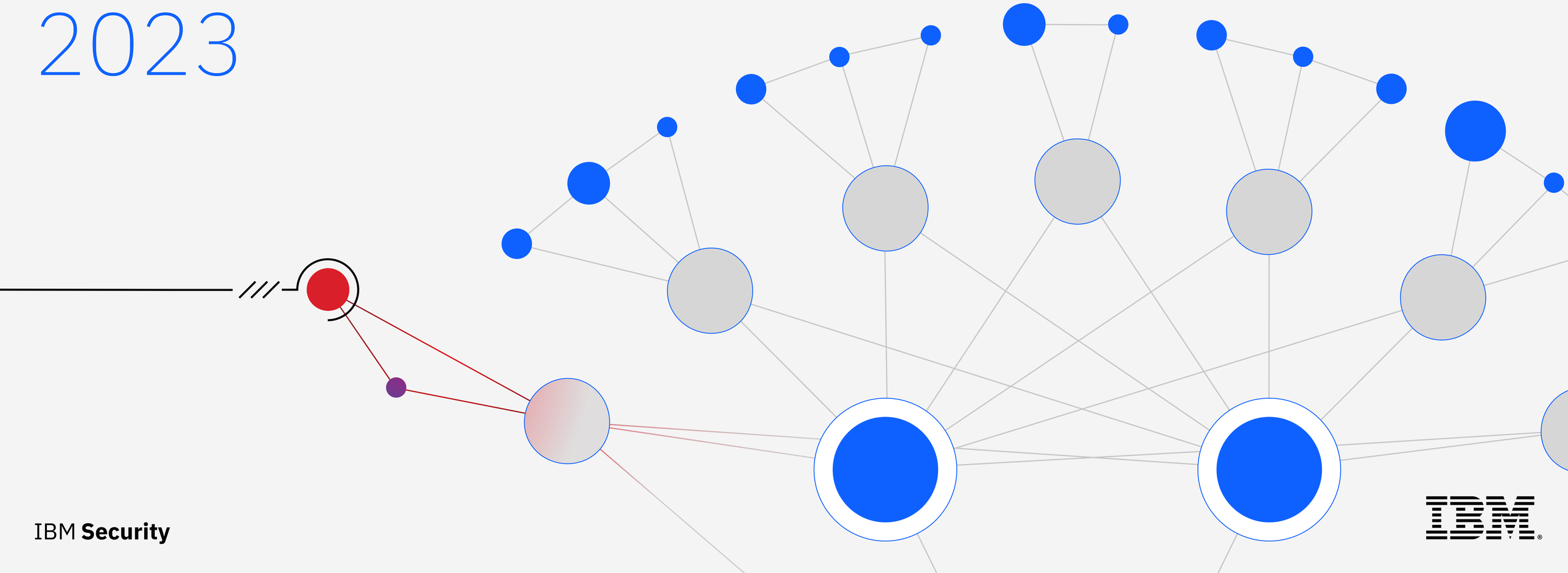
X-Force Threat Intelligence Index 2023

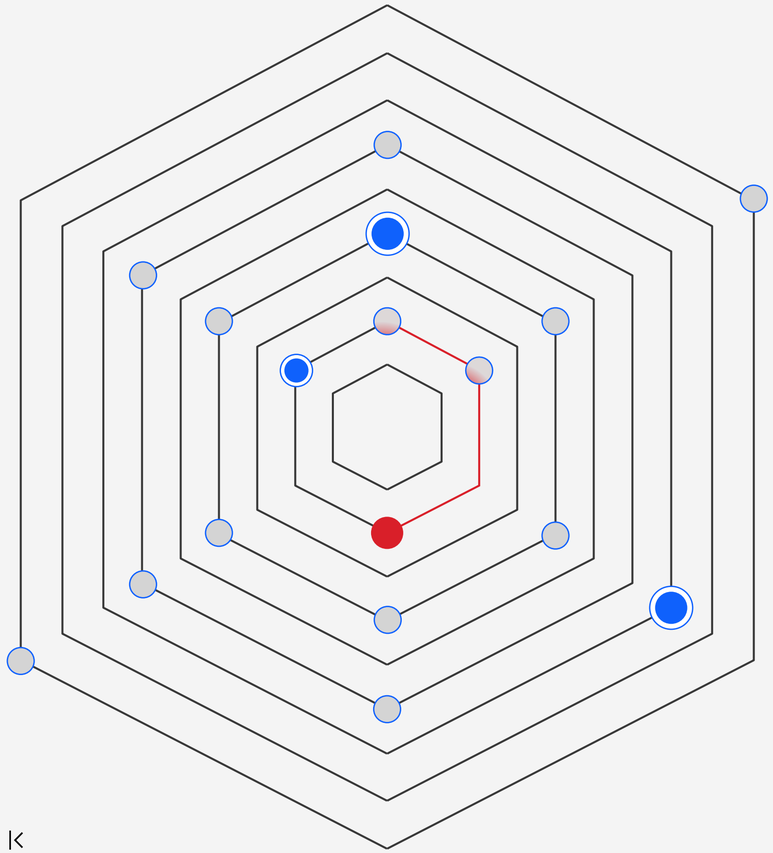


IBM **Security**

Table of contents

01

Executive summary



The year 2022 was another tumultuous one for cybersecurity. While there was no shortage of contributing events, among the most significant were the continuing effects of the pandemic and the eruption of the military conflict in Ukraine. Disruption made 2022 a year of economic, geopolitical and human upheaval and cost—creating exactly the kind of chaos in which cybercriminals thrive.

And thrive they did.

IBM Security® X-Force® witnessed opportunistic threat actors who capitalize on disorder, using the landscape to their advantage to infiltrate governments and organizations across the globe.

The IBM Security X-Force Threat Intelligence Index 2023 tracks new and existing trends and attack patterns and includes billions of datapoints ranging from network and endpoint devices, incident response (IR) engagements, vulnerability and exploit databases and more. This report is a comprehensive collection of our research data from January to December 2022.

We provide these findings as a resource to IBM clients, cybersecurity researchers, policymakers, the media and the larger community of security industry professionals and industry leaders. Today's volatile landscape, with its increasingly sophisticated and malicious threats, requires a collaborative effort to protect business and citizens. More than ever, you need to be armed with threat intelligence and security insights to stay ahead of attackers and fortify your critical assets.

So you too can thrive.

How our data analysis changed for 2022

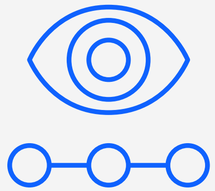
In 2022, we modified how we examined portions of our data. The changes allow us to offer more insightful analysis and align more closely to industry standard frameworks. That, in turn, enables you to make more informed security decisions and better protect your organization from threats.

Changes to our analysis in 2022 included:

- **Initial access vectors:** Adopting the MITRE ATT&CK framework to track initial access vectors more closely aligns our research findings with the broader cybersecurity industry and allows us to identify important trends at the technique level.
- **Exploits and zero day compromises:** Extrapolating from our robust vulnerability database—which includes nearly 30 years of data—helps lend context to our analysis and identify the actual threat posed by vulnerabilities. This process also lends context to the diminishing proportion of weaponizable exploits and impactful zero days.
- **Threat actor methods and their impact:** Uncoupling the steps threat actors take during an attack from the actual impact of an incident allowed us to identify critical stages of an incident. This process, in turn, uncovered areas that responders should be prepared to handle in the aftermath of an incident.

02

Report highlights



Top actions on objectives observed: In almost one-quarter of all incidents remediated in 2022, the deployment of backdoors at 21% was the top action on objective. Notably, an early year spike in Emotet, a multipurpose malware, contributed significantly to the jump in backdoor activity observed year over year. Despite this spike in backdoor activity, ransomware, which held the top spot since at least 2020, constituted a large share of the incidents at 17%, reinforcing the enduring threat this malware poses.

Extortion was the most common attack impact on organizations: At 27%, extortion was the clear impact of choice by threat actors. Victims in manufacturing accounted for 30% of incidents that resulted in extortion, as cybercriminals continued the trend of exploiting a strained industry.

Phishing was the top initial access vector: Phishing remains the leading infection vector, identified in 41% of incidents, followed by exploitation of public-facing applications in 26%. Infections by malicious macros have fallen out of favor, likely due to Microsoft's decision to block macros by default. Malicious ISO and LNK files use escalated as the primary tactic to deliver malware through spam in 2022.

Increase in hacktivism and destructive malware: Russia's war in Ukraine opened the door to what many in the cybersecurity community expected to be a showcase of how cyber enables modern warfare. Although the direst cyberspace predictions haven't come to fruition as of this publication, there was a notable resurgence of hacktivism and destructive malware. X-Force also observed unprecedented shifts in the cybercriminal world with increased cooperation between cybercriminal groups, and Trickbot gangs targeting Ukrainian organizations.

03

Key stats

27%

Percentage of attacks with extortion

Threat actors sought to extort money from victims in more than one-quarter of all incidents to which X-Force responded in 2022. The tactics they use have evolved in the last decade, a trend expected to continue as threat actors more aggressively seek profits.

21%

Share of incidents that saw backdoors deployed

Deployment of backdoors was the top action on objective last year, occurring in more than one in five reported incidents worldwide. Successful intervention by defenders likely prevented threat actors from fulfilling further objectives that may have included ransomware.

17%

Ransomware’s share of attacks

Even amid a chaotic year for some of the most prolific ransomware syndicates, ransomware was the second most common action on objective, following closely behind backdoor deployments and continuing to disrupt organizations’ operations. Ransomware’s share of incidents declined from 21% in 2021 to 17% in 2022.

41%

Percentage of incidents involving phishing for initial access
Phishing operations continued to be the top pathway to compromise in 2022, with 41% of incidents remediated by X-Force using this technique to gain initial access.

100%

Increase in the number of thread hijacking attempts per month
There were twice as many thread hijacking attempts per month in 2022, compared to 2021 data. Spam email leading to Emotet, Qakbot and IcedID made heavy use of thread hijacking.

52%

Drop in reported phishing kits seeking credit card data
Almost every phishing kit analyzed in the data sought to gather names at 98% and email addresses at 73%, followed by home addresses at 66% and passwords at 58%. Credit card information, targeted 61% of the time in 2021, fell out of favor for threat actors—data shows it was sought in only 29% of phishing kits in 2022, a 52% decline.

62%

Percentage of phishing attacks using spear phishing attachments
Attackers preferred weaponized attachments, deployed by themselves or in combination with links or spear phishing via service.

26%

Share of 2022 vulnerabilities with known exploits
Twenty-six percent of 2022's vulnerabilities had known exploits. According to data that X-Force has tracked since the early 1990s, that proportion has been dropping in recent years, showcasing the benefit of a well-maintained patch management process.

31%

Share of global attacks that targeted the Asia-Pacific region
Asia-Pacific retained the top spot as the most-attacked region in 2022, accounting for 31% of all incidents. This statistic represents a five percentage point increase from the total share of attacks to which X-Force responded in the region in 2021.

Top initial access vectors

In 2022, X-Force moved from tracking initial access vectors as broader categories, such as phishing and stolen credentials, to the initial access techniques listed within the MITRE ATT&CK Matrix for Enterprise framework. This shift allows X-Force to track important trends more granularly at the technique level. It also provides more readily consumable and cross-comparable data and aligns with the broader industry's standardization efforts.

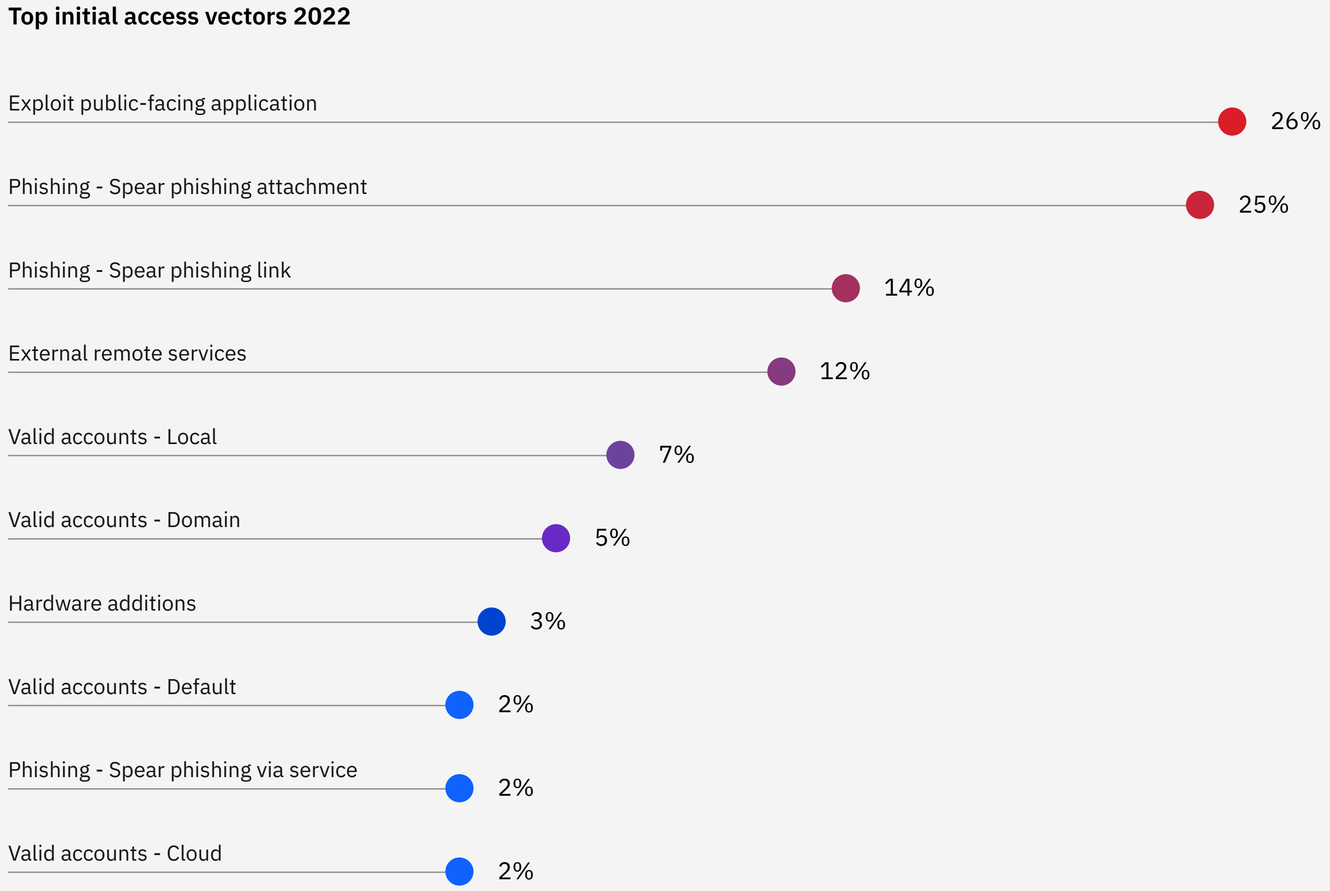


Figure 1: Top initial access vectors X-Force observed in 2022. Source: X-Force

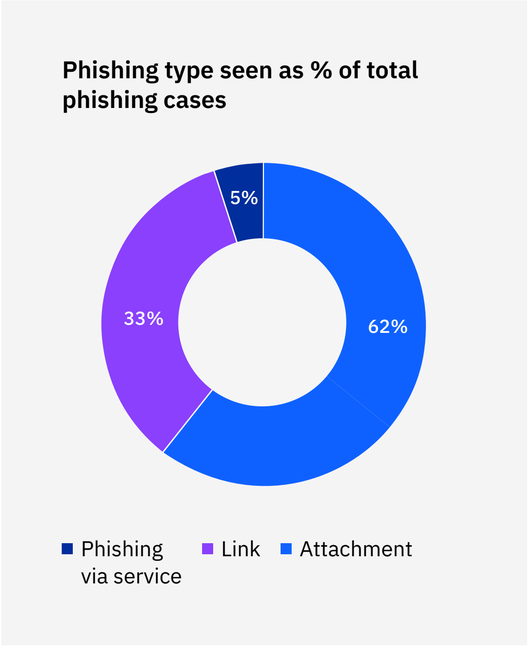


Figure 2: Types of phishing subtechniques as a percentage of total phishing cases observed by X-Force in 2022. Source: X-Force

Phishing

Phishing (T1566), whether through attachment, link or as a service, remains the lead infection vector, which comprised 41% of all incidents remediated by X-Force in 2022. This percentage holds steady from 2021 after having increased from 33% in 2020. Looking at all phishing incidents, spear phishing attachments (T1566.001) were used in 62% of those attacks, spear phishing links (T1566.002) in 33% and spear phishing as a service (T1566.003) in 5%. X-Force also witnessed threat actors use attachments alongside phishing as a service or links in some instances.

IBM X-Force Red data from 2022 further highlights the value of phishing and mishandled credentials to threat actors.

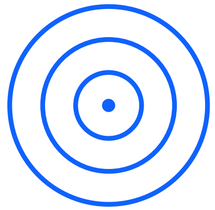
Across 2022's penetration tests for clients, X-Force Red found that approximately 54% of tests revealed improper authentication or handling of credentials. The X-Force Red Adversary Simulation team regularly performed spear phishing with QR codes targeting multifactor authentication (MFA) tokens. Many organizations lacked visibility into applications and endpoints exposed through identity access management and single sign-on (SSO) portals, such as Okta.

In second place, exploitation of public-facing applications (T1190)—defined as adversaries taking advantage of a weakness in an internet-facing computer or program—was identified in 26% of incidents to which X-Force responded.

This correlates to what past Threat Intelligence Index reports referred to as "vulnerability exploitation" and marks a drop from 34% in 2021.

In third place, abuse of valid accounts (T1078) was identified in 16% of the observed incidents. These are cases where adversaries obtained and abused credentials of existing accounts as a means of gaining access. These incidents included cloud accounts (T1078.004) and default accounts (T1078.001) at 2% each, domain accounts (T1078.002) at 5%, and local accounts (T1078.003) at 7%.

Credit card information dropped significantly from being targeted 61% of the time in 2021 to 29% of phishing kits in 2022.



Phishing kits lasting longer, targeting PII over credit card data

IBM Security analyzed thousands of phishing kits from around the world for the second year in a row and discovered kit deployments are operational longer and reaching more users. The data indicates that the lifespan of phishing kits observed has more than doubled year over year, while the median deployment across the data set remained relatively low at 3.7 days.

Overall, the shortest deployment lasted minutes and the longest, discovered in 2022, ran longer than three years. Our investigation found the following:

- One-third of deployed kits lasted approximately 2.3 days last year, more than double the length of the year prior when the same proportion lasted no longer than one day.
- Approximately half of all reported kits impacted 93 users, whereas in 2021, each deployment on average had no greater than 75 potential victims.
- The maximum total victims of one reported phishing attack was just over 4,000, although this was an outlier.
- Almost every reported phishing kit analyzed sought to gather names at 98%. This was followed by email addresses at 73%, home addresses at 66% and passwords at 58%.
- Credit card information dropped significantly from being targeted 61% of the time in 2021 to 29% of phishing kits in 2022.
- Lower instances of phishing kits seeking credit card data indicate that phishers are prioritizing personally identifiable information (PII), which allows them broader and more nefarious options. PII can either be gathered and sold on the dark web or other forums or used to conduct further operations against targets.

Top spoofed brands

The top brands observed being spoofed are made up mostly of the biggest names in tech. X-Force believes this shift from 2021's somewhat more diverse list is due to improved ability to identify the brands that a kit is configured to spoof, not just the one it's targeting by default. Many phishing kits are multipurpose, and the brand being spoofed can be changed by altering a simple parameter. For example, a kit can spoof Gmail by default, but a one-line update changes it into an attack spoofing Microsoft.

Stolen credentials for such services are valuable. Gaining access to accounts that victims use to manage entire portions of their online presence can open the door for access to other accounts. Attackers' focus on this form of initial access is highlighted in the 2022 Cloud Threat Landscape Report, which found a more than threefold increase at 200% of the number of cloud accounts being advertised for sale on the dark web over what was observed in 2021.

Top spoofed brands year over year

	2022	2021
1	Microsoft	Microsoft
2	Google	Apple
3	Yahoo	Google
4	Facebook	BMO Harris Bank
5	Outlook	Chase
6	Apple	Amazon
7	Adobe	Dropbox
8	AOL	DHL
9	PayPal	CNN
10	Office365	Hotmail

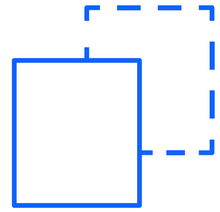
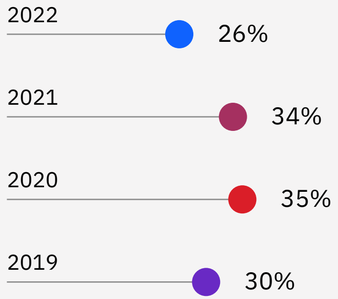


Figure 3: This chart identifies the top spoofed brands in 2021 and 2022, demonstrating that threat actors are increasingly focusing on large technology brands. Source: IBM phishing kit data

Share of incidents resulting from vulnerability exploitation over the last four years



Vulnerabilities

Vulnerability exploitation—captured for 2022 as exploitation of public-facing applications (T1190)—placed second among top infection vectors and has been a preferred method of compromise by attackers since 2019. Vulnerabilities were exploited in 26% of attacks that X-Force remediated in 2022, 34% in 2021, 35% in 2020 and 30% in 2019.

Not every vulnerability exploited by threat actors results in a cyber incident. The number of incidents resulting from vulnerability exploitation in 2022 decreased 19% from 2021, after rising 34% from 2020. X-Force assessed that this swing was driven by the widespread Log4J vulnerability at the end of 2021.

Exploitation for access is a key area of research that the team at X-Force Red Adversary Simulation Services pursued to keep simulating advanced threats. The team increased its focus on vulnerability research for exploitation of operating systems (OS) and applications to expand access and perform privilege escalation. This focus was largely due to past exercises with long-standing clients who have hardened traditional Active Directory attack paths and the need to pursue new attack paths.

While vulnerabilities are a common initial access vector, and the industry responds to several major ones in any given year, not every vulnerability is the same. It's important for decision makers to take a full view of the vulnerability landscape and ensure they're equipped with the necessary context to understand the real threat a given vulnerability poses to their networks.

Almost 30 years ago and predating the advent of the Common Vulnerabilities and Exposures (CVE) system, X-Force began building a robust vulnerability database. This database is now one of the most comprehensive in the cybersecurity industry. While vulnerabilities are a major risk to security, there are far more reported vulnerabilities than there are known weaponized exploits. Further, despite public attention on zero days, the actual number of known zero days is dwarfed by the total number of known vulnerabilities.

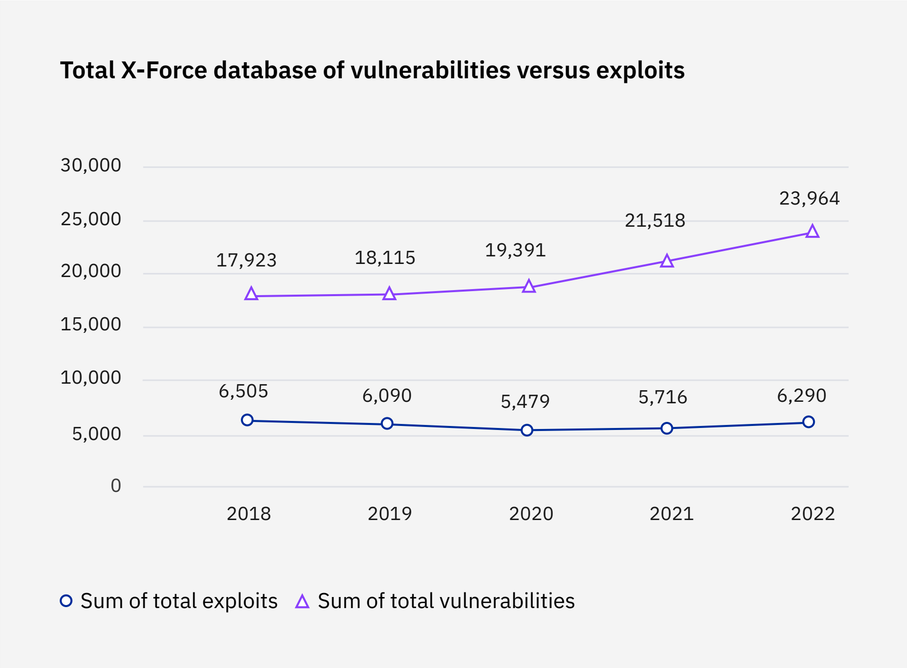


Figure 4: X-Force vulnerability database view showing vulnerabilities and exploits over the past five years.
Source: X-Force

Every year sees a new record number of vulnerabilities discovered. The total number of vulnerabilities tracked in 2022 was 23,964 compared to 21,518 in 2021. The trend of year-to-year vulnerability increases has persisted over the last decade. To the benefit of defenders, analysis of our vulnerability database showed the proportion of known, viable exploits to reported vulnerabilities decreasing in recent years—36% in 2018, 34% in 2019, 28% in 2020, 27% in 2021 and 26% in 2022.

These numbers can shift with the exposure of zero days and exploits being developed for older vulnerabilities—sometimes years after they're identified—and there are several potential explanations behind this decline. First, the establishment of formal bug bounty programs has incentivized the proactive discovery of vulnerabilities within applications. Additionally, a handful of widely popular and well-established vulnerabilities exist that already serve as a means of system exploitation for attackers, reducing the need for threat actors to develop new exploits. The drop is likely due to a combination of multiple factors but doesn't point to vulnerability exploitation becoming less of a threat.

While the proportion of exploits to vulnerabilities drops, the severity of those exploits X-Force tracks has increased in the last five years. In 2018, 58% of vulnerabilities had a Common Vulnerability Scoring System (CVSS) score of medium,

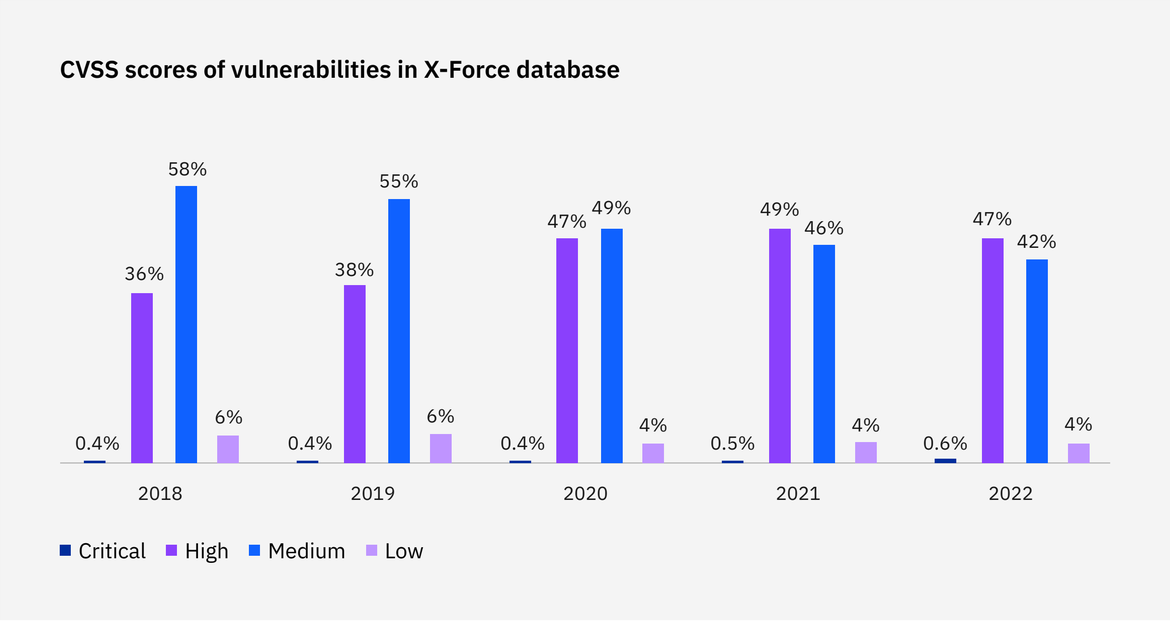


Figure 5: X-Force vulnerability database showing severity of vulnerabilities tracked in our system.
Source: X-Force

4.0-6.9 out of 10, compared to just under 36% high, 7.0-9.9. The spread between those two inverted in 2021, and high severity vulnerabilities now account for five percentage points more than those that scored medium.

Still, of all the vulnerabilities X-Force has tracked since 1988, 38% of them rank high, with only 1% coming in at the critical score of 10. Half of tracked vulnerabilities rank medium with the remaining 11% coming in at low, 3.9 and below. These scores alone don't correlate to the real-world severity of any one CVE, since it doesn't account for how exploitation is accomplished or if an exploit even exists. However, the scores do help defenders compare vulnerabilities and prioritize how quickly to address them. The Figure 6 graphic on the following page helps to put into perspective the true nature of the vulnerability problem facing the cybersecurity industry.

Operational technology (OT) vulnerabilities

Industrial control systems (ICS) vulnerabilities discovered in 2022 decreased for the first time in two years—457 in 2022 compared to 715 in 2021 and 472 in 2020. One explanation for this may be found in ICS lifecycles and how they're generally managed and patched. Attackers know that with demand for minimal downtime, long equipment lifecycles and older, less-supported software, many ICS components and OT networks are still at risk of older vulnerabilities. Infrastructure is usually in place for many years longer than standard office workstations, which extends the lifespan of ICS-specific vulnerabilities beyond those that can exploit IT.

The vulnerability problem

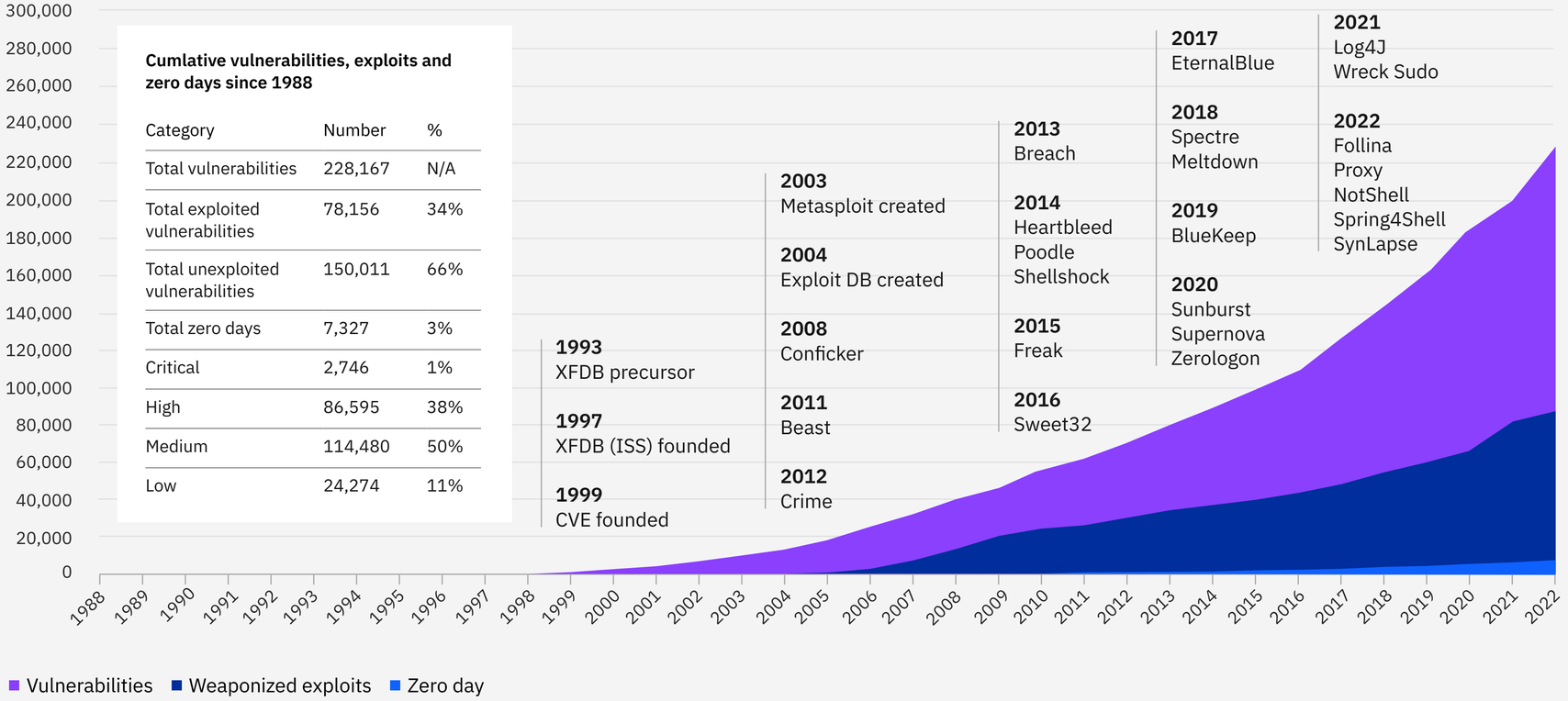


Figure 6: Graphic showing the growth of vulnerabilities, exploits and zero days since 1988. Also included is a timeline of major event involving vulnerabilities since 1993. XFDB stands for X-Force Database and Exploit DB stands for Exploit Database. Source: X-Force

Top actions on objectives

Previously, the X-Force Threat Intelligence Index examined the broad category of top attacks. For 2022, X-Force dissected this classification into two distinct categories: the specific actions threat actors took on victim networks, or adversary action on objective, and the intended or realized effect of that action on the victim, or impact.

According to X-Force Incident Response data, deployment of backdoors was the most common action on objective, occurring in 21% of all reported incidents. This was followed by ransomware at 17% and business email compromise (BEC) at 6%. Malicious documents (maldocs), spam campaigns, remote access tools and server access were discovered in 5% of cases each.

Top actions on objectives 2022

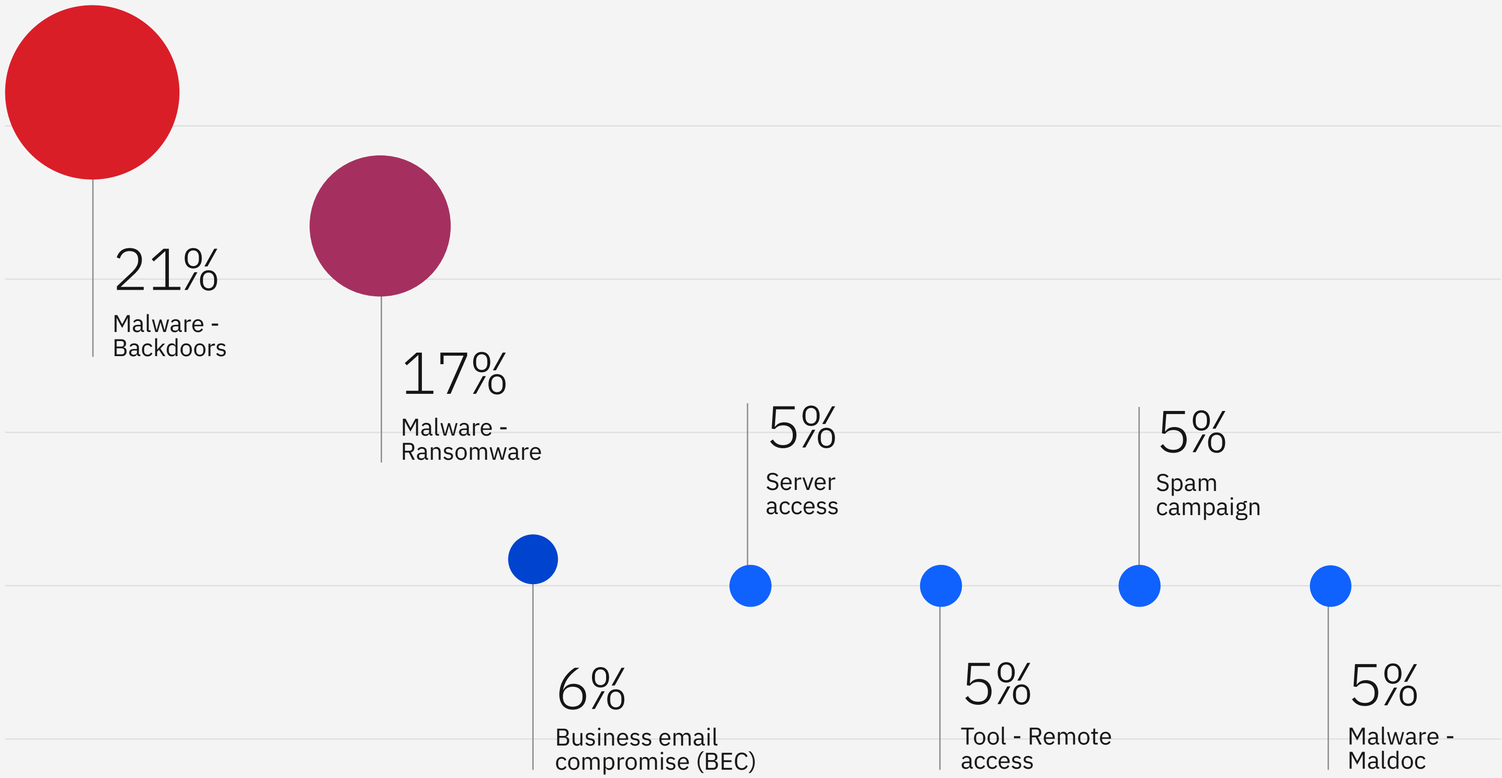


Figure 7: Top actions on objectives observed by X-Force in 2022. Source: X-Force

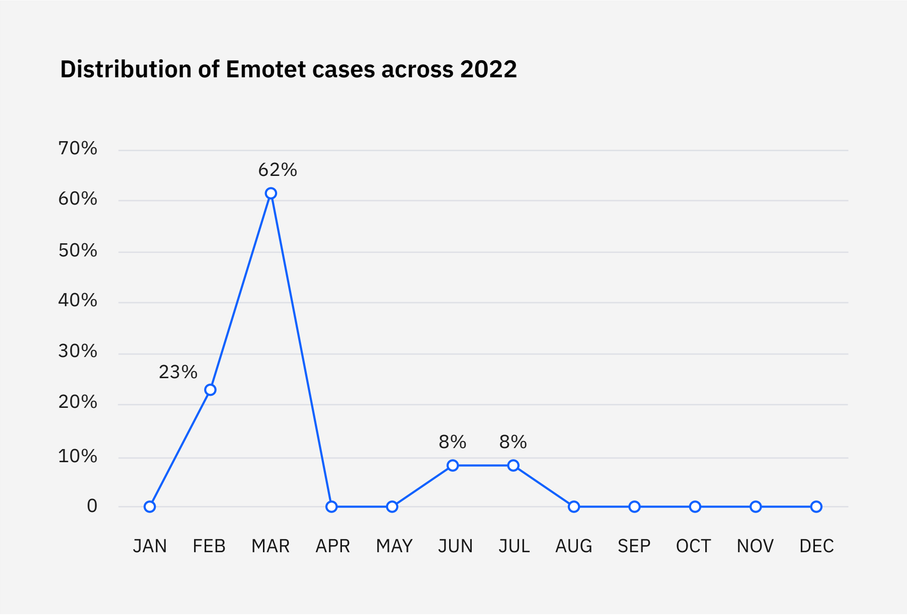


Figure 8: Graph showing spike in Emotet cases in early 2022. Source: X-Force

In cases where a backdoor deployment was classified as an action on objective, it's probable that the threat actor had additional plans when the backdoor was operationalized. Successful intervention by security teams or incident responders likely prevented the threat actor from fulfilling further objectives. Such further malicious activity would likely have included ransomware, as about two-thirds of those backdoor cases had the markings of a ransomware attack.

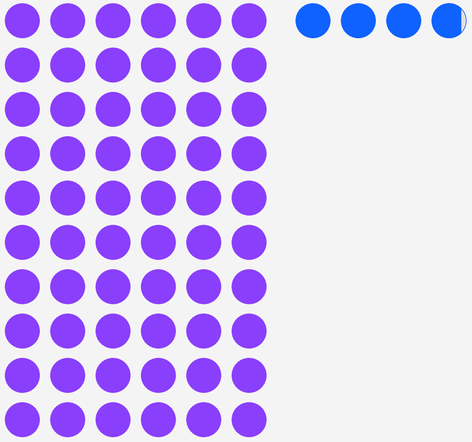
Increased backdoor deployment may also be due to the amount of money this kind of access can generate on the dark web. Compromised corporate network access from an initial access broker typically sells for several thousands of US dollars. This type of access may be sought by malicious actors looking to make a quick profit by avoiding issues with maintaining access while moving laterally and exfiltrating high-value data. Those malicious actors who lack access to the requisite malware to establish access themselves may also seek backdoors.

Initial access brokers typically attempt to auction their accesses, which X-Force has seen at USD 5,000-10,000, though final prices may be less. Others have reported accesses selling for USD 2,000-4,000, with one reaching USD 50,000. These amounts compare to the significantly lower price for something like a single credit card, seen offered for under USD 10.

Backdoors led to a notable spike in Emotet cases in February and March. That spike inflated the ranking of backdoor cases significantly, as those deployed in this timeframe account for 47% of all backdoors identified globally throughout 2022. Following Emotet's hiatus from July through November—after which it ramped back up for nearly two weeks at much lower volume—the number of backdoor cases dropped significantly.

Ransomware attack average duration

2019	2021
2+ months	3+ days



Ransomware

Even amid a chaotic year for some of the most prolific ransomware syndicates, ransomware was the second most common action on objective, following closely behind backdoor deployments and continuing to disrupt organizations' operations. Ransomware's share of incidents declined from 21% in 2021 to 17% in 2022.

An IBM Security X-Force study revealed there was a 94% reduction in the average time for the deployment of ransomware attacks. What took attackers over two months in 2019 took just under four days in 2021. With attackers moving faster, organizations must take a proactive, threat-driven approach to cybersecurity.

One particularly damaging way ransomware operators distribute their payload across a network is by compromising domain controllers. A small percentage, approximately 4%, of network penetration test findings by X-Force Red revealed entities that had misconfigurations in Active Directory that could leave them open to privilege escalation or total domain takeover. In 2022, X-Force also observed more aggressive ransomware attacks on underlying infrastructure, such as ESXi and Hyper-V. The potentially high impact of these attack methods underscores the importance of securing domain controllers and hypervisors properly.

Ransomware variants

As ransomware groups and related access brokers come and go, X-Force has seen regular churn in the top groups active in this space. X-Force encountered 19 ransomware variants in 2022, compared to 16 in 2021. LockBit variants comprised 17% of total ransomware incidents observed, up from 7% in 2021. Phobos tied with WannaCry for second at 11%. The top groups in 2022 displaced 2021's first place REvil, also known as Sodinokibi, with 37% of cases in 2021, and second place Ryuk with 13%, both down to 3%.

LockBit 3.0 is the latest variant of the LockBit ransomware family that's part of a ransomware-as-a-service (RaaS) operation associated with LockerGoga and MegaCortex. LockBit has been in operation since September 2019, and LockBit 3.0 was released in 2022. A significant portion of the LockBit 3.0 source code appears to have been borrowed from the BlackMatter ransomware.

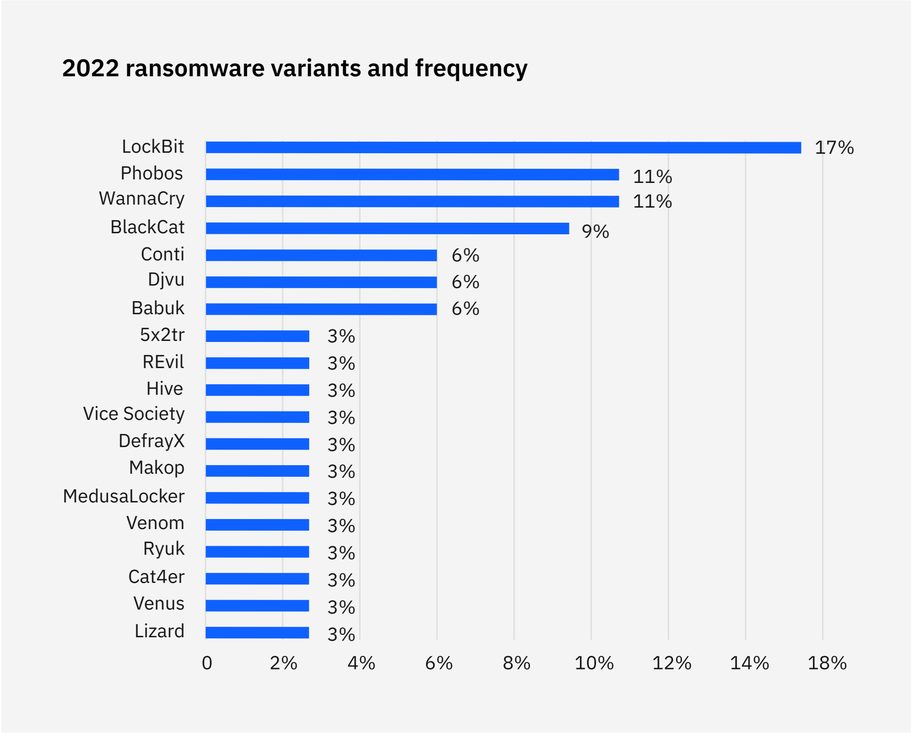


Figure 9: Ransomware variants and the frequency with which they were observed in X-Force Incident Response engagements in 2022. Source: X-Force

Researchers first discovered Phobos ransomware in early 2019. Based on similarities in code, delivery mechanisms, exploitation techniques and ransom notes, Phobos was identified as a fork of the previously known ransomware families Crysis and Dharma. Phobos has been commonly used for smaller-scale attacks, which involve lower ransom demands. Email phishing campaigns and exploitation of vulnerable Remote Desktop Protocol (RDP) ports are the main distribution methods observed for Phobos.

WannaCry, first seen in 2017, spreads itself by using EternalBlue to exploit the vulnerability in the Microsoft Server Message Block 1.0 (SMBv1) server (MS17-010). Several cases of WannaCry or Ryuk that X-Force saw in 2022 were the result of infections from three to five years ago and occurred on old, unpatched equipment, highlighting the importance of proper cleanup after such events.

Business email compromise (BEC)

BEC held its rank of third in 2022 with 6% of incidents to which X-Force responded. This rank is slightly lower than 8% of attacks in 2021 and 9% for fifth place in 2020. It displaced 2021's second place attack, which was server access attacks. This type of attack occurs when an attacker gains access to a server for unknown end goals—which in 2022 was more granularly classified by what type of access those actors achieved. Spear phishing links were used in half of BEC cases to which X-Force responded. Malicious attachments and abuse of valid accounts were used to enable BEC attempts in 25% of cases each.

06

Top impacts

X-Force also took a closer look at the effect of incidents on victim organizations to better understand the impact that threat actors sought to have through the incidents to which X-Force responded. With this information, organizations can get a better understanding of the most common impacts to plan responses to potential future incidents more effectively.

The analysis found that more than one in four incidents aimed to extort victim organizations—making it the top impact observed across incidents remediated by X-Force. The observed extortion cases were most frequently achieved through ransomware or BEC, and often included the use of remote access tools, cryptominers, backdoors, downloaders and web shells.

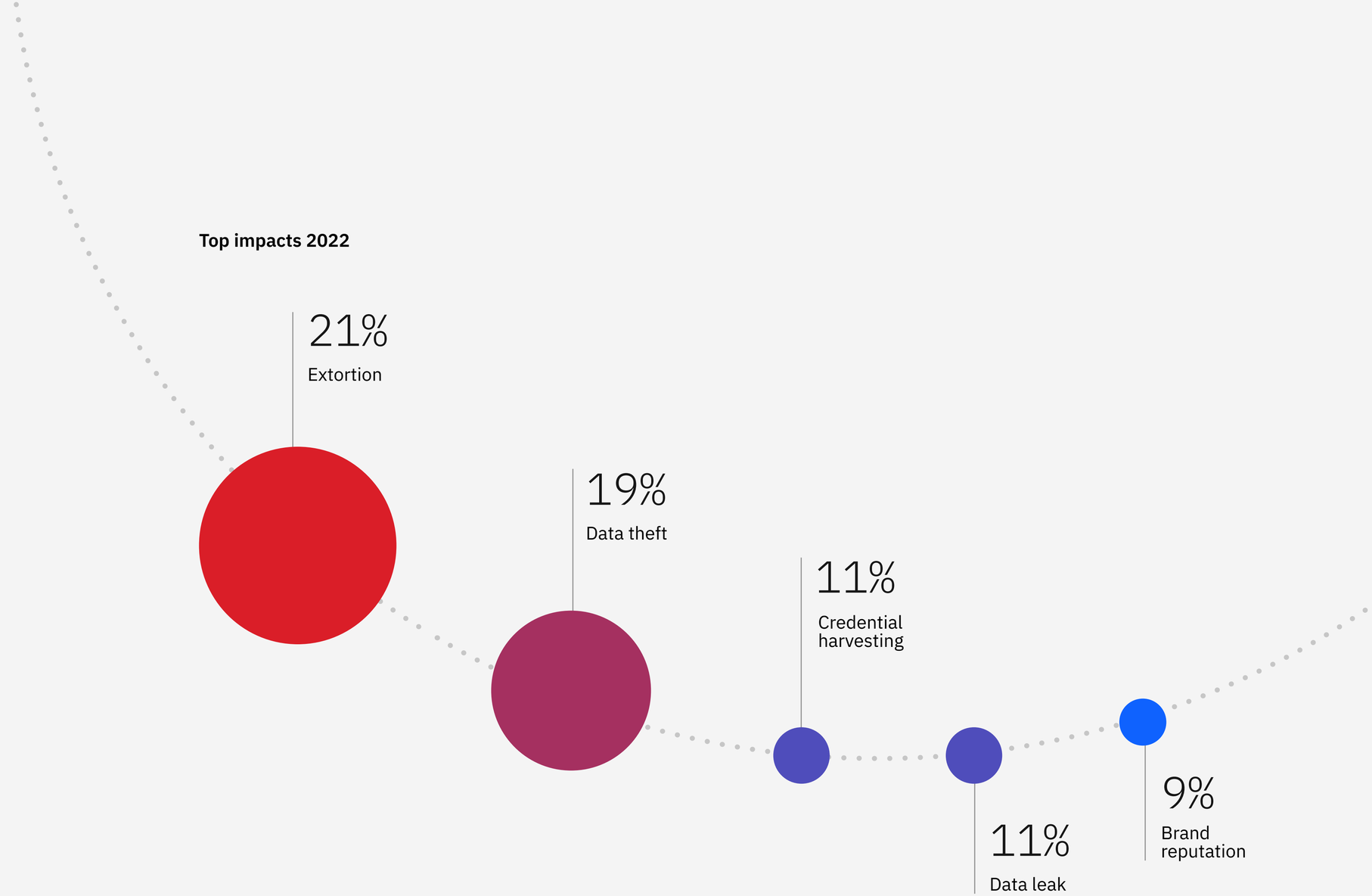


Figure 10: Top impacts X-Force observed in incident response engagements in 2022. Source: X-Force

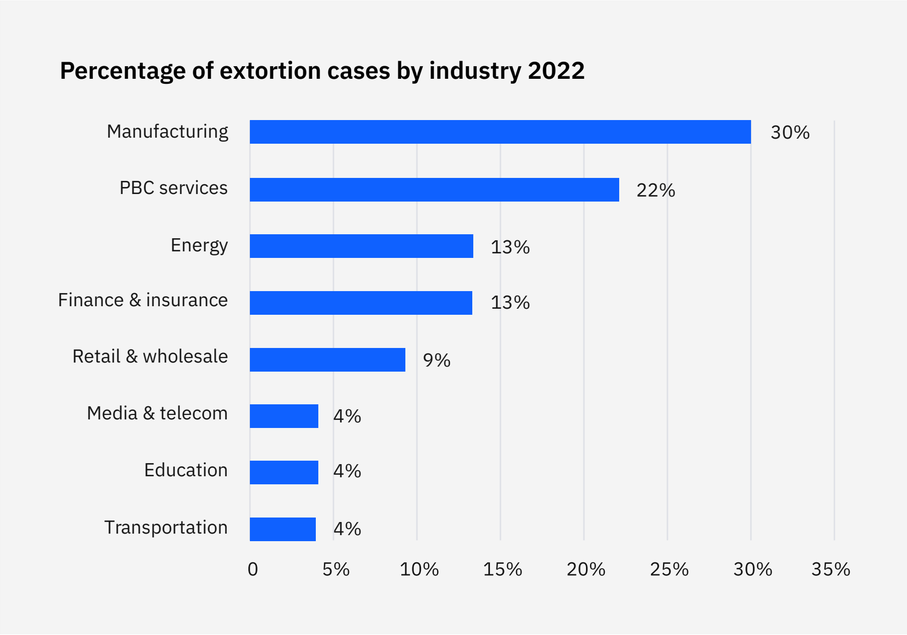


Figure 11: The percentage of extortion cases by industry X-Force observed in incident response engagements in 2022. Numbers do not add to 100% due to rounding. Source: X-Force

Data theft came in second and accounted for 19% of all incidents that X-Force remediated. Credential harvesting that led to stolen usernames and passwords and required corresponding mitigations accounted for 11%. Incidents where X-Force could identify targeted information actually leaked after being stolen was less common than the theft of data at 11%. Impacts to brand reputation, such as disruption to the services clients provide to their customers, accounted for 9% of incidents. See Appendix for the full list of impacts X-Force tracked. Incidents that impacted victims' brand reputation were mainly distributed denial of service (DDoS) attacks, which are also frequently used to extort victims to pay money to stop the attack.

Notable developments in online extortion[1-9]

Year	Event	Tactic
2013	Cryptolocker—one of the first major ransomware outbreaks	Data encryption
2014	DDoS 4 Bitcoin, Armada Collective	Ransom DDoS
2015	Chimera ransomware adds threat of leaking stolen data online	Double extortion
2017–18	BitPaymer and SamSam	Big game hunting
2020	Vastaamo ransomware case	Triple extortion

Extortion

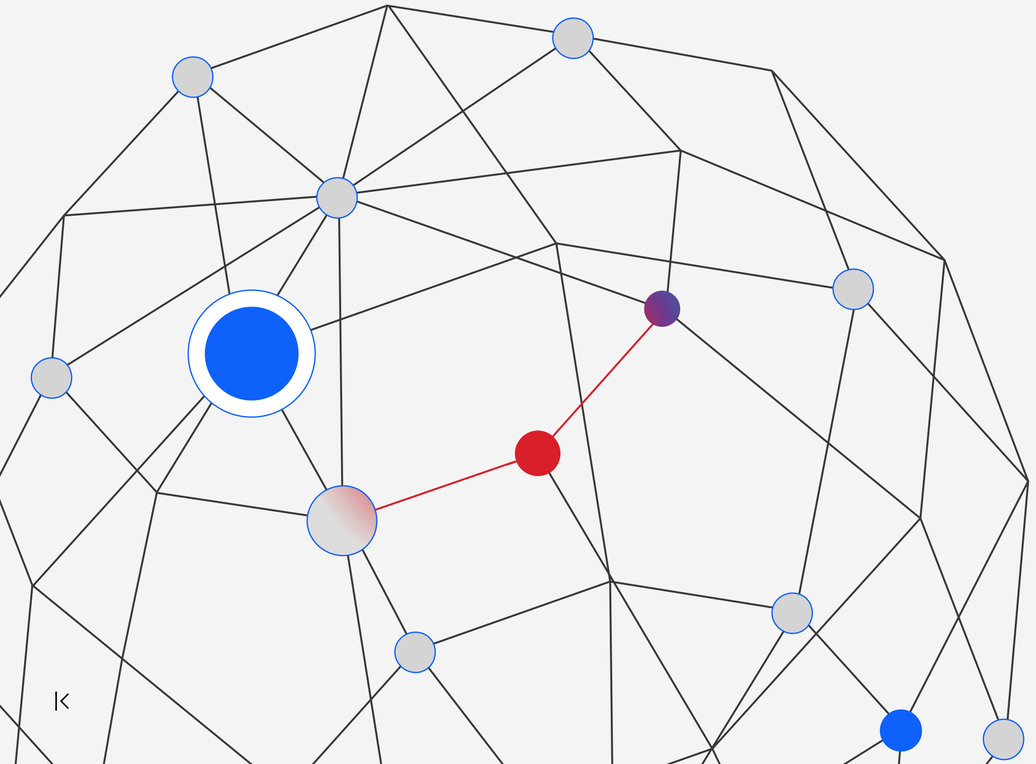
While extortion is most commonly associated with ransomware today, extortion campaigns have included a variety of methods to apply pressure on their targets. These include DDoS threats, encrypting data and, more recently, double and triple extortion threats combining several previously seen elements.

Another tactic that at least one ransomware group experimented with starting in 2022 was making the data they had stolen more accessible to downstream victims. By making it easier for secondhand victims to identify their data among a data leak, operators seek to increase the subsequent pressure on the organization targeted by the ransomware group or affiliate in the first place. In 2023, X-Force expects to see threat actors experimenting with enhanced or novel downstream victim notification to increase the potential legal and reputational costs of an intrusion.

Often, both defenders and victims of cyberattacks focus on the observed impacts to an organization by threat actors. However, it's important to consider the intentions of threat actors, their capabilities and how they evolve over time. This approach enables better discernment of what the next evolution of capabilities may be. Given the ever-expanding menu of extortion options and ransomware actors' primary goal of financial gain, the X-Force team assesses that threat actors will continue to evolve and expand their extortion methodologies to find new ways to pressure victims into paying.

07

Cyber-related developments of Russia’s war in Ukraine



Russian state-sponsored cyber activity following Russia’s invasion of Ukraine has not, as of this publication, resulted in the widespread and high-impact attacks originally feared by Western government entities. However, Russia has deployed an unprecedented number of wipers against targets in Ukraine, highlighting its continued investment in destructive malware capabilities. Furthermore, the invasion has led to the resurgence of hacktivist activity undertaken by groups sympathetic to either side, as well as a reordering of the Eastern European cybercriminal landscape.

Considering Russia’s demonstrated advanced capabilities for cyberattacks against critical infrastructure since 2015, international cybersecurity agencies issued a warning in April 2022. The warning mentioned potentially significant cyber operations and related disruptions in Ukraine and elsewhere. X-Force assessed the most significant threats that have emerged include the return of hacktivism and wiper malware, as well as significant shifts in the cybercriminal world. Most of these operations victimized entities centered in Ukraine, Russia and neighboring countries, but some have spread to other areas, as well.

Alternatively, defenders are adeptly employing the strides made in detection, response and information sharing that were developed over the last several years. Many of the early attempted wiper attacks were quickly identified, analyzed and publicized. These attacks include at least eight identified wipers and the discovery and disruption of a planned Russian cyberattack on Ukraine's electric grid in April 2022.

In cyberspace, the most widely-felt effects of the ongoing war come from self-proclaimed hacktivist groups operating in support of Ukrainian or Russian national interests. While many groups have formed since Russia's invasion and are operating against both Russian and Ukrainian networks to make political points, Killnet is one of the most prolific Russia-sympathetic groups. It has claimed DDoS attacks against public services, government ministries, airports, banks and energy companies based in North Atlantic Treaty Organization (NATO) member states, allied countries in Europe, as well as in Japan and the United States. Entities that fit Killnet's targeting profile should consider ensuring that DDoS mitigation measures are in place, such as engaging the services of a third-party DDoS mitigation provider.

Timeline of select hacktivist events 2022

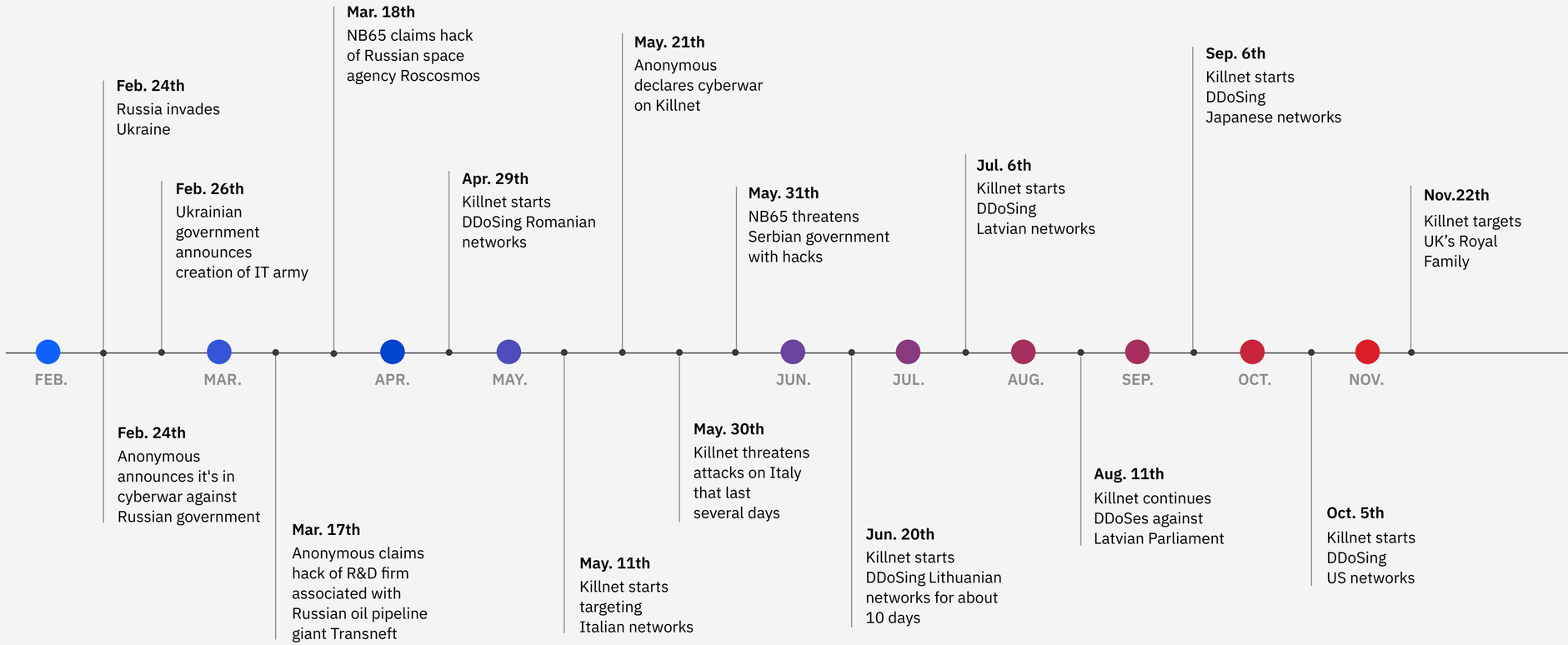


Figure 12: Image showing hacktivist events observed to date during the conflict in Ukraine.
Source: X-Force analysis of open source reporting

Wipers featured in Russia's war in Ukraine

Russia’s war in Ukraine stands out for the use of multiple wiper families deployed against multiple targets in rapid succession and on a scale not previously seen, as well as the use of malware alongside kinetic military operations.

These deployments include at least nine new wipers—AcidRain, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AwfulShred, OrcShred and SoloShred. These wipers were predominantly used against Ukrainian networks from before the initial invasion through the early stages of the war, mainly January through March 2022. While wipers have been used in the past, they have been mostly stand-alone campaigns against a limited set of targets. However, the notable exceptions of WannaCry and NotPetya, which spread indiscriminately after impacting their initial victims, raise concerns of such wipers either spreading more widely or being repurposed for malicious operations elsewhere.

X-Force continues to assess that Russian state-sponsored cyberthreat actors still pose significant threats to computer networks and critical infrastructure around the world. This judgment is based on longstanding Russian cyberoperations aimed at Ukrainian, European, NATO and US networks and attack operations executed by Russian threat groups since 2015.

Upheaval among Russian cybercrime groups

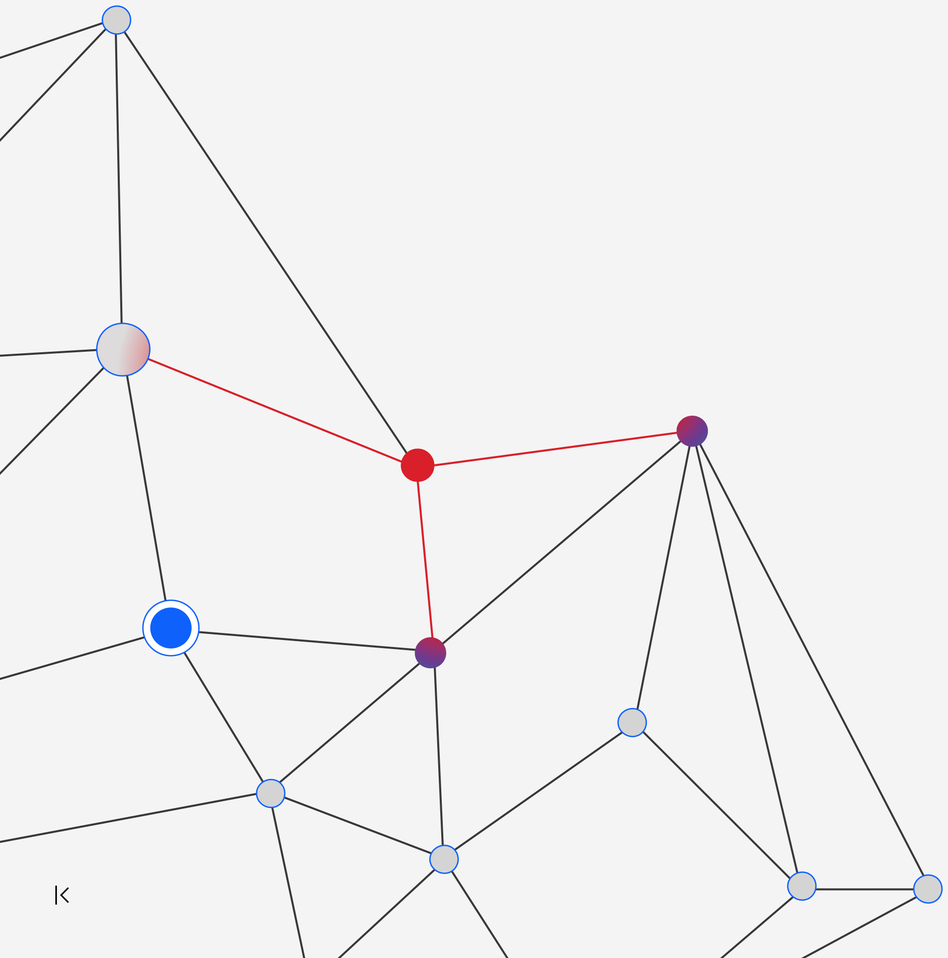
2022 was a tumultuous year for ITG23—one of the most prominent Russian cybercriminal syndicates primarily known for developing the Trickbot banking Trojan and Conti ransomware. The group suffered a series of high-profile leaks in early 2022, after publicly backing Russia's involvement in the war. Referred to as the ContiLeaks and TrickLeaks, they resulted in the publication of thousands of chat messages and the doxing of numerous group members. X-Force uncovered evidence indicating that ITG23 began systematically attacking in mid-April through at least mid-June of 2022—an unprecedented shift, as the group had not previously targeted Ukraine.

Additionally, the group has seemingly retired two of their most high-profile malware families, Trickbot and Bazar, and shut down their Conti ransomware operation. Various reports have suggested that a significant reshuffling of personnel may be occurring, with the group splitting into several factions and some members moving on entirely.

The shutdown of Trickbot and Bazar, which accounted for a significant number of infections in 2021, resulted in a void that has been quickly filled by malware families such as Emotet, IcedID, Qakbot and Bumblebee. Prior to its shutdown, ITG23 was still deploying Conti ransomware prolifically, accounting for a third of all ransomware engagements to which X-Force responded in the first quarter of 2022.

The group also released a new version of their Anchor malware, a stealthy backdoor that the group had traditionally deployed against high-profile targets. The upgraded version discovered by X-Force, and named AnchorMail, has a novel email-based command and control (C2) communication mechanism. The C2 server uses the Simple Mail Transfer Protocol Secure (SMTPS) and Internet Message Access Protocol Secure (IMAPS) protocols, and the malware communicates with the server by sending and receiving specially crafted email messages.

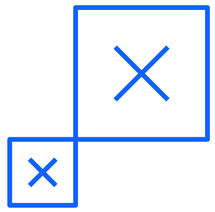
The malware landscape



Increase in USB-spreading worms

After X-Force observed Raspberry Robin infection attempts impacting organizations in mid-May 2022, the enigmatic worm began spreading quickly within victims' networks from users sharing Universal Serial Bus (USB) devices. The infections spiked in early June, and by early August Raspberry Robin peaked at 17% of infection attempts that X-Force observed. This peak was identified in the oil and gas, manufacturing and transportation industries. The 17% infection attempt rate in these industries is significant, since less than 1% of X-Force clients in total have seen the same strain of malware. X-Force also observed more Raspberry Robin activity from September through November 2022.

The spread of USB-based worms is enabled through social engineering and requires some physical access to a network or endpoint to infect successfully, whether by a legitimate user or some other means. X-Force advises ensuring your security tools block known USB-based malware, implementing security awareness training and disabling autorun features for any removable media. In especially sensitive environments, such as OT or where air gaps exist, it's safest to simply prohibit the use of USB flash drives entirely. If it's necessary to allow them, strictly control the approved number of portable devices for use in your environment in addition to implementing the previous suggestions.



Rust rises

The Rust Programming Language steadily increased in popularity among malware developers during 2022, thanks to its cross-platform support and low antivirus detection rates compared to other, more common languages. Similar to the Go language, it also benefits from a more convoluted compilation process that can make the malware more time-consuming to analyze for reverse engineers. Several ransomware developers have released Rust versions of their malware, including BlackCat, Hive, Zeon and most recently RansomExx. Additionally, X-Force has analyzed an ITG23 crypter written in Rust, along with the CargoBay family of backdoors and downloaders. The rising popularity of Rust highlights a continued focus across the ransomware ecosystem on innovating to evade detection.

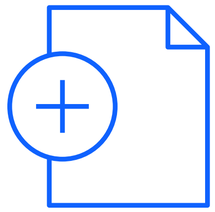
Vidar InfoStealer

X-Force noted a sudden influx of Vidar InfoStealer malware which began in June 2022 and continued through early 2023. First observed in 2018, Vidar is a malicious information-stealer Trojan, distributed as malware as a service (MaaS). The Trojan is usually executed by users clicking on malicious spam (malspam) links or attachments. Due to its extensive feature set, Vidar can be used to retrieve a wide variety of device information that includes credit card information, usernames, passwords and files, as well as taking screenshots of the user's desktop. Vidar can also steal Bitcoin and Ethereum cryptocurrency wallets.

Attacks through an information stealer (info stealer) are typically financially motivated. The stolen data is analyzed, and any valuable information is collated and organized into a database.

This database can then be sold on the dark web or through the private messaging app, Telegram. Threat actors may use the information to commit various types of fraud, such as applying for bank loans or credit cards, purchasing items online or making fraudulent health insurance claims.

Threat actors can use compromised login credentials to gain entry to corporate accounts and remote services. The average cost to use an info stealer is approximately USD 250 per month, and it's up to the users to deploy the malware of their choice. X-Force regularly sees marketplaces attempting to sell access captured by info stealer malware for USD 10-75. When access has been obtained, threat actors can easily use the hacked account's privileges as a starting point to initiate further malicious activity.



Evolution of malware delivery mechanisms

It has become increasingly commonplace for malware to be delivered through malicious Microsoft Office documents, usually attached to phishing emails. Malware developers created these documents containing malicious macros designed to execute malware when the document is opened. The use of macros for this purpose became so widespread that Microsoft Office products started including security warnings when opening macro-enabled documents. In July 2022, Microsoft began to block macro execution by default in documents received through email or from the internet.

As defenders increased their detection and prevention capabilities, threat actors began moving away from Visual Basic Application (VBA) to an older existing macro format within Microsoft Excel known as Macro 4.0. Malicious Excel documents have been used for quite some time. However, most security mechanisms were built around VBA macros within an Excel document. For a time, Excel Macro 4.0 macros provided a good means of evading detection. Around this same time, some threat actors began sending links within an email to take a victim to a dropper site to download the malicious documents rather than sending them as a mail attachment. As Microsoft made changes to allow administrators to disable Macro 4.0 and also block execution of macros downloaded from the internet, threat actors were forced to change tactics again.

After Microsoft’s changes, many malware authors still use macro-enabled Microsoft Office documents, but sophisticated groups adopted a more intricate and complex infection chain. These newer tactics involve a combination of HTML files that have a binary embedded within or a password-protected compressed file. Those files also contain an ISO image which may contain a LNK file, CMD file or other file types unlikely to be sent to an email recipient or downloaded from the internet. Others include remote template injection or exploitation of vulnerabilities. CVE-2021-40444, a remote code execution vulnerability in Microsoft HTML (MSHTML), is one example where a software component is used to render web pages in Microsoft Windows to execute the malware, rather than relying on macros.

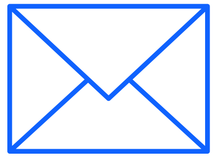
Spam data highlights ransomware threat and further illustrates macro trends

X-Force analyzed trends in phishing and spam email to better understand their overall effectiveness and use by threat actors. The investigation found that spam emails have been used regularly throughout the year to deliver malware, such as Emotet, Qakbot, IcedID and Bumblebee, which often lead to ransomware infections.

Malware[10-18]	**Ransomware**
Trickbot	*Conti*
Bazarloader	*Conti*, Diavol
IcedID	*Conti*, Quantum
Bumblebee	*Conti*, Diavol, Quantum
Emotet	*Conti*, BlackCat, Quantum
Qakbot	*REvil*, *Conti*, Black Basta
SocGholish	LockBit

The data in this table covers the period from late 2021 to the publication of this report. Italics indicate that the malware or ransomware was seen in 2022, but has not been observed by X-Force as of at least October 2022.

X-Force identified a surge of Qakbot activity in September 2022 that used HTML smuggling to compromise victims. Those infections are linked to extensive post-compromise activity, including reconnaissance, information gathering and deployment of additional payloads. Unchecked Qakbot infections throughout 2022 led to multiple Black Basta infections. X-Force saw ransomware attacks claimed on the Black Basta ransomware group's leak site markedly decrease during the break in Qakbot's phishing activity in the summer of 2022. X-Force expects the resumption of Qakbot activity will similarly be correlated with higher numbers of ransomware victims.



Circumventing macros

The use of ISO and LNK files has emerged as an important tactic to infecting victim organizations in response to Microsoft's macro changes starting in October 2021. This tactic includes both direct delivery of their payloads through those container files, as well as obfuscating macro-enabled files within them.

- ISO files and compressed files are being used to circumvent the mark of the web (MOTW) attribute that Microsoft is using to help targets enable malicious macros. While the ISO or compressed files will look to be downloaded from the internet, the macro-enabled attachment within it will not, allowing threat actors to continue this attack.
- Another way of getting around macro restrictions is to include payloads directly in LNK files that, when clicked, launch arbitrary commands mostly used to either download or load the next stages. Prior to early 2022, there was only one campaign in February 2021 that used this tactic. X-Force first saw it recurring in late February-March 2022 and now sees it regularly.

Additional trends that X-Force detected in threat actors' spam campaigns include the increased use of encrypted compressed archives as attachments and thread hijacking, as explained here.

- Encrypted compressed extensions, which are more difficult for antivirus software to detect and flag as malicious, were discovered more frequently in 2022. The average number of spam emails with such attachments delivered per week increased ninefold in 2022, compared to 2021 data since April of that year.
- Thread hijacking, in which threat actors insert themselves into existing email threads, is a longstanding tactic used to increase spam legitimacy and more effectively entice victims to engage. This tactic saw a marked rise in 2022—when compared to the majority of 2021—and tapered off by the spring, a trend that X-Force assesses is driven in large part by Emotet spamming.

Figure 13: Figures show percentage by month of total thread hijacking attempts detected in X-Force data since April 2021. Source: X-Force

– Emotet returned in November 2021 after the botnet was disrupted in January 2021. It continued activity into 2022, took a nearly four-month break starting mid-July, and returned for nearly two weeks in November 2022.

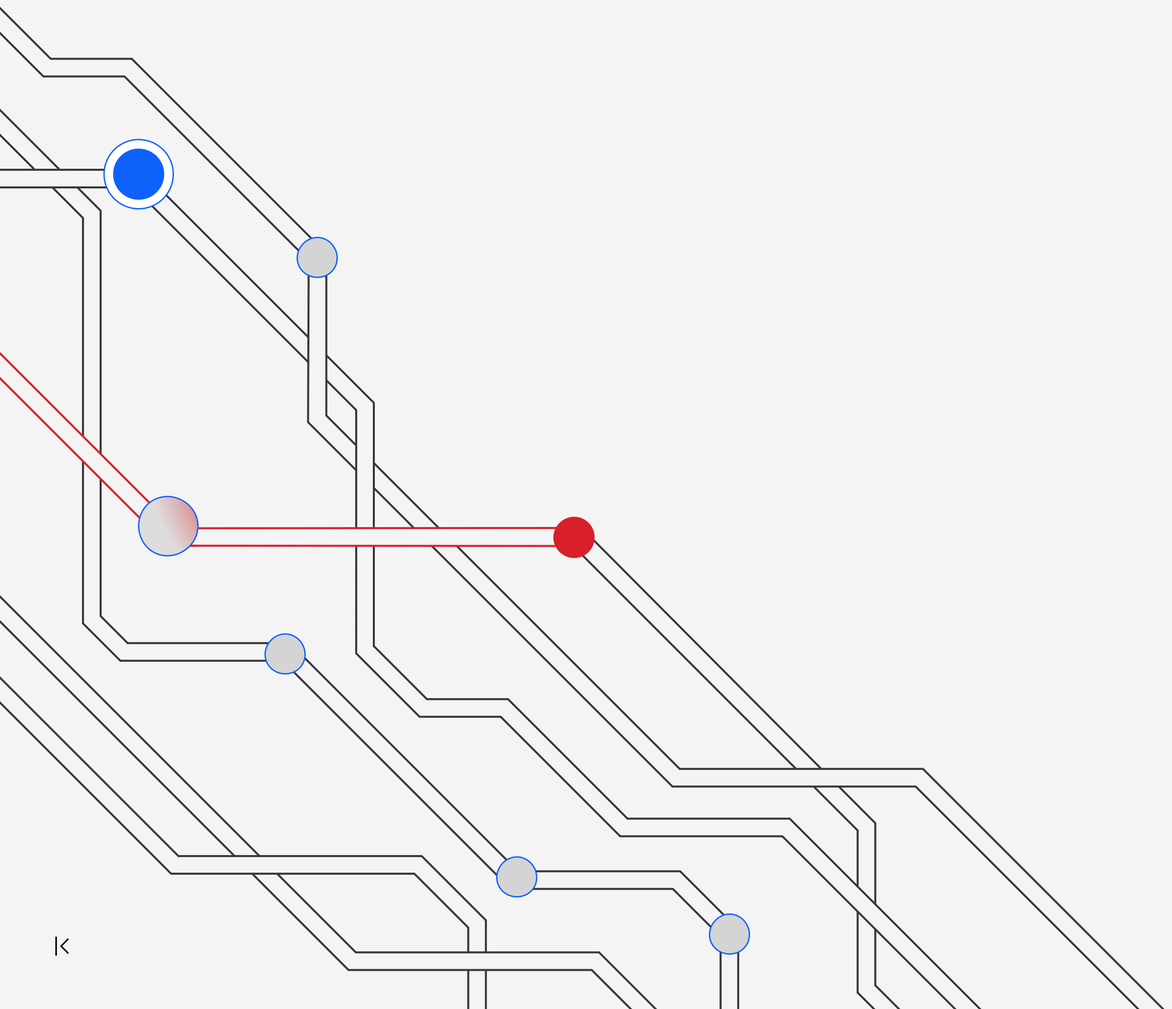
– The data showed just about twice as many regular attempts per month in 2022 compared to available data since April 2021. Thread hijacking was on an unsteady incline through May 2022, and its decline in the latter half of the year aligns roughly with Emotet's inactivity.

– Spam email leading to Emotet, Qakbot and IcedID made heavy use of thread hijacking. Emotet's return in November 2021 contributed to the unsteady increase through May 2022. The overall decline in the latter half of the year aligns with Emotet's hiatus from July through October and brief return in November 2022.

– Tracking thread hijacking and accurately distinguishing it from instances of actors simply adding a reply subject line header to a spam email is difficult and likely to become more so. For example, some threat actors have started to remove "Re:" subject line headers, likely because they are aware that these headers can be used to track their activity.

09

Threats to OT and industrial control systems



Threats to operational technology

2022 saw the discovery of two new OT-specific pieces of malware, Industroyer2 and INCONTROLLER, also known as PIPEDREAM, and the disclosure of many OT vulnerabilities called OT:ICEFALL. The OT cyberthreat landscape is expanding dramatically, and OT asset owners and operators need to be keenly aware of the shifting landscape.

X-Force looked more closely at OT-specific network attack and IR data to help derive insights on how threat actors are seeking to compromise clients in OT-related industries. Network attack data shows brute force attacks, use of weak and outdated encryption standards and weak or default passwords are common alerts in these industries' IT and OT environments.

Alerts indicating probable brute force attempts were most common among Incident Command System (ICS)-specific network attack data, followed closely by weak encryption alerts. The most common alerts for weak encryption concerned the continued use of Transport Layer Security (TLS) 1.0, an outdated and insecure encryption method deprecated in March 2021. Though the US government recommends reconfiguration to use TLS 1.2 or 1.3, National Institute of Standards and Technology (NIST) guidelines address in more depth the common reality. This reality is that older systems may need to continue using weaker versions of encryption to ensure continued functionality. Weak or default password alerts were also notable, especially given these are basic

vulnerabilities that make brute force attacks easier for attackers. Widespread and likely indiscriminate internal and external vulnerability scanning was the most common attack attempt against OT-related industries. The data revealed that old vulnerabilities and threats are still relevant today. A group of vulnerabilities discovered in 2021 by Cisco Talos in Advantech R-SeeNet monitoring software triggered a slim majority of vulnerability scanning alerts across OT industries in 2022. These vulnerabilities could allow attackers to execute arbitrary code or commands.

The second most common vulnerability, however, dates back to 2016—a filter bypass vulnerability in the Trihedral VTScada application, CVE-2016-4510, that could allow unauthenticated users to send HTTP requests to access files. Further highlighting the risks of older threats are attack types, like WannaCry and Conficker, which continue to pose significant threats to OT.

Manufacturing continues to be the most targeted OT industry

Looking at the subset of incidents in OT-related industries, manufacturing was the most attacked in 2022, according to the data. The industry was victimized in 58% of incidents X-Force assisted in remediating. Deployment of backdoors was the top action on objective, identified in 28% of cases in the manufacturing sector. Ransomware actors in particular find this industry to be an attractive target, likely due to these organizations' low tolerance for downtime.

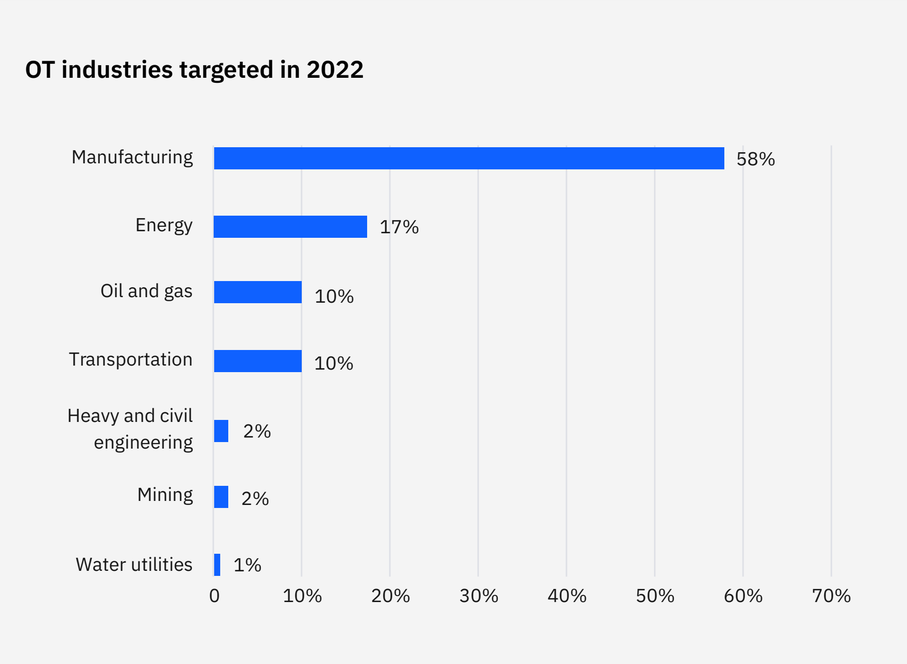


Figure 14: Proportion of IR cases by OT-related industry to which X-Force responded in 2022.
Source: X-Force

Looking at initial access vectors across cases in OT-related industries, spear phishing accounted for 38% of cases, including use of attachments at 22%, use of links at 14% and spear phishing as a service at 2%. Exploitation of public-facing applications took second place at 24%, following the broader industrywide trend. Detection of backdoors also led among these industries' incidents in 20% of cases, followed by ransomware at 19%. Extortion also remains in first among impacts at 29%, with data theft close behind in 24% of cases.

Another major vulnerability exploited in OT is lack of proper segmentation between OT and IT networks. The team at X-Force Red Adversary Simulation Services regularly targets weak segmentation to gain access to isolated OT environments. These environments include targeting jump servers, dual-homed operator workstations and reporting servers, such as data historians that expose web and SQL services from OT to corporate IT networks. Properly segmenting these portions of your networks and closely monitoring communication across them can keep assets safe.

Geographic trends

For the second year in a row, the Asia-Pacific region holds the top spot as the most-attacked region in 2022, accounting for 31% of the incidents to which X-Force IR responded. Europe followed closely behind with 28% of attacks and North America saw 25% of incidents. Asia-Pacific and Europe saw higher proportions of cases, increasing five percentage points and four percentage points respectively from 2021 figures, with a significant drop in the Middle East from 14% to 4%.

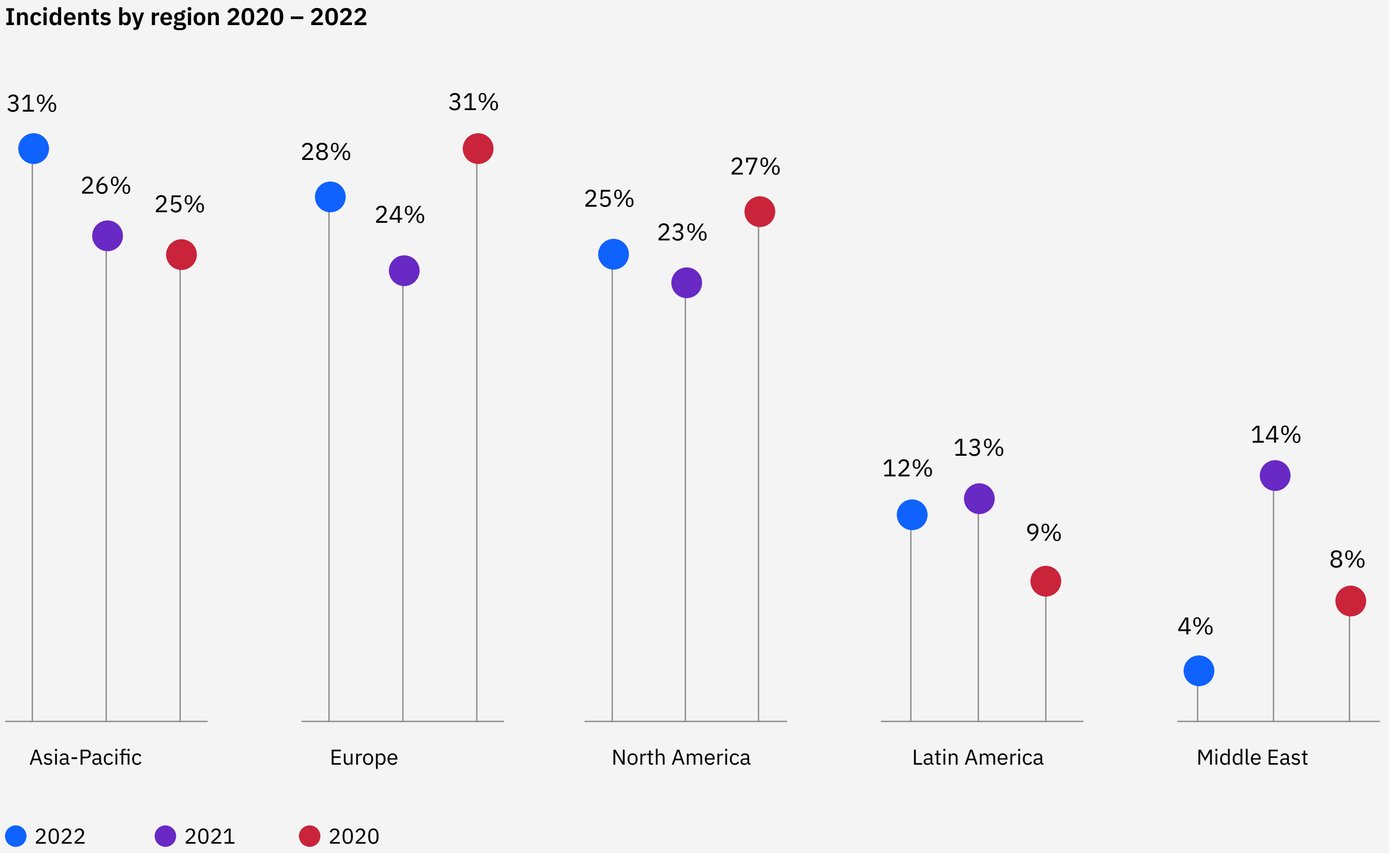


Figure 15: Proportion of IR cases by region to which X-Force responded from 2020-2022. Source: X-Force

#1 | Asia-Pacific

The Asia-Pacific region, specifically Japan, was the epicenter of the Emotet spike in 2022. While not directly related to the war in Europe, the surge of Emotet cases in Japan occurred alongside Russia's invasion of Ukraine, which other researchers in the cybersecurity community noted helped drive significant Emotet activity at the time. Spam campaigns were identified across several industries, with most cases occurring in manufacturing and finance and insurance. Emotet is delivered mainly through spam campaigns that use attention-grabbing headlines.

Manufacturing tops the list of attacked industries in this region in 48% of cases, with finance and insurance a distant second place at 18%.

Spear phishing by attachment was the top infection vector at 40% across this region, followed by exploiting public-facing applications at 22%. Cases of external remote services and spear phishing links tied for third place at 12%.

Deployments of backdoors were the most common action on objective in 31% of cases in the region. Ransomware placed second at 13% and maldocs third at 10%. Extortion was the most common impact observed in 28% of cases. Impacts to brand reputation was in second place at 22% and data theft was in third place at 19%.

Japan accounted for 91% of Asia-Pacific cases, the Philippines 5%, and Australia, India and Vietnam each at 1.5%.

The Asia-Pacific region saw manufacturing as the top-attacked industry at 48% of cases.

#2 | Europe

Europe saw a significant uptick in the deployment of backdoors starting in March 2022, just after Russia invaded Ukraine. Deployments of backdoors accounted for 21% of cases in the region and ransomware 11%. Remote access tools were identified in 10% of incidents to which X-Force responded. Of impacts to clients, 38% of cases X-Force observed in Europe were extortion-related, 17% resulted in data theft and 14% were credential harvesting. Europe was the region hardest hit by extortion, representing 44% of all extortion cases observed.

The exploitation of public-facing applications was the top infection vector used against European organizations, accounting for 32% of all incidents that X-Force remediated in the region, several of which led to ransomware infections. Abuse of valid local accounts came in second place at 18%, with spear phishing links following at 14%, notably down from 42% in 2021. This decrease in spear phishing links may be a result of better user awareness, stronger email security defenses or more effective defenses catching malware after installation.

Professional, business and consumer services tied with finance and insurance for the most-attacked industry, each ranking 25% of the cases to which X-Force responded. Manufacturing placed second with 12% of cases, and energy and healthcare tied for third place at 10%.

The United Kingdom was the most attacked country in Europe, accounting for 43% of cases. Germany accounted for 14%, Portugal 9%, Italy 8%, and France 7%. “X-Force also responded to smaller numbers of cases in Norway, Denmark, Switzerland, Austria, Greece, Greenland, Spain, and Serbia.

The United Kingdom was the most attacked country in Europe, accounting for 43% of cases.

#3 | North America

X-Force observed a slight increase in the number of incidents in North America, moving from 23% of all cases in 2021 to 25% in 2022.

Energy firms rose to the top of the victim list in North America, constituting 20% of all attacks to which X-Force responded in 2022. Manufacturing and the retail-wholesale sector tied for second place in 14% of cases each. While retail-wholesale held a similar position in 2021, the numbers for manufacturing represented a 50% decline from 2021. Professional, business and consumer services took third place in 2022 at 12%, amid a rise in ransomware and other malware-related cases.

The top identified infection vectors were exploitation of public-facing applications at 35% and spear phishing attachments at 20%. Ransomware incidents accounted for 23% of cases, a few of which were the result of detections of lingering infections of WannaCry or Ryuk dating back to 2018 or 2019, highlighting the importance of proper cleanup after such events. In the region, 12% of cases were botnets, with backdoors and BEC tying for third place at 10% each.

When looking at the top impact threat actors had, credential harvesting took the pole position at 25% of incidents that X-Force remediated in North America. Data leak and data theft tied for second place at 17% each, with extortion accounting for 13% of cases.

The United States accounted for 80% of the region's attacks compared to Canada's 20%.

North America's most commonly attacked organizations were energy firms at 20% of cases.

#4 | Latin America

For the purposes of reporting, IBM considers Latin America to include Mexico, Central America and South America.

Incidents in Latin America bucked global trends, returning retail-wholesale as the most-attacked industry at 28% of cases that X-Force remediated, and moved up from second place in 2021. The finance and insurance industry was the second-most targeted with 24% of cases, followed by energy at 20%.

Ransomware outstripped other attacks in Latin America, accounting for 32% of cases to which X-Force responded. Deployment of backdoors was the second-most identified action on objective at 16%, while BEC and email thread hijacking tied for third place at 11% each. Extortion and data theft were the most commonly seen impacts in the region at 27% of cases, with financial loss at 20%. Data destruction and leaks tied for third place at 13% of cases each.

Top initial access vectors included external remote services at 30% and exploitation of public-facing applications at 20%. Drive-by compromise, hardware additions, valid domain accounts, valid local accounts and spear phishing attachments accounted for 10% each.

In all the cases that X-Force responded to in Latin America, Brazil accounted for 67%, Colombia 17% and Mexico 8%. Peru and Chile split the remaining 8%.

In Latin America, Brazil accounted for 67% of cases to which X-Force responded.

#5 | Middle East and Africa

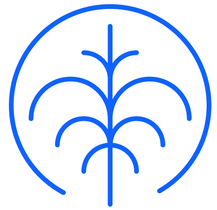
For the purpose of reporting, IBM considers the Middle East and Africa to include the Levant, Arabian Peninsula, Egypt, Iran and Iraq, and the entire African continent.

Deployment of backdoors was detected in 27% of cases to which X-Force responded in this region in 2022. Ransomware and worms tied for the second-most common attack type at 18% each. Extortion and financial loss each accounted for half of identified impacts in incidents across the region in 2021.

Spear phishing links were used for initial access in two-thirds of cases, and removable media accounted for the other third of the incidents that X-Force remediated in the Middle East and Africa. Finance and insurance was the most-targeted industry in the Middle East and Africa in 2022, accounting for 44% of incidents and down slightly from 2021 at 48%. Professional, business and consumer services accounted for 22% of attacks, with manufacturing and energy tying for third place at 11%.

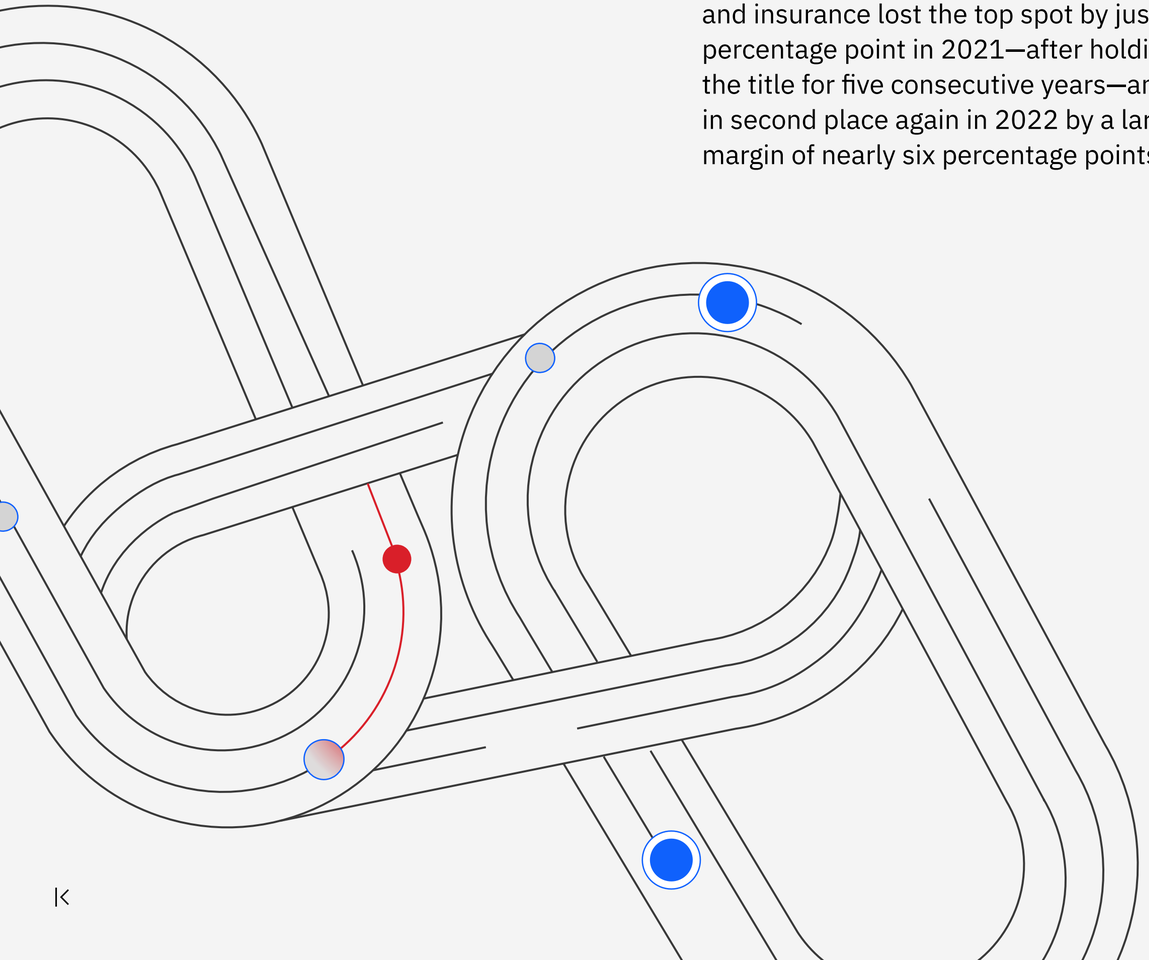
Saudi Arabia comprised two-thirds of the cases in the region to which X-Force responded. The remaining cases were split between Qatar, United Arab Emirates and South Africa.

The most common attack in this region was deployment of backdoors at 27% of cases.



Industry trends

For the second year in a row, manufacturing was the top-attacked industry, according to X-Force incident response data. Finance and insurance lost the top spot by just one percentage point in 2021—after holding the title for five consecutive years—and is in second place again in 2022 by a larger margin of nearly six percentage points.



Share of attacks by industry 2018 – 2022

Industry	2022	2021	2020	2019	2018
Manufacturing	24.8%	23.2	17.7	8	10
Finance and insurance	18.9%	22.4	23	17	19
Professional, business and consumer services	14.6%	12.7	8.7	10	12
Energy	10.7%	8.2	11.1	6	6
Retail and wholesale	8.7%	7.3	10.2	16	11
Education	7.3%	2.8	4	8	6
Healthcare	5.8%	5.1	6.6	3	6
Government	4.8%	2.8	7.9	8	8
Transportation	3.9%	4	5.1	13	13
Media and telecom	0.5%	2.5	5.7	10	8

24.8%

of X-Force incident response cases occurred in the manufacturing sector.

#1 | Manufacturing

Manufacturing was the top-attacked industry and by a slightly larger margin compared to 2021. In 2022, backdoors were deployed in 28% of incidents, beating out ransomware, which appeared in 23% of incidents remediated by X-Force. The percentage of backdoor deployments also was driven by the Emotet infection spike. Some of these cases could have led to ransomware attacks, among other more malicious activity, but they were identified early enough to be remediated.

Spear phishing attachments and exploitation of public-facing applications tied for the top two infection vectors at 28% each. External remote services came in second place at 14%, with spear phishing links and valid default accounts tied for third place as the initial access in 10% of cases.

Extortion was the leading impact to manufacturing organizations, seen in 32% of cases. Manufacturers notoriously have little-to-no tolerance for downtime, and this intolerance makes extortion a lucrative strategy for attackers. Data theft was the second-most common at 19% of incidents, followed by data leaks at 16%. The Asia-Pacific region saw the most incidents in manufacturing in approximately 61% of cases. Europe and North America tied for second place at 14%, Latin American at 8% and the Middle East and Africa at 4%.

18.9%

of X-Force incident response cases occurred in the finance and insurance sector.

#2 | Finance and insurance

Finance and insurance organizations made up less than one in five attacks to which X-Force responded in 2022, earning it second place. This percentage indicated a slight decrease over the past few years as other industries began to gain the attention of attackers, particularly manufacturing.

Finance and insurance organizations tend to be further along in both digital transformations and cloud adoption progress relative to other industries. As a result, attackers may need to work harder to successfully execute attacks against these organizations.

Backdoor attacks were the most commonly observed action on objective at 29%, followed by ransomware and maldocs at 11% each. The top infection vector was spear phishing attachments, used in 53% of attacks against this sector. Exploitation of public-facing applications came in second place at 18% of attacks, and spear phishing links were the initial access vector at 12% of cases.

Europe saw the highest volume of attacks on finance and insurance organizations with approximately 33% of all attacks, with Asia-Pacific a close second place at approximately 31%. Latin America experienced approximately 15% of incidents to which X-Force responded, with North America and the Middle East and Africa experiencing approximately 10% each.

14.6%

of X-Force incident response cases occurred in the professional, business and consumer services sector.

#3 | Professional, business and consumer services

The professional services industry includes consultancies, management companies and law firms. These services make up 52% of victims in this segment. Business services, by contrast, include firms, such as IT and technology services, public relations, advertising and communications. These services represent 37% of victims. Consumer services, encompassing home builders, real estate, arts, entertainment and recreation, accounted for 11% of cases. Together, they form the professional, business and consumer services category of the 2023 X-Force Threat Intelligence Index.

Professional, business and consumer services experienced ransomware and backdoor attacks most frequently in 18% of cases each. The top two infection vectors were the exploitation of public-facing applications and external remote services at 23% each. Spear phishing attachments and valid local accounts were the cause of 15% of cases each.

Extortion was the most common impact in 28% of cases, with data theft, credential harvesting and data leaks at 17% each. X-Force responded to 47% of cases in Europe, 33% in North America, 10% in Asia-Pacific, 7% in the Middle East and Africa, and 3% in Latin America.

10.7%

of X-Force incident response cases occurred in the energy sector.

#4 | Energy

Energy organizations, including electric utilities and oil and gas companies, were the fourth-most attacked industry—the same as 2021—representing 10.7% of attacks. The exploitation of a public-facing application was the most common infection vector at 40%. Spear phishing links and external remote services accounted for 20% of cases each. Botnets were the most frequent action on objective in 19% of cases, with ransomware and BEC tying for second place at 15%.

Data theft and extortion were noted in 23% of cases, followed by credential harvesting and botnet infections at 15% each. In all the cases that X-Force responded to worldwide, North American organizations were the most common victims at 46%, compared to Europe and Latin America at 23% each, and just under 5% in Asia-Pacific and the Middle East and Africa.

The energy industry remains under pressure from a variety of global forces, especially those exacerbated by Russia's war in Ukraine and how that has affected an already tumultuous global energy trade.

8.7%

of X-Force incident response cases occurred in the retail and wholesale sector.

#5 | Retail and wholesale

Retailers are responsible for the sale of goods to consumers and wholesalers. Wholesalers are typically responsible for the transportation and distribution of these goods directly from manufacturers to retailers or directly to consumers. The retail and wholesale industry was the fifth-most targeted industry, according to X-Force IR data, the same as its 2021 ranking.

The most common initial access vector in attacks on retail and wholesale was spear phishing emails with a malicious link at 33%. Compromised external remote services, spear phishing with malicious attachments and hardware additions accounted for 17% each.

Ransomware, backdoors and BEC were the most common actions taken by attackers, each comprising 19% of activities. Worms were identified in 10% of cases. Victims experienced extortion in 50% of cases, and credential harvesting and financial loss at 25% each. North America and Latin America experienced the most cases at 39% each, compared to Europe's 22%.

7.3%

of X-Force incident response cases occurred in the education sector.

#6 | Education

Incidents in education involved backdoor cases in 20% of attacks to which X-Force responded. Ransomware, adware and spam accounted for 13% each. Exploitation of public-facing applications was the most commonly observed initial access in 42% of cases, followed by spear phishing attachments at 25%. Phishing through service, through link and valid cloud and local account abuse comprised 8% of initial access vectors each. Data theft, data leak, extortion and reconnaissance were the impacts at 25% each. Asia-Pacific accounted for 67% of cases, North America for 27% and Latin America for 6%.

5.8%

of X-Force incident response cases occurred in the healthcare sector.

#7 | Healthcare

Healthcare dropped back to seventh place among the top 10 industries, further declining from sixth in 2021. The proportion of healthcare cases to which X-Force has responded has remained at approximately 5%-6% for the last three years. Backdoor attacks occurred in 27% of cases, and web shells in 18%. Adware, BEC, cryptominers, loaders, reconnaissance and scanning tools, and remote access tools comprised 9% each. Reconnaissance comprised most of the observed impacts at 50%, while data theft and digital currency mining were identified in 25% of cases each.

European-based targets accounted for 58% of incidents, with North American cases comprising the remainder at 42%.

4.8%

of X-Force incident response cases occurred in the government sector.

#8 | Government

Government targets were another top target of backdoors, comprising 25% of X-Force IR cases. This percentage tied with DDoS attacks, which also accounted for one-quarter of cases. The rich sensitive information in public sector networks is a common target of cyber espionage campaigns. This information can include extensive databases of PII and other information that could be used by state-sponsored groups or sold for profit by cybercriminals. Maldocs were identified in 17% of cases, and cryptominers, credential acquisition tools, ransomware and web shells split the remainder of cases at 83%.

Of the cases in this sector, X-Force was able to tie incidents to cybercriminals, insider threats that led to data destruction, hacktivists and state-sponsored threat groups conducting espionage, each in equal proportion.

Exploitation of public-facing applications and spear phishing attachments were the lead infection vectors at 40% each, while abuse of valid default accounts comprised 20%. Government entities in Asia-Pacific were the most targeted at 50% of cases, with Europe at 30% and North America at 20%.

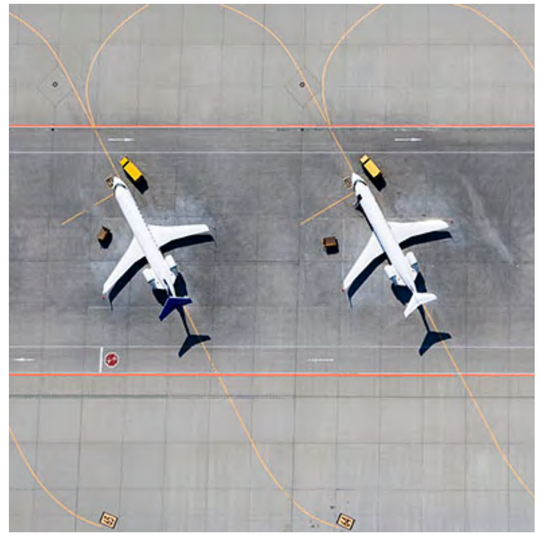
3.9%

of X-Force incident response cases occurred in the transportation sector.

#9 | Transportation

Down from seventh place in 2021, transportation returned to its 2020 ranking of ninth place. However, the industry still comprised roughly the same percentage of incidents to which X-Force responded. Phishing was the most common initial access vector in 51% of cases—evenly split between links, attachments and spear phishing as a service. Abuse of valid local accounts made up 33% of initial access vectors, with valid cloud accounts serving as the entry point for 17% of cases. The top actions on objectives were server access and deployment of remote access tools at 25% each, followed by spam campaigns, ransomware, backdoors and defacement in 13% of cases each.

Data theft was most common in 50% of cases, with extortion and impacts to brand reputation at 25% each. European transportation entities were the most targeted group, comprising 62% of cases, with Asia-Pacific in second place at just over 37%.



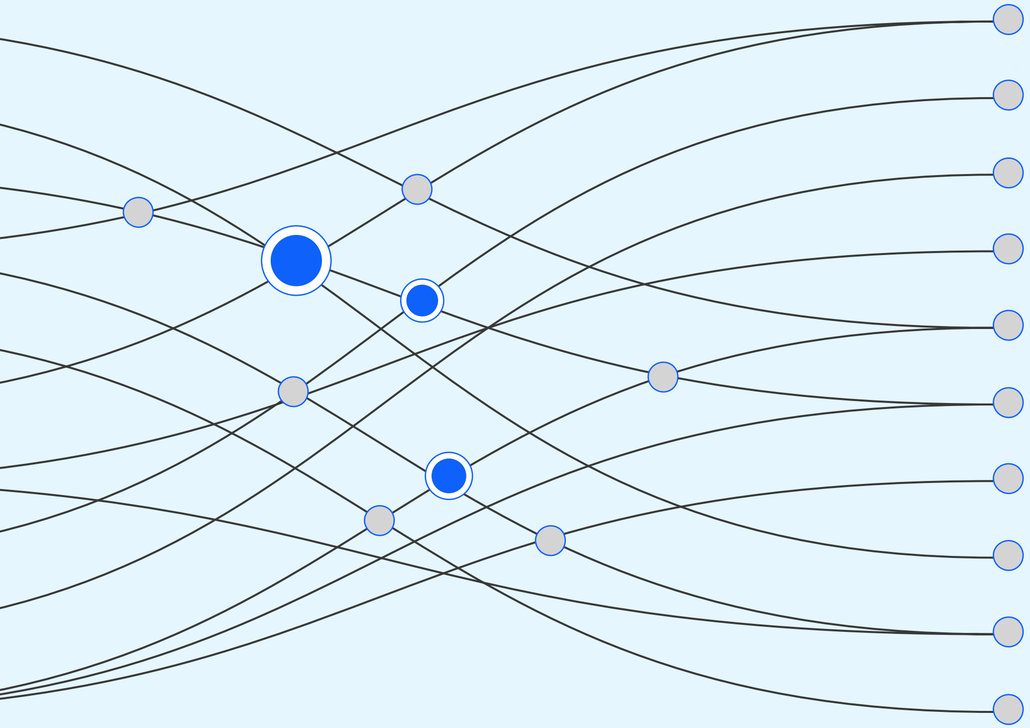
0.5%

of X-Force incident response cases occurred in the media and telecom sector.

#10 | Media and telecom

Media and telecommunications accounted for a small fraction of incidents to which X-Force responded, coming in last place for the second year running. Abuse of external remote services, such as VPNs and other access mechanisms, and valid domain accounts were the observed infection vectors. These vectors led to ransomware attacks. The actions observed in these cases included deployment of ransomware and data exfiltration tools. These actions, in turn, led to data theft, leak, destruction and extortion.

Recommendations



The following recommendations are actions you should take to secure your organization against malicious threats, including those presented in this report.

Manage your assets: “What do we have? What are we defending? What data is critical to our business?” These are the first questions any security team should answer to build a successful defense. Prioritizing discovery of assets on your perimeter, understanding your exposure to phishing attacks and reducing those attack surfaces further contribute to holistic security. Finally, organizations must extend their asset management programs to include source code, credentials and other data that could already exist on the internet or dark web.

Know your adversary: While many organizations have a broad view of the threat landscape, X-Force recommends organizations adopt a view that emphasizes the specific threat actors that are most likely to target your industry, organization and geography. This perspective includes understanding how threat actors operate, identifying their level of sophistication, and knowing which tactics, techniques and procedures attackers are most likely to employ.

Manage visibility: After understanding more about the adversaries most likely to attack, organizations must confirm they have appropriate visibility into the data sources that would indicate an attacker’s presence. Maintaining visibility at key points throughout the enterprise and ensuring alerts are generated and acted on in a timely manner are critical to stopping attackers before they can cause disruption.

Challenge assumptions: Organizations must assume that they already have been compromised. By doing so, teams can continually reexamine the following:

- How attackers can infiltrate their systems
- How well their detection and response capabilities fare against emerging tactics, techniques and procedures
- The level of difficulty for a likely adversary to compromise your most critical data and systems

The most successful security teams perform regular offensive testing including threat hunting, penetration testing and objective-based red teaming to detect or validate opportunistic attack paths into their environments.

Act on intelligence: Apply threat intelligence everywhere. Effective application of threat intelligence will enable you to analyze common attack paths and identify key opportunities for mitigating common attacks, in addition to helping develop high-fidelity detection opportunities. Application of threat intelligence should be coupled with understanding your adversaries and how they operate.

Be prepared: Attacks are inevitable; failure doesn't have to be. Organizations should develop incident response plans customized for their environment. Those plans should be regularly drilled and modified as the organization changes, with a focus on improving response, remediation and recovery time.

Having a reputable IR vendor on retainer reduces the amount of time it takes to get skilled responders focused on mitigating an attack. Additionally, including your IR vendor in response plan development and testing is critical and contributes to a more effective and efficient response. The best IR plans include a cross-organizational response, incorporate stakeholders outside of IT and test lines of communication between technical teams and senior leadership. Finally, testing your plan in an immersive, high-pressure cyber range exercise can greatly enhance your ability to respond to an attack.

Boost security with these actions:

- ☐ Manage your assets
- ☐ Know your adversary
- ☐ Manage visibility
- ☐ Challenge assumptions
- ☐ Act on intelligence
- ☐ Be prepared

About us

IBM Security X-Force

IBM Security X-Force is a threat-centric team of hackers, responders, researchers and analysts. The X-Force portfolio includes offensive and defensive products and services, fueled by a 360-degree view of threats.

In an age of relentless cyberattacks, a connected everything and increasing regulatory mandates, organizations need a focused security approach. X-Force believes the threat should be the focal point. Through penetration testing, vulnerability management and adversary simulation services, the X-Force Red team of hackers assumes the role of threat actors to find security vulnerabilities—exposing your most important assets. Through incident preparedness, detection and response and crisis management services, the X-Force Incident Response team knows where threats may hide and how to stop them. X-Force researchers create offensive techniques for detecting and preventing threats, while analysts with X-Force collect and translate threat data into actionable information for reducing risk.

With a deep understanding of how threat actors think, strategize and strike, X-Force can help you prevent, detect, respond to and recover from incidents and focus on business priorities.

If your organization would like support strengthening your security posture, schedule a one-on-one consultation with an IBM Security X-Force expert.

Schedule a consult →

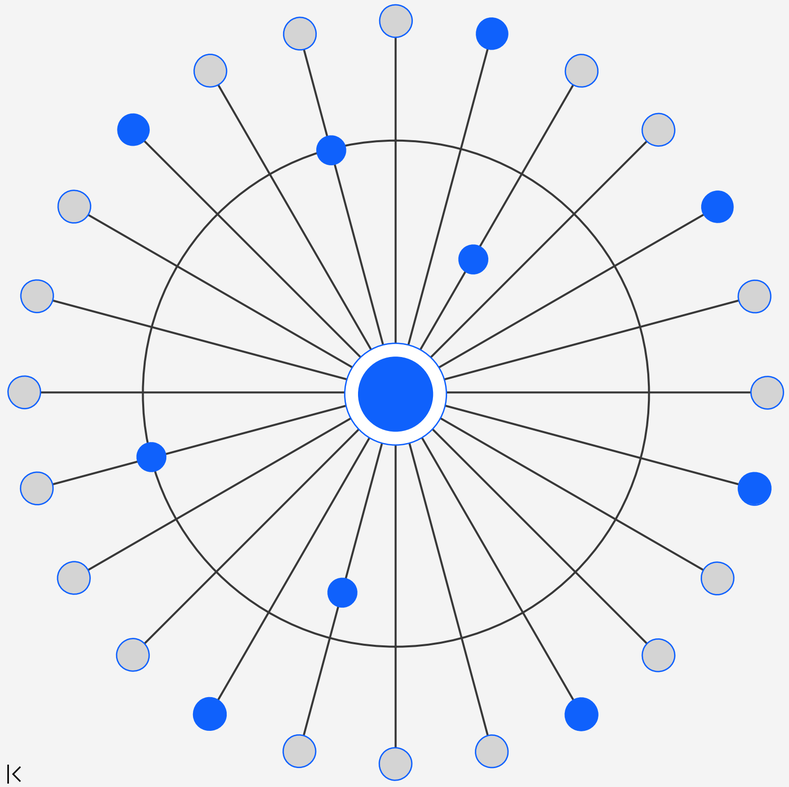
IBM Security

IBM Security adapts to your ever-expanding footprint and works in step with you to keep you on the right track. We help you ensure that you're always staying one step ahead—with greater speed and greater accuracy—with our dynamic AI and automation capabilities. Feel confident that you're making the right moves today and tomorrow with insights from our trusted team of industry-leading experts. From predicting threats to helping to protect data; working across vendors, or around the world; no matter where your business is headed, IBM Security can help you to strive for ambitious business goals, while exploring pivotal new technologies and helping minimize unexpected threats.

Learn more →

14

Contributors



Michael Worley
Christopher Caridi
Michelle Alvarez
Karlina Bakken
Yannick Bedard
Michele Brancati
Christopher Bedell
Joshua Chung
Scott Craig
Joseph DiRe
John Dwyer
Emmy Ebanks
Richard Emerson
Charlotte Hammond
Kevin Henson
Guy-Vincent Jourdan
Vio Onut
Mitch Mayne
Dave McMillen
Kat Metrick
Scott Moore
Golo Mühr
Andy Piazza
Benjamin Shipley
Christopher Thompson
Ole Villadsen
Reginald Wong
John Zorabedian

Appendix

List of impacts

Impacts	Impacts
Botnet	Digital currency mining
Brand reputation	Espionage
Credential harvesting	Extortion
Data destruction	Financial loss
Data leak	Production halted (OT)
Data theft	Reconnaissance

1. “A timeline of the biggest ransomware attacks,” CNET, 15 November 2021
2. “International action against DD4BC cybercriminal group,” Europol, 12 January 2016
3. “DD4BC, Armada Collective, and the Rise of Cyber Extortion,” Recorded Future, 7 December 2015
4. “A Brief History of Ransomware.” Varonis, 10 November 2015
5. “Inside Chimera Ransomware - the first ‘doxingware’ in wild,” MalwardBytes Labs, 8 December 2015
6. “Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware,” Crowdstrike, 14 November 2018
7. “Operators of SamSam Continue to Receive Significant Ransom Payments,” Crowdstrike, 11 April 2018
8. “Triple Extortion Ransomware: The DDoS Flavour,” PacketLabs, 12 May 2022
9. “They Told Their Therapists Everything. Hackers Leaked It All,” Wired, 4 May 2021
10. “BazarCall to Conti Ransomware via Trickbot and Cobalt Strike,” The DFIR Report, 1 August 2021
11. “Diavol Ransomware,” The DFIR Report, 13 December 2021
12. “Quantum Ransomware,” The DFIR Report, 25 April 2022
13. “Bumblebee Loader Linked to Conti and Used In Quantum Locker Attacks,” Kroll, 6 June 2022
14. “This isn't Optimus Prime’s Bumblebee but it’s Still Transforming,” Proofpoint, 28 April 2022,
15. “Understanding REvil: REvil Threat Actors May Have Returned (Updated),” Unit 42, 3 June 2022
16. “AdvIntel’s State of Emotet aka “SpmTools” Displays Over Million Compromised Machines Through 2022,” AdvIntel, 13 September 2022
17. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack,” NCC Group, 19 August 2022
18. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack,” NCC Group, 19 August 2022,

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2023