SOPHOS

CYBERTHREATS: A 20-YEAR RETROSPECTIVE

By John Shier, senior security advisor, Sophos

December 2020

Introduction

The cyberthreats that shaped information security

In security we spend a lot of time trying to decipher the future. Where's the next technology breakthrough? What are cybercriminals going to do next?

Annual threat reports provide an opportunity to look back at significant events of the past 12 months and identify trends for future development, action and protection. Looking back in time a little further helps to provide context for how we arrived at our current situation and why some things are the way they are. A long view of history can point to subtle changes or seismic shifts within an industry.

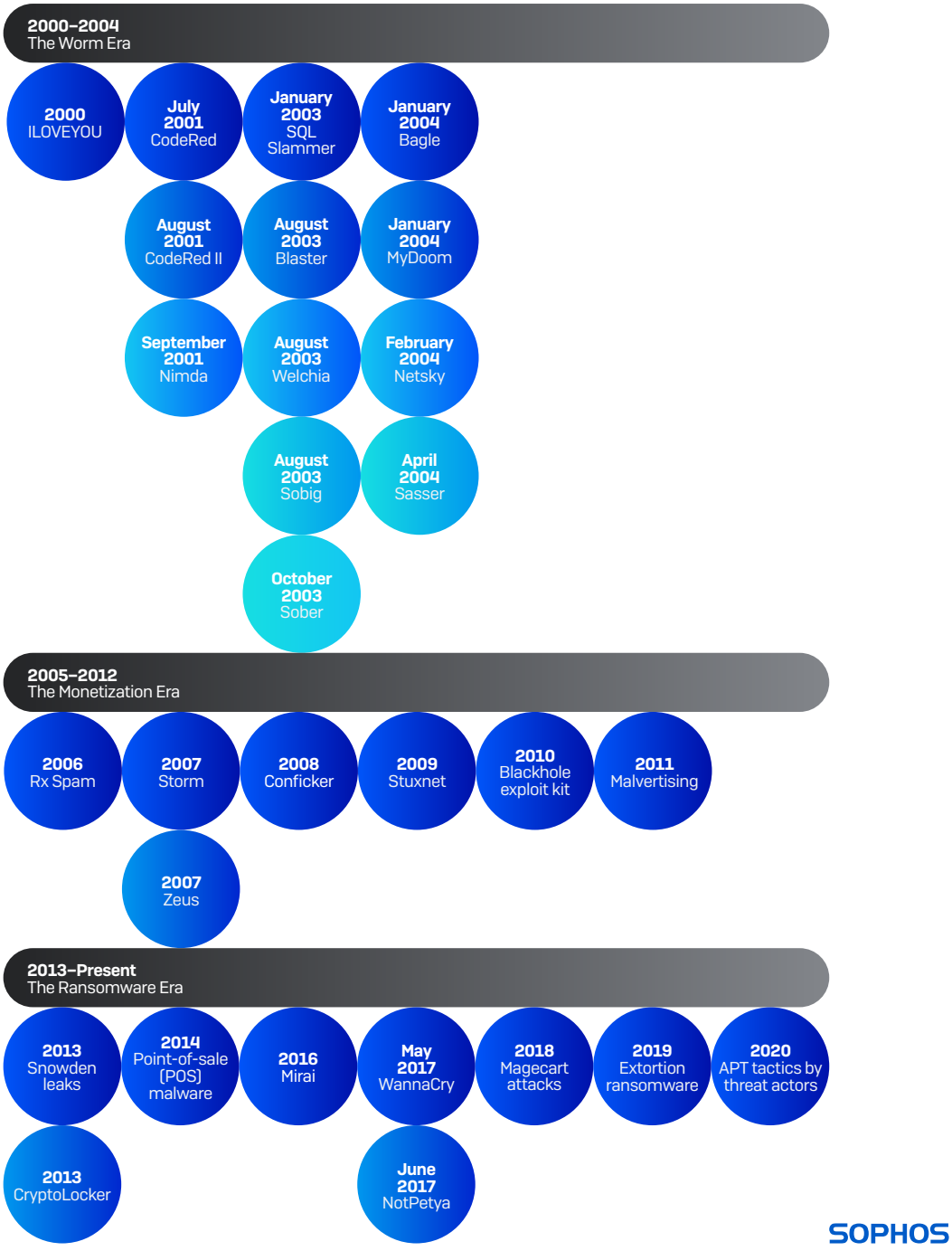
Information security became a bona fide industry and professional discipline at the beginning of the current millennium. What follows in this paper is a timeline of key threats and events from the past 20 years that helped to shape our industry.

Not all the events represent firsts, some represent significant moments, but each of them correlates with a change in security behavior or protection.

Some of these changes have persisted while others continue to be re-evaluated and updated. The evolution of our industry can be teased out of these moments and their impact will forever be encoded in the fabric of our discipline.

The cyberthreat timeline

The timeline is loosely categorized into three eras. Each era is defined by a threat or event that proliferated throughout that time: The Worm Era, The Monetization Era and The Ransomware Era.



SOPHOS

2000-2004 - The Worm Era

This era saw the emergence of some of the most prolific worms the information security world has ever seen. Cumulatively, these worms infected tens of millions of systems worldwide and cost over $100 billion in damages and remediation costs.

They affected our business processes, changed the way we protected our networks and led Microsoft to launch Patch Tuesday. This can also be seen as the time when malware became a mainstream media sensation. While there were worms that pre-dated this period, and ones that came after, this was certainly their most impactful era.

It started with love

ILOVEYOU launched the worm era in 2000, using social engineering tricks that persist today. ILOVEYOU was notable for its rapid spread, broad reach and impact. It is estimated that the ILOVEYOU worm infected at least 10% of internet-connected hosts in a matter of hours and caused up to $15 billion in damages and remediation costs.

In addition to affecting consumers and some of the world's largest companies, it caused the shutdown of government email systems, including The Pentagon, CIA, and the British Parliament.

What made ILOVEYOU successful was a combination of social engineering and insecure defaults in software.

ILOVEYOU preyed on simple human curiosity to set off a chain reaction that spread like wildfire around the globe. The worm not only inspired the song "Email" by the British pop duo the Pet Shop Boys, but also a movie starring Dean Cain titled "Subject: I Love you."

In response to ILOVEYOU and similar worms, Microsoft released an update to Outlook in June 2000 with four key changes:

- First, the patch prevented users from accessing unsafe attachments (i.e. executables)
- Second, it warned users if a program tried to access their address book
- Third, users were also warned if a program tried to send mail on their behalf
- And fourth, Outlook was moved from the "Internet zone" to the "Restricted zone", which disabled most automatic scripting

A wave of worms

Starting in 2001 with the release of the CodeRed worm (July 2001), famously named after the flavor of Mountain Dew its discoverers were drinking at the time, the IT world was rocked by a series of worms: Code Red II (August 2001), Nimda (September 2001), SQL Slammer (January 2003), Blaster (August 2003), Welchia (August 2003), Sobig.F (August 2003), Sober (October 2003), Bagle (January 2004), MyDoom (January 2004), Netsky (February 2004) and Sasser (April 2004).

Unlike ILOVEYOU and pre-2000 worms, which targeted Microsoft Outlook, these worms targeted operating system vulnerabilities, server applications and network infrastructure.

Many of these worms abused buffer overflow vulnerabilities in various versions of Windows, or in applications such as Internet Information Services (IIS) or SQL Server. The intent was not always clear, but in some cases the impact was severe.

CodeRed to Nimda

CodeRed used a buffer overflow vulnerability in IIS to spread itself and deface websites with "HELLO! Welcome to http://www.worm.com! Hacked By Chinese!". The worm was so pervasive that even Microsoft was impacted after failing to patch Hotmail servers.

It was followed two weeks later by CodeRed II. This worm used a slightly modified buffer overflow. In contrast to its namesake, CodeRed II focused largely on infecting internal network targets and installing a back door on infected machines.

Nimda, or "admin" spelled backwards, quickly surpassed the economic damage caused by previous worms.

Nimda was highly successful due to its use of five different infection vectors. Like many previous worms, it spread via email, but it could also spread by abusing open network shares, compromising web servers, and even leverage back doors left behind by previous worms.

Slammer

After a relatively quiet 15 months, Slammer set off another wave of worms in early 2003. It relied on another buffer overflow vulnerability and infected most of its victims within ten minutes of release.

What made it so successful was its size, weighing in at only 376 bytes. Slammer used a single UDP packet to deliver the worm. The targets were Microsoft database applications: SQL and MSDE.

Routers started crashing under increased traffic load, which forced other routers to constantly update their dynamic routing tables, causing further congestion and more routers to crash.

Doubling its infections every 8.5 seconds, Slammer took down large swaths of the internet in only 15 minutes, including ATM networks, a 911 call center, and a nuclear power plant. I remember sitting in a datacenter at the time furiously adding block rules for udp/1434 on as many firewalls as possible in an attempt to contain the worm as it tried to ravage our network.

Blaster to Bagle

There was another lull until Blaster kicked off the final nine-month stretch of worms in August 2003. Blaster was created by reverse engineering a Microsoft patch a couple of months before the first Patch Tuesday. The practice of reverse engineering patches was becoming so common that the day following Patch Tuesday became known as Exploit Wednesday.

Blaster exploited a buffer overflow vulnerability in the RPC service of Windows XP and 2000 systems and launched a DDoS attack against "windowsupdate.com" if the day of the month was greater than 15 or the month was September or later.

August 2003 also saw the release of two more worms. First there was Welchia, also known as the "Nachi worm," propagated using a similar RPC vulnerability as Blaster, but instead of causing damage it attempted to clean up Blaster infections.

Despite its attempt at being a "helpful worm," Welchia caused the shutdown of the US State Department's computer network for nine hours. The helpfulness of this worm was overshadowed by its aggressive scanning. Defenders had to prevent infected users from connecting to the network because their systems would start looking for Blaster infections to repair.

The second August worm was Sobig.F, which was both a worm and a trojan, and the fastest spreading worm to date.

Sobig and its many variants infected computers through email attachments and subsequently used a built-in SMTP engine. It was also capable of deactivating many antivirus programs of the day.

Sobig heralded two new phenomena: malware families and botnets-for-hire. After Sobig, it became more common to see multiple variants of the same malware. These new botnets gave spammers a convenient infrastructure to easily and anonymously send millions of unsolicited emails every day.

There were Sobig variants in the wild prior to August 2003 but the one that had the highest impact was the record-setting Sobig.F. This variant led Microsoft to offer a $250,000 bounty for information leading to the arrest of its creator. On September 10, 2003, Sobig.F deactivated itself.

Sobig was followed in October 2003 by the Sober family of worms. These were mass mailing worms that harvested address books and brought along their own SMTP engine to spread. In addition, Sober used fake web pages, pop-up ads and fake advertisements as a distribution mechanism.

Like its predecessor, Sober was clearly designed to be used as a spamming botnet.

During the monetization era that followed 2004, and after a stint promising free World Cup tickets, in May 2005 the Q variant of Sober began spreading links to German far-right websites to all PCs infected with the earlier P variant. According to SophosLabs, Sober accounted for 80% of all malicious spam circulating the internet at the time.

Then, in November 2005, Sober again shifted tactics and began posing as the FBI, CIA, or German BKA. The emails suggested that the recipient had visited illegal websites and needed to fill out a form explaining their actions. Later versions of the worm also started using celebrities as lures, namely Paris Hilton.

Returning to the worm era, the next major event was Bagle, in January 2004. Bagle started life as a mass-mailing worm but eventually became a prolific spam spreading botnet. It was incredibly successful due its aggressive development.

It was clear that the author was constantly monitoring how antivirus companies were blocking their creation.

For example, when the author noticed how antivirus vendors were blocking attachments, they placed the infected attachments in password protected archives, with the password in the message body. When that stopped working, the author put the password in an image instead.

Bagle was also one of the first threats to start using polymorphism. Botnets were becoming big business and competition was fierce.

A fight to the finish

A later variant of Bagle started an insult war with the Netsky worm's author. As competition for available targets heated up, Bagle began replacing infections of Netsky with copies of itself.

Thankfully, the onslaught of worms was nearing an end in 2004, but not before MyDoom struck and became the fastest spreading worm yet. A record that still stands today.

Some initially suggested that the worm was written to defend Linux's honor after a DDoS attack against SCO Group (which had made legal allegations against Linux OS), while others alleged that it had been commissioned by spammers.

In addition to spreading by email after pilfering address books, the worm also copied itself to the download folder of peer-to-peer sharing software Kazaa, masquerading as one of the following files: activation_crack, icq2004-final, nuke2004, office_crack, rootkitXP, strip-girl-2.0bdcom_patches, or winamp5.

It was reported at the time that 25% of all emails sent in 2004 were infected with MyDoom and damages were estimated at $38 billion.

The Netsky family of worms was the first of two worms created by 18-year-old German computer science student, Sven Jaschan. The worm is most famous for the insults being launched at the authors of Bagle and MyDoom within its code.

This back-and-forth skirmish led to a flurry of variants being released. In response to Bagle's opening gambit, Netsky deleted competing worms, namely Bagle and MyDoom, from infected computers.

Sasser, the second Jaschan creation, was thankfully the last in a series of worms that had forever changed the threat landscape.

Sasser did not spread via email but rather exploited an LSASS vulnerability in Windows XP and 2000 systems. Jaschan claimed that he created the worms to battle other, more destructive worms. SophosLabs reported in August 2004 that both Sasser and Netsky were responsible for 70% of all infections seen in the first half of that year.

The impact of the worm era

The early worms showed how readily people click on links in unsolicited attachments. They also demonstrated the effectiveness of the "double-extension" trick.

Unlike today, where most people use webmail through a browser, in the early years of the millennium most users, both at home and at work, relied on a full client to access email. Most computers had Outlook (at work) or Outlook Express (at home) installed.

The author of ILOVEYOU used a double extension on the payload (i.e. LOVE-LETTER-FOR-YOU.txt.vbs) that gave users a false sense of security. Windows has a default setting of suppressing double extensions for file types it knows. Therefore, users would see "LOVE-LETTER-FOR-YOU.txt" and think it was a harmless text file. To make matters worse, clicking on an attachment in Outlook (Express) in those days didn't display the file, it ran it!

Another notable impact is that in October 2003, Microsoft introduced Patch Tuesday, providing a structured and consistent approach to distributing patches.

Before this, patches were distributed ad-hoc or as part of service packs. Since patches to many of the vulnerabilities exploited by the worms were already available before the worms hit, the process was clearly not effective.

The ad-hoc patches were readily taken up by consumers, but enterprises were not prepared to constantly certify patches. They preferred the slower service pack model. Back then, the average time to patch a security vulnerability in an enterprise was about six months. Today, automatic patching is the norm and we hardly notice when many applications patch themselves.

There was also a deliberate effort to segregate networks as insurance against the next worm. Not only were firewalls being used to restrict inbound and outbound access to the internet, but they were increasingly being used internally.

This provided companies with choke points that could be easily closed in the event of an outbreak. More attention was paid to which ports were open and which hosts could communicate with each other.

Email filtering matured during this era. As worm authors kept trying to outsmart email filtering products, email filtering vendors added more detection tricks to their products. Defenders began blocking all sorts of file types in earnest.

And while email borne threats continued to proliferate, cybercriminals were already shifting their focus toward the next era: making money.

2005-2012 – The Monetization Era

This era saw the rise of cybercrime as a business. Prior to this, malware incidents were mostly associated with one of the following: curiosity, disruption, or notoriety.

Building on a cyberthreat landscape shaped by the worms, most of the new threats were designed for profit but many were still too noisy.

Spammers started aggressively pushing out all sorts of spam including luxury goods and pharmacy spam.

There was a new marketplace opening up for cybercriminals of differing talents. Exploit merchants found a niche within the evolving malware ecosystem. Their exploit kits helped drive "malvertising," which took advantage of an increasingly connected world.

Bulletproof hosting provided the infrastructure for all manner of cybercrime to flourish and proliferate like never before. Wherever there was the potential for financial gain, cybercriminals exploited those opportunities.

Cybercriminals, like their counterparts in the real world, got organized.

Affiliate networks and pharmacy spam

Spam had previously been a delivery mechanism for chain letters from an unwitting friend or relative, or a way to spread worms, but now it found a way to monetize itself through online scams.

As senior director of threat research at Sophos, Dmitry Samosseiko had written back in his VB2009 paper, "The stores sell fake watches, fake antivirus software, fake pills and fake love – the webmasters get their commission, making thousands of dollars per day." Pharmacy spam started appearing as a result of the proliferation of botnets-for-hire from the previous era.

The business model then shifted to rely on hundreds of affiliate networks, known as "Partnerka" in Russian.

These affiliates, who called themselves "webmasters," drove traffic to online stores run by cyber kingpins. While the Partnerka offered diverse products, chief among them was online pharmacy spam. This included the infamous "Canadian Pharmacy" spammers.

The online pharmacies provided a vast array of prescription medicines at discounted prices. The untimely death of Marcia Bergeron in 2006 marks the moment when these pharmacy scams went from merely financially motivated to criminally negligent.

With the help of bulletproof hosts, the Partnerka and their affiliates made untold billions from pharmacy spam. Others took note and financially motivated cybercrime was here to stay.

The Storm botnet

Once dubbed the world's "most powerful supercomputer," due to its size, the Storm botnet epitomized the monetization era.

Storm was designed for stealth and profit. At its peak, estimates of the botnet's size ranged from one million to 10 million infected computers. Storm deviated from its predecessors' playbook of noisy and aggressive to favor a more patient and silent approach.

Notoriety wasn't the goal; it was trying to amass as many infected hosts as possible. As the Storm worm extended its reach and assembled the Storm botnet, several key design decisions ensured its resilience.

Notably, it kept a low profile, often sitting dormant for months at a time awaiting instructions. Different parts of the botnet were responsible for specific tasks. Instead of relying on a central command-and-control (C2) infrastructure, Storm preferred a distributed peer-to-peer model. These features made it much more difficult for defenders to isolate and disable the botnet.

Not only were the C2 servers distributed, but Storm also used fast-flux DNS and polymorphism to evade defenders.

When it wasn't busy infecting computers, Storm was capable of launching DDoS attacks against anti-spam sites (Spamhuas & 419eaters) and security researchers (Joe Stewart.) Many of Storm's features became standard for future botnets.

Zeus

First identified in July 2007, the Zeus/Zbot trojan and its many offspring grew into some of the most prolific threats we've ever seen.

Zeus/Zbot is a "banking" trojan and these target users primarily through spam, phishing, advertising, drive-by-downloads, or social engineering. Zeus started life as a basic banking trojan, but in keeping with the era's theme, quickly developed into a full feature crimeware kit and "Crimeware-as-a-Service" was born.

Zeus licenses started at $1,000, but the author offered customized versions at a higher fee, which included 24/7 support and were distributed through affiliates.

The author of Zeus allegedly retired and sold the code to its competitor, SpyEye, in 2010.

The source code for Zeus was leaked online in 2011, which enabled less technical cybercriminals to learn from one of the most well-known malware kits to date. Leaked Zeus code was allegedly responsible for a number of variants, including Citadel, Gameover Zeus, ICE-9, CIDEX, Ramnit, Dridex, Kronos, Tinba and Panda.

Both Zeus and Gameover Zeus were implicated in spreading the ransomware, CryptoLocker. Its use was the subject of a multi-national fraud investigation that resulted in over 100 arrests.

The Conficker worm

Conficker's appearance signaled the return of the super-spreading worm.

First detected on November 21, 2008, Conficker rapidly infected millions of computers worldwide but did not result in much damage.

Despite five years having passed since the introduction of Patch Tuesday, and the lessons from past worms, Conficker still caught the world by surprise.

Conficker propagated by exploiting a vulnerability in the Windows Server service, the infamous MS08-067 (CVE-2008-4250) vulnerability - a number forever burned in my memory. Microsoft issued an emergency out-of-band patch for this critical vulnerability nearly a month (October 23, 2008) before the Conficker outbreak, but many did not patch their systems.

With estimates of up to 15 million infected hosts, Conficker infected indiscriminately, including the armed services of France, Britain and Germany.

One notable feature that set Conficker apart was its use of the as-yet-unreleased MD6 cryptographic hash function to protect its payload. With this and other tricks learned from previous malware, Conficker was considered one of the most advanced threats to date.

Unpatched and infected systems still exist and detections for this threat are still showing up in telemetry. Aside from a later variant dropping a spambot and scareware, we still don't know the worm's true purpose.

Stuxnet

Stuxnet, believed to be the world's costliest cyberattack to develop, was a digital weapon targeting a physical system.

Stuxnet was allegedly developed by the NSA's Tailored Access Operations group and Israel's Unit 8200 as an alternative to a traditional kinetic military strike. Originally used against industrial control systems in Iran's nuclear enrichment centrifuges at the Natanz facility, Stuxnet found its way into the wild and began infecting non-Iranian computers.

While the Stuxnet attack achieved its specific goal of damaging nuclear centrifuges, it failed to stop Iran's nuclear enrichment program. Two additional advanced persistent threats (APTs), Duqu (2011) and Flame (2012,) were a direct result of Stuxnet's development.

Further, the unintended release into the wild of Stuxnet handed cybercriminals at least four zero-day vulnerabilities that could be used to attack general targets.

Stuxnet's enduring legacy is that it permanently opened the door to nation-states' use of digital solutions in analog conflicts. We would see this repeated with the Shamoon (2012) attack on Saudi Aramco and the BlackEnergy 3 (2014) attack on the Ukrainian power grid.

The story of Stuxnet was featured in the 2016 documentary "Zero Days."

The Blackhole exploit kit

Blackhole wasn't the first exploit kit (EK). That honor belongs to MPack from 2006. However, the emergence of the Blackhole exploit kit (BHEK) in 2010 provided another way for cybercriminals to coordinate and monetize their specialties.

Exploit kits were the glue that held together different parts of the cybercrime ecosystem, including spammers, exploit merchants, traffic aggregators, website hackers and malware authors.

Blackhole was so prolific in its heyday that many defenders had to separate their threat stats by "Blackhole" and "not-Blackhole."

Exploit kits prefer drive-by downloads as their infection vector. The BHEK drove the underground exploit market to produce more vulnerabilities than could be consumed by any one platform. Many vulnerabilities focused on some of the most deployed and unpatched applications: Java, Adobe Reader, Shockwave and Flash.

The payloads dropped by the BHEK included ransomware's precursor, FakeAV, rootkits and Zeus. So successful was the BHEK and its subscription business model that when its author, Dmitry "Paunch" Fedotov, was arrested in late 2013 many of the copy-cat exploit kits started jockeying for position in the void left by Blackhole's absence.

In 2015, the Angler EK took top spot by specializing in zero-day vulnerabilities.

Malicious advertising

Following earlier attacks against prominent sites, malicious advertising ("malvertising") also found its stride during this era. Aided and abetted by Blackhole and other exploit kits, malvertising increased 2.5-fold in 2011 and an estimated 10 billion ad impressions were compromised by malvertising in 2012.

Malvertising campaigns attacked some of the web's largest sites, driving home the message that there was no such thing as a "safe site."

By 2011, online advertising generated over $30 billion in revenues in the US alone. This was driven by an ever-growing number of users surfing the internet, providing an ever-increasing pool of targets for cybercriminals.

Key to malvertising's success was the infiltration of the advertising ecosystem. This could be accomplished by compromising the ad networks or real-time bidding services, posing as legitimate advertising firms representing bogus brands, or as bogus firms representing legitimate brands.

Whatever the ruse, malvertising was used to deliver any number of payloads, including spyware, adware, cryptominers and eventually, ransomware. Although Windows was the primary target, the platform agnostic nature of malvertising meant that it could also infect Macs, Chromebooks and mobile devices.

The impact of the monetization era

The events of this era led to an improvement in email filtering due to unprecedented levels of spam and the growing threat of phishing.

Exploit kits and malvertising led to further filtering of web content.

The increased threat from drive-by downloads while browsing online, and the abundance of vulnerabilities for many popular applications that made exploit kits and malvertising possible, also drove the adoption of application control technologies and patch management software.

We started seeing browsers auto updating and sandboxing themselves and the gradual deprecation of some of the most vulnerable applications. Although for some applications (such as Adobe Flash), it wasn't fast enough.

In response to the Conficker worm, in 2009 Microsoft made two important changes to the way its operating systems handled USB drives. First, AutoPlay no longer supported the AutoRun functionality for non-optical removable media. Second, Microsoft added a notification in the pop-up dialogue to indicate a program was running from external media. These are the kinds of slow gradual changes that we see from time-to-time that increase both awareness and security.

Exploits kits and malvertising also resulted in exponential growth of the market for vulnerabilities during this era. It didn't help that nation-state-sponsored attackers were releasing zero-days into the wild.

Malvertising eroded whatever trust was left in online advertising. At first, they were merely a nuisance, with all their popping over and popping under, but by now they were dangerous. Ad blockers proliferated. Consumers, advertisers and content creators have been locked in a pitched battle over fair access to content ever since.

We also started seeing unprecedented industry cooperation. To combat Conficker, an industry working group was formed in February 2009. The clear and present threat of malvertising also elicited the forming of the Anti-Malvertising Task Force.

Cooperation between the information security industry, law enforcement and payment processors had a profound impact on cybercriminals' money-making operations, such as that implemented by the Reveton trojan.

In the early part of the monetization era, payment processors started banning FakeAV operators from accepting credit card payments. Coupled with greater awareness and protection, criminals moved to "police lockers."

Distributed by the Zeus-derived Citadel trojan, the Reveton trojan began to spread in 2012. The malware would lock the user's session posing as a local law enforcement agency and accuse victims of illegal activity such as downloading unlicensed software, movies or music, and collecting child sexual abuse material.

The malware demanded a fine be paid in the form of prepaid cash services, such as Green Dot MoneyPak, Ukash and Paysafe. Cracking down on these payment alternatives the criminals were left with only one option: cryptocurrency.

2013-Present – The Ransomware Era

Ransomware is not the only defining event during this era, but it has certainly had the greatest impact.

There's an argument to be made that we should have seen it coming. After all, the idea wasn't new. The first recognized ransomware threat was the AIDS trojan of 1989. Extortion had been the motive behind many DDoS campaigns. Police lockers were heading in the same direction but weren't devastating enough.

Modern ransomware found the right blend of technology and urgency. While all other threats continue to exist, nothing has come close to rivaling ransomware's destructive force.

Damage estimates from ransomware attacks are in the trillions of dollars. It has exposed many weaknesses in IT defenses, spawned new technologies and new industries and, unfortunately, it has also had a profound impact on healthcare providers and other critical industries.

Moreover, many of today's cyberattacks ultimately end with the release of ransomware and, like exploit kits, it has provided a nitro-fueled boost to an already thriving cybercrime ecosystem.

The Snowden leaks

The Snowden leaks revealed to the world the extent to which our privacy was under attack. Not only were cybercriminals in the game but, as many had suspected, so were our own governments. Edward Snowden's stolen material dwarfed all previous leaks, including Chelsea Manning's incendiary leaked material from 2010.

The Snowden documents were immediately divisive. The reactions by government, consumers and the technology industry, which prompted reforms in many areas, have been dubbed the "Snowden effect."

Many of the reactions re-ignited the privacy versus national security debate at all levels of society. On one side, government officials decried the leaks. NSA Director General, Keith Alexander said the leaks caused "irreversible and significant damage," and Director of National Intelligence, James Clapper argued that the leaks had degraded the intelligence communities' capabilities and damaged relationships.

Critics argued that there hadn't been a rethinking of the propriety of NSA surveillance activities nor how broad government surveillance policies ought to be. Setting aside the hero or traitor debate, thanks to these and other leaks, our communications are now more secure than ever.

The film "Citizenfour," based on Snowden and the NSA leaks, won Best Documentary at the 87th Academy Awards.

CryptoLocker

With respect to FDR, I believe September 5, 2013 to be information security's "date which will live in infamy." That's the date when CryptoLocker was unleashed on the world.

During its short existence, CryptoLocker provided future criminals with a winning formula by mating two existing technologies: encryption and cryptocurrencies.

Three months after its launch, one of the Bitcoin wallets used by CryptoLocker to collect payments contained nearly $30 million. To date the damages associated with ransomware are in the trillions of dollars.

What has made ransomware so enduring is the irreversible nature of the attack - when no backups are available - coupled with an independence from traditional payment methods.

The Reveton trojan from the previous era lacked the permanence of modern ransomware and relied on commercial payment solutions. This made it easier to recover from an attack - often a reboot was all that was necessary - and for law enforcement to track and prosecute the offenders.

CryptoLocker and many of its offspring also resurrected an old threat vector that had been dormant for over a decade: document malware.

Since then, many groups behind some of the most prolific ransomware families have honed their skills and adapted to a changing environment. No individual or industry is immune from a ransomware attack. No one technology is enough to stop it. What started as a novel, but probably inevitable, idea has grown into a problem of epic proportions.

There are over 1,000 ransomware families – although, thankfully, not all of them are active. The threat landscape was changed forever by CryptoLocker and its aftershocks are still being felt.

Payment card data theft

Using RAM scraping malware, cybercriminals stole hundreds of millions of credit card numbers from retailers, including from attacks against the US retail giants Target (2013) and Home Depot (2014).

Payment card data theft has seen a few iterations over the years. Those that remember the "zip-zap" or manual credit card impression machines will also remember how easy it was to steal credit card information simply by holding onto the carbon paper in between the different receipts. Even if you didn't have carbon paper, a simple pencil rubbing was all that was necessary.

As card processing became digital, the same information that was once captured physically was also encoded in the magnetic strip on the back of the card. This meant that physical skimmers, installed on ATMs or gas pumps, could be used to read the information and be collected for later use or re-sale.

The problem with physical devices is they do not scale very well. Enter RAM scraping malware.

This type of malware is installed on point-of-sale (POS) devices. The purpose of the malware is to intercept the track data as it's being passed from the card reader to the terminal.

Using this type of malware, criminals stole hundreds of millions of pieces of payment card data, including credit/debit card numbers, PINs, expiration dates, card security codes, and cardholder names. In some of the breaches, criminals also stole personal information, such as addresses, phone numbers and email addresses.

So large were the dumps that they drove down the price of stolen credit cards for sale on the underground.

Many large, mostly US-based, retailers were hit between 2012 and 2014. The high-profile attacks forced massive changes in POS hardware and software and accelerated the adoption of chip-enabled cards in the US.

The Mirai botnet

Mirai was a striking example of cybercriminals exploiting new technologies. Not content with "pwning" traditional computers, they started going after other internet-connected devices. The result was a botnet capable of massive DDoS attacks.

Mirai was first developed in late 2015 but had its most profound impact in 2016. This is when the botnet infected hundreds of thousands of vulnerable routers and DVRs. It was used in DDoS attacks against krebsonsecurity.com, the French web host OVH and DNS services provider, Dyn.

The attack on Dyn took down many high-profile websites, such as GitHub, Twitter, Reddit, SoundCloud, Spotify and others. What was shocking was that it only needed to use 10% of its estimated 550,000 compromised devices to take down Dyn. Had the entire power of the botnet been unleashed, it could have been much worse.

The way Mirai identified its victims was by scanning for devices that respond to telnet (tcp/23) and using a table of factory default usernames and passwords to gain access.

Once connected to a device, Mirai installed a copy of itself and began scanning the internet for additional devices to infect. Like Bagle and Netsky before it, Mirai would also clean up any competing botnet infections prior to installing itself.

Later Mirai variants and other internet of things (IoT) malware started exploiting vulnerabilities in all sorts of connected devices. Mirai and its many replicas were used sporadically after the initial wave of attacks, but most have been relatively quiet for some time.

However, with the number of connected devices increasing exponentially, cybercriminals now have a toy capable of delivering DDoS attacks like never before.

Mirai is the subject of an EP, "Four Pieces for Mirai (Overture)," by James Ferraro.

WannaCry

WannaCry, the first ransomware-worm hybrid, demonstrated yet again how a lapse in patching can have dire consequences. WannaCry relied on exploits stolen from the NSA between 2013 and 2016 and publicly released by The Shadow Brokers in April 2017.

Microsoft learned that the exploits had been stolen in January 2017 and took the unusual step of delaying the February patch bundle until March so they could issue a fix. Unfortunately, much like the worms of the past, patch uptake wasn't quick or complete enough, despite a near 60-day head start.

In addition, operating systems that were out of support - Windows XP and Windows Server 2003 - but still in use were not initially covered by the release.

The WannaCry attack began on May 12, 2017. The malware used the EternalBlue vulnerability, developed by the NSA, to exploit the Windows Server Message Block (SMB) protocol.

Another vulnerability, a back door called DoublePulsar, also developed by and stolen from the NSA was found on tens of thousands of infected systems.

The attacks forced Microsoft to release out-of-band updates for unsupported products in an attempt to stem the attack.

Security researchers furiously scoured the worm's code to try and find a weakness. Luckily, the worm's authors had built in a kill switch, and the domains were registered and sinkholed later that day, but not before hundreds of thousands of hosts had been infected and billions of dollars in damages had been accrued.

While the impact was felt globally, the motive for the attack remains unclear.

The Bitcoin wallets associated with WannaCry collected a little over $140,000 USD. On August 2, 2017 the wallets were drained of all funds. In December 2017, the US, UK and Australia accused North Korea of perpetrating the attack.

Much like Conficker, WannaCry is now part of the background radiation of the internet. There are still unpatched systems, beaconing in the darkness and attempting to find victims.

NotPetya

Having just recovered from May's WannaCry attacks, the world was rocked again in June 2017 when NotPetya struck.

It highlighted how vulnerable global supply chains can be to cyberattacks. What started as an attack against a Ukrainian accounting software company, NotPetya crippled some of the world's largest shipping and logistics companies.

The attacks began on or around April 14, 2017 with the quiet infiltration of the software company's update servers. The attackers then began modifying the accounting software MeDoc.

In May, the update servers began distributing XData ransomware, possibly as a test for what was to come. Then, on June 27, the update servers began spreading NotPetya.

The malware was a modified version of Petya ransomware that incorporated worm-like functionality. In a cruel twist of fate, NotPetya also used the EternalBlue vulnerability to spread. Thankfully, unlike WannaCry, this worm was not designed to spread externally.

NotPetya also used mimikatz, the credential dumping tool, to capture available credentials in memory and the Sysinternals tool, PsExec to spread laterally across internal networks. Unlike its namesake, NotPetya's ransomware component was only a distraction and not its main goal.

The ultimate goal was to scramble an infected machine's disk at the sector level, thus making it unrecoverable.

This made two major, global cyberattacks in two months directly attributable to the NSA's carelessness. Reportedly causing over $10 billion in damages, some of the affected companies have yet to fully recover.

Magecart

As physical retailers improved their security, the skimming community set its sights on online shopping.

Active since 2014, Magecart malware specializes in web-skimming. The malware is employed by at least 12 different groups to silently hack e-commerce sites in order to hoover up personal and financial information at an unprecedented rate.

The attack involves compromising websites using known vulnerabilities, implanting Magecart code and extracting credit card numbers, names and card security codes (CVV2) to an attacker-controlled server.

In other cases, thieves use a supply chain compromise to go after third-party companies who are providing services to the e-commerce sites.

The Magecart attacks are yet another example of how cybercriminals have been specializing and cooperating. Software developers will create web-skimming kits capable of stealing credit card information at scale. Website hackers will compromise e-commerce sites and sell access to the buyers of the skimming kits. Pilfered card data can then be sold to markets that specialize in stolen card data. Finally, buyers of the stolen card data can use it to make online purchases.

Thousands of sites to date have been victims of the various Magecart groups. Unfortunately, there isn't much that online shoppers can do to protect themselves against this threat besides carefully monitoring their spending accounts for fraud.

Attacks deploying Magecart have hit online retailers both large and small, including 2018's high profile attacks against Newegg, Ticketmaster and British Airways.

Double extortion

Following the extortion of the city of Johannesburg in 2019, the criminals behind Maze ransomware picked up a new trick: double extortion.

They not only encrypted and stole data, but also threatened to publish the stolen data if companies didn't pay. This additional social pressure turned the screws even tighter on victims. Especially those that were undecided about whether to pay the ransom or not.

In one case, we witnessed attackers attempting to turn the employees of a victim company against their own executives and IT department for the company's refusal to negotiate with the crooks. This latest development followed a long line of other tricks aimed at increasing the payment rate.

Unfortunately, even if a company was capable of fully recovering from a ransomware attack without paying the ransom, they could still find themselves in regulatory hot water.

Under the threat of a public data breach some companies might opt to pay the ransom rather than any official fines imposed upon them. Paying the ransom might be the cheaper option of the two, considering the recovery costs and brand damage that are also associated with a breach.

Not wanting to waste a good opportunity, the double extortion tactic has been copied by many other ransomware crews. A recent interview with an individual allegedly affiliated with REvil ransomware believes that the future of ransomware will "be data extraction and not simply data denial."

The only solution to this Gordian knot is to not become a victim in the first place. Something that is easier said than done.

Once an APT tool exists, it exists for everyone

A trend that started a couple of years ago: the wider adoption of nation-state-sponsored tools and tactics, went mainstream in 2020.

It's a trend we've seen play out many times in our industry. A group creates a new tool or pioneers a new tactic and it is quickly adopted by all sides. Penetration testers add them to their bag of tricks. Professional cybercrime gangs use them in attacks to devastating effect, while other attack groups bake them into point-and-shoot toolkits for novices to use.

Often these new tools or tactics come from nation-state-sponsored attack groups that have the resources necessary to develop novel attacks.

For cybercriminals, it's very much a copy and paste operation. Especially when they know the tool or tactic has proven its effectiveness and that defenders are usually slow to react to novel attacks.

This gives the adversaries a head start and immediately increases the success rate of their attacks.

The downside of this, besides better tooling for the cybercriminals, is that nation-state-sponsored groups are starting to blend into the background. If every attacker is using the same tools it can be harder to distinguish one group from another.

The good news is that mounting a defense against APTs should also take care of the cybercriminal threat.

Encryption

In response to the Snowden leaks there was a groundswell of activity to get everything encrypted.

Google started encrypting all the traffic between its datacenters in response to the joint NSA-GCHQ program MUSCULAR.

In the face of the NSA's bulk collection program, PRISM, big tech companies stared adding TLS everywhere they could. Apple, and eventually Google, turned encryption on by default in their mobile operating systems.

Conversations around privacy and surveillance are front and center in many policy debates. Thanks to Snowden - this is not an implicit approval of his actions but a fact - over 80% of the web is encrypted, and that's a good thing.

The impact of the ransomware era

Ransomware has turned our world upside down in more ways than I can count.

It's laid bare the failures by many organizations to do some of the basic security work, whether intentional or not.

It's made us re-evaluate our security controls, build or strengthen security cultures within our organizations, create new industries and innovate new products.

But more than that, it has made it strikingly clear that getting security right is difficult, but we must not be deterred from doing the necessary work that our digital world requires. To make ransomware go away forever, we must stop paying the cybercriminals. Until that time, we must keep fighting.

There have been other cybersecurity impacts from this era.

For instance, in the wake of the attacks against retailers, the payment card industry accelerated the adoption of chip-enabled cards in the US. This, in turn, pushed POS vendors to include chip readers in their handheld devices and add encryption to all stages of the payment transaction process.

They are also leveraging whitelisting of applications and code signing of binaries to ensure the integrity of their systems.

The eventual move to accepting tap payments has also improved transaction security. The strengthening of brick-and-mortar shopping security led cybercriminals down the path of least resistance to start targeting e-commerce platforms.

Now Visa, Mastercard, and American Express are addressing this new threat by offering tokenization services to online merchants in an effort to devalue payment card data. They are also joining the fight by providing scanning and analysis services for online merchants to notify them of compromises.

Responding to evolving threats

The nation-state-sponsored threat and its cybercriminal copycats have given us plenty to worry about and we're continuously adjusting our response.

Sometimes, the best defense means doing something we should already be doing, such as patching and layered defense. At other times it means rolling out existing technologies that we know are an effective mitigation, such as multi-factor authentication or application control.

But sometimes we need to innovate completely new technologies to combat novel threats, such as machine learning.

In reality, we must do it all if we wish to remain one step ahead of cybercriminals. The creation of the MITRE ATT&CK framework, for one, has provided the defender community with a common taxonomy for adversary tactics and techniques.

Taken from the playbooks of nation-state-sponsored adversaries, the framework allows us to coordinate and organize our defenses against real-world observations. When we have visibility into the inner workings of our most advanced antagonists, it becomes easier to mount a coherent defense.

Conclusion

I hope you've enjoyed reading this trip down memory lane as much as I have enjoyed writing it.

We've come a long way in 20 years, and while there have been some harrowing moments, it's important to reflect on our progress and celebrate our successes. The technological progress the world has witnessed would not be possible if it wasn't for the professionals who work tirelessly every day to make the internet safer and more secure.

As our industry matures, we continue to demonstrate how the security industry is no longer the world of "no." We're enablers, collaborators, and innovators. One of our lasting legacies is that we continue to come together to solve problems. Whether it's the Conficker working group, any number of ISACs, the Cyber Threat Alliance, hacker cons, or the recent COVID-19 Cyber Threat Coalition, we get things done.

The problems of this era, and those to come, are challenges we will rise to.

As the African proverb states, "If you want to go fast, go alone. If you want to go far, go together." As we go together into the next 20 years, let's remember that the fight is honorable and it's worth it.

Appendix: sources and references

https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg_(book)

https://www.cl.cam.ac.uk/~rja14/book.html

https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms

https://en.wikipedia.org/wiki/ILOVEYOU

https://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/?c=y&page=2

https://www.computerhope.com/vinfo/iloveyou.htm

https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/VBS~LoveLet-AA.aspx

https://nakedsecurity.sophos.com/2008/10/15/you-have-not-received-an-ecard/

https://nakedsecurity.sophos.com/2009/05/04/memories-love-bug-worm/

https://nakedsecurity.sophos.com/2015/05/04/memories-of-the-love-bug-15-years-ago-today/

https://nakedsecurity.sophos.com/2020/05/04/iloveyou-the-love-bug-virus-20-years-on-could-it-happen-again/

https://en.wikipedia.org/wiki/Subject%3A_I_Love_You

https://www.imdb.com/title/tt1227182/?ref_=fn_al_tt_1

https://en.wikipedia.org/wiki/Release_(Pet_Shop_Boys_album)

https://genius.com/Pet-shop-boys-e-mail-lyrics

https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in-2020

https://www.fastcompany.com/90500378/iloveyou-virus-microsoft-steven-sinofsky-book

https://news.microsoft.com/2000/06/08/outlook-email-security-update-now-available/

https://en.wikipedia.org/wiki/Code_Red_(computer_worm)

https://www.sophos.com/en-us/press-office/press-releases/2001/07/pr_au_20010731codered.aspx

https://www.biz.netvigator.com/chi/pdf/eps_whitepaper.pdf

https://web.archive.org/web/20110722192419/http://www.eeye.com/Resources/Security-Center/Research/Security-Advisories/AL20010717

https://web.archive.org/web/20060628174538/http://pcworld.com/news/article/0,aid,56504,00.asp

https://en.wikipedia.org/wiki/Code_Red_II

https://web.archive.org/web/20070427010621/http://www.pcworld.com/article/id,57584-page,1/article.html

https://web.archive.org/web/20191213105201/http://www.unixwiz.net/techtips/CodeRedII.html

https://web.archive.org/web/20041205102928/http://eeye.com/html/research/advisories/AL20010804.html

https://en.wikipedia.org/wiki/Nimda

https://nakedsecurity.sophos.com/2011/09/16/memories-of-the-nimda-virus/

https://web.archive.org/web/20160807233000/http://www.kaspersky.com/about/news/virus/2001/Information_about_the_Network_Worm_Nimda_

https://www.f-secure.com/v-descs/nimda.shtml

https://en.wikipedia.org/wiki/SQL_Slammer

https://www.theregister.com/2003/02/06/slammer_why_security_benefits/

http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf

https://www.wired.com/2003/07/slammer/

https://www.securityfocus.com/news/6767

https://en.wikipedia.org/wiki/Blaster_(computer_worm)

https://web.archive.org/web/20081101140521/http://www.vnunet.com/vnunet/news/2123165/fbi-arrests-stupid-blaster-b-suspect

https://docs.microsoft.com/en-us/archive/blogs/michael_howard/why-blaster-did-not-infect-windows-server-2003

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Msblast.A

https://en.wikipedia.org/wiki/Welchia

https://www.cnn.com/2003/TECH/internet/09/24/state.dept.virus/index.html

https://www.giac.org/paper/gcih/517/welchia-worm/105720

http://www.internetnews.com/ent-news/article.php/3065761/Friendly+Welchia+Worm+Wreaking+Havoc.htm

https://en.wikipedia.org/wiki/Sobig

https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Sobig-F/detailed-analysis.aspx

https://www.theregister.com/2008/01/09/sobig_anniversary/

https://malware-history.fandom.com/wiki/Sobig

https://www.theregister.com/2003/06/18/fresh_variant_to_tedious_worm/

https://en.wikipedia.org/wiki/Sober_(worm)

https://www.itnews.com.au/news/world-cup-sober-worm-goes-stellar-63271

https://www.itnews.com.au/news/this-time-its-the-sober-causing-world-cup-problems-63262

http://news.bbc.co.uk/2/hi/technology/4552197.stm

http://news.bbc.co.uk/2/hi/technology/4466016.stm

https://www.smh.com.au/technology/bogus-fbi-emails-virus-20051126-gdmir5.html

https://www.technewsworld.com/story/47764.html

https://en.wikipedia.org/wiki/Bagle_(computer_worm)

https://securelist.com/the-bagle-botnet/36046/

https://www.itnews.com.au/news/new-botnet-threats-emerge-from-lethic-and-bagle-164540

https://a51.nl/sites/default/files/pdf/MessageLabsIntelligence_2010_Annual_Report_FINAL1.pdf

https://en.wikipedia.org/wiki/Mydoom

https://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/

https://www.wired.com/2009/07/mydoom/

https://www.youtube.com/watch?v=PuMj6ioMflY

https://web.archive.org/web/20040803165453/http://seattletimes.nwsource.com:80/html/businesstechnology/2001859752_spamdoubles18.html

https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~MyDoom-A/detailed-analysis.aspx

https://en.wikipedia.org/wiki/Netsky_(computer_worm)

https://en.wikipedia.org/wiki/Sven_Jaschan

https://web.archive.org/web/20041217054347/http://www.stern.de/computer-technik/internet/index.html?id=525454&eid=501069

https://en.wikipedia.org/wiki/Sasser_(computer_worm)

https://www.sophos.com/en-us/press-office/press-releases/2004/05/va_sasserattack.aspx

https://www.sophos.com/en-us/press-office/press-releases/2004/05/va_sasserarrest.aspx

https://www.sophos.com/en-us/press-office/press-releases/2004/05/va_sasserreward.aspx

https://www.sophos.com/en-us/press-office/press-releases/2004/05/va_sassertip.aspx

https://www.sophos.com/en-us/press-office/press-releases/2004/05/va_sasser.aspx

https://www.theregister.com/2004/09/20/sasser_kiddo_offered_job

https://www.politico.com/magazine/story/2014/12/pharma-spam-113562

https://www.sophos.com/it-it/medialibrary/PDFs/technical%20papers/samosseikovb2009paper.pdf

https://www.theglobeandmail.com/news/national/counterfeit-drugs-caused-womans-death-coroner-concludes/article688808/

https://www.spamhaus.org/rokso/evidence/ROK6271/yambo-financials/mycanadianpharmacy-corp

https://www.spamhaus.org/statistics/spammers/

https://www.spamhaus.org/rokso/spammer/SPM1099/canadian-pharmacy

https://en.wikipedia.org/wiki/Storm_Worm

https://www.schneier.com/blog/archives/2007/10/the_storm_worm.html

https://en.wikipedia.org/wiki/Storm_botnet

https://web.archive.org/web/20071024002252/http://blogs.zdnet.com/security/?p=533

https://web.archive.org/web/20071023183243/http://blogs.zdnet.com/security/?p=592

https://en.wikipedia.org/wiki/Zeus_(malware)

https://en.wikipedia.org/wiki/Gameover_ZeuS

https://archives.fbi.gov/archives/news/stories/2010/october/cyber-banking-fraud

https://www.bbc.com/news/world-us-canada-11457611

https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

https://www.reuters.com/article/idUSTRE69S54Q20101029

https://www.securityweek.com/zeus-source-code-leaked-really-game-changer

https://web.archive.org/web/20110513075130/https://threatpost.com/en_us/blogs/zeus-source-code-leaked-051011

https://web.archive.org/web/20110512142925/http://www.csis.dk/en/csis/blog/3229

https://web.archive.org/web/20110527234131/http://csis.dk/en/csis/blog/3176/

https://www.csoonline.com/article/2361420/coding-flaw-leaves-zeus-admin-panels-easily-exploited.html

https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree

https://blog.trendmicro.com/trendlabs-security-intelligence/cryptolocker-its-spam-and-zeuszbot-connection/

https://en.wikipedia.org/wiki/Conficker

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067

https://web.archive.org/web/20130521144730/http://news.techworld.com/security/114307/experts-bicker-over-conficker-numbers/

https://msrc-blog.microsoft.com/2009/04/28/autorun-changes-in-windows-7/

https://web.archive.org/web/20090501143516/https://blogs.technet.com/mmpc/archive/2009/04/28/windows-addresses-the-changing-autorun-threat-environment.aspx

https://www.metafilter.com/91971/Conficker-in-control

https://web.archive.org/web/20090214153502/http://mtc.sri.com/Conficker/

https://en.wikipedia.org/wiki/Stuxnet

https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

https://www.nytimes.com/2019/09/04/magazine/iran-strike-israel-america.html

https://en.wikipedia.org/wiki/Duqu

https://en.wikipedia.org/wiki/Flame_(malware)

https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf

https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

https://en.wikipedia.org/wiki/Blackhole_exploit_kit

https://en.wikipedia.org/wiki/MPack_(software)

https://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/

https://krebsonsecurity.com/2013/12/who-is-paunch/

https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-2/

https://blog.malwarebytes.com/threats/exploit-kits/

https://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/

https://en.wikipedia.org/wiki/Malvertising

https://www.iab.com/insights/2011-full-year-iab-internet-advertising-revenue-report/

https://www.iab.com/insights/2012-full-year-iab-internet-advertising-revenue-report/

https://web.archive.org/web/20131215073437/https://otalliance.org/resources/malvertising.html

https://www.malwarebytes.com/pdf/infographics/malvertising-and-ransomware.pdf

https://www.malwarebytes.com/malvertising/

https://www.clickz.com/billions-of-web-ads-carried-malware-in-2010/52856/

https://blog.chromium.org/2008/10/new-approach-to-browser-security-google.html

https://itlaw.wikia.org/wiki/Conficker_Working_Group

https://web.archive.org/web/20110608152105/www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf

https://archive.is/20160327013002/http://www.reuters.com/article/idUS124679+08-Sep-2010+MW20100908

https://en.wikipedia.org/wiki/Edward_Snowden

https://www.npr.org/2013/09/20/224423159/the-effects-of-the-snowden-leaks-arent-what-he-intended

https://thehill.com/policy/technology/218155-intelligence-chief-says-snowden-leaks-created-perfect-storm

https://en.wikipedia.org/wiki/Citizenfour

https://mashable.com/2013/10/30/silent-circle-lavabit-darkmail-email/

https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html

https://en.wikipedia.org/wiki/CryptoLocker

https://www.blockchain.com/btc/address/1ACKcumkx4M3aQisMMLq32EubPkUNiUfTC

https://en.wikipedia.org/wiki/Mirai_(malware)

https://threatpost.com/mirai-fueled-iot-botnet-behind-ddos-attacks-on-dns-providers/121475/

https://en.wikipedia.org/wiki/Four_Pieces_for_Mirai_(Overture)

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

https://msrc-blog.microsoft.com/2017/02/14/february-2017-security-update-release/

https://www.theregister.com/2017/05/16/microsoft_stockpiling_flaws_too/

https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack

https://whois.domaintools.com/iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack/

https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/

https://twitter.com/actual_ransom/status/892928051360784384

https://twitter.com/actual_ransom/status/894605282642472961

https://en.wikipedia.org/wiki/Petya_(malware)

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

https://nakedsecurity.sophos.com/2017/06/28/new-petya-ransomware-all-you-wanted-to-know-but-were-afraid-to-ask/

https://nakedsecurity.sophos.com/2017/06/28/deconstructing-petya-how-it-spreads-and-how-to-fight-back/

https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc

https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/

https://en.wikipedia.org/wiki/Web_skimming

https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/

https://www.zdnet.com/article/inbenta-blamed-for-ticketmaster-breach-says-other-sites-not-affected/

https://www.inbenta.com/en/inbenta-and-the-ticketmaster-data-breach/

https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Klijnsma.pdf

https://blog.nasstar.com/magecart-time-to-focus-on-web-security-to-mitigate-digital-skimming-risk/

https://www.cnet.com/news/best-buy-data-breach-24-7-ai/

https://www.zdnet.com/article/city-of-johannesburg-held-for-ransom-by-hacker-gang/

https://www.bleepingcomputer.com/news/security/ransomware-attack-shuts-down-city-of-johannesburgs-systems/

https://www.bleepingcomputer.com/news/security/ransomware-gangs-team-up-to-form-extortion-cartel/

https://news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/

https://www.advanced-intel.com/post/an-interview-with-unkn-sheds-light-on-revil-s-operations-future-victims

https://letsencrypt.org/stats/

https://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/

https://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks/

https://www.latimes.com/world/la-xpm-2013-sep-12-la-fg-wn-clapper-snowden-disclosures-20130912-story.html

https://en.wikipedia.org/wiki/EMV#Implementation

https://www.emvco.com/wp-content/uploads/2020/03/20200306_EMVCo_EMV_Chip_Deployment_Stats.pdf

https://www.zdnet.com/article/visas-plan-against-magecart-attacks-devalue-and-disrupt/

https://www.mastercard.com/gateway/processing/security/tokenization.html

https://network.americanexpress.com/globalnetwork/products-and-services/security/tokenization-service/

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

20201207 WPEN (NP)

SOPHOS