X-Force Threat Intelligence Index 2019

IBM **Security**

Table of Contents

Overview

IBM Security develops intelligent enterprise security solutions and services to help today's businesses prepare for tomorrow's cyber security threats.

To keep fellow security professionals updated on relevant and potentially damaging cyberthreats to their organizations, our teams regularly release blogs, white papers, webinars, and podcasts about emerging threats and attackers' Tactics, Techniques, and Procedures (TTPs).

IBM Security releases the IBM X-Force Threat Intelligence Index annually, which summarizes the most prominent threats raised by our research teams from over the past year. The purpose is to provide both defensive and red teams with information that can help better secure their organizations.

Data and insights are derived from IBM X-Force monitored security clients, incident response services, and penetration testing engagements. **IBM X-Force research teams monitor data across 70 billion security events per day in more than 130 countries**—along with data derived from non-customer assets such as spam sensors and honeynets. X-Force researchers also run spam traps around the world and monitor **tens of millions of spam and phishing attacks daily,** analyzing **billions of web pages and images** to detect fraudulent activity and brand abuse in order to protect our customers.

In 2018, many organizations across all industries faced unmanageable levels of cyberthreats brought on by the changing threat landscape, the risk of exposure, and an ever-growing attack surface. The optimum strategy to respond to this combination of factors is to make security an integral part of culture and overall structure.

Key findings from IBM X-Force's data analysis for 2018 highlight our insights into various verticals, attack tactics, and major vulnerabilities that emerged during the year:

- **The finance and insurance industry—at 19 percent of total attacks and incidents—continues to be the most targeted industry, attracting attackers in every geography. Coming in second, at 13 percent of total attacks and incidents, is transportation services,** which includes airline, bus, rail, and water transportation services. We expect the transportation sector to continue rising as an attractive target for malicious actors, because of the industry's reliance on information technology to facilitate operations, its ubiquitous need for integration of third-party vendors, and its vast supply chain. These factors make for a larger attack surface than other industries. A breach of any segment of the transportation industry's supply chain can have a severe cascading effect upon multiple businesses and millions of global travelers.

- **In 57 percent of the breaches IBM X-Force Incident Response and Intelligence (IRIS) responded to in 2018, threat actors moved away from using malicious files in their attacks, favoring other methods to carry out their objectives.** Our team noted attackers are increasingly "living off the land," opting for existing tools, such as PowerShell or WMI command-line (WMIC) utility, within victim environments to achieve their objectives and maintain persistence. The use of PowerShell for malicious activities, such as injecting malware directly into memory to enhance obfuscation and evade antivirus detection software, was observed in attacks globally and cross-industry.

- **Looking at the targets of phishing attacks in 2018, in 27 percent of the phishing incidents attackers targeted the users of webmail services.** Given the increase in organizations moving to services hosted in the cloud[1], we expect cloud resources to continue to be a popular target.

- **Over the past several years, ransomware has become a popular cyber-attack for those looking to make money quickly and easily. However, more recently, criminals seem to use less ransomware[2] and are instead increasingly leveraging coin-mining malware.[3]** Malicious coin mining or "cryptojacking" is the act of installing a cryptocurrency miner on the victim's endpoint without their knowing it, thus enslaving their device to slowly gather coins for the attacker. This operation taxes the device's CPU/GPU, is costly in terms of electric power, and can cause damage to devices as they overheat. But cryptojacking is more than just utilizing computer resources. If coin-mining

malware is on organizational networks, it can mean the threat actor has breached the network and it's allowing the network to be exploited by other malicious actors with different, more detrimental objectives. No threat can be considered benign: Even a seemingly simple compromise can lead to a pivot in attacker TTPs. IBM X-Force has discovered illicit cryptojacking attacks are on the rise while ransomware seems to be on the decline. Over the course of 2018, attempts to install ransomware on X-Force monitored devices in Q4 (Oct.- Dec.) declined to less than half (45 percent) of the attempts in Q1. Meanwhile, cryptojacking attacks more than quadrupled in the same timeframe increasing 450 percent.

Before we delve into the details of our report, below are additional key findings from IBM X-Force's data analysis for 2018:

EMERGING AND RELENTLESS THREATS

- Publicly disclosed misconfiguration incidents increased 20 percent year-over-year. Even so, misconfigurations were not responsible for as many compromised records as 2017 — there was a 52 percent decrease in records compromised because of this threat vector.

- Necurs remained the world's top malware-sending botnet in 2018. With few exceptions, all major malware spam campaigns in 2018 were distributed by Necurs.

- In the banking Trojan arena, financially motivated threat actors' use of TrickBot variants made this financial malware the most actively tracked gang in 2018. The Gozi Trojan (aka, Ursnif) is grazing the top as the second-most active financial malware gang.

- Turning to the major vulnerabilities that affected organizations at scale in 2018, Spectre and Meltdown were the most significant vulnerability disclosures of the year, affecting many of the computer processor chips manufactured in the last 20 years. These hardware vulnerabilities could allow an attacker to gain access to data in protected memory. Mitigating these vulnerabilities through workarounds or available patches is necessary to protect against potential exploitation.

CYBERTHREAT LANDSCAPE: TOP OF THE CHARTS BY INDUSTRY AND GEOGRAPHY

- In 2018, the media sector topped the chart with 40 percent of publicly disclosed incidents. Half of these incidents involved misconfigured cloud servers and other improperly configured systems that leaked data or allowed a remote attacker to exploit the asset.

- According to data from X-Force-monitored global spam traps, the US topped the chart as the number one host of malware command-and-control (C&C) servers in 2018 with 36 percent of the total number of C&C servers.

- As for the top spam distributor, nearly 40 percent of all spam in 2018 originated from China. The lion's share of this statistic can be attributed to two major spam campaigns launched from Chinese-based hosts in 2018. In February and March, X-Force observed a large campaign that harvested email addresses—and between July and September a high-volume phishing campaign that contained random text followed by URLs that directed users to one of eight different malicious domains.

Part 1

Analyzing the Attack Surface: Most Relevant Threats

This section highlights security threats that are relentless and have consistently plagued enterprises for the past five years—as well as those that are more recently emerging and increasing in sophistication or prevalence.

Relentless Threats We Will Continue to See In 2019

THE INADVERTENT INSIDER

Inadvertent threat actors are insiders in your company who unwittingly compromise the environment. Two of the most prolific ways X-Force researchers have observed inadvertent insiders leaving organizations open to attack is by falling for phishing scams or social engineering, and through the improper configuration of systems, servers, and cloud environments, and by foregoing password best practices.

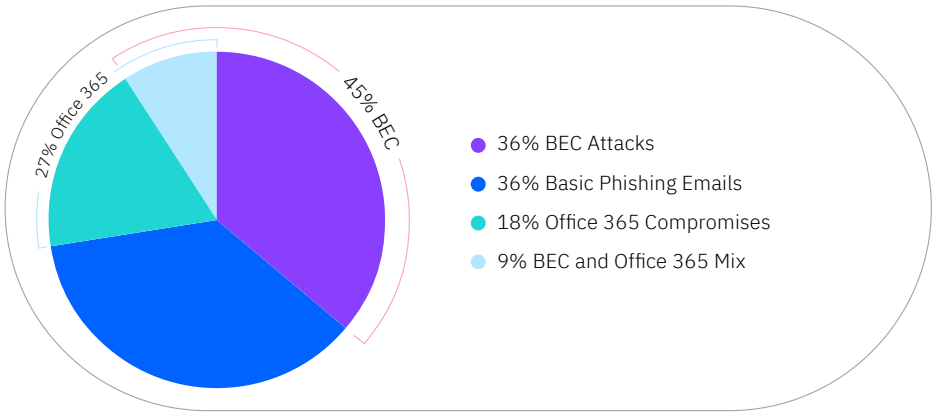
FALLING FOR PHISHING AND BUSINESS EMAIL COMPROMISE SCAMS

Nearly one-third—29 percent—of attacks analyzed by X-Force IRIS involved compromises via phishing emails. Of those, 45 percent involved business email compromise (BEC) scams, also known as "CEO fraud" or whaling attacks.

When it comes to the most lucrative types of social engineering scams, BEC has been a growing tide for several years spanning all industries and geographies. BEC scams purport to originate from an owner or CEO or a high-ranking employee. They are sent to those who control the company's bank accounts with instructions to execute a confidential wire transfer. The transfer ends up in accounts the criminals control. The FBI reports that BEC fraud has been growing rapidly in the US and across the globe, having cost organizations $12.5 billion at last count.[4]

Figure 1:

Phishing Categories Observed by X-Force IRIS in 2018



In 27 percent of the phishing incidents tracked, including those involving BEC scams, users of Microsoft Office 365 were the top targets, who had their email accounts compromised via web access. X-Force notes in this type of scam, the attacker most typically sets up an Office 365 account then sends a SharePoint invitation to edit a file. When the user attempts to open the file, they are presented with a fraudulent OneDrive log-in screen. This allows the attacker to steal the victim's credentials, and then use their account to send legitimate-looking emails to their supply chain instructing customers to wire money to a bank account different from the legitimate one they may have used in the past.

HUMAN ERROR CONTINUES TO FACILITATE BREACHES

Misconfigured cloud servers that include publicly accessible cloud storage, unsecured cloud databases, and improperly secured rsync backups, or open internet connected network area storage devices contributed to the exposure of more than 990 million records in 2018. This represents 43 percent of the more than 2.7 billion compromised records tracked by X-Force research for the year. While this number is notably lower than the 2 billion records compromised in 2017, the total number of publicly disclosed incidents that were attributed to misconfigured assets still increased 20 percent, year-over-year.

A 2018 survey indicated that misconfiguration is now the single-biggest risk to cloud security, with 62 percent of surveyed IT and security professionals noting it as a problem, followed by misuse of employee credentials or improper access at 55 percent, and non-secure interfaces at 50 percent.[5] Misconfigured systems often give attackers access to a plethora of data including email addresses, user names, passwords, credit card and health data, and national identification numbers. In one of the largest incidents in 2018, a major marketing firm leaked 340 million records of personal data including addresses, phone numbers, family structures, and extensive profiling data.[6]

Misconfigured systems could potentially expose internal company communications across a firm's entire global footprint and even lead to detrimental exposure of intellectual property, trade secrets, and the organization's strategic plans. Leaked login data from misconfigured assets can be used in targeted brute-force attacks where user IDs and passwords are reused across multiple assets and websites. Exposed data could also be used as part of larger identity theft schemes and to perform fraudulent activity. While most publicly disclosed breaches involving misconfigurations appear to be the result of inadvertent actions, a malicious insider could purposefully expose data and make it appear as an unintentional act.

MALWARE, SPAM, AND THE NOTORIOUS NECURS BOTNET

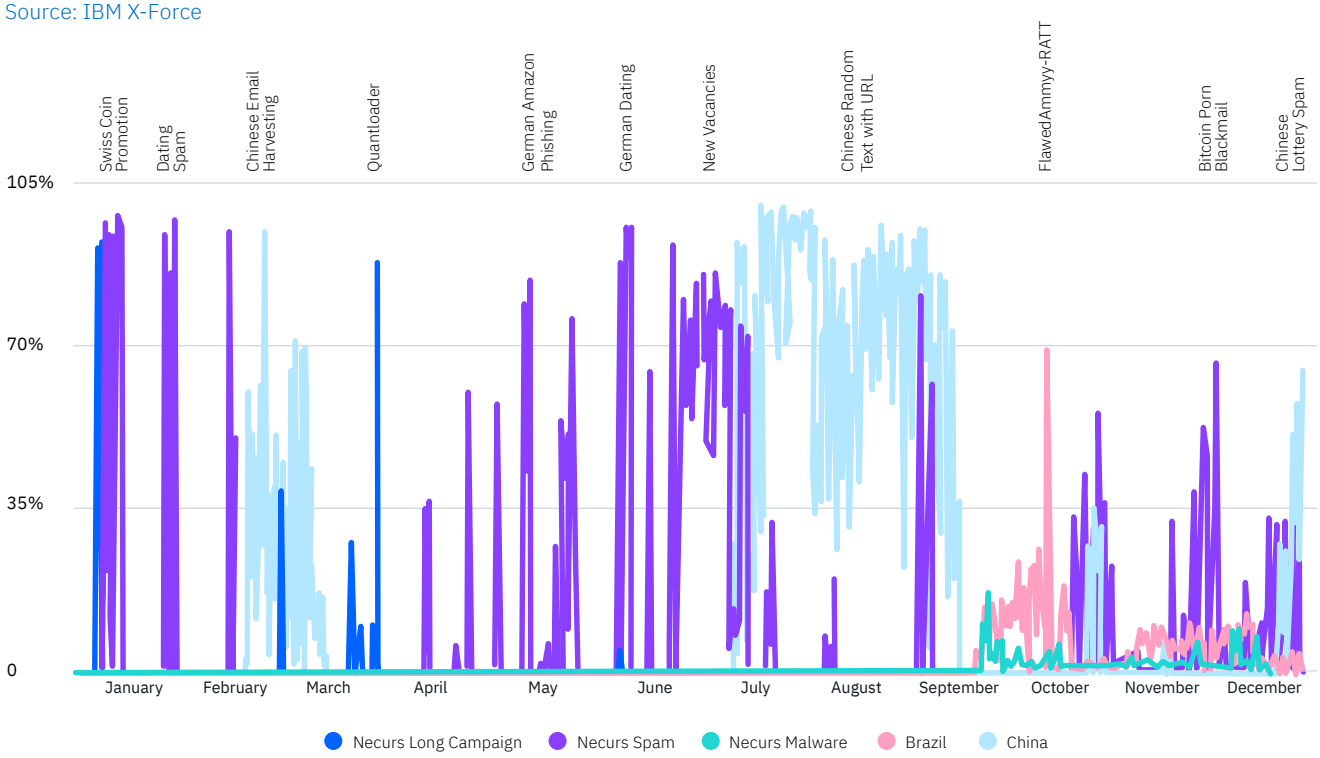
Spam and malware went hand in hand in 2018 and remained relentless in terms of campaigns spreading malicious links and attachments to users all over the world.

The top distributor of malware spam in 2018 was the Necurs botnet, which is operated by a cybercrime gang that targets users all over the globe. With very few exceptions, all major malware campaigns in 2018 were distributed by Necurs—especially those perpetrated by major cybercrime gangs or the operators of ransomware or banking Trojans.

Figure 2:

Necurs Campaigns as % of Total Spam in 2018

Source: IBM X-Force



While it continued to distribute banking malware and ransomware as it did in 2017, Necurs has also diversified its spamming to distribute other types of malicious email, such as dating spam, penny stock scams, cryptocurrency phishing and scams, and online banking phishing, to name a few.

Spam featuring attacks on cryptocurrency users emerged in large spam campaigns during early 2018. According to X-Force research, in January 2018, a Necurs campaign promoted the little-known cryptocurrency Swisscoin (SIC), repeating its 2017 "penny stock" campaign tactics to manipulate the value of this coin. Involving itself with cryptocurrency later in the year, Necurs used Bitcoin as a payment method in a number of major blackmail and extortion campaigns.

In its ongoing efforts to evade security controls and reach users via email, Necurs' malware campaigns in March and April continued to shuffle its obfuscation tactics. X-Force notes that the botnet's operators, who (for the most part) serve malware gangs, added an additional layer of complexity to their attack chain. To avoid detection, they distributed malicious zipped Microsoft internet shortcut files with ".url" file extensions. Once the file was opened, the Quant Loader malware downloaded. This malware is capable of distributing ransomware and password stealers. These tactics changed in various campaigns but were usually aimed to add steps to the malware delivery and deployment to evade security controls.

In terms of campaign recipients, Necurs botnet operators have moved away from wide-cast nets. Instead, they shifted strategy to include targeted attacks for specific audiences. In a notable blackmail campaign Necurs targeted users in their own language, setting up an automated content selection to match the recipient's email's top-level domain (TLD). That way, those receiving email from a .fr domain, got their extortion email in French, and those with a .de email domain received their email in German.

Targeting different sectors in a comparable manner, August 2018 saw Necurs deliver industry-specific emails with a remote-access Trojan in tow. For example, when the malware spam targeted the banking sector, Necurs directed it at recipient domains containing the word, "bank."

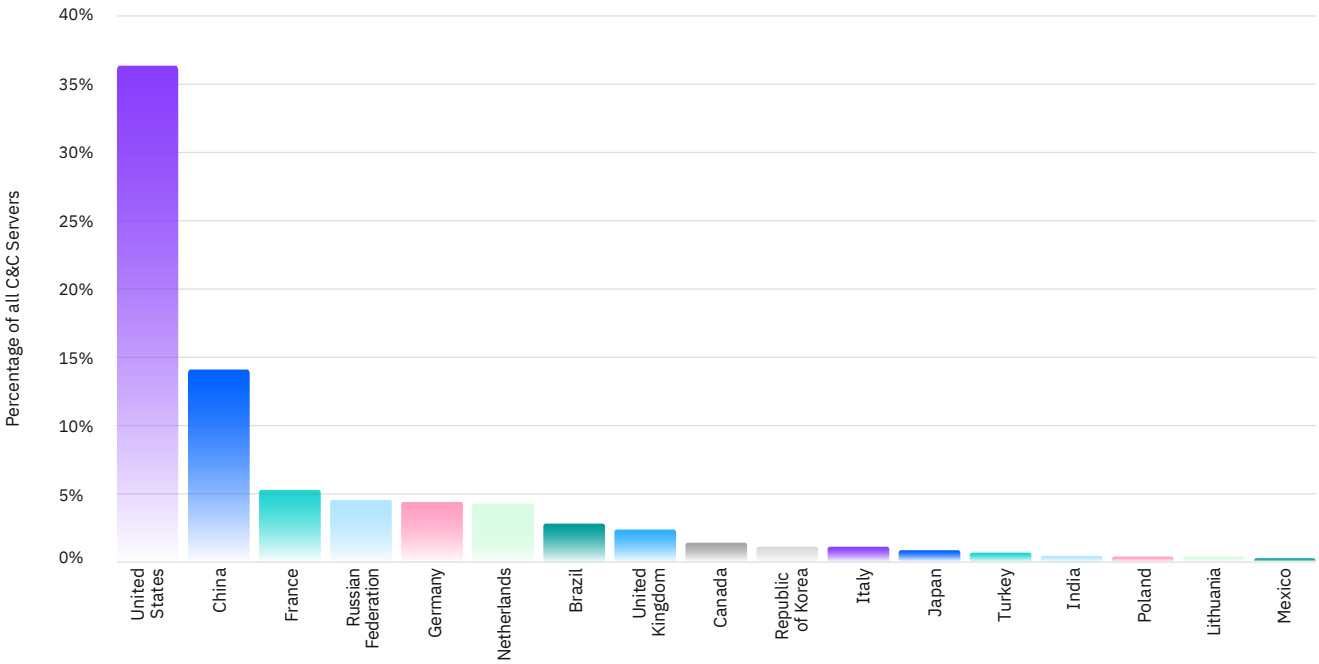
The malware behind these attacks was the "FlawedAmmyy-RAT," first used in generic spam campaigns that targeted users indiscriminately[7] and later delivered to users in targeted attacks.[8]

The majority of the Necurs botnet C&C servers were in the United States. This comes as no surprise, as the United States hosted 36 percent of the total number of C&C servers globally, followed by China, which hosted nearly 14 percent of the C&C servers. France, at a distant third, hosted a little over five percent of the total number of C&C servers. France shared its third rank with Russia and Germany, followed by the Netherlands, Brazil, and the UK.

Figure 3:

Top Hosting Countries of Malware C&C Servers

Source: IBM X-Force



In spam-originating countries where local IP addresses have been recorded as sending the most spam, China ranked at the top of the chart, with nearly 40 percent of all spam sent from Chinese IP addresses. This can be attributed to two major spam campaigns in 2018. The first campaign emerged in February and March and sought to harvest email addresses and the second arose between July and September 2018 containing random text and leading recipients to one of eight different phishing domains.

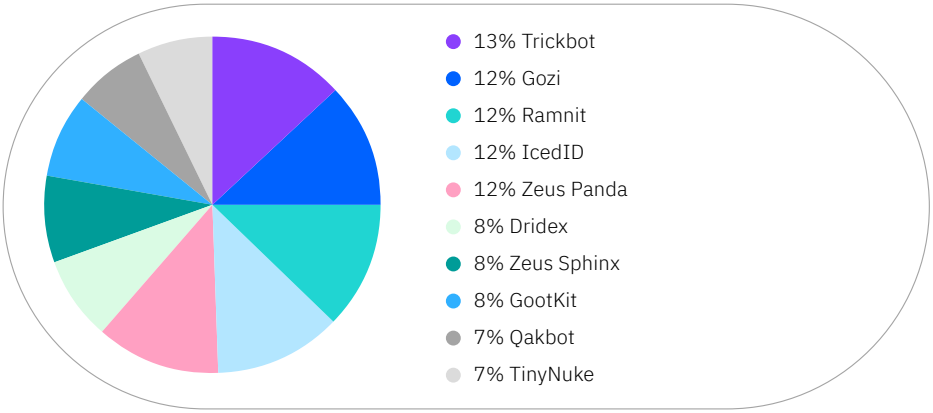
FINANCIAL MALWARE

Banking Trojans were the business of organized crime in 2018, with the global chart topped by familiar malware families, such as TrickBot, Gozi, Ramnit, or IcedID. Financially motivated threat actors' use of TrickBot variants made this financial malware the most actively tracked gang in 2018, according to X-Force researchers' analysis of global banking Trojan activity.

Figure 4:

Most Prevalent Financial Malware in 2018

Source: IBM X-Force



The chart above shows 2018's most prevalent financial malware with TrickBot making up 13 percent of campaign, followed by long time cybercrime-as-a-service gang, Gozi (aka Ursnif).

In third place is the Ramnit Trojan, which focuses its attacks on UK banks. Ranking fourth on the chart is the IcedID Trojan. Discovered by X-Force researchers in September 2017, IcedID and one of its distributors, Emotet, resurfaced in 2018, despite a significant decline in activity in 2017.

GOZI GRAZING THE TOP FOR SECOND YEAR IN A ROW

Gozi's rise to the top ranks of the global malware chart is marked by a long and sordid history of plaguing organizations, making it the longest-standing banking Trojan in the wild today. In circulation since 2006, it gained widespread media attention in 2010, when its source code was mistakenly leaked, giving rise to new variants of the malware. In 2013, Gozi was reported to be responsible for infecting more than one million computers globally and causing tens of millions of dollars in losses.[9] Gozi has managed to dominate the financial malware arena because its operators are well-organized, with links to an increasing number of actors across different geographical hubs. Renting the botnet's services to seasoned cybercriminals in a cybercrime-as-a-service model, Gozi's operators have the means to develop new capabilities that circumvent technological advances in banking security and it continues to operate over what has a been a long period in the cybercrime arena.

ICEDID ON THE RISE AGAIN

After a comparatively quiet period for IcedID in 2018,[10] the malware made a comeback attributable to collaboration with the TrickBot gang, which began distributing IcedID in mid-2018.

Returning the favor, IcedID has distributed TrickBot to infected machines on its own botnet in some of its 2018 campaigns, indicating a possible partnership between the two gangs. Given TrickBot's wide scope of activity in dozens of countries around the globe, it's possible the two gangs have sharpened their geographical focus on users in the US and Canada. We anticipate IcedID to remain one of the most prevalent financial malwares in 2019—especially in the North American region, which has been its traditional attack turf.

NEWCOMERS BACKSWAP AND DANABOT

Although neither is a prevalent threat yet, DanaBot and BackSwap's activity steadily increased in 2018. Third-party researchers discovered DanaBot in May 2018 targeting users in Australia via emails containing malicious URLs.[11] It evolved to targeting users in Poland in September 2018.[12] BackSwap emerged in March 2018 targeting Polish banks[13] and in August 2018 X-Force researchers found this malware targeting several major banks in Spain.[14]

BackSwap is most often delivered to users via malware spam, concealed in an attachment of a productivity file such as Microsoft Word, or bundled inside other programs. The limited number of targeted banks in each country in 2018 suggests BackSwap was in testing, and there could possibly be a wider scope of attack for this Trojan in 2019.

Emerging Threats

Emerging threats are those that have surfaced within the last couple of years and show no signs of slowing down.

EVADING DETECTION AND LIVING OFF THE LAND

Despite the prevalent use of financial malware to target bank accounts, the use of malicious software in attacks may be on the decline. Only 43 percent of attacks analyzed by X-Force IRIS in 2018 revealed threat actors who used file system-resident malware.

Making up for the drop in classic malware use, X-Force IRIS has been observing the widespread global use of PowerShell in cyber-attacks. PowerShell is a versatile tool that can execute code from memory and provide entry directly to a device's core. This includes unbounded access to Windows Application Programming Interfaces (APIs), full access to the Windows Management Instrumentation (WMI), and access to the .NET Framework.

PowerShell is useful in data collection and analysis, but it is also favored by malicious actors who use it to forego the file system and inject malicious code directly into memory, thus enhancing obfuscation, and often evading security controls designed to detect malware deployments.

Threat actors of all skill levels have expanded their capabilities using PowerShell over the last few years. IBM X-Force IRIS has seen cases wherein complete malicious toolkits were contained within PowerShell scripts. Attackers also used PowerShell to gather credentials, and then leveraged it to conduct network reconnaissance and data theft. The availability of PowerShell allowed them to "live off the land" and perform malicious actions such as injecting shellcode directly into memory.

Even coin-mining malware is jumping on the PowerShell bandwagon. GhostMiner is the first-known file-less mining malware discovered. It uses PowerShell evasion scripts that allow it to run from memory without leaving any files on the victim's device.[15] It contains advanced process-killing functions, executed via PowerShell, to detect and eliminate other coin-mining infections that may be present on the same device, so it can maintain exclusive access to system processing power. On top of the more common devices, GhostMiner can infect systems running MSSQL, phpMyAdmin, and Oracle WebLogic servers.

X-Force IRIS anticipates that in 2019 threat actors will continue to leverage PowerShell to compromise networks. Scripting their way in, we expect to see the the use of PowerShell obfuscation to evade AV detection and running code directly in memory to avoid evolving security controls in endpoint detection solutions.

With PowerShell taking on a larger role in adversarial toolsets, its use and abuse is reminiscent of the risk that arose when attackers started relying on JavaScript.

It's therefore important for organizations to inspect for issues that go beyond the file system and to conduct active threat assessments that look at PowerShell differently. They should seek relevant IoCs to detect current and historical threats across the enterprise.

A NEW DAWN FOR COIN-MINING MALWARE?

Cybercriminals are always seeking new methods of financial gain. Over the last several years, ransomware has become a popular choice for cyber-attack. However, criminals are increasingly leveraging coin-mining malware[16] over ransomware,[17] installing miners on victim endpoints and enslaving them, thus slowly generating coins for the attacker.

Cybercriminals are also not ones to spend money on expensive hardware, nor do they legitimately mine cryptocurrency. Instead, they develop various tools and tactics that infect the hardware of both corporate servers and individual users by spreading cryptojacking malware to do the work for them.

Cybercriminals have the advantage in this exploding trend, as the two most common infection vectors are phishing as well as code that can be injected into web sites with weak security controls. A wide range of "out of the box" affiliate programs, open mining pools, and miner builders currently exist for free on the internet and are at an attacker's disposal. Additionally, attackers are increasing the sophistication of obfuscation capabilities for coin-mining malware,[18] giving attackers the ability to infect more devices and web resources to collect coins over time.

Spreading to every part of the globe, financially motivated threat actors in Eastern Europe and North Korea have taken special notice of the profitability of coin-mining malware since consumers in these regions have adopted the use of cryptocurrency as a regular payment method for everyday transactions.[19]

With the growing proliferation of cryptocurrencies and virtual tokens in many countries—and especially in developing economies[20]—several nations including Georgia, Belarus, and Poland, have introduced or adopted legislation that both recognizes cryptocurrency and regulates crypto-mining.[21,22,23] Indeed, the low-cost of energy in some Eastern European nations significantly reduces the cost of mining, making crypto-mining a lucrative business opportunity for residents—and in some cases a means for inviting foreign investment.[24,25] Unfortunately, this profitable model also attracts more cybercriminal factions to illegally mine coins, riding on the hardware and mining efforts of legitimate users.

Facing continued international sanctions over its nuclear program, North Korea in 2018 continued focusing on cryptocurrency mining as part of its revenue generation tactics. Early in 2018, North Korea[26] was seen mining the privacy-conscious cryptocurrency Monero and having it sent to a university in North Korea. The campaign did not last very long, likely because the value of Monero was relatively low at the time.[27]

While North Korea may continue its foray into crypto-mining, most of its activities involve the direct compromises of cryptocurrency exchange platforms. Reports indicate just five attacks attributed to the Lazarus group have netted North Korea over $571 million in stolen crypto-coins.[28]

ATM ATTACKS

The risk of compromise of Automated Teller Machines (ATMs) has seen an increase in 2018, as both financially-motivated criminals and state-sponsored groups actively exploited various ATM vulnerabilities.

Threats targeting ATMs triggered numerous US law enforcement alerts such as:

- **January 2018:** The US Secret Service places alerts on ATM "Jackpotting" attacks wherein adversaries with physical access to ATMs plant malware to dispense cash on demand.[29]

- **August 2018:** The FBI places alerts on "cash-out attack," wherein attackers use malware to compromise a bank or payment card processor's networks, steal mass-amounts of card data then produce cloned payment cards that can withdraw money from numerous ATMs around the globe in a coordinated operation. In this attack, known as an "Unlimited Operation," the attackers can disable fraud controls on a card's account, eliminating withdrawal limits on the ATM for larger-scale thefts.[30]

- **September 2018:** An alert notes an uptick in skimming attacks, also known as ATM Wiretapping or Eavesdropping. Criminals drill physical holes into ATMs and use a combination of magnets and medical devices to install cameras on ATM PIN pads. Using these makeshift skimming devices, they steal magnetic card data and the victim's PIN. They then empty their accounts at ATMs.[31]

- **October 2018:** A joint FBI/DHS alert suggests a North Korean state-sponsored group known as HIDDEN COBRA (or LAZARUS) has been targeting ATMs in Asia and Africa since 2016. The campaign is titled FASTCash and relies on the compromise of switch application servers at the bank. It intercepts financial messages and replies with a fraudulent response that enables unauthorized withdrawals.[32] It has stolen millions of dollars in the process.[33]

Globally, from 2017 to 2018, X-Force Red, an autonomous team of veteran hackers within IBM Security, reports a 300 percent increase in the annual number of banks requesting ATM testing, including both software and hardware tests.

Interest in this type of testing in the ASEAN region, which includes Vietnam, Cambodia, Thailand, and India, has been particularly high, likely due to major ATM attacks monetized in the region.

While further reports and evidence are still pending, banks in these countries were some of the most targeted ATM operators on a global scale, especially by state-sponsored threat groups.[34,35,36]

Considering the multiple government and law enforcement alerts on large-scale, and the oftentimes coordinated ATM attacks, requests for this type of testing is likely to continue rising.

Part 2

Most Frequently Targeted Industries

In previous years' X-Force Index reports, the most frequently targeted industries have been determined based on attack and security incident data from a representative set of X-Force sensors in each industry. This year's report not only takes into consideration these sensors to determine the most frequently targeted industries, but also includes data and insights derived from incident response services and publicly disclosed incidents.

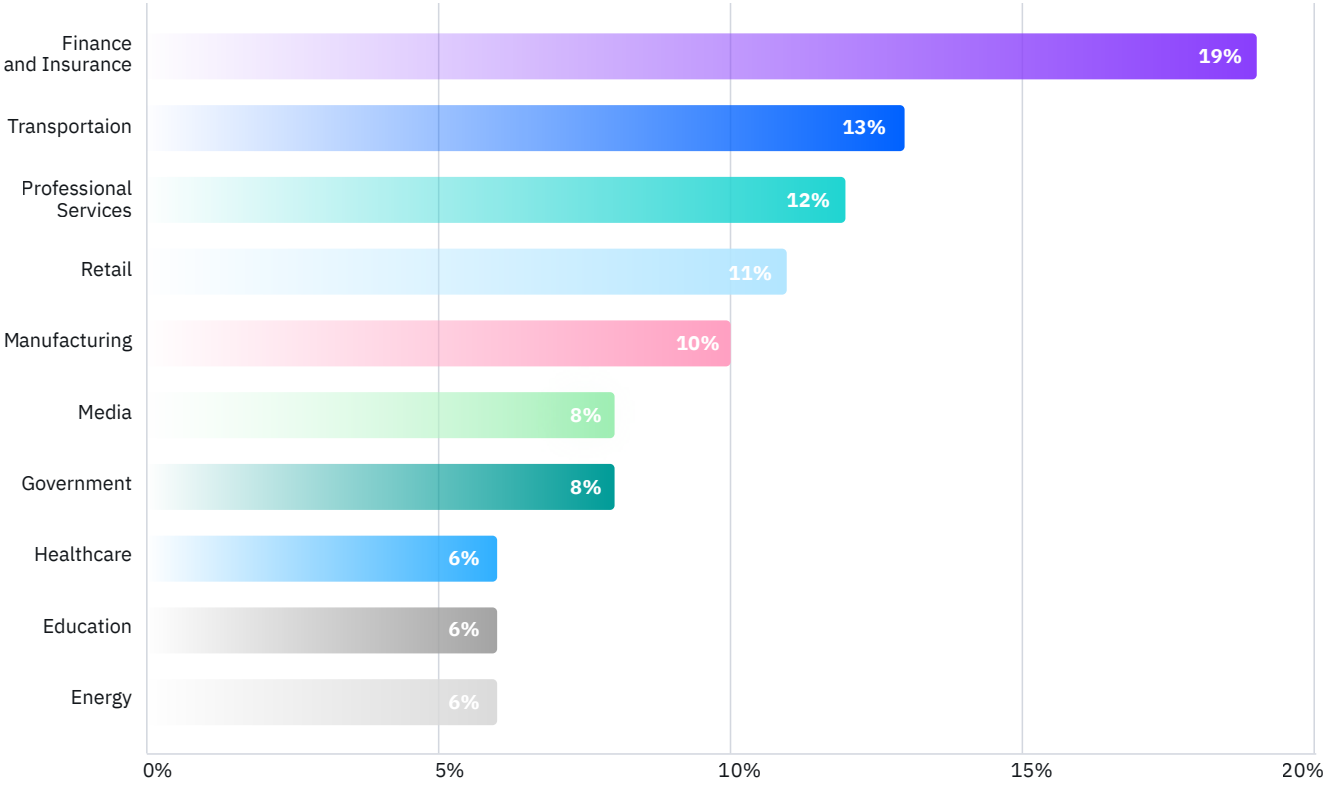
To compile the list, we ranked each category or data set individually. We then combined the rankings to arrive at a combination ranking. This combination of data sets offers a more holistic representation of the top targeted sectors, presenting attacks on monitored networks, data from actual breaches we have investigated, and data from publicly disclosed breaches.

In this year's report, we also expanded the list to include the top-ten targeted industries to provide a more complete picture of the threat landscape.

Figure 5

Most Frequently Targeted Industries in 2018

Source: IBM X-Force



1: Finance and Insurance | 19%

According to X-Force data analysis, the finance and insurance sector has been the most-attacked industry for three years in a row, with 19 percent of total attacks and incidents in 2018.

Fortunately, many organizations in this industry are cognizant of their vulnerability to cyber-attacks and are actively preparing for a potential crisis. Roughly one-third of participating organizations experiencing an immersive cyber incident simulation at the X-Force Command Cyber Range were in the financial services sector.

The allure financial services presents to a cybercriminal is clear: customer bank account information or payment card data can be monetized rapidly. Access to bank networks and switches for shifting large sums of money into criminal-controlled accounts, or robbing customer or employee Personally Identifiable Information (PII) can all lead to direct financial profit or be sold on the dark web.

Financially-motivated threat actors pose the most significant threat to the financial services industry, with threats from nation state groups in this sector, increasing over the past three years and resulting in the direct theft of millions of dollars from banks around the globe.[37]

2: Transportation Services | 13%

The second most targeted sector, transportation services, includes airlines, bus & rail, and water transportation services, ranked second in 2018, and experienced 13 percent of total attacks and incidents.

This sector, part of any country's critical infrastructure, is an attractive target for malicious threat actors. From financially motivated attackers seeking payment card information, PII, and loyalty-reward accounts to state-sponsored, advanced persistent threat (APT) groups aiming to disrupt the economy or target intellectual property data, attacks on the sector are on the rise.

The transportation industry's extensive reliance on information technology to facilitate operations and its use of third-party vendors, presents an extended attack surface for various types of threat actors that either seek access to targeted data or aim to cause disruption.

In the aviation industry, for instance, airplane manufacturers' accelerated adoption of information technology into aircraft and aviation systems that inevitably interact with legacy technology, may create targets of opportunity for threat actors. Vulnerable areas of the aviation industry include critical systems that facilitate ground-to-air satellite communications, navigation, radar, air traffic control, and other operations and efficiencies that rely on such hybrid systems, both in software and hardware.

The global scope and integration of the transportation industry supply chain exponentially increases potential vectors for malicious actors to gain access to proprietary data, or critical transportation systems, as well as targeting of industrial IoT systems (IIoT).

The compromise or damage to any segment of the transportation industry can have severe cascading effects upon multiple businesses and millions of travelers all over the world.

3: Professional Services | 12%

The professional services sector—made up of companies that provide specialized consulting services, such as legal, accounting, and architecture firms—have come under increased risk for cyber-attack over the past several years.

Malicious actors have discovered the value of the information these companies process and house. Combined with their smaller security budgets, limited security staff, and a relatively immature security posture (in most cases), this sector is as vulnerable as it is lucrative.

As the third-most targeted industry, this sector experienced 12 percent of all attacks and incidents.

The 2018 IBM-sponsored Ponemon Cost of a Data Breach study found the services industry was the second-most likely industry to suffer a data breach, and that a data breach in this sector could typically cost a firm $181 per breached record—$33 higher than average cost per record for all industries combined.[38]

4: Retail | 11%

As the fourth-most targeted industry, retail experienced 11 percent of the total attacks and incidents in 2018. Retail companies sell products to consumers and businesses—from automobiles and apparel, to electronics, food, and furniture.

More importantly, this sector works in hybrid mode: Services are extended to customers both onsite and over the internet, making for a decentralized and heterogenous operational environment. Retailers are attacked with Point-of-Sale (PoS) malware, skimming, and counterfeit card heists. They also experience sophisticated attacks on their web applications and service portals by fraudsters and organized cybercriminals.

Additionally, the proliferation of mobile apps used for retail shopping and the mobile devices used in retail stores are emergent gateways for attackers. Merchants lose $3.29 per dollar to fraud, a 24 percent increase over 2017.[39] Rising rates of card-not-present (CNP) fraud are forcing retailers to reassess their vulnerability to new and sophisticated threats.

Attackers have many reasons to infiltrate retailers' company networks: They look for sensitive and confidential information such as payment card data, customer PII, and supply-chain contacts. With a variety of malicious actors targeting this sector, attacks have become ever-more damaging, and a breach of a major US retailer disclosed in March 2018 resulted in the loss of the personal information for approximately 150 million customers of its diet and fitness mobile app.[40] According to 2018 Ponemon Cost of a Data Breach study, a breach on this scale is considered a mega-breach, and it could cost the victim another $350 million (on average) to remedy.[41]

5: Manufacturing | 10%

The fifth-most targeted industry is manufacturing, which includes companies that make a wide variety of goods, from chemicals and machinery to transportation equipment and electronics, and Internet-of-Things (IoT) devices. It experienced 10 percent of the total attacks and incidents.

The 2018 IBM-sponsored Ponemon study on the cost of data breaches found industrial manufacturing was also the third-most likely sector to experience a data breach.[42] As the majority of cyber incidents in the manufacturing sector do not involve customer information that is subject to legal disclosure regulations, the percentage of publicly disclosed events in this industry is low when compared with other sectors. The numbers are therefore likely to be higher than those reported.

Most attacks on manufacturing companies appear to target intellectual property (IP) and trade secrets. Confidential business communications, such as executives' email correspondence or company bank accounts are particularly lucrative targets for cybercriminals, nation-state groups, and even paid hackers hired by a competitor. This sector also absorbs many BEC attacks since manufacturers often wire substantial amounts of money to countries in Asia, Africa, and other developing regions.

While only a handful of incidents in the manufacturing sector have included attacks on industrial control systems or infrastructure, future trigger events or new attack tactics may lead to damage to physical infrastructure—and potentially human lives. At a time when organizations feel outmatched by nation-state hackers,[43] the manufacturing sector must rethink the security of its operational zones and its preparedness to respond to potential attacks of this nature.

6: Media | 8%

The media sector, the sixth-most targeted industry, includes companies that produce, process, or distribute information and entertainment content. It also includes sub-industries, such as computer software and telecommunications, among others.[44]

This industry made up eight percent of the total attacks and incidents. The media sector also experienced the most publicly disclosed incidents, at 40 percent in 2018. Half of these publicly disclosed media incidents involved misconfiguration of systems or cloud servers, rather than premeditated attacks.

7: Government | 8%

The seventh-most targeted industry is government, and it experienced eight percent of the total attacks and incidents. X-Force researchers assess nation-state-backed groups are those most likely to target this sector.

Depending on the type of objective the attack has, nation-state sponsored groups that breach government resources may use, sell, or deliver compromised information to their respective governments, typically for economic or political gain. Many times, these attacks are after top-secret intellectual property. In other attacks, stolen data is used in espionage for the establishment of surveillance operations.

In 2018, X-Force notes high-profile incidents that targeted American government institutions in search of IP and PII from military bodies. The first incident involved the compromise of a US Air Force captain's computer to steal sensitive information about military drones.[45] In the second incident, attackers targeted the US Department of Defense, capturing information on 30,000 US government employees who report to the Pentagon. The data was breached via a system that maintained employee travel records operated by a third-party vendor.[46]

8: Healthcare | 6%

Cybersecurity in the eighth-most targeted industry, healthcare, guards not only protected health information (PHI) and payment card data, but critical systems and devices that—for some patients—can mean the difference between life and death.

The 2018 Ponemon Cost of a Data Breach study reveals the healthcare industry has the highest cost per record breached in a cyber incident, at $408. This cost is nearly twice the amount of the next-highest industry—financial services—at $206 per record breached, and far above the grand average of $148.

While credit cards and even personal identification numbers can be changed, a medical history cannot be modified. Once breached, thieves can use this information to set up new identities, bank accounts, credit and loans, obtain medication in a victim's name, undergo surgery in someone else's name, and even file insurance claims using stolen information.

According to X-Force researchers, most of the evidence from cases wherein stolen healthcare data was used, suggests financially-motivated cybercriminals are the primary attackers of the healthcare industry. By infecting employee devices and breaching networks, they aim to steal then sell medical records on the dark web or encrypt devices, and then hold them for ransom—knowing ongoing operations will probably suffer a critical outage that will force organizations to react, and often pay up.

9: Education | 6%

The education industry, the ninth-most targeted industry, is attractive to attackers due to the sensitive—and lucrative—nature of some emerging research projects, as well as the wealth of PII on students, faculty staff, and organizations associated with universities and schools.

X-Force researchers assess nation-state sponsored threat actors are those most likely to breach university networks, based on their motivation for attacking this sector, and their capability for doing so. Moreover, educational institutions do not typically boast a large in-house security team and may not have many security controls in place. They also control a large network of users who can easily bring in malware from personal devices or email.

Aside from nation-states, educational institutions may be targeted by financial criminals looking to take over bursary accounts and student identities. Another relevant threat are hacktivists looking to champion a cause by holding an institute for ransom or threatening to release stolen data.

10: Energy | 6%

Organizations in the energy sector are a prime target for cyber-attacks. To begin, they are the backbone of every country's critical infrastructure. Energy is central to the economic, national security, and day-to-day function of cities and industries.

Threat actors targeting this sector are most often deployed by hostile nation-states. Destructive Shamoon attacks affecting oil and gas organizations in Saudi Arabia and the United Arab Emirates (UAE) resurfaced in December 2018, highlighting the vulnerability of this industry and the detrimental effect of outages on operations and revenue.[47] First emerging in 2012 and later in 2016 targeting oil and gas industry, Shamoon is a wiper malware designed to destroy computer hard drives by wiping the master boot record (MBR), making data irretrievable. Unlike ransomware, which holds the data hostage for a fee, Shamoon attacks cannot be reversed for a payment.[48]

Financially motivated cybercriminals may also attack energy companies if they believe they can monetize the attack quickly by stealing sensitive information and selling it to a competitor, or by targeting the company's bank accounts.

Hacktivists with an environmental agenda or others attempting to make a political statement of some kind have also been part of the landscape of threat actors who attack the energy sector. They are likely to do so again.

An attack on the energy sector has a greater potential for subsequent outage and cascading effects on additional sectors when compared with attacks on other industries, since every enterprise, government, and military operation tends to rely on energy for its everyday function.

Part 3

Growing Attack Surface and Rising Risk

140K Vulnerabilities and Counting

IBM X-Force Red tracks the public disclosures of vulnerabilities in software products, analyzing hundreds of sources where vulnerabilities and known exploits are disclosed. Currently, there are more than 140,000 vulnerabilities recorded.

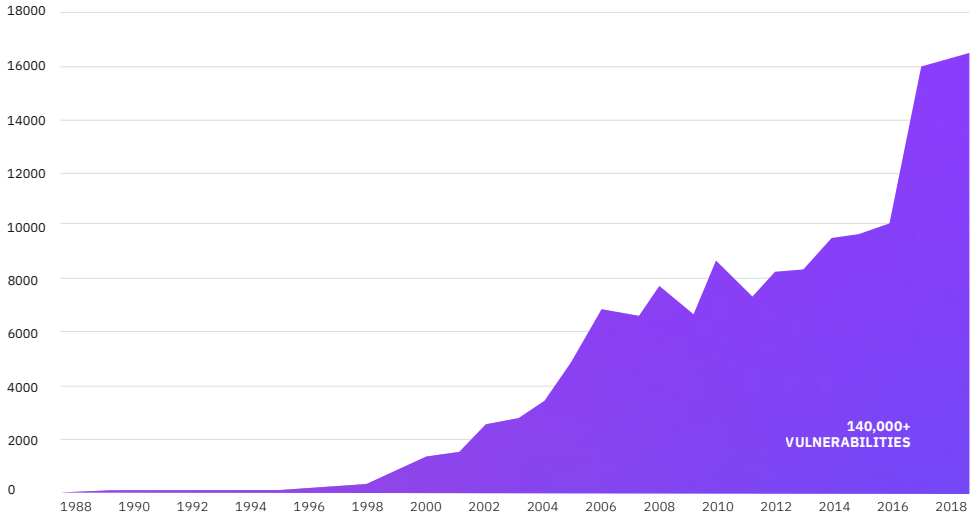
Over the last several years, there has been a significant increase in the number of vulnerabilities disclosed globally and the rate at which they are being reported. In fact, nearly one-third (30 percent) of all vulnerabilities documented by X-Force researchers and disclosed in the last three decades have been reported in the past three years alone, accounting for more than 42,000 vulnerabilities.

This exponential growth in flaws and vulnerabilities is a product of the ever-expanding attack surface as new players such as IoT devices, and other smart technologies enter the fray. This growth adds to existing vulnerabilities among different platforms, such as web applications that make up nearly one-quarter of the total number of vulnerabilities recorded in 2018.

Figure 6:

Total Recorded Vulnerabilities Year Over Year

Source: X-Force Red Vulnerability Database



How does the immense attack surface translate to the impact it has on individual organizations? While enterprises are not vulnerable to every threat, the number of applicable threats is still daunting.

The X-Force Red team is hired to break into organizations and uncover risky vulnerabilities that criminal attackers use for personal gain. In 2018, IBM X-Force Red's Vulnerability Management Services identified an average of 1,440 unique vulnerabilities, per organization.

Unpatched vulnerabilities are an attackers' gateway into organizational networks and devices. When there are exploits freely available on the internet, even the more novice attackers can attempt—and successfully breach critical assets.

Internet of Things and Industrial Internet of Things

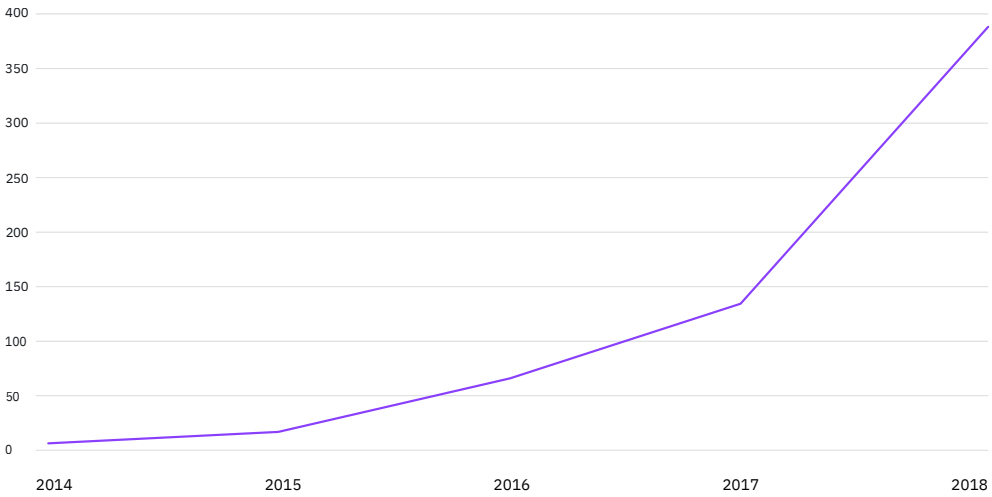
It's predicted nearly 13 billion IoT sensors and devices will be in use in the consumer segment by 2020.[49] These devices have already had a significant impact on the IoT vulnerability landscape.

In 2018, there was a 5,400 percent increase in the number of IoT vulnerabilities recorded over the number reported just five years earlier.

Figure 7:

Number of IoT Vulnerabilities Since 2014

Source: X-Force Red Vulnerability Database



IoT vulnerabilities have increased 5400% over the last five years

Flaws and security holes in IoT devices leave organizations and consumers vulnerable to large botnets of internet-connected "things." In 2016, the Mirai botnet (which caused internet-wide disruption) was the first major wake-up call for organizations to acknowledge this type of threat.[50] Since then, Mirai successors such as Aidra, Wifatch, and Gafgyt, which leverage parts of Mirai's code,[51] and newcomers such as the BCMUPnP_Hunter[52] and Torii[53] botnets have amassed access to hundreds of thousands of devices to spread their Distributed Denial of Service (DDoS) attack malware, coin-mining malware, and spam.

After the wide-spread attacks that featured IoT devices in the past three years, we anticipate attackers will continue to target consumer devices, such as routers, CCTV cameras, and IIoT-connected devices such as smart meters and grids to carry out attacks in 2019 and beyond.

Attackers will bank on some manufacturers' forgoing security-by-design as they rush products to market. Attackers make those products their favorite go-to targets where they can exploit large numbers of devices with the same vulnerabilities. Attackers are also likely to continue exploiting administrators' failure to change default passwords and patch vulnerable devices unless these security basics are prioritized by more organizations in the coming year.

The growing adoption of Smart City technologies such as intelligent transportation systems, disaster management, and the IIoT is also contributing to the growth of an exploitable "smart" attack surface.[54] IBM X-Force Red and ThreatCare researchers found 17 zero-day vulnerabilities in these commonly-used technologies in 2018, as reported in The Dangers of Smart City Hacking whitepaper.

Billions of Records and Hundreds of Gigabytes

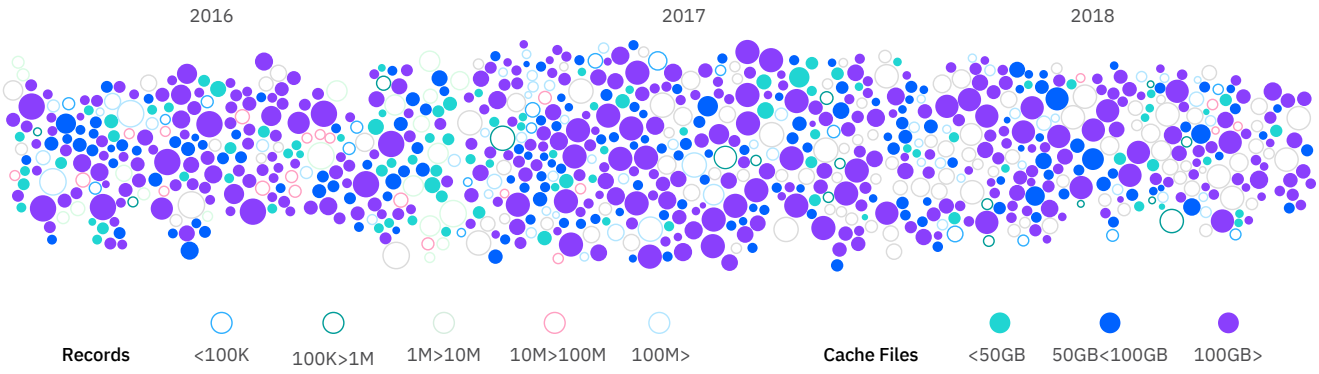
X-Force has been tracking and reporting publicly disclosed security incidents and data breaches since 2011. Figure 8 illustrates a sampling of security incidents reported during 2016, 2017 and 2018.

Over the last three years, more than 11.7 billion records and over 11 Terabytes of data were leaked or stolen in publicly disclosed incidents. To put the enormity of terabytes in perspective, 11 terabytes is the equivalent of nearly five billion single-spaced typewritten pages.[55]

Figure 8:

Sampling of the Impact Security Incidents by Records and Cache Files Compromised, Time and Impact, 2016 through 2018

Source: IBM X-Force



Size of circles estimates relative impact of incident in terms of cost to business, based on publicly disclosed information regarding leaked records and financial losses.

These compromised records and caches of data contained PII, such as social security numbers, addresses, phone numbers, banking/payment card information, or passport data. In some cases, the attack exposed Personal Health Information (PHI), which may include PII as well as medical information such as test and laboratory results as well as medical insurance information. In some cases, stolen data can include an organization's entire digital footprint.

Nation-state supported espionage groups and cybercriminals are typically the sort of threat actor that pursues PII and PHI of users, customers, and/or employees. Nation-state sponsored espionage groups seek out this type of data in their country's ongoing effort to build comprehensive databases of identities they plan to surveil or illegally use. Stolen PHI can allow hostile nations to better understand intelligence targets and the potential vulnerabilities of nationals living abroad.

On the financially-motivated side, cybercriminals often combine phishing and commodity malware to gain access to key PII databases. In addition, lesser skilled cybercriminals and factions are known to search for poorly-secured databases that may be vulnerable to SQL injection attacks, and then use automated attack tools to compromise them. Primarily, cybercriminals seek PHI to monetize troves of PII information often contained within the PHI records, usually for financial fraud and identity-theft scenarios.

The Paradigm Shift: Major Hardware Vulnerabilities

Addressing the broad attack surface presented by the ever expanding domain of software and connected devices, and protecting customer and employee data, are not the only challenges facing businesses and their security teams.

2018 ushered in a new era of hardware security challenges that forced enterprises and the security community to rethink the way they approach hardware security. Researchers disclosed several variants of the same fundamental underlying vulnerability that affects nearly every computer chip manufactured in the past 20 years. Dubbed Spectre (CVE-2017-5753)[56] and CVE-2017-5715)[57] and Meltdown (CVE-2017-5754),[58] these vulnerabilities can allow an attacker to gain unauthorized access to confidential data in protected memory using a side-channel attack.

These vulnerabilities present a growing number of exploitation possibilities and sub-vulnerabilities that continue to emerge over time. The domain of hardware vulnerabilities is not new, but its emergence in severe potential attack scenarios has raised it to top of mind for many organizations needing to update equipment and patch hardware on critical production assets.

Millions of Malicious Domains Blocked

The expanding attack surface also includes the internet's surface, and therefore a never-ending stream of malicious domains, making safe internet browsing an ever more challenging task to achieve.

Quad9, a freely available Domain Name Server (DNS) service created and sponsored by a collaboration between IBM, Packet Clearing House (PCH), and Global Cyber Alliance (GCA), blocks an average of ten million DNS requests to malicious sites daily.[59]

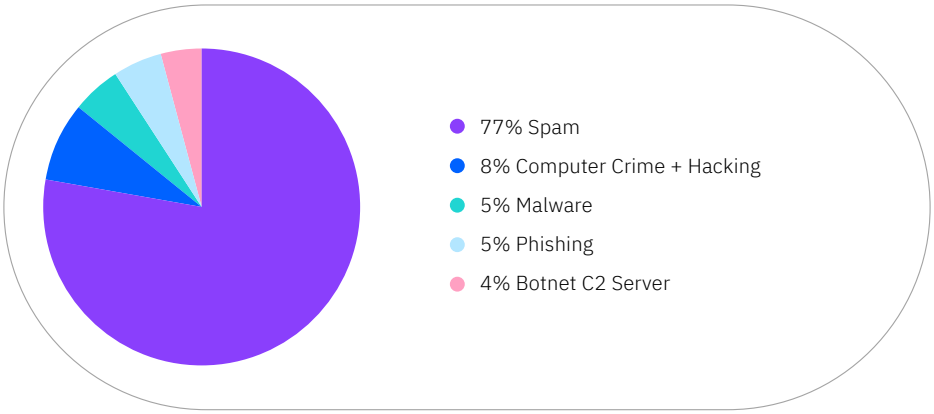
As part of this collaborative effort to make the internet a safer place, IBM provides a list of malicious domains to Quad9 and receives back privacy-filtered counts of DNS lookup events correlated to those domains.

The chart below shows the distributions of malicious domain types recorded by IBM Security in 2018.

Figure 9:

Malicious Domain Categories Blocked by Quad9

Source: Quad9 blocked categories as correlated with IBM Security threat intelligence



According to a sampling of Quad9 data correlated with IBM Security threat intelligence, more than 77 percent of the malicious DNS requests on Quad9 solicited users to access them via spam emails. This is not a surprise, as spam is still one of the most effective ways to reach internet users, spread scams and malware, and infect users with ransomware. For instance, a spam email can lead users to an infection zone where they are tricked to click a link or to open an attachment that eventually gets the user to download and run a malicious file with ransomware inside.

More than eight percent of access requests made by users to malicious URLs lead to phishing domains where hackers host fake websites that steal user credentials, credit card numbers and other information they can monetize. Another five percent of the malicious DNS requests lead to C&C domains where botnets use them to establish communication channels to either exfiltrate confidential data or detonate attacks. Nearly four percent were DNS requests to domains that distribute malware. Such programs can help attackers compromise users or a network remotely to exfiltrate data or move laterally within the network to achieve other objectives.

More than 77 percent of the malicious URLs blocked by Quad9 solicited users to access them via spam emails

While spam, malware, and phishing sites are visited by unwitting users duped by unsolicited email, the sites in the hacking category may be accessed by cyber-criminals who operate malware control hubs or access underground forums where information about hacking, fraud, and other crime is readily available. However, there can also be legitimate reasons for accessing these sites, as security professionals may visit them while conducting research.

Part 4

Two Sides of the Same Coin: Mitigating Threats and Increasing Preparedness for a Breach

Organizations with a mature security posture don't just take a proactive approach to mitigating threats, they also train their staff for worst-case scenarios. To do that, they plan and then continuously review their Incident Response Plans (IRP) to understand the impact of a potential breach from a remediation perspective.

Taking Proactive Measures

We have covered our findings from the ever-evolving threat landscape, but knowing what to expect is only half the battle. Being prepared to respond is what can win that battle, or at the very least minimize impact.

The expanding attack surface offers attackers a myriad of opportunities that target organizations. While attackers need only be successful once, there are several proactive measures for defenders that companies can take to mitigate threats—both the emerging and the relentless types:

- **Financially motivated cybercriminals and nation-state groups target a wide range of industries.** Integrate threat intelligence into institutional risk management models to consider likely threat actors, infection methods, and potential impact to critical business processes. By mapping out and understanding likely adversaries, your organization can better evaluate the risk for direct impact and collateral damage. In addition, threat intelligence can inform the organization's risk assessment process and help prioritize the hardening of assets by identifying threat sources and threat events with up-to-date information about threat group TTPs.

- **Attackers are targeting users of cloud services and misconfigured cloud servers are exposing customer and employee data.** Organizations should check and monitor settings on cloud service architecture—do not maintain default settings. Vet third-party cloud vendors for high security standards before choosing to do business with them. Ensure you are aware of who controls each component of your cloud infrastructure and define policies for where and how security measures are deployed. Implement the same security policies you would employ for classic IT infrastructure.

- **Exploitation of an organization's supply chain or third-party relationships can allow attackers to gain access to their primary targets.** Numerous industries, such as Transportation and Manufacturing, are particularly vulnerable to this type of attack. To mitigate this threat, organizations can vet third parties for high security standards before choosing to do business with them. Continuous monitoring of supply-chain vendors for compliance with security requirements is also important as is encrypting communications.

REMEDIATION

Even organizations with a mature security posture and robust mitigation practices and solutions in place may be susceptible to a cyber incident. Knowing how to remediate after responding to a cyber-attack and shutting down the source of the compromise is a crucial piece of the recovery process: It can impact how quickly normal business operations resume. The remediation process is both a technical and non-technical process—it also can be an emotional one.

At the onset of a crisis, teams typically work 24/7 until they can recover critical areas of the business and get most processes back online according to a predetermined business continuity plan, disaster recovery plan, and business priorities at the time of the incident.

It is imperative that team leaders make sure people are well-rested and well-fed during the crisis phase to allow them to function well under pressure as they continue to make strides toward the recovery of business functions and advance their investigation. Mistakes can happen when people become overly tired and this is often overlooked during lengthy emergency situations. It can be beneficial to have arrangements for sleeping on site and food delivery codified into the IRP.

Remediation is also not a time for standard project management. This is a time of crisis and decisions need to be made more quickly and with less time spent on group agreement. To this end, a lead person should be designated to be responsible for making key decisions.

Knowing how to remediate after responding to a cyber-attack and shutting down the source of the compromise is a crucial piece of the recovery process

Once the crisis has subdued and business-as-usual has resumed, however, “lessons learned” discussions should begin to take place and be documented.

Questions such as “How can we bolster our IRP to make it easier to perform under pressure?” must be asked. Other vital questions include: “Is there an opportunity to incorporate threat intelligence into other areas of the business?”, “Have we adequately defined all of our crown jewels?” or, “Is more segmentation needed to isolate certain areas of the network?”

What Does 2019 Have In Store?

An organization caught unprepared during a cyber incident stands to lose millions of dollars to response and remediation, as well as numerous other breach expenses.[60] Organizations prepared to face an attack will be in a better position in 2019 to protect their critical assets from cyberthreats.

Now that we're in the GDPR era, the need to address this significant regulation could exacerbate the problem of protecting the expanding attack surface. For instance, European organizations will need to go through work councils to receive approval to deploy endpoint protection tools in the wake of a cyber incident, because of privacy regulations. This can give attackers a significant advantage to harvest data for an extensive amount of time—upward of 30 to 90 days.

Unpatched vulnerabilities will continue to be exploited by attackers. Manual penetration testing should be performed in addition to automated scanning. Whereas automated tools can find known vulnerabilities, manual testing finds the unknown vulnerabilities that tools alone cannot find.

Going beyond penetration testing, organizations with a more mature security program should test and drill their blue teams in red team engagements and find out how they can handle an advanced adversarial attack when they encounter one in real life.

Phishing and malware will also continue to be relentless threats, leveraged by both cybercriminals and APT actors that require organizations to address the inadvertent actor risk. Routinely providing employee education and test campaigns with updated phishing techniques used by attackers can help mitigate these threats.

In 2019, it is crucial that organizations make a concerted effort to assess their ability to respond to an incident efficiently by participating in simulated cyber-attacks. These exercises can help organizations identify gaps in their processes, which can potentially be addressed prior to an attack.

Preparing for response should include a designated IR team, preferably one that's composed of participants from different departments. Organizations that have an in-house IR team responded to attacks faster and better and saved considerable costs in the process. The average cost savings with an Incident Response team was $14 per record. In a breach like one that impacted a major hotel late last year, that would be multiplied by 500 million records.[61]

To begin, the team could work with tabletop exercises and runbooks, but it is most helpful to regularly drill the response flow and strive to improve its results on every subsequent drill.

To continuously innovate and renovate the IRP, teams can join discussion groups and share successful practices with other teams to continually sharpen IR plans and reduce the potential damage from an impending attack.

Contributors

Chenta Lee
Andrey Iesiev
Mark Usher
Dirk Harz
Martin Steigemann
Marc Noske
Abby Ross
Scott Moore
Limor Kessem
Tomer Agayev
Claire Zaboeva
Camille Singleton
Dave McMillen
Dave Bales
Joshua Chung
Michelle Alvarez

About X-Force

IBM X-Force studies and monitors the latest threat trends, advising customers and the general public about emerging and critical threats, and delivering security content to help protect IBM customers. From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your critical assets. IBM Security protects some of the most sophisticated networks in the world and employs some of the best minds in the business.

References

1. www.forbes.com/sites/forbestechcouncil/2018/07/05/four-trends-in-cloud-computing-cios-should-prepare-for-in-2019/#6327136d4dc2
2. securityintelligence.com/are-ransomware-attacks-rising-or-falling
3. www.helpnetsecurity.com/2018/12/19/coinmining-malware-surge/
4. www.bankinfosecurity.com/fbi-alert-reported-ceo-fraud-losses-hit-125-billion-a-11206
5. Neelum Khan, "New Report Spotlights Misconfigurations as the Biggest Threat to Cloud Security," Netskope, September 20, 2018, https://www.netskope.com/blog/new-report-spotlights-misconfigurations-as-the-biggest-threat-to-cloud-security.
6. www.wired.com/story/exactis-database-leak-340-million-records/
7. www.cyber.nj.gov/threat-profiles/trojan-variants/flawedammyy
8. exchange.xforce.ibmcloud.com/collection/Necurs-spreads-FlawedAmmyy-RAT-using-Excel-Internet-Query-attachments-c34ee7d56e1c32ab3592e47bae9f9f53
9. www.justice.gov/usao-sdny/pr/three-alleged-international-cyber-criminals-responsible-creating-and-distributing-virus
10. securityintelligence.com/news/banking-trojans-trickbot-and-iceid-partner-for-distribution-and-development/
11. www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
12. securityintelligence.com/news/danabots-anti-vm-update-shows-how-quickly-financial-cyberthreats-evolve/
13. www.cert.pl/en/news/single/backswap-malware-analysis/
14. securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/
15. www.techrepublic.com/article/ghostminer-fileless-cryptomining-malware-has-code-that-kills-itself-and-other-strains/
16. www.helpnetsecurity.com/2018/12/19/coinmining-malware-surge/
17. securityintelligence.com/are-ransomware-attacks-rising-or-falling/
18. www.ccn.com/malware-not-found-how-cryptojackers-employ-sophisticated-methods-to-avoid-detection/
19. www.statista.com/statistics/660158/consumers-by-country-using-crypto-currency-for-payments-europe/
20. medium.com/haloplatform/cryptocurrency-helps-developing-countries-3129811559a0
21. stat.gov.pl/metainformacje/interpretacje-klasyfikacji/interpretacje-informacje-o-zmianach/
22. cointelegraph.com/news/from-russia-to-macedonia-how-cryptocurrencies-are-regulated-in-eastern-europe
23. cointelegraph.com/news/belarus-signs-super-liberal-blockchain-support-legislation
24. venturebeat.com/2018/06/23/whats-behind-eastern-europes-crypto-boom/
25. bitcoinist.com/republic-georgia-emerges-global-leader-cryptocurrency-mining/
26. www.wsj.com/articles/in-north-korea-hackers-mine-cryptocurrency-abroad-1515420004
27. www.ccn.com/north-korea-appears-to-have-run-a-short-lived-bitcoin-mining-operation/
28. thenextweb.com/hardfork/2018/10/19/cryptocurrency-attack-report/
29. www.secretservice.gov/data/press/releases/2018/18-JAN/GPA_01-18_ATM_Jackpotting_Attack.pdf
30. krebsonsecurity.com/2018/08/fbi-warns-of-unlimited-atm-cashout-blitz/
31. krebsonsecurity.com/2018/09/secret-service-warns-of-surge-in-atm-wiretapping-attacks/
32. www.us-cert.gov/ncas/alerts/TA18-275A
33. www.theverge.com/2018/11/8/18075124/north-korea-lazarus-atm-fastcash-hack-millions-dollars-stolen
34. krebsonsecurity.com/2018/08/indian-bank-hit-in-13-5m-cyberheist-after-fbi-atm-cashout-warning/
35. www.bankinfosecurity.com/atm-heist-in-japan-a-9265
36. www.reuters.com/article/thailand-banking-theft/thailand-seeks-russian-over-350000-atm-cyber-heists-idUSL3N1BC2PE
37. www.reuters.com/article/us-northkorea-cybercrime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO
38. www.ibm.com/security/data-breach
39. chargebacks911.com/lexisnexis-true-cost-of-fraud/
40. www.nbcnews.com/tech/security/under-armour-says-data-hacked-150m-myfitnesspal-app-accounts-n861406
41. www.ibm.com/security/data-breach
42. www.ibm.com/security/data-breach
43. www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#548dafac1c78
44. www.hoovers.com/industry-facts.media.1450.html
45. www.cnn.com/2018/07/10/politics/us-reaper-drone-materials-hacker-theft/index.html
46. www.forbes.com/sites/leemathews/2018/10/14/department-of-defense-data-breach-exposes-30000-employees/#51c939451a6b
47. www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
48. securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/
49. www.forbes.com/sites/louiscolumbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/#62b7b2a23ecc
50. securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/
51. nakedsecurity.sophos.com/2018/11/23/mobile-and-iot-attacks-sophoslabs-2019-threat-report/
52. www.scmagazine.com/home/security-news/iot-botnet-bcmupnp_hunter-targets-routers-with-vulnerable-upnp-feature/
53. blog.avast.com/new-torii-botnet-threat-research
54. iiot-world.com/connected-industry/report-on-state-of-iiot-adoption-and-maturity-in-three-industries/
55. www.neatorama.com/2008/07/08/terabyte/
56. cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753
57. cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715
58. cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754
59. https://www.quad9.net/"Quad9 aggregates "noisy" block events created by automated bots, so the actual block volume may be four to 10 times higher."
60. newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses
61. www.consumer.ftc.gov/blog/2018/12/marriott-data-breach

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
February 2019

IBM **Security**