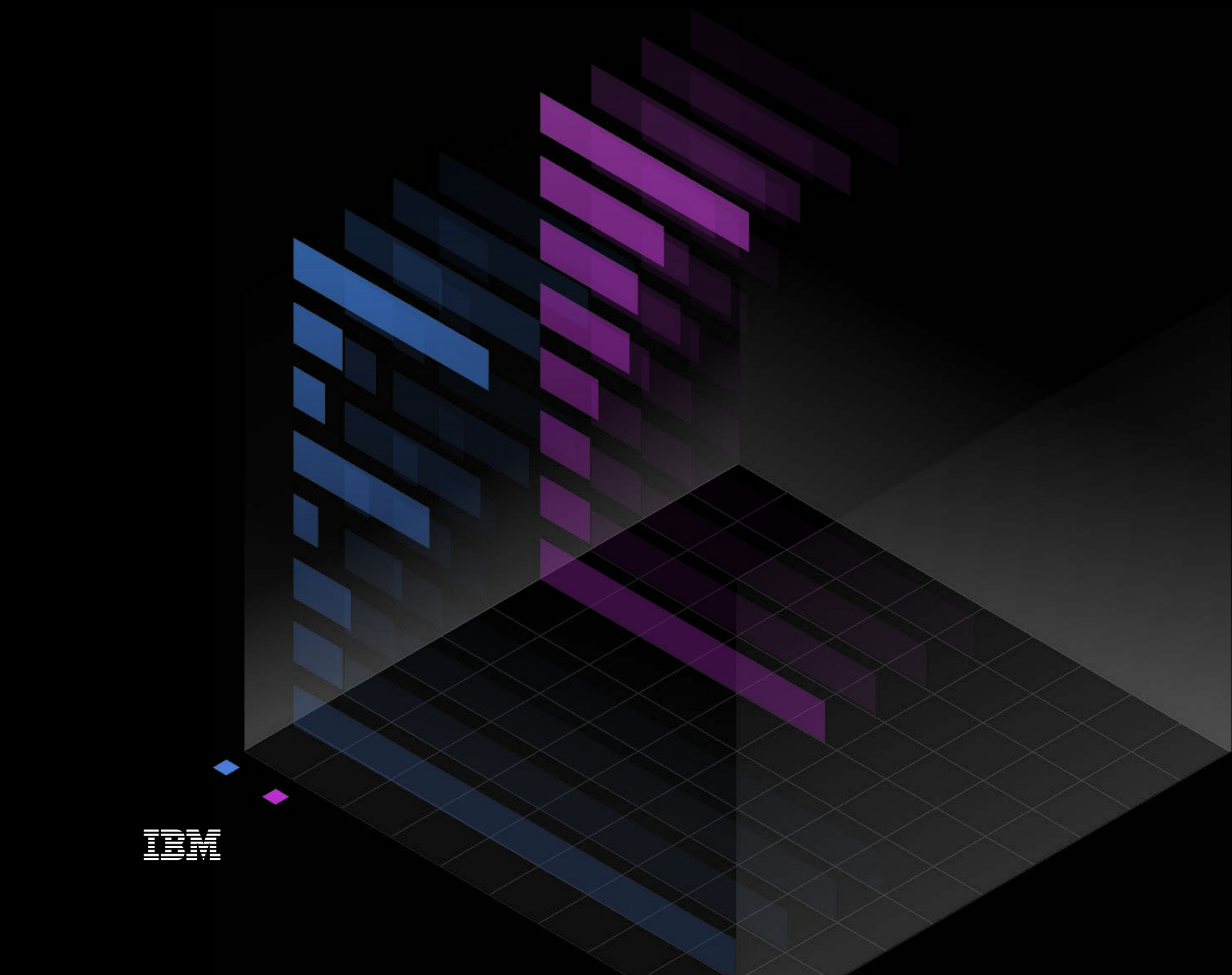
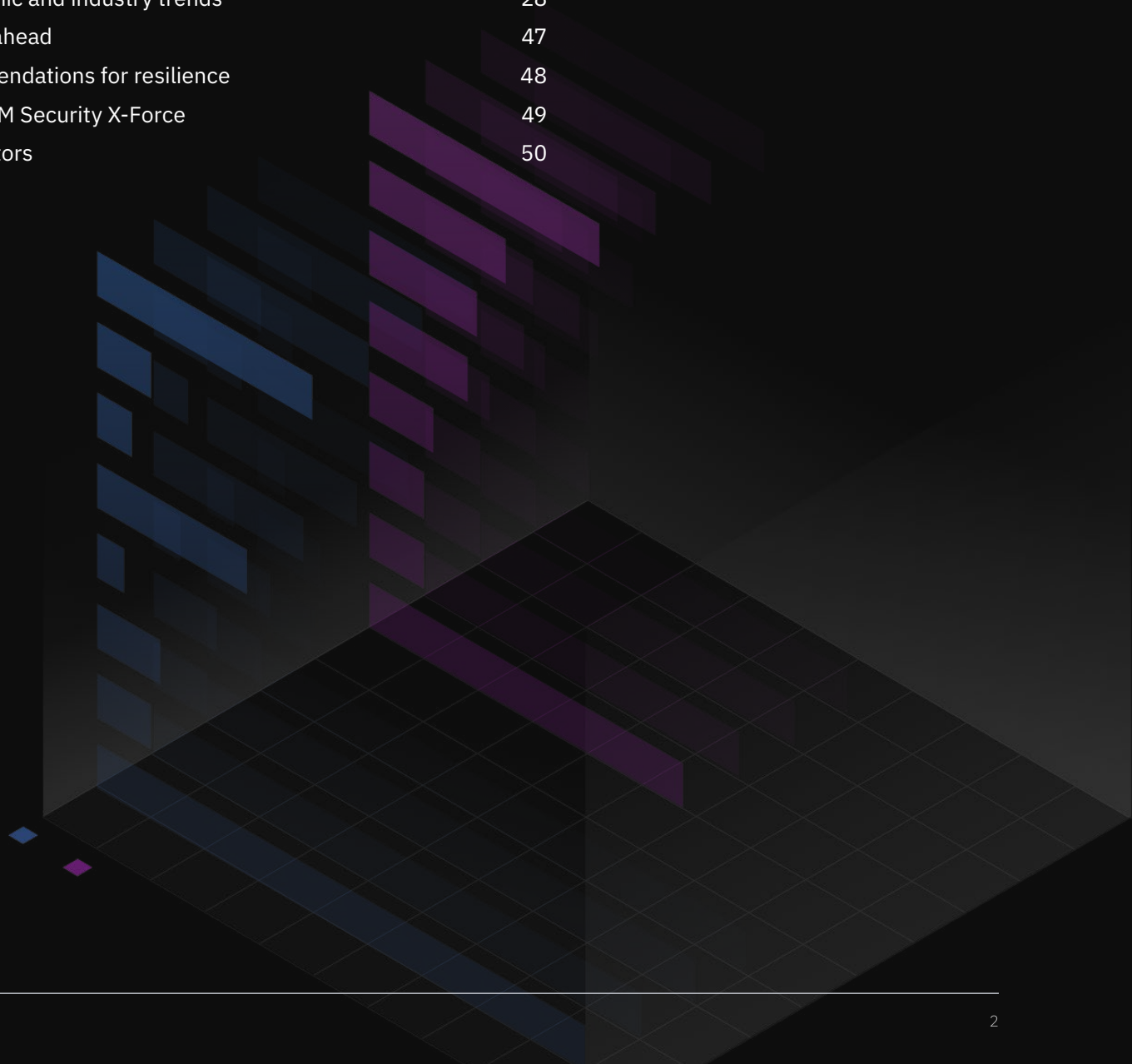
IBM Security

X-Force Threat Intelligence Index 2021



IBM

Contents



Introduction

The year 2020 was without a doubt one of the most consequential and transformational in recent memory: A global pandemic, economic turmoil impacting millions of people's lives, and social and political unrest. The reverberations from these events affected businesses in profound ways, with many making a major shift to distributed workforces.

In the cyber realm, the extraordinary circumstances in 2020 handed cyber adversaries opportunities to exploit the necessities of communication networks and provided rich targets in supply chains and critical infrastructure. The year ended as it began, with the discovery of a globally consequential threat that required rapid response and remediation. An attack which has largely been attributed to a nation state actor, which leveraged a backdoor in network monitoring software to attack government and private sector organizations, demonstrated how third-party risk should be anticipated, but can't be predicted.

To help meet the challenges of these times, IBM Security X-Force assesses the cyber threat landscape and assists organizations in understanding the evolving threats, their associated risk, and how to prioritize cybersecurity efforts. In addition to the premium threat intelligence we provide to customers, we analyze the wealth of data we gather to produce the X-Force Threat Intelligence Index, an annual check-in on the threat landscape and how it's changing.

Among the trends that we tracked, ransomware continued its surge to become the number one threat type, representing 23% of security events X-Force responded to in 2020. Ransomware attackers increased the pressure to extort payment by combining data encryption with threats to leak the data on public sites. The success of these schemes helped just one ransomware gang reap profits of over $123 million in 2020[1], according to X-Force estimates.

Manufacturing organizations weathered an onslaught of ransomware and other attacks in 2020. The manufacturing industry overall was the second-most targeted, after finance and insurance, having been the eighth-most targeted industry in 2019. X-Force discovered sophisticated attackers using targeted spear phishing campaigns in attacks against manufacturing businesses and NGOs involved in the COVID-19 vaccine supply chain.

1. All cost totals in the report are in U.S. dollars.

Threat actors were also innovating their malware, particularly malware that targeted Linux, the open source code that supports business-critical cloud infrastructure and data storage. Analysis by Intezer discovered 56 new families of Linux malware in 2020, far more than the level of innovation found in other threat types.

There is reason to hope that 2021 will shape up to be a better year. Trends are notoriously hard to predict, but the one constant thing we can rely on is change. Resilience in the face of rising and falling challenges in cybersecurity requires actionable intelligence and a strategic vision for the future of a more open, connected security.

In the spirit of strength through community, IBM Security is pleased to offer the 2021 X-Force Threat Intelligence Index. The findings in this report can help security teams, risk professionals, decision-makers, researchers, the media and others, understand where threats have been in the past year and help prepare for whatever comes next.

Executive summary

IBM Security X-Force drew on billions of data points collected from our customers and public sources between January and December 2020 to analyze attack types, infection vectors, and global and industry comparisons. The following are some of the top findings presented in the X-Force Threat Intelligence Index.

23%

Ransomware share of attacks

Ransomware was the most popular attack method in 2020, making up 23% of all incidents IBM Security X-Force responded to and helped remediate.

$123 million+

Estimated profits from top ransomware

X-Force conservatively estimates that Sodinokibi (also known as REvil) ransomware actors alone made at least $123 million in profits in 2020 and stole around 21.6 terabytes of data.

25%

Top vulnerability share of attacks in Q1 2020

Threat actors capitalized on a path traversal Citrix flaw, exploiting this vulnerability in 25% of all attacks in the first three months of the year and 8% of total attacks in all of 2020.

35%

Scan-and-exploit share of top infection vectors

Scanning and exploiting vulnerabilities jumped up to the top infection vector in 2020, surpassing phishing which was the top vector in 2019.

#2

Manufacturing rank in top attacked industries

Manufacturing was the second-most attacked industry in 2020, up from eighth place in 2019, and second only to financial services.

5 hours

Length of attack-training videos on a threat group server

Operational errors by Iranian nation-state attackers allowed X-Force researchers to discover around 5 hours of video on a misconfigured server, yielding insight into their techniques.

100+

Executives targeted in precision phishing campaign

In mid-2020, X-Force uncovered a global phishing campaign that reached more than 100 high ranking executives in management and procurement roles for a task force acquiring personal protective equipment (PPE) in the battle against COVID-19.

49%

ICS-related vulnerability growth rate, 2019-2020

Industrial control systems (ICS)-related vulnerabilities discovered in 2020 were 49% higher year-over-year from 2019.

56

Number of new Linux malware families

The number of new Linux-related malware families discovered in 2020 was 56, its highest level ever. This represented a 40% year-over-year increase from 2019.

31%

European share of attacks

Europe was the most-attacked geography in 2020, experiencing 31% of attacks observed by X-Force, followed by North America (27%) and Asia (25%).

Top attacks of 2020

Understanding the attack landscape can assist security teams in prioritizing resources, drilling for the most likely scenarios, and identifying shifts in attacker techniques.

The following sub-sections will provide insights on the top attack trends X-Force identified in 2020: ransomware is undeniably the top attack type, followed distantly by data theft and server access attacks. In terms of initial attack vectors, scan and exploit rose to first place in 2020, followed by phishing and credential theft.[2]

Top 3 attack types

1. Ransomware (23% of attacks)
2. Data theft (160% increase since 2019)
3. Server access (233% increase since 2019)

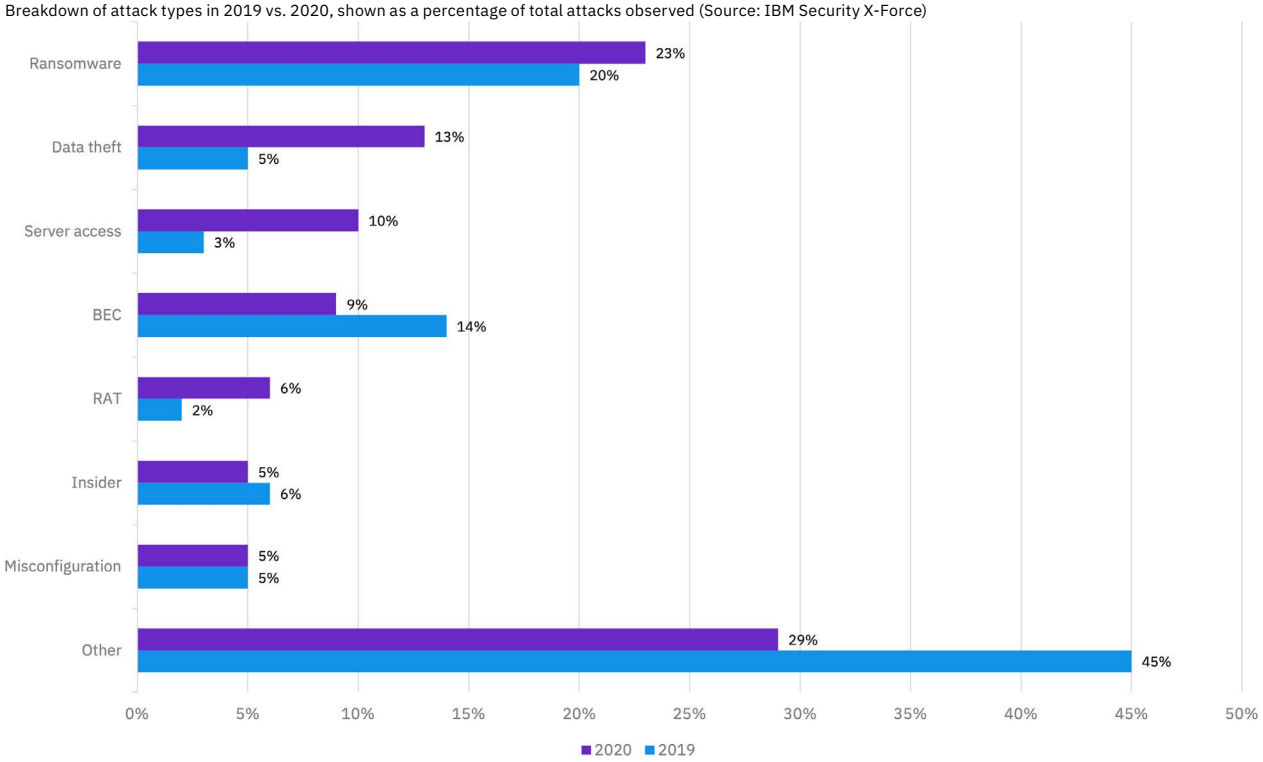
Top 3 initial attack vectors

1. Scan-and-exploit (35% of attacks vs. 30% in 2019)
2. Phishing (33% of attacks vs. 31% in 2019)
3. Credential theft (18% of attacks vs. 29% in 2019)

Figure 1

Top attack types, 2020 vs. 2019

Breakdown of attack types in 2019 vs. 2020, shown as a percentage of total attacks observed (Source: IBM Security X-Force)



2. “Attacks” and “incidents” are used interchangeably in this report. An incident refers to an organization’s hotline call to the X-Force Incident Response team that results in the investigation and/or remediation of an attack or suspected attack.

Ransomware business boomed

59%

of ransomware attacks used a double extortion strategy

$123 million+

Estimated profits made by Sodinokibi operators in 2020

Ransomware attacks made up 23% of all incidents observed in X-Force engagements in 2020, up from 20% the year prior, suggesting that more cybercriminals are finding ransomware to be profitable.

Threat actors carried out ransomware attacks predominantly by gaining access to victim environments via remote desktop protocol, credential theft, or phishing—attack vectors that have been similarly exploited to install ransomware in prior years.

Ransomware actors are finding greater success in attacks by expanding their attack chain. The most successful ransomware groups X-Force observed in 2020 were focused on creating ransomware-as-a-service (RaaS) cartels and outsourcing key aspects of their operations to cybercriminals that specialize in different aspects of an attack.

Fifty-nine percent of ransomware attacks used a double extortion strategy, according to X-Force incident response data. Since organizations can opt to recover from backups and not pay the ransom, attackers have shifted tactics to not only encrypt data and render it impossible to access. They also stole it, and then threatened to leak sensitive data if a ransom was not paid. Certain ransomware providers even held auctions on the dark web to sell their victims' stolen sensitive information.

In fact, X-Force's most conservative estimate places total Sodinokibi ransom revenue at $123 million in 2020 through the use of these extortion tactics. Ransomware developers have essentially found a way to circumvent organizations' reliance on backed up data, as they can use the threat of leaking data as leverage to extort payment.

The threat of reputational loss due to sensitive data being leaked has the potential to cause significant damage to the business and its customers, which could lead to lawsuits and hefty regulatory fines in addition to the costs of a lengthy recovery. When ransomware attackers publicly disclose sensitive data on leak sites, these breaches are often picked up by press, further adding to the reputational harm associated with these attacks. X-Force analysis of public breach data indicates that ransomware-related data leaks made up 36% of public breaches in 2020.

Sodinokibi most common ransomware type

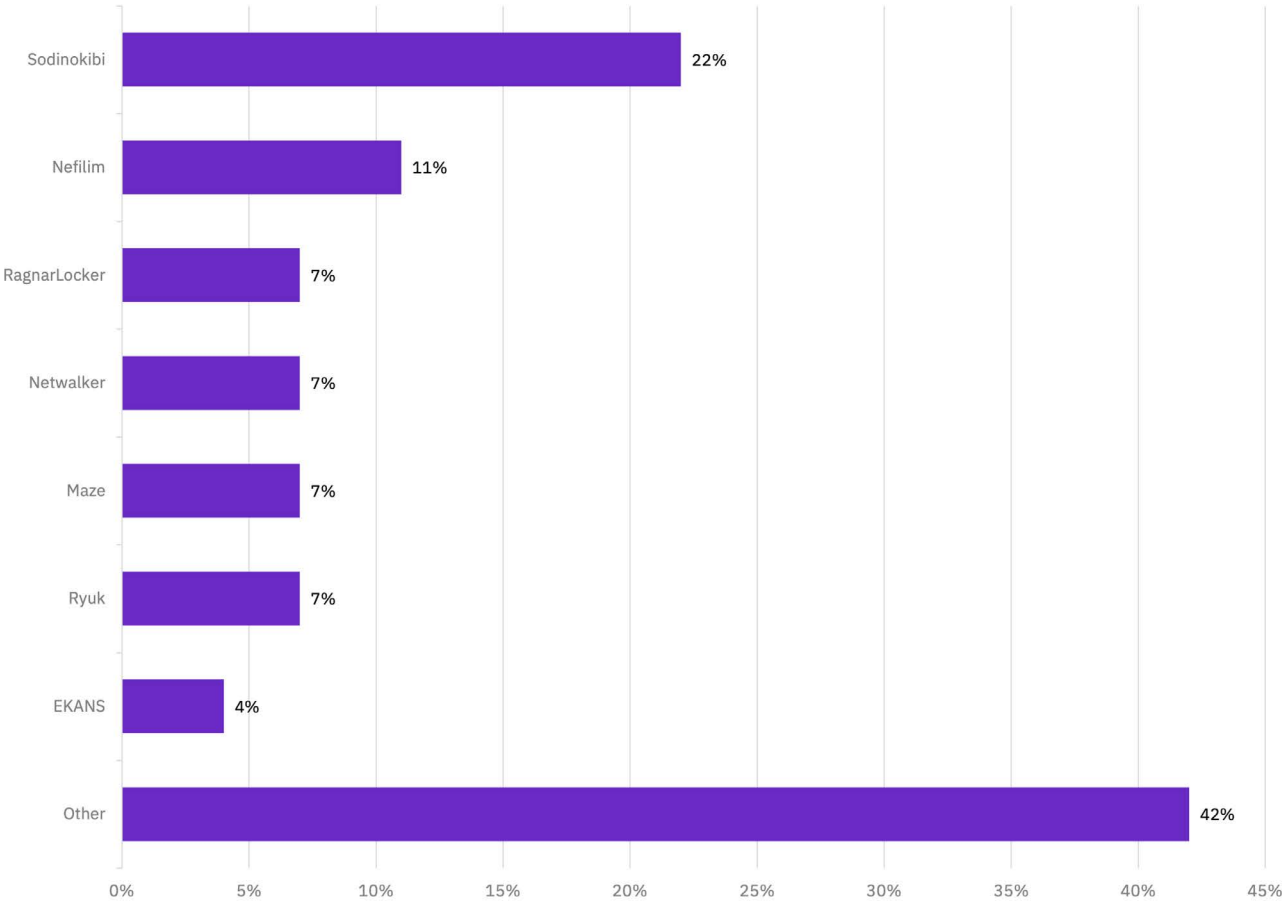
The top two ransomware types observed by X-Force in 2020 included Sodinokibi (22% of ransomware incidents) and Nefilim (11%) – both of which blend data theft with ransomware attacks.

Additional ransomware types frequently seen by X-Force were RagnarLocker (7%), Netwalker (7%), Maze (7%), Ryuk (7%) and EKANS (4%), while the remaining 42% of ransomware attacks were comprised of small samples of other types such as Egregor, CLOP, Medusa and others.

Figure 2

Top ransomware types

Percentage breakdown of ransomware types observed in 2020 (Source: IBM Security X-Force)



As Sodinokibi was the most common ransomware type X-Force observed in 2020, we gathered an appreciable amount of data and insight on these attacks and tracked them closely—not only Sodinokibi attacks on IBM clients, but all of the group's claimed attacks.

Several patterns from this research have emerged:

— Sodinokibi ransomware attacks peaked in June or July 2020 and then rose again after a brief lull in August and September, potentially related to threat actor availability, vacations, and alternate employment obligations.

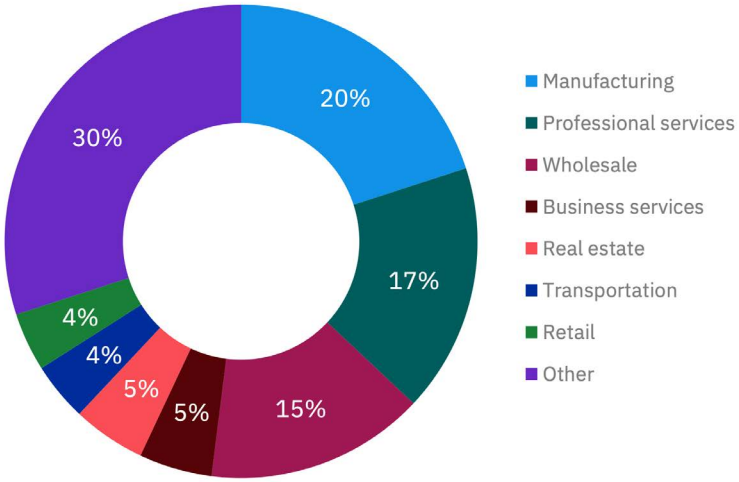
— Manufacturing, professional services and wholesale were the most commonly targeted industries by Sodinokibi, potentially because Sodinokibi actors assessed organizations in these industries have a low tolerance for downtime—perhaps especially during the pandemic—or house especially sensitive data. *(see figure 3)*

— Ransom demands from Sodinokibi tended to be around 1% - 5% of the victim organization's total yearly revenue, and in one case was $42 million.

Figure 3

Sodinokibi ransomware attacks by industry

Percentage breakdown by industry of Sodinokibi ransomware attacks observed in 2020
(Source: IBM Security X-Force)



Sodinokibi ransomware by the numbers

Most targeted geographies

1. United States (58%)
2. UK (8%)
3. Australia (5%)
4. Canada (3%)

Estimated revenue
2020 total: $123 million+
August 2020 alone: $55 million

Total estimated data theft:
21.6 terabytes

Nearly two-thirds of Sodinokibi victims in 2020 paid a ransom and around 43% had their data leaked, according to X-Force estimates.

Recommendations for responding to a ransomware attack

Preparation is key: Implement and practice a response plan for a ransomware attack, including blended ransomware and data theft extortion techniques.

Safely store data backups offline: Backups can enable your organization to quickly and independently recover from a ransomware attack.

Implement defense-in-depth: Use a multi-faceted approach, such as employing multifactor authentication on every access point into a network, ensuring endpoint visibility, proactive threat hunting, performing regular penetration tests to identify weak points in a network, and quickly patching and mitigating known vulnerabilities.

The Definitive Guide to Ransomware

Register to download the whitepaper >

Data theft

Data theft—or an attacker taking sensitive victim data—accounted for 13% of attacks remediated by X-Force in 2020, increasing significantly from 5% of attacks in 2019.

A flurry of Emotet malware attacks in September and October 2020 accounted in large part for the significant increase in data theft attacks—these Emotet attacks, largely in Asia, made up 46% of the data theft activity X-Force remediated in 2020.

Manufacturing bore the brunt of data theft attacks in 2020, experiencing 33% of all data theft incidents. Energy came in second, at 21% of attacks, with finance and insurance third at 17% of data theft attacks.

Server access attacks

Server access was the third most common attack type in 2020, accounting for 10% of all attacks remediated by X-Force Incident Response in 2020. A server access attack involves a threat actor gaining unauthorized access to a victim's server, either by exploiting stolen server credentials, exploiting a vulnerability, or other means.

Nearly 36% of the server access attacks X-Force Incident Response observed in 2020 targeted the finance and insurance sector, with business services (14%), manufacturing (7%) and healthcare (7%) also getting hard hit.

Threat actors' successful exploitation of CVE-2019-19781, a path traversal Citrix flaw, drove the trend of server access attacks.

Citrix vulnerability CVE-2019-19781

X-Force data indicated that 15% of incidents in the first half of 2020 were directly related to Citrix vulnerability CVE-2019-19781 – over 15 times more than any other vulnerability. This vulnerability, disclosed in December 2019, affects the Citrix Application Delivery Controller (ADC), Citrix Gateway, and NetScaler Gateway. The vulnerability allows an attacker to perform arbitrary code execution on a vulnerable Citrix server.

Exploitation by the numbers: CVE-2019-19781

- 59% of all incidents in January 2020
- 25% of all incidents in Q1 2020
- 15% of all incidents in the first half of 2020
- 8% of total incidents X-Force remediated in 2020
- 25,000+ known vulnerable Citrix servers

Multiple groups seize on Citrix vulnerability

X-Force was aware of multiple threat actor groups taking advantage of CVE-2019-19781 in 2020, to include state-sponsored threat groups as well as financially motivated cybercriminals. These include:

— Hive0088 (AKA APT41; suspected Chinese state-affiliated)

— ITG07 (AKA Chafer, alleged Iran state-affiliated)

— Sodinokibi (AKA REvil) ransomware actors

— Maze ransomware actors

Gaining access to systems through this vulnerability, attackers in various cases installed remote access trojans (RATs) such as Adwind, deployed Trickbot and Cobalt Strike intermediate malware, and even deployed ransomware, including Sodinokibi and Maze. Some attackers also used it to gain access to networks for ransomware attacks.

Top 10 most exploited vulnerabilities of 2020

The following is a list of the top 10 vulnerabilities exploited in 2020. Of note, just two of the vulnerabilities on this list were actually disclosed in 2020, underscoring the continuing threat from old vulnerabilities. Throughout 2020, threat actors were more likely to exploit a vulnerability from 2019 or earlier, probably based on the difficulty associated with exploiting many of the vulnerabilities revealed in 2020 and the difficulty in patching older vulnerabilities that many organizations encounter.

1. **CVE-2019-19871**: Citrix Application Delivery Controller
2. **CVE-2018-20062**: NoneCMS ThinkPHP Remote Code Execution
3. **CVE-2006-1547**: ActionForm in Apache Software Foundation (SAF) Struts
4. **CVE-2012-0391**: ExceptionDelegator component in Apache Struts
5. **CVE-2014-6271**: GNU Bash Command Injection
6. **CVE-2019-0708**: “Bluekeep” Microsoft Remote Desktop Services Remote Code Execution
7. **CVE-2020-8515**: Draytek Vigor Command Injection
8. **CVE-2018-13382** and **CVE-2018-13379**: Improper Authorization and Path Traversal in Fortinet FortiOS
9. **CVE-2018-11776**: Apache Struts Remote Code Execution
10. **CVE-2020-5722**: HTTP: Grandstream UCM6200 SQL Injection

Top infection vectors

Driven by the heavy exploitation of CVE-2019-19781, scanning and exploiting vulnerabilities jumped into first place as the most common initial infection vector employed by threat actors, at 35% of all incidents with a known attack vector[3] remediated by X-Force. In comparison, scan and exploit acted as an infection vector for only 30% of attacks the year prior.

Scan and exploit attacks generally require few resources and can be automated and scaled to target a wide variety of victims, which may account for why this vector saw such a high volume in 2020. In addition to the path traversal vulnerability in Citrix, scan and exploit attacks in 2020 included targeting of the Heartbleed vulnerability, vulnerable or misconfigured management protocols, and exploitation of the cryptographic vulnerability CVE-2017-9248.

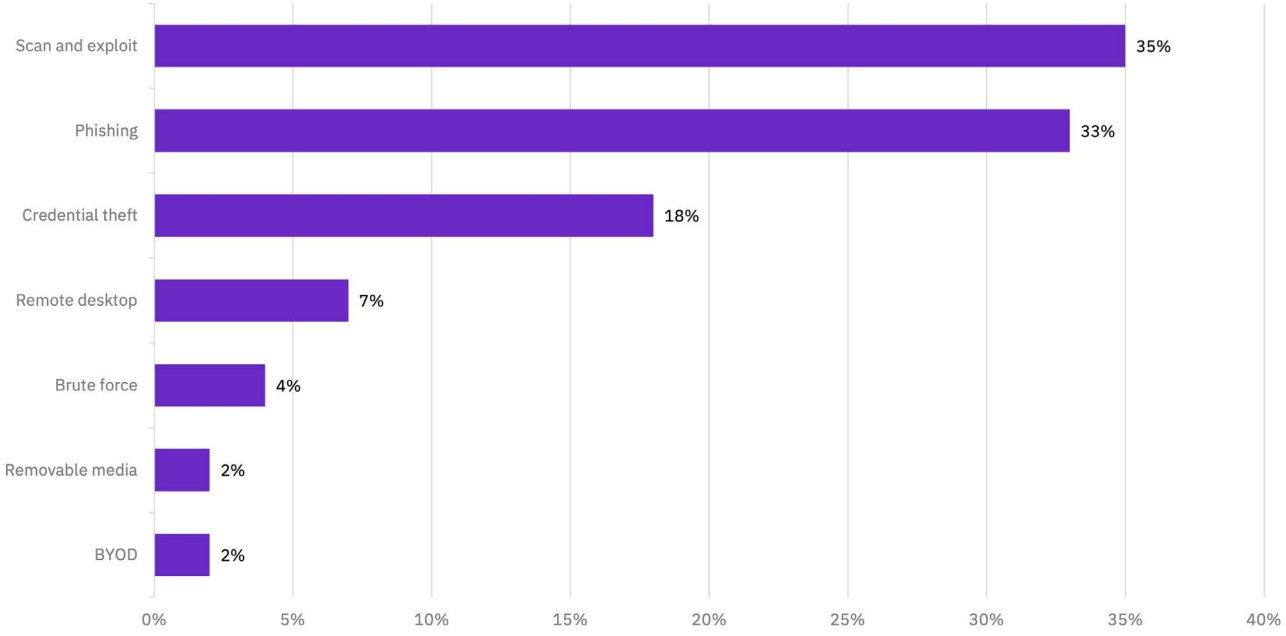
Phishing was the second most commonly used infection vector, employed in 33% of attacks—slightly up from 31% last year—suggesting that attackers' changing techniques and defensive mechanisms against phishing are keeping pace.

Credential theft accounted for only 18% of attacks, a significant drop from 29% last year, suggesting that threat actors are using scan and exploit techniques in place of credential theft for many compromises in 2020, most likely due to greater success rates for scan and exploit attacks.

Figure 4

Top initial attack vectors

Percentage breakdown of seven initial attack vectors observed by IBM Security X-Force Incident Response in 2020 (Source: IBM Security X-Force)



3. Several incidents had no known attack vector, and so are not included in this data.

Advanced threat actors

Throughout 2020, X-Force observed some threat groups making operational errors, thus unwittingly showing their hand and providing valuable insights to X-Force researchers. In other cases, tracking advanced threat actors yielded valuable insight into COVID-19-related threats, including how threat actors target vaccine distribution and continue to capitalize on the pandemic for phishing lures.

Iranian threat groups caught red handed

In September 2020, X-Force analysts found infrastructure associated with Hive0082 phishing activity. Hive0082, also referred to as Silent Librarian, COBALT DICKENS or TA407, has been actively targeting global academic institutions since at least 2013 despite multiple public disclosures of their activity.

The September 2020 activity did not widely differ from prior operations; however, operators left metadata from tooling used to spoof the valid login pages of the academic resources being targeted. Specifically, X-Force researchers noted the continued use of the "Single File" chrome extension in these campaigns which can capture the time stamp of the machine copying a website. Several of the spoofed websites used in this campaign contained "Iran Daylight Time" timestamps, a likely error on behalf of the Hive0082 operator. *(see figure 5)*

Figure 5

Hive0082 phishing activity

Metadata from Hive0082 spoofed webpage showing Iran Daylight Time timestamp (Source: IBM Security X-Force)

```
</script>
<!--
Page saved with SingleFile
url: [redacted]
saved date: Mon Apr 08 2019 13:20:57 GMT+0430 (Iran Daylight Time)
-->
```

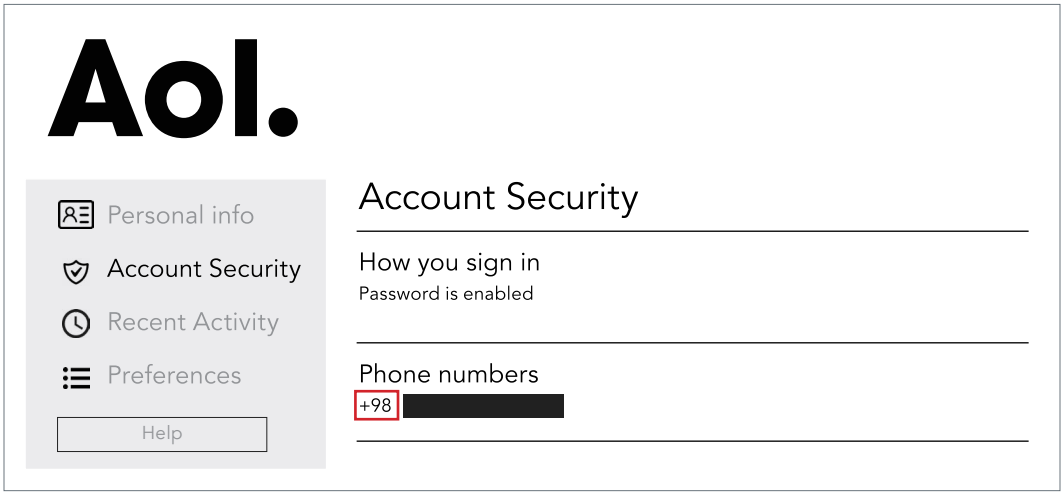
In an additional example, the mistakes of another Iranian state-sponsored threat group X-Force tracks as ITG18 provided unprecedented insight into their operations. The group has a history of operational security mistakes, specifically basic server configuration errors that in the past have resulted in the disclosure of their victims and in one case, ransomware on one of their operations servers.

In May 2020, X-Force discovered another misconfigured server belonging to ITG18 that contained over 40 gigabytes of video and data files. The videos detailed the steps and technology used by ITG18 to perform their reconnaissance operations against compromised accounts. The videos also contained metadata about their operations that inadvertently revealed ITG18 VPN infrastructure, threat actor phone numbers and several failed phishing attempts against US government targets.

Figure 6

ITG18 training AOL account

Misconfigurd ITG18 server revealed threat actor phone number associated with an AOL account used for training
(Source: IBM Security X-Force)



The insight gained from operational errors used by both of these groups allowed X-Force threat intelligence analysts to warn targets of ongoing activity, gain insight into training techniques and password stealing methodologies, and identify infrastructure being used in real time for malicious activities. This insight, in turn, has allowed us to better protect and warn a wide variety of potential victim organizations.

COVID-19 phishing campaigns

During the course of ongoing research on Coronavirus-related cyber activity, X-Force uncovered various COVID-19 related phishing campaigns by advanced threat actors against the COVID-19 supply chain.

Attacks on vaccine cold chain

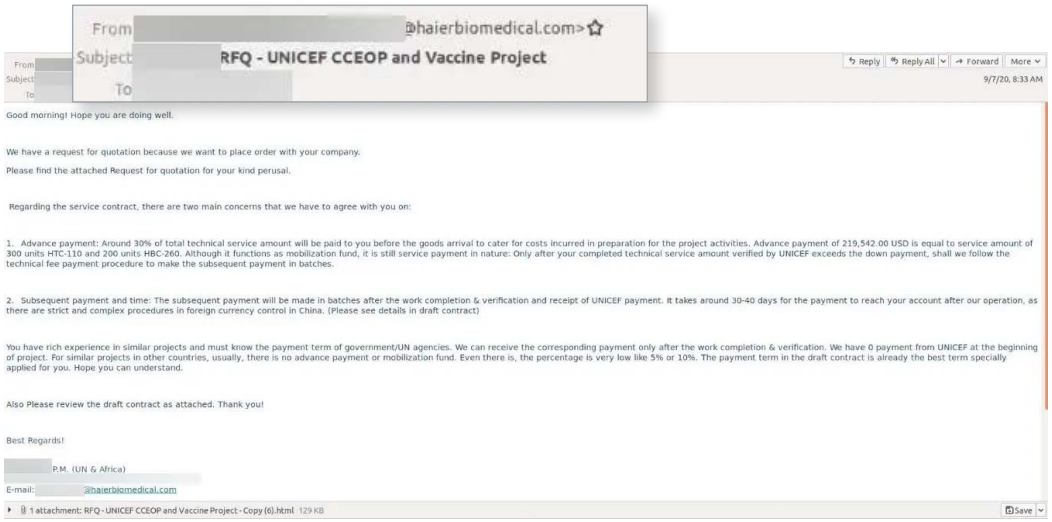
In October 2020, X-Force Threat Intelligence observed a wave of phishing emails targeting individuals, organizations and supranational entities having a potential interest in technologies associated with the safe distribution of a COVID-19 vaccine. The uncovered activity imitates the United Nations Children's Fund's (UNICEF) and Gavi Vaccine Alliance Cold Chain Equipment Optimization Platform (CCEOP) used to distribute vaccines globally. While currently unattributed, nation state-sponsored attackers were potentially behind these attacks.

This was a well calibrated phishing campaign designed by an adversary who was likely seeking to gain advanced insight into transport and distribution processes of a COVID-19 vaccine, through credential harvesting. Targets included the European Commission's Directorate-General for Taxation and Customs Union, as well as organizations within the energy, manufacturing, website creation, and software and internet security solutions sectors. These are global organizations headquartered in Germany, Italy, South Korea, Czech Republic, greater Europe, and Taiwan.

Figure 7

COVID-19 vaccine phishing

Example of phishing email used in COVID-19 vaccine cold chain attacks
(Source: IBM Security X-Force)



PPE supply chain attacks

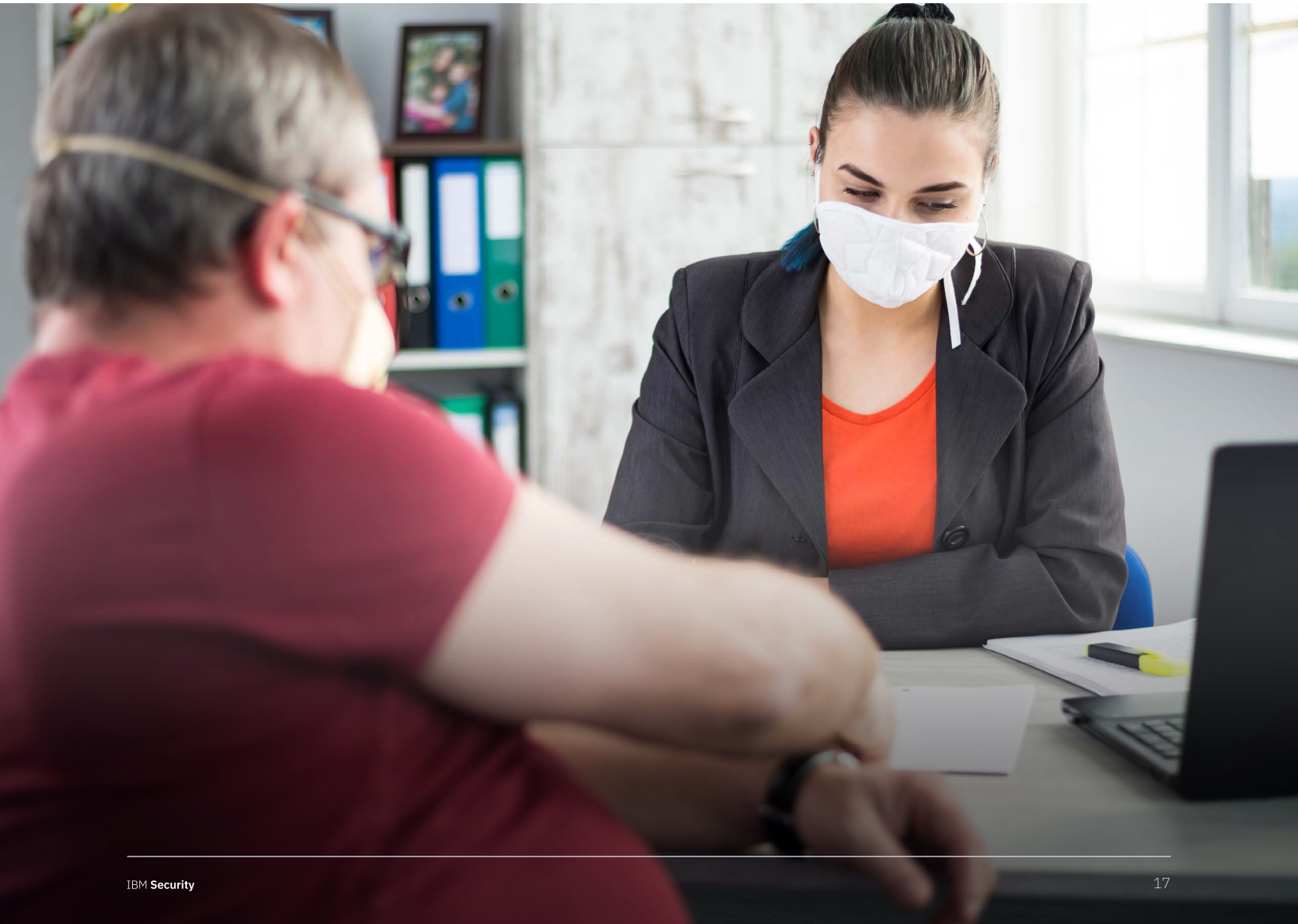
In May 2020, X-Force research uncovered targeting of a German multinational corporation associated with a German government-private sector task force to procure personal protective equipment (PPE). This discovery represents a precision-targeting campaign exploiting the race to secure essential PPE.

Threat actors behind this campaign targeted more than 100 high ranking executives in management and procurement roles within this organization and its third-party ecosystem. Overall, X-Force observed approximately 40 organizations targeted in this campaign. Given the extensive targeting observed of this supply chain, it's likely that additional members of the task force could be targets of interest in this malicious campaign, requiring increased vigilance.

Campaign targeting Ukraine

Separately, between mid-March and mid-April 2020, X-Force uncovered malicious .docx files likely attributed to ongoing suspected Hive0051 (aka Gamaredon) activity. This new activity appears to be consistent with Hive0051's established pattern of operations, which focuses on targeting entities based in Ukraine.

The contents of the malicious document files we uncovered used a mixture of COVID-19 and geopolitically themed lures spoofing Ukrainian government entities and NGOs. It's highly likely that the group was leveraging the ongoing geopolitical developments and current concerns surrounding the COVID-19 outbreak to exploit Ukraine's domestic population, or entities with a significant interest in regional developments.



Threats to OT and ICS

Operational technology (OT) threats have the potential to lead to real-world effects: chemical spills, machinery malfunctions, or even crashes of passenger vehicles. Thus, X-Force is prioritizing research and analysis on operational technology, using our proprietary data sources to provide unique insight into threats against organizations that include operational technology networks.

To examine attack patterns on OT in 2020, X-Force analysts tracked incidents at manufacturing, oil and gas, transportation, utilities, construction and mining organizations that had the potential to affect OT networks.

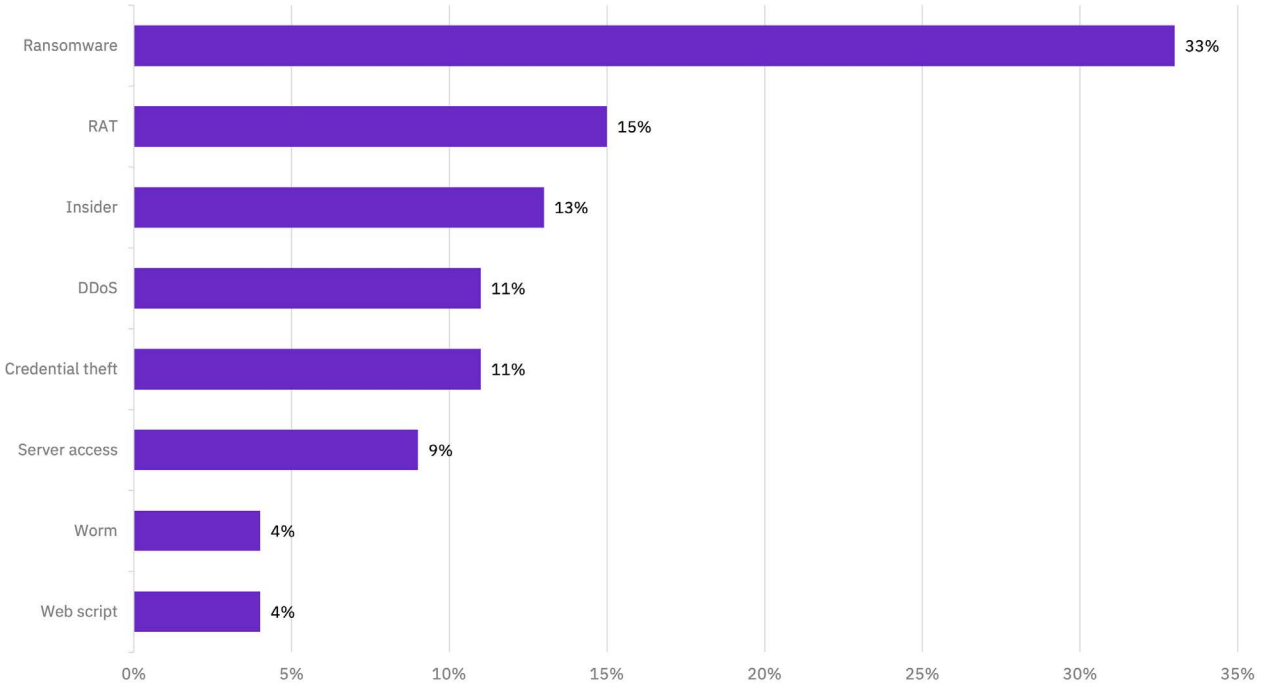
Ransomware

Ransomware attacks were the most common threat to OT from X-Force incident response data, echoing the overall attack trends X-Force observed in 2020. Ransomware attacks made up 33% of all attacks on OT in 2020. This trend suggests that threat actors may be finding organizations with OT networks to be particularly attractive for ransomware attacks. Of the ransomware attacks X-Force observed against OT organizations in 2020, EKANS, Nefilim, Medusa, PJX, and Egregor are some of the top ransomware strains.

Figure 8

Attack types against OT

Percentage breakdown of attack types observed in 2020 against organizations with OT (Source: IBM Security X-Force)



Remote access trojans

Remote access trojans (RATs) were the second most common attack type against OT in 2020, making up 15% of all attacks, according to X-Force incident response data. RATs allow a threat actor access to a device and enable covert surveillance on that device. Trickbot, Adwind, and jRAT are some of the RATs X-Force Incident Response observed on OT-connected networks in 2020.

Insider threats

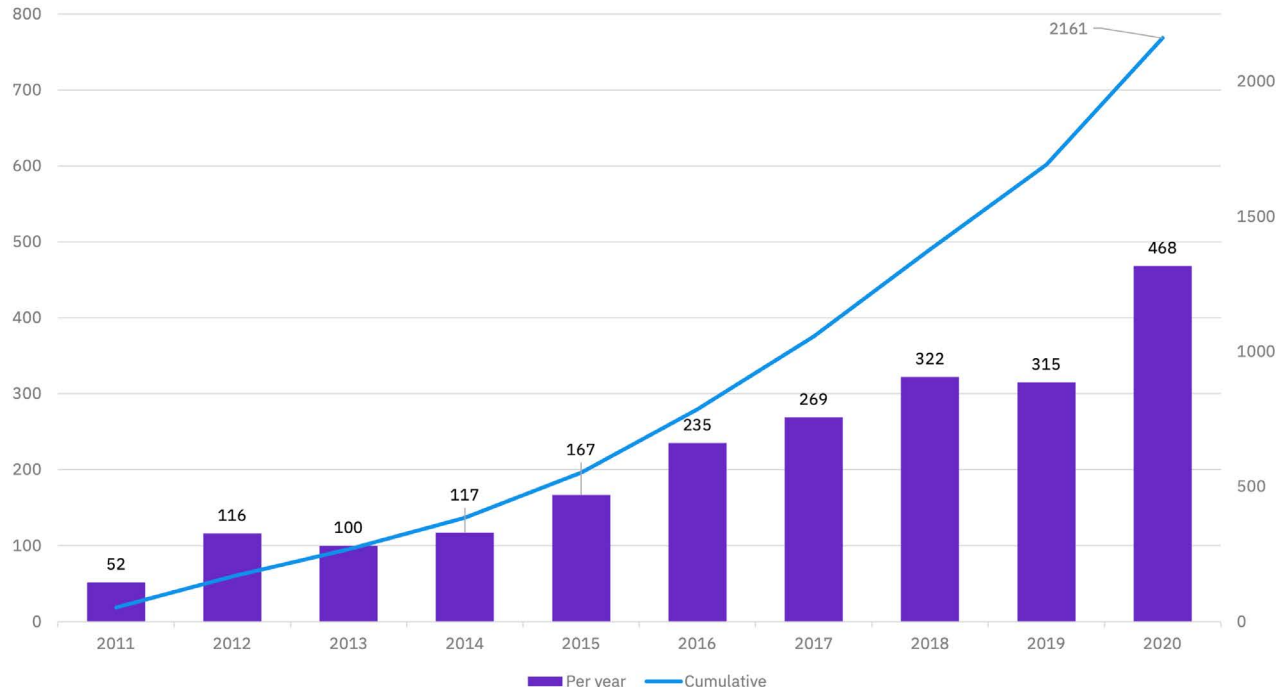
Insider incidents made up 13% of all OT-related incidents in 2020, with about 60% of those involving malicious insiders and about 40% involving negligence, according to X-Force data. Malicious insider incidents observed by X-Force included employees establishing connections to suspicious websites associated with malware, and employees potentially selling proprietary company information on third-party websites.

Vulnerabilities in industrial control systems

Figure 9

ICS vulnerabilities, 2011-2020

Number of disclosed vulnerabilities targeting ICS, per year and as a cumulative total of the years 2011-2020 (Source: IBM Security X-Force)



X-Force tracking reveals that vulnerabilities in ICS platforms continue to rise, reaching a new high in 2020, following a slight decrease the year prior. In fact, X-Force observed a 49% year-over-year increase in ICS vulnerabilities in 2020. ICS vulnerabilities are concerning as they increase risk for operational technology systems and have the potential to lead to destructive kinetic effects.

Top spoofed brands

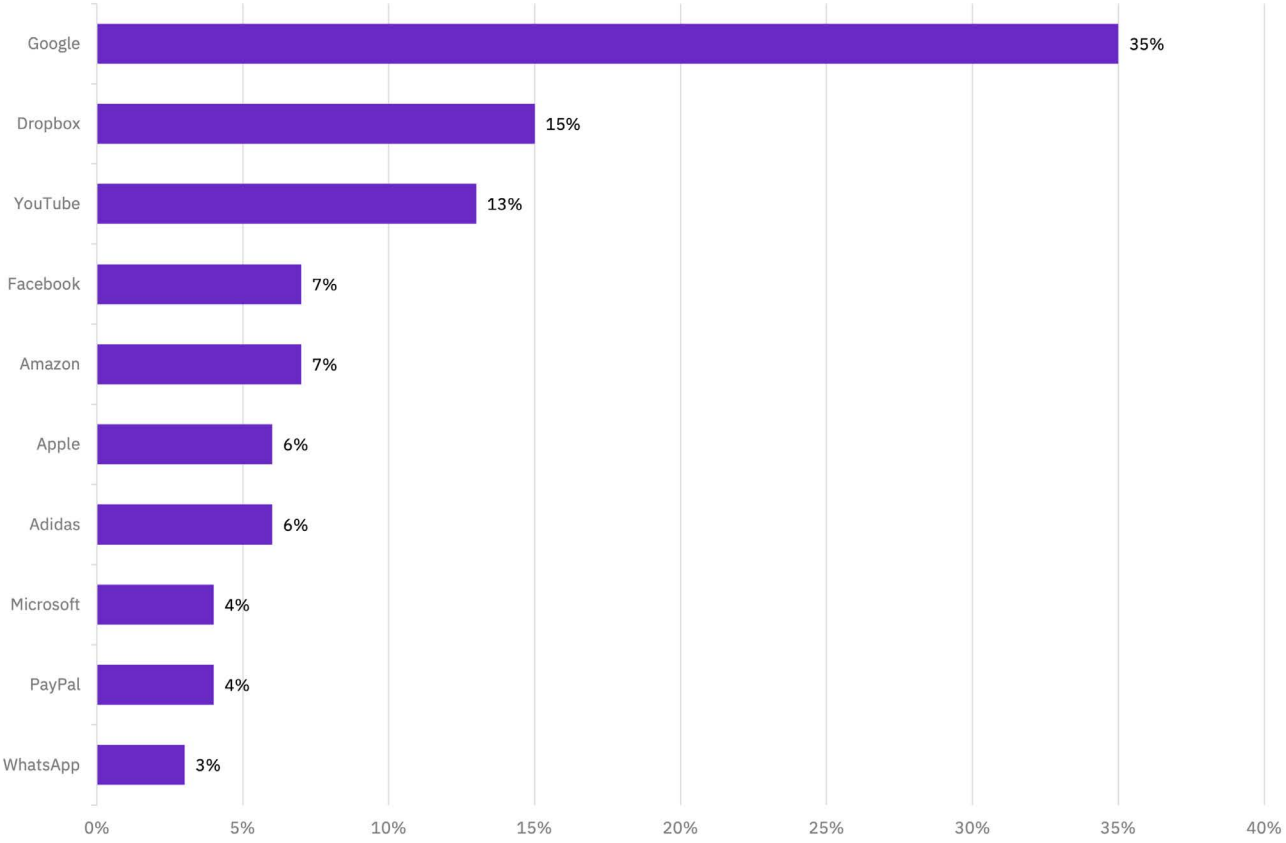
Quad9 data tracks malicious domains to warn and protect users from threat actor activity related to those domains. On average, Quad9 blocks 10 million malicious domain name system (DNS) requests every day, and IBM identifies malicious domains on average eight days earlier than other threat intelligence providers. X-Force is a Quad9 partner, helping organizations secure internet communications through trusted DNS.

Similar to 2019, X-Force and Quad9 continued to track the top spoofed brands used in malicious domains for 2020. These are brands that threat actors attempt to mimic, capitalizing on their popularity and trust with users to trick victims into opening an email, clicking on a link, or divulging sensitive information that can then be used in an attack.

Figure 10

Top 10 spoofed brands

Breakdown of the top 10 brands spoofed in spam in 2020, as a percentage of the 10 brands shown (Source: Quad9)



Technology and social media organizations continue to be at the top of the list for spoofed brands, with Google, Dropbox and YouTube leading in terms of the percentage of brands spoofed in 2020. Google continues to be the leading spoofed brand, following its top percentage in 2019. Adidas and PayPal also made it into the top 10 in 2020, along with several top spoofed brands from the year prior: Amazon, Apple, Microsoft and Facebook. The majority of Adidas spoofing activity occurred in January—suggesting it was unrelated to the pandemic—but appears to have been related to Superstar and Yeezy sneakers. PayPal's launch into the top 10 is most likely related to financially related cybercriminals seeking to steal credentials or funds.

Threat actors probably gravitate toward spoofing technology and social media organizations based on their popularity and users' expectation of accessing these assets digitally. In addition, spoofing email and email-associated platforms such as Google Gmail or Microsoft 365 is a common threat actor technique, judging from X-Force incident response data. These brands are also easily monetized by threat actors, as compromised accounts associated with these popular platforms can be easily sold on the dark web for a profit.

New malware threats

As threat actors continue to adjust, evolve, and transform malware, several malware development trends are emerging from the data. Above all others, the proliferation of malware targeting Linux was the dominant trend of 2020, followed closely by an increase in malware written using the Go programming language. A dramatic rise in Emotet malware in fall 2020 demonstrated a reemergence of the threat from this strain. Each of these trends points to one ultimate goal from threat actors: more effectively evading detection techniques.

Year of the Linux threat

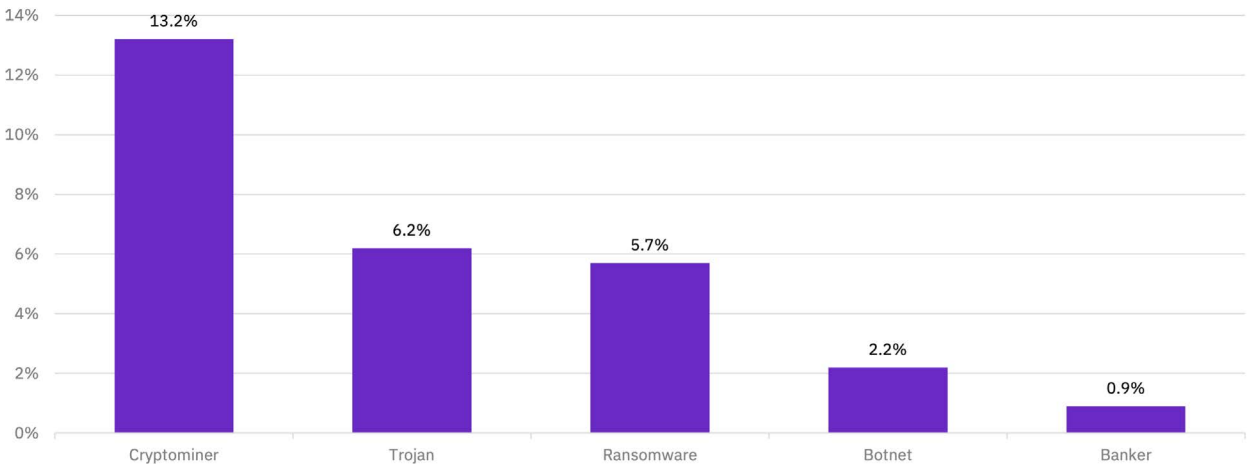
Researchers at Intezer—a malware code comparison company that collaborates with IBM Security—observed an increased effort by attackers to invest in crypto-miners and trojans, likely in an attempt to adapt to target more modern infrastructure such as the cloud—where Linux already powers 90% of the workload and adoption has been accelerating even further due to the effects of COVID-19.

In 2020, attackers focused more of their effort on developing Linux crypto-miners and ransomware, likely due to more organizations transitioning their servers to the cloud and the expandable processing power that cloud environments provide. The graph in *figure 11* shows the average percentage of new code used to develop different types of Linux malware in 2020.

Figure 11

Level of new code innovation in Linux malware

Average percentage of new code used to develop Linux malware, by malware type, 2020 (Source: Intezer)

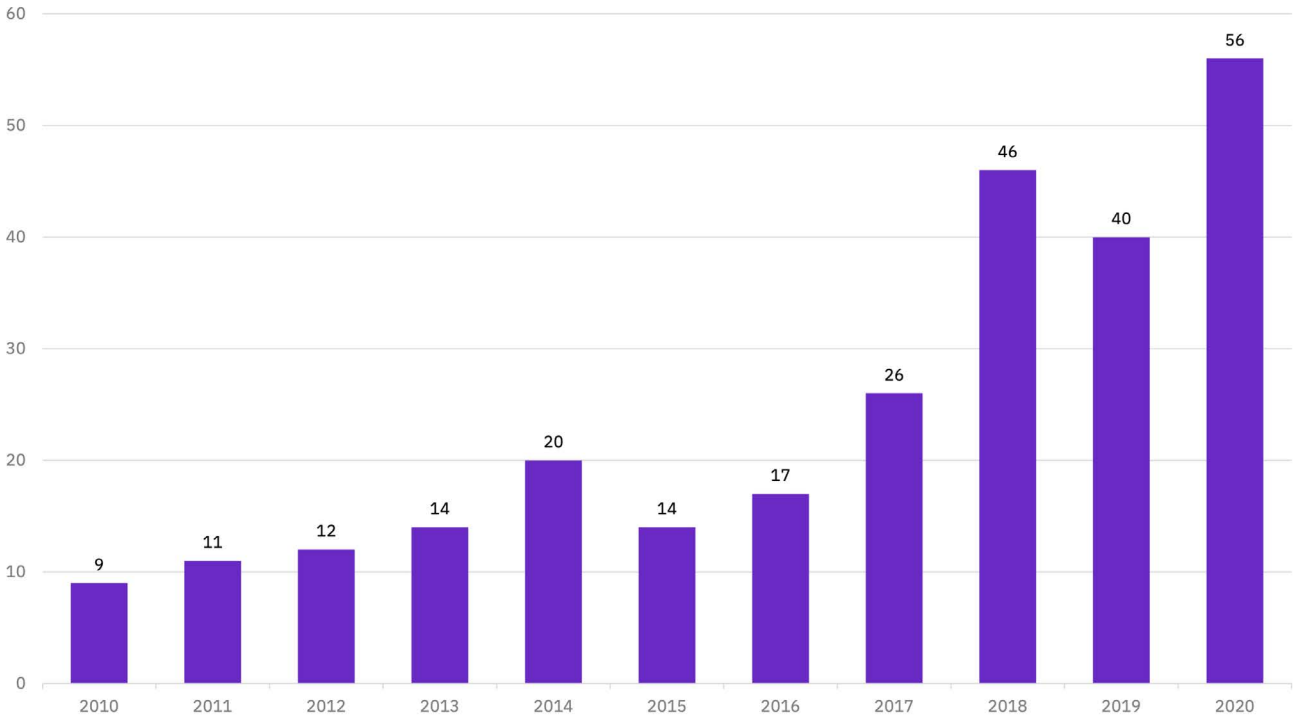


Since 2010, Intezer has observed a rise in new Linux malware families, with 2020 finding the highest count ever reported, at 56—a 40% year-over-year increase from 2019. There is a clear trend that highlights the increase in malware families entering the Linux threat landscape.

Figure 12

New Linux malware families, 2010-2020

Number of new Linux malware families per year (Source: Intezer)



X-Force malware reverse engineers likewise observed an increase in Linux malware in 2020 employed in IBM Security X-Force incidents. Near the beginning of 2020, multiple threat actors who were exploiting the path traversal flaw (CVE-2019-19871) were also developing malware to target vulnerable NetScaler devices such as NotRobin malware. Towards the second half of 2020, malware engineers observed several indications that threat actors that had previously focused on Windows malware were now including Linux malware in their arsenal.

For example, IBM Security X-Force observed Linux ransomware variants during Incident Response engagements that had previously only been seen targeting Windows systems. These include a Linux variant of the Defray911/RansomEXX ransomware, and a Linux variant of the SFile ransomware.

New ‘Go-to’ language

Throughout 2020, X-Force malware reverse engineers have increasingly noted threat actors’ use of Go (short for Golang) programming language to create new malware. The Go programming language is an open-source language similar to C, designed to enhance programming productivity and was released in 2012.

Throughout 2020, malware written in Go increased 500% from January to its peak in June and continued to be frequently used through the end of the year, underscoring the growing popularity of this programming language for threat actors. In contrast, we saw very few malware samples written in Go in 2019. We observed Go used frequently in 2020 for ransomware, and it appears to be popular among threat actors targeting OT networks, in addition to being used by multiple threat actors with a wide variety of targets.

Attackers write in Go because it is so easy to deploy in multiple systems. Instead of writing separate malware for Linux or Windows or OS X, Go allows the attacker to write the malware once, and then compile the same source code for a wide variety of platforms. This results in malware that can be run on a range of different operating systems.

Go binaries also help to avoid detection by creating a single “package”. Unlike malware written in other languages, Go-based malware can statically link all of their libraries inside the code. This means the malware can operate independently, without any additional droppers or sideloading required, making it easier to evade anti-virus detection. However, the same feature also results in a very large binary, which might preclude Go malware from being used as a phishing attachment.

Intezer has also observed that several APT attackers are adopting Go as the programming language of choice to develop cross-platform malware that target both Windows and Linux systems:

— **APT28 (ITG05):** A Russian nation-state group. In December 2020 this group leveraged COVID-19 as phishing lures to deliver the Go version of Zebrocy malware.

— **APT29 (ITG11):** A separate Russian nation-state group. Intezer Analyze was able to identify a WellMail Linux variant because it shares code with the IOC in a UK report.

— **Carbanak (ITG14 or FIN7):** Large cybercriminal group. One Linux sample shares code with a Carbanak Windows sample from 2019, which is how it was identified by Intezer.

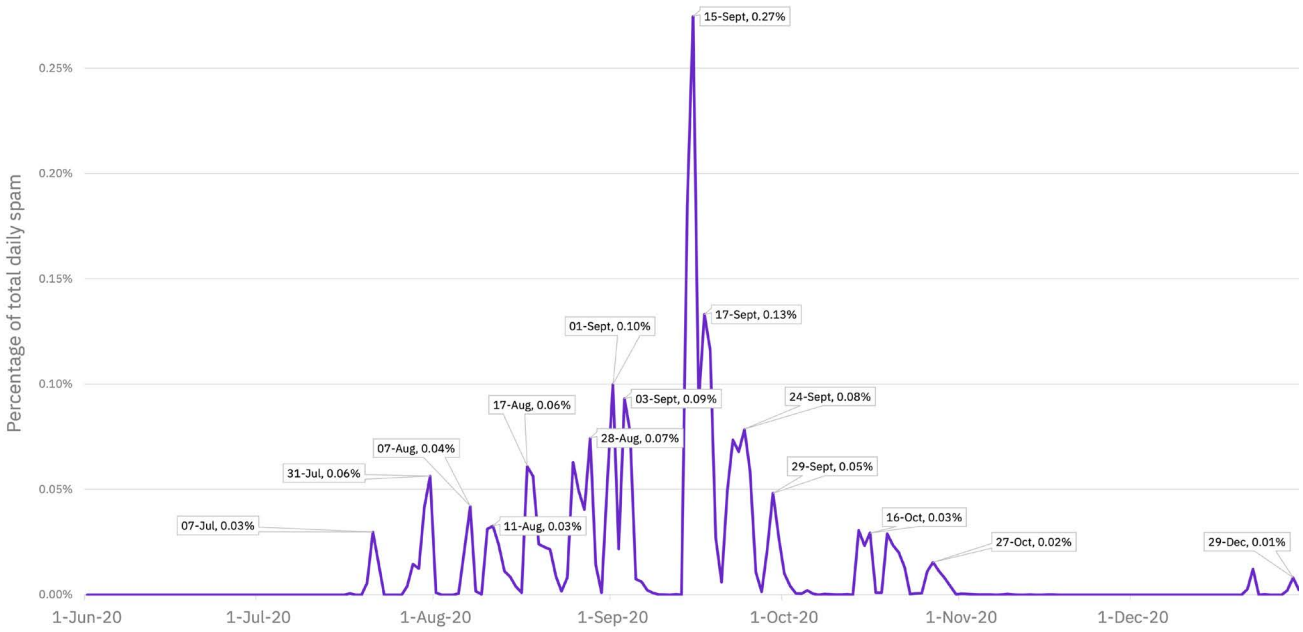
Emotet makes a comeback

IBM spam and phishing traps tracked Emotet closely in 2020 and detected a pronounced lull in the malware's activity in spring and early summer. The malware re-emerged in July 2020, however, and was very active throughout September and October, especially in Japan. Emotet malware operators probably took a hiatus to improve elements of the malware's detection evasion capabilities, based on X-Force observations of new anti-analysis capabilities.

Figure 13

Emotet spam trend, June-December 2020

Volume of daily Emotet spam as a percentage of total daily spam, June-December 2020 (Source: IBM Security X-Force)



Emotet is largely spread via spam campaigns. IBM spam traps observed all Emotet malware in 2020 spread through email attachments with Office Word malicious macros. The malware also appeared to be riding the wave of other spam campaigns such as standard casino spam or sextortion campaigns, forwarding these emails and then attaching a malicious payload. The Emotet malware can also read through and respond to legitimate email conversations with infected attachments, taking on a guise of legitimacy. IBM analysis has also revealed that the majority of Emotet spam is sent on working weekdays.

X-Force intelligence analysts uncovered new features in Emotet malware samples, such as anti-analysis capabilities. These updates indicate continued investment in Emotet by threat actors and that this malware family is likely to continue posing a threat to organizations globally.

Financial cybercrime

Financial malware in the cybercrime arena continues to pose a threat to financial and other organizations, as threat actors continue to innovate and new threats emerge. In 2020, IBM Trusteer observed cybercrime gangs use a highly automated process to empty bank accounts via mobile banking fraud, and remote overlay attacks became even more common in 2020, particularly in Europe.

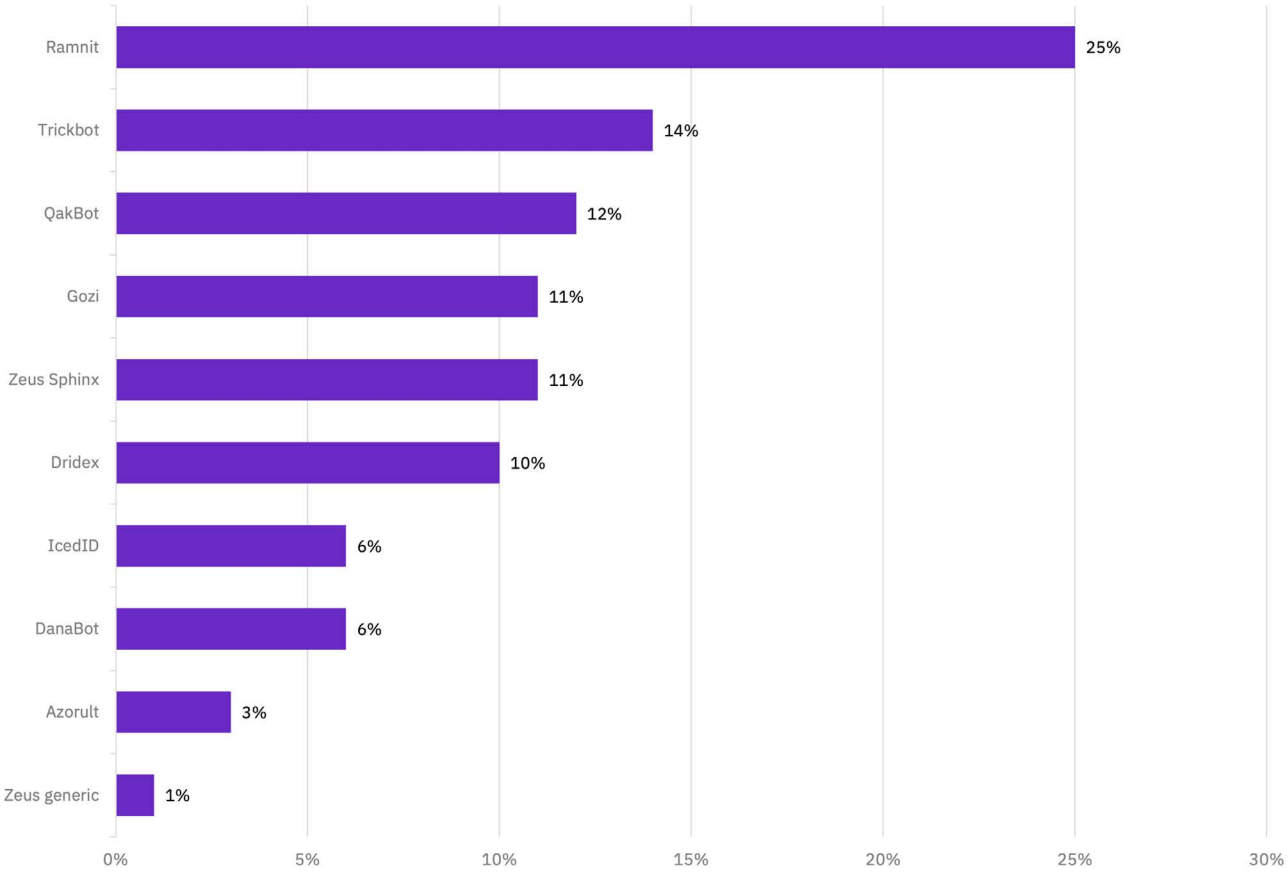
Top banking trojans

The top financial malware families of 2020 were more of the usual suspects, without surprises or any newcomers for the year. That is not to say that the existing financial cybercrime gangs did not evolve and add ways to attack and monetize crimeware over the year.

Figure 14

Top 10 banking trojan families

Breakdown of the top banking trojans in 2020, shown as a percentage of the top 10 (Source: IBM Trusteer)

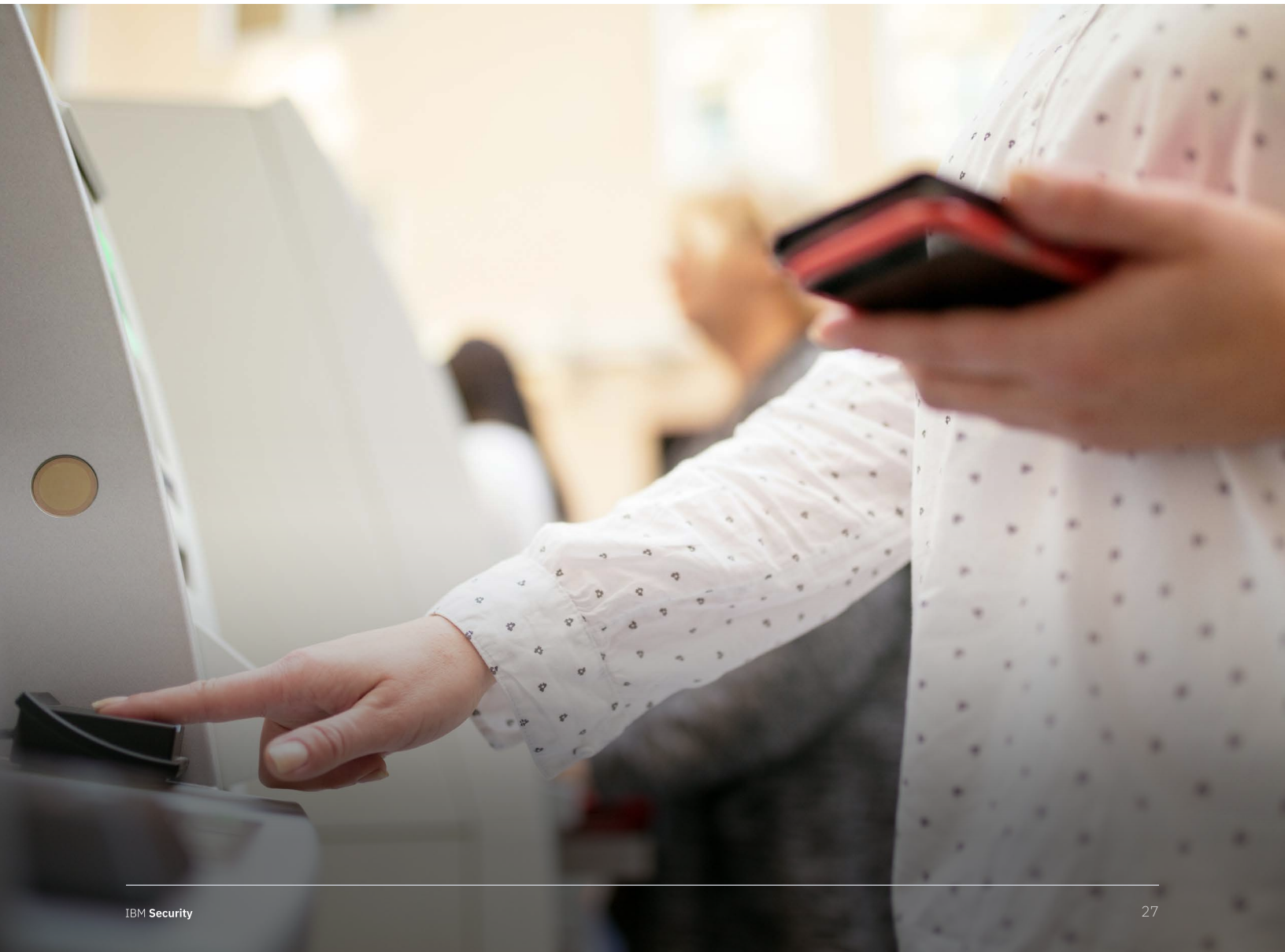


Banking trojan highlights

1. **Ramnit:** Moved up to number one from second place last year. This malware continues to be operated by a closed cybercrime gang, diversifying its monetization models and adapting to different target geographies. Attacks still focus on both consumers and business accounts.

2. **Trickbot:** Often found deploying Ryuk ransomware, this malware fell from the number one spot to number two most likely as a result of the short-lived takedown in October 2020. This malware originates from Eastern Europe, targeting businesses, business banking, and large companies.

3. **Qakbot:** In third place, this malware is spread to company networks by the Emotet botnet and in 2020 has featured attacks with the ProLock ransomware as a strategy to further monetize its footholds. This malware also originates from Eastern Europe, targeting businesses, business banking, and large companies.



Geographic and industry trends

Every geography and industry faces a unique attack landscape, as different threat actors, motivations, assets and geopolitical events drive activity in each region and industry. This section will provide a breakdown of the overall attack trends highlighted in this paper, discussing in greater detail how those trends and others affected each geography and industry.

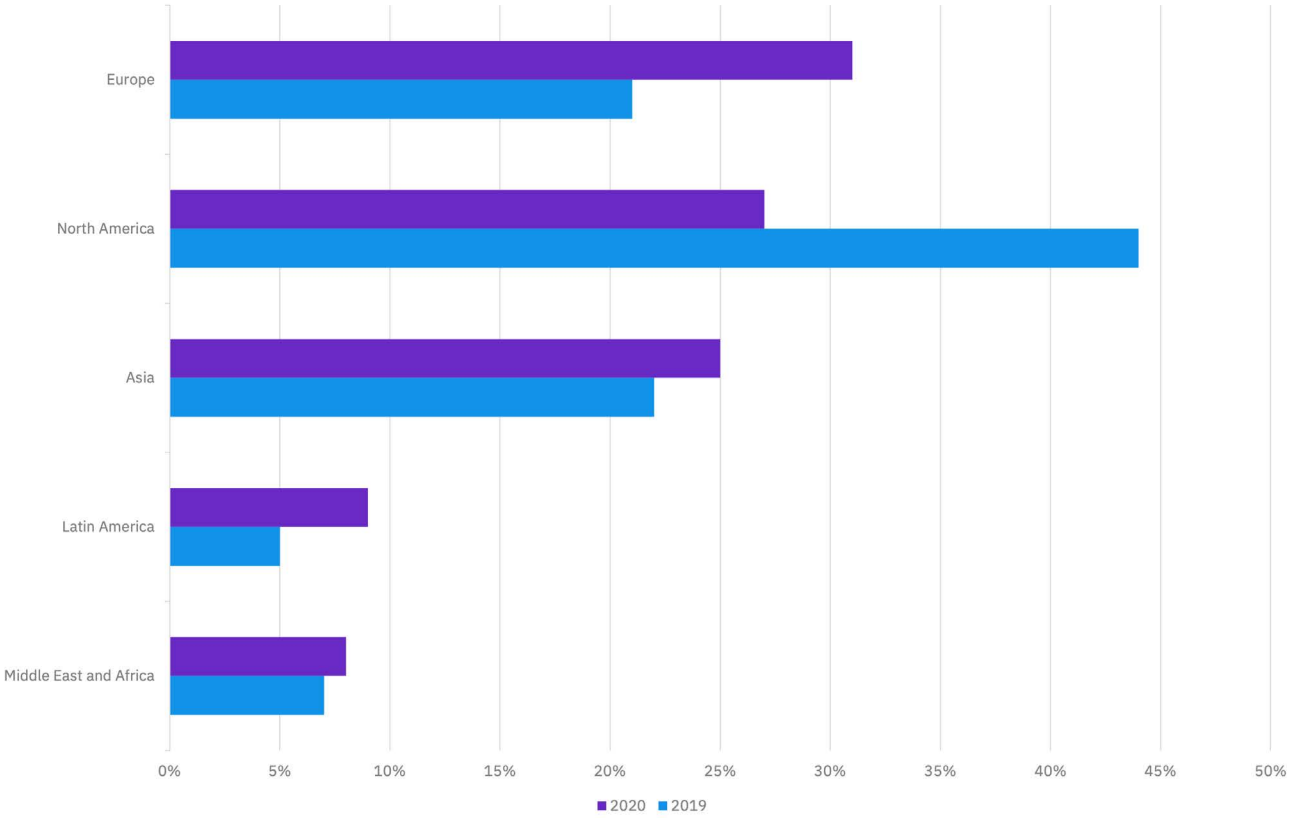
Geographic impact

Europe, North America and Asia suffered the bulk of attacks in 2020, attracting threat actor activity probably due to the high percentage of the world's wealth that circulates on these continents—over 89% of the world's gross domestic product (GDP). Of these three, attacks on European organizations grew the most, driven by ransomware, insider and server access attacks.

Figure 15

Geographic breakdown of attacks, 2020 vs. 2019

Geographic distribution of total attacks in X-Force incident response, 2020 vs. 2019 (Source: IBM Security X-Force)



Europe

— **Attack volume:** IBM Security X-Force observed that 31% of attacks in 2020 occurred in the European region, up significantly from 21% in 2019 and bumping Europe up to be the top-attacked geography worldwide in 2020.

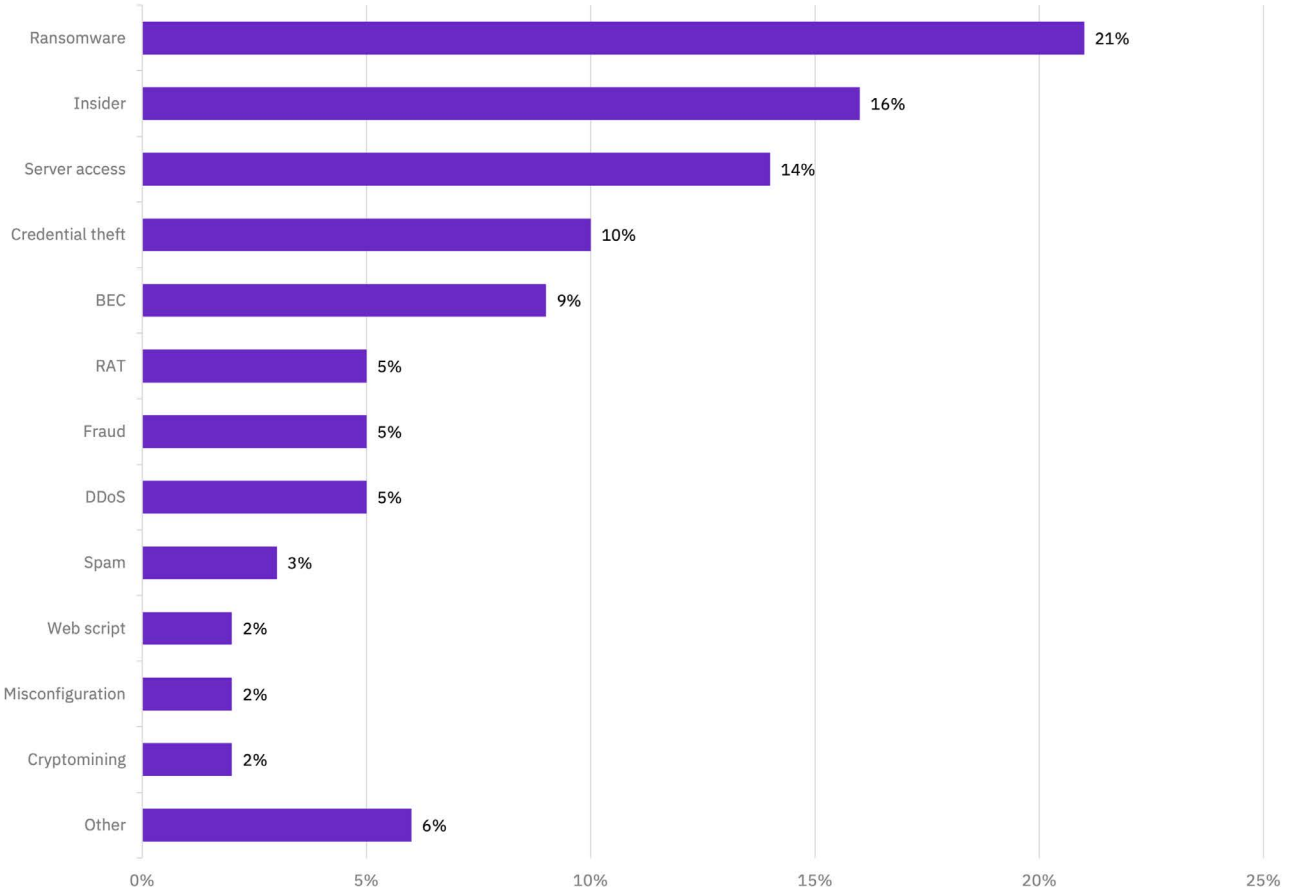
— **Attack types:** Ransomware was the top attack type for Europe in 2020, making up 21% of attacks—a significant volume, yet lower than the ransomware attack rate against North America. Europe by far experienced the most insider attacks in 2020, seeing twice as many such attacks as North America and Asia combined. Europe also experienced a high volume of server access attacks—14% of all attacks on the continent in 2020. Credential theft, business email compromise (BEC), remote access trojans (RATs), fraud and DDoS also affected European organizations in 2020 to a lesser extent. Europe experienced 33% of all attacks that exploited CVE-2019-19781 worldwide in 2020—higher than any other geography.

— **Countries under attack:** The United Kingdom, Switzerland, France and Italy were the most-attacked countries in Europe in 2020.

Figure 16

Europe attack types

Breakdown of total attacks on Europe by attack type, from X-Force incident response data, 2020 (Source: IBM Security X-Force)



North America

— **Attack volume:** North America experienced 27% of all attacks X-Force remediated in 2020, dropping the geography down to second-most attacked worldwide. This drop stands in stark contrast to 2019, when the region suffered 44% of all attacks. An increased attack rate in Europe and Asia are the most significant contributors to this shift.

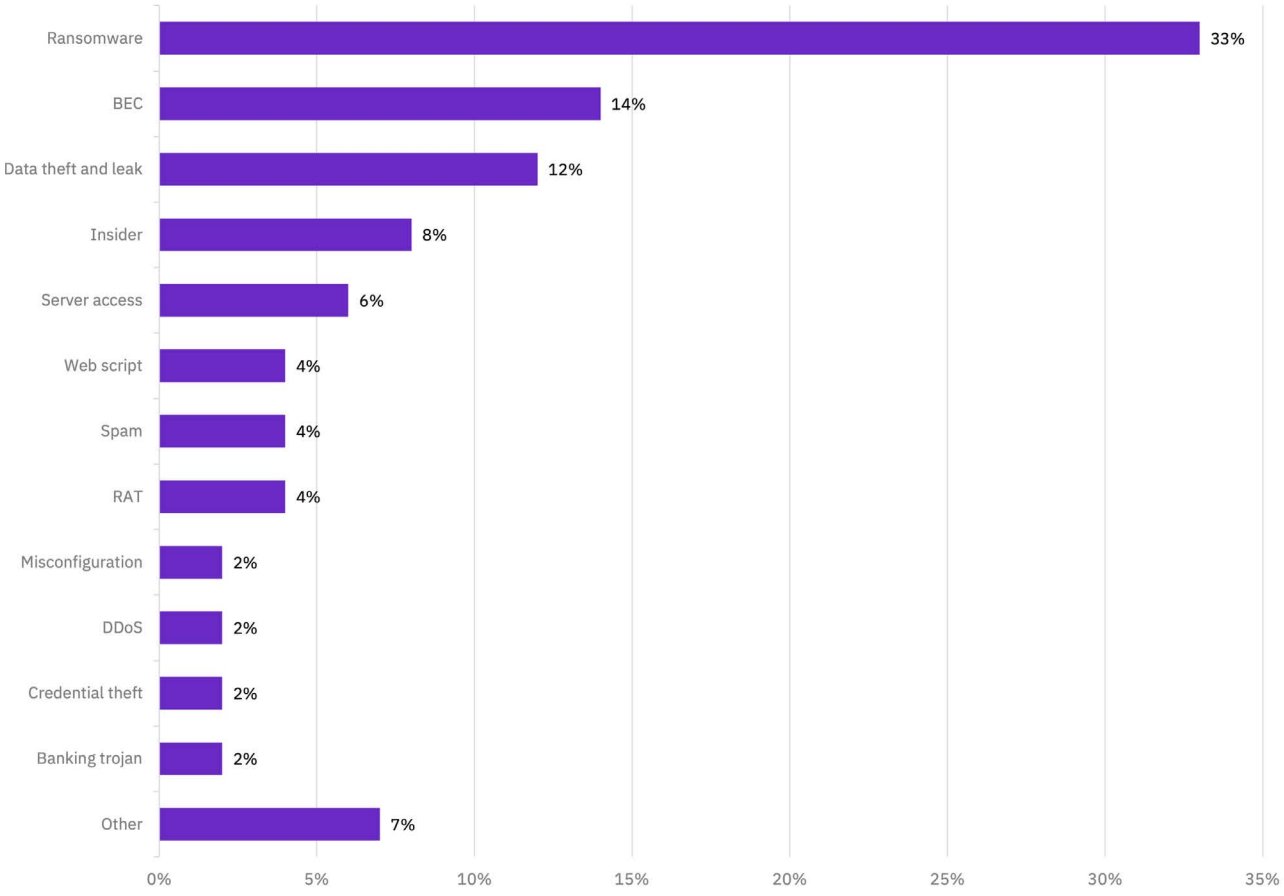
— **Attack types:** North America experienced more ransomware attacks than any other region in pure numbers—translating to 33% of all the attacks on North America in 2020. BEC, data theft and data leaks, as well as RATs also hit North American organizations in high volumes through 2020. North America also experienced 29% of the attacks that exploited CVE-2019-19781 in 2020—the second highest after Europe.

— **Countries under attack:** The United States was the most-attacked North American country in 2020, followed by Canada.

Figure 17

North America attack types

Breakdown of total attacks on North America by attack type, from X-Force incident response data, 2020 (Source: IBM Security X-Force)



Asia-Pacific

— **Attack volume:** The Asia-Pacific region accounted for 25% of all attacks observed by IBM Security X-Force in 2020, up from 22% as observed in the region in 2019.

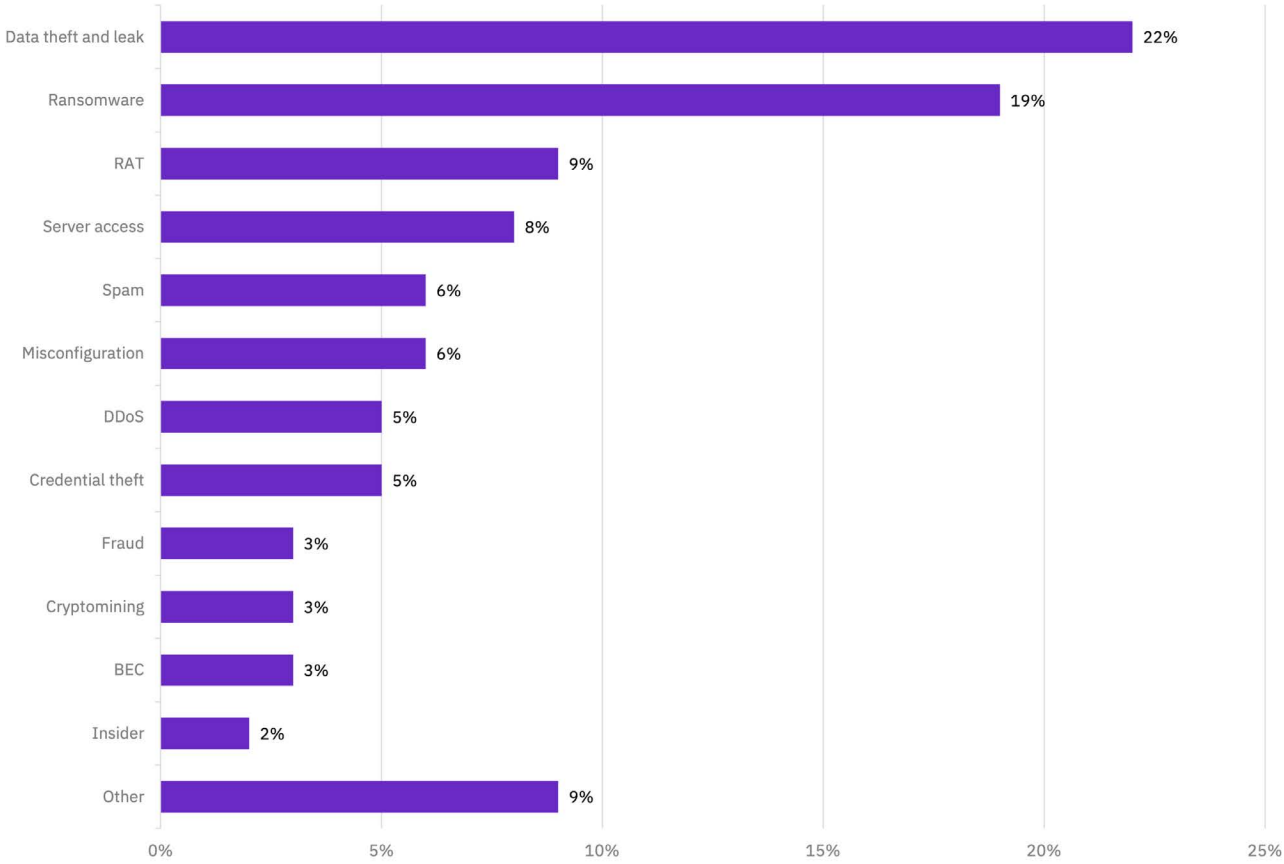
— **Attack types:** Data theft was the most common attack type in Asia in 2020, driven largely by a flurry of Emotet data theft attacks in the fall of 2020 and making up 22% of all attacks in the region—surpassing even ransomware. Ransomware attacks made up 19% of all attacks in Asia in 2020, and including strains such as PJX and Locky. Asia-Pacific experienced more attacks involving RATs than any other geographic region in the world, with remote access trojans making up 9% of all attacks in the region in 2020. Asia also experienced 21% of all attacks exploiting CVE-2019-19781 in 2020. BEC attacks were less common in Asia than others in 2020, potentially due to implementation of multifactor authentication. Manufacturing and finance and insurance were the top two industries targeted in the Asia-Pacific area.

— **Countries under attack:** Japan was the top attacked country in Asia in 2020, followed distantly by India and then Australia.

Figure 18

Asia attack types

Breakdown of total attacks on Asia by attack type, from X-Force incident response data, 2020 (Source: IBM Security X-Force)



Central and South America

— **Attack volume:** Organizations in Central and South America experienced 9% of total attacks IBM Security X-Force observed in 2020, up from 5% in 2019.

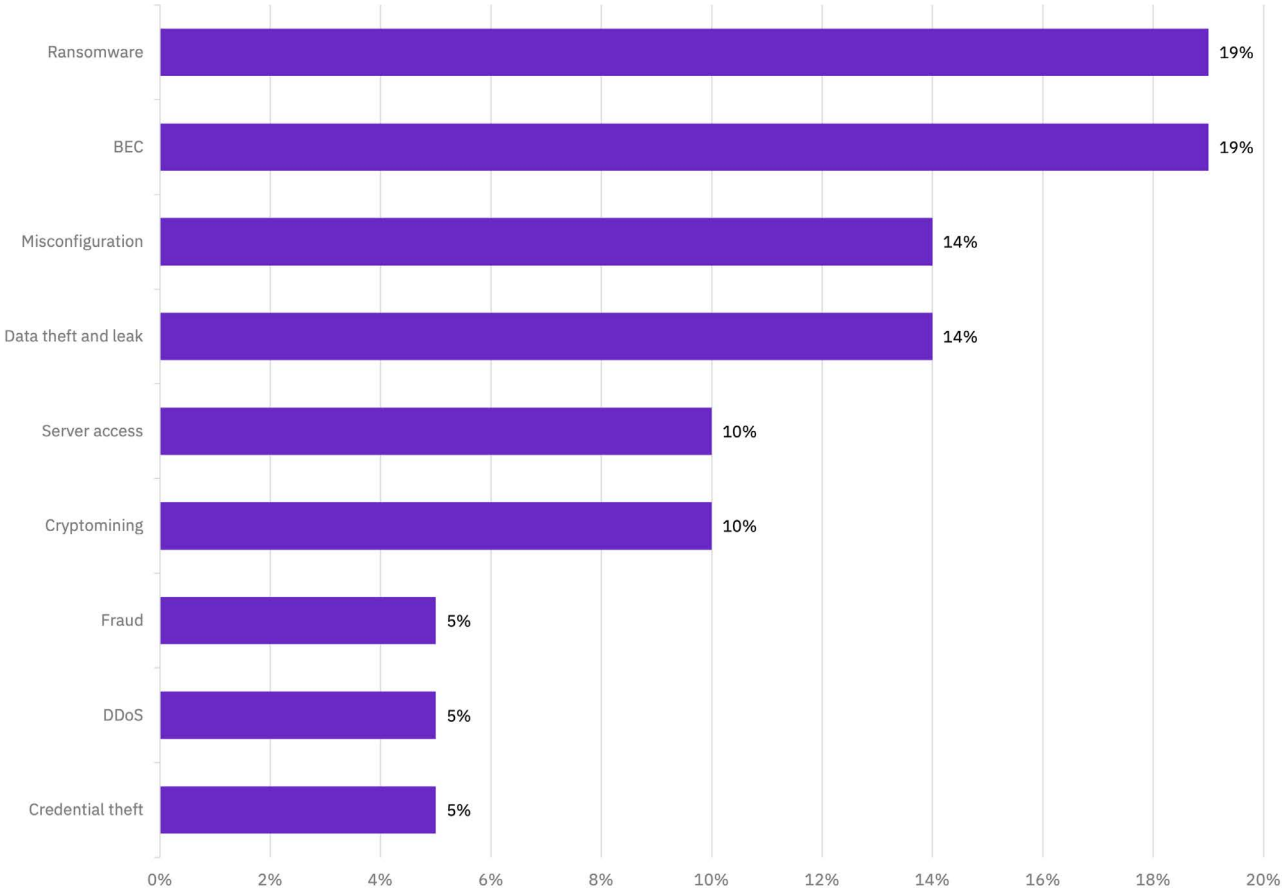
— **Attack types:** BEC tied with ransomware for the top attack type in Central and South America—both accounting for 19% of attacks in the region—followed closely by misconfiguration and data theft and leak. Notably, Central and South America experienced more misconfiguration incidents than North America or Europe. Server access attacks, on the other hand, did not affect Central and South America to the same extent as they have other geographies in 2020.

— **Countries under attack:** Brazil was the top attacked country in Central and South America in 2020.

Figure 19

Central and South America attack types

Breakdown of total attacks on Central and South America by attack type, from X-Force incident response data, 2020 (Source: IBM Security X-Force)



Middle East and Africa

— **Attack volume:** Organizations in the Middle East and Africa experienced 8% of attacks according to X-Force data in 2020, up slightly from 7% the year prior.

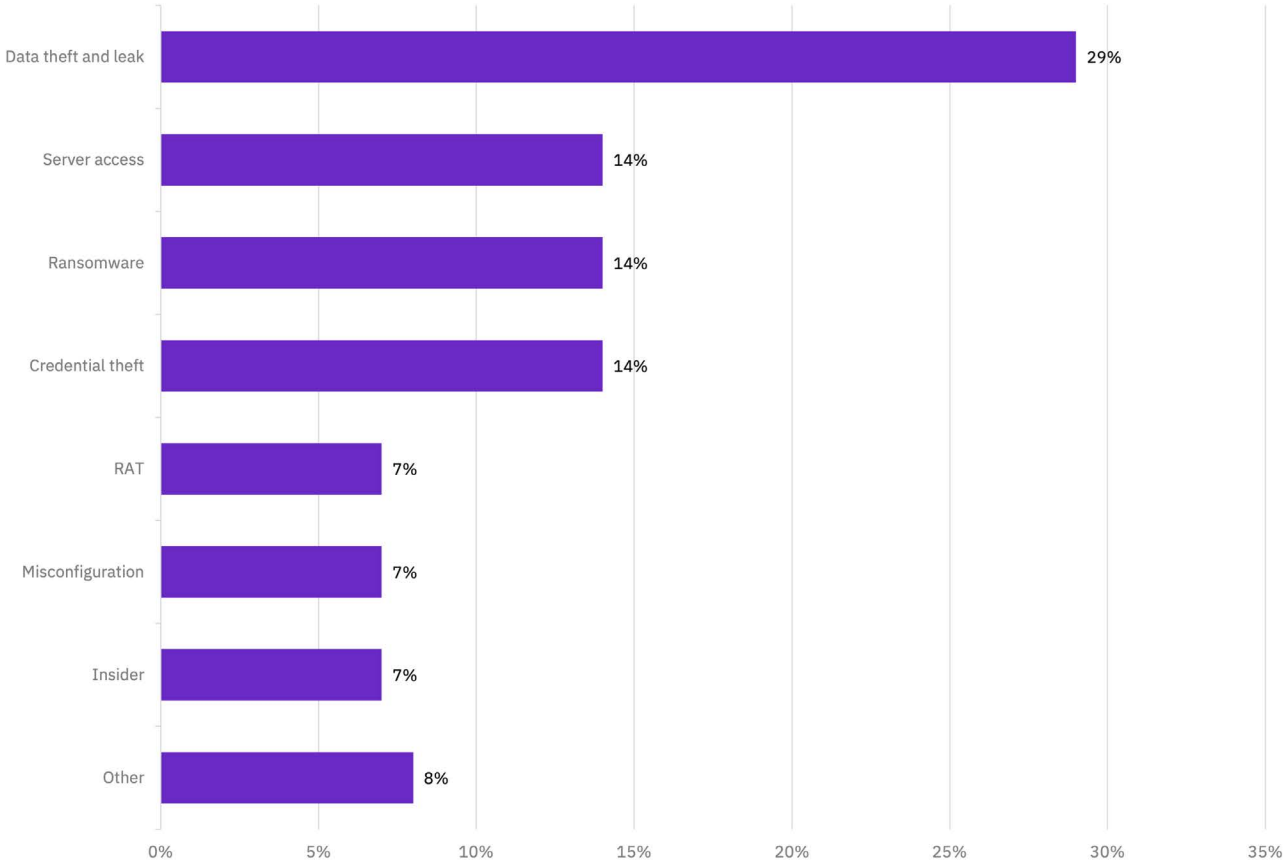
— **Attack types:** Data theft and leak was by far the most common attack type in the Middle East and Africa in 2020, accounting for a significant 29% of attacks in the region. Server access, ransomware and credential theft all tied for second place, at 14% of attacks each. RATs, misconfiguration and insider threats also affected organizations in the Middle East and Africa in 2020.

— **Countries under attack:** Saudi Arabia, the United Arab Emirates, South Africa and Turkey were the top attacked countries in the Middle East and Africa in 2020.

Figure 20

Middle East and Africa attack types

Breakdown of total attacks on Middle East and Africa by attack type, from X-Force incident response data, 2020 (Source: IBM Security X-Force)



Top attacked industries

Each year, X-Force identifies the top 10 most-attacked industries and ranks them according to percentage of attacks. For the fifth year in a row, the finance and insurance industry was the most-attacked industry, underscoring the significant interest threat actors have in these organizations.

Several other industries have shifted significantly since last year's rankings (see *figure 21* for comparative rankings of the top 10 industries in 2020 vs. 2019). Manufacturing—ranked as eighth most attacked in the 2019 report—jumped to second place in 2020. This may be driven by the interest malicious actors have in targeting infrastructure with connections to operational technology. Similarly, energy jumped from ninth place in 2019 to third place in 2020, further underscoring attackers' focus on OT-connected organizations in 2020. Healthcare jumped from last place in 2019 to seventh place in 2020, probably driven by COVID-related healthcare attacks and a barrage of ransomware attacks against hospitals. Transportation targeting continued to drop in 2020, falling to ninth place, compared to coming in third in 2019, potentially related to less transportation utilization during the pandemic.

Figure 21

Top 10 industries by attack volume, 2020 vs. 2019

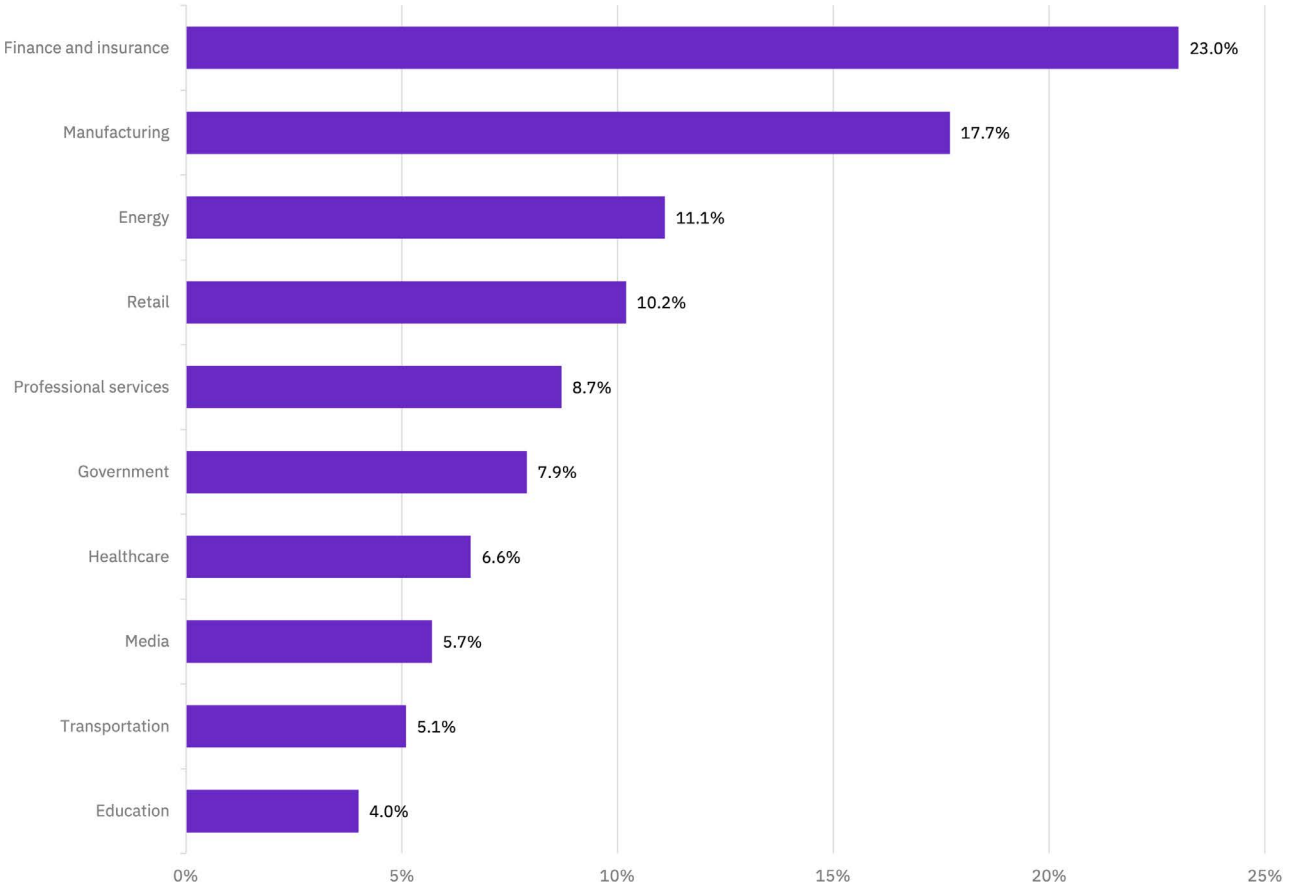
(Source: IBM Security X-Force)

Sector	2020 rank	2019 rank	Change
Finance and insurance	1	1	-
Manufacturing	2	8	6
Energy	3	9	6
Retail	4	2	-2
Professional services	5	5	-
Government	6	6	-
Healthcare	7	10	3
Media	8	4	-4
Transportation	9	3	-6
Education	10	7	-3

Figure 22

Breakdown of attacks on the top 10 industries

Top attacked industries in 2020, shown as a percentage of attacks on the top 10 industries (Source: IBM Security X-Force)

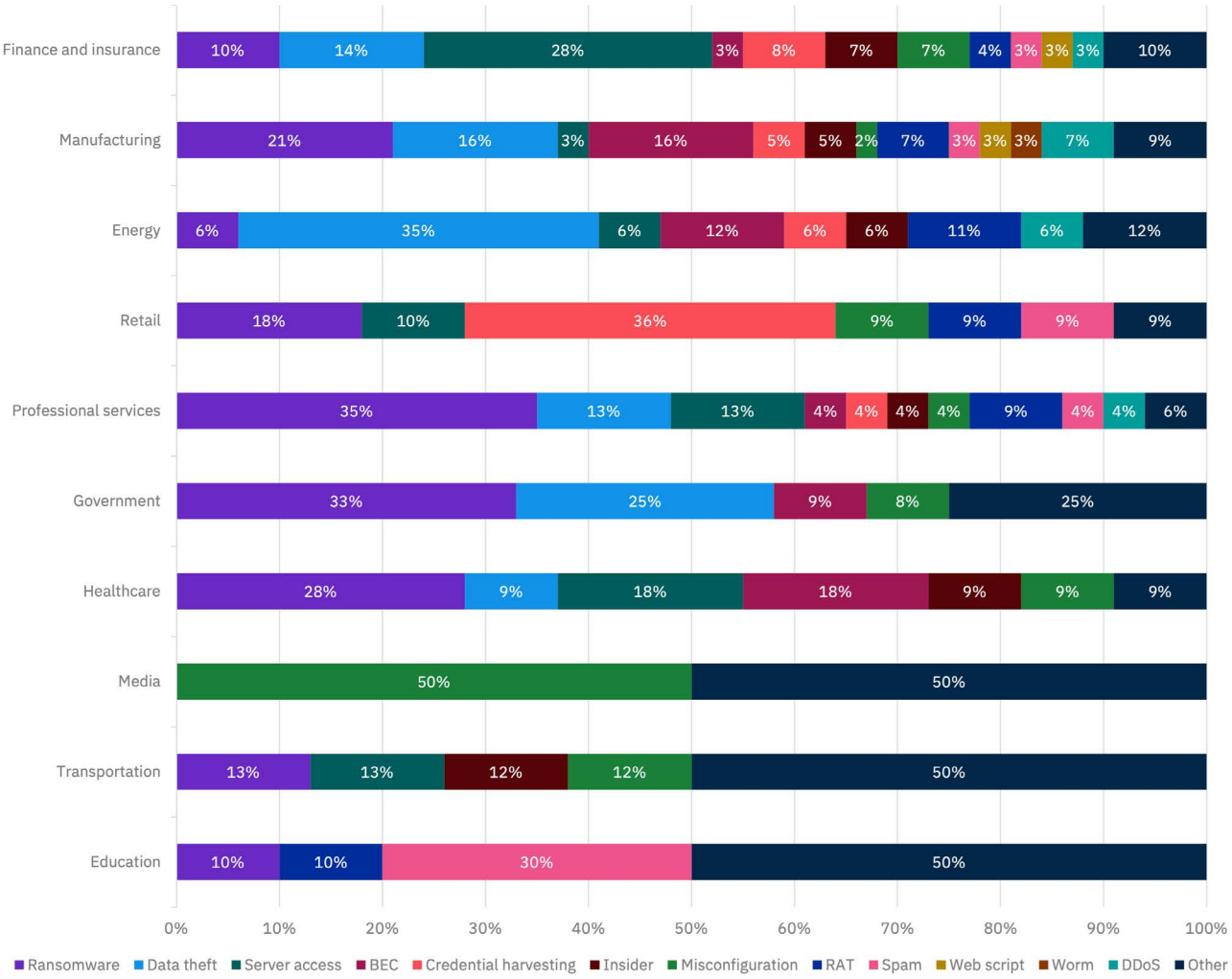


The chart in *figure 22* shows the percentage of attacks on each of the top 10 industries, with 23% of attacks on the top 10 against the finance and insurance industry. Manufacturing was targeted by 17.7% of attacks on the top 10 industries, followed by energy (11.1%) and retail (10.2%), while the rest of the top 10 were targeted by under 10% of attacks each.

Figure 23

Industry attack types

Percentage breakdown of industry attacks by type, from X-Force incident response data, 2020 (Source: IBM Security X-Force)



The chart in *figure 23* portrays the top attacks on each industry from X-Force incident response data. This data and the percentages derived therefrom will be described in greater detail in each of the following sections.

Finance and insurance

28%

of attacks on finance and insurance in 2020 were server access attacks.

10%

of attacks on finance were ransomware.

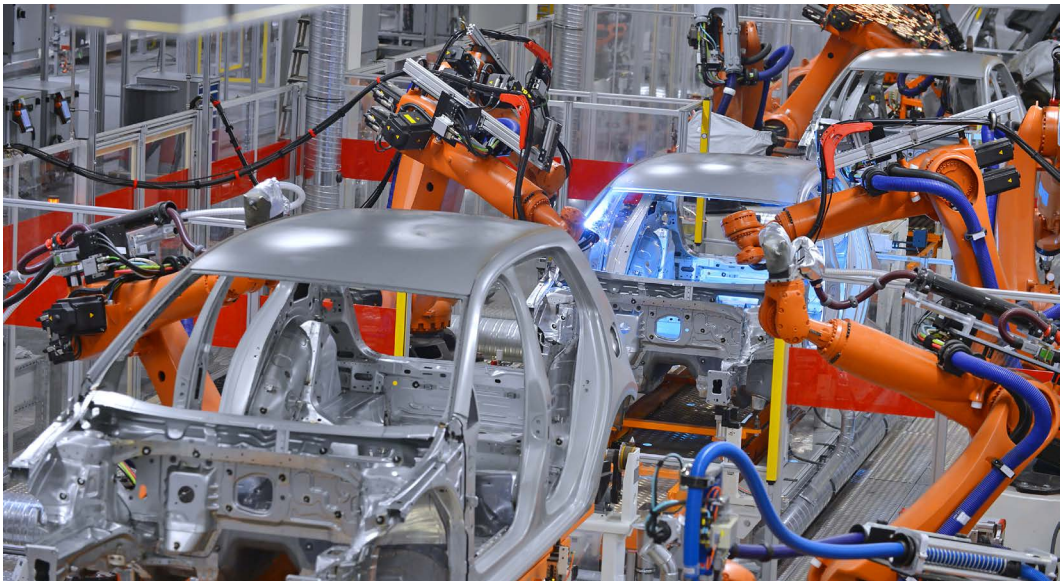
Since 2016, the finance and insurance sector has been ranked as the most attacked industry, a position it continued to hold in 2020. Financial institutions experienced 23% of all attacks we analyzed in 2020, up from the 17% of attacks the sector experienced in 2019.

Of all industries, finance and insurance experienced the highest number of server access attacks—primarily related to Citrix vulnerability CVE-2019-19781—when compared to other industries. Server access attacks made up 28% of all attacks on finance and insurance, and the industry tied with manufacturing for the highest percentage of attacks that exploited CVE-2019-19781, at 22%.

The highly regulated nature of the finance and insurance sector and finance organizations' proactive approach to identifying and addressing server access attacks probably contributed to the high percentage of attacks on this sector.

In addition, finance and insurance experienced fewer ransomware attacks when compared to other industries, such as manufacturing, professional services and government. Only 10% of attacks on this industry in 2020 were ransomware. Ransomware attackers have probably found non-finance organizations to be more profitable for ransomware attacks, potentially because of strong security controls in place at finance and insurance organizations, or because attackers assess that industries such as manufacturing and professional services have a lower tolerance for downtime related to ransomware attacks.

Manufacturing



21%

of attacks against manufacturing were ransomware.

4x

more BEC attacks experienced in manufacturing companies than any other industry.

Manufacturing ranked as the second-most attacked industry in 2020, up from eighth place in 2019, and received 17.7% of all attacks on the top ten industries—more than double the 8.1% of attacks it experienced last year. Threat actors' renewed focus on manufacturing—the industry also ranked second place in 2015, and third place in 2017—underscores its attractiveness as a target, especially for ransomware, BEC, and remote access trojan attacks.

Twenty-one percent of attacks on manufacturing in 2020 were from ransomware—a significant percentage indicating that threat actors find manufacturing to be a profitable sector for ransomware attacks. And, in pure numbers, manufacturing experienced more ransomware attacks than any other sector. This sector's low tolerance for downtime—often amounting to millions of dollars in losses for each hour of downtime—is probably a contributing factor in its high profitability for threat actors.

In addition to ransomware, BEC made up 17% of attacks on manufacturing in 2020—in pure numbers more than four times more BEC attacks than any other industry. Manufacturing organizations often need to procure multiple parts from several different suppliers, creating multiple avenues for threat actors to insert themselves into email conversations and redirect funds meant to pay for manufacturing supplies. Many attacks on manufacturing appear to be targeting money through social engineering, rather than targeting operational technology.

Manufacturing also experienced 22% of all attacks that exploited CVE-2019-19781 in 2020, tying for first place with the finance and insurance industry.

Energy

35%

of attacks on the energy industry were attempted data theft and leak.

Receiving 11.1% of attacks on the top 10 industries in 2020, energy ranked as the third-most attacked industry, up from ninth place the year prior. Server access attacks on energy—and particularly those exploiting CVE-2019-19781—hit energy organizations hard in 2020, and this industry came in fourth place after healthcare for the highest number of such attacks.

Data theft and leak was the top attack type for the energy sector, accounting for 35% of all attacks in this sector, and underscoring the threat from information-stealing malware and phishing attacks. Many of these attacks were against oil and gas companies in particular.

BEC attacks, digital currency mining, ransomware, remote access trojans, and server access attacks also affected the energy industry in 2020, but not notably more than other sectors. In fact, ransomware attacks against energy accounted for only 6% of all attacks against the industry—considerably lower than many of the other top attacked verticals.

Retail

36%

of attacks on retail were credential theft.

18%

of attacks on retail were ransomware.

The retail industry ranked as fourth-most attacked in 2020, down from second place last year, and received 10.2% of all attacks on the top 10 industries, down from 16% last year. As a hub of credit card payments and other financial transactions, retail has long been a target of choice for malicious threat actors.

Retail experienced more credential theft attacks than any other attack type, making up 36% of the attacks it experienced in 2020, and surpassing in pure numbers all other sectors for credential theft attacks. The industry also suffered from ransomware attacks in 2020—making up 18% of total attacks on retail. Nearly all of these ransomware attacks came from Sodinokibi attacks, according to X-Force incident response data.

To a lesser extent, DDoS attacks, fraud, misconfiguration, RATs and server access attacks also affected the retail industry, indicating that threat actors are using a range of attack types to infiltrate retail organizations for financial gain.

Professional services

35%

of attacks on professional services in 2020 were ransomware attacks—a higher percentage than any other industry.

13%

of attacks on professional services were data theft and another 13% were server access.

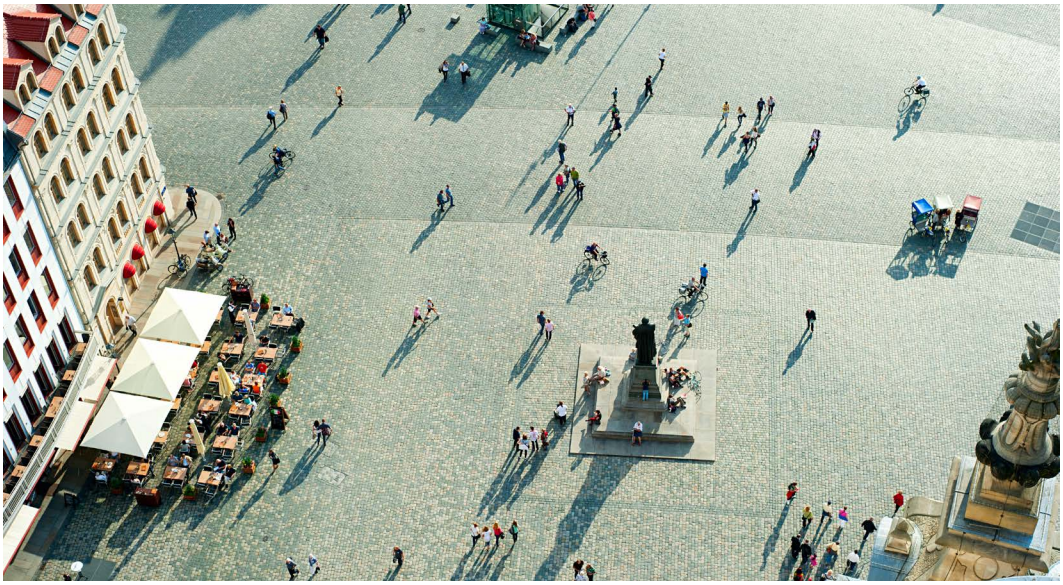
Professional services ranked as the fifth-most attacked industry in 2020 and received 8.7% of all attacks on the top ten industries—holding its same rank as in 2019, when it received 10% of all attacks. Professional services organizations are particularly attractive to attackers because of the avenue they provide to additional victims.

Ransomware made up 35% of incidents at professional services firms in 2020—the highest percentage out of all industries—and in terms of raw numbers of ransomware attacks, the professional services sector came in second only to manufacturing. Some ransomware attackers in 2020—such as Sodinokibi—went after professional services firms aggressively in 2020, including law firms. The sensitive data these firms hold on their clients, and in some cases celebrity clients, possibly led threat actors to believe these firms would be more likely to pay a ransom to prevent the leak of sensitive data. One law firm's data was put up for auction for $40 million dollars, underscoring the high price ransomware attackers perceive they can obtain for professional services firms' data.

In addition to ransomware attacks, data theft and server access attacks hit professional services hard in 2020, accounting for 13% of attacks each on the industry. These trends suggest that injection attacks and vulnerability exploitation on professional services firms are common as threat actors seek access to sensitive data.

Remote access trojans were the third-most common attack type against professional services, making up 9% of attacks on the industry.

Government



33%

of attacks on government were ransomware—the second highest percentage out of all industries.

25%

of attacks on government were attempted data theft and leak.

The public sector—including defense, public administration, and government-provided services—ranked as sixth most attacked in the 2020 ranking, receiving 7.9% of all attacks on the top ten industries. This places government in the same spot as its 2019 ranking, when it received 8% of attacks on the top ten industries. From IBM Security X-Force incident response data, it appears that ransomware attacks plagued government organizations the most in 2020, followed closely by data theft.

Thirty-three percent of the attacks on government organizations in 2020 were ransomware attacks—second highest only after professional services. This continues an ongoing trend of ransomware attacks against government localities, yet in 2020 X-Force Incident Response also observed government judicial systems and government transportation entities in the crosshairs of ransomware. Nearly 50% of ransomware attacks X-Force observed on government entities in 2020 were from Sodinokibi threat actors, following on a trend the group began in September 2019 with a barrage of ransomware attacks against 23 municipalities in Texas.

The second most common attack type against government organizations was data theft and leak, underscoring the threat of data theft and espionage for government entities. Data theft and leak attacks made up 25% of attacks against government in 2020. Foreign governments, cybercriminals, and even hacktivists have all demonstrated an interest in stealing data from government organizations.

To a lesser extent, BEC attacks also affected government in 2020, making up 9% of all attacks on this sector—the fourth-highest percentage of BEC attacks across the industries we examined. More robust implementation of multifactor authentication technologies has the potential to bring this percentage down in the future.

Healthcare

28%

of attacks on healthcare were ransomware.

17%

of CVE-2019-19781 incidents targeted healthcare.

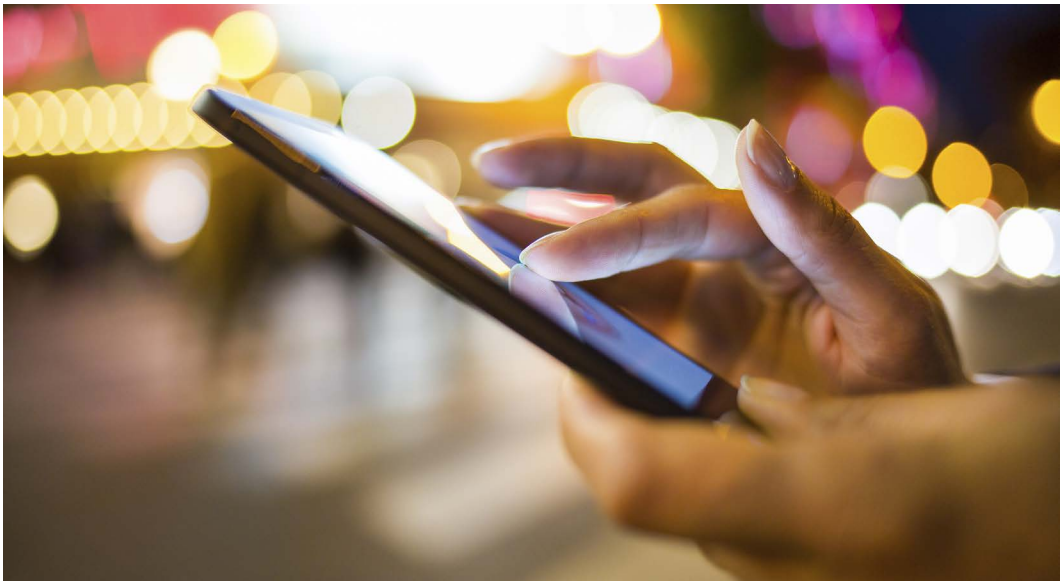
In 2020, healthcare ranked as the seventh most attacked industry, receiving 6.6% of all attacks on the top ten industries—up from tenth place and 3% of attacks in 2019. This is an appreciable jump, and reflects the heavy targeting that healthcare received during the COVID-19 pandemic in 2020, from ransomware attacks to threat actors targeting COVID-related research and treatments.

Nearly 28% of attacks on healthcare in 2020 were ransomware. Ransomware attacks on healthcare can be particularly devastating—grimly illustrated by a ransomware attack on a German hospital in September 2020 that forced an ambulance to take a patient to a different hospital 20 miles away, after which the patient died. While German authorities determined that the ransomware attack did not play a decisive role in the death, in the future such attacks might directly lead to deaths.

When security researchers became aware of Ryuk cybercriminals' plans to attack over 400 US hospitals in late October, US law enforcement and several security companies—including IBM Security X-Force—rushed to notify potential victims and identify mitigation measures. Thankfully, only seven of potentially over 400 hospitals were hit by Ryuk within the following week.

In addition to ransomware, exploitation of CVE-2019-19781 to gain access to healthcare networks was common in 2020. In fact, healthcare was the third-most exploited industry through this CVE, making up 17% of such attacks on all industries. In at least one instance involving this CVE on a healthcare network, threat actors combined their activity with PowerShell and Cobalt Strike for lateral movement and executing on objectives.

Media and information communications



90%

of all malicious DNS squatting targeted the media, by far the most-spoofed industry.

The media and information communications industry came in at eighth most attacked in 2020, receiving 5.7% of all attacks on the top ten industries—down from fourth place last year, when it received 10% of attacks. This sector includes telecommunications and mobile communications providers, as well as media and social media outlets that can play a critical role in political outcomes, especially during election years.

X-Force data identifies misconfiguration as the most common attack type on media in 2020, underscoring the importance of correctly configuring cloud instances to prevent unintended data leakage.

Quad9 data indicates that media was the top industry that malicious actors attempted to spoof by creating similar URLs to legitimate media outlets. Nearly 90% of all malicious DNS squatting—where a domain name is misleadingly similar to a legitimate webpage—involved media outlets. This trend follows from the top brand spoofing trends noted earlier in this report and demonstrates that threat actors are seeking to capitalize on the popularity and trust consumers have in media organizations.

Transportation

25%

of attacks against transportation in 2020 involved a malicious insider or misconfiguration.

Converse to manufacturing, transportation made a significant jump in the IBM Security X-Force rankings this year—but downward, to ninth place, down from third place in 2019 and second place in 2018. Transportation experienced 5.1% of all attacks in 2020, down from 10% in 2019.

There may be several reasons for this decrease in targeting in 2020. For example, a decrease in transportation use in 2020 due to the COVID-19 pandemic and stay-at-home orders may have decreased the profitability of this sector for threat actors—both cybercriminals attempting to capture financial information and nation-states tracking persons of interest. In addition, increased and effective security controls in the industry and harnessing of threat intelligence may be contributing to the decline in attacks observed in this sector.

Malicious insider and misconfiguration incidents had a disproportionately significant impact on transportation in 2020, particularly when compared with other industries. Together, these two attack types accounted for nearly 25% of the attacks on transportation last year.

The threat of insider attacks against transportation is significant, particularly given that some of the most damaging cyber attacks—including those that might lead to loss of life—become most feasible when an insider is involved.

Ransomware and server access attacks accounted for another 26% of attacks on transportation in 2020.

Education

50%

of attacks on education in 2020 were spam or adware.

10%

of attacks were ransomware.

The education sector ranked as tenth-most attacked in 2020, receiving 4.0% of all attacks on the top ten industries. This moves education down from the seventh-most attacked position in 2019, when it received 8% of all attacks.

Spam and adware were common attack types against education in 2020, together making up 50% of all attacks in the education sector. Approximately half of these originated from spam—a higher percentage than any other industry—highlighting the threat to education organizations from phishing-related threats.

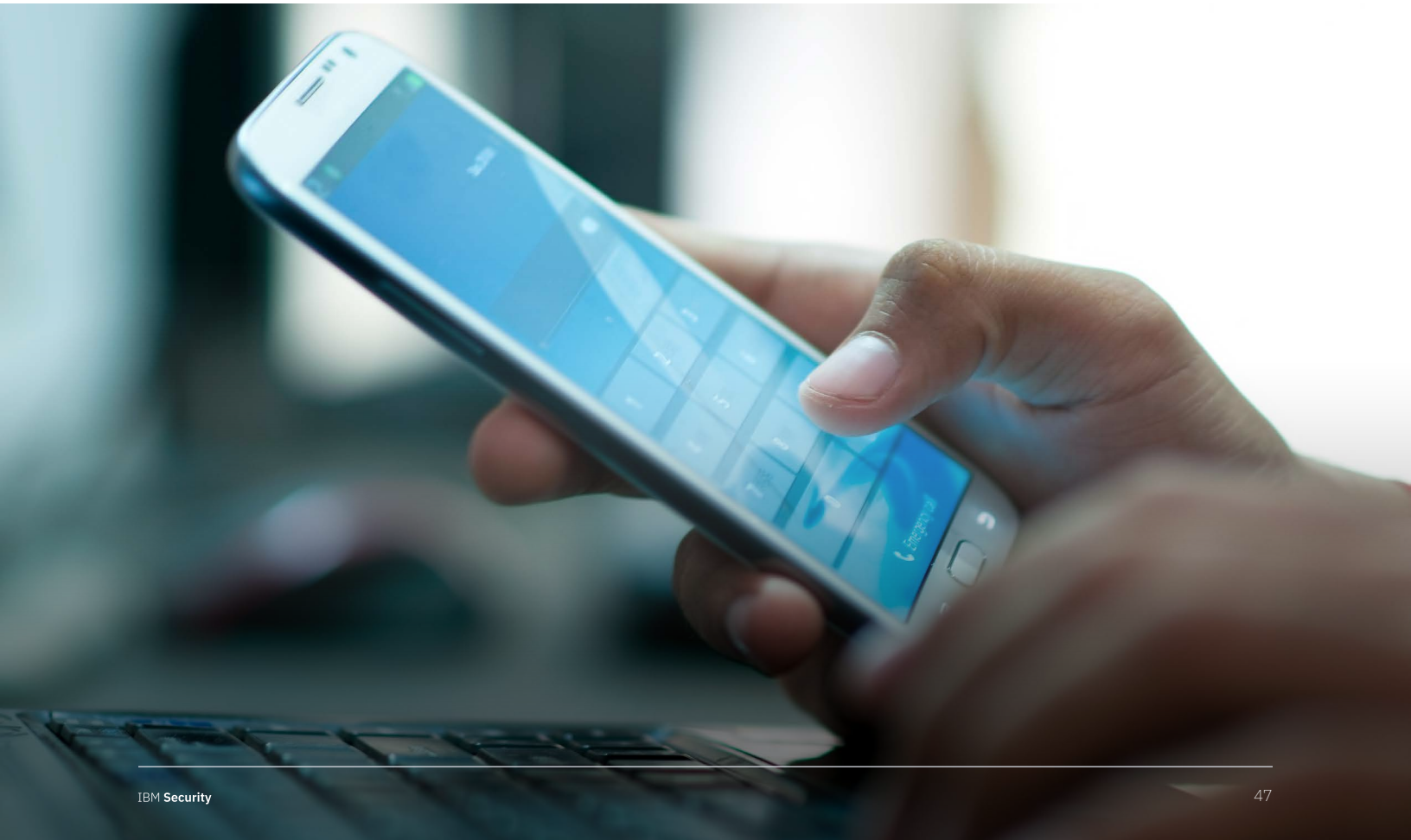
The education sector also experienced ransomware attacks, according to X-Force data, although not to as significant an extent as other industries. Ransomware accounted for 10% of attacks on Education in 2020. Public breach data indicates that several schools and universities were hit with ransomware in 2020, with several of these opting to pay the ransom.

Botnets, fraud, and RATs also contributed to attacks on the education sector. Common cybercriminal attack techniques, phishing, and commodity malware appeared to be frequent threats to education organizations in 2020.

Looking ahead

In 2021, a mix of old and new threats will require security teams to consider a lot of risks simultaneously. Based on X-Force analysis, these are some of the key takeaways for priorities in the next year.

- **The risk surface will continue to grow in 2021.** With thousands of new vulnerabilities likely to be reported in both old and new applications and devices.
- **Double extortion for ransomware will likely persist through 2021.** Attackers publicly leaking data on name and shame sites increases threat actors' leverage to command high prices for ransomware infections.
- **Threat actors continue to shift their sights to different attack vectors.** Targeting of Linux systems, operational technology (OT), IoT devices, and cloud environments will continue. As targeting of these systems and devices becomes more advanced, threat actors may rapidly shift efforts, especially following any high-profile incident.
- **Every industry has its share of risks.** 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.



Recommendations for resilience

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

X-Force recommends the following steps that organizations can take to better prepare for cyber threats in 2021:

Get in front of the threat rather than react to it. Leverage threat intelligence to better understand threat actor motivations and tactics to prioritize security resources.

Preparation is key for a response to ransomware. Planning for a ransomware attack—including a plan that addresses blended ransomware and data theft extortion techniques—and regularly drilling this plan can make all the difference in how your organization responds in the critical moment.

Double check your organization's patch management structure. With scanning and exploiting being the most common infection vector last year, harden your infrastructure and reinvigorate internal detections to find and stop automated exploitation attempts quickly and effectively.

Protect against insider threats. Use data loss prevention (DLP) solutions, training, and monitoring to prevent inadvertent or malicious insiders from breaching your organization.

Build and train an incident response team within your organization. If that's not a possibility, engage an effective incident response capability for prompt response to high-impact incidents.

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.

Implement multifactor authentication (MFA). Adding layers of protection to accounts continues to be one of the most efficient security priorities for organizations.

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 the organization's security, especially with 2020 data showing a resurgence in ransomware activity.

About IBM Security X-Force

IBM Security X-Force delivers insights, detection, and response capabilities to help clients improve their security posture.

IBM Security X-Force Threat Intelligence combines IBM security operations telemetry, research, incident response investigations, commercial data, and open sources to aid clients in understanding emerging threats and quickly making informed security decisions.

Additionally, the highly-trained X-Force Incident Response team provides strategic remediation that helps organizations achieve better control over security incidents and breaches.

X-Force combined with the IBM Security Command Center cyber range experiences train clients to be ready for the realities of today's threats.

Throughout the year, IBM X-Force researchers also provide ongoing research and analysis in the form of blogs, white papers, webinars and podcasts, highlighting our insight into advanced threat actors, new malware, and new attack methods. In addition, we provide a large body of current, cutting-edge analysis to subscription clients on our Premier Threat Intelligence platform.

Take the next step

Learn about orchestrating your incident response with IBM Security >

About IBM Security

IBM Security works with you to help protect your business with an advanced and integrated portfolio of enterprise security products and services, infused with AI, and a modern approach to your security strategy using a zero trust principles, helping you thrive in the face of uncertainty. By aligning your security strategy to your business; integrating solutions designed to protect your digital users, assets, and data; and deploying technology to manage your defenses against growing threats, we help you to manage and govern risk that supports today's hybrid cloud environments.

Our new modern, open approach, the IBM Cloud Pak for Security platform, is built on RedHat Open Shift and supports today's hybrid multi cloud environments with an extensive partner ecosystem. Cloud Pak for Security is an enterprise-ready containerized software solution that enables you to manage the security of your data and applications –by quickly integrating your existing security tools to generate deeper insights into threats across hybrid cloud environments– leaving your data where it is, allowing easy orchestration and automation of your security response.

For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Contributors

Lead author:
Camille Singleton

Contributors:
Allison Wikoff
Ari Eitan (Intezer)
Charles DeBeck
Charlotte Hammond
Chenta Lee
Chris Sperry
Christopher Kiefer
Claire Zaboeva
David McMillen
David Moulton
Dirk Hartz
Georgia Prassinos
Ian Gallagher (Intezer)
John Zorabedian
Joshua Chung
Kelly Kane
Lauren Jensen
Limor Kessem
Mark Usher
Martin Steigemann
Matthew DeFir
Megan Radogna
Melissa Frydrych
Michelle Alvarez
Mitch Mayne
Nick Rossman
Patty Cahill-Ingraham
Randall Rossi
Richard Emerson
Salina Wuttke
Scott Craig
Scott Moore

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2021