credentials. They then used that information to gain access to Target servers. They used malware, code-named trojan.POSRAM, to infect Target's POS system. This technique allowed attackers to steal data from POS terminals that lacked Internet access. The attackers then moved the stolen data to off-site FTP servers and sold it on the digital black market.

INDUSTRY RESPONSE

Target ultimately settled for $39 million with affected banks and $10 million with affected customers, but the total cost of the breach is now estimated over $300 million, making it one of the most expensive data breaches to date. As a result, C-level executives today regularly discuss information security as a key topic, and security professionals have started investing in detection and response technologies to help quickly identify breaches.

What? My computer can hold me hostage!?

CryptoLocker was introduced in 2013, representing the first crypto-ransomware. Propagated via infected email attachments, this malware encrypts files on your system and then offers to decrypt them for a price. While the malware was cracked in 2014, it managed to extort around $3 million dollars from victims. Now that's the real Wolf of Wall Street.

What is crypto-ransomware?

This type of ransomware encrypts files stored on a user's computer or mobile device. The files are scrambled and unreadable until a decryption key is used to restore it. When the files are encrypted, they are essentially taken hostage and a ransom demand is displayed.

Why CryptoLocker mattered

CryptoLocker was one of the earliest and most effective ransomware variants, with its bitcoin addresses (crypto currency bank accounts) handling as much as $27 million worth of bitcoin in 2013. Unfortunately, the success of CryptoLocker spawned a number of unrelated and similarly named ransomware trojans working in essentially the same way.

INDUSTRY RESPONSE

In June 2014, the United States Department of Justice officially announced Operation Tovar – a consortium of law enforcement agencies (including the FBI and Interpol), security software vendors, and several universities – had disrupted the Gameover Zues botnet, which had been used to distribute CryptoLocker and other malware.

NO ONE IS SAFE

When James Franco and Seth Rogen start causing nation-state hacking, no one is safe. Sony Pictures Entertainment found this out the hard way in 2014 when the Guardians of Peace, allegedly sponsored by North Korea, breached their network and stole personal employee information. The group later released embarrassing emails from executives and successfully pushed to have *The Interview* pulled from movie theaters.

What is a Server Message Block worm tool?

SMB worms propagate through network storage shares using the Microsoft file sharing protocol. These worms are usually more sophisticated in nature than typical worms, using vulnerabilities in SMB or by brute-forcing authentication.

Why the Sony Pictures Entertainment hack mattered

This was the first alleged state-sponsored attack that directly targeted a private organization. The breach was then used to influence the release of an upcoming movie that was a political satire of North Korea.

The Guardians of Peace claimed to have had access for at least a year prior to being discovered and reportedly took more than 100 terabytes of data from Sony. The attack also temporarily shut down Sony's computers, costing them major production time.

INDUSTRY RESPONSE

In January 2015, U.S. President Barack Obama issued an executive order enacting additional sanctions against the North Korean government and a North Korean arms dealer, specifically citing the cyber attack and ongoing North Korean policies.

SINNERS AND SAINTS...

While “twerk” and “selfie” were being added to the dictionary, perhaps Merriam-Webster should have been defining the “Snowden Effect.” Sinner or saint, no one can deny that 2013 became the year of Snowden. Wanted for espionage by the U.S. since he walked out of an NSA facility with thousands of classified documents, this traitor/whistleblower brought to light the mass surveillance systems employed by the NSA.

What is an insider data breach?

Snowden is a prime example of an insider data breach. Depending on perspective, he can be classified as either an internal attacker, or a whistleblower, that simply walked out with sensitive company data. This type of breach is often the most difficult to defend against since it does not rely on exploitations of technical vulnerabilities.

Why Snowden Mattered

The Snowden data leak was a huge pie in the face to the NSA. A government organization with security literally in its name lost troves of sensitive information. The data leak revealed numerous surveillance programs and sparked a national debate on the difference between whistleblower and traitor. It also made the world realize the privacy and security implications of all the data shared online.

Snowden was named *Time's* Person of the Year runner-up in 2013, behind Pope Francis, and was voted as The Guardian's person of the year in 2013.

INDUSTRY RESPONSE

United States federal prosecutors filed a criminal complaint against Snowden, charging him with theft of government property, and two counts of violating the Espionage Act through unauthorized communication of national defense information and "willful communication of classified communications intelligence information to an unauthorized person." After fleeing the U.S., Snowden sought asylum in Russia, where he is still believed to be today.

While Mr. Robot fans clambered to learn everything they could about the fictitious fsociety, the largest breach of government data in the history of the United States was happening at The Office of Personnel Management (OPM). Close to 22 million records were stolen, including personally identifiable information such as social security numbers and addresses, and even background-check information and fingerprints. Why did the Chinese take this information? Perhaps because it was there.

What is an external data breach?

The OPM hack was an external data breach, carried out by an attacker outside the organization. In an external data breach, attackers must first infiltrate the network, and then they can collect sensitive information and exfiltrate the data.

Why OPM mattered

It was one of the first significant nation-to-nation hacks of information. The attackers are suspected of making off with security clearance information and fingerprints of government employees, including possibly secret agents. They used two distinct hacks, one that quickly breached OPM, the other that targeted OPM contractors and used stolen credentials to access the OPM network (much like the Target breach).

INDUSTRY RESPONSE

The breach was discovered by OPM personnel. The hack highlighted weaknesses in the U.S. Government's "EINSTEIN" IPS system, particularly around detecting HTTPS attacks, and has caused them to rethink their security practices.

Not Quite the end

We finish off our journey of hacking terror not by exploring the scary Yahoo data breach that resulted in a whopping 1 billion stolen user accounts. Instead, we look at how a nation-state took a bearish approach to hacking the Democratic National Committee (DNC). With the end goal of influencing the 2016 U.S. presidential election, Russian hacking groups Cozy Bear and Fancy Bear allegedly stole sensitive emails from the DNC, which were ultimately released by WikiLeaks.

What is a spear phishing attack?

A spear phishing attack is an email or electronic communications scam that targets individuals, organizations or businesses, with the intent of stealing data for malicious purposes. The DNC breach is believed to have started with a spear-phishing attack that retrieved insider credentials allowing attackers to log into servers and install malware.

Why the DNC hack mattered

This attack was the first time a nation-state allegedly carried out a hack to gather information to influence another government's election process. The alleged nation-state timed the disclosure of the stolen information to have the biggest impact on manipulating public opinion, making it a great example of cyber information warfare and propaganda.

INDUSTRY RESPONSE

The hacking programs were removed by cyber security firm CrowdStrike, and the U.S. Intelligence Community continues to investigate the attack. However, government, security and technology professionals are now more concerned than ever about how the Internet and cyber can be used for information warfare. With social media and "fake news" having a major impact on how information is spread and digested, the industry must work to combat criminals looking to control a narrative.

What's Next?

As you can see from the major threats over the past several decades, cyber criminals continue to evolve. In fact, over the coming months and years, we expect hackers to increasingly leverage new attack methodologies like ransomworms and IoT botnets, and adopt newly available technologies like artificial intelligence (AI) for their own corrupt purposes. That's why strong, unified defenses are imperative.

Protect your network

with WatchGuard's Total Security Suite

Total Security. Total Simplicity.
Total Visibility. Maximum Performance.

A unified approach to network security that delivers complete network protection in a single, easy-to-deploy solution.

LEARN HOW OUR SUITE CAN PROTECT YOU.