



# X-Force Threat Intelligence Index<sup>2020</sup>



Produced by IBM X-Force Incident Response and Intelligence Services (IRIS)

# Table of Contents

<b>Summary and Key Trends</b>	<b>4</b>
<b>Targeting and Initial Infection Vectors</b>	<b>6</b>
Explosive Growth in Operational Technology (OT) Infrastructure Targeting	6
Records Breached Grows Dramatically	8
Targeting of IoT Devices Includes Enterprise Realms	9
Phishing Tops Initial Access Vectors in 2019 Attacks	11
<b>Malware Trends</b>	<b>13</b>
Destructive Malware Attacks Dramatically Increase	13
Ransomware and Cryptominers Aggressive in 2019	15
Top Innovators in 2019 Malware Code Evolution	16
Banking Trojans and Ransomware – A Treacherous Matrimony That Keeps Getting Worse	19
<b>Spam and Phishing Trends</b>	<b>21</b>
2017 Vulnerabilities Continue to Star in 2019 Spam	21
Spam Botnets Hosted in the West, Impact Globally	23
Spam Victims by Geography	24
Blocked Malicious Domains Highlight Prevalence of Anonymization Services	25
Phishing Impersonated Tech Companies, Social Media	26
Top 10 Spoofed Brands	28

# Table of Contents

<b>Most Frequently Targeted Industries</b>	<b>29</b>
Finance and Insurance	30
Retail	31
Transportation	32
Media & Entertainment	33
Professional Services	34
Government	35
Education	36
Manufacturing	37
Energy	38
Healthcare	39
<b>Geo-Centric Insights</b>	<b>40</b>
North America	41
Asia	42
Europe	43
Middle East	44
South America	45
<b>Preparing for Resilience in 2020</b>	<b>46</b>
<b>Moving Forward with Key Takeaways</b>	<b>47</b>
<b>About X-Force</b>	<b>48</b>

## Summary and Key Trends

IBM Security develops intelligent enterprise security solutions and services to help your business build resilience today for the cybersecurity threats of tomorrow.

To update security professionals about the most relevant threats, IBM X-Force regularly releases 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, summarizing the year past in terms of the most prominent threats raised by our various research teams to provide security teams with information that can help better secure their organizations.

Data and insights presented in this report are derived from IBM Security managed security services, incident response services, penetration testing engagements, and vulnerability management services.

IBM X-Force research teams analyze data from hundreds of millions of protected endpoints and servers, along with data derived from non-customer assets such as spam sensors and honeynets. IBM Security Research also runs spam traps around the world and monitors tens of millions of spam and phishing attacks daily, analyzing billions of web pages and images to detect attack campaigns, fraudulent activity, and brand abuse, to better protect our customers and the connected world we live in.



## X-Force Incident Response and Intelligence Services (IRIS) compiled IBM Security software and security services analyses from the past year, which show that 2019 was a year of reemerging old threats being used in new ways.

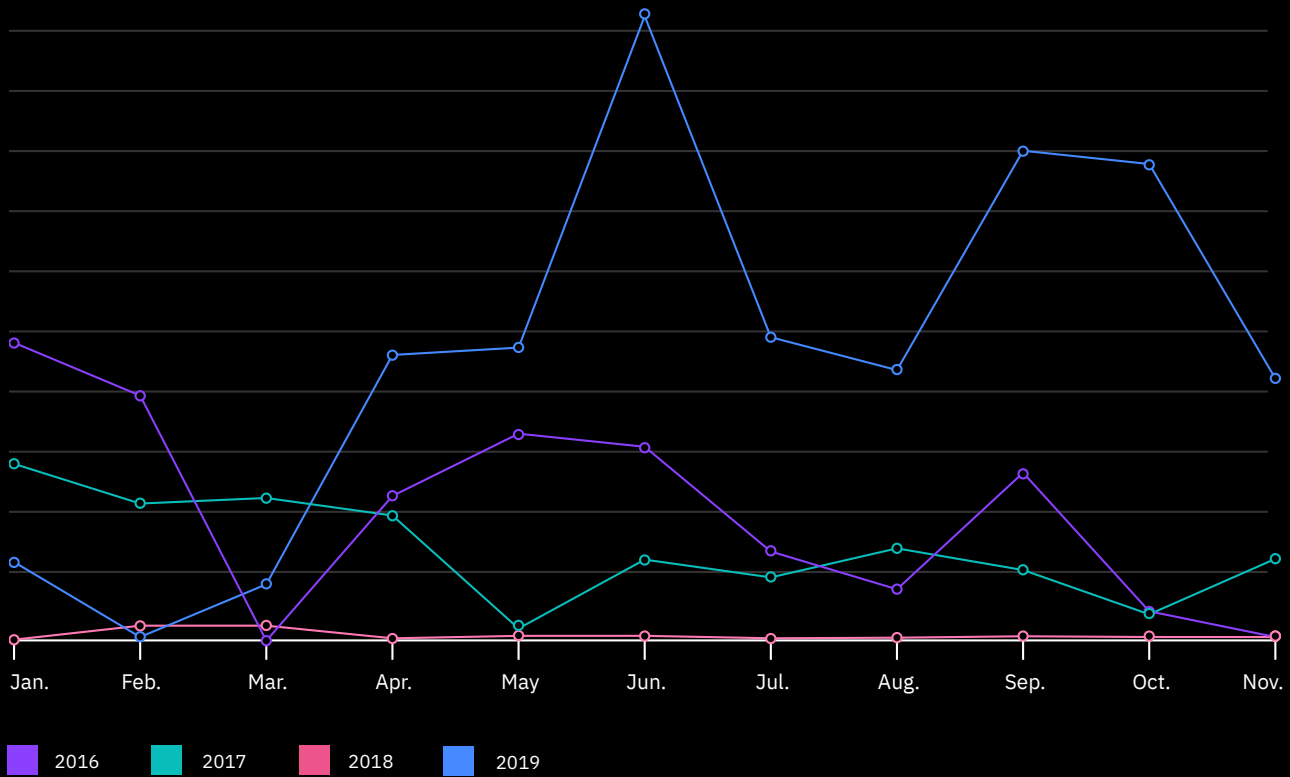
- According to X-Force data, a 2000 percent increase in operational technology (OT) targeting incidents in 2019 could portend the rising interest of threat actors to attack industrial systems as we move into 2020.
- Over 8.5 billion records were compromised in 2019, a number that's more than 200 percent greater than the number of records lost in 2018. The inadvertent insider can largely be held responsible for this significant rise. Records exposed due to misconfigured servers (including publicly accessible cloud storage, unsecured cloud databases, and improperly secured rsync backups, or open internet connected network area storage devices) accounted for 86 percent of the records compromised in 2019.
- The malware landscape shifted in 2019, with threat actors returning to ransomware and building out botnets. Throughout 2019, X-Force IRIS responded to ransomware engagements in 12 different countries in 5 different continents and across 13 different industries. Additionally, destructive malware activity shows that this potentially catastrophic malware trend continues to be a rising threat.
- The top three initial infection vectors seen in X-Force IRIS engagements in 2019 were a very close first, second, and third: Phishing (31 percent), Scan and Exploit (30 percent) and Stolen Credentials (29 percent). Phishing, most notably, went from making up nearly half of the total incidents in 2018 to less than a third in 2019. By contrast, the scanning and exploitation of vulnerabilities increased to nearly one-third of the incidents from only making up eight percent in 2018.
- X-Force analysis of global spam activity indicates that spam email continues to use a limited subset of vulnerabilities, with particular focus on just two CVEs: 2017-0199 and 2017-11882. Both of these are patched vulnerabilities that have accounted for nearly 90 percent of the vulnerabilities threat actors attempted to exploit via spam campaigns.
- Though Financial Services retained its top spot as the most targeted sector in 2019, industry-specific targeting highlighted shifting priorities for threat actors, with Retail, Media, Education, and Government all moving up on the global chart of the most targeted sectors.
- New to the X-Force Threat Intelligence Index this year are geo-centric insights, providing data on observed trends from around the world. IBM Security continues to track multiple threat actors targeting all geographies, and this report highlights key threat actors targeting each region, observed attacks from 2019, and potential dates of cybersecurity interest in 2020.

The following sections of this annual report go over the top-level trends and drill down to information on what shaped them in 2019.

# Targeting and Initial Infection Vectors

**Figure 1:**  
Operational technology (OT) attack trends

Monthly OT attack volume, comparing the years 2016-2019 (Source: IBM X-Force)



## Explosive Growth in Operational Technology (OT) Infrastructure Targeting

IBM X-Force data indicates that events in which threat actors targeted Industrial Control Systems (ICS) and similar Operational Technology (OT) assets increased over 2000 percent since 2018. In fact, the number of events targeting OT assets in 2019 was greater than the activity volume observed in the past three years.

Most of the observed attacks were centered around using a combination of known vulnerabilities within SCADA and ICS hardware components, as well as password-spraying attacks using brute force login tactics against ICS targets.

Some reported activity focused on ICS attacks has been associated with two known threat actors, and coincided with the spike in the attack timeline we observed in our telemetry. Two specific campaigns were carried out by the [Xenotime](#) group and by IBM Hive0016 ([APT33](#)) who reportedly [broadened their attacks](#) on ICS targets.

The overlap between IT infrastructure and OT, such as Programmable Logic Controllers (PLCs) and ICS, continued to present a risk to organizations that relied on such hybrid infrastructures in 2019.

The convergence of IT/OT infrastructure allows IT breaches to target OT devices controlling physical assets, which can greatly increase the cost to recover. For example, in early 2019, IBM X-Force IRIS assisted in responding to a breach at a global manufacturing company, where a ransomware infection starting on an IT system moved laterally into OT infrastructure and brought plant operations to a halt. The attack impacted not only the company's own operations but also caused a ripple effect in global markets.

X-Force IRIS security assessments delivered to our customers through 2019 highlighted the vulnerability of OT systems, which often use legacy software and hardware. Keeping production systems that can no longer be patched and are riddled with older vulnerabilities that have long become public means that even if OT systems are not internet facing, unpatched OT systems might be easy prey. In cases of lateral movement, after an attacker gains the first foothold, these systems can be accessed from inside the network and harmed by relatively simple exploitation techniques.

Although the ICS network attack trend shown in Figure 1 has been in a downward motion since early October 2019, X-Force expects that attacks against OT/ICS targets will continue to increase in 2020, as various threat actors plot and launch new campaigns against industrial networks across the globe. With more than 200 new ICS-related CVEs released in 2019, IBM X-Force's vulnerability database shows that threats to ICS will likely continue to grow in 2020.

---

X-Force expects that attacks against ICS targets will continue to increase in 2020, as various threat actors plot and launch new campaigns against industrial networks across the globe.

---

## Records Breached Grows Dramatically

The number of breached records jumped significantly in 2019 with over 8.5 billion records exposed – more than three times greater than 2018 year-over-year. The number one reason for this significant rise is that records exposed due to misconfigurations increased nearly tenfold year-over-year. These records made up 86 percent of the records compromised in 2019. This is a stark departure from what we reported in 2018 when we observed a 52 percent decrease from 2017 in records exposed due to misconfigurations and these records made up less than half of total records.

Notably, there was actually a decrease in the number of misconfiguration incidents in 2019 of 14 percent year-over-year. This fact implies that when a misconfiguration breach did occur, the number of records affected was significantly greater in 2019. Nearly three-quarters of the breaches where there were more than 100 million records breached were misconfiguration incidents. In two of those misconfiguration incidents which occurred in the Professional Services sector the exposed record count was in the billions for each incident.

This significant increase in lost records across industries highlights the growing risk of data breaches, even for organizations in sectors that were not typically considered prime targets.

2019 breached records

8.5 billion

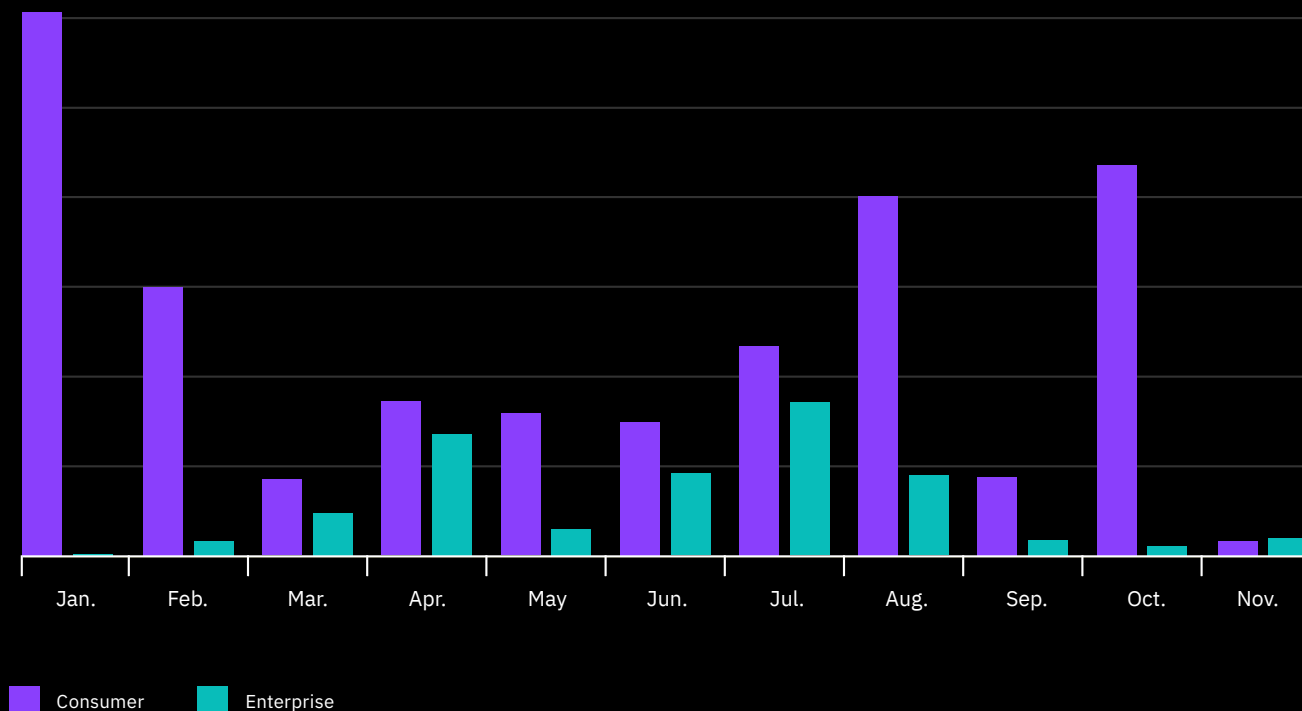




**Figure 2:**

## Consumer vs. enterprise IoT attacks

Monthly volume of consumer vs. enterprise IoT attacks in 2019 (Source: IBM X-Force)



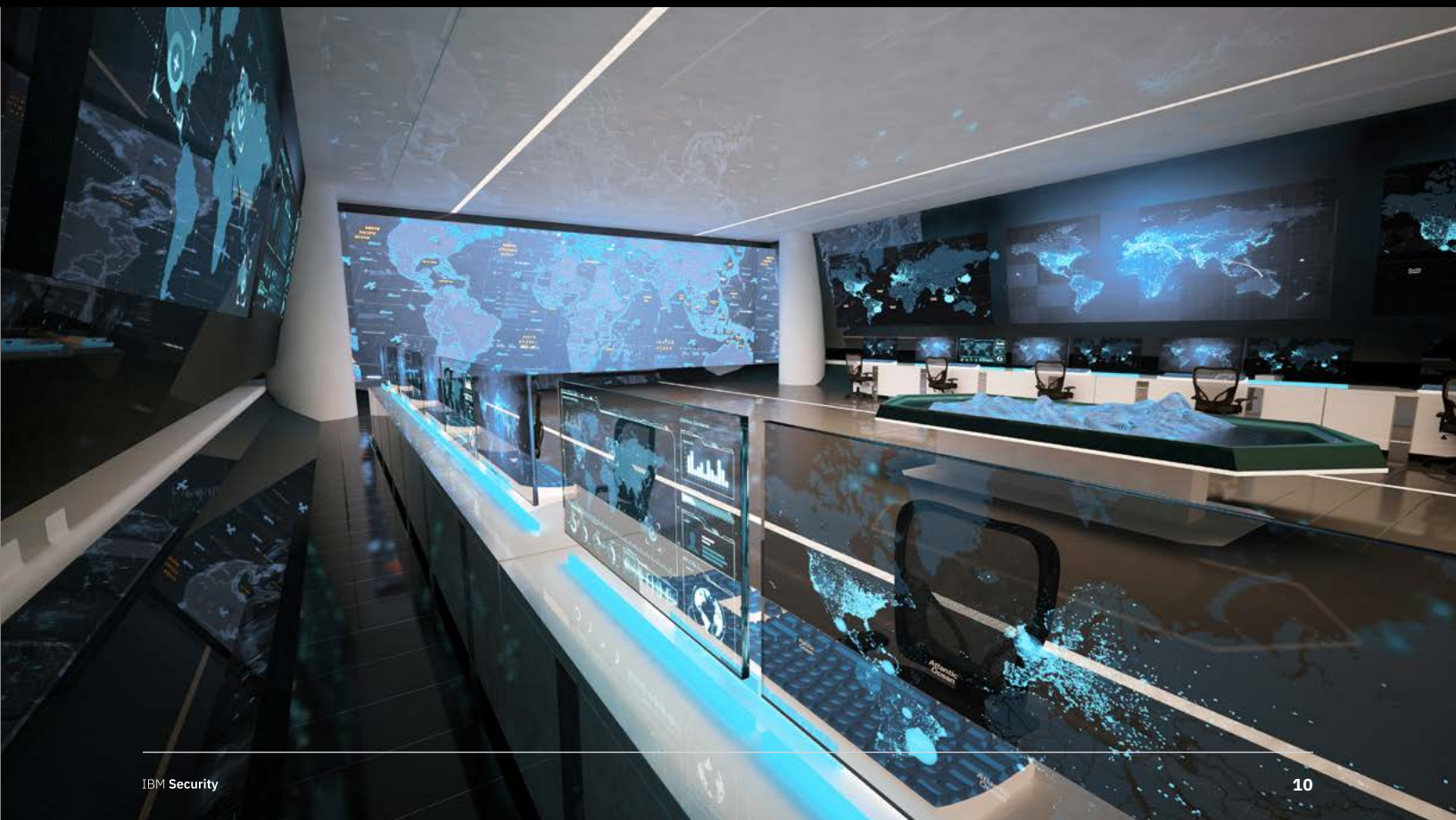
### Targeting of IoT Devices Includes Enterprise Realms

With over [38 billion devices](#) expected to be connected to the internet in 2020, the Internet of Things (IoT) threat landscape has been gradually shaping up to be one of the threat vectors that can affect both consumers and enterprise level operations by using relatively simplistic malware and automated, often scripted, attacks.

Within the sphere of malicious code used to infect IoT devices, IBM X-Force research has tracked multiple Mirai malware campaigns in 2019 that have notably shifted from targeting [consumer electronics](#) to targeting enterprise-grade hardware as well – activity that we did not observe in 2018. Compromised devices with network access can be used by attackers as a pivoting point in potential attempts to establish a foothold in the organization.

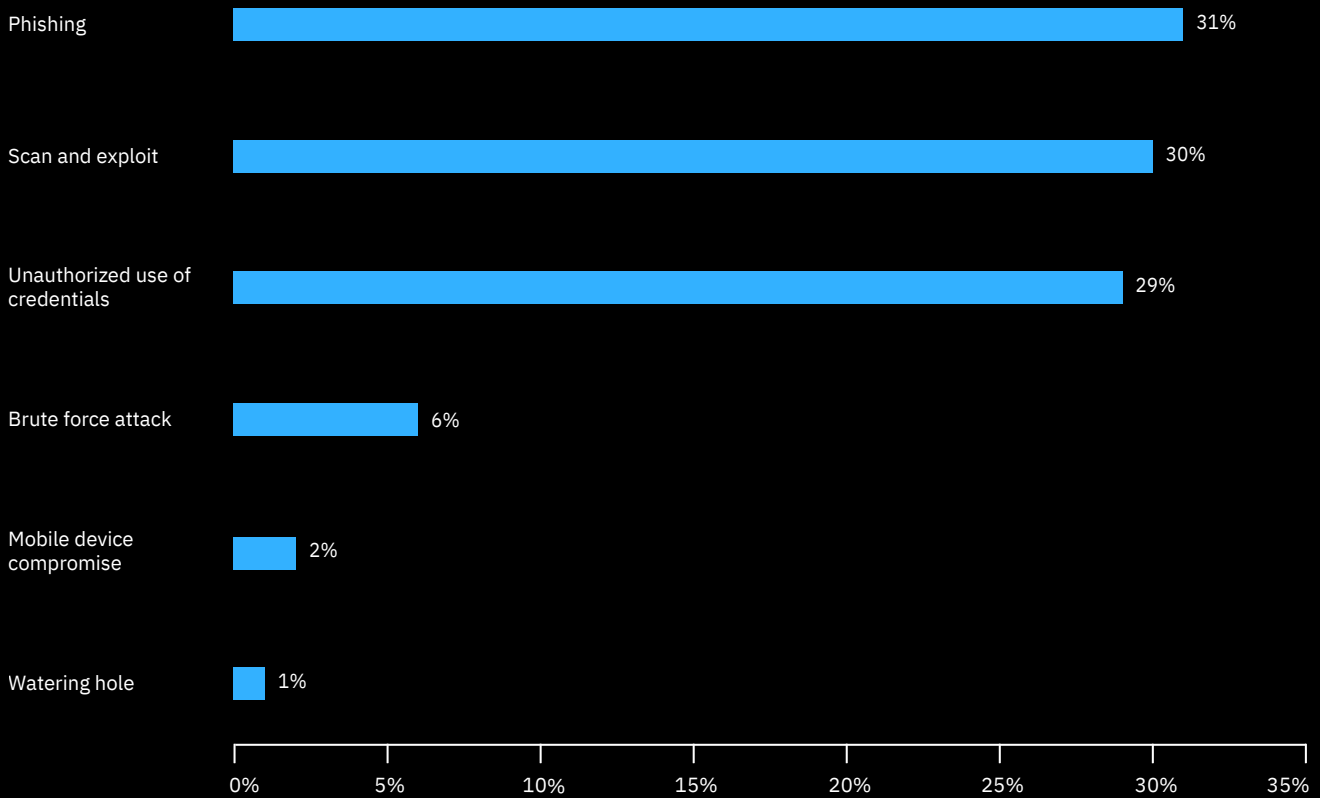
Mirai is a prolific IoT malware that has been used in the hands of multiple attackers since 2016 to cause [mass disruption](#) by infecting large numbers of IoT devices and using them in distributed denial of service (DDoS) attacks. In our analysis of 2019 campaigns, we have found that TTPs of those wielding the Mirai malware have robustly changed since 2018, and in 2019 focused on targeting enterprise hardware in addition to consumer electronics.

Looking into attacks that affected IoT devices in 2019, we have observed the widespread use of command injection (CMDi) attacks containing instructions to download malicious payloads targeting various types of IoT devices. Most of these injection attacks are automated by scripts that scan for and attempt to infect devices en masse. If the targeted IoT device is susceptible to these injection attacks, the payload is downloaded and executed, effectively drafting the device to a large IoT botnet. One of the most common enablers of these attacks are IoT devices with weak or default passwords that can be easily guessed by a humble [dictionary attack](#).



### Figure 3: Top initial access vectors

Breakdown of the top 6 initial attack vectors in 2019, as a percentage of the six access vectors shown (Source: IBM X-Force)



### Phishing Tops Initial Access Vectors in 2019 Attacks

IBM X-Force IRIS's extensive [incident response capability](#) provides valuable insight on attacker methods and motivations.

At 31 percent, phishing was the most frequent vector used for initial access in 2019, but that is down from 2018 when it comprised nearly half of the total.<sup>1</sup>

<sup>1</sup> The 2019 X-Force Threat Intelligence Index reported that nearly one-third—29 percent—of attacks analyzed by X-Force IRIS involved compromises via phishing emails. This number has since been adjusted to account for additional evidence that surfaced post publication for several incidents increasing that percentage to 44 percent for 2018.



Most notably in 2019, attackers increasingly scanned target environments for vulnerabilities to exploit, with incident responders finding this technique used in 30 percent of incidents – up from only 8 percent of total incidents the previous year.

Threat actors have plenty of choices on what to scan and exploit, with IBM X-Force tracking over 150,000 vulnerabilities that have been publicly disclosed. While sophisticated adversaries may develop zero-day exploits, relying on known exploits occurs more frequently as such exploits allow adversaries to gain an initial foothold without having to expend resources to craft new TTPs, saving their best weapons for the most heavily defended networks. Furthermore, attackers bank on organizations not keeping up-to-date with their patch application, even for vulnerabilities where patches have been available for some time. For example, instances of WannaCry infection continue to be observed more than two years since the initial infection and the patch (MS17-010) becoming widely available.

The use of stolen credentials where threat actors use previously obtained credentials to access target organizations came in at a close third at 29 percent. Often these credentials may be stolen from a third-party site or obtained via a phishing attempt against the targeted organization. Threat actors can use stolen credentials to blend in with legitimate traffic, making detection even more challenging.

Brute force attacks dropped year-over-year to a distant fourth position with 6 percent of all cases, followed by BYOD devices at 2 percent as the initial access point into targeted organizations.

X-Force researchers observed a notable uptick in threat actor activity in June and July of 2019, with the number of events eclipsing totals for all of 2019 to that point. While the reason for this sudden surge in activity is unknown, the summer months appear to be more active in terms of spam as well, with peak spam volume recorded in August of 2019. It's possible that threat actors were simply noisier and more easily detected, or that a change in threat actor tactics or tools generated significant activity. Short term peaks of activity are less likely to be the result of new threat actors entering the market, as such new entries would be expected to create a sustained increase in activity rather than a temporary spike.

# Malware trends

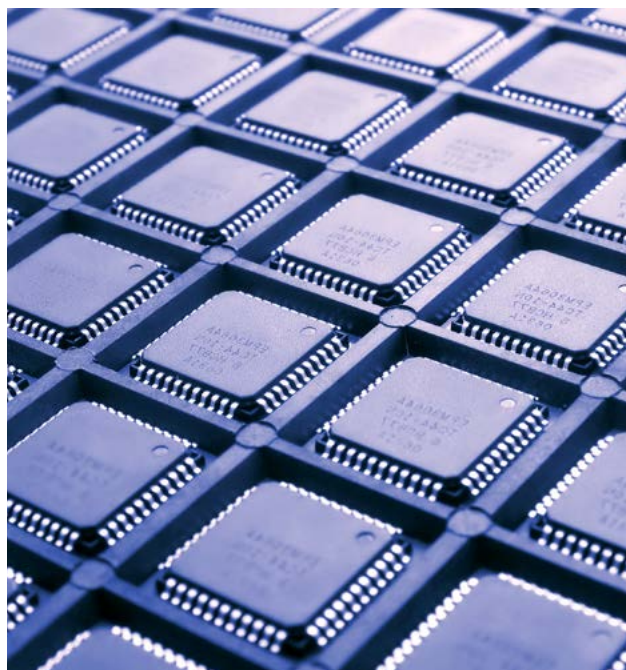
## Destructive Malware Attacks Dramatically Increase

IBM X-Force IRIS investigations indicate that destructive malware attacks became more frequent and increased in geography and scope through 2019.

Wielded by both cybercriminals and nation state actors, destructive malware is malicious software with the capability to render affected systems inoperable and challenge reconstitution. Most destructive malware variants cause destruction through the deletion or overwriting of files that are critical to the operating system's ability to run. In a few cases, destructive malware may send tailored messages to industrial equipment to cause malfunction. Included in our definition of destructive malware is the type of ransomware that's capable of wiping data from machines or irreversibly encrypting data on a machine.

Between the second half of 2018 and the second half of 2019 X-Force IRIS responded to the same number of destructive attacks year-over-year, highlighting that this potentially catastrophic malware trend continues to put organizations at risk.

Historically, destructive attacks typically came from nation state adversaries. However, we have been observing a trend where more strains of financially-motivated ransomware are incorporating destructive elements into the attack, with variants such as LockerGoga and MegaCortex making their [destructive attack](#) debuts in late 2018 and early 2019.



---

Destructive attacks are estimated to cost an average of \$239 million, over 60 times more than the average cost of a data breach.

---

In late 2019, X-Force IRIS highlighted the discovery of a new destructive malware we named [ZeroClear](#). This wiper targeted the energy sector in the Middle East and was attributed by IBM to an Iran-affiliated APT group ITG13<sup>2</sup>, also known as APT34/OilRig.

X-Force IRIS estimates that the [cost of a destructive malware attack](#) to companies can be particularly high, with large multinational companies incurring a cost of \$239 million per incident, on average. This cost estimate is over 60 times greater than the average 2019 [cost of a data breach](#) as calculated by the Ponemon Institute. Unlike data breaches that steal or expose data, destructive attacks typically see the destruction of up to three-quarters or more of devices on the victimized organization's networks.



<sup>2</sup> ITG stands for IBM Threat Group, a term which is further discussed in the Most Frequently Targeted Industries. X-Force uses ITG names, with alternate names for threat groups indicated in parentheses after the ITG name.

---

## Ransomware and Cryptominers Aggressive in 2019

The counts of malware variants and attacks using malware trend up and down through the year, but nonetheless, insight into the types of threats that should take priority can help organizations better manage risk.

In the first half of 2019, approximately 19 percent of attacks we observed were related to ransomware incidents, compared to only 10 percent of attacks in the second half of 2018. In Q4 2019 there was a 67 percent increase in ransomware engagements compared to Q4 the previous year. Throughout 2019, X-Force IRIS responded to ransomware engagements in 12 different countries in 5 different continents and across 13 different industries.

This surge may be attributed to growing numbers of threat actors and campaigns launched against a variety of organizations in 2019. Of note were municipal and public institutions that suffered ransomware attacks, as well as local [government agencies](#) and healthcare providers. Attacks on these types of organizations often caught them unprepared to respond, more likely to pay a ransom, and in some cases under extreme stress to recover from the attack due to threat to public safety and human life.

X-Force data shows that in the cases of ransomware attacks, the top attack vector in 2019 was attempted exploits against vulnerabilities in the Windows Server Message Block (SMB) protocol to propagate through the network. This tactic, which was used previously in [WannaCry attacks](#), accounted for over 80 percent of observed attack attempts.

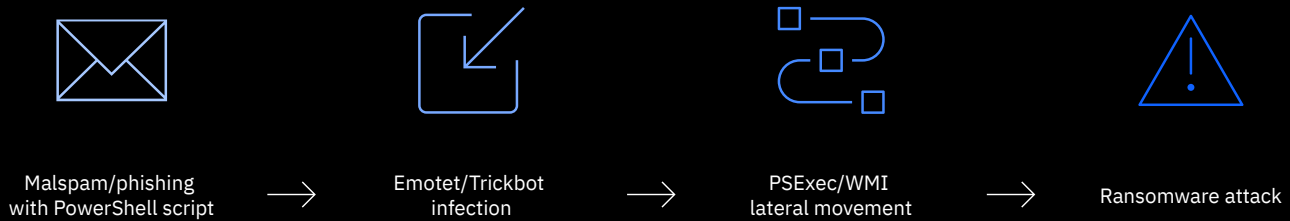
---

In Q4 2019 there was a 67 percent increase in ransomware engagements compared to Q4 2018.

---

## Figure 4: Multi-stage ransomware infection

Ransomware attack via a multi-stage infection routine (Source: IBM X-Force)



Attacks against vulnerable versions of the SMB protocol can be automated, making this a low-cost option for threat actors to attempt and easier to scale in the quest to affect as many systems as possible in one attack.

Threat actors also often used commodity downloaders, such as Emotet and TrickBot, to execute ransomware on a targeted system. This technique often leveraged PowerShell to download the malware and spread it using native functions, such as PSEXec or Windows Management Instrumentation (WMI), which can be harder to detect.

Attackers use multiple stages to infect users, instead of a direct hit with the ransomware, to give them better control over the attack, to evade controls and detection, and to plant the seeds of a ransomware operation that would encompass enough devices to entice victims to pay. The return on their investment of patience and planning is big: within five months, Ryuk attacks amassed more than [\\$3.7 million](#) for their crime gang. In another instance, an attack on nursing homes in the US led to a [\\$14 million](#) ransom demand from Ryuk operators.

Ransomware was not the only type of malware to spike in 2019. Another type of malware that was extremely popular in 2019 was cryptocurrency mining code.

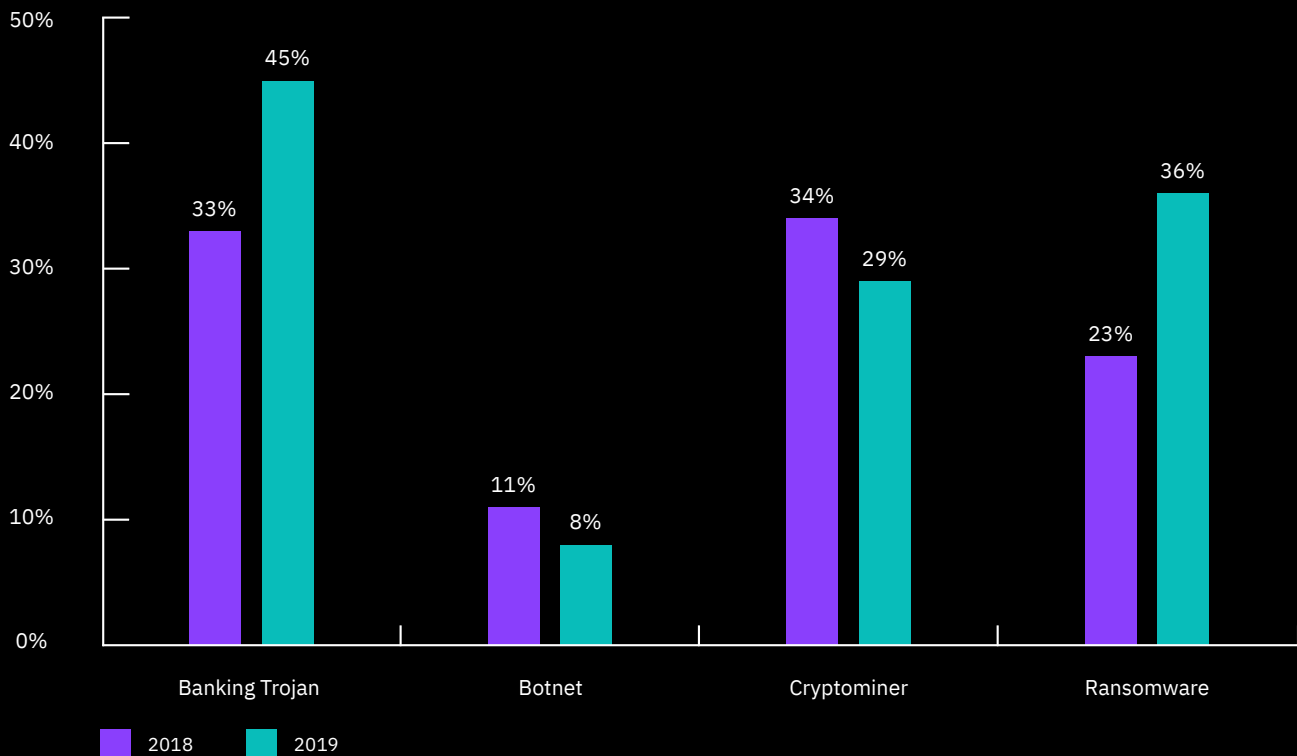
Per X-Force telemetry, cryptomining activity spiked to unprecedented levels mid-year 2019, with activity volume in June almost exceeding all other cryptomining activity for the entirety of the year.

While malware trends rise and fall according to the motives and resources of those operating botnets, this spike could be related to the tripling in value of Monero, a cryptocurrency often used by malware miners.



## Figure 5: Malware genetic code innovation

Percentage of new (previously unobserved) code by category, 2018-2019 (Source: Intezer)



### Top Innovators in 2019 Malware Code Evolution

Drawing on previous X-Force collaboration in detecting new malware variants, Intezer used its genetic malware analysis technology revealing the genetic origins of all software code to identify code similarities and code reuse to measure malware “innovation.” This measure of innovation is the extent to which threat actors invested in developing new code, suggesting that adversaries are looking to expand their threat capabilities and evade detection.

Data from Intezer shows that, in 2019, threat actors focused primarily on developing and evolving the codebase of banking Trojans and ransomware, while maintaining a high level of effort towards modifying and creating cryptomining malware strains.

This section of the report was written in collaboration between IBM X-Force and [Intezer](#) researchers. Intezer performs genetic analysis on malware’s binary code.

In 2019, banking Trojans had the highest level of new code (45 percent), followed by ransomware (36 percent). Historically IBM has seen threat actor interest and investment in malware types effective against enterprise users, suggesting these malware families may target enterprises in 2020. If they do not constantly evolve, banking Trojans and ransomware operators will face extinction as the malware will see faster detection and reduce the attacks' return on investment over time.

Cryptominers showed a drop in innovation in 2019, but the volume of mining activity was still high, suggesting that threat actors continue to develop new versions of cryptominers but are increasingly relying on previous code. Based on IBM's experience, these simplistic malware codes often rely on other, non-malicious forefathers, like [XMRig](#) for example, modified to harvest coins in an illegitimate way. New miners are also written for different purposes, like harvesting coins [on IoT devices](#), or at the other extreme – on [infected servers](#), where CPU power is greater than on smaller devices and individual PCs.

By contrast, generic botnet malware (11 percent) had less code innovation year-over-year, indicating lesser investment in modifying its capabilities. IBM has observed these types of codes pushed to users from spam or malvertising. The main role of generic botnet malware is to gain some foothold on an infected device, but their functionality remains minimal, which can explain why they do not see a higher level of code evolution.

Going into 2020, these code innovation trends may be indicative of the types of malware that will require more effort to identify and contain due to the investment to constantly evolve its code.

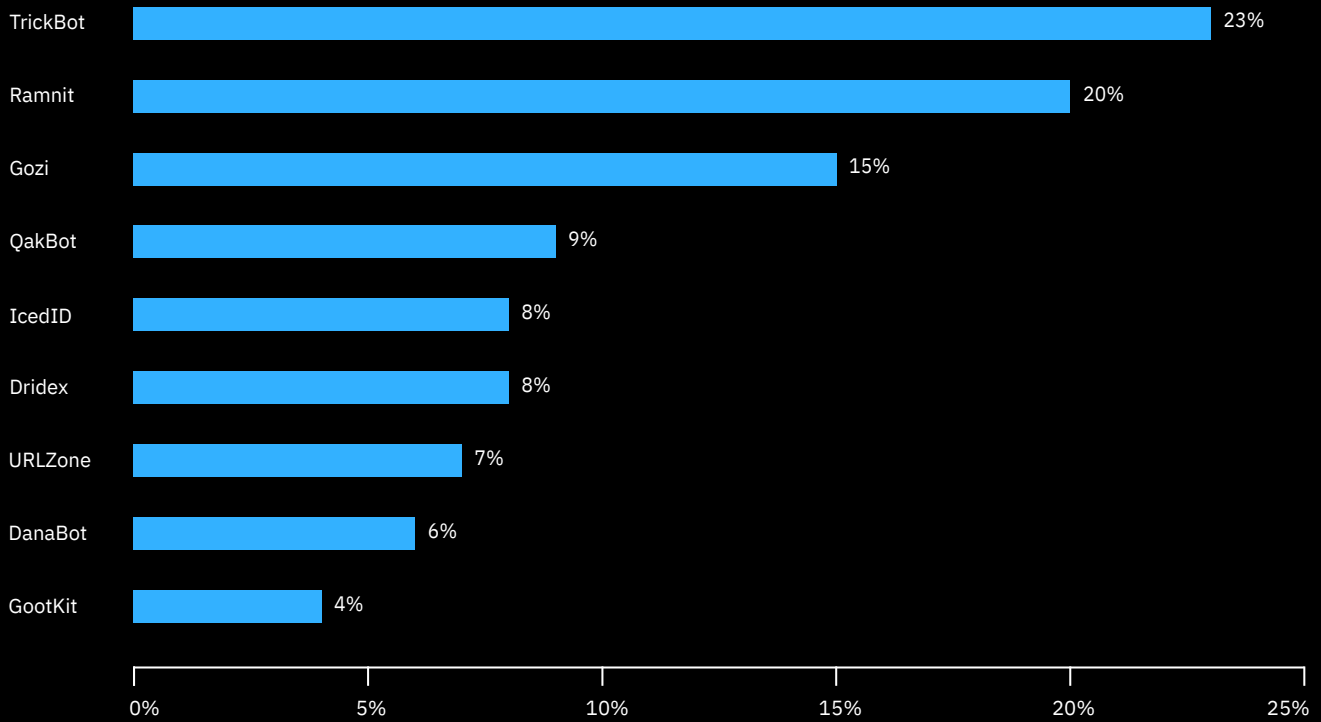
---

In 2019, threat actors focused on developing and evolving the codebase of banking Trojans and ransomware.

---

## Figure 6: Top banking Trojan families

Breakdown of top banking Trojan families in 2019, as a percentage of the nine Trojan families shown (Source: IBM X-Force)



### Banking Trojans and Ransomware – A Treacherous Matrimony That Keeps Getting Worse

The financial malware arena became a mainstream issue a little over a decade ago, with the rise of malware like the Zeus Trojan, which at the time was the first commercial banking Trojan in general availability to the cybercrime world. A review of the 2019 financial crime landscape marks a clear trend for the top banking Trojan gangs: these malware botnets are increasingly being used to open the door for targeted, high-stakes ransomware attacks.

A chart of the most active Trojan families in this category for 2019 looks rather similar to the one we produced in the 2018 annual roundup. TrickBot, Gozi, and Ramnit remain in the top three positions. These Trojans are operated by organized groups that offer varying business models to other cybercrime actors, like botnet-as-service schemes and distribution through compromised assets.

The gang operating TrickBot has been, by far, the most active crimeware group in the cybercrime arena in 2019. This activity was expressed in various aspects:

- Frequency of code updates and fixes (code, version and feature evolution)
- Frequency and scale of infection campaigns
- Frequency and volume of attack activity

Gangs that made headlines with high-stakes ransomware attacks in 2019 are also those who introduced [high-stakes wire fraud](#) attacks to the cybercrime arena in 2015. In a sense, the overarching strategy is the same, only the tactics are modified over time: target businesses for a bigger bounty.

Additionally, reports from late 2019 indicate that [ITG08](#), (FIN6) which has historically been focused on mass-theft of payment card data, has been diversifying its TTPs as well. It now aims to include [deployment of ransomware](#) on enterprise networks. Accumulating, then selling or using stolen card data can take time and effort to monetize, whereas a ransomware attack has the potential to net millions in one fell swoop, luring more gangs to take on the ransomware and cyber-extortion route.

#### **The top examples of banking Trojans diversifying to ransomware are:**

##### **Dridex**

Previously spread LokiBot to user devices, now deploys BitPaymer/ DopplePaymer on enterprise networks.

##### **GootKit**

Suspected deployer of LockerGoga on enterprise networks. LockerGoga emerged in early-2019 and has since been part of [crippling attacks](#) on businesses.

##### **QakBot**

Deploys MegaCortex on enterprise networks.

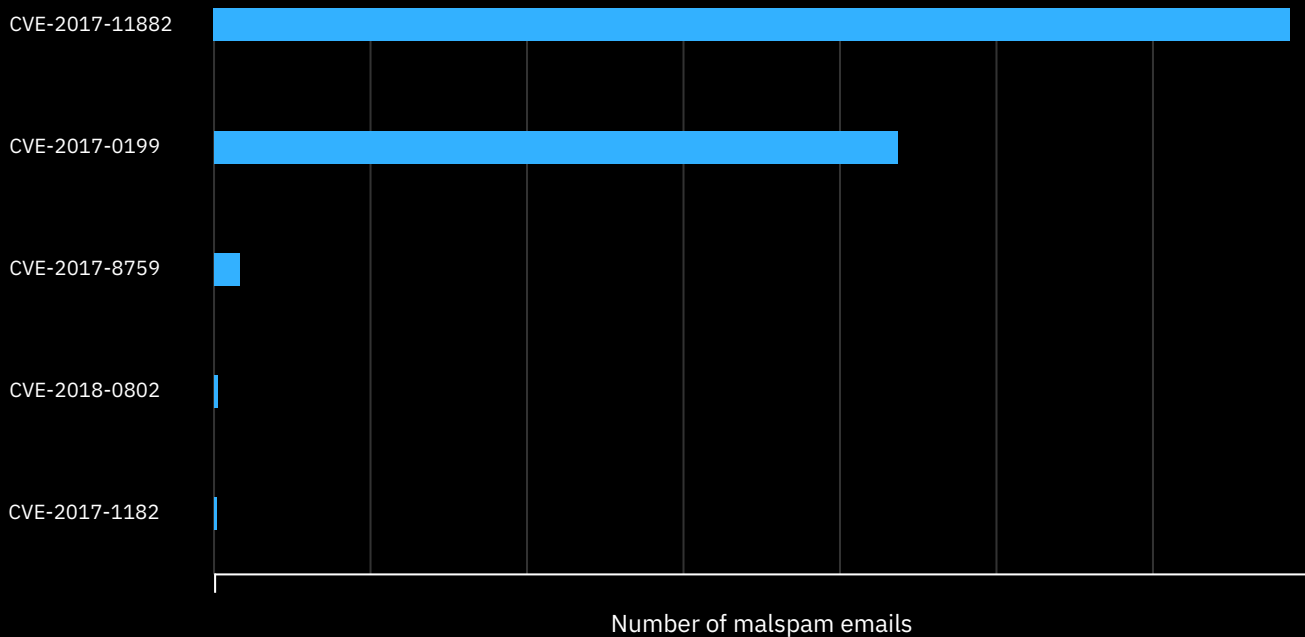
##### **TrickBot**

Deploys Ryuk on enterprise networks.

# Spam and Phishing Trends

## Figure 7: Top vulnerabilities leveraged in malspam

Breakdown of top vulnerabilities leveraged in malspam attachments in 2019, by volume (Source: IBM X-Force)



### 2017 Vulnerabilities Continued to Star in 2019 Spam

IBM X-Force runs spam traps around the world and monitors tens of millions of spam messages and phishing emails daily. Our teams and technology analyze billions of web pages and images to detect fraudulent activity and brand abuse.

X-Force analysis of global spam activity indicates that spam email continues to use a limited subset of vulnerabilities, with particular focus on just two CVEs: 2017-0199 and 2017-11882. Both of these are patched vulnerabilities that have accounted for nearly 90 percent of the vulnerabilities threat actors attempted to exploit via spam campaigns. Both these CVEs affect Microsoft Word and do not require user interaction beyond opening a booby-trapped document.

Our event data shows that the frequency in which these two vulnerabilities were used by attackers in 2019 exceeded the use of any other Microsoft Word remote code execution vulnerability by a ratio of nearly 5 to 1.

While these two vulnerabilities show up in considerable amounts of spam email, there is no indication as to how successful they might be in exploiting users. That being said, spam is often a numbers game; with sufficient volume, even a small success rate is enough to generate value for threat actors. Since many users and even organizations [can lag behind on patching certain issues](#), it is possible to still see devices compromised by older bugs.

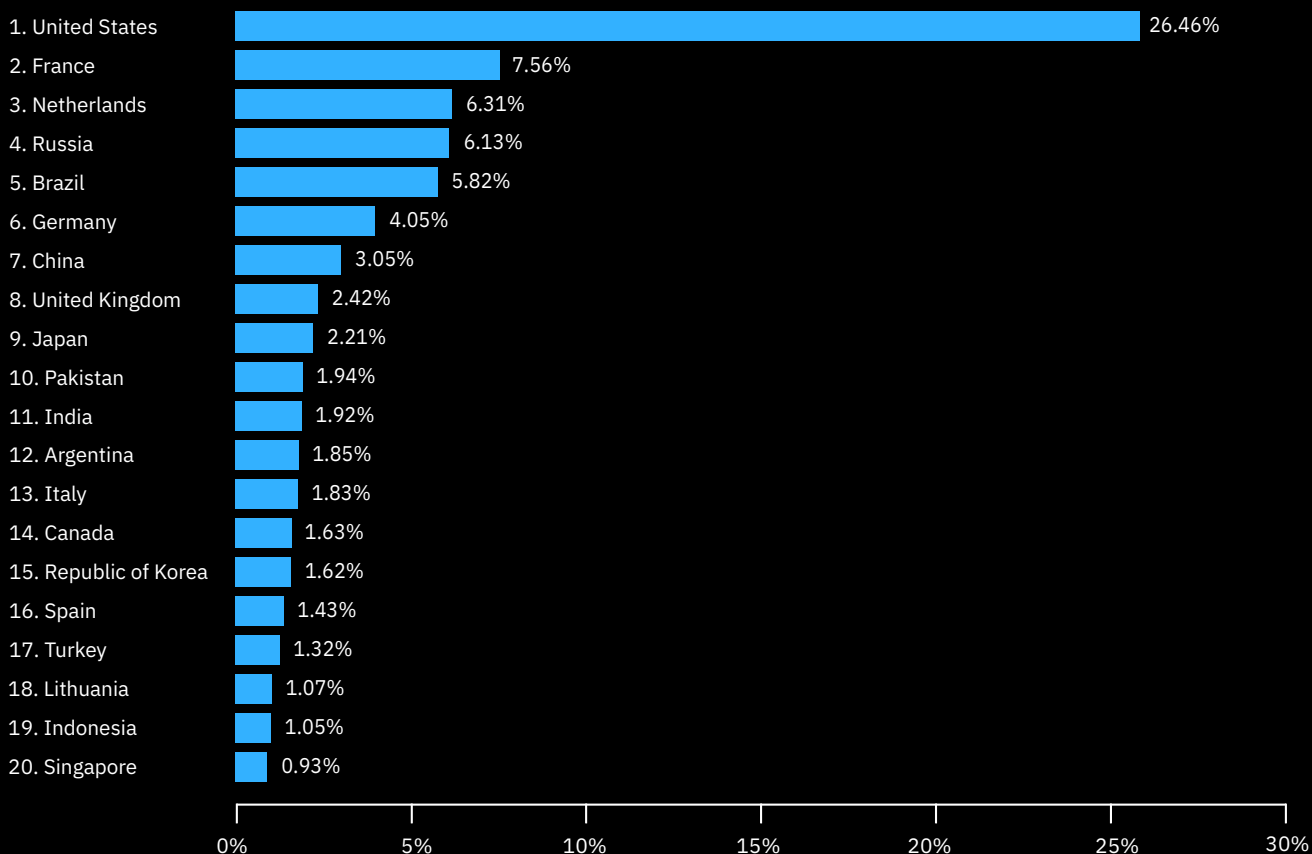
There may be many explanations for the popularity of older vulnerabilities, including the ease of incorporation and availability of free document generators, their continued effectiveness, or their versatility to drop a variety of malicious payloads.

The continued use of old vulnerabilities highlights the long tail of malicious activity and how significant vulnerabilities can still be leveraged against users years after disclosure and patch release.



### Figure 8: Top 20 spam C2 hosting countries

Top 20 countries according to their share of spam command and control (C2) servers globally in 2019. (Source: IBM X-Force)



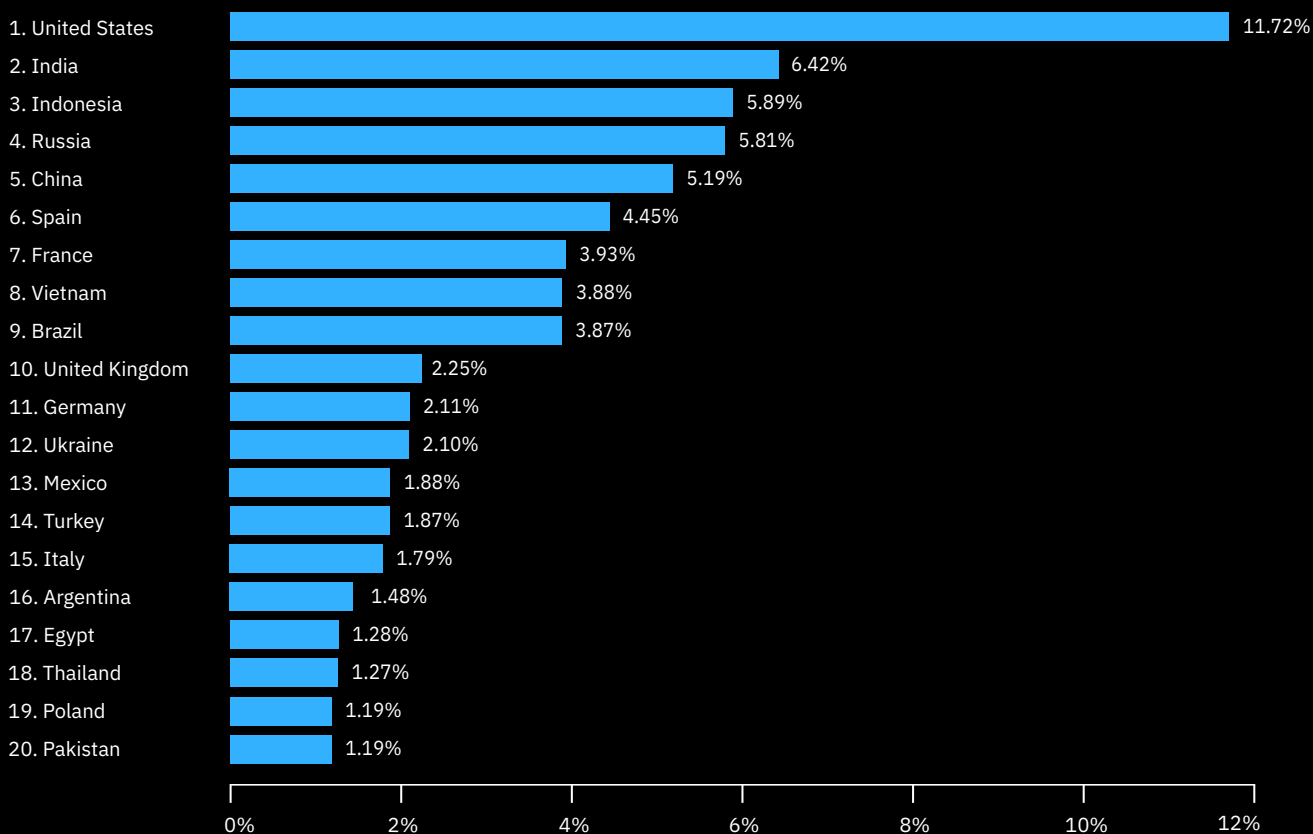
### Spam Botnets Hosted in the West, Impact Globally

IBM X-Force's research into spam botnets looks at a variety of geo-specific data points linked with command and control (C2) infrastructure for spam botnets. One of the parameters we looked at is the geo-location where botnet C2s are hosted. In 2019, we have found that C2s were primarily hosted in North America and Western European countries, having accounted for over half of all observed C2 instances in 2019. The remaining C2 hosting was spread across a larger variety of regions.

In many cases, spam botnet C2 infrastructure is hosted on compromised servers, and the use of North American and European servers is in line with the common understanding that these countries generally have more consistent server uptime. Moreover, cybercriminals prefer to host their attacks on local resources that are less likely to raise red flags when traffic from these servers interacts with devices and networks in the target geography.

**Figure 9:**  
**Top 20 countries for spam botnet victims**

Top 20 countries according to their share of spam botnet clients (victims) globally in 2019. (Source: IBM X-Force)



### Spam Victims by Geography

Victims of spam botnets in 2019 spanned the globe, with the United States having the most victims, followed by India, Indonesia, Russia and China. This distribution of targeting aligns with spammers' motivation to reach as many recipients as possible with high-volume spam campaigns. Naturally, countries where the population is larger see a greater number of spam emails wash ashore.



---

## Blocked Malicious Domains Highlight Prevalence of Anonymization Services

When it comes to keeping networks safer from online threats, one common practice is to prevent users and assets from communicating with potentially or known malicious domains. To minimize the risk, most organizations use blocking lists to blacklist suspicious IP addresses. With the same idea on a global level, Quad9, a freely available Domain Name Server (DNS) service<sup>3</sup>, blocks an average of 10 million DNS requests to malicious sites daily.

According to a sampling of [Quad9](#) data correlated with IBM Security threat intelligence, URLs found in spam email made up the majority of suspect DNS requests, with 69 percent of all requests in 2019. While down from 77 percent in 2018, the spam URL category still makes up the most significant category of malicious domains overall. A drop of 8 percentage points could be attributed to the anonymization services category, which made up 24 percent of DNS requests.

Email spam remains one of the most effective ways to reach the largest number of potential victims thanks to large spam botnets, like the Necurs botnet, that can spew dozens of millions of spam emails per day. Malicious domains often spread malware to distribute ransomware, credential stealing scripts, or links to further scams, and are designed to fool the end user by looking legitimate or impersonating a brand they know.

Linking to malicious URLs in spam email is also the method of choice for the vast majority of financially-motivated actors as it allows them to cast a wide net with minimal effort, or opt for geo-specific targeting that can limit the exposure to their scams.

The chart in Figure 10 shows the distributions of malicious domain types recorded by IBM Security in 2019.

---

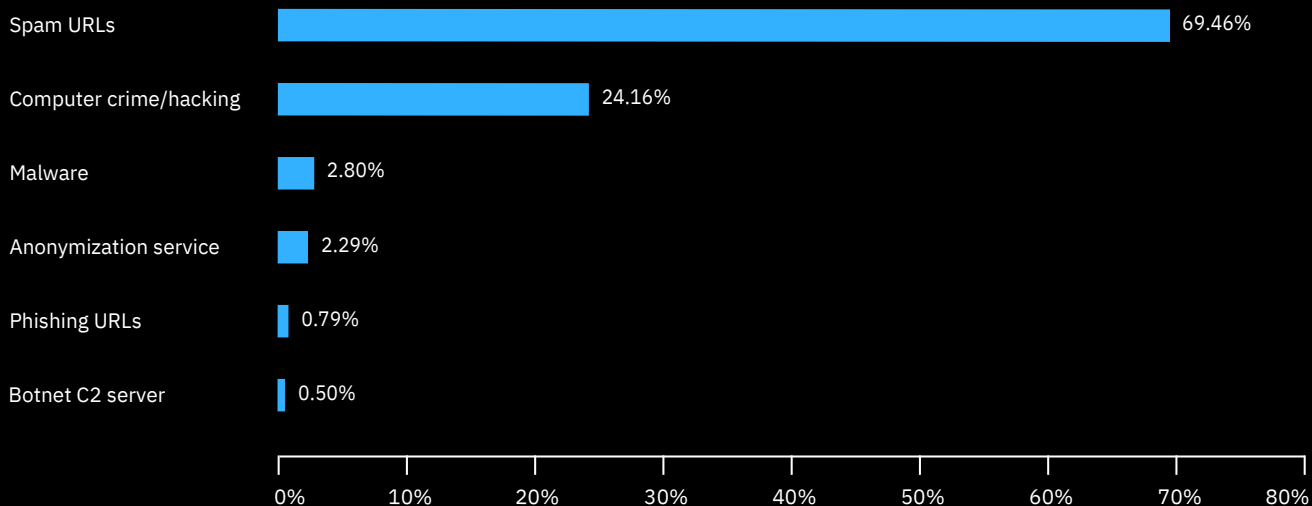
Email spam remains one of the most effective ways to reach the largest number of potential victims.

---

<sup>3</sup> Quad9 was created and sponsored through a collaboration between IBM, Packet Clearing House (PCH), and the Global Cyber Alliance (GCA).

## Figure 10: Top malicious domain threat types

Breakdown of top malicious domain threat types, as a percentage of the six types shown, in 2019 (Source: IBM X-Force and Quad9)



### Spam URLs:

Domains linking to sites affiliated with spam campaigns, often a nuisance but not affiliated with further criminal activity

### Anonymization services:

Domains linking to anonymization providers which hide traffic from further viewing

### Computer crime/hacking:

Domains specifically identified as engaging in criminal behavior, such as sites hosting web browser exploitation scripts

### Phishing URLs:

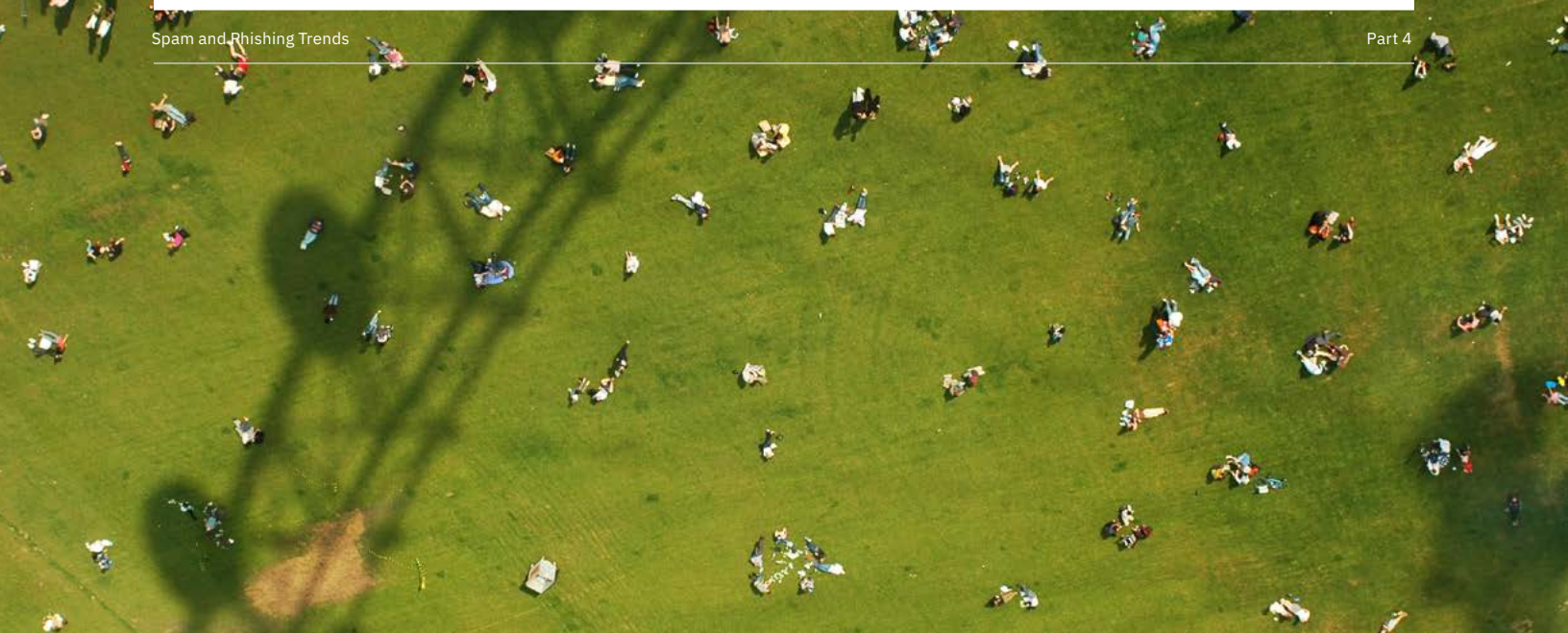
Domains masquerading as other, legitimate domains, usually in an attempt to gain credential data or other sensitive information from the user

### Botnet command and control:

Domains linking to botnet activity and potentially infecting visitors

### Malware:

Domains hosting known malware



Anonymization providers, like Tor, for example, allow users to anonymize the source of their internet traffic by browsing through nodes operated by other actors. Though anonymization services can, and often do, serve a legitimate purpose in providing users with enhanced privacy of their web browsing activity, this activity also can make it more difficult or impossible to track and block malicious activity.

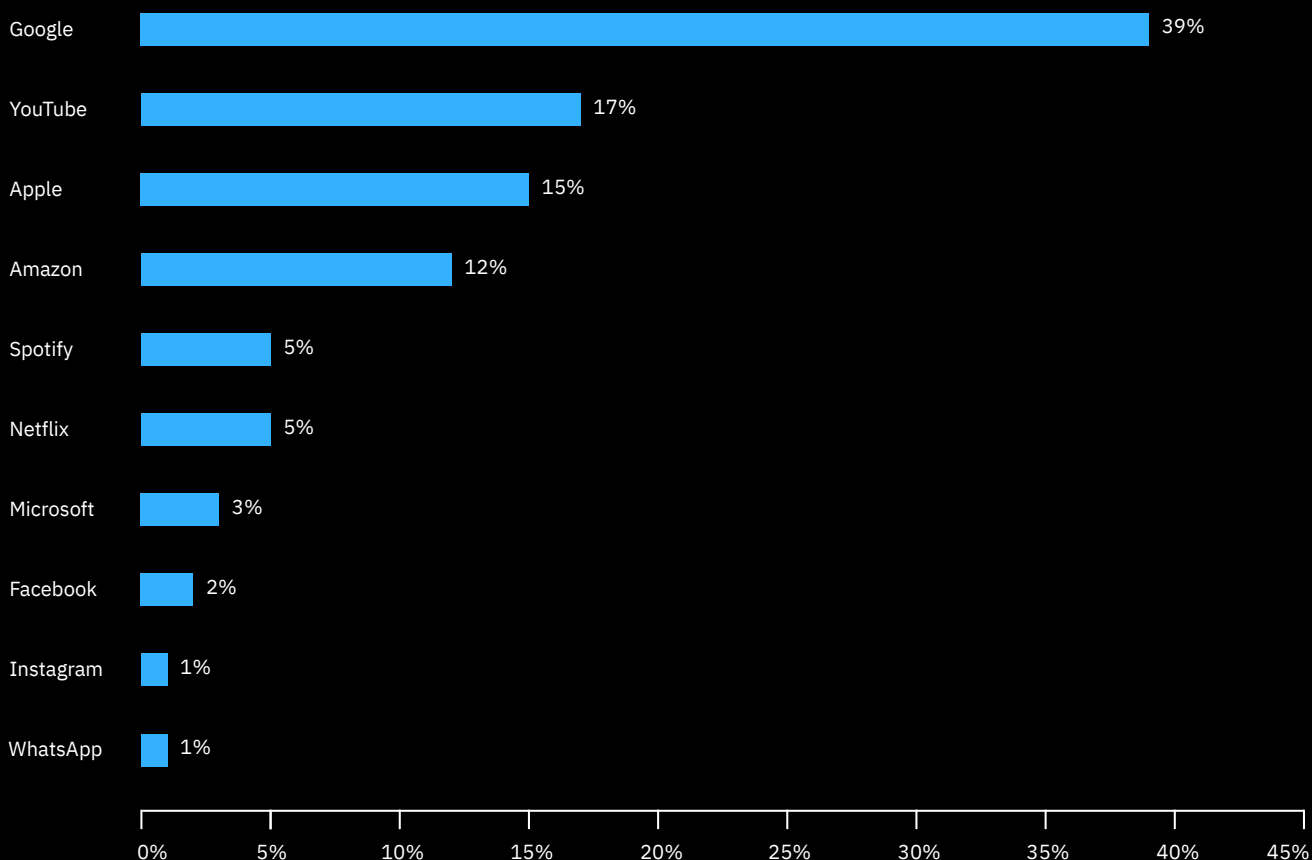
Anonymization is a common tactic used by cybercriminals attempting to cover their tracks because it can be used to obfuscate malicious links, exfiltrate data without triggering Data Loss Prevention (DLP) rules, or to pull down additional malicious payloads before the remote server's IP can be blocked.

Four percent of the malicious DNS requests were categorized as computer crime or blackhat hacking webpages, where some criminals are known to attempt web browser exploitation, distribute information about fraud, or engage in other types of online crime. This relatively low number is likely due to the fact that these links are either routed through anonymization nodes or detected and blocked by company proxies and firewalls, and consequently shut down.

**Figure 11:**

## Top 10 spoofed brands

Breakdown of the top 10 brands spoofed in spam in 2019, as a percentage of the 10 brands shown (Source: IBM X-Force)



### Phishing Impersonated Tech Companies, Social Media

Phishing continued to be a key threat vector in 2019, and X-Force data shows the most commonly spoofed brands in phishing campaigns were technology and social media platforms. Spoofed domains can be difficult for users to visually discern, and often mirror legitimate domains used by the impersonated company. An authentic-looking website can help convince a user to divulge personal data on a malicious website if it resembles the original closely enough.

This data was obtained by analyzing all the malicious domains blocked by Quad9 in 2019 and based on IBM X-Force's domain-squatting detection.

Targeting social media or content streaming sites, such as Instagram and Spotify, may not provide threat actors with readily monetizable data, like stealing Google or Amazon accounts. However, threat actors may be hoping that individuals re-use passwords between accounts and services and will try to use harvested credentials to gain access to more valuable accounts held by the same user.

## Most Frequently Targeted Industries

In today's threat landscape, the specificity of some types of attacks according to threat actor motivations means cybersecurity risk management can look very different from one sector to another.

To get a bird's eye view of the most targeted industries every year, X-Force researchers rank the volume of attacks we observed for each sector. The most frequently targeted industries have been determined based on attack and security incident data from X-Force managed networks, data and insights derived from our incident response services, and publicly disclosed incidents.

**Figure 12:**  
**Top 10 industries targeted**

Top 10 targeted industries ranked by attack volume, 2019 vs. 2018 (Source: IBM X-Force)

Sector	2019 rank	2018 rank	Change
Financial Services	1	1	-
Retail	2	4	2
Transportation	3	2	-1
Media	4	6	2
Professional services	5	3	-2
Government	6	7	1
Education	7	9	2
Manufacturing	8	5	-3
Energy	9	10	1
Healthcare	10	8	-2

Figure 12 is a comparative chart of the top most-aggressed industries in 2019 and their standing as compared to 2018.

It is easy to see that, while there was no surprise on the financial services front, the retail industry has been garnering increased interest from attackers. The same was true for media and entertainment companies, education, and government agencies.

The following sections drill down into the relative frequency of targeting based on diverse data sources and our findings for each of these industries in 2019. Some industry descriptions highlight threat actors that were particularly active in targeting the sector in recent years, but this list is not exhaustive and includes data prior to 2019. X-Force IRIS tracks and profiles dozens of nation-state sponsored and cybercriminal groups. Unattributed activity and campaigns discovered in the wild are tracked within activity "HIVES." Once activity has met a strict analytic threshold it transitions to an IBM Threat Group (ITG), which are based on collections of TTPs, infrastructure, targeting, and tradecraft.

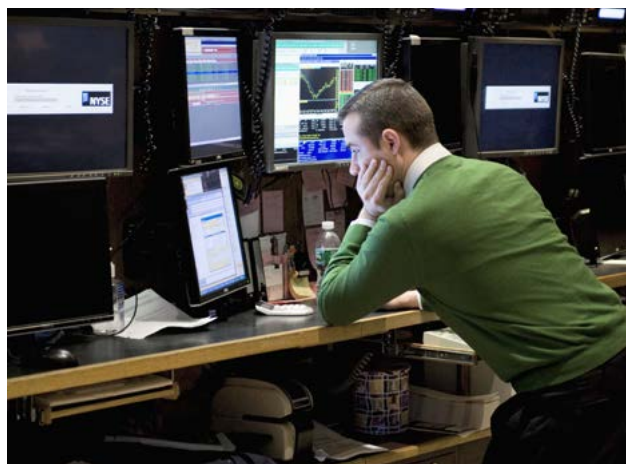
## Finance and Insurance

For four years running, the Finance and Insurance sector was the most-attacked industry in 2019. Attacks on this sector accounted for 17 percent of all attacks in the top 10 attacked industries.

It is likely that financially-motivated cybercriminals make up the greatest portion of active cyber threat actors targeting financial entities, and the allure of financial companies to a cybercriminal is clear: potentially significant and rapid payouts—in the millions for a successful attack.

Data from X-Force incident response engagements showed finance and insurance was first among the top targeted industries, despite a smaller number of publicly disclosed data breaches

This suggests that finance and insurance companies tend to experience a higher volume of attacks relative to other industries but are likely to have more effective tools and processes in place to detect and contain threats before they turn into major incidents. Financial companies are also more inclined to test their response plans under fire and make up the bulk of organizations using the [IBM Security Command Centers](#) to prepare and practice for a cyberattack. Extensively testing incident response plans and teams against relevant scenarios proved effective at mitigating financial damages from a data breach, according to the 2019 [Cost of a Data Breach Report](#)<sup>4</sup> conducted by the Ponemon Institute and sponsored by IBM Security. Breached organizations that extensively tested their incident response plan—in a cyber range environment, for example—lost on average \$320,000 less than the overall mean cost of a data breach of \$3.92 million.



Dominant 2019 threat groups targeting organizations in the financial sector were ITG03 (Lazarus), ITG14 (FIN7), and various [Magecart](#) factions. Banking Trojans like TrickBot, Ursnif, and URLZone were some of the top threats that plagued banks in 2019 by taking over and defrauding their customers' accounts.

<sup>4</sup> The annual Cost of a Data Breach Report is conducted by Ponemon Institute and sponsored by IBM.

## Retail

The retail industry was the second-most attacked of all industries, according to 2019 X-Force data. This sector was affected by 16 percent of all attacks on the top 10 industries, a marked increase from its fourth-place rank and 11 percent of attacks in 2018. This industry experienced the second largest number of network attacks in 2019.

The retail industry made it to the second position in 2019 based on X-Force IRIS data and publicly disclosed data breach information. The most common type of threat actors targeting retail organizations are financially-motivated cybercriminals, who target the industry to obtain consumer personally identifiable information (PII), payment card data, financial data, shopping history, and loyalty program information. Cybercriminals typically use this data to take over customer accounts, defraud customers, and reuse the data in various identity theft scenarios.

A popular attack technique used by cybercriminals to target retailers in 2019 was point-of-sale (POS) malware and e-commerce payment card skimming, each aiming to siphon payment card information during a transaction via physical payment terminals or online, respectively.

In particular, a set of cybercriminal factions grouped under the umbrella term [Magecart](#), has been targeting third-party payment platforms and [well-known online retailers](#) directly to inject malicious JavaScript code into the card payment pages of their websites. The code is executed as part of the checkout process to transmit the victim's payment card information to the cybercriminals—in addition to it getting the intended vendor.

X-Force IRIS incident responders observed these types of attacks first-hand in multiple breaches in 2019 and note that while the malicious code snippets could be rather basic, the back-end compromise of underlying platforms can cause an aggregate impact where criminals were able to hit [thousands of shops](#) using the same technique across the board.



### Prominent threat groups that have targeted the retail sector include:

ITG14 (FIN7)	Hive0061 (Magecart 10)
HIVE0065 (TA505)	Hive0062 (Magecart 11)
ITG08 (FIN6)	Hive0066 (Magecart 12)
Hive0038 (FIN6)	Hive0067 (FakeCDN)
Hive0040 (Cobalt Gang)	Hive0068 (GetBilling)
Hive0053 (Magecart 2)	Hive0069 (Illum Group)
Hive0054 (Magecart 3)	Hive0070 (PostEval)
Hive0055 (Magecart 4)	Hive0071 (PreMage)
Hive0056 (Magecart 5)	Hive0072 (Qoogle)
Hive0057 (Magecart 6)	Hive0073 (ReactGet)
Hive0058 (Magecart 7)	Hive0083 (Inter Skimmer)
Hive0059 (Magecart 8)	Hive0084 (MirrorThief)
Hive0060 (Magecart 9)	Hive0085 (TA561)

In addition to online e-commerce skimmers, point-of-sale malware [continues](#) to be a popular technique cybercriminals use against retailers at their brick and mortar locations to siphon payment card data from point-of-sale machines and back-end servers during a transaction or as the data is written to memory.

## Transportation

The transportation sector is considered part of any country's critical infrastructure. Companies in this sector mobilize the economy through three principal types of transportation, including ground, maritime, and air transport, for both industrial and consumer services. This sector was the third-most attacked in 2019, with attacks dropping in frequency from 13 percent in 2018 to 10 percent in 2019.

The ranking of the transportation industry in third place after finance and retail underscores the growing appeal of data and infrastructure operated by transportation companies. These assets attract cybercriminals and nation-state threat actors alike. Information held by transportation companies presents an attractive target for cybercriminals, potentially including PII, biographic information, passport numbers, loyalty program information, payment card data, and travel itineraries.

Within this sector, airlines and [airports](#), in particular, are increasingly being targeted by cybercriminals and [nation-state](#) adversaries seeking to track travelers of interest or [monetize travelers' personal information](#) by selling it on the dark web.

Cyberthreats to the transportation industry come with added risk compared to other sectors, given the potential kinetic effect an attack could have, putting human lives at risk, as well as the potential to cascade impact to other industries that rely on transportation services to carry out their operations.

Threat actor groups targeting the transportation sector varied through 2019, with both cybercriminal groups and nation state adversaries launching attacks on organizations across the globe.



### Prominent threat groups that have targeted the transportation sector include:

ITG07 (Chafer)	ITG17 (Muddywater)
ITG09 (APT40)	Hive0016 (APT33)
ITG11 (APT29)	Hive0044 (APT15)
ITG15 (Energetic Bear)	Hive0047 (Patchwork)



## Media & Entertainment

The fourth-most attacked industry in the X-Force ranking for 2019 was the media sector, having experienced 10 percent of all attacks on the top 10 industries. The media sector was up from 8 percent in 2018 and climbed from sixth to fourth position.

The media sector includes high-profile sub-industries such as telecommunications, as well as companies that produce, process and distribute news media and entertainment. The media and entertainment industry is a high-value target for cyberattackers seeking to influence public opinion, control information flows, or protect the reputation of their organization or country. In particular, nation-state groups can see negative media content as a significant threat to their national security, while cybercriminals are finding attacks on media and entertainment to be financially lucrative as they can hold stolen pre-aired media for ransom.

Opportunistic cybercriminals and nation state adversaries generally targeted this sector in 2019.



### Prominent threat groups that have targeted the media & entertainment sector include:

ITG03 (Lazarus)  
Hive0003 (Newscaster)  
Hive0047 (Patchwork)

## Professional Services

The professional services industry features various companies that provide specialized consulting services to other sectors. Some examples are firms that supply legal, accounting, HR, and specialized customer support, to name a few. This sector experienced 10 percent of all attacks on the top 10 industries according to X-Force data, down from 12 percent in 2018.

Publicly disclosed data breach information indicates that professional services also had the greatest number of records breached out of all industries in our ranking. Many of these firms acquire highly sensitive data from their customers—including data for legal proceedings, accounting and tax purposes—which can become a lucrative target for attackers seeking monetary gain or insider information.

In addition, this industry includes technology companies, which have been increasingly targeted because of the third-party access they possess and can be leveraged by attackers attempting to breach the larger and potentially more secure organizations they serve.

In addition, the day-to-day workflow of professional services firms tends to create natural attack vectors for criminals through phishing emails and malicious macros. Many professional services firms rely heavily on productivity files, such as Word and Excel document attachments, to write contracts, communicate with clients, and complete the day-to-day tasks. The use of macros is one of the most notorious attack vectors cybercriminals exploit to plant malicious scripts in the types of files no organization can afford to completely block.

Notable threat actor groups that targeted professional services in 2019: ITG01 ([APT10](#), Stone Panda), a nation-state sponsored group that appears to originate from China.



## Government

The government sector is the sixth-most attacked industry in our ranking, having received 8 percent of attacks on the top 10 industries, unchanged year-over-year but having risen in the overall ranking from seventh position in 2018.

The government sector is a high-value target for nation-state cyber actors that seek to gain an advantage over perceived adversaries, hackers seeking to expose compromising information or prove their technical prowess, and cybercriminals seeking monetary gain through extortion or stolen data.

Municipal governments have particularly come under attack in recent years, as cybercriminals seek to collect extortion money from organizations that are less likely to be as [secure](#) as those in the [private sector](#). Government entities possess assets of value to threat actors, chiefly confidential information and possible state secrets, which can include PII on government employees and agents, financial information, internal communications, and the functionality of critical networks.

Nation-state actors have demonstrated long-term interest in attacking government sector entities, and X-Force IRIS assesses that they are the most capable at doing so. Increasingly in 2019, however, cybercriminal groups also targeted government entities, seeking to encrypt and hold for ransom data that governments need to operate, particularly on the [municipal or provincial level](#).



In 2019, over 70 government entities were hit with ransomware between [January and July alone](#). Cybercriminals also stole data—including from defense websites—and later leaked it on [the dark web](#). Hacktivists notoriously find the government an attractive target, particularly if there is a controversial issue on which they desire to make a statement. Government organizations often lack the same level of cybersecurity funding as their private sector counterparts, while still needing to maintain consistent service for constituents, further [exacerbating](#) the challenge posed to these organizations by threat actors.

Notable threat actor groups targeting government agencies in 2019: varied cybercriminal actors and nation-state sponsored groups.

## Education

The education sector experienced 8 percent of all attacks on the top 10 industries, up from 6 percent in 2018, making it the seventh-most attacked industry in our ranking.

The education industry presents an array of valuable assets to financially-motivated and nation-state actors. From [intellectual property \(IP\)](#) to [PII](#), education organizations are an ample target for different types of threat actors.

Each with a different motivation, adversarial actors have used a variety of initial infection vectors to breach the networks of academic institutions, but the most commonly observed method remains phishing emails, often tailored to the specific academic institution or research area.

Education sector organizations often have a large and varied IT infrastructure and digital footprint. They operate different assets that serve an elevated number of users ranging from staff to students and contractors. This vast attack surface which threat actors can leverage for various malicious activities is more challenging to secure. Reports released in [October 2019](#) indicated that at least 500 schools were hit by cyberattacks, mostly ransomware, in 2019, in the US alone.

Some notable examples of more sophisticated attacks in this sector include nation-state threat actors who compromised university networks and then used them as a staging ground to infect media organizations and [military contractors](#). Similarly, attackers seeking out US-funded research, are regularly looking for ways to breach university networks to steal intellectual property that can sometimes be [priceless](#). IBM



### Prominent threat groups that have targeted the education sector include:

- ITG05 (APT28)
- ITG12 (Turla Group)
- ITG13 (APT34)
- ITG15 (Energetic Bear)
- ITG17 (Muddywater)
- Hive0075 (DarkHydrus)

X-Force IRIS assesses with high confidence that this industry will continue to be targeted by financially-motivated and state-affiliated actors seeking to gain access to valuable information.

Notable threat actor groups targeting this sector in 2019 included opportunistic cybercriminal factions and nation-state adversaries from [China, Russia, and Iran](#).

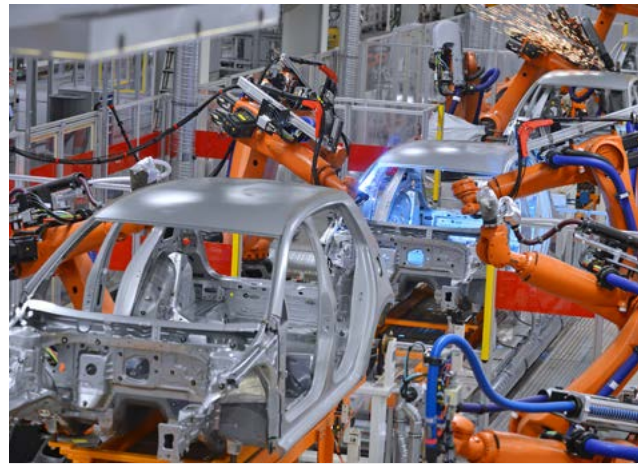
## Manufacturing

Moving the economy through metals, chemical, capital goods and electronics, manufacturers are not exempt from IT threat and threats affecting the connected OT floor. With 8 percent of all attacks on the top 10 attacked industries, manufacturing ranks as the eighth most attacked industry in our ranking, dropping from 10 percent in 2018.

While it is possible that this sector has been seeing fewer attacks year-over-year, the drop in numbers may reflect the fact that in many cases, data breaches in the manufacturing sector do not involve information that is necessarily subject to legal disclosure and regulations. As a result, attacks are not always publicly disclosed, which can make it appear as though manufacturers are attacked less often than they actually are.

Manufacturers are also organizations that operate both IT and OT environments, and are therefore subject to the same threats that affect ICS and SCADA systems. But while information security in this sector has [lagged behind](#) in the past, the successful public response by a Norwegian manufacturer to a major ransomware attack in 2019 could be indicative of shifting approaches to cybersecurity [by this industry](#).

Cybercriminals or nation-state actors seeking financial gain and IP data probably pose the greatest cyberthreat to companies in the manufacturing sector. One of the most common attack techniques used against manufacturers in 2019 was Business Email Compromise (BEC) fraud—especially if they frequently do business with [foreign suppliers](#). In such cases, company email servers, or even just email accounts, are compromised by attackers who insert themselves into existing communication threads to eventually divert millions of dollars to accounts they control.



### Notable threat groups that targeted the manufacturing industry included:

ITG01 (APT10)  
ITG09 (APT40)  
HIVE0006 (APT27)  
Hive0013 (OceanLotus)  
Hive0044 (APT15)  
Hive0076 (Tick)

Manufacturers are also prone to supply chain attacks and can be exploited by nation-state adversaries to plant backdoors or malware in the products they manufacture and ship to other countries.

On the financial motivation front, attackers could be targeting manufacturers for trade secrets and intellectual property. Research that has taken an organization years to develop can harness a quick profit for cybercriminals on the dark web or boost a nation state's economic or defense advantage—especially in the case of defense and military equipment manufacturers.

Ransomware, phishing attacks, and SQLi injection attacks also tended to frequently hit the manufacturing industry, according to X-Force data.

## Energy

The energy sector is the ninth-most targeted industry in our ranking, having received 6 percent of all attacks and incidents on the top 10 industries in 2019. This sector's standing remains unchanged from 2018, when it suffered 6 percent of attacks as well.

Companies in the energy sector prove to be rich targets for cyberattacks in part due to their importance as the backbone of every country's critical infrastructure. Energy, in its various forms, is paramount to the economic, national security, and daily functioning of [cities and industries](#).

The objectives of attacks on the energy sector are varied. Some lucrative assets within energy companies, such as customer data, financial material, trade secrets, and proprietary technology information are similar in value to those found in companies in other industries.

What sets the energy industry apart from others is the possibility of physical disruption and destruction of ICS systems and the SCADA systems that manage them. These systems can be highly valuable targets to adversaries who wish to monitor or even control operations within a targeted facility, especially when it comes to cyberwarfare situations and touches on [nuclear facilities](#) in rival countries, for example. This industry has also been targeted by destructive malware, such as ZeroCleave.

A successful attack on an ICS system designed to disrupt operations can have devastating effects on customers who rely on power, gas, oil, or any other resource coming from the energy sector. Examples of such attacks and their detrimental effects have been observed in the past in a series of incidents that targeted power plants in the Ukraine, allegedly carried out by Russia and aiming for [physical destruction](#).



### Notable threat groups that have targeted this sector include:

ITG01 (APT10)	HIVE0006 (APT27)
ITG09 (APT40)	Hive0016 (APT33)
ITG07 (Chafer)	Hive0044 (APT15)
ITG11 (APT29)	Hive0045 (Goblin Panda)
ITG12 (Turla Group)	Hive0047 (Patchwork)
ITG13 (APT34)	Hive0076 (Tick)
ITG15 (Energetic Bear)	Hive0078 (Sea Turtle)
ITG17 (Muddywater)	Hive0081 (APT34)
Hive003 (APT35)	

## Healthcare

The tenth-most targeted industry, healthcare, accounted for 3 percent of all attacks on the top 10 industries, down from eighth position and 6 percent of attacks in 2018.

The preponderance of evidence suggests that financially-motivated cybercriminals are the primary attackers against healthcare industry networks and medical devices, either aiming to steal and then sell medical records on the dark web, or to encrypt network connected devices to disrupt activity and hold companies for ransom.

The disruption of hospital and nursing home networks has been able to pressure healthcare organizations to pay for ransomware attacks in order to restore their operations sooner and protect human lives. In some cases, the ransom is just too preposterous, like a \$14 million demand that followed a 2019 Ryuk attack.

As we move into 2020, the healthcare sector will have to continue to evolve its security posture to protect data. In view of frequent ransomware attacks, hospitals must strengthen incident response capabilities, and look out for emerging attacks on insecure medical devices that could be exploited to lead to an easy compromise and pivoting by motivated attackers.

Notable threat actor groups targeting this sector included financially motivated cybercrime groups such as those operating the Ryuk ransomware. While ransomware attacks do highlight the crisis that could develop when hospitals are affected, we are not seeing a persistent nation-state interest in this sector.



## Geo-Centric Insights

Threat actors targeted all geographies in 2019, with the greatest levels of activity observed in North America, Asia, and Europe.

X-Force researchers also found threat actor activity targeting the Middle East and South America in 2019, with the former consisting of more hacktivist and nation-state attacks while South America was primarily impacted by financially-motivated actors.

In this section we will dive deeper into attacks in these geographies to better understand the nature of the targeting X-Force observed, the key threat actors focused on each area, and key dates to be aware of in 2020 for potential rises in threat actor activity. Some geographies highlight threat actors that were particularly active in targeting the area in recent years, but this list is not exhaustive and includes data prior to 2019. This section uses the IBM Threat Group nomenclature as described above, and draws on data from IBM's global incident response as well as [publicly disclosed breach data](#).





## North America

North America ranked the highest in all categories for targeting by threat actors, constituting 44 percent of incidents in 2019.

North America contains a host of potential targets and maintains a significant amount of internet infrastructure, making it a ripe target for criminal actors. In 2019, North America saw over 5 billion records compromised.

IBM responded to multiple North American incidents in 2019 that used commoditized malware—codes that can be bought on underground marketplaces or obtained for free. Commodity malware can be difficult to attribute, but can be very effective in achieving criminal objectives.

Nation-state actor activity targeting North America remained constant, but no major incidents were observed in 2019. The recent trade negotiations between the United States and China may lead to increased targeting of organizations that do business in both regions, and these organizations should maintain vigilance as long as these negotiations remain inconclusive.

### Upcoming events with historic cybersecurity significance:

July 13  
(Democratic National Convention, United States)

August 24  
(Republican National Convention, United States)

November 3  
(US Presidential Election)

### Threat actor groups that have targeted this region include:

ITG05 (APT28)	Hive0006 (APT27)
ITG08 (FIN6)	Hive0003 (APT35)
ITG11 (APT29)	ITG01 (APT10)
ITG15 (Energetic Bear)	ITG03 (Lazarus)
Hive0082 (Cobalt Dickens)	ITG04 (APT19)
Hive0042 (Kovter)	ITG09 (APT40)
Hive0016 (APT33)	ITG07 (Chafer)
Hive0013 (OceanLotus)	

### Most notable attack activity observed in X-Force incident response engagements in 2019:

Business Email Compromise, Ransomware, nation-state targeting of financial sector.

## Asia

Asia received the second-highest risk rating from X-Force analysis, having the second-highest incident count in public breaches and constituting 22 percent of incidents in 2019. Asia had over 2 billion records breached in 2019, second only to North America for the year.

A significant number of threat actors focused targeting on Asia-affiliated organizations, especially in the Korean peninsula, Japan, and China. Many observed attacks within this region followed nation-state actor TTPs. One example was ITG10, likely North Korean actors that target South Korean entities. Another example is ITG01, likely Chinese actors, targeting Japan.

Recent geopolitical events in Asia have increased the likelihood of nation-state affiliated activity in this region. Democracy protests in Hong Kong and the subsequent crackdown have put China on edge. Increased tensions between North Korea and its neighbors has emboldened the regime. Indian absorption of the Kashmir region has similarly led to heightened tensions in the region.

Moving into 2020, monitoring of these potentially volatile geopolitical stakes is crucial to understanding the risk posed to organizations operating in this region.

### Upcoming events with historic cybersecurity significance:

July 24  
(Tokyo 2020 Olympics)  
October 10  
(Taiwan Independence Day).

### Threat actor groups that have targeted this region include:

Hive0013 (OceanLotus)	ITG16 (Kimsuky)
Hive0044 (APT15)	Hive0016 (APT33)
Hive0045 (Goblin Panda)	Hive0040 (Cobalt Gang)
Hive0049 (Samurai Panda)	Hive0047 (Patchwork)
ITG01 (APT10)	Hive0063 (DNSpionage)
ITG03 (Lazarus)	Hive0076 (Tick)
ITG05 (APT28)	Hive0079 (Labrynth Cholima)
ITG06 (APT30)	Hive0006 (APT27)
ITG09 (APT40)	Hive0003 (APT35)
ITG10 (APT37)	ITG15 (Energetic Bear).
ITG11 (APT29)	

### Most notable attack activity observed in X-Force incident response engagements in 2019:

PowerShell attacks, insider threats, ransomware.

## Europe

Europe fell victim to similar levels of malicious activity as Asia, coming in at 21 percent of incidents.

Unlike Asia, which is mostly affected by rivaling nation states, Europe appeared to be primarily targeted by financially-motivated threat actors. This difference may be explained by the greater potential for theft from European-based companies based on currency exchange rates. Alternatively, criminal motivations could be in pursuit of intellectual property, which can be sold to competitors for significant gain.

The British exit from the European Union (Brexit) may have reverberations in hacktivist circles moving into 2020, but no observed activity occurred in 2019. Additionally, upcoming elections in major E.U. countries (Germany, France) could potentially be targets for nation-state actors looking to influence policy in these countries.

### Upcoming events with historic cybersecurity significance:

January 31  
(UK exits European Union under Article 50)

June 28  
(Ukraine Constitution Day/NotPetya Anniversary).

### Threat actor groups that have targeted this region include:

ITG05 (APT28)	ITG17 (Muddywater)
ITG08 (FIN6)	Hive0006 (APT27)
ITG12 (Turla)	Hive0003 (APT35)
ITG15 (Energetic Bear)	Hive0013 (OceanLotus)
ITG09 (APT40)	Hive0044 (APT15)
ITG07 (Chafer)	Hive0063 (DNSpionage)
ITG11 (APT29)	
ITG14 (FIN7)	

### Most notable attack activity observed in X-Force incident response engagements in 2019:

RDP compromise, POS malware, insider threats.

## Middle East

X-Force IRIS observed a number of nation-state affiliated incidents that affected organizations in the Middle East in 2019, but overall metrics for threat actor activity were relatively low in 2019, with 7 percent of incidents in this region.

There could be a number of explanations for the reduced activity, such as other geographies providing a greater return on investment for cybercriminal activity. However, unlike other geographies, the Middle East had a higher proportion of hacktivist and nation-state activity compared to other parts of the world.

The hacktivist activity could relate to the political unrest in the region in 2019, with multiple major incidents involving Iran. Similarly, nation-state activity, such as ITG13 pursuing Iranian state interests, followed state objectives in targeting organizations in the energy sector in this region with [destructive attacks](#).

Political unrest and kinetic warfare in Yemen continue to produce the risk of cyberthreat activity, in which actors on all sides of the conflict are using [cyberattacks](#) to spread their message and generate revenue. These risks will likely continue into 2020 as different parties continue to publicly threaten one another in that ongoing conflict.

### Upcoming events with historic cybersecurity significance:

November 21  
(2022 Club World Cup football tournament, Qatar)

### Threat actor groups that have targeted this region include:

Hive0044	Hive0016 (APT33)
ITG07 (Chafer)	Hive0006 (APT27)
ITG13	Hive0003 (APT35)
Hive0081 (APT34)	ITG17 (Muddywater)
Hive0078 (Sea Turtle)	ITG12 (Turla)
Hive0075 (DarkHydrus)	ITG11 (APT29)
Hive0063 (DNSpionage)	ITG10 (APT37)
Hive0047 (Patchwork)	ITG09 (APT40)
Hive0022 (Gaza Cybergang)	ITG05 (APT28)
	ITG01 (APT10)

### Most notable attack activity observed in X-Force incident response engagements in 2019:

Destructive malware, DDOS attack, web script.

### South America

South America struggled with significant cybercriminal activity in 2019 but did not receive the same level of focus as the top three geographies, accounting for only 5 percent of incidents. However, year-over-year activity continues to rise in this region, with X-Force observing an uptick in significant incident response activities, especially in the retail and financial services sectors.

Observed incidents in this region included ransomware activity, which continued to grow in popularity throughout 2019.

#### Upcoming events with historic cybersecurity significance:

June 12  
(2020 Copa America football tournament, Colombia and Argentina).

#### Threat actor groups that have targeted this region include:

- |                       |                    |
|-----------------------|--------------------|
| Hive0081 (APT34)      | ITG17 (Muddywater) |
| Hive0044 (APT15)      | ITG12 (Turla)      |
| Hive0016 (APT33)      | ITG11 (APT29)      |
| Hive0013 (OceanLotus) | ITG05 (APT28)      |
| Hive0003 (APT35)      | ITG03 (Lazarus)    |
|                       | ITG01 (APT10)      |

#### Most notable attack activity observed in X-Force incident response engagements in 2019:

Business Email Compromise, Ransomware, nation-state targeting of financial sector.



## Preparing for Resilience in 2020

Based on IBM X-Force findings in this report, keeping up with threat intelligence and building strong response capabilities are impactful ways to mitigate threats in the evolving landscape, regardless of which industry or country one operates in.

Our team recommends a number of steps that each organization can take to better prepare for cyber threats in 2020:

- Leverage threat intelligence to better understand threat actor motivations and tactics to prioritize security resources.
- Build and train an incident response team within your organization. If that's not a possibility, engage an effective incident response capability to ensure prompt response to high-impact incidents. In 2019, IBM Security observed that containing impacts significantly cut back on associated costs, with our team's prompt intervention in a MegaCortex infection stopping the ransomware attack mid-stream and preventing thousands of dollars in [damage](#).
- Stress test your organization's incident response plan to develop muscle memory. Tabletop exercises or cyber range experiences can provide your team with critical experience to improve reaction time, reduce downtime, and ultimately save money in the case of a breach.
- Implementing multifactor authentication (MFA) continues to be one of the most efficient security priorities for organizations. In 2019 credential theft or re-use was one of the most commonly observed attack method used by threat actors, and MFA can effectively inhibit this attack before it takes hold.
- Ensure the organization has a solution in place to detect and block spoofed domains, such as [Quad9](#), due to the prevalence of phishing as an attack vector.
- Have backups, test backups, and store backups offline. Not only ensuring the presence of backups but also their effectiveness through real-world testing makes a critical difference in ensuring the organization's security.

## Moving Forward with Key Takeaways

### In 2020, organizations will need to be concerned about old and new threats.

- The risk surface will continue to grow in 2020, with more than 150,000 current vulnerabilities and new ones reported regularly.
- With over four times as many records breached in 2019 as in 2018, the year 2020 could see another big number of lost records due to breaches and attacks.
- Threat actors continue to shift their sights to different attack vectors, with increased targeting of IoT devices, Operational Technology (OT), and connected industrial and medical systems, to name a few.
- Malware use by threat actors continues to fluctuate, with ransomware, cryptominers, and botnets all taking lead at different points in 2019. We expect this trend to continue in 2020, meaning organizations will need to protect themselves against varied threats that change over time.
- High levels of code innovation for ransomware and cryptominers likely implies these threats will continue to evolve in 2020, necessitating better detection and containment capabilities.
- Spam activity continues unabated, requiring diligent blacklisting, vulnerability patching and threat monitoring by organizations.
- The year-over-year shift in industry-specific targeting highlights the risk to all industry sectors and a need for meaningful advancements and maturity in cybersecurity programs across the board.
- Organizations can use their geographic location to help identify the most likely attackers and attack motivations to estimate and mitigate some of the relevant risks they could face.

## 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.

## Contributors

Michelle Alvarez  
Dave Bales  
Joshua Chung  
Scott Craig  
Kristin Dahl  
Charles DeBeck  
Ari Eitan (Intezer)  
Brady Faby (Intezer)  
Rob Gates  
Dirk Harz  
Limor Kesseem  
Chenta Lee  
Dave McMillen  
Scott Moore  
Georgia Prassinis  
Camille Singleton  
Mark Usher  
Ashkan Vila  
Hussain Virani  
Claire Zaboeva  
John Zorabedian

Learn more  
about IBM  
Security





© Copyright IBM Corporation 2020

**IBM Security**

New Orchard Rd  
Armonk, NY 10504

Produced in the United States of America  
February 2020

Produced in the United States of America  
February 2020

IBM, the IBM logo, [ibm.com](http://ibm.com), and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [ibm.com/legal/copytrade.html](http://ibm.com/legal/copytrade.html)

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.