

X-Force Threat Intelligence Index 2024



Contents

[01 →](#)
Executive summary

[02 →](#)
Report highlights

[03 →](#)
Top initial access
vectors

[04 →](#)
Top actions on
objectives

[05 →](#)
Top impacts

[06 →](#)
Cyberwarfare

[07 →](#)
Generative AI: The new
cyberthreat frontier

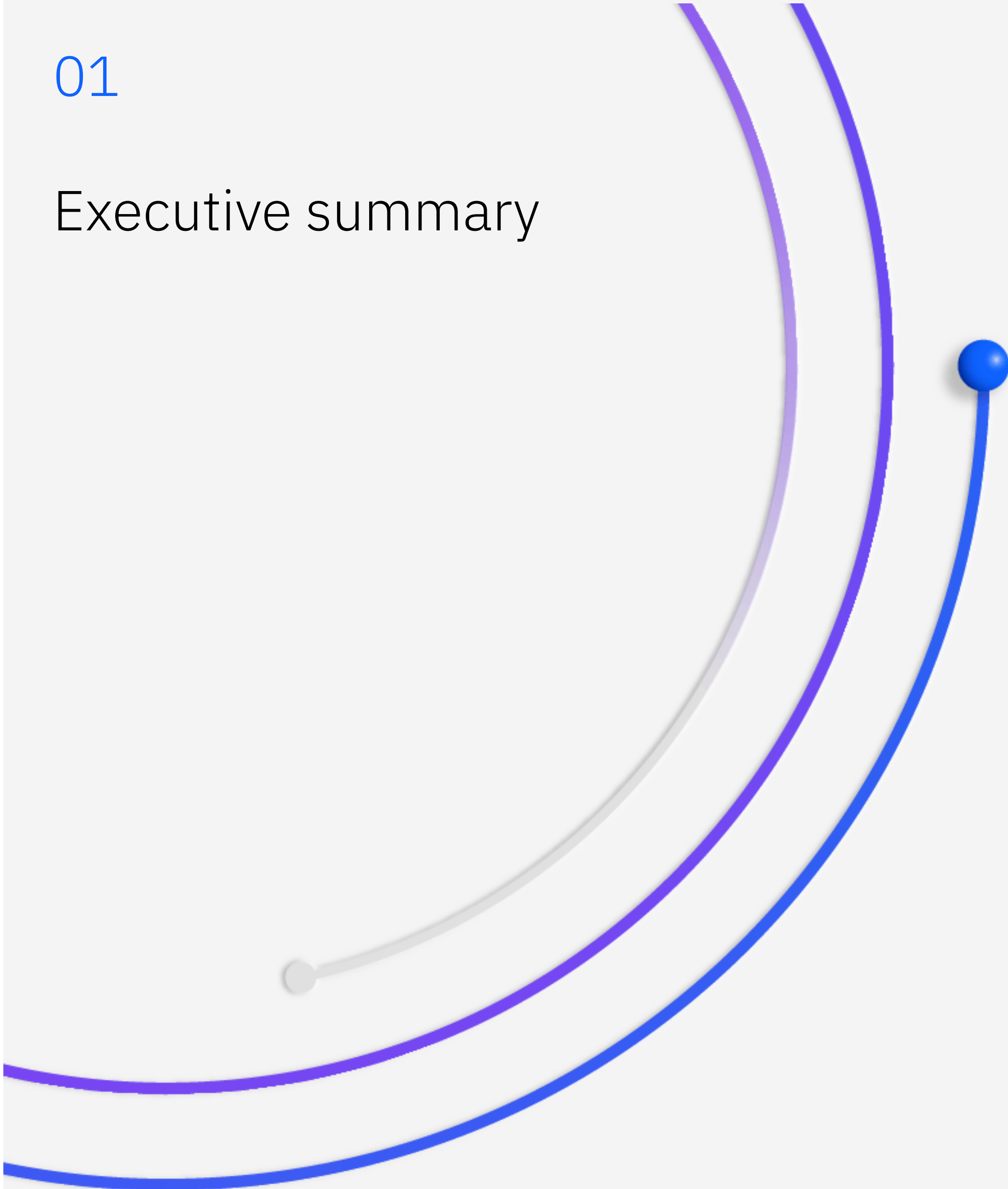
[08 →](#)
Geographic trends

[09 →](#)
Industry trends

[10 →](#)
Recommendations

[11 →](#)
About us

Executive summary



The biggest shift the IBM® X-Force® team observed in 2023 was a pronounced surge in cyberthreats targeting identities. Attackers have a historical inclination to choose the path of least resistance in pursuit of their objectives. In this era, the focus has shifted towards *logging in* rather than *hacking in*, highlighting the relative ease of acquiring credentials compared to exploiting vulnerabilities or executing phishing campaigns. Lack of identity protections was corroborated by IBM X-Force penetration testing data for 2023, which ranked *identification and authentication failures* as the second most common finding.

Additionally, X-Force observed a 100% increase in “Kerberoasting” during incident response engagements. Kerberoasting is a technique focused on compromising Microsoft Windows Active Directory credentials through Kerberos tickets. This indicates a technique shift in how attackers are acquiring identities to carry out their operations.

The prominence of *valid accounts* as a preferred initial access technique among cybercriminals—tying with phishing for the first time—was another notable development. This access technique is accompanied by an upsurge in malware

designed to steal information, known as infostealer malware, activities that bolster the dark web's stolen credentials marketplace. This multifaceted shift underscores the symbiotic relationship among various elements in the cybercrime ecosystem.

It's clear that attackers have recognized the difficulty defenders have in distinguishing between legitimate identity use and unauthorized misuse. This escalation in targeting of identities in cyberattacks underscores the critical importance for organizations to proactively identify, eliminate and audit potential attack vectors within their dynamic networks. These measures are pivotal in reducing

the attack surface, unveiling latent risks and autonomously remediating incidents that are independent of impending threats.

Last year will also go down in history as a generative artificial intelligence (gen AI) breakout year. Policy makers, business executives and cybersecurity professionals are all feeling the pressure to adopt AI within their operations. And the rush to adopt gen AI is currently outpacing the industry's ability to understand the security risks these new capabilities will introduce. However, a universal AI attack surface will materialize once adoption of AI reaches a critical mass, forcing organizations to prioritize security defenses that can adapt to AI threats at scale.

In an attempt to identify key milestones that will indicate when a common AI threat landscape will mature, X-Force assessed previous technology disrupters and their threat maturity milestones. Based on the analysis, X-Force predicts threat actors will begin to target AI broadly once the market coalesces around common deployment models and a small number of vendors. This analysis suggests that AI market dominance is the milestone that will trigger attacker investment in attack toolkits targeting AI.

Despite looming gen AI-enabled threats, X-Force hasn't observed any concrete evidence of generative AI-engineered cyberattacks to date or a rapid shift in attackers' goals and objectives from

previous years. Although X-Force observed a notable drop in ransomware attacks on enterprises in 2023, extortion-based attacks continue to be a driving force of cybercrime this past year. These extortion-based attacks were only surpassed by *data theft and leak* as the most common impact observed in X-Force incident response engagements globally.

The IBM X-Force Threat Intelligence Index offers these insights as a resource to IBM clients, researchers in the security industry, policy makers, the media and the broader community of security professionals and business leaders. It's our intent to keep all parties informed of the current threat landscape so they can make the best decisions for reducing risk.

Report highlights

71%

Increase year over year in volume of attacks using valid credentials

For the first time ever, abusing valid accounts became cybercriminals' most common entry point into victim environments. It represented 30% of all incidents X-Force responded to in 2023.

11.5%

Drop in enterprise ransomware incidents

Despite remaining the most common action on objective (20%), X-Force observed a drop in enterprise ransomware incidents. This drop is likely to impact adversaries' revenue expectations from encryption-based extortion as larger organizations are stopping attacks before ransomware is deployed and opting against paying and decrypting in favor of rebuilding if ransomware takes hold.

32%

Percentage of data theft and leak incidents

Data theft and leak rose to the most common impact for organizations, indicating more groups are favoring this method to obtain financial gains.

266%

Upsurge in use of infostealers

X-Force has observed threat groups who have previously specialized in ransomware showing increasing interest in infostealers. And a number of prominent new infostealers recently debuted and demonstrated increased activity in 2023, such as Rhadamanthys, LummaC2 and StrelaStealer.

30%

Share of security misconfigurations among web application vulnerabilities identified

X-Force penetration testing engagements revealed that the most observed web application risk across client environments globally was security misconfigurations. Of these misconfigurations, the top offenses included allowing concurrent user sessions in the application, which could weaken multifactor authentication (MFA) through session hijacking.

32%

Percentage of incidents that involved malicious use of legitimate tools

Nearly one-third of incidents that X-Force responded to were cases where legitimate tools were used for malicious purposes, such as credential theft, reconnaissance, remote access or data exfiltration.

50%

Market share threshold likely to trigger attacks against AI platforms

X-Force analysis indicates that the establishment of AI market dominance will signal AI attack surface maturity. This analysis suggests that once a single AI technology approaches 50% market share, or when the market consolidates to three or less technologies, the cybercriminal ecosystem will be incentivized to invest in developing tools and attack paths targeting AI technologies.

84%

Percentage of critical infrastructure incidents where initial access vector could have been mitigated

For a majority of incidents on critical infrastructure that X-Force responded to, the initial access vector could have been mitigated with best practices and security fundamentals, such as asset and patch management, credential hardening and the principle of least privilege.

25.7%

Share of manufacturing attack incidents within the top 10 attacked industries

Manufacturing was once again the top attacked industry in 2023 for the third year in a row, representing 25.7% of incidents within the top 10 attacked industries. Malware was the top action on objective observed at 45%. Ransomware accounted for 17% of incidents.

31%

Increase in attacks year over year in Europe

Europe also experienced the highest percentage of incidents (32%) out of the five geographic regions. Malware was the most observed action on objective accounting for 44% of incidents.

Top initial access vectors

One of the top initial access vectors in 2023—jumping from third to first place—was the abuse of valid accounts identified in 30% of the observed incidents X-Force responded to. As defenders increase their detection and prevention capabilities, attackers are finding that obtaining valid credentials is an easier route to achieving their goals, considering the alarming volume of compromised yet valid credentials available—and easily accessible—on the dark web. X-Force found that cloud account credentials alone make up 90% of for sale cloud assets on the dark web, making it easy for threat actors to take over legitimate user identities to establish access into victim environments. Attacker use of valid accounts as an initial access vector appears to have a significant impact on the required response efforts, as well.

Top initial access vectors in 2023 versus 2022

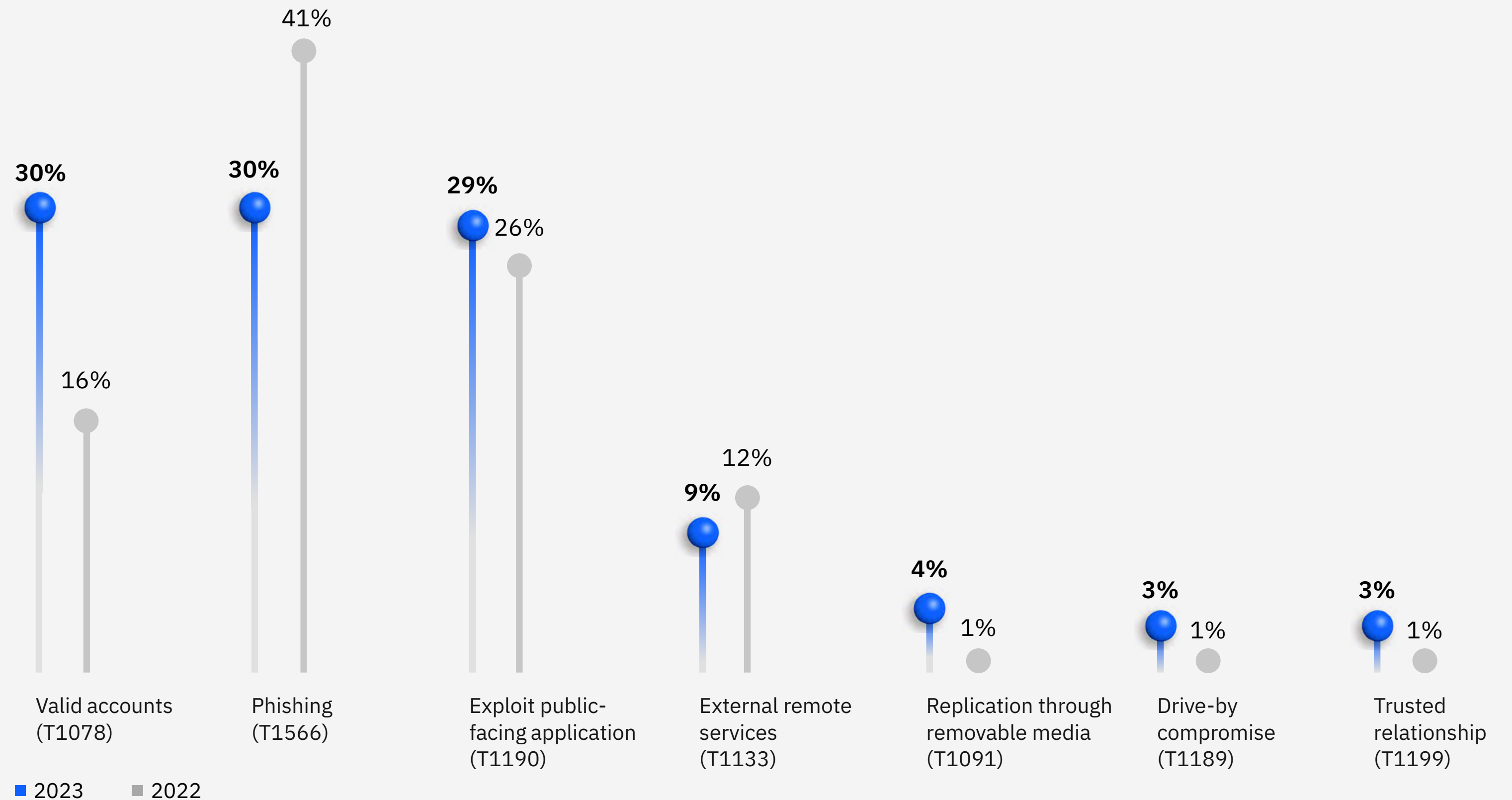


Figure 1: Top initial access vectors X-Force observed in 2022 and 2023. Sources: X-Force and MITRE ATT&CK Matrix¹ for Enterprise framework

In 2023, major incidents where the attacker leveraged a valid account for initial access were associated with more complex response measures by defenders—190% greater than the average incident.

As we will analyze further in the report, we identified a concerning trend in the rise of infostealers and ransomware groups pivoting to infostealing malware. These shifts suggest that threat actors have revalued credentials as a reliable and preferred initial access vector. As threat actors invest in infostealers to grow their credential repository, enterprises are pushed into a new defense landscape where identity can no longer be guaranteed.

Phishing, whether through an attachment, link or as a service, also comprised 30% of all incidents remediated by X-Force in 2023. Although tied

for first place in 2023, the volume of phishing is down by 44% from 2022.

The significant drop in observed compromises through phishing is likely a reflection of both continued adoption and reevaluation of phishing mitigation techniques and strategies, as well as attackers shifting to the use of valid credentials to gain initial access. Using compromised valid credentials is a quick, direct route into the environment. Whereas IBM X-Force Red data indicates that human-crafted phishing emails are time-intensive, requiring on [average 16 hours](#) to craft one. However, it's worth noting that X-Force assesses that phishing is expected to be one of the first malicious use cases of AI that cybercriminals will invest in, theorizing that it's far from done scaling.

In fact, X-Force data shows that AI can generate a deceptive phish in 5 minutes, a potential time savings of nearly 2 days for attackers.

Furthermore, X-Force responded to multiple cases involving email compromises that circumvented MFA measures using [adversary-in-the-middle](#) (AitM) attacks. These attacks started with an initial phishing message that directed users to a reverse-proxy phishing page, which allowed attackers to relay traffic between the user and the legitimate site and thus collect user credentials, MFA input and session cookies. In multiple cases, X-Force observed the threat actor leverage their initial access to carry out both internal and external phishing attempts, as well as further abuse of credentials, to access additional applications.

In third place, exploitation of public-facing applications—defined as adversaries taking advantage of a weakness in an internet-facing computer or program—was identified in 29% of incidents, which is slightly higher than what we observed in 2022.

In 2023, numerous organizations experienced cyberattacks as a result of [widespread exploitation of managed file transfer \(MFT\) tools](#), such as MOVEit and GoAnywhere. MFT exploitation poses a high risk, as these internet-connected file transfer services facilitate the immediate access of sensitive enterprise data by attackers. Until 2023, many defenders overlooked the high-risk nature of MFT tools, leading to inadequately protected

deployments without proper detection and response strategies. This lack of consideration provided threat actors with a significant time advantage, allowing them to scale their attacks undetected. Last year's mass exploitation of MFTs, and the ongoing efforts of ransomware groups focusing on data extortion, underscore the need for organizations to fully understand their enterprise architecture. To facilitate this understanding, organizations should develop threat models that map out their systems and the associated attack paths to their sensitive data stored on premises, in the cloud, or through third parties.

Security misconfigurations top web application risk

New to the 2024 IBM X-Force Threat Intelligence Index, X-Force reviewed hundreds of findings from our penetration testing data to reveal the top Open Worldwide Application Security Project (OWASP) web application security risks. The most observed risk across client environments globally was security misconfigurations, accounting for 30% of total findings. Of this category, penetration testers found more than 140 findings of ways that attackers can exploit misconfigurations. Of these misconfigurations, the top offenses included allowing concurrent user sessions in the application at 15%, which could weaken MFA through session hijacking, verbose error messages at 12% and excessive session timeouts at 8%.

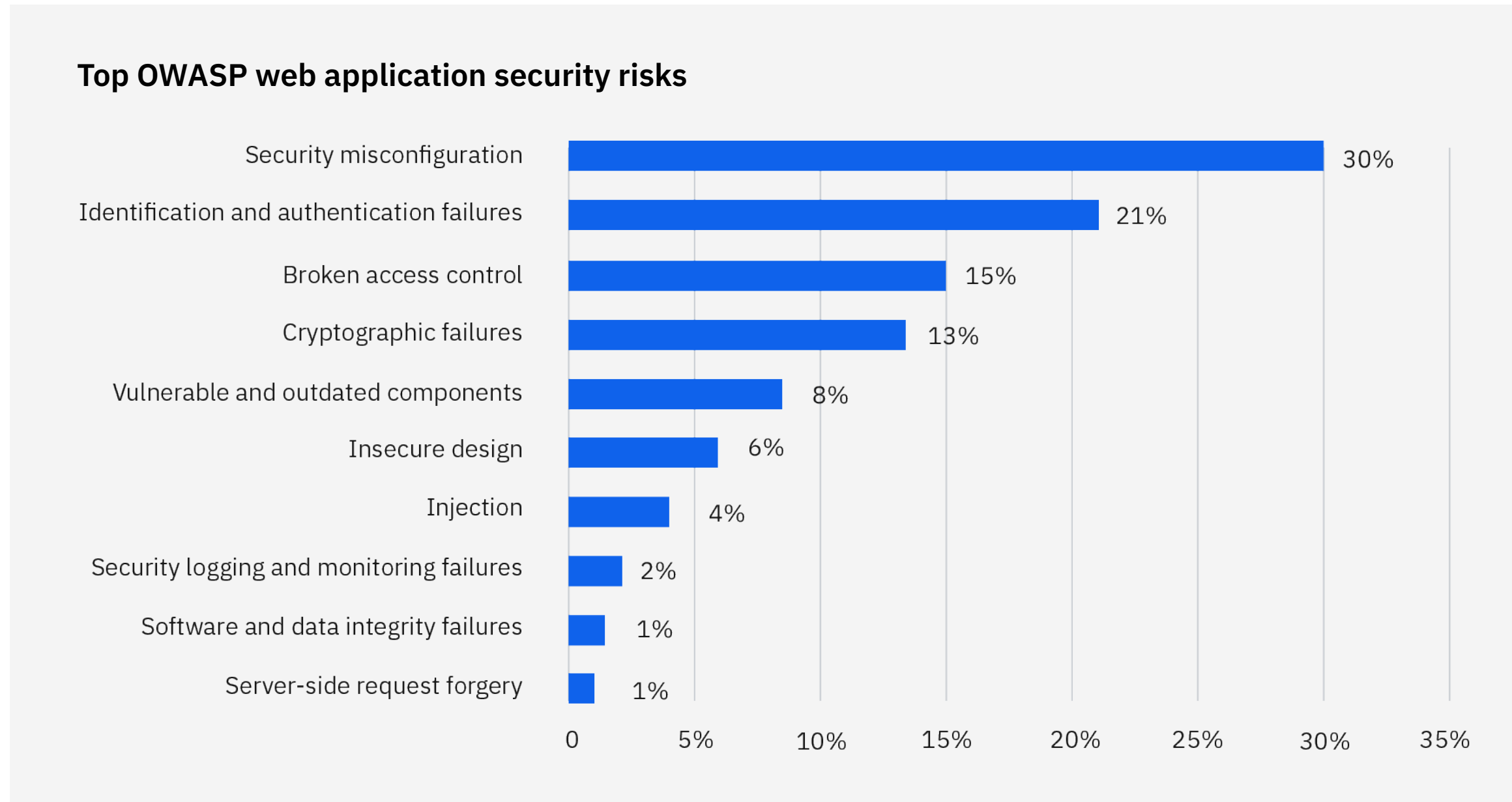


Figure 2. Top OWASP web application security risks based on penetration testing data. Source: X-Force

In second place, identification and authentication failures made up 21% of the most observed web application security risks. Of these findings, the top offenses were weak password policies that included Active Directory password policies (19%), usernames verifiable through errors (17%), Server Message Block (SMB) signing not required and URLs containing sensitive information at 8% each.

Zero-day decline

Every year there are a few vulnerabilities that catch enterprises by surprise and cause widespread damage. In 2023, the CL0P ransomware group exploited a vulnerability in the file transfer application MOVEit, common vulnerabilities and exposures (CVE)-2023-34362, to [expose](#) information on millions of individuals.

While zero-day vulnerabilities garner notoriety, the reality is that zero-day vulnerabilities make up a very small percentage of the vulnerability attack surface—currently at 3% of total vulnerabilities tracked by X-Force. In 2023, there was a 72% drop in the number of zero days compared to 2022 with only 172 new zero-day vulnerabilities. Furthermore, from 2021 to 2022, there was a 44% decrease of new zero-day vulnerabilities, from 1,105 CVEs added in 2021 to 614 CVEs added in 2022. This decrease is likely indicative of attackers finding other less resource-intensive methods to gain entry, such as exploitation of older vulnerabilities or use of valid credentials, compromised or purchased.

The vulnerability problem

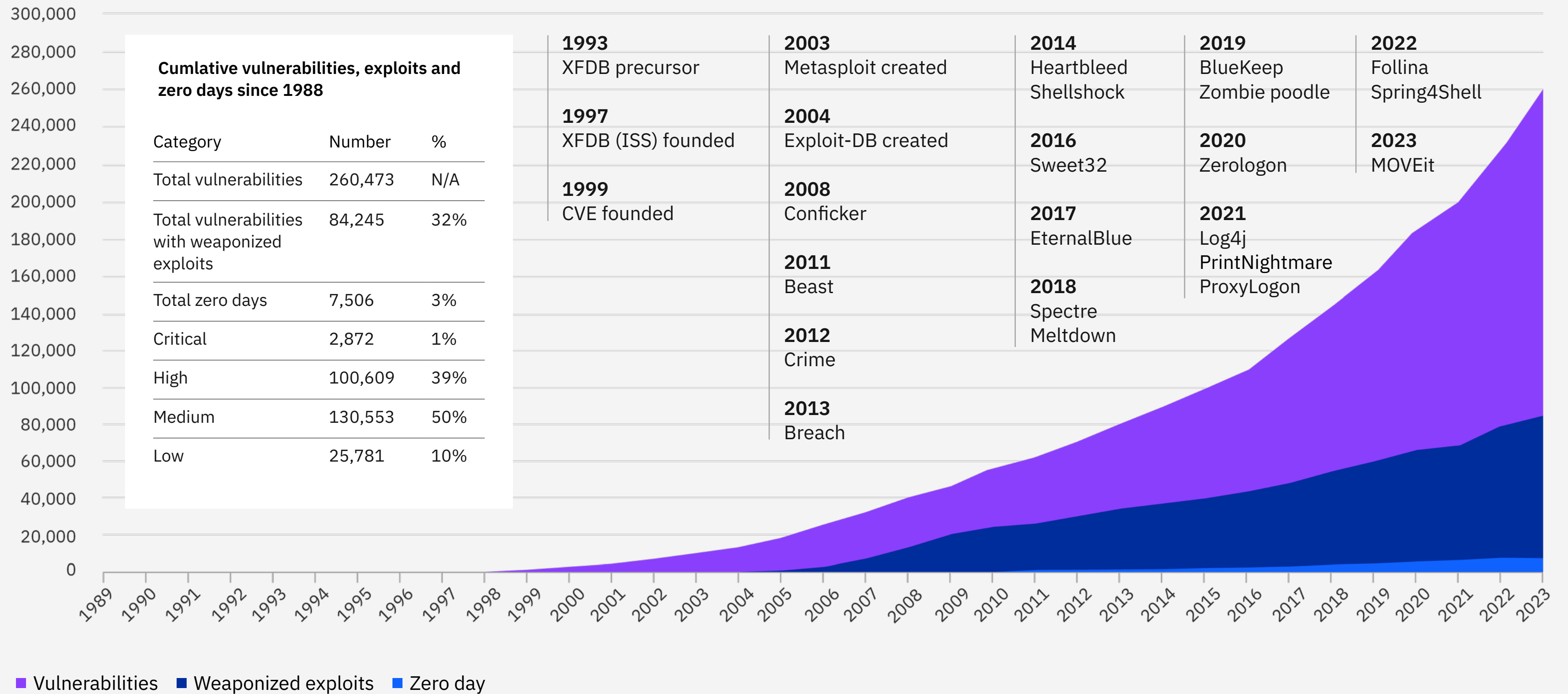


Figure 3: The growth of vulnerabilities, exploits and zero days since 1993. Also included is a timeline of major events involving vulnerabilities since 1993. The X-Force Vulnerability Database is one of the oldest and largest vulnerability databases in the world and reached its 30-year anniversary in 2023.

Linux vulnerabilities

The importance of securing Linux® systems has risen in prominence as increasing amounts of malicious activity targeting Linux have appeared. Malware developers are increasingly [developing Linux malware](#) and creating Linux variants of existing malware families. These changes to the Linux threat landscape highlight the criticality of systems hardening and monitoring for malicious activity.

Methodical vulnerability management is a key aspect of proactive defense. According to Red Hat® Insights vulnerability data from 2023, 92% of customers were found to have at least one CVE with known exploits in their environment at the time of scanning. Furthermore, 81% had three or more CVEs with known exploits in their environment. More than half (67%) had

at least one CVE rated as *Critical*, while 25% had five or more *Critical* CVEs in their environment. Additionally, the majority (80%) of the top ten vulnerabilities with the highest number of hits detected across systems in 2023 were given a *High* or *Critical* Common Vulnerability Scoring System (CVSS) base severity score.

Most threat activity targeting Red Hat Enterprise Linux systems in 2023 was associated with widely distributed threats. According to statistics from the Red Hat Insights malware detection service, the top threats detected were Linux rootkits, malware associated with the recently dismantled [IPStorm botnet](#), which enabled proxying of malicious traffic through compromised devices, and the [PGMiner](#) cryptocurrency mining botnet.

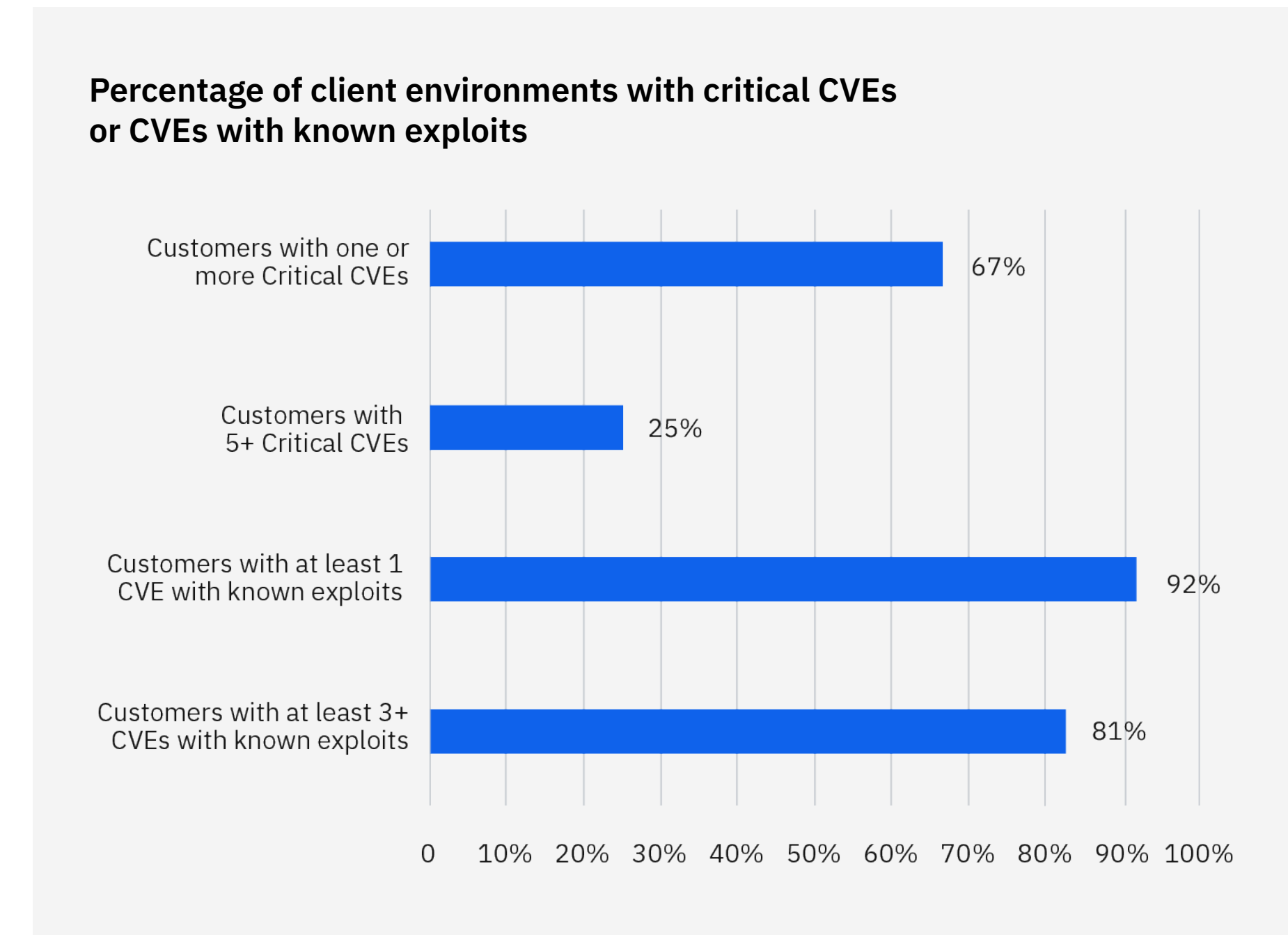


Figure 4: Percentage of client environments with Critical CVEs or CVEs with known exploits. Source: Red Hat Insights

Top actions on objectives

According to IBM X-Force Incident Response data, deployment of malware was the most common action threat actors took on victim networks, occurring in 43% of all reported incidents. Of the total incidents, 20% were ransomware cases. Backdoors and crypto miners were discovered in 6% and 5% of cases, respectively. The remaining malware incidents included infostealers, loaders, bots, worms, web shells and downloaders.

Top actions on objectives 2023

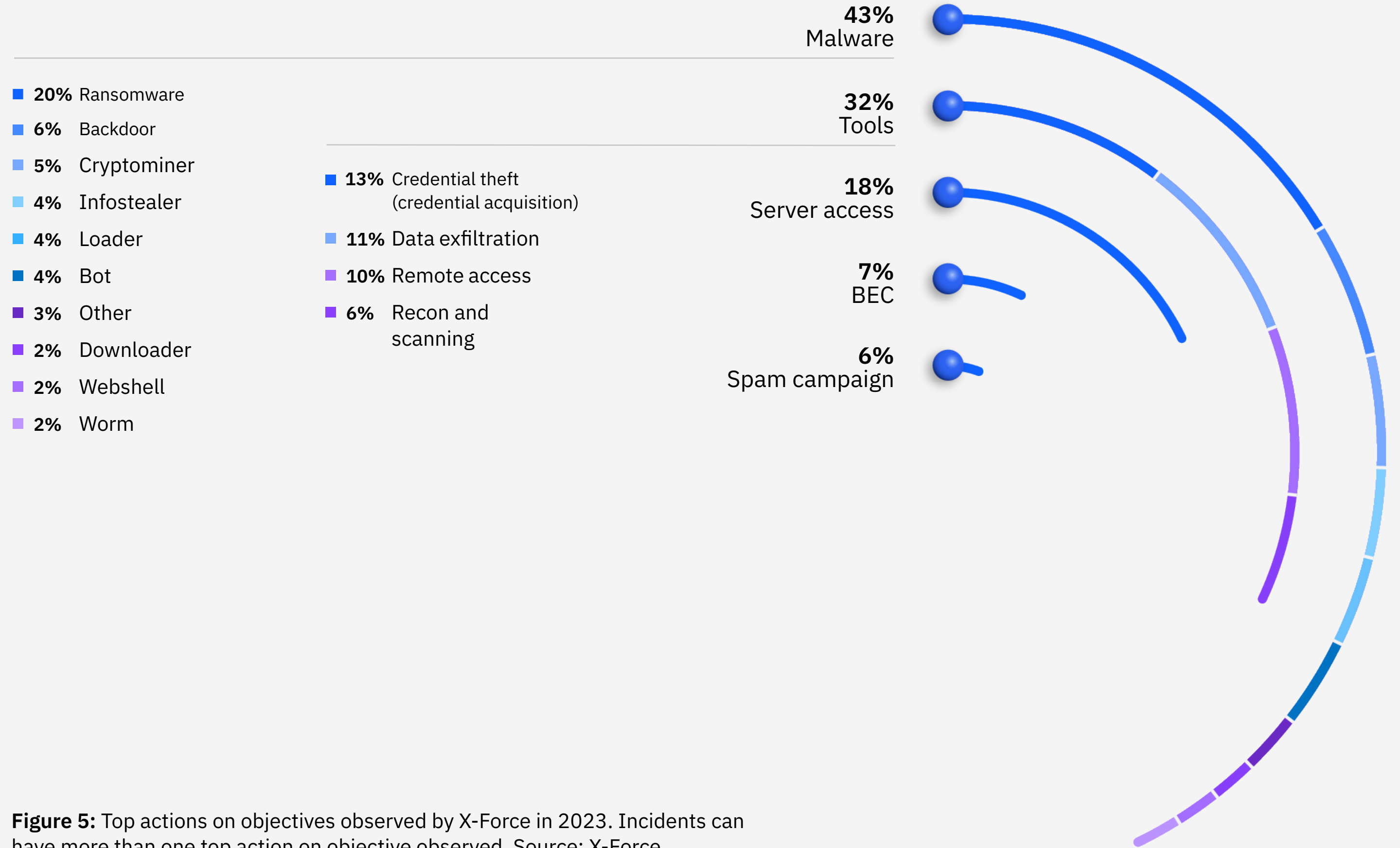


Figure 5: Top actions on objectives observed by X-Force in 2023. Incidents can have more than one top action on objective observed. Source: X-Force

This year, X-Force also reviewed cases to identify where legitimate tools were used for malicious purposes, which was observed in 32% of cases. For example, X-Force has observed vulnerability scanners used to conduct reconnaissance or adversary simulation tools to exfiltrate data. These tools were used to perform credential theft in 13% of total cases, followed by data exfiltration (11%), remote access (10%) and reconnaissance (6%).

Ransomware

Although X-Force responded to less ransomware cases in 2023, down 11.5% year over year, ransomware and ransomware-affiliated groups continued to target organizations globally, with multiple variants receiving upgrades to expand their targeting and functionality. The top ransomware variants observed by X-Force were BlackCat, CL0P, LockBit, BlackBasta and Royal.

In 2022, ransomware was topped slightly by backdoors as the top attack X-Force responded to after dominating the IBM X-Force Incident Response activity since 2018. In 2023, although ransomware moved back to the top action on objective, X-Force observed a continued reduction in ransomware incident response activity.

However, analysis of ransomware extortion sites indicate ransomware activity globally has increased in 2023. The contradictory data points appear to be attributed to similar data presented in last year's IBM X-Force Threat Intelligence Index. X-Force clients have continued to improve their capabilities to detect and respond to the precursors of a ransomware event, backdoors, lateral movement and identity abuse.

For instance, X-Force responded to several cases involving Qakbot and other types of infections that were caught before ransomware would have likely been deployed. In addition, as we'll indicate in the next section, data theft and leaks remain the top impacts observed across IBM X-Force Incident Response engagements.

These observations suggest that threat actors are no longer limiting themselves to ransomware attacks to commit extortion. They're looking at other attack types to deliver on their objectives. For example, X-Force responded to multiple incidents associated with the CLOP ransomware group's widespread data extortion attacks through MOVEit exploitation.

Although the names of the most prominent ransomware operations continued to shift, X-Force [uncovered new evidence](#) linking many current families to past operations. While the Conti ransomware group—tracked by X-Force as ITG23—famously shut down in 2022, X-Force found evidence indicating connections to new ransomware projects. These new projects included Quantum, Royal, Zeon and BlackBasta ransomware, as well as the Karakurt data extortion group.

These operations also appear to share many of the same connections to initial access malware distribution groups, such as IcedID, Emotet, Bumblebee, Qakbot and Gozi. X-Force also discovered a campaign likely undertaken by former members of the Conti ransomware group that leveraged a false [claim of successful data theft](#) as lure material. As such, the criminal core behind ITG23 is still prominent on the cybercriminal threat landscape.

Ransomware operations that maintained their branding upgraded their operations, demonstrating resiliency. BlackCat developers, for instance, debuted [a new variant](#) of the malware dubbed Sphynx in early 2023, which introduced a number of new capabilities to make the ransomware more difficult to detect. Affiliates also

have been observed evolving their tactics, techniques and procedures (TTPs) across the attack chain, including using a QR code for victims to access the ransom note. Additionally, ransomware operators continue to develop Linux versions of their ransomware. In 2023, new Linux variants of ransomware families were introduced, including CLOP and Royal.

Initial access to ransomware deployment

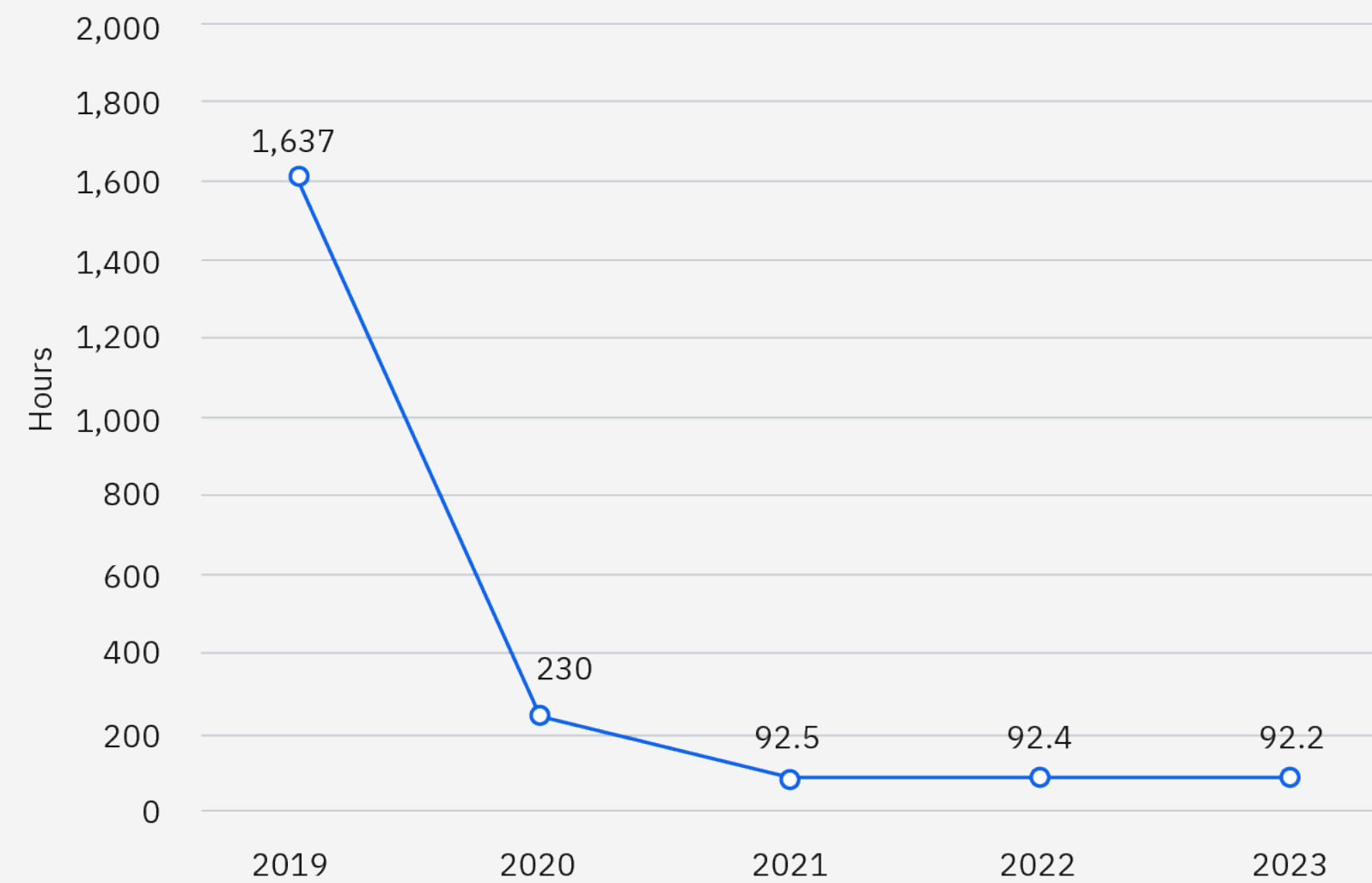


Figure 6: Time between initial access and ransomware deployment. Source: X-Force

Ransomware attack timelines

X-Force performed an analysis of ransomware attacks between 2022 and 2023 to determine if there were any changes in the time it takes for an attacker to carry out a ransomware attack. The average duration of an enterprise ransomware attack—the time between initial access and ransomware deployment—reduced slightly to 92.21 hours (3.84 days) in 2023 from 92.48 hours (3.85 days) in 2022.

This minimal reduction in the ransomware attack lifecycle appears to be directly related to a 38.44% reduction in time spent between obtaining domain administrator privileges and ransomware deployment. Analyzing the incident data from the attacks, with the largest reductions of time between obtaining domain administrator

privileges and ransomware deployment, indicates that the attackers spent less time exfiltrating data than in previous years.

It appears attackers are requiring more time to obtain administrative privileges to Active Directory compared to 2021. However, this additional time may be an indication that 2021 was a statistical outlier and mainly due to attackers leveraging exploits like Zerologon and PrintNightmare.

X-Force analysis didn't reveal any substantial changes in the tools, techniques and procedures used by threat actors leveraged in ransomware attacks in 2023 compared to 2021. It's worth noting that this year's analysis includes data from all mass deployment ransomware attacks, as opposed to our 2022 [original analysis](#), which examined a subset based on initial access.

Top impacts

The top impact to organizations was data theft and leak, making up 32% of the incidents X-Force responded to—accounting for 19% of the incidents in 2022. This increase aligns with the rise in observed infostealer activity and use of legitimate tools to exfiltrate data. Furthermore, extortion incidents more than doubled in 2023, and the share of all incidents that were extortion increased from 21% in 2022 to 24% in 2023.

As mentioned, extortion-based attacks remained one of the driving forces of cybercrime in 2023 with threat actors leveraging various attack types to deliver on their extortion objectives.

Top impacts 2023

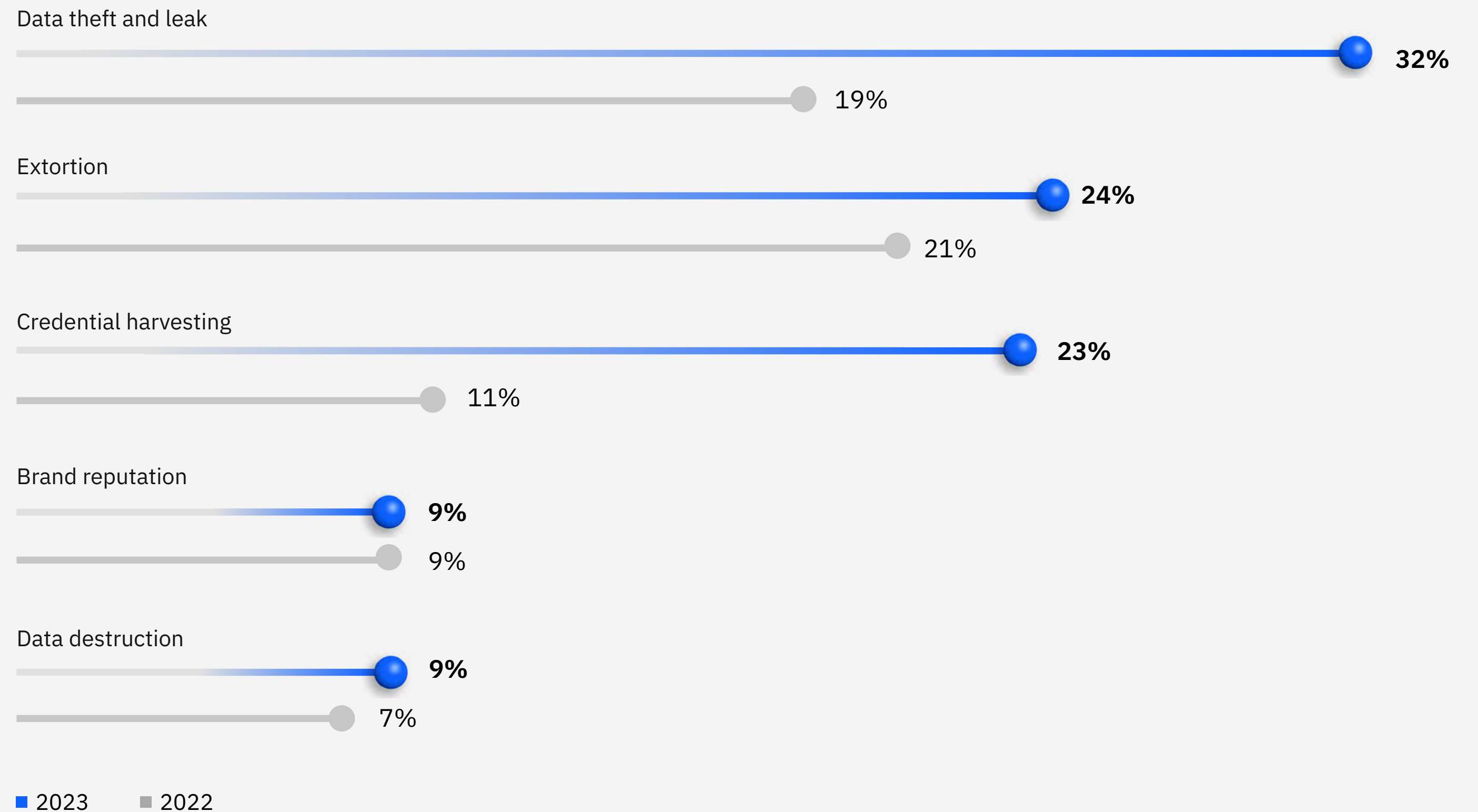


Figure 7: Top impacts X-Force observed in incident response engagements in 2023. Incidents can have more than one impact observed. Source: X-Force

The proliferation of ransomware attacks over the past few years, coupled with the massive efforts taken to combat and prevent them, has potentially pushed threat actors into simplifying their process. For example, threat actors are increasingly experimenting with extortion-based campaigns that do not rely on ransomware to encrypt data. Instead, the threat can be related to theft of and exposure to sensitive internal victim data. Not only is this method a less resource-intensive attack path, it may also be an indicator that data extortion tactics create the most pressure to elicit payment.

The malware landscape

Evolution of malware delivery mechanisms

Threat actors have reacted to changes in the security environment by introducing increasingly complex infection chains and attempting new methods of malware delivery. In 2023, X-Force observed² actors using popular methods, such as email campaigns, leveraging:

- OneNote files with embedded scripts
- PDF files containing malicious links
- Microsoft Software Installer (MSI) and Nullsoft Scriptable Install System (NSIS) executables disguised as document files

Another tactic that X-Force observed, one which gained popularity in 2023 but appears to have since declined, is HTML smuggling. This method leverages HTML5 and JavaScript functionality to download or construct a malicious payload when the HTML page is opened in a web browser. X-Force also frequently observes .url (internet shortcut) files in attack chains leading to the final payload. Malware distribution through malicious disk image files (ISO, IMG and VHD) and LNK files, which was noted in the 2023 X-Force Threat Intelligence Index, has also continued to be observed with decreased frequency.

There has also been an observed uptick in email campaigns using Microsoft Office documents to deliver malware through exploits rather than malicious macros. Documents weaponized with CVE-2017-11882, an arbitrary code execution vulnerability within the Microsoft Office equation editor, increased in popularity in the past year. Remote template injection, a technique to bypass email gateway controls by sending phishing emails that retrieve malicious office templates after delivery, was also observed in 2023.

In addition, threat actors have increasingly turned to malware delivery vectors beyond email, the most noteworthy of which is the use of fraudulent Google and Bing Ads,

also known as malvertising, to distribute malware through fake software downloads. Their payloads have included infostealers and backdoors, some of which have led to ransomware attacks.

X-Force has also observed additional threat actors using fake browser updates to distribute malware, including infostealers and the NetSupport remote administration tool. The Gootloader group continues to use SEO poisoning effectively to infect organizations, which can lead to ransomware attacks. X-Force also continued to observe SEO poisoning leveraged by SolarMarker, which has both infostealer and backdoor capabilities.

Over the past year, it has also become increasingly common for threat actors to use complex execution chains. The use of several stages where the malicious behavior is spread across multiple components, along with invoking living off the land tools, increases detection difficulty by analysts and security technologies such as endpoint detection and response (EDR).

Complex execution chains also hinder the analysis capabilities of sandbox technologies by requiring several stages of execution until the final payload. Malware developers can implement anti-sandbox checks at multiple stages, increasing the likelihood that the sandbox analysis fails. With a reduction in sandbox detections,

there's a reduction in the likelihood of security researchers gaining access to valuable resources, such as command and control panels and more advanced tools.

One example of a complex execution chain discovered and analyzed by X-Force in 2023 is the infection chain for [WailingCrab malware](#). Although this infection chain is initialized through an email campaign with a PDF attachment, the final payload isn't executed until 7 additional steps take place.

Infostealers on the rise

The past year has seen a significant rise in the number of and threat actor interest in infostealers. Infostealers can be leveraged to facilitate fraud or theft by compromising financial or personal information. However, infostealers have also been frequently linked to more impactful attacks against enterprises by facilitating initial access through stolen credentials.

X-Force noted a 266% increase in infostealer-related activity in 2023 compared to 2022. That upward trend likely contributed to the rise of abuse of valid accounts, the top initial access vector X-Force observed. Infostealers have long been a staple of the criminal underground marketplace, and many operate as a malware-as-a-service (MaaS) model.

In addition to the well-established stealers, such as RedLine, Vidar and Raccoon, several prominent new infostealers, which debuted in the latter half of 2022, demonstrated increased activity throughout 2023, such as Rhadamanthys, LummaC2 and StrelaStealer. Different infostealer families target different types of information, from platform-specific credentials to password managers to browser history.

Also, observations of established stealers, such as Agent Tesla, FormBook, Snake Keylogger, Vidar, AZORult and Lokibot, X-Force observed activity by the following recently introduced stealer families:

Infostealer name	Target Information	Description
Ducktail	Targets Facebook credentials, Facebook-related cookies, anti-cross-site request forgery (CSRF) tokens, MFA codes and data associated with Facebook Ads Manager	Ducktail targets information required to hijack Facebook business accounts, which is then used to carry out malicious advertisement campaigns. It uses the Telegram messaging application for its command and control infrastructure (C2).
Sys01 Stealer	Steals cookies, login information and other sensitive information, including Facebook business account information	Sys01 Stealer is written in Hypertext Preprocessor (PHP) and, like Ducktail, also focuses on stealing Facebook information, such cookies and login data.
StrelaStealer	Steals Outlook and Thunderbird email credentials	StrelaStealer focuses on stealing email credentials and has been observed by X-Force as being distributed in phishing campaigns targeting Spain and Italy, and to a lesser extent Germany.
Rhadamanthys	Collects information from multiple applications, including browsers, mail clients, virtual private network (VPN) services, two-factor authentication (2FA), password managers, file transfer protocol (FTP) clients, notes, chat and messenger apps, cryptocurrency wallets, remote desktop apps and gaming clients	Rhadamanthys is a jack-of-all-trades infostealer that can also find and exfiltrate files from the file system and gather detailed system information.

Infostealer name	Target Information	Description
DarkCloud	Targets information primarily related to credentials, credit card data and cryptocurrency	DarkCloud is a general-purpose stealer that can also log keystrokes and take screenshots.
Nemesis	Stores credentials, cookies, credit cards, bookmarks, autofill data, browser history, crypto wallet data and clipboard data	Nemesis is a .NET infostealer observed by X-Force as being deployed by the FIN7-linked Minodo backdoor during campaigns operated by former members of the TrickBot/Conti syndicate.
StealC	Collects system information, files, cryptocurrency wallets, browser data and data from email and messaging applications, including Outlook, Discord, Telegram and Steam Chat	StealC steals targeted information based on instructions from its C2 server and can download and execute payloads in addition to stealing data commonly targeted by infostealers.
LummaC2	Collects sensitive data, including login credentials; bank details; cryptocurrency wallet information, such as Binance and Ethereum; browser extension details, for example, MetaMask for 2FA; and data from applications such as AnyDesk and KeePass; and targets Windows operating systems (Windows 7 to 11) and at least 10 browsers, including Google Chrome, Microsoft Edge and Mozilla Firefox	LummaC2, also known as Lumma, is written in C and distributed through a MaaS model. It first emerged in 2022 and includes a loader capable of delivering additional payloads.

The success of infostealers has not gone unnoticed by other players in the cybercrime marketplace. Threat groups who have largely specialized in ransomware, such as ITG23, also known as TrickBot and Conti, and LockBit have both been linked to infostealers. Campaigns linked to ITG23 have been observed distributing the Vidar infostealer in late 2022. In 2023, ITG23's interest in infostealers grew to include campaigns involving the LummaC2 and Nemesis stealers during the first half of the year

followed by the Rhadamanthys stealer in November. Meanwhile, LockBit [announced its desire to purchase the Raccoon Stealer source code](#).

Research contributions by Intezer further highlight the increasing value of infostealers to the criminal ecosystem. By performing an analysis on how much a malware family's source code is changing based on uniqueness of code versus code recycling, Intezer found that infostealers topped the list in 2023 for most unique

malware samples targeting Microsoft Windows. It made up 17.8% of samples, indicating continued investment in infostealer innovation.

As threat actors invest in infostealers and X-Force observes a developing trend around identity abuse—through credential harvesting or abuse of valid accounts—we expect it to impact defenders' detection timelines.

Abuse of cloud services

Threat actors continue to abuse a wide range of public and private cloud services for malware distribution and operation, allowing them to evade network detection mechanisms by masquerading as legitimate traffic.

Discord and Telegram in particular have attracted significant threat actor attention, as multiple aspects of the platforms' functionality can be abused in service of malicious activity. Threat actors have misused Discord for [C2](#), abused the functionality of the platform's [content delivery network \(CDN\)](#) to host and distribute malware, and used its webhook functionality to [exfiltrate data](#) from infected systems. Additionally, X-Force observed a

novel technique in 2023 whereby a Discord C2 channel used the [native Discord bot capabilities](#).

[WailingCrab](#), a malware discovered by X-Force in 2023, is a multistage malware that uses the Discord CDN to host further WailingCrab stages and other additional payloads. In addition to Discord, the malware was also notable for abusing the MQ Telemetry Transport (MQTT) protocol, which is a lightweight protocol designed for communication between Internet of Things (IoT) devices. WailingCrab uses the public MQTT broker EMQX for its C2 communications, which lets it hide the true address of its C2, as well as allowing the C2 communications to masquerade as legitimate MQTT traffic.

[GraphicalNeutrino](#) malware is another notable example, which uses the cloud-based collaboration platform Notion for its C2 communications. This malware uses the platform's API to send requests to a Notion database where it stores victim information and receives commands and additional payloads. Notably, this malware is used by a group that has been [assessed](#) to overlap with Russian espionage group APT29, which IBM tracks as ITG11.

We expect that a variety of threat actors and groups may explore the functionality of cloud services for malicious use.

Adoption of penetration testing techniques

Threat actors have remained interested in leveraging identity abuse to carry out their attacks and, in 2023, X-Force observed threat actors targeting identity services for privilege escalation rather than endpoint credential harvesting techniques. The shift in behaviors appears to be in response to improvements in endpoint detection and response capabilities in preventing traditional credential harvesting techniques such as [OS Credential Dumping: LSASS Memory \(T1003.001\)](#).

Between 2022 and 2023, X-Force noted a 100% increase in Kerberoasting attacks, targeting the Kerberos authentication protocol commonly used in Microsoft Windows Active Directory environments. This method involves extracting password hashes by manipulating service principal names (SPNs) to request Kerberos tickets

on behalf of other accounts, enabling attackers to crack passwords and gain unauthorized access.

X-Force observed attackers focusing on SPNs associated with service accounts, as these accounts often hold higher permissions, facilitating broader access to data and systems. Financially motivated attackers in 2023 also targeted Active Directory Certificate Services (AD CS) for privilege escalation, exploiting CVE-2022-26923 to potentially elevate their privileges to domain administrator. Although Microsoft patched this vulnerability in update KB5014754, successful attacks can still occur depending on key distribution center (KDC) configurations, underscoring the importance of vigilant patch management and secure service settings.

Active Directory Certificate Services attack diagram

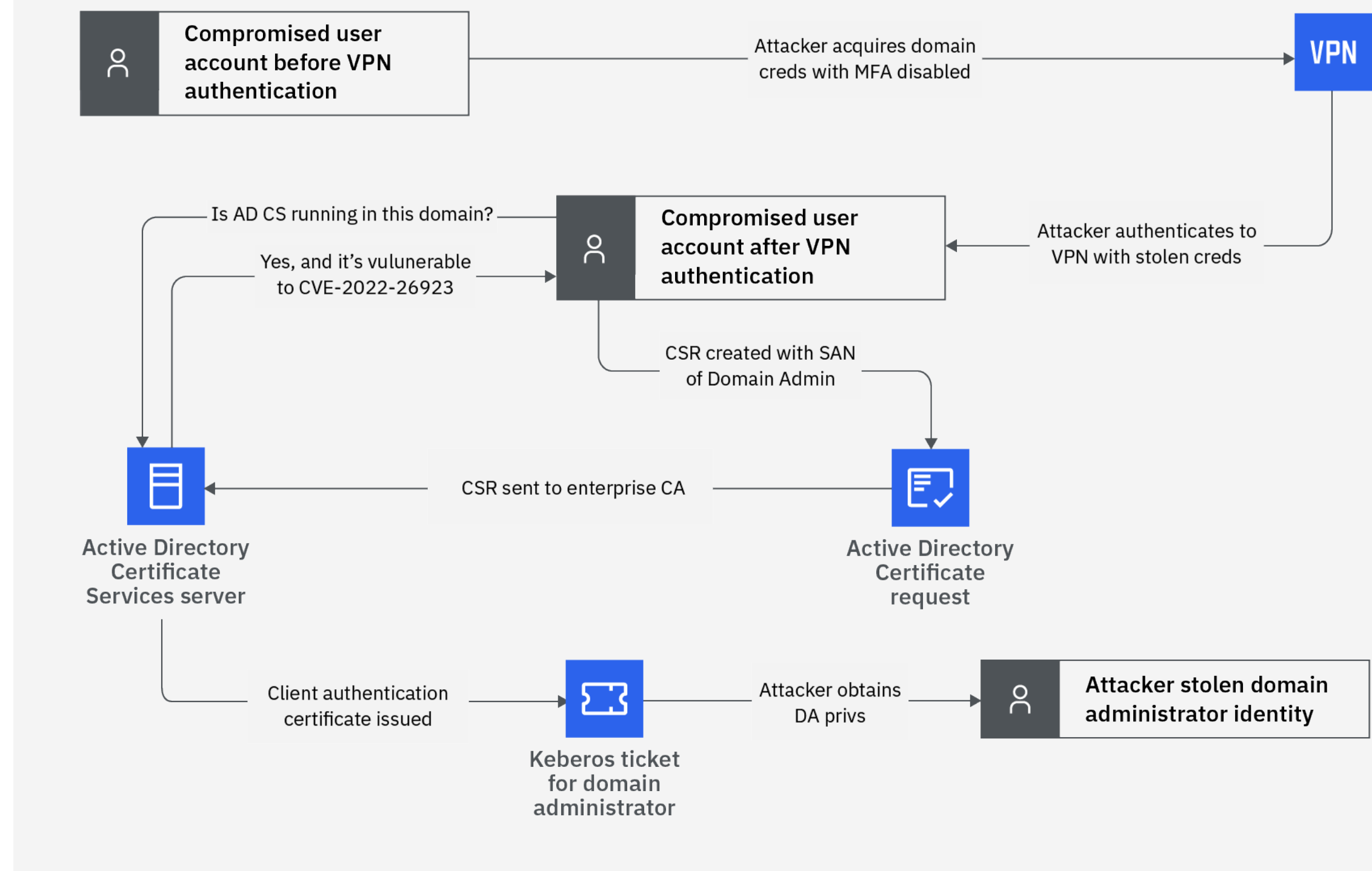
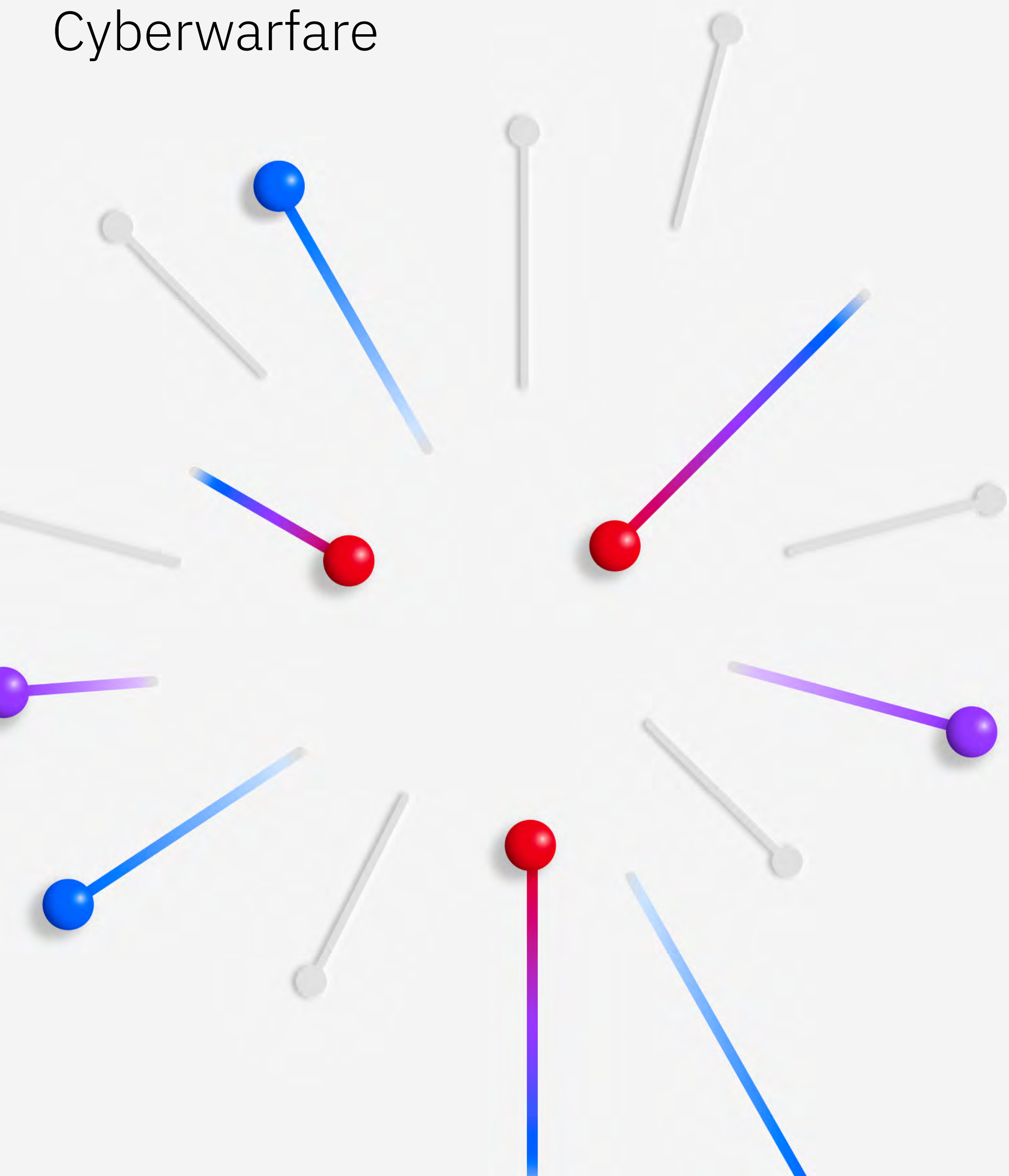


Figure 8: Active Directory Certificate Services attack diagram. Source: X-Force

Cyberwarfare



Russia-Ukraine conflict

Throughout the course of 2023, X-Force has actively monitored countless Russian state-sponsored attacks, leveraging evolving tools and TTPs to carry out offensive operations against Ukraine and its allies. Of note, Hive0051, which shared overlap with [Gamaredon](#), has accelerated its development efforts to support expanding operations since the onset of the ongoing conflict. [X-Force analysis](#) identified three key changes to capabilities: an improved multichannel approach to Domain Name System (DNS) fluxing, obfuscated multistage scripts and the use of fileless PowerShell variants of the Gamma malware.

As of October 2023, X-Force observed a significant increase in Hive0051 activity. This activity features a new multichannel approach of rapidly rotating C2 infrastructure. The approach facilitated at least 1,027 active infections with more than 327 unique malicious domains observed in a single 24-hour period.

While Hive0051 has used DNS fluxing to avoid detection as early as December 2022, the [automated synchronized fluxing of dynamic DNS records](#) across Telegram channels and Telegraph sites at scale suggests an elevation in actor resources and capability.

In addition, by deploying multiple consecutive stages of the Hive0051 exclusive Gamma variant malware, the actor is able to remap victims to separate sets of actor-controlled C2 fluxing clusters.

Looking forward, it's highly likely that Hive0051 will continue to foster evolving methodologies to facilitate operations potentially indicating increasingly elevated levels of capability.

In 2023, X-Force observed criminal threat actors leveraging the ongoing conflict in Ukraine to craft well-manufactured phishing campaigns. Since Russia's invasion of its neighbor, the theme of the conflict has been used as lure material.

In late May, X-Force identified Hive0117 using this approach. The group capitalized on changes to Russian laws associated with the delivery of digital military conscription notices. It mimicked those email notices to deliver its signature DarkWatchman malware. The scale of the campaign extended across Russia, as well as multiple states that were once part of the Soviet Union. As the conflict continues, we assess that it's highly likely that threat actors will continue to attempt to use the conflict for lure material, especially targeting entities associated with connections to the ongoing war.

Threat actors also performed distributed denial-of-service (DDoS) attacks with varying levels of success. A Microsoft outage that took place in the summer of 2023 was linked by

a spokesperson to [Anonymous Sudan](#), a DDoS group that does not claim pro-Russian sentiment but is linked to the Russia-sympathetic group Killnet. DDoS group [NoName057\(16\)](#), which explicitly distanced itself from Killnet, claimed attacks against Italian targets in the summer of 2023 and justified the attacks with anti-Ukrainian rhetoric.

Although more impactful attacks were threatened, such as [Killnet's threat](#) against the European banking system, we have yet to observe the magnitude of activity implied by these threats and the statements of related group.

Israel-Hamas conflict

In response to the war between Hamas and Israel, X-Force has observed various claimed hacktivism operations related to the crisis in the region. Most targets were in the financial sector, government, travel and transportation industries, and the preponderance of observed activity originated from pro-Palestinian groups targeting Israel. Telegram was the social media outlet of choice for most threat actors and where claims of their activities were posted. As the situation developed, X-Force did observe some pro-Israel hacktivist groups calling for action, in addition to recent posts from Gonjeshke Darande, also known as Predatory Sparrow.

In addition, X-Force [uncovered multiple lure documents](#) that predominately feature the ongoing Israel-Hamas war to facilitate the delivery of the ITG05 exclusive Headlace backdoor. X-Force tracks ITG05 as a likely Russian state-sponsored group consisting of multiple activity clusters, sharing overlaps with industry-identified threat actor groups APT28, UAC-028, Fancy Bear and Forest Blizzard. The newly discovered campaign is directed against targets based in at least 13 nations worldwide and leverages authentic documents created by academic, finance and diplomatic centers.

For organizations located in the region, X-Force recommended that clients review their network security posture for readiness against malicious hacktivist activity, including DDoS, website defacement or enumeration of networked devices vulnerable to data disclosure. Contacting a DDoS mitigation provider, having and practicing a DDoS incident response plan, and ensuring that incident responders have up-to-date contact information for DDoS mitigation and internet service providers help organizations that are targets mitigate attacks.

Generative AI: A new cyberthreat frontier



X-Force hasn't been able to confirm the use of gen AI in current malicious campaigns. However, there are some threat actors paying attention to the marketing value of AI and showing it in the services they allegedly offer. Two tools available to attackers that were built to be unrestricted or semi-restricted large language models (LLMs) for cybercriminals that stood out are FraudGPT and WormGPT. These tools are advertised on various forums and Telegram channels—each supporting the capability to craft phishing emails, among other malicious activities.

In August 2023, WormGPT developers released a statement that they would be shutting down the project, claiming that it gained unforeseen popularity, and that news reporting mischaracterized it.

FraudGPT is a euphemism for the services offered by CanadianKingpin12 (CK12), a cybercriminal service broker and associate of a likely self-organized group called the Cashflow Cartel (CFC), based on an assessment made by X-Force. On the CFC's bot-driven Telegram channel, a user may choose to purchase illegal services that include credit cards, hacked accounts and AI capabilities, with prices ranging from USD 90 to USD 700 based on the service.

As X-Force didn't pay to experiment with any of these services, it wasn't possible to confirm the extent to which this tool could or could not support cybercriminals in their offensive cyber operations.

Indicators of AI attack surface maturity

While X-Force hasn't observed confirmed AI-engineered campaigns to date, it's expected that cybercriminals will seek to leverage AI in their operations and, as previously illustrated, they're already exploring how. In fact, X-Force has observed AI and GPT mentioned in over 800,000 posts in illicit markets and dark web forums in 2023, as evidence of cybercriminals' interest in the technology. While it's not unlikely to see AI-enabled attacks reported in the near term, X-Force assesses that proliferated activity won't be established until the pace of enterprise AI adoption matures.

With that likelihood in mind, X-Force took a deep dive into the cybercrime industry to reflect on technological enablers and

milestones that fostered cybercriminal activities in the past. Doing so helps us identify future industry trends that are likely to create opportunities for criminals—amid the rate of enterprise AI adoption that's anticipated over the next decade.

In review of the past three years of the X-Force Threat Intelligence Index and IBM X-Force Cloud Threat Landscape Report, cybercriminals have largely focused their operations on the following attack types:

- Ransomware
- Business email compromise (BEC)
- Cryptojacking

X-Force performed a deep analysis of the incident data surrounding these three attack types. The research revealed common themes in terms of tools, software or platforms—correlating rate of tech adoption with rate of exploitation—helping us establish an indicator of AI attack surface maturity.

As we'll illustrate here, the findings suggest that attackers will begin to build at-scale attacks targeting specific technologies once the technologies establish market dominance. Based on the data analyzed, market dominance can be interpreted as when a single technology approaches

50% market share or when the market consolidates to three or less technologies. Our analysis indicates.

- **Windows Server market dominance triggered the development of point-of-sale (POS) malware and human-operated ransomware attacks, which relied upon Active Directory.** In 2006, Windows Server became the most widely used server OS and subsequently Active Directory established further dominance in the directory service market. Three years later, nation-state actors began leveraging Active Directory to carry out

their operations. By 2014, cybercriminals created attack paths upon Windows and Active Directory setting the stage for human-operated ransomware attacks in the years following.

- **Losses from BEC scams saw a sharp upward climb once Microsoft 365 neared 50% market share adoption.** In 2019, Office 365 (now Microsoft 365) represented 48% of the market share when losses from BEC scams exceeded USD 1.7 billion and 25% of phishing attacks bypassed Microsoft's security mechanisms. Within a year, the FBI issued a warning that attackers were

abusing Office 365 in BEC attacks using phishing kits designed to mimic cloud-based email services.

- **The infrastructure-as-a-service (IaaS) market consolidation supercharged the crypto mining malware expansion.** Between 2017 and 2018 the cloud IaaS market consolidated from 14 players down to six with the top three vendors controlling roughly 60% of the market. During the same time, an 8,500% increase in crypto mining was reported.

The ransomware era

In 2000, Active Directory was released to the market as part of Windows Server 2000. By the following year, Microsoft’s share in the server operating system market had jumped to 49%.³ And by 2006, Windows surpassed UNIX in the server OS market making Active Directory the dominate player in the directory services market—after which we began to observe attackers exploiting the technology.

Just as Figure 9 illustrates, exploitation gradually increases as tech adoption scales. Nation-state actors were the first to set their sights on Active Directory, leveraging it in famous attacks between 2009 and 2011, such as NightDragon⁴ operations and the attack against RSA.⁵

The market path to ransomware

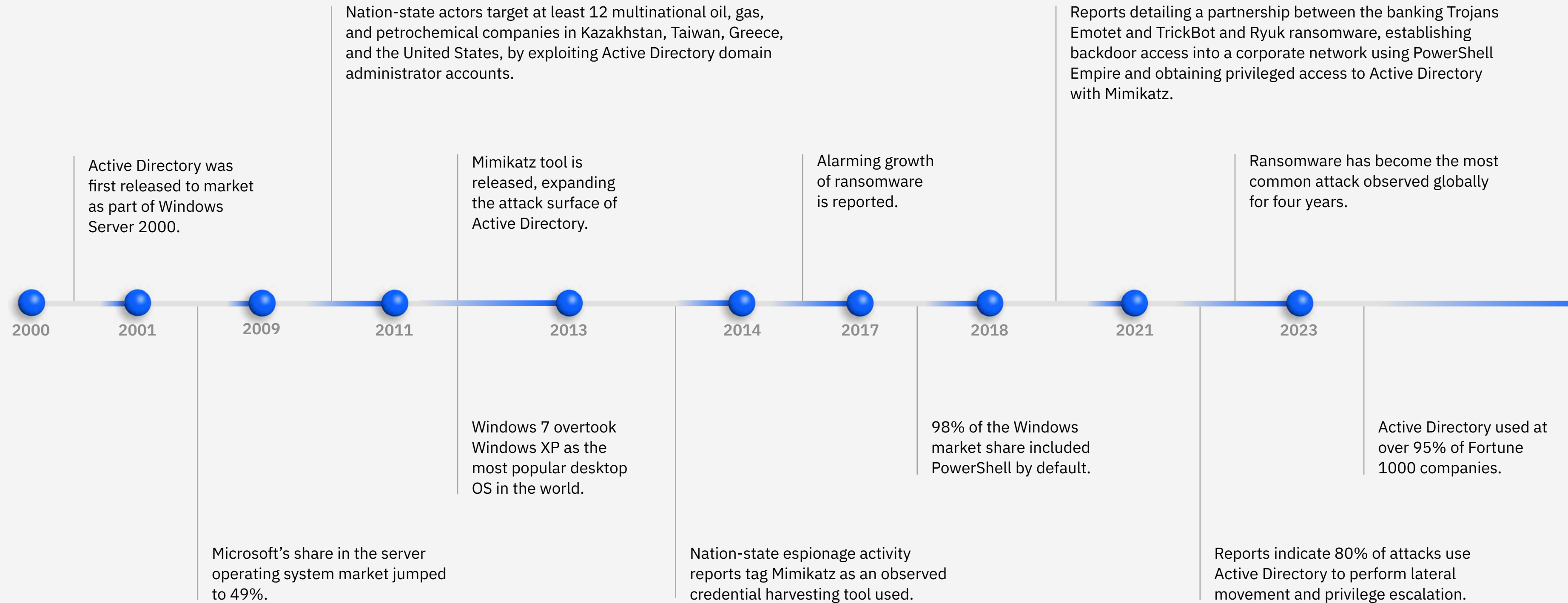


Figure 9: Timeline of Active Directory adoption and exploitation. Source: X-Force

In 2011, French security researcher Benjamin Delpy released the credential harvesting tool Mimikatz,⁶ significantly reducing the technical capability requirements to steal domain credentials. Nation-state and financially motivated attackers quickly adopted the tool to carry out their operations.

2014, dubbed the “year of POS malware” by Trend Micro,⁷ saw financially motivated actors adopting advanced persistent threat (APT)-style attacks, leveraging Mimikatz and Active Directory to move throughout the network to gain access to the POS systems.^{8,9} The attack chains established during the 2014 POS attacks set the stage for the emergence of human-operated

ransomware attacks in the future as evidenced by the POS threat actor groups migrating their operations from POS to ransomware.¹⁰

Today, Active Directory is used at over 75,000 companies globally,¹¹ while a 2021 industry report¹² states that 80% of attacks use Active Directory to perform lateral movement and privilege escalations. The pattern is similar with PowerShell, which was included by default in 98% of Windows installs by 2017.¹³

As it became commonplace within the enterprise network, tools such as PowerShell Empire were created to simplify PowerShell-based attacks,¹⁴ and were

rapidly adopted by threat actors to carry out their attacks. Together, the market dominance of Active Directory and ubiquity of PowerShell enabled a years-long ransomware spree. Ransomware went on to become the most common attack type observed for three years in a row according to our threat intelligence.

It’s worth noting that Active Directory and PowerShell in and of themselves don’t make an organization any more or less secure. However, the default deployment configuration, which was the most common deployment¹⁵ of Active Directory, does provide a known technical landscape in which attackers can plan an attack upon.

The BEC success story

The FBI started tracking BEC scams in 2013 as “emerging financial cyberthreats” targeting businesses.¹⁶ The rapid adoption of email in the 2000s was the defining factor in the decades-long success of BEC and overall phishing attacks.

To meet the demand for BEC campaigns, the criminal market narrowed its focus and created phishing tools specifically for compromising corporate email services. The historical evidence suggests that as the technology market coalesces around different technologies, such as Microsoft 365 for email, the criminal developers creating tools for BEC attacks tailored their tools to match ubiquitous technologies.

Following the users: BEC takes to Office 365

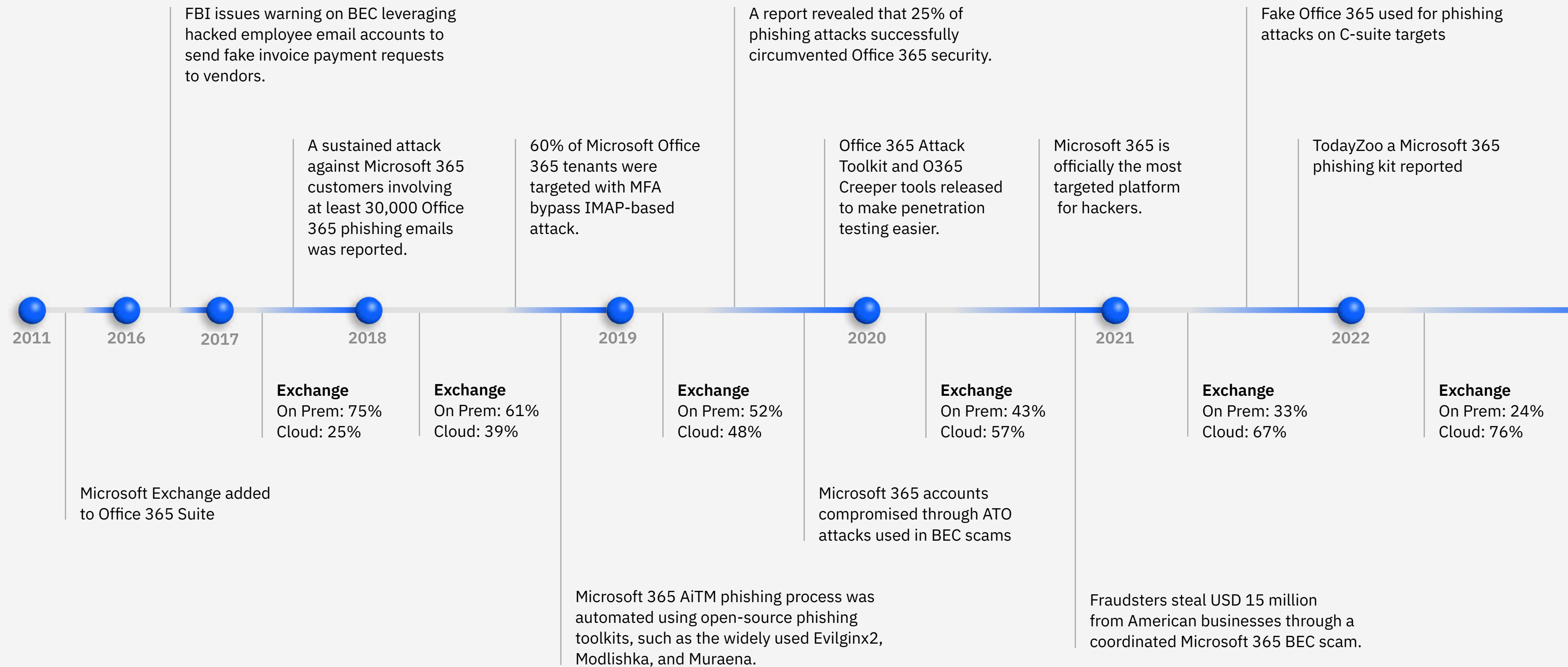


Figure 10: Timeline of email technology adoption and the rise of BEC attacks. Source: X-Force

In 2016, Microsoft 365, then known as Office 365, was in use by 8.5% of Fortune 500 companies.¹⁷ That year is also when the FBI warned about the dramatic increase in BEC scams targeting businesses, resulting in significant financial losses.¹⁸ That same year multiple ransomware¹⁹ and phishing^{20, 21} attacks exploiting Microsoft 365 were reported.

As market adoption grew over the coming years, the volume of phishing and BEC attacks tied to the technology began to steadily increase, as did financial losses for businesses. By 2019, Office 365 represented 48% of the market

share²² and the Cybersecurity and Infrastructure Security Agency (CISA) had issued an advisory²³ regarding Office 365 configurations that could lead to compromises. At the same time, the FBI's Internet Crime Complaint Center received 23,000 complaints related to BEC and email account compromise (EAC) scams,²⁴ leading to adjusted losses exceeding USD 1.7 billion that same year.

Throughout the decade, attackers evolved their TTPs, innovating to bypass security measures put in place to further protect against the growing risk of phishing and investing in an attack surface that seemed to keep growing. In 2023, Microsoft 365

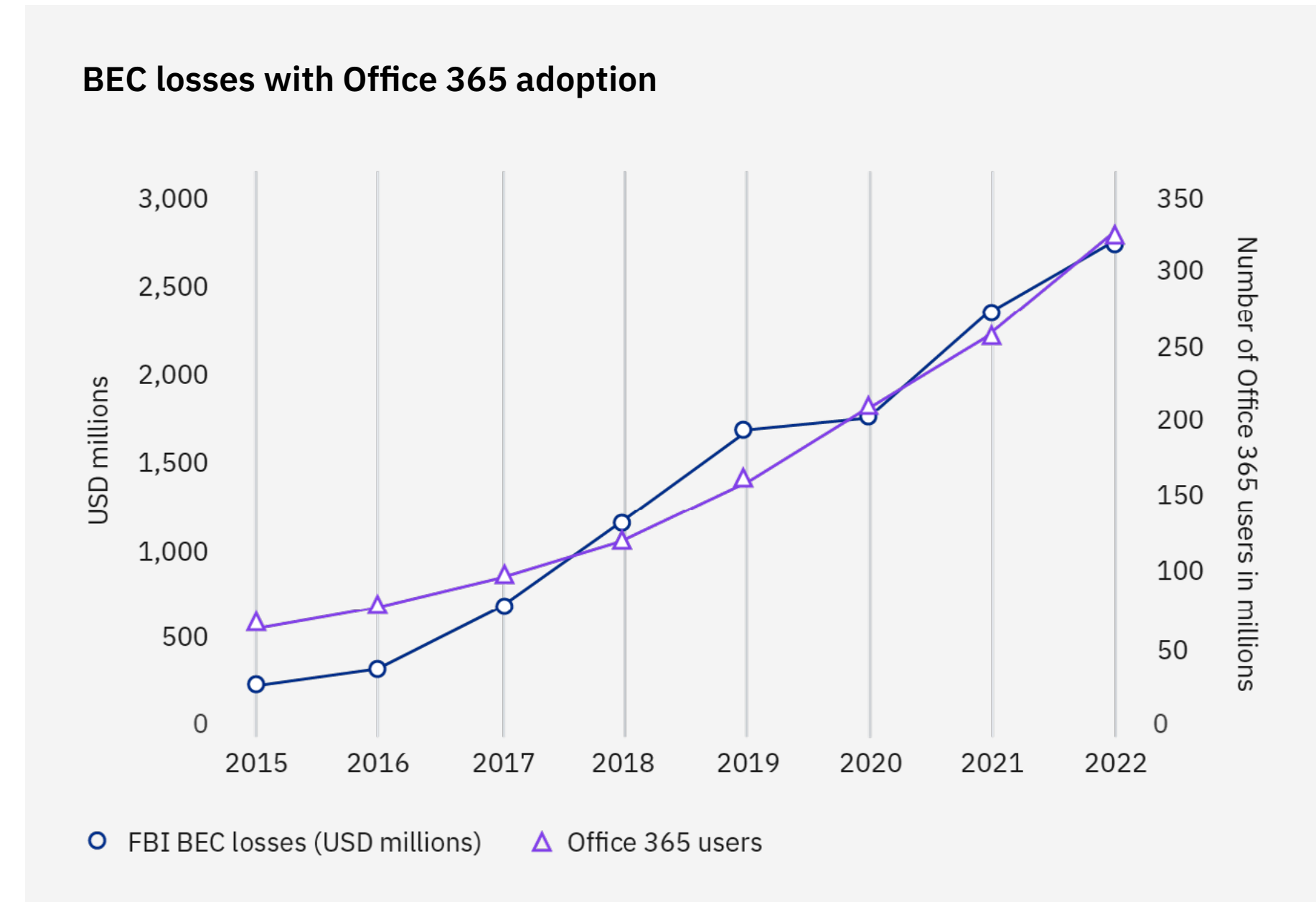


Figure 11: Timeline of FBI reported losses due to BEC attacks and the adoption of Microsoft 365. Source: X-Force and the FBI

adoption among big companies grew to 83%.²⁵ Reinforcing how attackers have adapted to Microsoft 365 adoption for enterprises, Egress' Email Security Risk Report stated that 92% of organizations have fallen victim to a successful phishing attack in their Microsoft 365 environment in 2023.²⁷

Graphing out the FBI reported losses due to BEC attacks and the adoption of Microsoft 365 year over year shows similar trendlines, indicating that attackers have adapted their TTPs to the market trends regarding technology adoption. Since the

FBI began tracking BECs as their own category in 2015, the dollar amount of losses has steadily increased year over year with significant jumps in 2017, 2018 and 2019. BEC losses increased respectively by 87.5%, 77.78% and 41.67% over the previous year. These BEC attacks have been so successful that the FBI reported in 2022 that USD 2.7 billion in losses were reported, making it the second most costly criminal type tracked in the report.²⁶

Cryptojacking

Cryptojacking became a feature of the cyberthreat landscape shortly after the introduction of cryptocurrency. In 2011, early manifestations of this activity took the form of Trojans, which leveraged the resources of compromised endpoints to mine cryptocurrency, specifically Bitcoin.²⁸ This type of malware used GPU resources, rather than CPUs, due to higher computing power and, therefore, higher returns but had fewer targets due to limited GPU use within general purpose computing.²⁹

During the period 2017–2018, cryptojacking significantly shifted in nature. First, cryptojacking became much more common. Over time, changes in computing capabilities and the introduction of cryptocurrencies, such as Ethereum and Monero, had enabled cybercriminals to shift their focus back to abusing devices’ CPU resources, which are much more widely found compared to GPU hardware.²⁹ Crypto mining activity had skyrocketed, largely targeting home network devices and endpoints.^{30, 31}

Cryptojacking’s crosshairs follows IaaS market consolidation

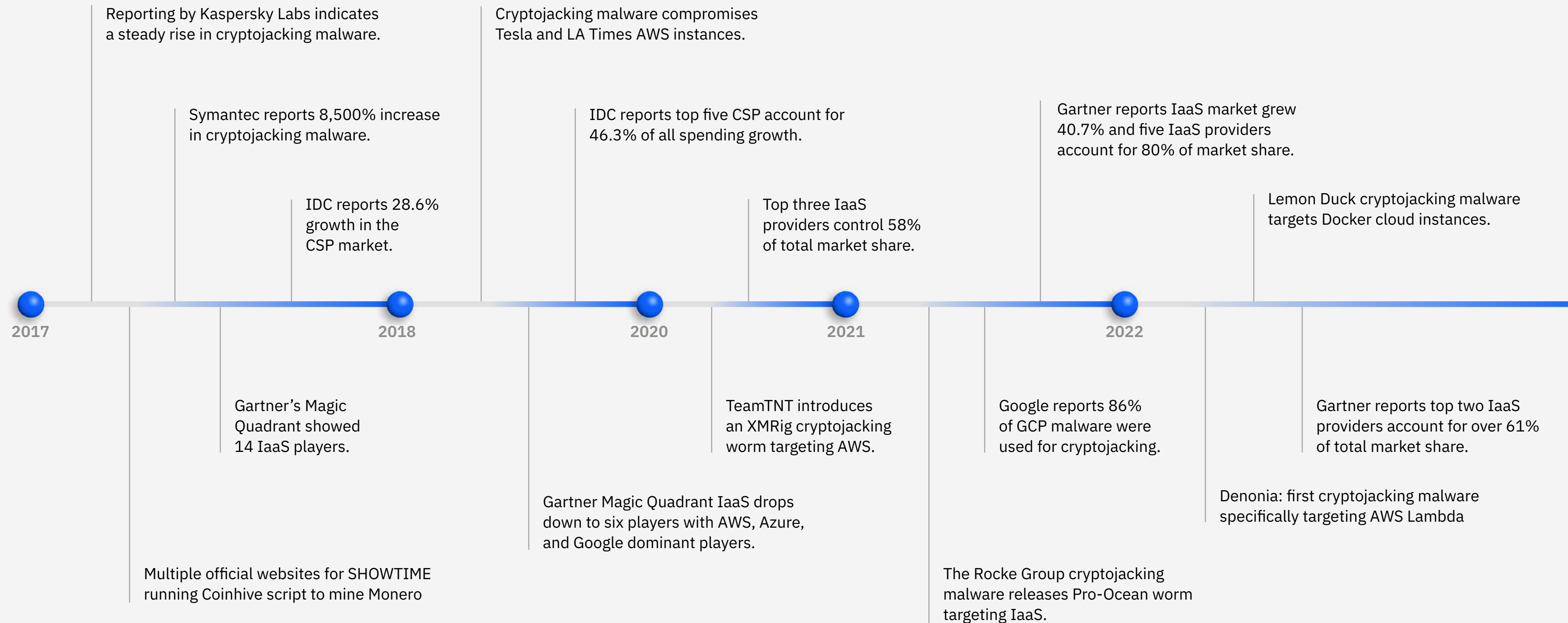


Figure 12: Timeline of the market consolidation of cloud IaaS offerings and cryptojacking developments. Source: X-Force

Additionally, increased observations of cryptojacking in 2017–2018 coincided with unprecedented prices for cryptocurrencies Bitcoin, Ethereum and Monero that same year, which likely further incentivized this activity.^{32, 33, 34} While large ransomware operations would surge in later years as the ransomware-as-a-service model took root, for a brief period in 2018 cryptojacking vied with ransomware as the growing threat in the spotlight.^{29, 35, 36} Some cybercriminal groups associated with ransomware also began incorporating capabilities targeting cryptocurrency, for example TrickBot, Rakhni Trojan.^{37, 38} X-Force research in 2018 found a 45% decrease in ransomware attacks compared to a 450% increase in cryptojacking activity.³⁹ This same period saw the market consolidation of cloud IaaS offerings, as illustrated in Figure 12.

Threats to generative AI: What looms ahead?

These patterns suggest that for cybercriminals to see ROI from attacking AI platforms and for developing easy-to-use tools on the criminal underground, the technology they're targeting must be ubiquitous across most organizations in the world. Otherwise, cybercrime attacks would require too much time and money, negatively impacting profits. Defenders should consider the AI market share as an indicator for the AI attack surface's maturity.

While more organizations say they are developing AI models, and AI is being used in different solutions, the AI market is currently in a pre-mass market period. Startups and established corporations are both jostling for a design favored by the market. This period will end with

the emergence of a design favored by the market that has enough proprietary innovations and an open enough architecture to be adopted by the majority of consumers.

Once AI market dominance is established—when a single technology approaches 50% market share or the market consolidates to three or less technologies—we assess it will trigger the maturity of AI as an attack surface. The result will be that cybercriminals will then further mobilize and increase their investment in attacking AI.

Geographic trends

In 2021 and 2022, the Asia-Pacific region held the top spot as most impacted region, with Europe trailing behind as the second-most impacted. In 2023, Europe earned the number one spot as the most-impacted region, accounting for 32% of incidents to which X-Force responded. North America represented 26% of incidents, while Asia-Pacific saw 23%, Latin America 12% and the Middle East and Africa 7%.

Incidents by region 2020–2023

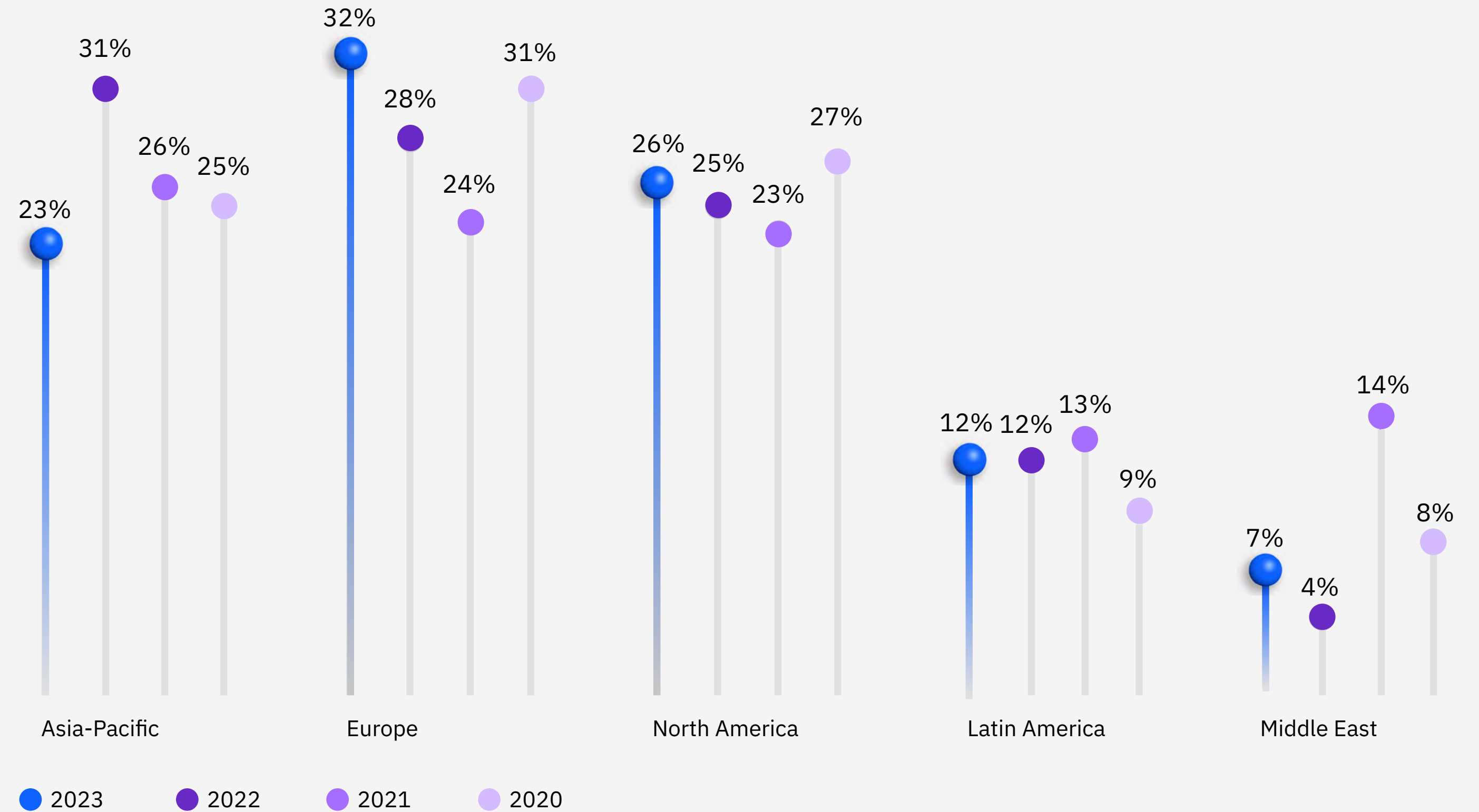


Figure 13: Proportion of incident response cases by region to which X-Force responded from 2021 through 2023. Source: X-Force

■ Europe experienced the most ransomware attacks globally with 26%



#1 | Europe

With Europe coming in at number one overall, malware was the most observed action on objective, accounting for 44% of incidents. Europe experienced the most ransomware attacks globally with 26%, which partly contributed to its rise in ranking in 2023. A large [ransomware campaign](#) in February 2023 dubbed ESXiArgs impacted organizations across Europe and targeted a vulnerability in VMware ESXi servers (CVE-2021-21974). The use of legitimate tools for malicious purposes and server access cases rounded out the top three actions on objective, representing 29% and 18% respectively.

Europe's [high use of cloud](#) platforms may also result in a potentially larger attack surface compared to other regions, especially if attackers are able to obtain valid cloud accounts to gain initial access. In 30% of incidents, attackers used valid accounts, whether cloud, domain or local, to compromise European organizations. Phishing tied with the use of valid accounts at 30%, while the exploitation of public-facing applications and use of external remote services accounted for 20% each. The top three impacts to European-based organizations were credential harvesting at 28%, extortion at 24% and data leak at 16%.

Manufacturing moved from second place in 2022 to the most-attacked industry, accounting for 28% of incidents. Professional, business and consumer services placed second with 25% of cases and in third place was finance and insurance at 16%, surpassing energy, which held fourth place at 14%.

The United Kingdom was the most attacked country in Europe, accounting for 27% of cases. Germany accounted for 15%, Denmark 14%, Portugal 11%, and Italy and France each represented 8%. X-Force also responded to smaller numbers of cases in Greece, Austria, Greenland, Spain, Poland, Switzerland, Netherlands, Ukraine and Belgium.

■ In North America, the use of valid accounts was the top initial access vector at 41%



#2 | North America

North America continues to climb slightly year over year, moving from 23% of all cases in 2021 to 25% in 2022 and now 26% in 2023, making it the second most impacted region globally. The top actions on objective in this region were the deployment of malware and the use of legitimate tools for malicious purposes, accounting for 46% of incidents each. The most prevalent malware observed across incidents were backdoors at 14% and ransomware and bots at 11% each. Server access cases came in second at 21% and BEC cases made up 7%, placing it at a distant third.

The use of valid accounts was the top initial access vector at 41% of incidents. The prevalence regarding the use of valid domain accounts is a new trend from 2022, where the exploitation of public-

facing applications was the top initial access vector in North America. This shift is likely due to threat actors attempting to evade EDR and network detection and response (NDR) products by using credentials acquired from criminal markets, infostealers or other credential harvesting campaigns. At 32% of incidents, the exploitation of public-facing applications still made up a large share in 2023, placing it in second place and the use of phishing rounded out the top three at 27%.

Credential harvesting remained the top impact, accounting for a slightly larger share of incidents (28%) in 2023 than in the previous year (25%). Data theft and extortion tied for second place at 24% each, and reconnaissance accounted for 20% of cases X-Force remediated in North America.

Professional, business and consumer services rose from third place in 2022 to the most-targeted industry in North America in 2023, accounting for 22% of cases. The retail and wholesale sector remained in second place at 18% and healthcare rose one spot from fourth place in 2022 to third place in 2023, accounting for 15% of incidents. Energy, which was in first place in 2022, dropped to sixth place in 2023, making up 9% of incidents.

The United States accounted for 86% of the region's attacks compared to Canada's 14%.

■ Backdoors saw a significant falloff, going from 31% in 2022 to 3% in 2023



#3 | Asia-Pacific

Dropping from first place in 2022 to third in 2023, the Asia-Pacific region accounted for 23% of incidents X-Force responded to globally. Malware was the top action on objective once again, representing 45% of attacks with ransomware accounting for 17% of incidents and infostealers at 10%. Backdoors, which accounted for 31% in 2022, made up only 3% of cases in 2023. The use of legitimate tools for malicious purposes placed second at 28% with tools that exfiltrate data one of the most observed at 14% of incidents. Server access cases, accounting for 14% of incidents, was the third most observed action on objective against Asia-Pacific organizations.

Phishing was the top initial access vector, accounting for 36% of incidents. Exploitation of public-facing applications came in a close second at 35% of incidents. The use of valid accounts, abuse of trusted relationship and replication through removable media all tied for third, accounting for 12% of the cases each. Top impacts to this region were brand reputation and data theft at 27% each, followed by extortion, data destruction and data leak all accounting for 20% of cases.

Manufacturing, represented in 46% of the incidents, was the most-attacked industry in Asia-Pacific for the second year in a row. The finance and insurance, and transportation industries tied for second, accounting for 12% of cases each, while education was third at 8%. Japan accounted for 80% of Asia-Pacific cases, and Australia 11%.

■ 33% of cases X-Force observed in Latin America were data leak related

#4 | Latin America

Latin America was once again the fourth most impacted region in the globe in 2023, accounting for 12% of cases that X-Force responded to. For the purposes of reporting, IBM considers Latin America to include Mexico, Central America and South America. X-Force continues to observe [new and improved campaigns](#) that target Latin America specifically, emphasizing a worrying trend of increased risk to the region in the future.

Malware, and specifically ransomware, was once again the top action on objective observed across incidents in this region, representing 31% of the attacks. Server access and use of tools for malicious purposes each accounted for 23% of cases. Exploitation of public-facing applications moved from second to first place for

initial access vectors, comprising 45% of the cases. The use of phishing and valid accounts tied for second at 22% of cases each. Replication through removable media followed at 11%.

Of impacts to clients, 33% of cases X-Force observed in Latin America were data leak related. 22% resulted in extortion or had an impact on brand reputation and illicit financial gain, botnet, data theft and credential harvesting, each represented 11% of cases.

Once again, retail-wholesale returned as one of the most attacked industries at 25% of cases that X-Force remediated. Finance and insurance tied for first place, moving up from second place in 2022. IBM has observed an uptick in campaigns leveraging

[malicious Chrome extensions](#), the majority of which focused on Latin American financial entities. X-Force has also seen increased development and activity of .NET-based banking Trojans targeting banking customers in Latin America, such as [BlotchyQuasar](#), [KLBanker](#) and [Banker.FN](#). Several industries tied for second: mining, manufacturing and energy at 14% each.

Brazil remained the most attacked country in Latin America, making up 68% of all the cases that X-Force responded to in Latin America. Colombia accounted for 17% and Chile 8%.



■
50% of incidents X-Force responded to in the Middle East and Africa involved malware

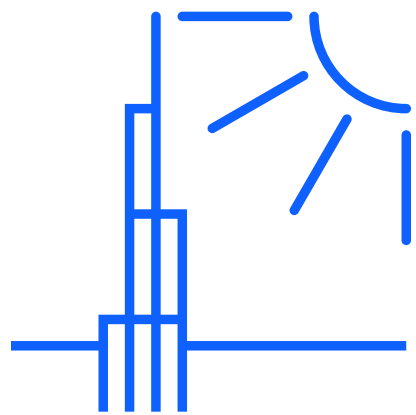
#5 | Middle East and Africa

The Middle East and Africa region, which encompasses the Levant, the Arabian Peninsula, Iran and Iraq, and the entire African continent, was the fifth most targeted geographic region, representing 7% of incidents in 2023. In half of the incidents X-Force responded to in this region, the deployment of malware was observed. At 17% each, DDoS, email threat hijacking, server access and the use of legitimate tools for malicious purposes represented the remaining top actions on objectives.

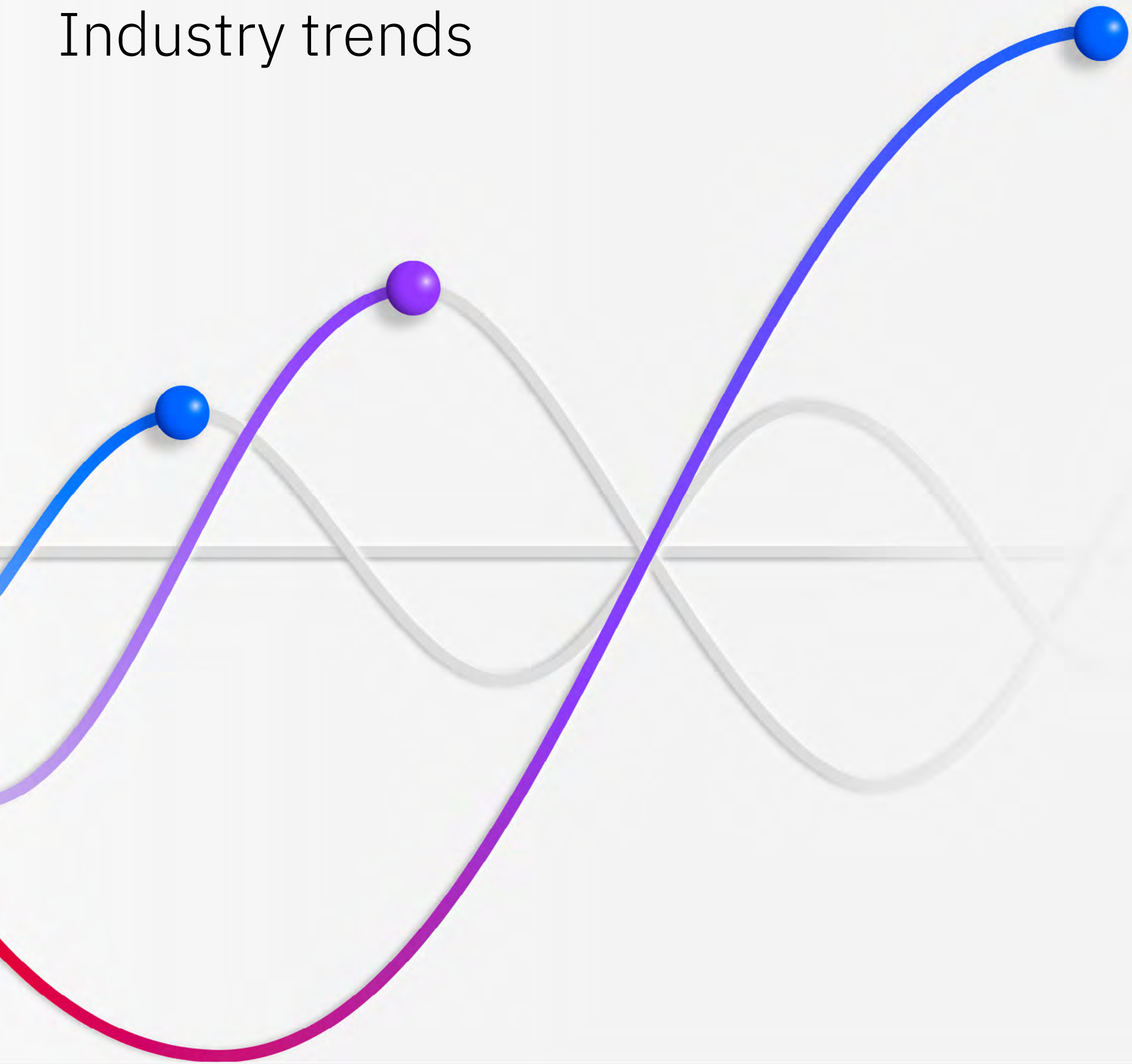
The use of valid local accounts at 52% and valid cloud accounts at 48% were the main initial infection vectors used on organizations in the Middle East and Africa region and espionage was the top impact.

Once again, the finance and insurance industry was the most attacked industry within the Middle East and Africa region, representing 38% of incidents. It was followed by transportation services and energy, which tied at 19%, and professional, business and consumer services at 13%.

Saudi Arabia remained the most targeted country in this region, comprising 40% of incidents, with United Arab Emirates at 30% and Mauritius at 12%.



Industry trends



For the third year in a row, manufacturing was the top-attacked industry, according to X-Force incident response data. The finance and insurance industry was in second place again for the third year in a row. Share of attacks across energy, retail and wholesale, healthcare, transportation and arts, entertainment and recreation sectors increased year over year.

Notably, 69.6% of attacks that X-Force responded to in 2023 were against critical infrastructure organizations.⁴⁰ Attackers exploited public-facing applications in 30% of incidents, making it the most common cause of attacks on critical infrastructure, with phishing and the use of valid accounts closely following, each representing 29% and 25% of attacks observed.

Malware was deployed in 44% of incidents, with ransomware making up most of those attacks at 23%. Use of legitimate tools for credential acquisition, remote access and data exfiltration, was also a common action on objective seen in 34% of incidents.

About a third of attacks on critical infrastructure led to data theft and leak, with extortion and credential harvesting following at 29% and 24%, respectively. The data reaffirmed that critical infrastructure is a high-value target to adversaries, wagering on these organizations' low threshold for downtime to advance on their objectives.

Share of attacks by industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

45%

of manufacturing attacks employed malware

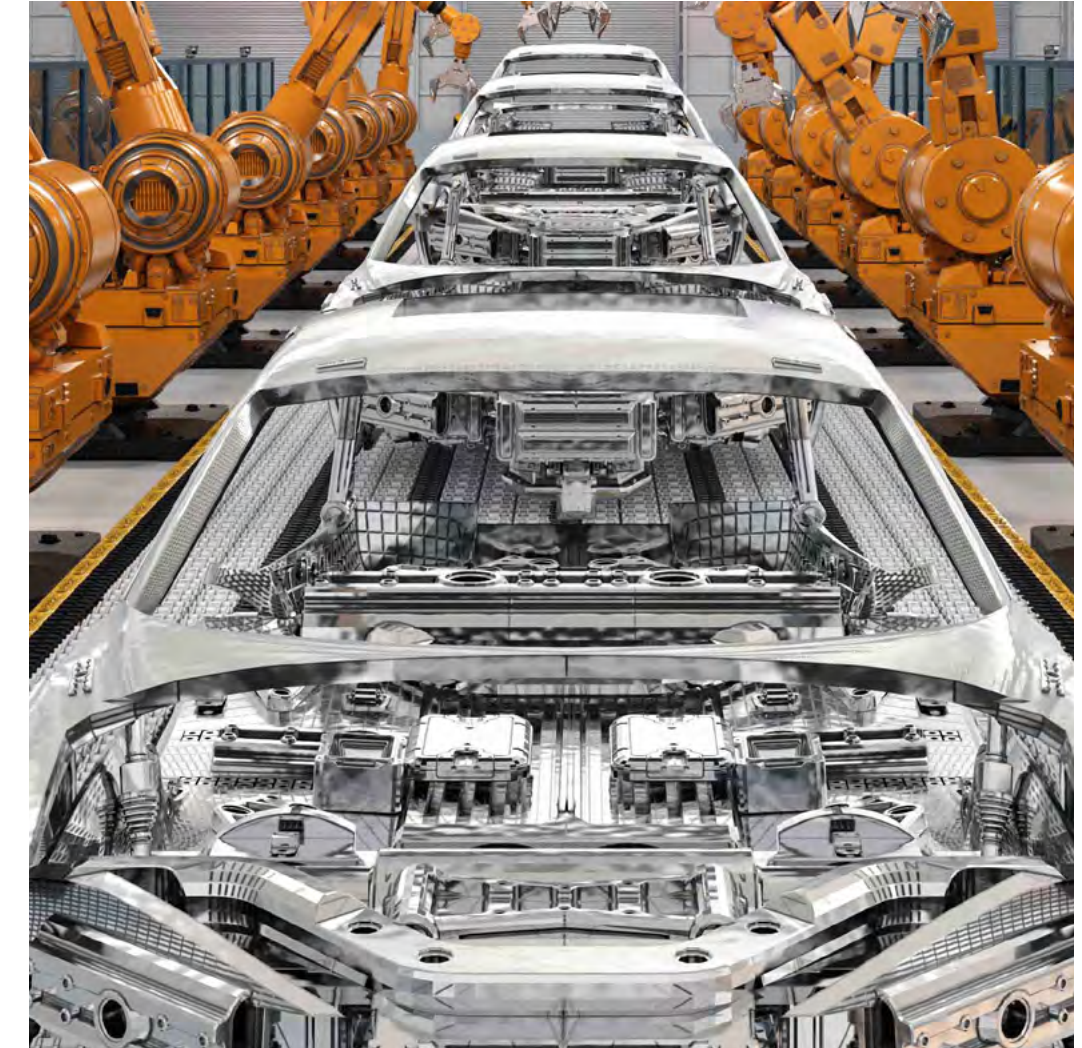
#1 | Manufacturing

Manufacturing was once again the top attacked industry in 2023 for the third year in a row, representing 25.7% of incidents within the top 10 industries. Malware was the top action on objective observed at 45%. Ransomware accounted for 17% of incidents, which is what was observed in 2022. The use of legitimate tools for malicious purposes was observed in 31% of incidents, with the use of tools to steal credentials the top offender at 17%. Server access incidents accounted for 21% of the cases, which is an increase from 2022 where these cases accounted for 17%.

Credential harvesting and data theft and leak were both the top impacts on manufacturing organizations, involved in

36% of incidents each, followed by data destruction and extortion at 16% of cases each. Phishing was the top initial infection vector, representing 39% of incidents, impacting the manufacturing industry, followed by exploitation of public-facing applications at 33%, and abuse of external remote services at 22% of cases.

Once again, the Asia-Pacific region saw the most incidents in manufacturing in approximately 54% of cases. Europe saw the second most at 26%, followed by North America at 12% and Latin American at 5%.



38%

of finance and insurance incidents involved malware

#2 | Finance and insurance

Finance and insurance trailed behind manufacturing as the second most attacked industry in 2023 for the third year in a row, representing 18.2% of incidents to which X-Force responded. Malware was the most common action on objective observed, accounting for 38% of incidents within the finance and insurance industry, with ransomware accounting for 25% of cases. Server access cases came in second at 25% of attacks, while the use of legitimate tools for malicious purposes was the third most observed action on objective, accounting for 19% of incidents.

Extortion was the top impact observed on finance and insurance organizations in 2023 at 35%, followed by botnet at 28%

and credential harvesting at 19%. The use of phishing was the most common initial infection vector at 28%, followed closely by the use of valid accounts in 27% of cases remediated by X-Force. The third most observed initial access vector was the abuse of external remote services at 27%.

Europe once again experienced the highest percentage of incidents in the finance and insurance industry at 37%, while Latin America saw the second most at 17% with North America, the Middle East and Africa, and the Asian-Pacific each experiencing 15% of attacks.



22%

of professional, business and consumer services malware cases involved crypto miners

#3 | Professional, business and consumer services

The professional, business and consumer services sector was the third most attacked industry, accounting for 15% of cases. The professional services industry includes consultancies, management companies and law firms. These services make up 34% of victims in this segment. Business services include firms such as IT and technology services, public relations, advertising and communications. These services represent 42% of victims. Consumer services, encompassing home builders, real estate, arts, entertainment and recreation, accounted for 24% of cases.

Malware cases represent half of observed incidents in the professional, business and consumer services sector. Notably, crypto

miners were the most observed malware, accounting for 22% of all cases. The use of legitimate tools for malicious purposes was the second most observed action on objective, accounting for 21% of incidents and spam campaigns and server access cases tied for third representing 14% of attacks each.

The top infection vector was the use of valid accounts observed in 46% of incidents. In second place was phishing at 31% and exploitation of public-facing applications came in third at 24% of attacks. Digital currency mining and credential harvesting tied as the most common impact, representing 27% of cases each, followed by extortion at 18% of cases.



X-Force responded to 49% of cases in Europe, 36% in North America, 7% in the Asia-Pacific, 5% in the Middle East and Africa, and 3% in Latin America.

43%

of energy cases
involved malware

#4 | Energy

Energy organizations, including electric utilities and oil and gas companies, were the fourth most attacked industry, representing 11.1% of attacks. Malware was the most common action on objective observed, representing 43% of cases, with ransomware cases accounting for 22% of attacks. The use of legitimate tools for malicious purposes was the second most observed action on objective, accounting for 36% of incidents and server access incidents followed at 21%.

Data theft and leak accounted for the top impact on energy organizations at 33% of observed cases, followed by digital

currency mining and extortion tying for 22% of incidents each. The exploitation of public-facing applications was the top initial infection vector, representing half of the cases, followed by the use of valid local accounts at 38% and replication through removable media in 13% of cases.

Europe experienced the highest percentage of incidents within the energy sector at 43%, followed by North America at 22%, Latin America at 14% and the Middle East and Africa and Asia-Pacific at 11% each.



50%

of incidents in the retail and wholesale industry involved malware

#5 | Retail and wholesale

In 2023, the retail and wholesale industry accounted for 10.7% of all incidents to which X-Force responded. 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.

Malware was the most common action on objective observed, accounting for 50% of incidents within the retail and wholesale industry, with ransomware accounting for 26% of total cases. BEC cases came in second at 38% of attacks, while the use of legitimate tools for malicious purposes, server access and spam campaigns tied as the third most observed action on objective, accounting for 13% of incidents each.

The top impacts observed on retail and wholesale organizations in 2023 at 25% each were illicit financial gain, reconnaissance and extortion. The use of valid accounts was the most common initial infection vector at 43%, followed by phishing and the exploitation of public-facing applications, each representing 29% of the cases. Leveraging drive-by compromise was observed in 14% of cases.

North America experienced the highest percentage of incidents in this industry at 56%, while Latin America saw the second most at 32% and Europe experienced 11% of attacks.



59%

of healthcare incidents involved valid account abuse

#6 | Healthcare

Moving up one spot from the seventh most attacked in 2022 to sixth most attacked in 2023 and accounting for 6.3% of total attacks is healthcare. The use of legitimate tools for malicious purposes was the most observed action on objective, accounting for 43% of incidents, and spam campaigns and malware cases tied for second, representing 29% of attacks each. Email thread hijacking and server access cases each represented 14%.

The top infection vectors observed in the healthcare industry was the use of valid accounts at 59% of incidents. The exploitation of public-facing applications

at 21% and the use of phishing at 20% rounded out the top three. The top impact observed was credential harvesting, accounting for half of the cases, followed by reconnaissance, data leak and extortion, each representing 25% of the cases.

X-Force responded to 50% of cases in North America, 38% in Europe, 6% in the Asia-Pacific and 6% in Latin America.



40%

of government incidents
involved phishing incidents

#7 | Government

Accounting for 4.3% of incidents—and moving up one spot from 2022—government was the seventh most attacked industry in 2023. The use of legitimate tools for malicious purposes and DDoS attacks were the most observed actions on objective, each accounting for 33% of incidents. Server access, adware and malware each accounted for 17% of cases.

The top infection vector observed in government was phishing at 40% of incidents. The exploitation of public-facing applications, replication through removable media and drive-by compromises were each observed in 20% of cases. The top impacts observed were credential harvesting, data leak, extortion and botnet activity, each representing 33% of the cases.

In 2023, government entities, though representing a small fraction of reported incidents, witnessed an uptick in cybersecurity threats, according to X-Force, compared to 2022. Despite being the least likely to meet ransom demands, governments remain attractive targets for criminal threat actors.

The persistence of cybercriminals in targeting government networks is fueled by the vast amount of sensitive data these entities possess, obtained through the wide range of services provided to companies and people. Successful breaches could result in the leakage of state-level intelligence, classified assets and personal identifiable information (PII). Such leakage poses risks, such as identity theft, creation of forged documents, unauthorized access



to organizations and the takeover of privileged accounts through the sale of stolen data in dark marketplaces.

X-Force responded to 64% of cases in North America, 26% in the Asia-Pacific and 9% in the Middle East and Africa.

67%

of transportation incidents involved data leak and extortion

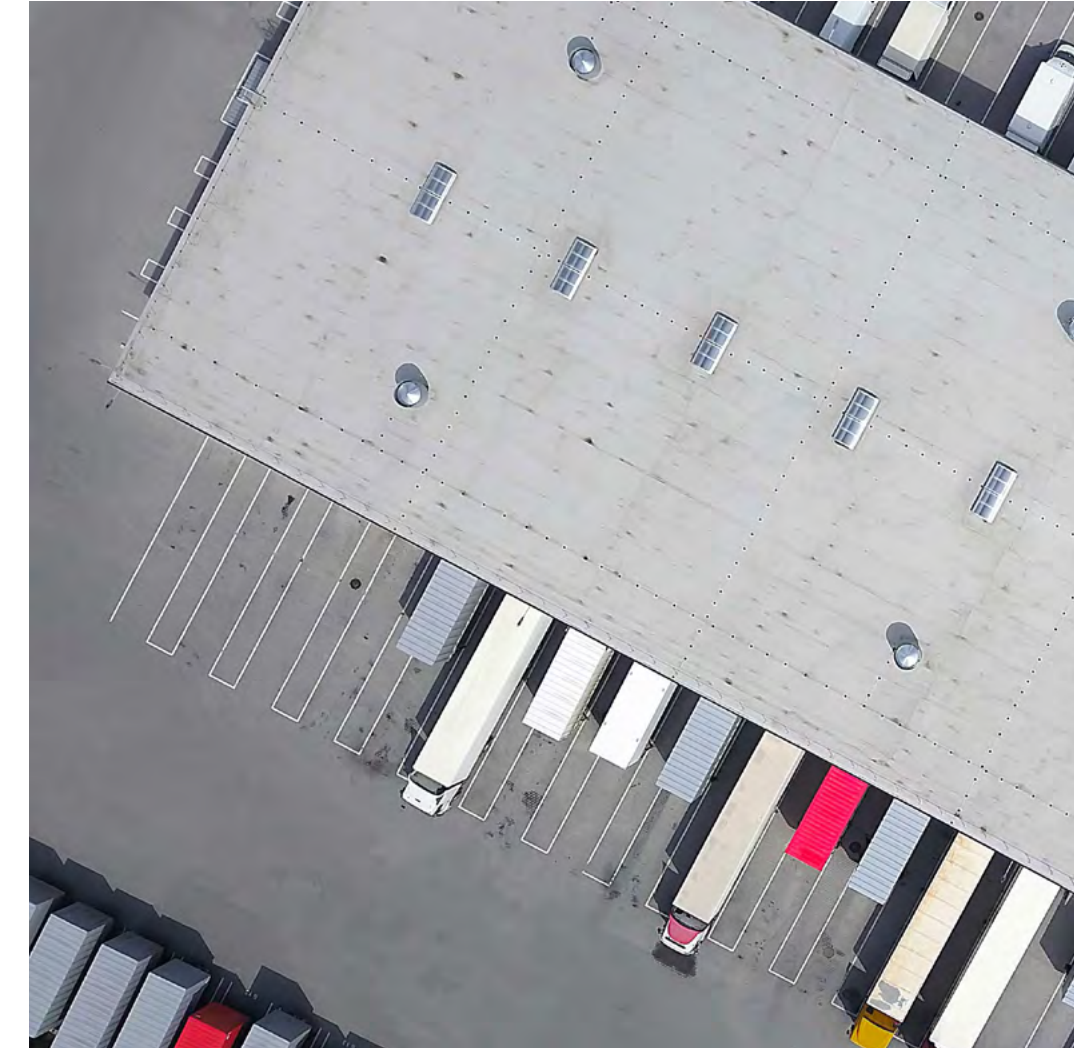
#8 | Transportation

Up from ninth place in 2022, transportation accounted for 4.3% of incidents and ranked eighth in 2023. Malware and the use of legitimate tools for malicious purposes were the top actions on objective observed, both representing 38% of attacks. Server access attacks were observed in 13% of incidents.

Data leak and extortion were both the top impacts on transportation organizations, involved in 67% of incidents each, followed by data destruction at 33%. The exploitation of public-facing applications

and use of phishing were the top initial infection vectors, each representing 50% of incidents impacting the transportation industry, followed by use of valid local accounts, used in 25% of attacks.

Unlike 2022, where European transportation entities were the most targeted group, in 2023, the Asia-Pacific experienced the most attacks at 63%. The Middle East and Africa accounted for 27% of attacks in this industry, while Europe accounted for 10%.



2.8%

of incidents remediated by X-Force were in the education sector

#9 | Education

Dropping from sixth place in 2022 to ninth place in 2023, education accounted for 2.8% of incidents remediated by X-Force. Notably, malware was the most commonly observed action on objective, while X-Force also observed the use of legitimate tools for malicious purposes in a larger portion of incidents.

Data theft, data destruction and extortion were the top impacts on education organizations. Top initial infection vectors included phishing and the use of valid accounts. Most commonly, X-Force responded to incidents across education in North America and the Asia Pacific.



1.2%

of incidents X-Force responded to involved media and telecommunications

#10 | Media and telecommunications

Media and telecommunications accounted for only 1.2% of incidents to which X-Force responded, coming in last place for the third year running. The use of legitimate tools for malicious purposes and server access were commonly observed actions on objective. Media organizations were predominantly targeted in the Middle East, the Asia Pacific and Europe regions.



Recommendations



In 2023, the combination of a rise in infostealers and the abuse of valid account credentials to gain initial access has exacerbated defenders' identity and access management challenges. The threat landscape's newly found focus on identities highlights organizations' risks that exist on devices outside of their visibility. Enterprise credential data can be stolen from compromised devices through credential reuse, browser credential stores or accessing enterprise accounts directly from personal devices.

The speed of an intrusion has increased due to effective, repeatable attack paths—as seen with the massive exploitation of MFT tools and Kerberoasting attacks—and the growing efficiency in the criminal marketplace through realized competitive advantage. And while ransomware and other malware continue to plague organizations, cybercriminals have begun to explore how to leverage AI in their operations.

Given these trends, how should organizations respond and where should they start?

Reduce the risk of credential harvesting attacks

Deploying [EDR](#) tools on all servers and workstations in your environment helps detect malware, including infostealers and ransomware. The tools can also detect anomalous behavior, such as the exfiltration of data, querying of sensitive information or the creation of new accounts or folders on sensitive systems.

Leverage experts to learn more about how to build and operationalize [threat hunting](#) within your environment. If resources are limited, extend your team by using AI to handle up to 85% of alerts and gain 24x7 protection with [threat detection and response services](#). Additionally, use [threat intelligence](#) to identify key opportunities for mitigating new and emerging threats from attackers looking to steal your credentials.

Harden your credential management practices to protect your system or domain credentials by implementing MFA and strong password policies to include use of passkeys, and leverage hardened system configurations that make accessing credentials more difficult. Credential harvesting attacks are also often carried out through phishing and watering hole attacks.

Routinely provide employee education with updated phishing techniques used by attackers. Scrutinize all third-party traffic—treat it as untrusted until otherwise verified. Watering hole attackers often leverage legitimate resources to deliver their malware.

Reduce blast radius

Cybersecurity blast radius refers to the potential impact of an incident given the compromise of particular users, devices or data. For example, if an account with administrative privileges is compromised, the blast radius is greater than if a normal nonprivileged account is given the ability to move laterally and access additional data across the network.

Given the importance of data security and identity management in the current threat landscape, organizations should consider [implementing solutions](#) to reduce the damage that a data security incident could potentially cause.

Strategies to reduce blast radius:

- Implement a least-privileged framework.
- Provide identity and network segmentation.
- Implement data security and protection solutions.
- Provide continuous monitoring and [incident response](#).

Know your dark web exposure

Attackers may leverage harvested credentials for their own exploits, trade them on the dark web—or both. The data that’s available about your organization on the dark web highlights the risk that resides outside your network perimeter’s control.

Employ [dark web capabilities](#) that:

- Find at-risk credentials and session keys.
- Check your executive’s digital identities to find overexposure of PII, criticism against executives and fraudulent profile creation in social networks.
- Scan social networks, channels related to your sector, and blogs and advertising for unauthorized brand use.
- Identify leaked priority, confidential and sensitive data.
- Assess forums, credit card markets, Telegram channels, chat rooms and discussions, code repositories, document and file repositories, surface web crawlers, and paste sites checking for credential exposure and stolen session keys.

Remove fragmented identity silos

Properly deploying a product-agnostic [identity fabric](#) can extend modern security and detection and response capabilities to outdated applications and systems. Simplify identity management through a single [identity and access management](#) (IAM) provider to administer identity governance, manage workforce and consumer identity and access, and control privileged accounts. Streamline the undertaking with [identity and security experts](#) to help you define and manage solutions across hybrid cloud environments, transform governance workflows and demonstrate compliance.

Implement a DevSecOps approach and testing

X-Force found that the most observed risk across client environments globally in 2023 was security misconfigurations and, of those found, the top offenses included allowing concurrent user sessions in the application. Limit the possibility of session hijacking by [implementing a DevSecOps approach](#) and use secured, encrypted connections (HTTPS) and implement session timeouts and prompt for reauthentication. Engage [penetration testing services](#) to test your applications, networks, hardware and personnel to identify vulnerabilities and weaknesses across all your assets.

Have a plan

Despite organizations' best efforts to reduce the risk of attack, incidents can happen. Having [incident response](#) plans that are customized for your environment is key to reducing the time to respond, remediate and recover from an attack. Those plans should be regularly drilled and 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.

Establish secured AI+ business models

Securing AI is broader than AI itself. Organizations can leverage existing guardrails to help secure the AI pipeline. The key tenets to focus on are securing the AI underlying training data, the models, and the use and inferencing of the models, but also the broader infrastructure surrounding the models. The same access points that cybercriminals are leveraging to compromise enterprises pose the same type of risk to AI. And as organizations offload operational business processes to AI, they also need to establish governance and make operational guardrails central to their [AI strategy](#).

About us

IBM X-Force

IBM 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 IBM 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 IBM 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 X-Force analysts 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 briefing with an IBM X-Force expert.

[Schedule a briefing →](#)



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 strive for ambitious business goals, while exploring pivotal new technologies and helping minimize unexpected threats.

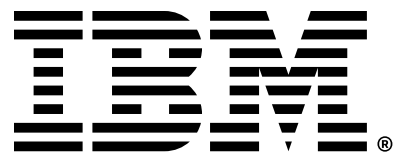
[Learn more](#) →

Contributors

Christopher Caridi
John Dwyer
Georgia Prassinos
Kat Metrick
Austin Zeizel
Joshua Chung
Dave McMillen
Benjamin Shipley
Charlotte Hammond
Golo Mühr
Ole Villadsen
Joseph Fasulo
Claire Zaboeva
Melissa Frydrych-Dean

Richard Emerson
Camille Singleton
Michelle Alvarez
Andy Piazza
Karlina Bakken
Yannick Bedard
Christopher Bedell
Johnny Shaieb
Scott Lohr
Scott Moore
Guy Vincent Jourdan
Vio Onut
Julien Cassagne

1. MITRE ATT&CK Matrix, 19 July 2019.
2. These observations were made within the X-Force global intelligence honeypot.
3. Microsoft server share jumps in 2001, CNET, 25 September 2002.
4. Global Energy Cyberattacks: “Night Dragon,” McAfee, 10 February 2011.
5. RSA Blames Breach on Two Hacker Clans Working for Unnamed Government, Wired, 11 October 2011.
6. ManyKatz: How Active Directory Hacks Went Mainstream, QOMPLX, 2020.
7. The Evolution of Cybercrime and Cyberdefense, Trend Micro and the U.S. Secret Service, 2018.
8. The Untold Story of the Target Attack Step by Step, Aorato Labs, August 2014.
9. Deconstructing the 2014 Sally Beauty Breach, Krebs on Security, 7 May 2015.
10. The Evolution and Exploits of FIN7: From PoS Malware to Ransomware Dominance, Cyware, 31 August 2023.
11. Market Share of Microsoft Active Directory, 6sense.
12. Secure Active Directory and Disrupt Attack Paths, Tenable, 2021.
13. Desktop Windows Version Market Share Worldwide, Statcounter, December 2023.
14. Publicly Available Tools Seen in Cyber Incidents Worldwide, Cybersecurity & Infrastructure Security Agency, 30 June 2020.
15. Sony Hack: Too Easy and Predicted by “The Paramount Brief” 5 Years Ago (Who’s Next & Is The Whole World Sitting on a Ticking Bomb?), Cyber-Security-Blog.com, 22 December 2014.
16. Business E-Mail Compromise: Cyber-Enabled Financial Fraud on the Rise Globally, Federal Bureau of Investigation, 27 February 2017.
17. As Big Companies Move Email to the Cloud, Microsoft Shows Strength, Fortune, 1 February 2016.
18. FBI Warns of Dramatic Increase in Business E-Mail Scams, FBI, 4 April 2016.
19. Widespread in Office 365: Zero-Day Virus Email Ransomware Attack, Avanan, 27 June 2016.
20. Avanan: New Puny-Phishing Attack on Office 365 Email Users, Avanan, 12 December 2016.
21. New Phishing Scam Using Microsoft Office 365, ALM and Credit Union Times, 13 December 2016.
22. Deployment breakdown for Microsoft Exchange Server mailboxes worldwide from 2018 to 2022, Statista, 5 September 2023.
23. Microsoft Office 365 Security Observations, Cybersecurity & Infrastructure Security Agency, 13 May 2019.
24. Internet Crime Complaint Center (IC3), Federal Bureau of Investigation.
25. Essential Microsoft Office Statistics In 2024, ZipDo, Global Commerce Media GmbH, 8 August 2023.
26. Email Security Risk Report: Uncovering inbound and outbound threats in Microsoft 365, Egress, 2023.
27. Internet Crime Report 2022, Federal Bureau of Investigation, 2023.
28. More Bitcoin malware: this one uses your GPU for mining, Ars Technica, 17 August 2011.
29. Move Over, Ransomware: Why Cybercriminals Are Shifting Their Focus to Cryptojacking, IBM, 17 July 2018.
30. By the Numbers: Are Your Smart Home Devices Being Used as Cryptocurrency Miners? Trend Micro, 5 October 2017.
31. Executive Summary: 2018 Internet Security Threat Report, Symantec, March 2018.
32. Ethereum hits another record high after bitcoin and is now up over 5,000% since the start of the year, Tech Transformers, 12 June 2017.
33. Two-Week Rally Pushes Monero to New Record High, CoinDesk, 13 September 2021.
34. Cryptojacking rates increased by 85 times in Q4 2017 as bitcoin prices spiked: report, The Verge, 22 March 2018.
35. Why cryptocurrency mining malware is the new ransomware, ZDNet, 28 June 2018.
36. Internet Organised Crime Threat Assessment 2018, Europol, 11 January 2019.
37. TrickBot’s Cryptocurrency Hunger: Tricking the Bitcoin Out of Wallets, IBM, 15 February 2018.
38. Adapting To The Times: Malware Decides Infection, Profitability With Ransomware or Coinminer, Trend Micro, 9 July 2018.
39. Cryptojacking Rises 450 Percent as Cybercriminals Pivot From Ransomware to Stealthier Attacks, IBM, 26 February 2019.
40. Critical infrastructure in this report is defined as organizations in the financial services, manufacturing, energy, transportation, healthcare, government, education and telecommunications sectors.



© Copyright IBM Corporation 2024

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2024

IBM, the IBM logo, IBM Security, and X-Force are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on [ibm.com/trademark](https://www.ibm.com/trademark).

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat is a trademark or registered trademark of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware is a registered trademark or trademark of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.