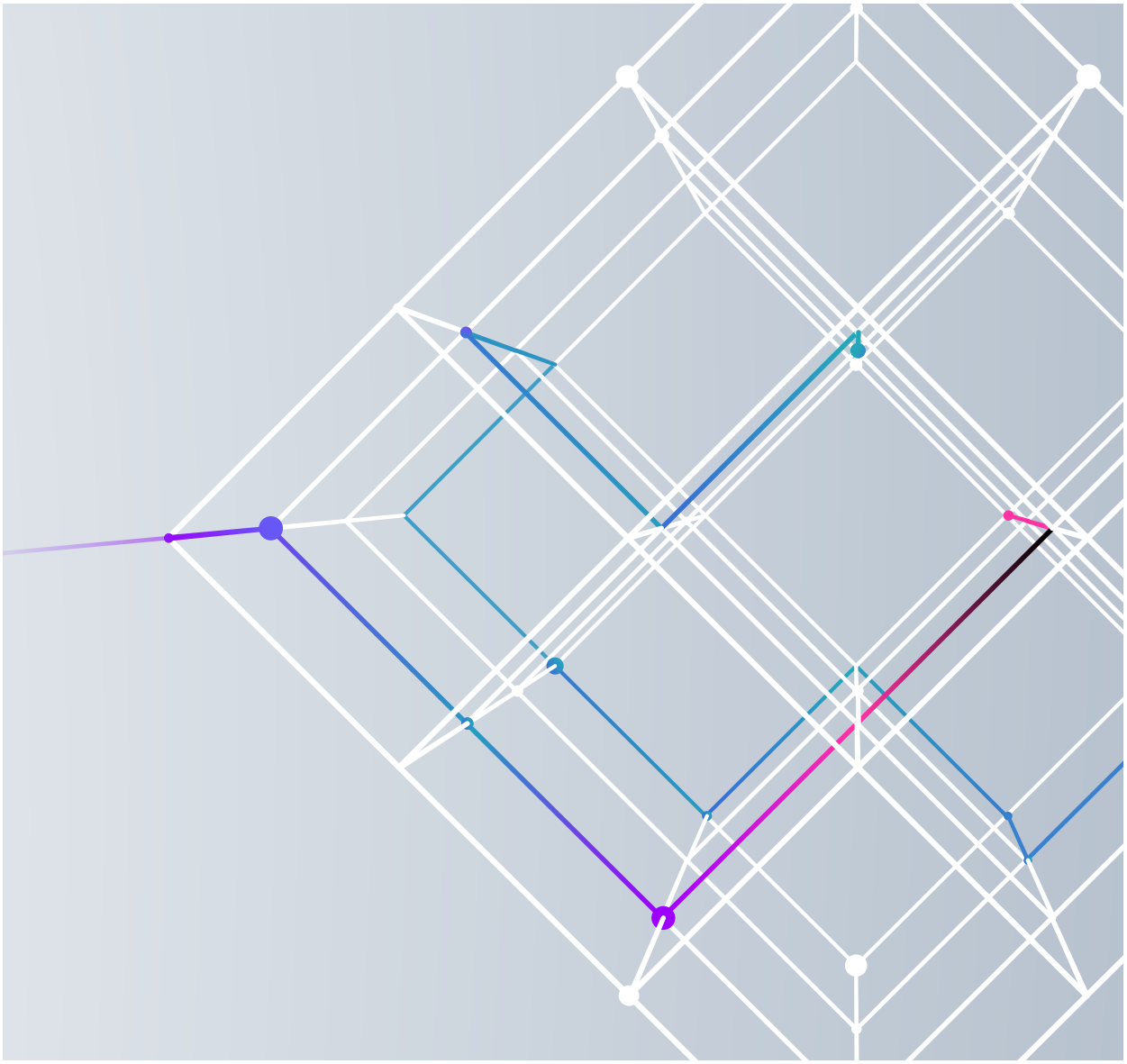
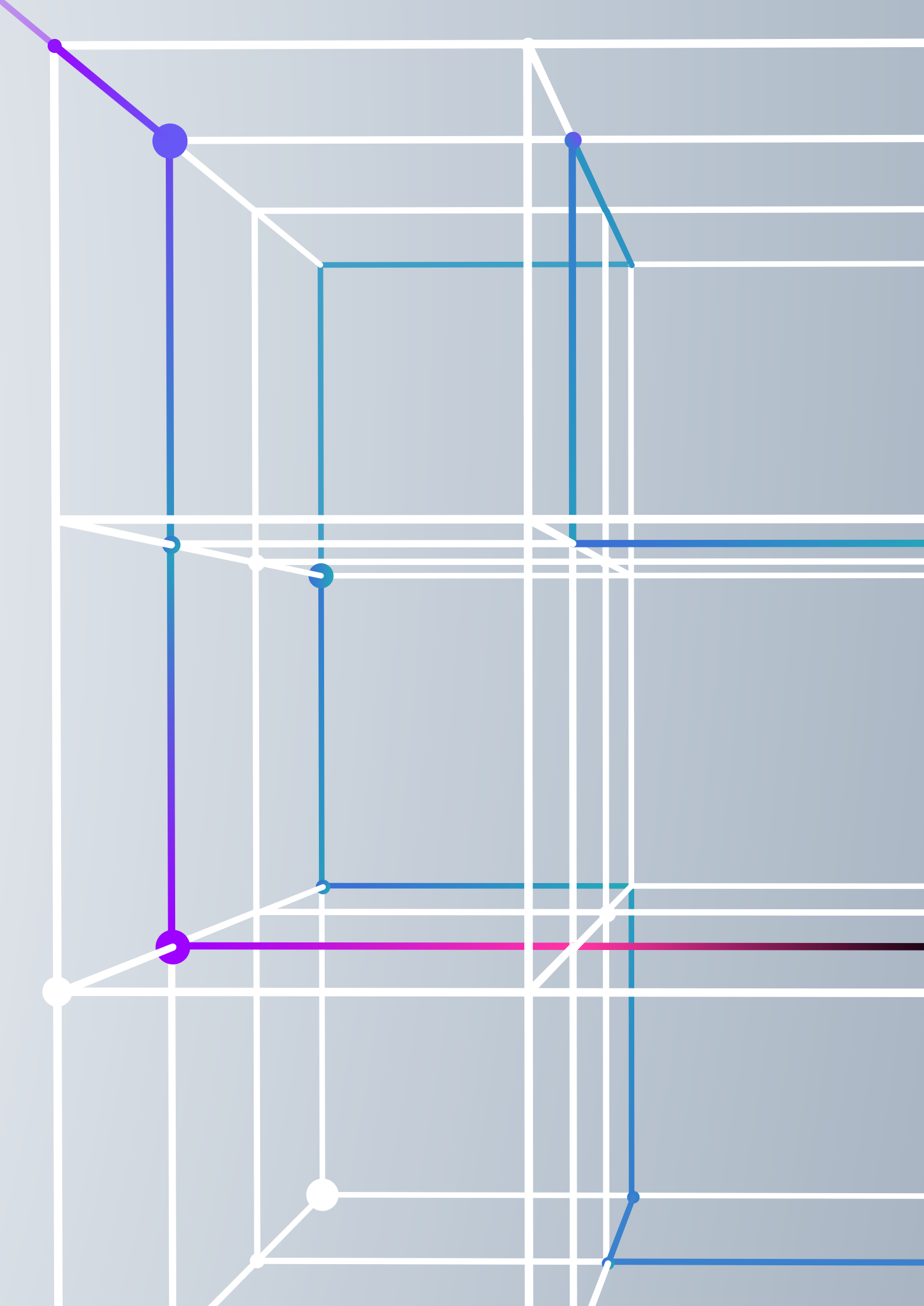


IBM X-Force 2025 Threat Intelligence Index

Red Hat

IBM



Foreword

The pattern is familiar. Organizations devote ever-growing resources to detect threats, protect networks, and deter disruption. And despite this, cyberattacks continue to grow in scale, speed, and sophistication.

But over the past 18-24 months, there has been a marked change in tactics. Threat actors are pursuing broader-scale campaigns—demonstrating a level of coordination, automation, and prowess not seen before—and raising the likelihood and impact associated with operational risks. Unlike incidents of the past, where data breaches and reputational harm were the greatest concern, widescale business disruption is now a real possibility—something every boardroom needs to be aware of and act upon.

A campaign conducted by Salt Typhoon, an advanced persistent threat (APT) group, exemplifies this troubling trend. In 2024, this threat actor group compromised virtually every major US telecommunications provider—in addition to targets in dozens of other countries—impacting supply chains, energy infrastructure, transportation, healthcare, and other critical services, including breaches of highly sensitive government systems.[1]

As the Salt Typhoon attack demonstrates, threat actors are becoming more proficient at hiding illicit activity. They are massively increasing their use of compromised credentials to log in to networks, precluding any need to hack in. And doing so makes this activity much harder to detect and isolate. When threat actors use public cloud infrastructure, it becomes far more difficult for cyberdefenders to discern between safe and unsafe workloads.

The new litmus test is how well we can defend against resourceful threat actors conducting campaign-oriented, supply chain attacks. While we can use standard cyber risk practices to mitigate individual threats, what we are seeing is the emergence of a categorically different kind of risk—one that seeks to exploit our growing reliance on interconnectivity and common digital services.

To see things differently, we ourselves need to change. CISOs can play a decisive role in advocating change—starting with the C-suite and boardroom—but also raising awareness and accountability across the organization and in collaboration with ecosystem partners.

The growing coordination and complexity of attacks points to a need for a multifaceted and multilateral response. Awareness and accountability need to extend to every partner in our ecosystem—so we are standing together. Many sentries make a vital, more secure community. This isn't such a radical notion. In fact, it's exactly what cyber adversaries are doing by building crime-as-a-service communities and malware marketplaces on the dark web.

When executives understand that "what happens to my partners also happens to me," they can take the necessary steps to support greater supply chain and ecosystem-level awareness and accountability. Coordination is critical to preventing intrusions, enabling rapid response, and mitigating the impact of attacks. Real-time threat intelligence, advanced multilayered defense platforms, zero trust network segmentation, and AI-powered monitoring are all essential components.

As stewards of trust, we are protecting not only our organizations and each other, but the integrity, values, and opportunities that bind us.

Since 1993, IBM has gathered, analyzed, and shared information and expertise about cyber attackers to help organizations navigate the evolving threat landscape. The IBM X-Force 2025 Threat Intelligence Index focuses on observations from our expert team of analysts, researchers, and hackers, tracking how threat actors get in, what they do when they're in, and the impact caused by each breach. With these insights, we look forward to helping you stay one step ahead of cyberthreats, reinforce your organization's operational resilience, and build strong, strategic partnerships that create cyber advantage now and into the future.

Key takeaways

Manufacturing is the #1-targeted industry, four years in a row.

Manufacturing organizations continued to experience significant impacts from attacks, including extortion (29%) and data theft (24%), targeting financial assets and intellectual property. Defying the declining trend in malware, manufacturing had the highest number of ransomware cases in 2024 as attackers continue to exploit outdated legacy technology in this industry.

Asia-Pacific region sees a 13% increase in attacks.

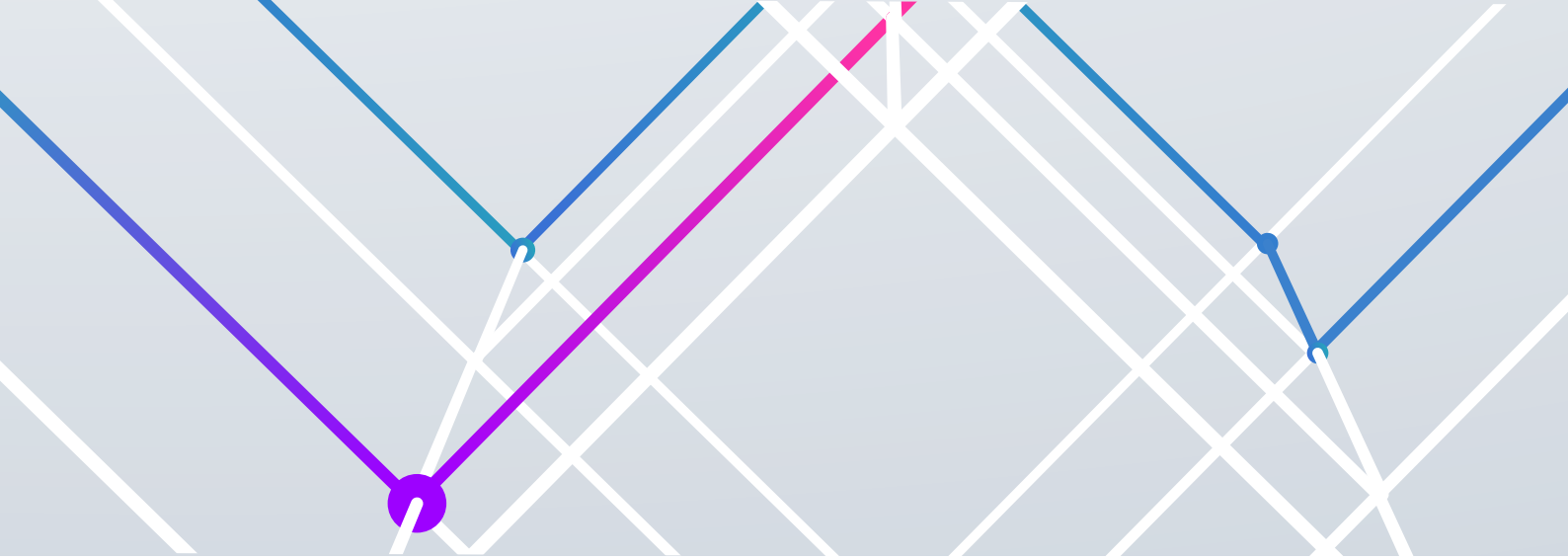
Asia-Pacific (APAC) experienced the largest share of incidents in 2024 (34%). This underscores APAC's growing exposure to cyberthreats, likely due to its critical role in global supply chains and its position as a technology and manufacturing hub.

Threat actors add AI to their toolboxes.

Our analysts have documented that threat actors are using AI to build web sites and incorporate deepfakes in phishing attacks. We have also observed threat actors applying gen AI to create phishing emails and write malicious code.[2]

Number of infostealers delivered via phishing emails per week increases by 84%.

Year-over-year, X-Force is seeing a rise in infostealers delivered via phishing emails and credential phishing. Both result in active credentials that may be used in follow-on, identity-based attacks. Phishing has emerged as a shadow infection vector for valid account compromises. By clicking on links that seem legitimate, users can unknowingly open the door to infostealer malware that siphons sensitive data from victims. Because adversaries hide and deliver malware payloads more cleverly, it can take longer to detect than ransomware and data breaches.



Identity-based attacks make up 30% of total intrusions.

For the second year in a row attackers adopted more stealthy and persistent attack methods, with nearly one in three attacks that X-Force observed using valid accounts. A surge in phishing emails distributing infostealer malware and credential phishing fuels this trend, which may be attributed to attackers leveraging AI to scale attacks.

Ransomware makes up 28% of malware cases.

While ransomware made up the largest share of malware cases in 2024 at 28%, X-Force observed a decline in ransomware incidents overall. This is the third year that ransomware incidents have declined. This may be part of a larger decline in ransomware attacks due to businesses being more reluctant to pay ransoms and increased government actions against ransomware groups.

4 out of top 10 vulnerabilities most mentioned on the dark web are linked to sophisticated threat actors.

All top 10 vulnerabilities had publicly available exploit code or were being exploited in the wild, with 60% of these having a public exploit available from less than two weeks after disclosure -- including several zero day vulnerabilities. This raises the risks for businesses as sophisticated threat actors, including nation-state actors, leverage dark web anonymity to acquire new tools and resources.

26% of attacks against critical infrastructure exploit public-facing applications.

One in four attacks exploited vulnerabilities in common public-facing or internet accessible applications. After gaining access, threat actors use active scanning techniques post-compromise to identify new vulnerabilities, gain additional access, and move laterally in compromised environments. Most importantly, attackers seek to escalate privileges to gain access to core services. The longer a threat remains undetected, the greater the risk. Long dwell times allow adversaries to mask their activity by “living off the land”—stealing data weeks or even months after an initial breach.[3]

Introduction

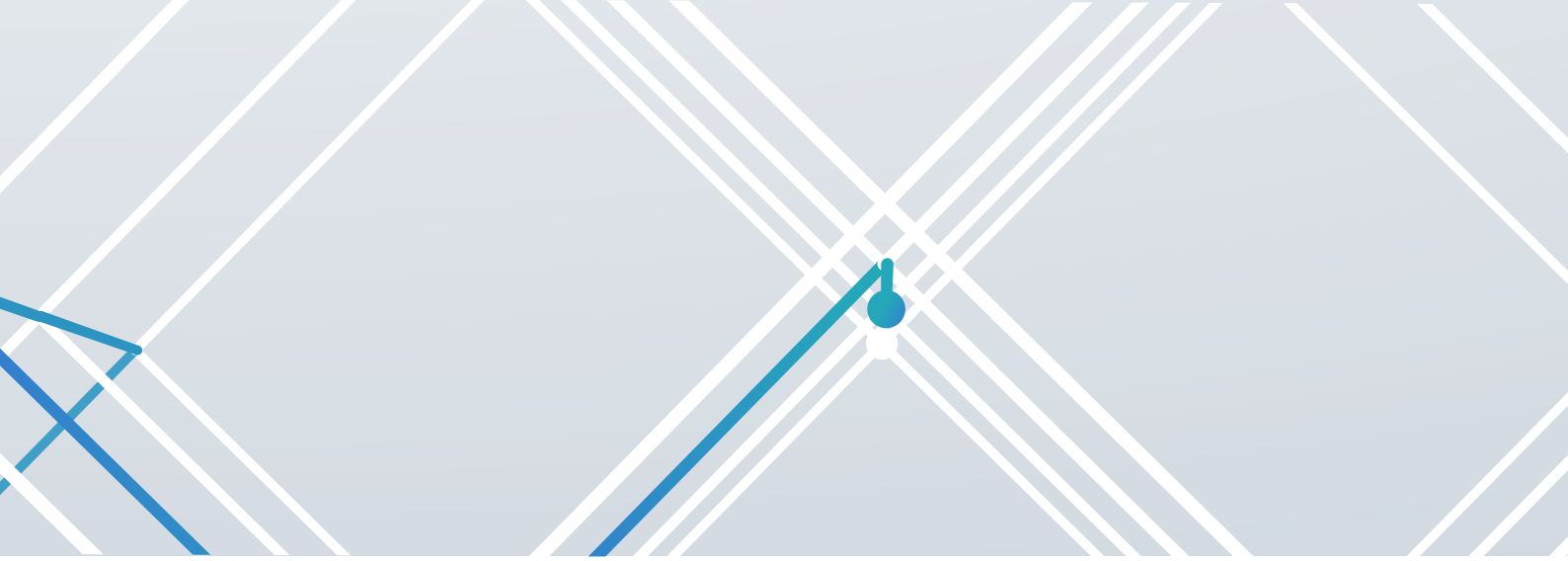
This year, we've seen shape-shifting cyber adversaries gain more access, move across networks more easily, and create new outposts in relative obscurity.

Equipped with advanced tools, threat actors are increasingly using compromised log-in credentials rather than brute-force hacking. The damage they inflict continues to grow as the global average cost of a data breach hit a record $4.88 million in 2024.[4]

What's even more concerning is that data breaches are often only the start of larger and more coordinated campaigns. Threat actors openly trade exploits on the dark web to target critical infrastructure such as power grids, health networks, and industrial systems. Ransomware and infostealer operators exfiltrate millions of credentials from enterprises and extort victim organizations in multiple ways. And as businesses manage multiple cloud environments and accelerate AI adoption, attack surfaces expand and create new gaps in identity that attackers exploit to steal critical data.

Cybercriminals are increasingly adopting stealthy tactics and prioritizing data theft over encryption and exploiting identities at scale. A surge in phishing emails delivering infostealer malware and credential phishing are fueling this trend—and may be attributed to attackers leveraging AI to scale distribution.

Generative AI is emerging as a new and growing addition to the toolbox of nation-state-backed threat actors, cybercriminals, hacktivists, and others. These adversaries are avid adopters, especially as they launch social engineering campaigns and high-tempo information operations. AI and automated solutions can magnify the impact of infostealers, expedite the fabrication of credentials, and make it easier to amplify the speed and scale of intrusions at lower cost.



Ransomware comprises nearly one-third (28%) of malware incident response cases and 11% of security cases, representing a decline over the last several years. This likely reflects an evolution in defensive tactics, such as increased collaboration with law enforcement, to take down the infrastructure of prominent botnets linked to ransomware attacks.

While the evolved defensive tactics are encouraging, ransomware attacks are still a notable threat. In fact, analysis of dark web data reveals a 25% increase in ransomware activity year-over-year—painting a different picture. Adoption of a cross-platform approach to ransomware, supporting both Windows and Linux, also appears to be the norm among ransomware threat groups—expanding attack surfaces. Although ransomware is being overshadowed by other tactics, it remains a major threat vector. The most dangerous trend in ransomware is the use of multiple extortion tactics. These attacks return dividends many times over.

With the increased effectiveness of endpoint detection and response (EDR) solutions detecting backdoor intrusion efforts via phishing, threat actors have shifted to using phishing as a shadow vector to deliver infostealer malware. In 2024, we observed an 84% increase in infostealers delivered via phishing. There was also a 12% year-over-year increase of infostealer credentials for sale on the dark web, suggesting increased usage.

Despite the magnitude of these challenges, we found that most organizations still don't have a cyber crisis plan or playbooks for scenarios that require swift responses. Quick, decisive action is required to counteract the faster pace with which threat actors, increasingly aided by AI, can conduct attacks, exfiltrate data, and exploit vulnerabilities.

The intersection of AI and cybersecurity

2023 was the “breakout year” for generative AI (or gen AI). And what we expected began to take shape—threat actors are using AI to build web sites and incorporate deepfakes in phishing attacks. X-Force found threat actors applying gen AI to create phishing emails and write malicious code.[5]

However, in terms of attackers building at-scale attacks targeting specific AI technologies, last year we predicted that once the technologies establish market dominance—when a single technology approaches 50% market share or when the market consolidates to three or fewer technologies—attackers will be incentivized to invest in attack toolkits targeting AI models and solutions.[6] Are we there yet? Not quite, but adoption is growing. The percentage of companies integrating AI into at least one business function has dramatically increased to 72% in 2024, up 55% from the previous year.[7]

New technologies, such as gen AI, create new attack surfaces. Security researchers are sprinting to find and help fix vulnerabilities before attackers do. We expect vulnerabilities in AI frameworks to become more common over time, such as the remote code execution vulnerability X-Force found in a framework for building AI agents.[8] Recently, an active attack campaign targeting a widely used open source AI framework was discovered, affecting education, cryptocurrency, biopharma, and other sectors.[9] Weaknesses in AI technology translate into vulnerabilities for attackers to exploit.

Another example of potential attack surfaces exposed in this new landscape is through machine learning operations (MLOps) platforms. These are used by enterprises of all sizes to develop, train, deploy, and monitor large language models (LLMs) and other foundation models (FMs), as well as the gen AI applications built on these models.[10]

As adoption grows, attacks on AI infrastructure and tools will gain traction. Organizations should prepare now for threats by securing the AI pipeline from the start, including underlying training data, models, and the broader infrastructure surrounding the models. Yet, this doesn’t appear to be the current practice across many organizations, with only 24% of generative AI projects secured.[11]

However, despite the evolving tools and different technologies attackers leverage—whether new gen AI tools or new AI infrastructure—the security fundamentals to thwart these attacks remain the same.

Our research shows threat actors are using valid credentials to log in; exploit unpatched vulnerabilities; and to a slightly lesser extent, phish their way in—with or without AI assistance. Organizations need to develop and run their own cybersecurity playbooks—seeking to identify exposures, assess risks, and mitigate incident impacts. But playbooks also need to account for who is responsible for specific actions, such as which party is accountable (and potentially liable) for securing a genAI solution offered by a third-party.

"Cybercriminals are most often breaking in without breaking anything – capitalizing on identity and access management gaps proliferating from complex hybrid cloud environments. Compromised credentials offer attackers multiple potential entry points with effectively no risk."

Mark Hughes,
Global Managing Partner for Cybersecurity Services, IBM

Top initial access vectors

The top initial access vector observed in 2024 was a tie between exploitation of public facing applications and use of valid account credentials, both representing 30% of X-Force incidence response engagements.

The abuse of valid account credentials is an area we highlighted last year after observing a dramatic rise, continuing the theme of "hackers don't break in, they log in." This continues to be a problem and an initial access vector that adversaries are quick to exploit.

Threat actors obtain valid credentials to use during attacks via a range of methods. Data from our dark web analysis and incident response engagements continue to point to infostealer malware as being prevalent across industries. Additionally, credentials are still purchased and sold in large quantities on dark web marketplaces.

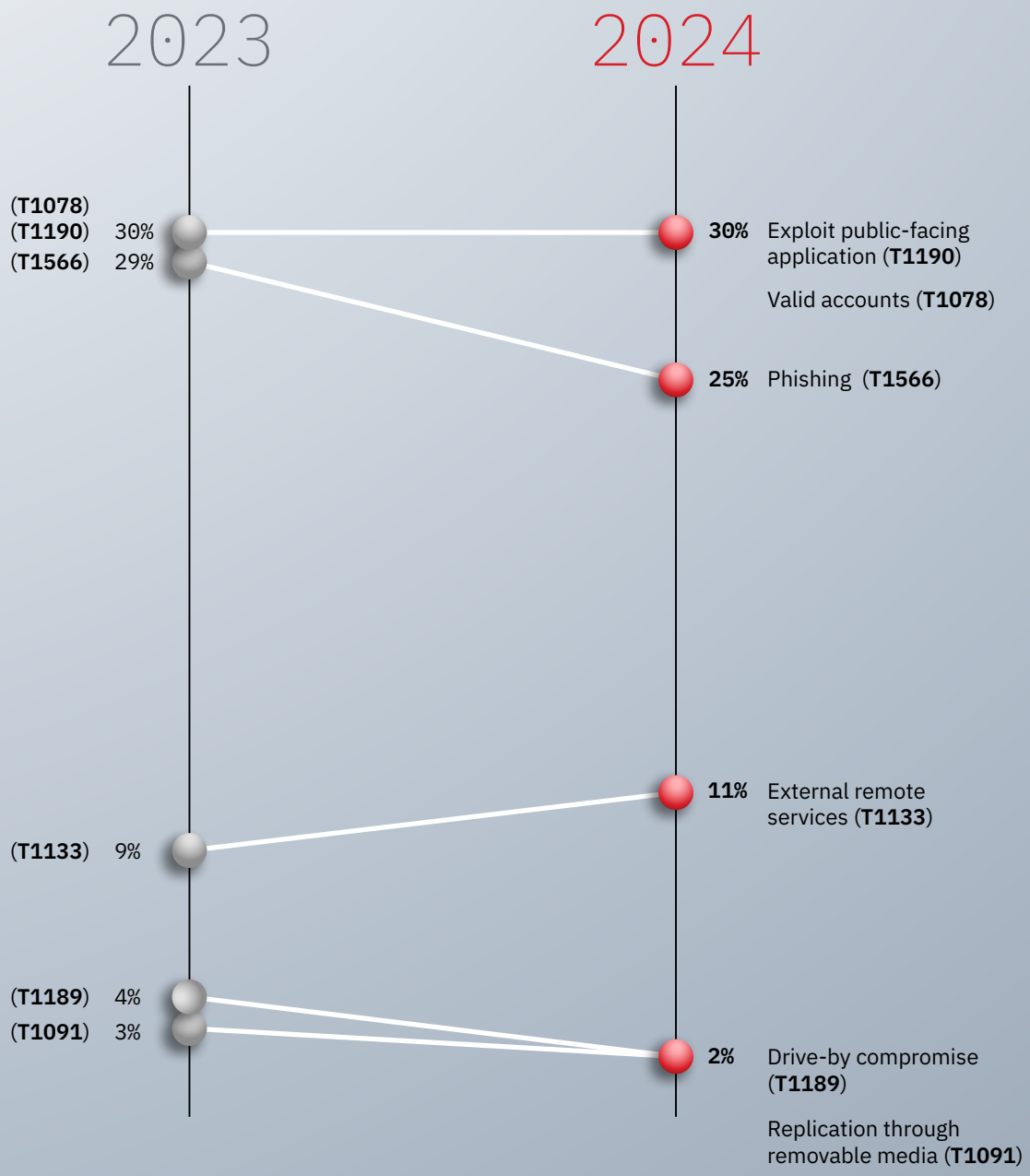
While multifactor identification (MFA) adoption has grown, we observed attackers selling adversary-in-the-middle (AITM) phishing kits and custom AITM attack services on the dark web to help bypass typical defensive measures. In 2024, X-Force specifically responded to cases involving this technique, globally and cross-industry. Widescale availability of credentials on the dark web, along with increased access to MFA codes and services to circumvent MFA, suggests a thriving access-as-a-service criminal market.

Phishing, whether through attachment or links, rounded out the top three compromises. The share of successful phishing compromises has declined steadily over the last several years from 46% in 2022 to 29% in 2023 to now just 25% of all incidents remediated by X-Force in 2024. Despite the development of some cybercriminals investing in AI to carry out phishing attacks, this method continues to be a less successful method for compromising environments than exploiting vulnerabilities or using valid credentials.

This is likely because enterprises continue to thwart phishing attempts—regardless of whether the phish used AI or not—by adopting and revaluating phishing mitigation techniques and strategies.

FIGURE 1

Top methods used by threat actors to gain access to victim environments



The figure describes access methods according to the MITRE ATT&CK framework for enterprise, a globally accessible knowledge base of adversary tactics drawn from real-world observations.[12] Percentages are based on number of X-Force incident response engagements.

Phishing as a shadow infection vector for valid account compromise

Compared to previous years, the volume of phishing emails distributing persistent backdoor malware has declined significantly. High-volume distributors of malware leading to ransomware attacks – including Emotet, TrickBot, IdedID, Qakbot, Gozi, and Pikabot – have largely dropped off the radar. Deploying persistent malware on an endpoint through an email is much more likely to be detected by endpoint detection and response (EDR) solutions, forcing threat actors to adapt strategies and focus on identities. This manifested in an increase in the use of infostealers and a shift towards credential phishing.

Infostealer bot frameworks enable attackers to design infostealer behaviors and create server-based management panels where infostealers send data. We observed a rise of 84% more infostealers delivered on average via phishing emails per week in 2024 versus 2023. Early data from 2025 suggests an even greater increase of 180% of weekly volume compared to 2023.

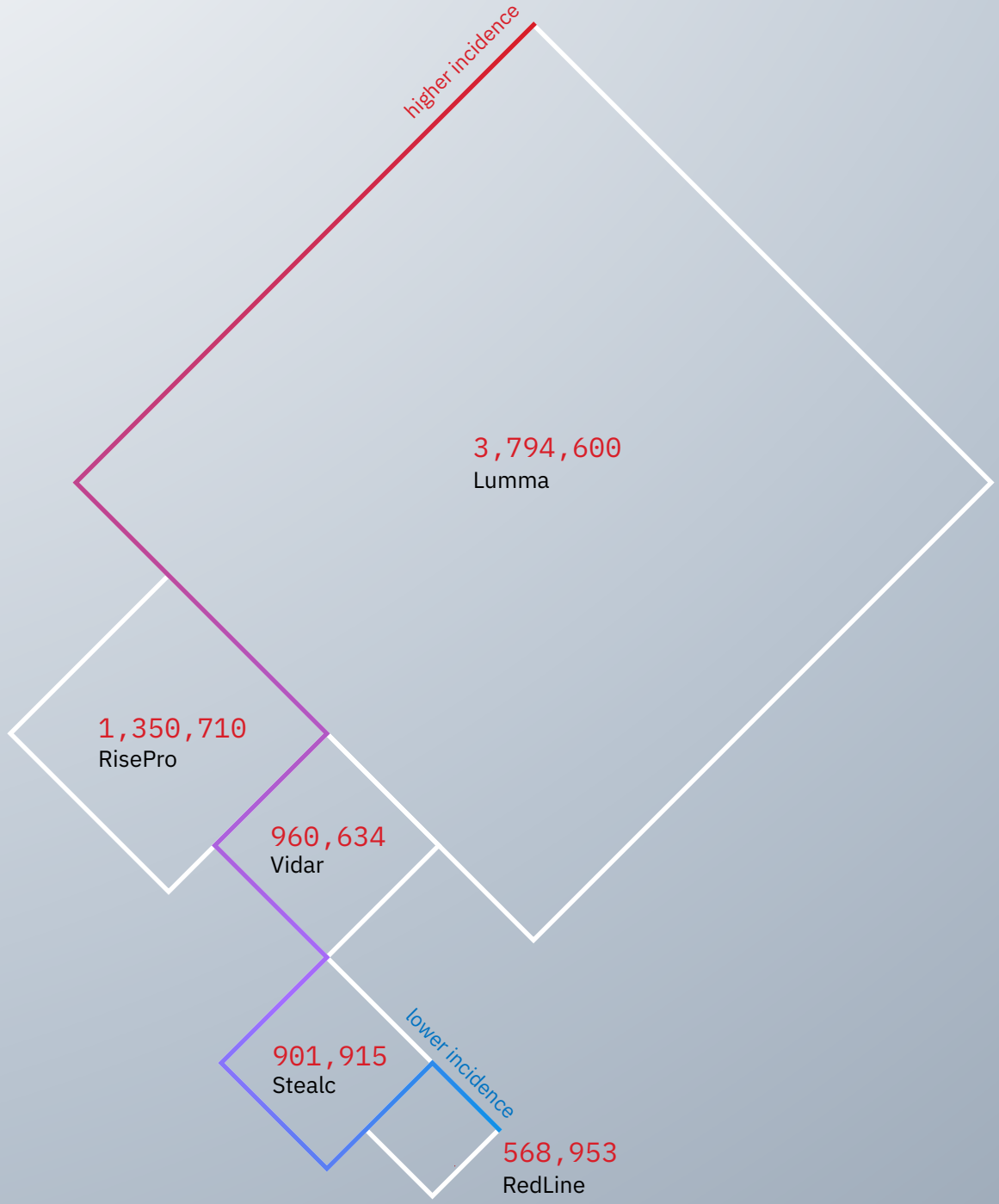
By using infostealers, threat actors can quickly exfiltrate credentials before detection without keeping a persistent backdoor as an initial foothold. The most common infostealer malware distributed directly via phishing was AgentTesla, followed by FormBook, SnakeKeylogger, and PureLogs Stealer.

We also observed an increase in Hive0145 email campaigns distributing the Strela Stealer infostealer. Hive0145 is an initial access broker focused on targeting victims throughout Europe with Strela Stealer malware. This infostealer has been in existence since at least 2022 and has always been purely focused on exfiltrating email credentials, leading to business email compromise. Since then, Hive0145 has experimented with several advanced techniques to improve campaign effectiveness.

Throughout 2024, we recorded a significant increase in volume, especially in the second half of the year. As of July 2024, this threat actor began using a new technique—dubbed attachment hijacking—to weaponize legitimate invoice-related emails which were previously stolen to further spread Strela Stealer.[13]

FIGURE 2

Top five infostealers seen on dark web forums



Analysis of dark web data reveals listings of infostealer advertisements increased 12% in 2024 over the previous year. The number one infostealer listing by a wide margin was Lumma, followed by RisePro, Vidar, Stealc and RedLine. Each listing can contain hundreds of credentials. Sources: IBM X-Force and Cybersixgill.

Additional infostealers analyzed in 2024 include well-established names such as Lumma, RisePro, Vidar, Stealc, Amadey, AgentTesla, AZORult, LokiBot, DanaBot, newer families such as Byakugan, FireStealer, ACR Stealer, DoomStealer, and WhiteSnake, and even MacOS targeted stealers such as MetaStealer and CloudChat.

The second change we observed in 2024 is an increase in credential phishing. Malicious URLs redirect victims to fake login sites for popular applications and harvest credentials.Both credential phishing and infostealer malware harvest active credentials for use in follow-on attacks.. For second-stage attacks, the vector is use of valid accounts, one of the most common initial access vectors during the last two years.

However, it is almost impossible to trace back to the origin of the compromised credentials. It is likely, that for many valid accounts incidents, the actual infection vector was a premeditated credential phishing or infostealer malware campaign, a fact that cannot be accurately reflected in the statistic of initial access vectors.

Although by the numbers it might seem like phishing risks are decreasing, it's just become more challenging to determine where the risk originated. Valid credentials still must be sourced from somewhere. While it can be difficult to prove, most compromised credentials came from infostealers and credential harvesting campaigns, of which an increasing amount is delivered via phishing.

Deploying persistent malware on an endpoint through an email is much more likely to be detected by EDR solutions, forcing threat actors to adapt strategies and focus on identities.

Infostealers, a persistent and growing threat

Infostealers are malicious software programs designed to steal valuable information. Attack vectors typically include phishing emails, malicious websites, or infected software downloads.

Increasingly, infostealers are distributed through techniques such as SEO poisoning and Google Ads, drive-by attacks, and software supply chain compromises.

Once installed, infostealers run in the background to take screenshots, capture keystrokes, access passwords, and compromise financial and personal information without user knowledge. They have also been frequently linked to more impactful attacks against enterprises by allowing attackers to gain access through stolen login credentials. Infostealers have long been a staple of the criminal marketplace, and many operate as a malware-as-a-service (MaaS) model.

Cloud-hosted phishing

In one of our most significant findings, our research reveals that over the past year, threat actors have shifted to using cloud hosting services to facilitate mass phishing campaigns. These campaigns have increased significantly in volume. The abuse of cloud hosting services often guarantees attackers a trusted URL, domain, and IP for use in their phishing campaigns—at least as long as the cloud hosting service fails to detect the abuse and act. For most providers, the sheer mass of abused accounts can be overwhelming. Adversaries require payloads to stay up only until victims click the link.

Latin America (LATAM) is one of the most severely impacted regions for phishing campaigns. Throughout 2024 threat actors have significantly ramped up the volume of LATAM-targeted campaigns abusing cloud hosting services.

These landscape changes make it much more difficult for defenders to prevent successful phishing attacks. Organizations cannot realistically block PDFs and URLs in emails because they are used everywhere across everyday operations. Furthermore, organizations cannot block legitimate cloud hosting services.

The only way to help avoid this is using time-sensitive threat intelligence tools to block URLs flagged as malicious and by relying on layered defenses to reduce impact if users take the phishing email bait. This means using endpoint detection and response (EDR) to detect info-stealing malware and using passkeys and MFA to reduce the risk of credential harvesting campaigns. The LATAM region is especially targeted and should remain vigilant against phishing campaigns. An effective way to counter the scale of these attacks is through the use of AI tools and automation.

What is cloud-hosted malware?

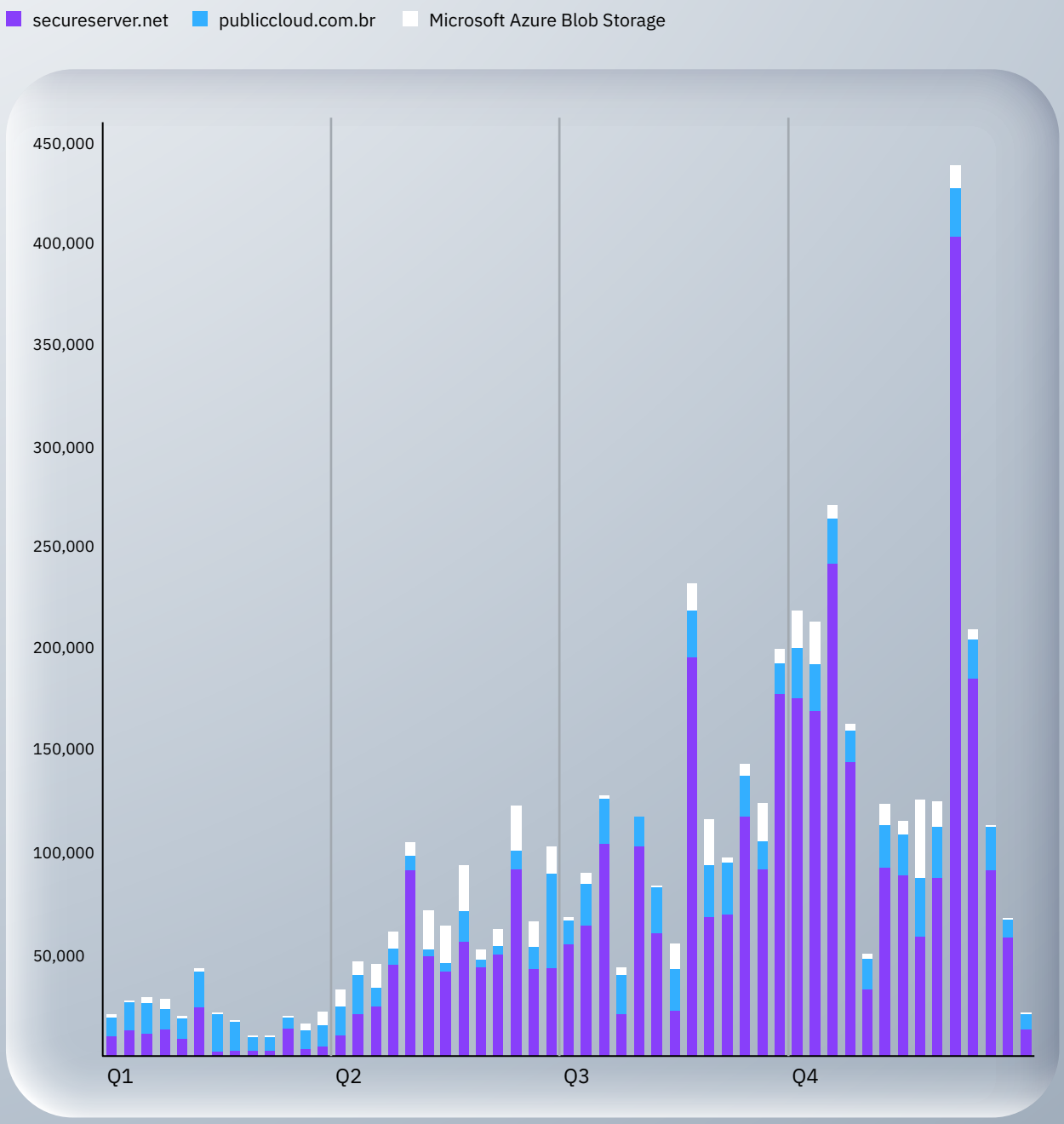
Cloud-hosted malware refers to malicious software, including worms, trojans, ransomware, or infostealers that use cloud services for hosting, distribution and/or command and control operations.

Attackers use malware hosting services to house and distribute malware and support browser exploits and drive-by downloads to infiltrate vulnerable computers.

Cloud-hosted malware attacks have proliferated because of increased reliance on cloud services, the inherent vulnerabilities of cloud estates, and the ease of distribution and persistence enabled by cloud infrastructure. Although cloud environments provide security features, they can be exploited when not properly configured, when vulnerabilities are not patched, or when policies are not updated.

FIGURE 3

Incidence of spam and malware hosted on major public cloud environments



Number of observed spam email messages with links to a given cloud hosting provider. Threat actors seek to mask malicious activity by using popular cloud hosting services. The cloud hosting services secureserver.net (purple), publiccloud.com.br belonging to Locaweb Serviços de Internet (blue) and Microsoft Azure Blob Storage (white) have been abused heavily as a means to distribute credential phishing sites and banking trojan malware such as Grandoreiro, Mekotio and Guildma. NOTE: The use of a specific cloud provider for hosting malicious content is not indicative of a security flaw in the platform but illustrates where attackers choose to stage malware. Often, attackers choose well-known and established providers as a way to fool victims by hiding nefarious activities amongst other legitimate workloads, making those activities harder to identify and isolate. Source: IBM X-Force.

PDFs and URLs taking over malware spam

In 2024, we observed a clear decrease in direct malware attachments such as ZIP archives or maldocs in phishing emails. Malicious ZIP and RAR attachments dropped by 70% and 45% respectively, with a similar drop observed for Excel and Word documents.[14] Malware is increasingly distributed via malicious URLs, both directly in phishing emails and through PDF attachments. This may be a result of better malware scanners in email solutions, which have become more accurate at detecting malware, but often cannot classify URLs or URLs inside benign attachments as malicious.

Obfuscation is becoming an important tactic for threat actors, and PDF malware disguises malicious URLs by encrypting them, hiding them in compressed streams or using hexadecimal representations which can also hinder automated analysis of email security solutions. Of all PDFs, 42% used obfuscated URLs, 28% hid their URLs in PDF streams, and 7% were delivered in an encrypted form along with a password.

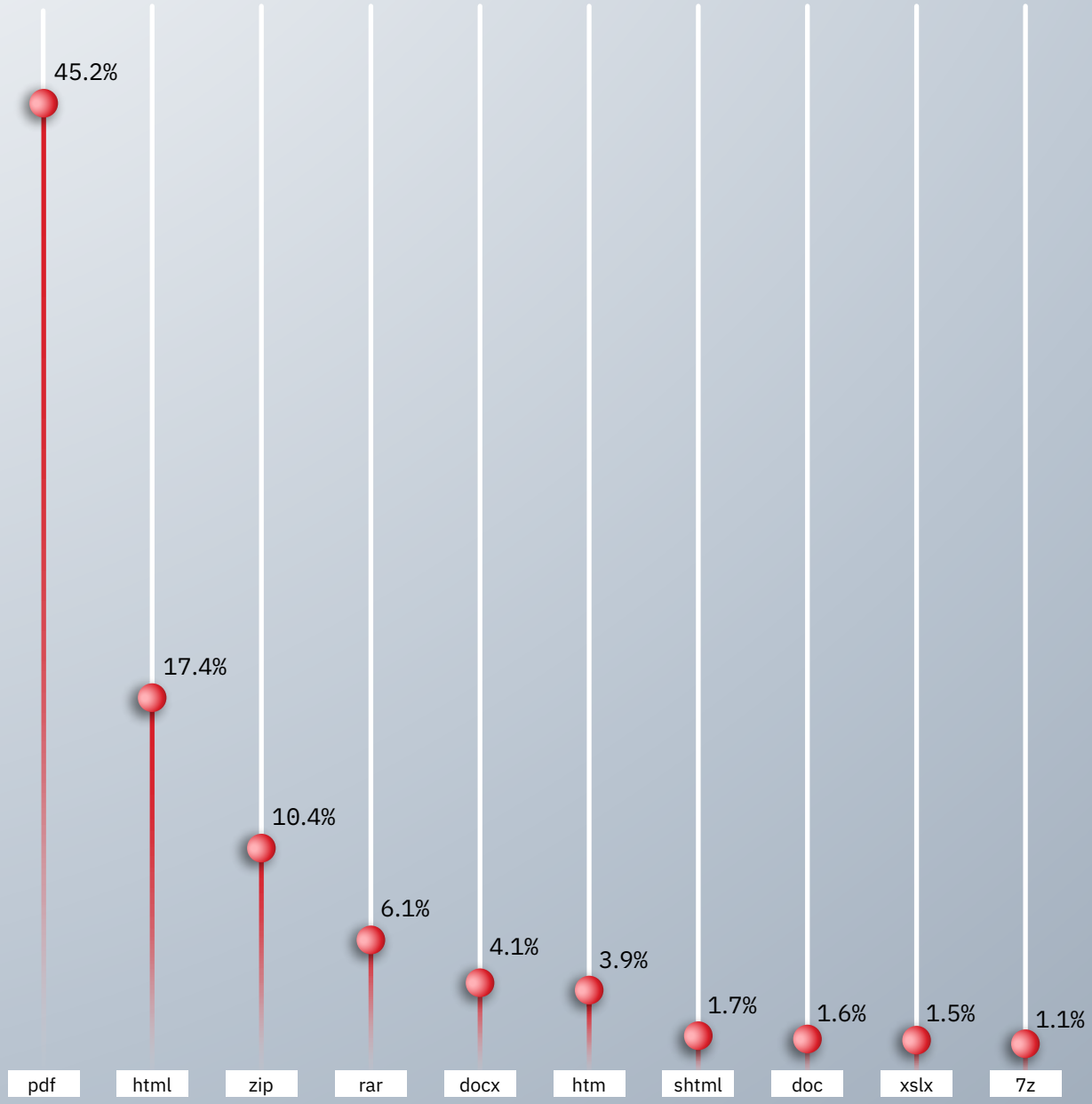
Several threat actors were observed using PDFs to deliver malware through malicious URLs, including Hive0118 and Hive0137. These are ex-ITG23 affiliated distributors, which used PDFs with embedded links in several campaigns in the first half of 2024 to deliver malware and AITM links.[15] These distributors have started experimenting with new attachment types such as PDFs with obfuscated URLs, documents with embedded URLs and others to load a wide arsenal of malware including Pikabot, DarkGate, NetSupport, T34-Loader and Warmcookie.

In 2024, PDF files were also commonly used in LATAM-targeted phishing campaigns to deliver links leading to banking trojan malware.

Obfuscation is becoming an important tactic and PDF malware disguises malicious URLs by encrypting them, hiding them in compressed streams, or using hexadecimal representations to hinder automated analysis.

FIGURE 4

PDFs rank as the top malicious attachment file type



PDFs are a common file format, with a complex structure that makes it easier for threat actors to hide malicious code. They are a popular choice for attackers to deliver malware via email and other means because many potential victims use PDFs frequently and may not be as suspicious of PDF attachments. Source: IBM X-Force.

The success of vulnerability exploitation

30% of the incidents X-Force responded to in 2024 involved the exploitation of public-facing applications. For many organizations, this is magnified by vulnerability patch management challenges. Furthermore, in 25% of these cases, we observed active scanning post-compromise—meaning attackers used vulnerability scanning tools to identify additional vulnerabilities, gain additional access, and move laterally in the compromised environment.

Threat actors exploit known vulnerabilities in common applications and infrastructure services and the attack vector is simply a matter of acting on this knowledge. Bots and automation tools acquired on the dark web can target an organization's key infrastructure applications and services.

Unfortunately for cyber defenders, there is no shortage of vulnerabilities to exploit. Since 1993, we have categorized over 300,000 unique vulnerabilities. Included are nearly 65,000 vulnerabilities with a publicly available exploit, many of which attackers have used to compromise environments. In other words, nearly a quarter of all vulnerabilities have an associated weaponized exploit that can be leveraged by threat actors.

Also, of note, the number of vulnerabilities has increased rapidly over the past eight years and grown threefold. This could be attributed to many factors. Perhaps the most likely is a growing reliance on shared cloud infrastructure and services. Attacking common cloud infrastructure is a prized opportunity for threat actors to deploy malware at scale and expand their potential for disruption. This is another compelling reason why zero trust principles, such as network segmentation, are essential for cyberdefenders. By isolating workloads, we limit the potential blast radius of attacks.

What are common vulnerabilities and exposures (CVEs), weaponized exploits, and zero days?

The CVE system provides a unique way to identify publicly known cybersecurity vulnerabilities and exposures occurring in software, hardware, and other digital systems.

It allows organizations to track security issues effectively and share knowledge, enabling security teams to refer to the same vulnerability in a consistent manner, even across different systems.

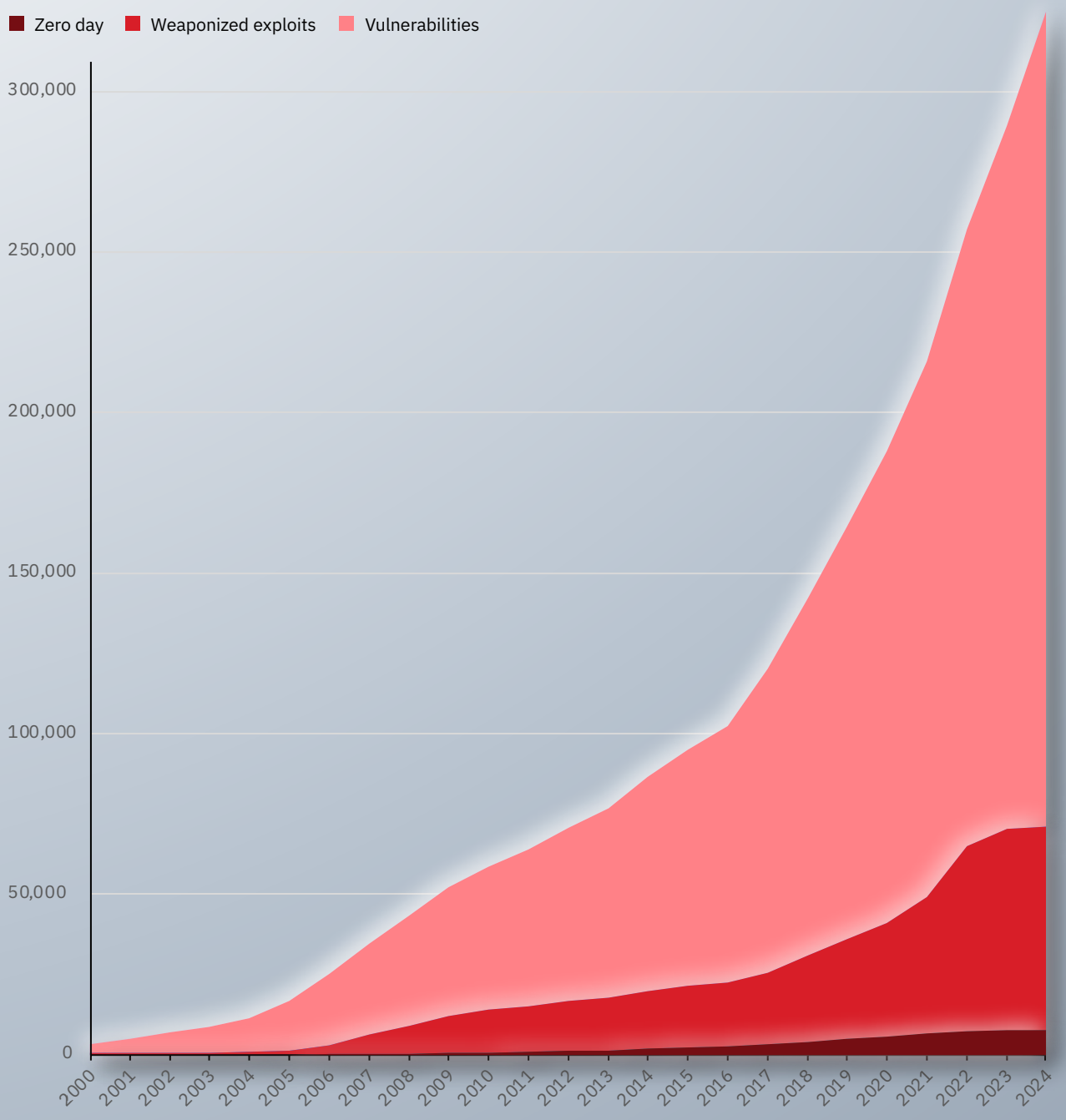
MITRE Corporation maintains a publicly listed catalog of CVEs, and the CVE list feeds the US National Vulnerability Database (NVD) which quickly enriches each CVE once it has been published.

In addition to pooling intelligence about common vulnerabilities and threat vectors, organizations also benefit from sector and industry-specific resources such as information sharing and analysis centers (ISACs). Typically managed by non-profit organizations, ISACs help critical infrastructure operators protect facilities, employees, and customers from cyber and physical security threats.

Weaponized exploits, often involving malicious payloads or malware, are attack tools used by threat actors to exploit vulnerabilities and target specific systems.

FIGURE 5

Growth of vulnerabilities, exploits, and zero days



The growth of vulnerabilities, exploits and zero days since 2000. The IBM X-Force Vulnerability Database is one of the oldest and largest vulnerability databases in the world. Source: IBM X-Force.

Vulnerabilities and the dark web

In collaboration with Cybersixgill, X-Force has reviewed the 10 most mentioned common vulnerabilities and exposures (CVEs) on the dark web. These include mentions from numerous dark web marketplaces. According to our research, out of hundreds of vulnerabilities, the top three mentioned CVEs in 2024 were:

1

CVE-2024-21762 (27%)—Fortinet FortiOS could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write flaw in a secure sockets layer virtual private network (SSNVPN). By sending specially crafted HTTP requests, an attacker could exploit this vulnerability to execute arbitrary code or commands on the system.

2

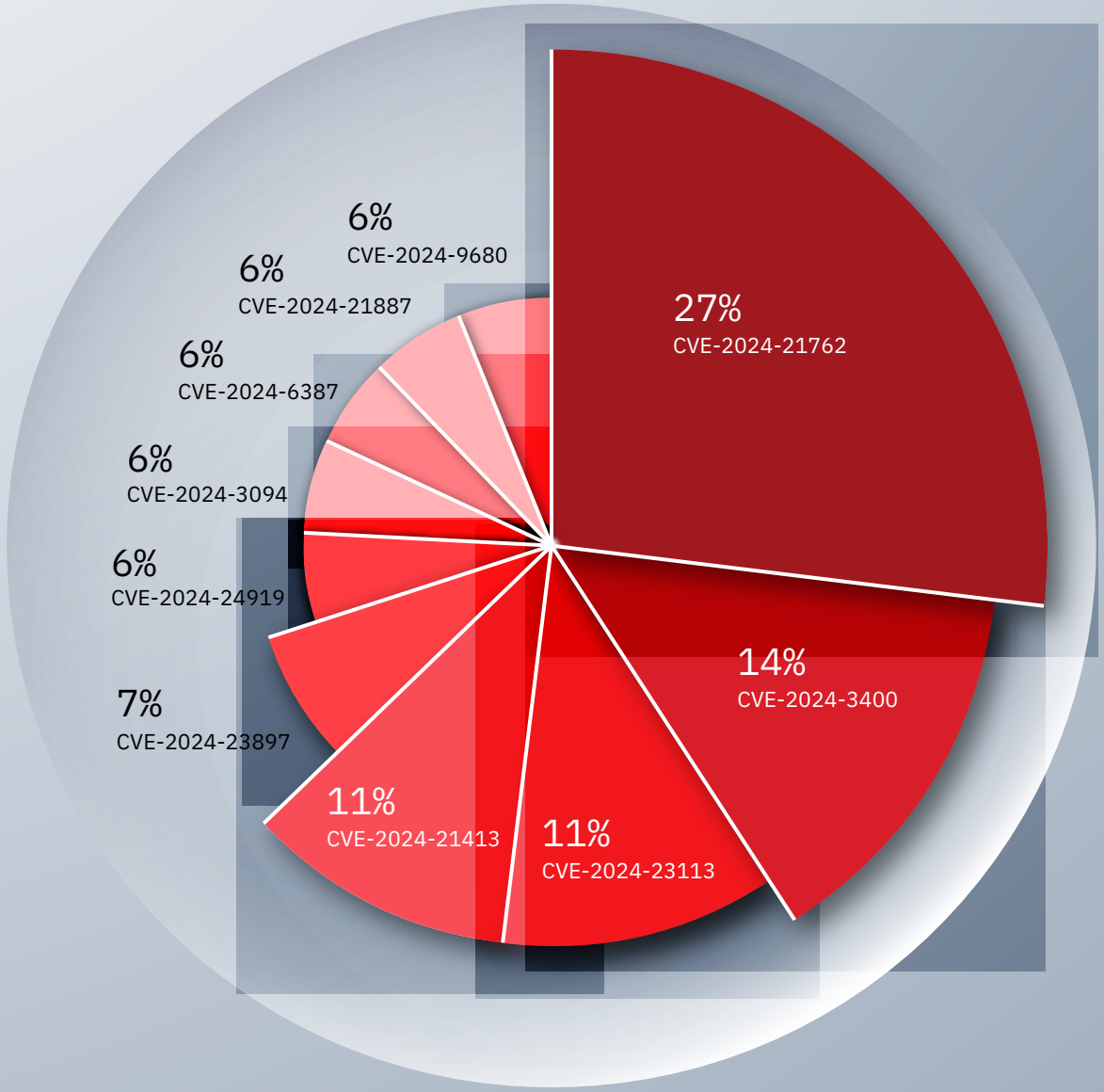
CVE-2024-3400 (14%)— Palo Alto Networks PAN-OS could allow a remote attacker to execute arbitrary command on the system, caused by a command injection vulnerability in the GlobalProtect feature. An attacker could exploit this vulnerability to inject and execute arbitrary code on the system with root privileges.

3

CVE-2024-23113 (11%)—Fortinet FortiOS could allow remote attackers to execute arbitrary code on systems, by using an externally controlled format string in the fgfmd daemon. By sending specially crafted requests, an attacker could exploit this vulnerability to execute arbitrary code or commands.

FIGURE 6

Top 10 CVEs discussed on dark web forums



Shown as a percentage of the top 10 CVEs discussed on the dark web. Sources: IBM X-Force and Cybersixgill.

All top 10 vulnerabilities had publicly available exploit code or were found being actively exploited in the wild last year. 60% of these vulnerabilities had a public exploit available less than two weeks after disclosure—including several zero day vulnerabilities. Remote code execution is possible with eight of these vulnerabilities. The remaining two allow for an attacker to obtain sensitive information.

Apart from CVE-2024-9680, a remote code execution vulnerability affecting Mozilla Firefox, all top 10 CVEs were disclosed in the first half of 2024. And readers should understand that the disclosure date of a vulnerability plays a factor in terms of placement in the top 10, as earlier disclosure means more time for dark web discussions. The fact that these specific vulnerabilities have been discussed most suggests a strong interest by threat actors in exploiting them. Given that many other vulnerabilities discussed and disclosed earlier in the year didn't make the top 10, we think there's more to these vulnerabilities that makes them worthy of further attention.

Several of these CVEs have been linked to sophisticated threat actor groups, including nation-state actors:

CVE-2024-24919

A vulnerability in Check Point Security Gateway could allow a remote attacker to obtain sensitive information. This issue has been linked to several APT groups, including UNC2452, APT29, Royal, BITWISE SPIDER, and Akira.[16]

CVE-2024-23897

A vulnerability in Jenkins weekly and Jenkins LTS could allow a remote attacker to obtain sensitive information. The threat actor, Intelbroker, leveraged this vulnerability to conduct a supply chain attack.[18]

CVE-2024-3400

A zero-day vulnerability in Palo Alto Networks PAN-OS could allow a remote attacker to execute arbitrary commands on vulnerable system. UTA0218, potentially a China-based threat actor, was observed exploiting this vulnerability.[17]

CVE-2024-9680

A vulnerability in Mozilla Firefox could allow a remote attacker to execute arbitrary code on a vulnerable system. The Russia-aligned APT group known as RomCom was observed exploiting this vulnerability.

Four of the top 10 vulnerabilities impacting networking appliances include Fortinet FortiOS (CVE-2024-21762, CVE-2024-23113), Check Point Security Gateway (CVE-2024-24919) and Ivanti Connect Secure and Ivanti Policy Secure Gateways (CVE-2024-21887).•In February 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory about Volt Typhoon, a China-based APT actor that has compromised the IT environments of multiple US-based critical infrastructure organizations. The advisory notes this APT is gathering intelligence about US critical infrastructure and pre-positioning themselves to enable lateral movement to OT (Operational Technology) assets to disrupt functions in communications, energy, transportation systems, water and wastewater systems. CISA further notes this APT actor typically gains initial access by exploiting vulnerabilities in public-facing network appliances.

Knowing the most discussed CVEs on the dark web can inform defenders on which vulnerabilities require prioritized patching. In addition, threat intelligence teams should actively search the dark web for sensitive code that has been exfiltrated, which less sophisticated threat groups can quickly weaponize to target those organizations.

A screenshot of a dark web posting (see Figure 7) highlights the availability of exploit codes for two network appliance vulnerabilities (CVE-2024-24919, CVE-2024-21762) and two other vulnerabilities in the top 10 (CVE-2024-21413, CVE-2024-3400).

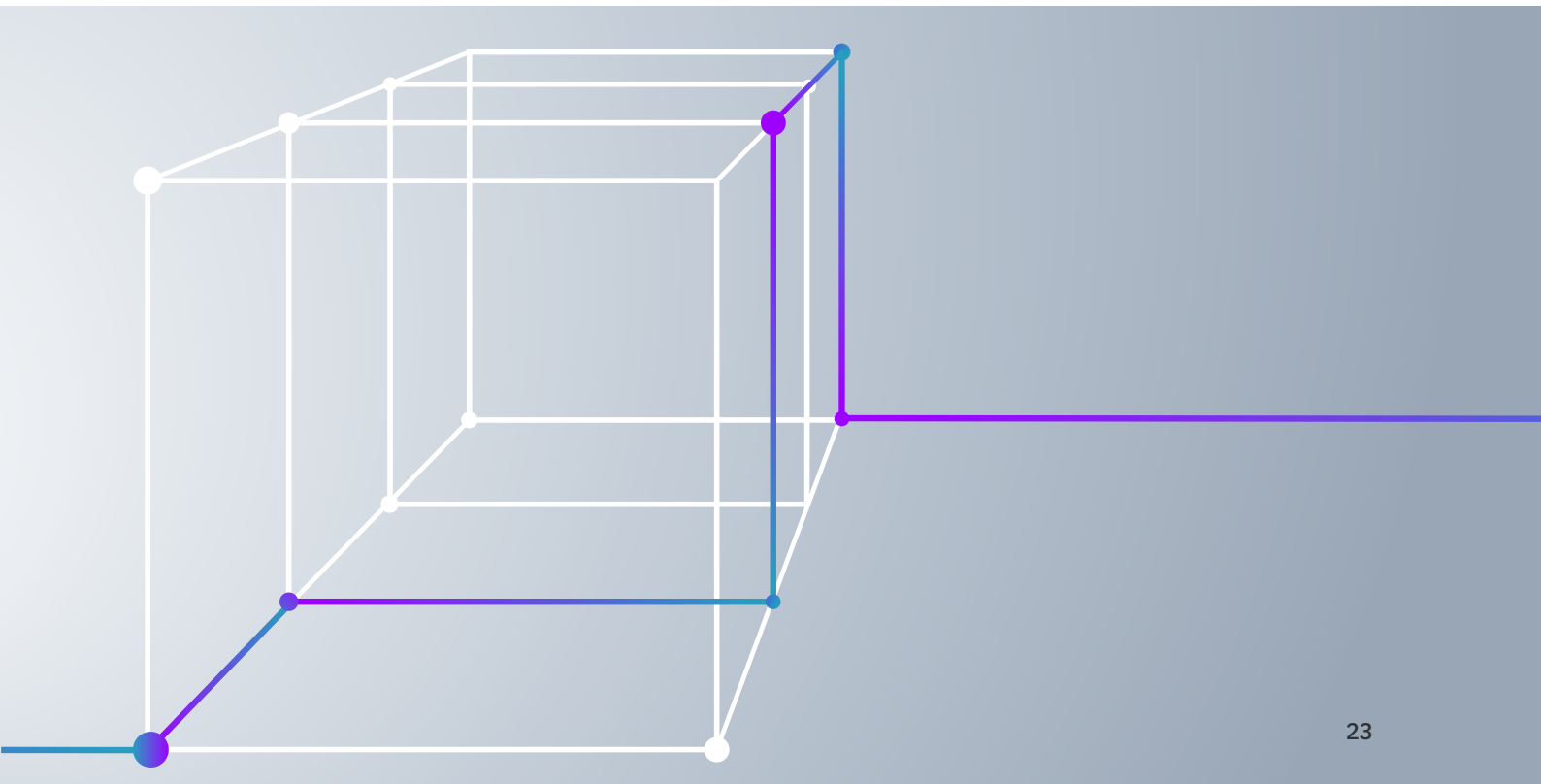
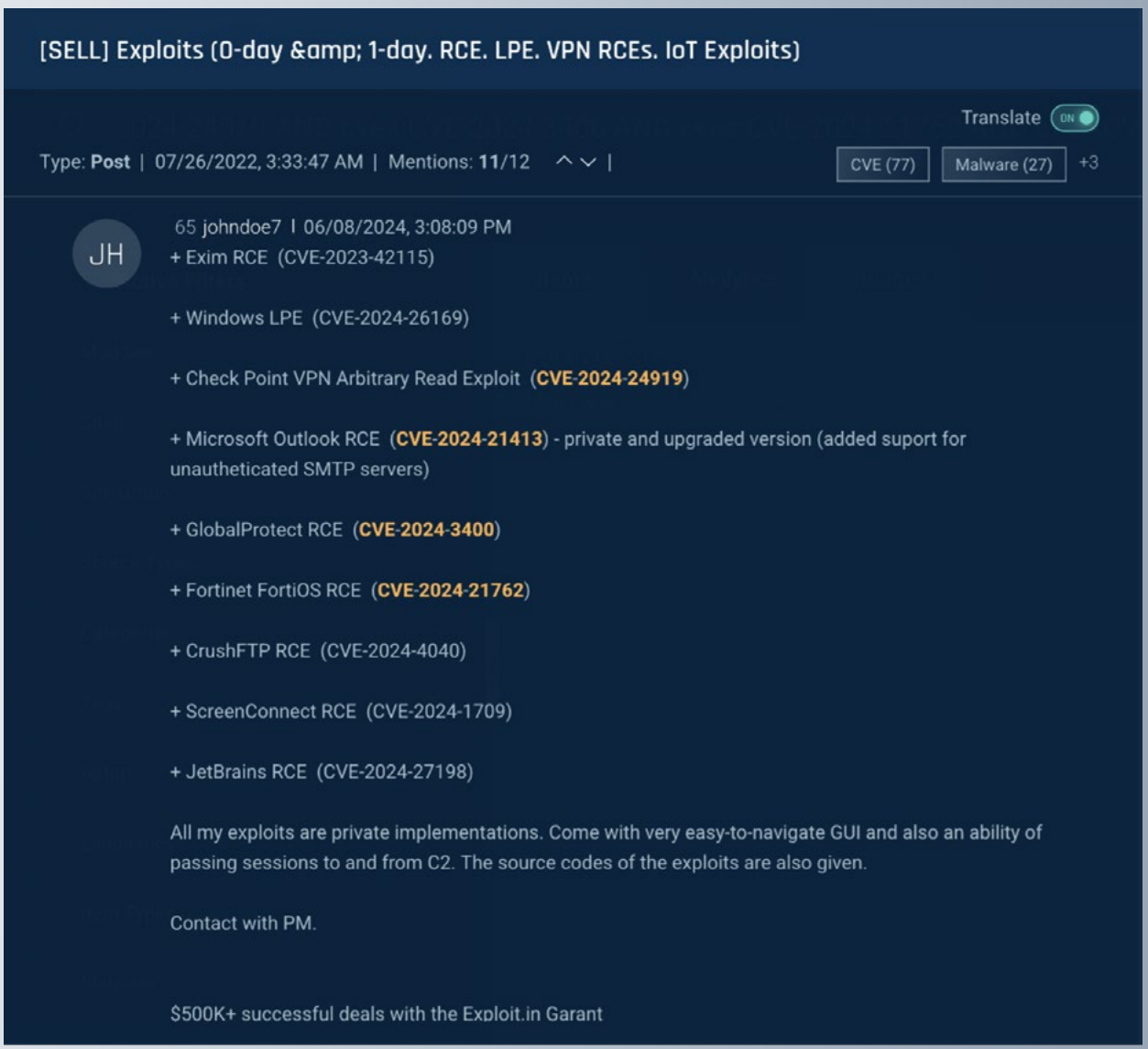


FIGURE 7

Dark web posting advertising exploits for sale



A screenshot of a dark web posting highlights the availability of exploit codes for two network appliance vulnerabilities (CVE-2024-24919, CVE-2024-21762) and two other vulnerabilities in the top 10 (CVE-2024-21413, CVE-2024-3400). Source: Cybersixgill.

Cybercrime marketplaces

The dark web and cybercrime-as-a-service

The dark web is a cloistered area of the internet that can only be reached by using specialized software that allows users to visit websites anonymously. Although it can be used legitimately by journalists, whistleblowers, and researchers to communicate without being tracked, the dark web is also commonly used by criminals involved with drugs and arms trafficking, stolen data, and other illegal activities. This is the marketplace where threat actors buy and sell cybercrime as a service (CaaS) software.

Mimicking software-as-a-service business models, CaaS transforms hacking into a subscription service available to threat actors around the world. CaaS provides hacking tools for criminals to launch distributed denial of service (DDoS) phishing, malware, spyware, credential stuffing, and an ever-expanding range of other cybercrime attacks and activities.[20]

Mimicking software-as-a-service business models, cybercrime as a service (CaaS) software transforms hacking into a subscription service available to threat actors worldwide.

Red Hat Enterprise Linux vulnerabilities

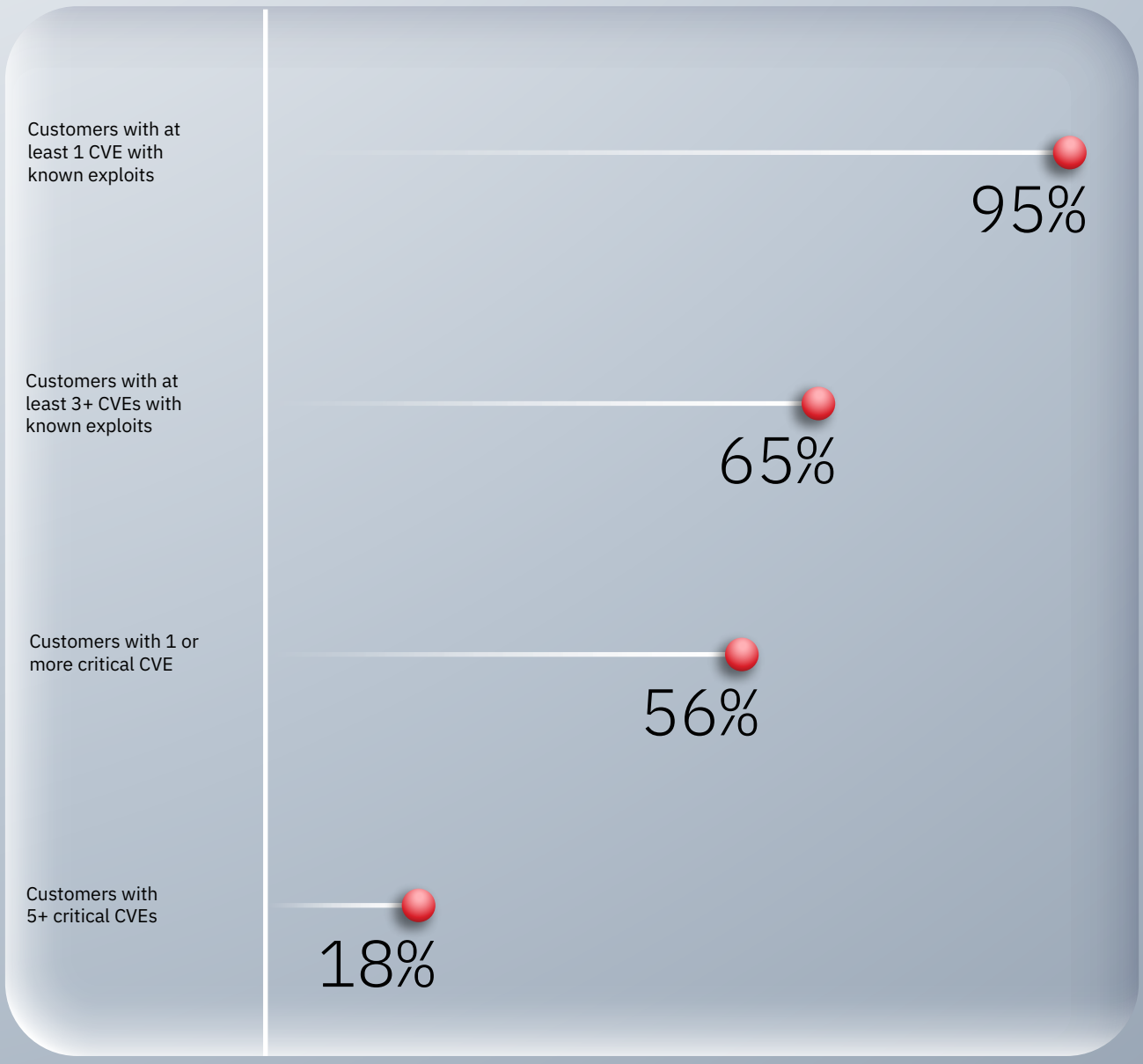
Securing enterprise Linux environments is critical because they host essential applications, databases, and services. Linux use cases include web server, application development, cloud container, and virtualization frameworks.

In collaboration with Red Hat Insights, X-Force found that 95% of Red Hat Enterprise Linux customers were vulnerable to at least one CVE with a publicly available exploit. Additionally, 65% had at least three CVEs with known exploits. While this data is representative of Red Hat Enterprise Linux environments, it provides an indication of what many organizations are likely facing in terms of exposure to vulnerability exploitation.

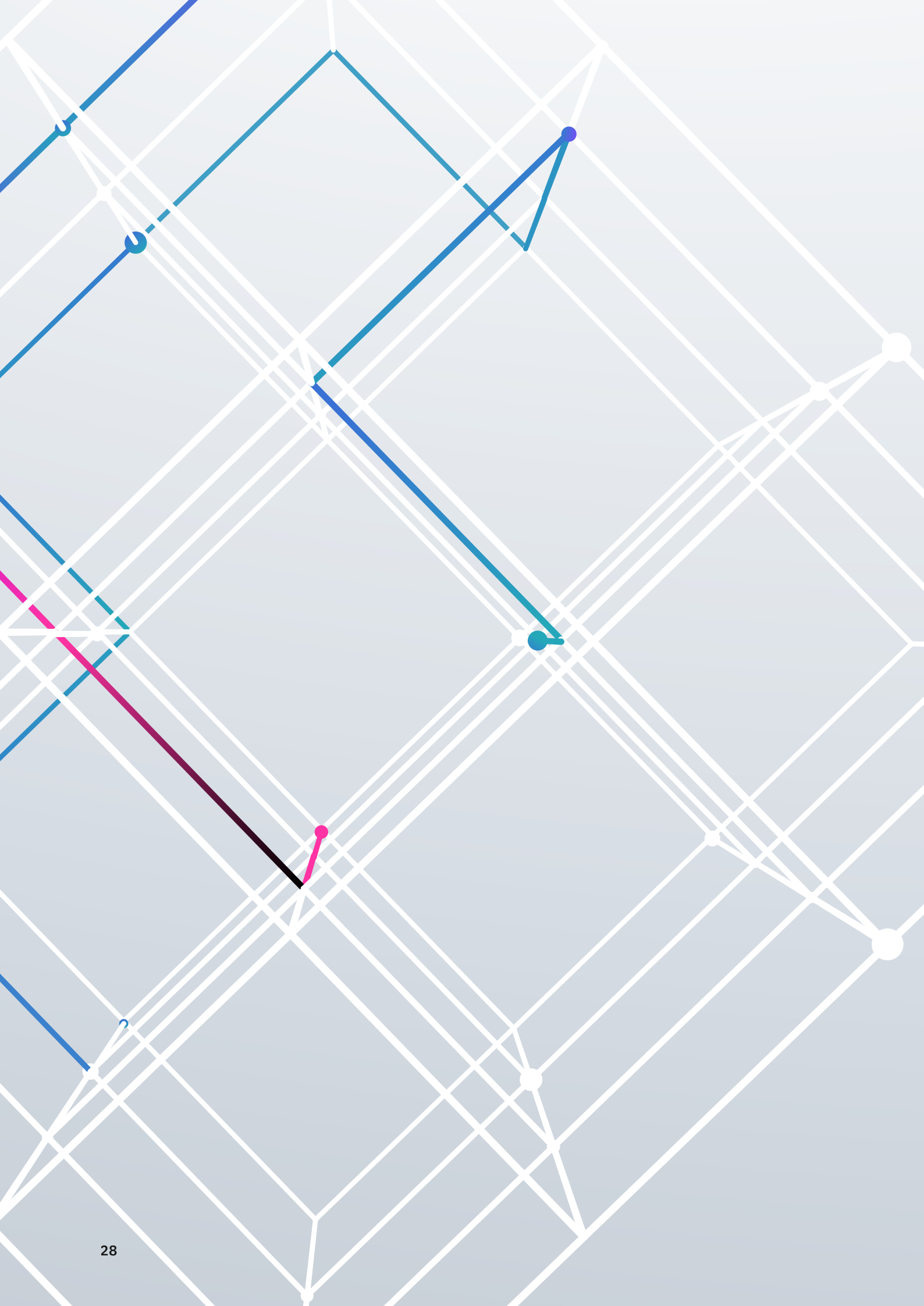
Furthermore, more than half of Red Hat Enterprise Linux customers' environments had at least one critical CVE unaddressed. Even more concerning, 18% of organizations faced five or more vulnerabilities, meaning that nearly one in five organizations are operating with five or more CVEs.

FIGURE 8

Linux client environments with critical CVEs or CVEs with known exploits



Source: Red Hat Insights.



Top actions on objectives

Actions on objectives are steps or activities taken to achieve a defined objective or goal. In a cybersecurity context, these measurable and actionable steps are part of a larger plan directly linked to threat actor objectives.

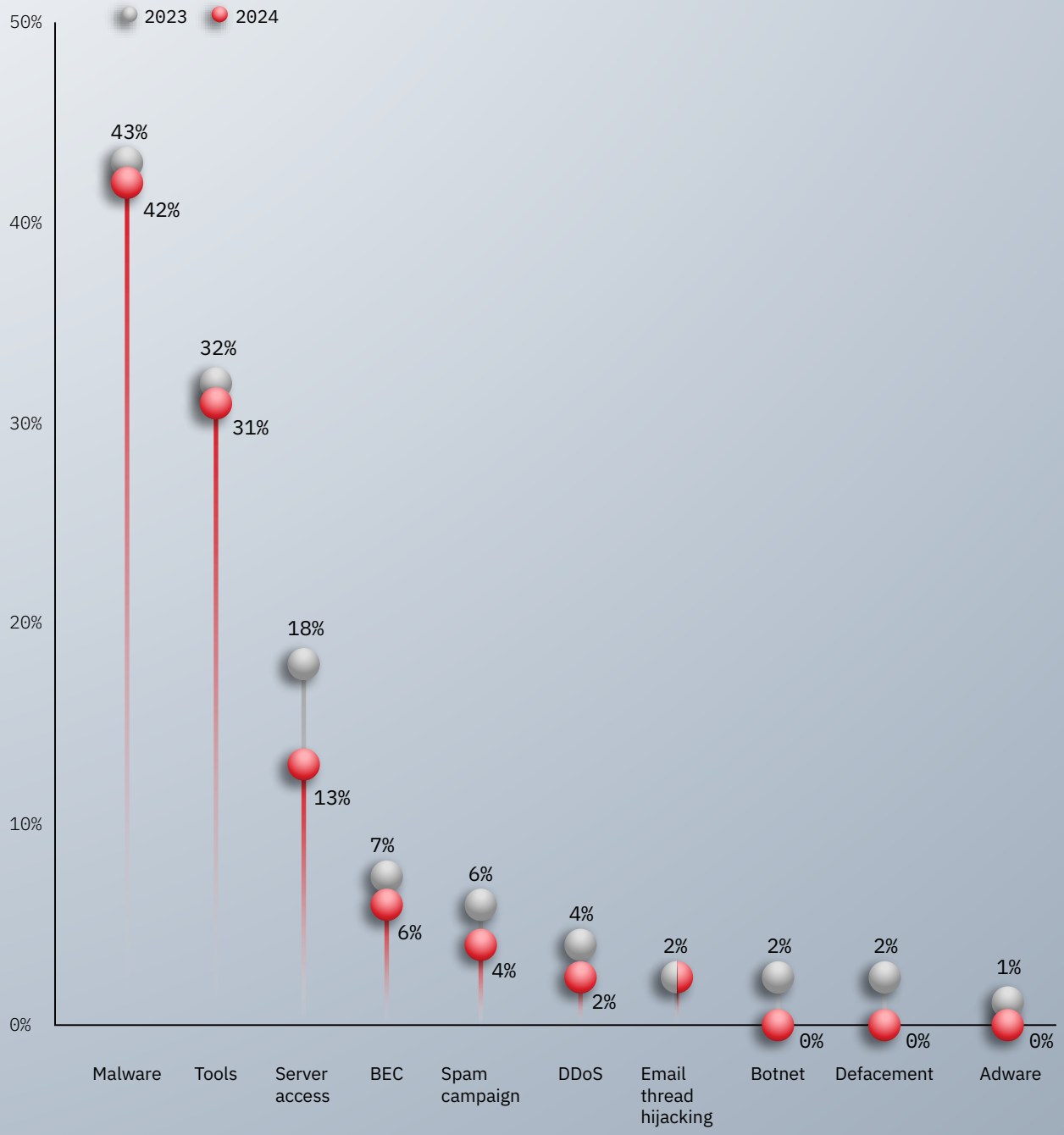
According to X-Force incident response data, the deployment of malware was the most observed action on objectives, making up 42% of cases, just slightly less than the prior year. Of all the malware cases, 28% involved ransomware, followed by backdoors and webshells, at 20% and 13% respectively.and webshells at 20% and 13% respectively.

"Businesses need to shift away from an ad-hoc prevention mindset and focus on proactive measures such as modernizing authentication management, plugging multi-factor authentication holes and conducting real-time threat hunting to uncover hidden threats before they expose sensitive data."

Mark Hughes,
Global Managing Partner for Cybersecurity Services, IBM

FIGURE 9

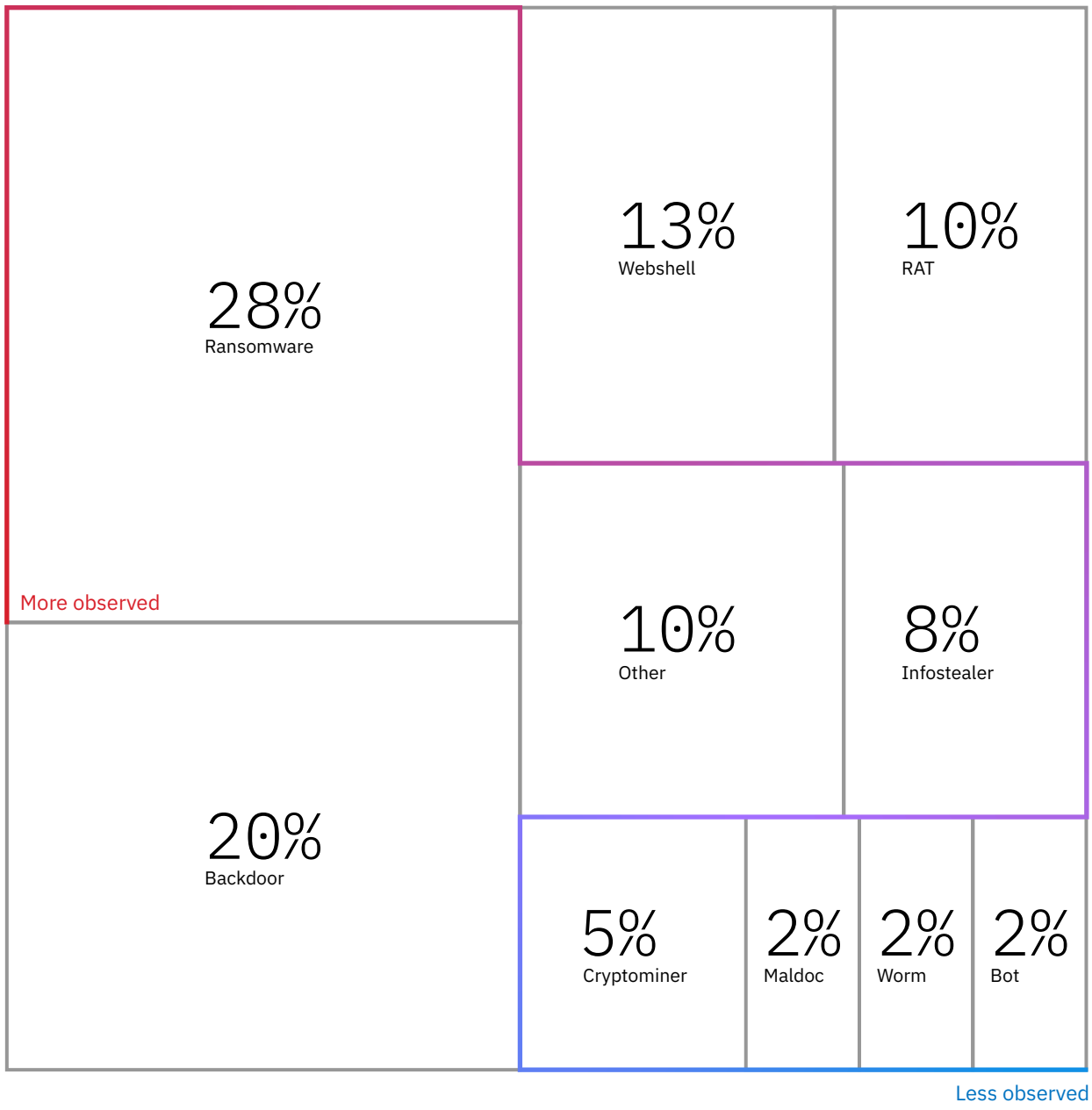
Top actions on objectives observed in 2024 compared to 2023



Incidents can have more than one observed action on objective. Source: IBM X-Force.

FIGURE 10

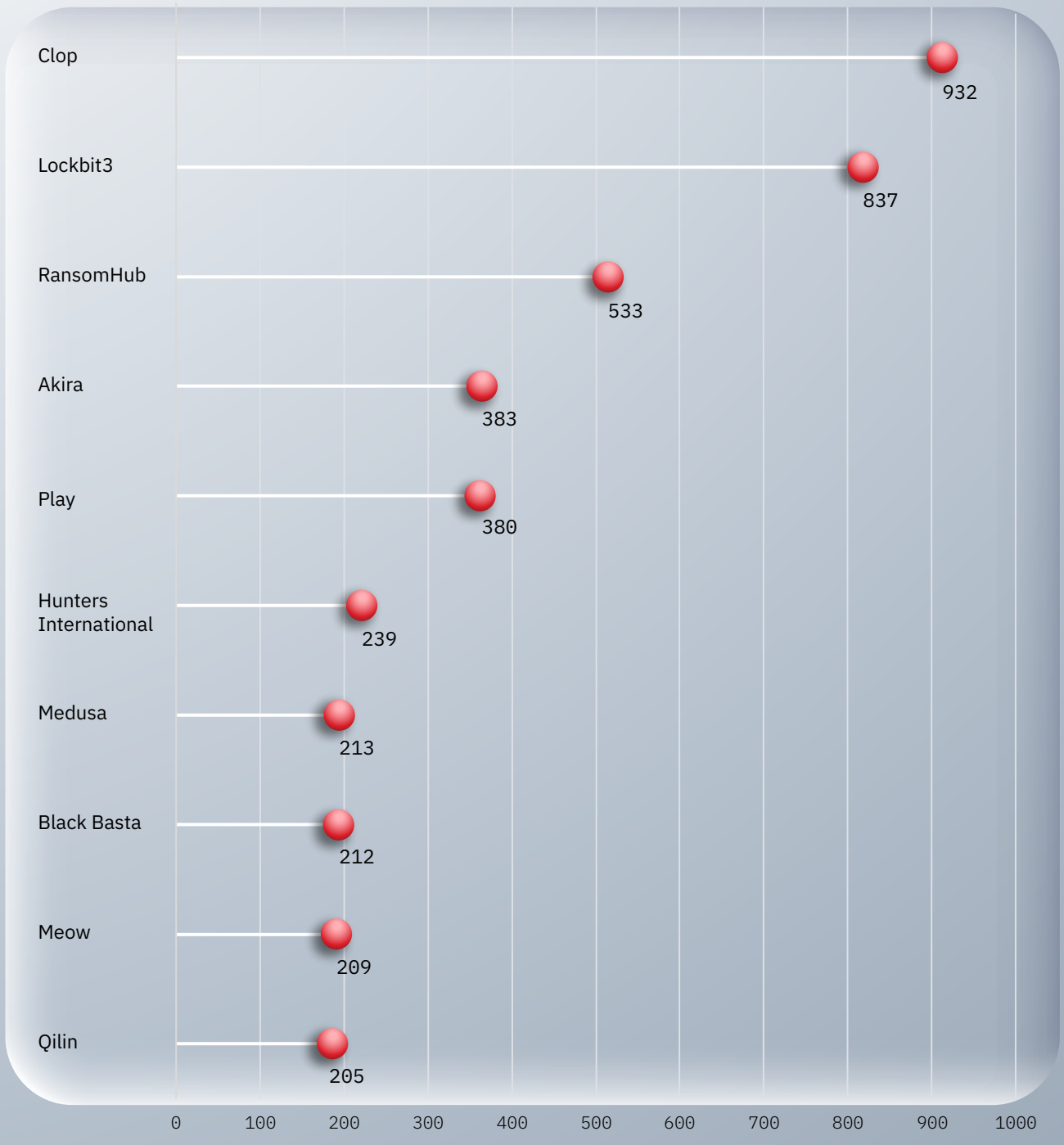
Distribution of types of malware cases as a percentage of total malware incidents



Source: IBM X-Force.

FIGURE 11

Top ransomware by volume of dark web events



A ransomware event on the dark web is defined as a claim made by a threat actor group that an organization has been impacted by ransomware."Sources: IBM X-Force and Cybersixgill.

Ransomware landscape

Our review of data from the dark web—combined with telemetry data, incident response case documentation, and malware analysis—suggests that Akira, LockBit, Black Basta, RansomHub, and Hunters International were among the most active ransomware families over the past year. In 2024, the most discussed ransomware events were associated with CLOP, followed by LockBit 3.0 and RansomHub (see Figure 11). A ransomware event on the dark web is when a threat actor group claims an organization has been impacted by ransomware.

For the past several years, we have reported that ransomware groups were increasingly creating Linux versions of their ransomware exploits in addition to targeting Windows environments. This now appears to be the norm, with all ransomware groups listed above adopting a cross-platform approach and supporting both Windows and Linux, and occasionally additional platforms such as ESXi hypervisors and FreeBSD. There are also reports of ransomware groups increasingly using the bring-your-own-vulnerable-driver (BYOVD) technique to escalate privileges and terminate processes such as EDR.

However, despite the larger share of ransomware cases relative to other types of malware, and a 25% increase in ransomware events on the dark web, we have observed an overall decline in ransomware incident response engagements for a third year in a row.

This could be attributed to several factors. One reason for this decline is that high-volume distributors of malware—which often precipitate ransomware attacks—have been on the decline. Another reason is that over the past few years international law enforcement agencies have been increasingly collaborating to take down the infrastructure of prominent botnets which have often been the gateway to ransomware attacks.

The impact of takedowns on the malware landscape

In August 2023, a multinational takedown operation significantly disrupted the Qakbot botnet linked to follow-on ransomware attacks from groups such as Black Basta, Conti, and REvil.[21] Qakbot briefly returned in December 2023, but their recovery was short-lived, and the malware disappeared again in January 2024.

In May 2024, a Europol-led coalition of international law enforcement agencies formed the “Operation Endgame” task force to identify, investigate, and take down prominent cybercrime groups. On May 30, 2024, Operation Endgame announced that they had taken down networks and infrastructure relating to IcedID, SystemBC, Pikabot, Pikabot, Bumblebee, and TrickBot.[22] The takedown included over 100 servers and 2,000 domains linked to malicious activity, as well as arrests and asset seizures.

As a result of these takedowns, we have seen increased diversification and turnover in the malware activity of actors associated with cybercrime groups such as ITG23, (Wizard Spider, TrickBot Group), ITG25 (Lunar Spider, IcedID), and ITG26 (Qakbot, Pikabot). Previously well-established malware families linked to these groups are no longer operational and we have seen threat actors turn to other malware, including new and short-lived families, as cybercrime groups attempt to replace botnets that were taken down.

PikaBot, considered to be Qakbot's replacement, has not been observed since Operation Endgame, and Bumblebee took several months to recover, only returning in October 2024. The IcedID malware also appears to have been retired and replaced by IceNova (aka Latrodectus), which managed to make it through the takedowns relatively unscathed, with activity picking back up in June 2024 and continuing throughout the rest of the year.[23]

Malware crypters

Crypter software is used by cybercriminals to disguise malware so it can slip through security programs. X-Force tracks many malware crypters linked to ITG23-affiliated actors, which provide insights into the malware used by these groups and their relationships with other actors.[24]

Over the past year we have observed these crypters—which were historically and predominantly used to deploy malware such as Qakbot, IcedID, TrickBot, Bumblebee, and Pikabot—used with an increasingly diverse range of payloads. These include backdoors such as Broomstick (aka Oyster), IceNova (aka Latrodectus), DarkGate, Brute Ratel, Cobalt Strike, WarmCookie, and SSLoad, infostealers such as ACR Stealer, LummaC2, Rhadamanthys, Stealc, RisePro, DoomStealer, and FireStealer, and ransomware including Black Basta, BlackSuit, INC, and Rhysida.

SystemBC is a well-known proxy malware which has been in use since 2018 and is often used by ransomware groups such as BlackBasta, LockBit, and Rhysida. However, we have also seen several new families over the past couple of years, suggesting that this type of malware may be increasing in popularity. These include:

GhostSocks, a Golang-based proxy malware, advertised on Russian underground forums since the end of 2023.

PortStarter, a Golang-based proxy malware, predominantly used by VanillaTempest, a group known for deploying ransomware such as Rhysida and INC.

Supper, a proxy malware/backdoor written in C++, linked to the Vanilla Tempest group and also reportedly observed in an Interlock ransomware incident.

Crypter software is used by cybercriminals to disguise malware so it can slip through security programs.

Proxy malware and obfuscation tactics

We have observed an increase in proxy malware, which is malware with the ability to operate as a Socks5 proxy and forward requests between a C2 (Command and Control) server and target systems."

Threat actors may install proxy malware to act as a backdoor to a target network, disguise network traffic,or act as part of a proxy service botnet.[25]

Threat actors' ability to obfuscate—or operate in the shadows—is the real danger. Increasing use of obfuscation tactics is a consequence of threat actors' desire to leverage widely available cloud infrastructure and services, and complicate mitigation efforts by making workload inspection and validation activities more costly and expertise-intensive.

Malware payloads delivered via SEO poisoning and malvertising

A common infection vector used by threat actors is to hide malware within fake or trojanized installers of legitimate applications. Users are then tricked into downloading and running malicious installers via techniques such as phishing, SEO poisoning, and malvertising. SEO poisoning uses search algorithms to promote malicious web pages, and malvertising directs users to bogus websites where their data can be stolen.

These tactics play a significant part in the chain of compromise by spoofing legitimate websites, thereby obtaining valid credentials that enable simple log in (i.e. avoiding the need to hack in).

In early 2024, we observed Hive0133, an initial access broker and email distributor that overlaps with the group TA544, delivering PDFs containing malicious links which led to the download of ZIP files, hosted on Discord, containing trojanized versions of the Notepad++ application. One of the application's dynamic link libraries (DLLs) was replaced with a malicious version containing the WailingCrab malware which would be executed via DLL sideloading upon execution of the legitimate Notepad++ executable.

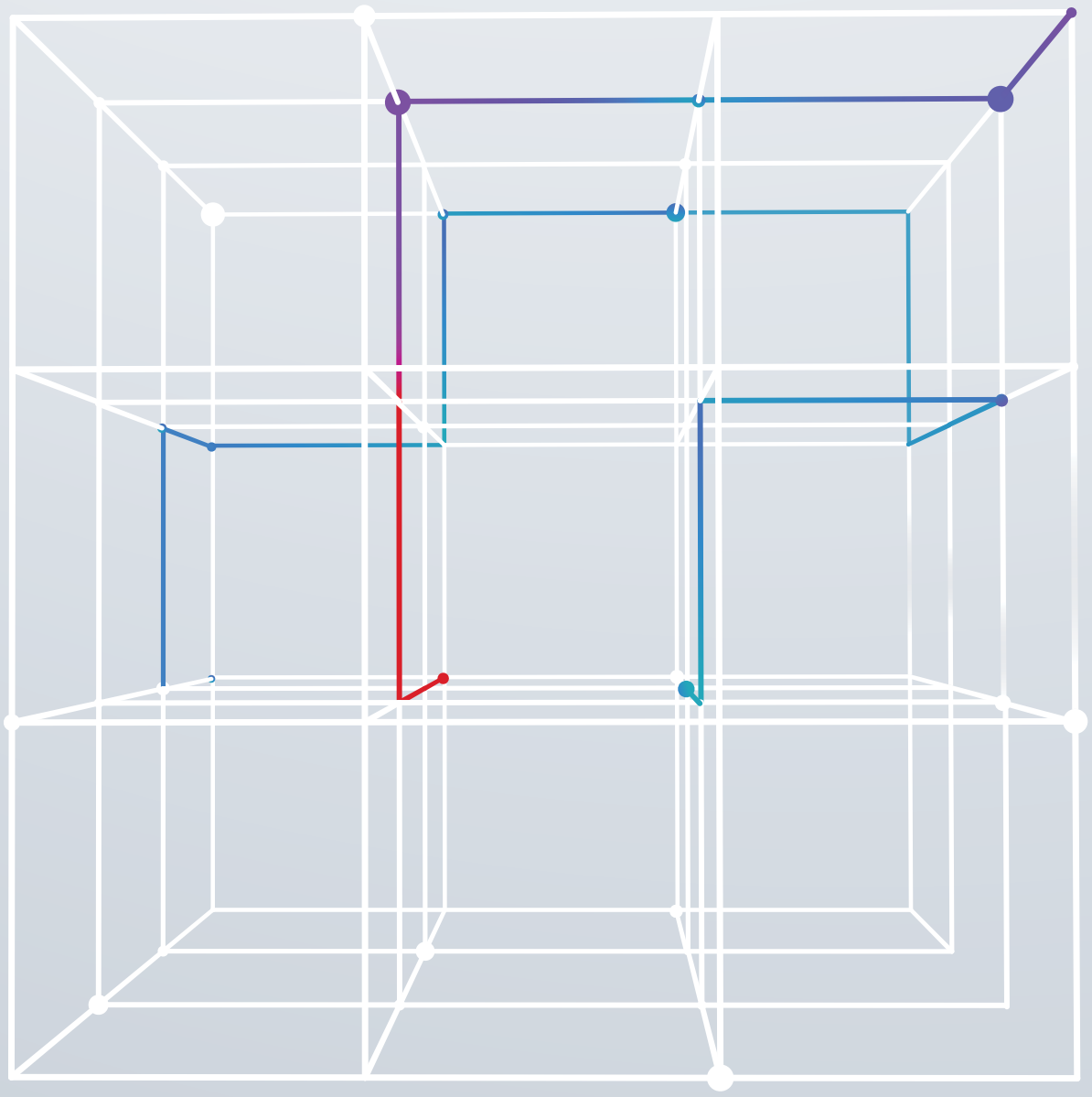
In mid-2024 we observed Hive0118—an initial access broker and email spammer known for delivering Qakbot and Pikabot malware—use trojanized MSIX and APPX installers of popular applications such as Google Chrome, AnyDesk, and Microsoft Teams to deliver FakeBat downloader scripts.

We have also observed similar techniques from Latin America-based threat actor groups. Throughout 2024, X-Force observed the Byakugan infostealer being distributed to users throughout Latin America, specifically Brazil, with Portuguese-language phishing emails. The phishing emails encouraged users to download a fake Adobe Reader installer which would then install the Byakugan malware.

Since June 2023, and throughout the first half of 2024, there were several prominent Nitrogen malvertising campaigns, which impersonated legitimate websites for popular tools such as Putty, FileZilla, and AdvancedIPScanner, and leveraged Google and Bing pay-per-click (PPC) advertisements to trick victims into downloading malicious installer files. This led to the installation of malware such as Cobalt Strike and BlackCat ransomware.

In one incident, a Google search resulted in a user downloading a trojanized version of the Angry IP Scanner tool, which led to the installation of SharpRhino malware, linked to the Hunters International ransomware group.

Credentials are valuable because they open the door to additional access vectors and offer attackers additional options such as extortion, data theft and data leak.



Top impacts on victim organizations

In 2024, the top impact experienced by victim organizations was credential harvesting, occurring in 29% of incidents.

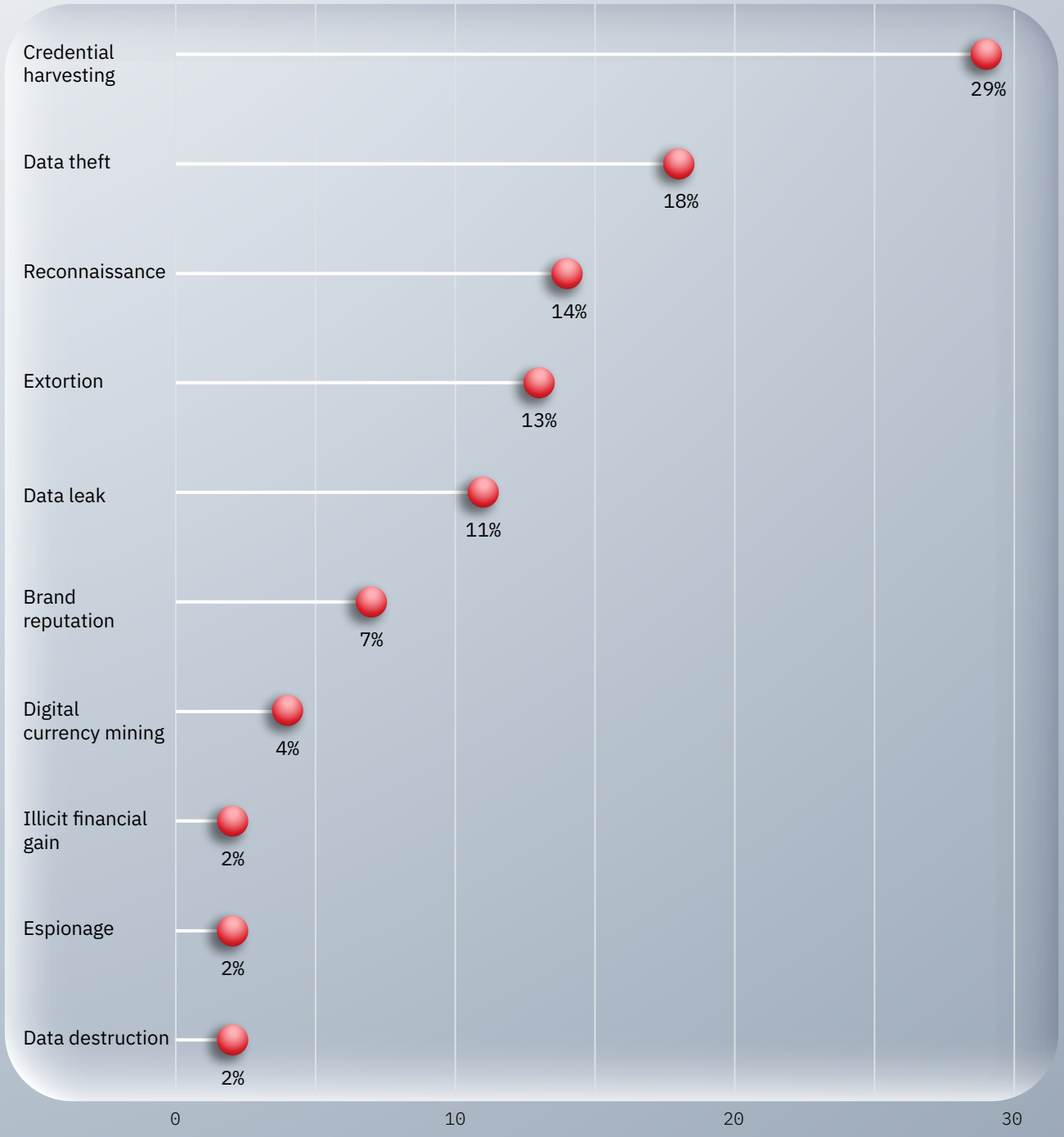
Credentials are valuable because they open the door to additional access vectors and offer attackers additional options such as extortion, data theft and data leak. Often, attackers leverage stolen credentials to burrow inside a victim environment, making detection and remediation more difficult.

Data theft was the second most observed impact and was seen in 18% of incidents. In fact, credentials or data were stolen in nearly half of all cyberattacks, highlighting a growing challenge in securing both data and identities.

The theft of data is often, but not always, accompanied by a subsequent ransom demand. Extortion following a ransom demand occurred in 13% of cases, taking the fourth spot. Threat actors extort victims in many ways. Traditionally, ransomware has been used to encrypt systems and urge victims to pay for decryption keys. More recently, however, threat actors have extorted victims without using ransomware. In these cases, stolen data is often used to pressure victims into paying for retrieval.

FIGURE 12

Top impacts observed in incident response engagements (2024)



Incidents can have more than one impact observed. Source: IBM X-Force.

Geographic trends

All geographic trend findings are compiled from X-Force research, telemetry data, and findings from incident response engagements.

#1

Asia-Pacific – 34%

The APAC region experienced the most attacks in 2024, accounting for 34% of all incidents investigated. Attackers frequently employed malware-ransomware (22%), recon/scanning tools (11%), and server access (11%) as their primary actions on objective. The extensive reliance on external remote services (45%) and the exploitation of public-facing applications (18%) as initial access vectors underscored vulnerabilities in APAC's digital infrastructure. Initial access vectors are the means used by attackers to gain a foothold in a network.

For the APAC region, key impacts—the intended or realized effect of an action on the victim—included data theft (12%), credential harvesting (10%), and extortion (10%). These reflect the sector's susceptibility to attacks targeting sensitive data and operational disruption. The manufacturing sector remained the most targeted industry, representing 40% of incidents, followed by finance and insurance (16%) and transportation (11%).

Japan was the most targeted APAC country, with 66% of all incidents investigated. The Philippines, Indonesia, Korea, and Thailand each represented 5% of cases.

#2

North America – 24%

The North America region was second in terms of incidents investigated, accounting for 24% of incidents in 2024. The most common actions on objective included tool-remote access (17%), malware-backdoor (17%), and server access (13%), signaling attackers' focus on system control and data exfiltration. The primary initial access vector was exploitation of public-facing applications (40%), followed by exploitation of valid accounts-cloud (27%).

The credential harvesting (40%) impact dominated incidents in the region, followed by data theft (30%) and espionage, extortion, and brand reputation damage (10% each). The manufacturing sector was the most targeted, representing 24% of all incidents investigated, while finance and insurance (20%) and professional, business, and consumer services (20%) also faced significant threats.

The United States was the most targeted country in North America representing 86% of incidents, with Canada at 14%.

#3

Europe – 24%

Europe ranked as the third most targeted region in 2024, accounting for 24% of incidents. Server access (15%), tool-credential acquisition (12%), and malware- ransomware (9%) were the most common actions observed, with attackers leveraging exploitation of public-facing applications (36%) as the leading initial access vector.

Credential harvesting (46%) was the dominant impact, followed by data leak (31%) and data theft (15%), showcasing the attackers' focus on monetizing sensitive information. The professional, business, and consumer services sector led with 38% of incidents, followed by finance and insurance (18%) and manufacturing (18%).

The United Kingdom was the most targeted country in Europe with 25% of incidents, followed by Germany (18%) and Austria (14%).

#4

Middle East – 10%

The Middle East and Africa region accounted for 10% of global incidents in 2024, maintaining its position as the fourth most targeted region. Attackers predominantly employed malware-infostealer (50%) and recon/scanning tools (50%), reflecting a focus on gathering sensitive data and identifying exploitable vulnerabilities.

The leading initial access vector was phishing-spearphishing attachments (67%), underscoring the continued reliance on social engineering to compromise systems.

Exploitation of public-facing applications (33%) also played a significant role, highlighting vulnerabilities in exposed infrastructure across the region.

The finance and insurance sector remained the most targeted industry, representing 61% of incidents, reflecting the region's growing financial landscape and associated risks. Other targeted industries included energy (17%), professional, business, and consumer services (11%), transportation (6%), and media (6%).

Saudi Arabia was the most targeted in this region making up 63% of incidents. The United Arab Emirates saw 16% of incidents.

#5

Latin America – 8%

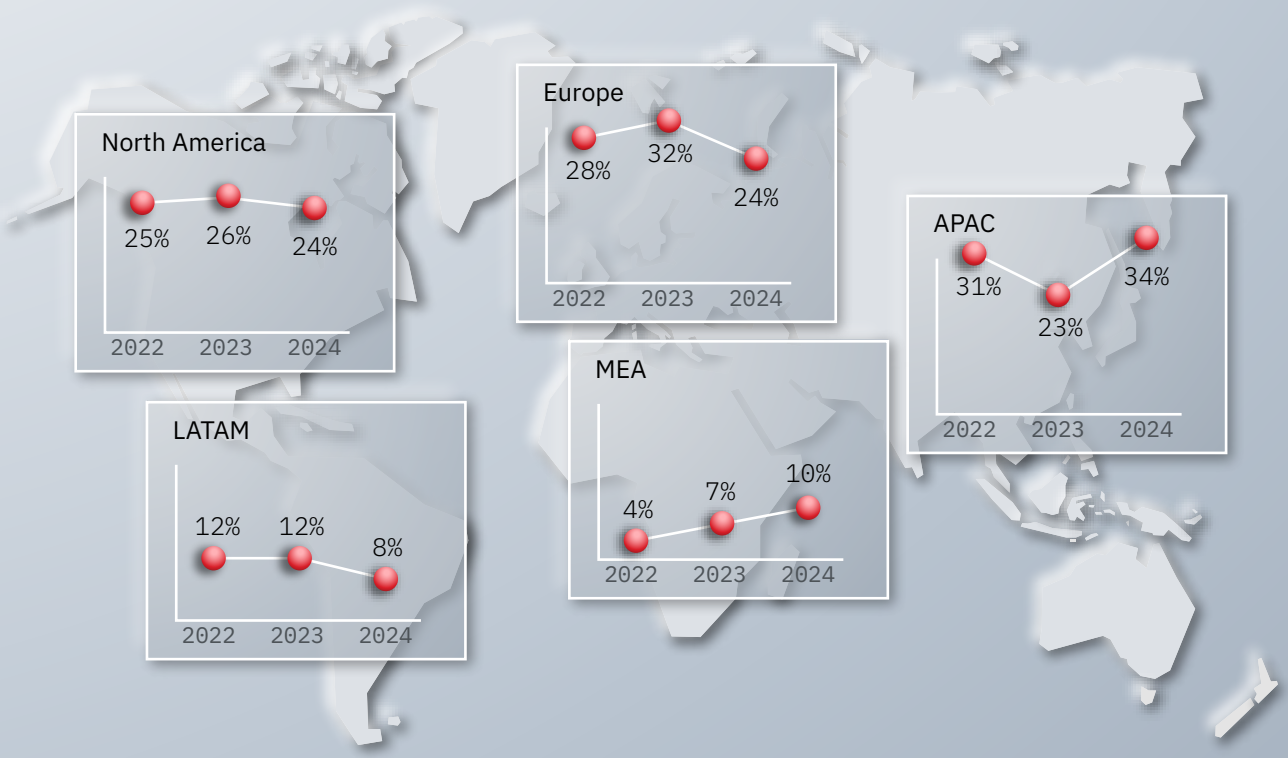
Latin America (LATAM) accounted for 8% of incidents in 2024, with targeted campaigns focused on critical infrastructure and financial systems continuity. Attackers frequently used exploitation of public-facing applications (50%) as the primary initial access vector, followed by phishing-spearphishing attachments (25%) and valid accounts-domain (25%).

The leading impacts were credential harvesting (40%) and extortion (40%), with brand reputation damage (20%) also observed. The finance and insurance sector led with 33% of incidents—followed by manufacturing (20%); energy (20%); and professional, business, and consumer services (13%).

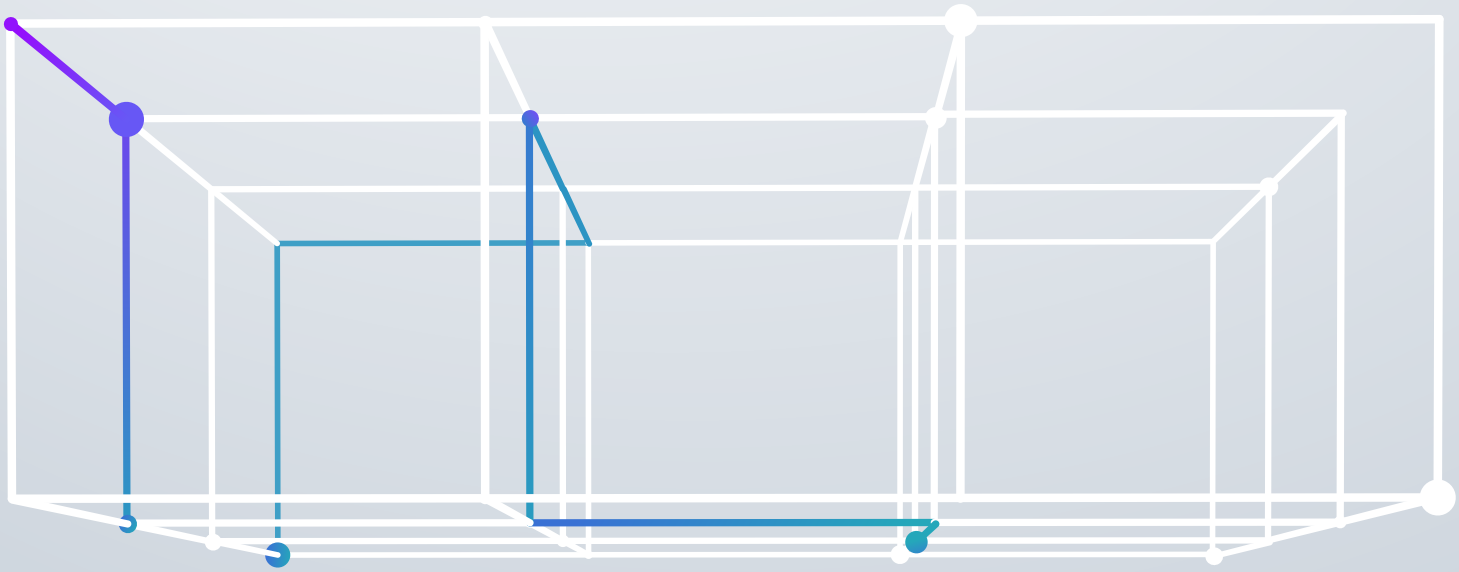
In LATAM, Brazil was the most targeted country with 53% of incidents, followed by Mexico and Peru, both with 13%.

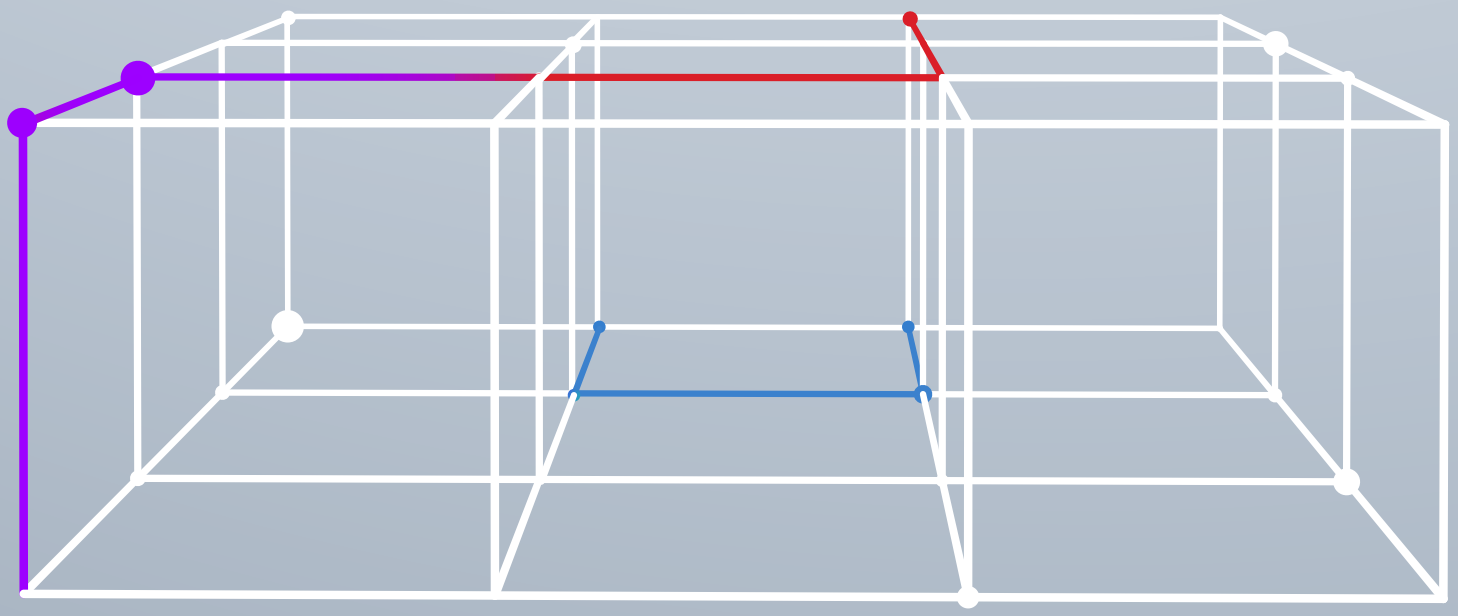
FIGURE 13

Incident response cases by geographic region



Source: IBM X-Force.





Industry trends

An analysis of X-Force incident response engagements highlights the industries most impacted by cyberattacks in 2024.

Manufacturing retained its position as the most targeted sector, representing 26% of incidents, emphasizing its critical role in global supply chains and the value of industrial-sector intellectual property. Finance and insurance followed as the second most attacked industry, accounting for 23%, reflecting the sector's sensitivity to data breaches and ransomware campaigns.

Of particular interest to governments and utilities, 70% of attacks in 2024 involved critical infrastructure. In this subset, the use of valid accounts made up 31% of initial access vectors, followed by phishing and exploiting public facing applications, both at 26%. Malware was deployed in 40% of cases and ransomware was the malware of choice, occurring in 30% of malware deployments.

The use of legitimate tools was observed in 38% of attacks against critical infrastructure organizations while server access was the objective in 12% of incidents. Credential harvesting, data theft, and extortion were the top three impacts felt by victims in this category, accounting for 27%, 23%, and 20% respectively.

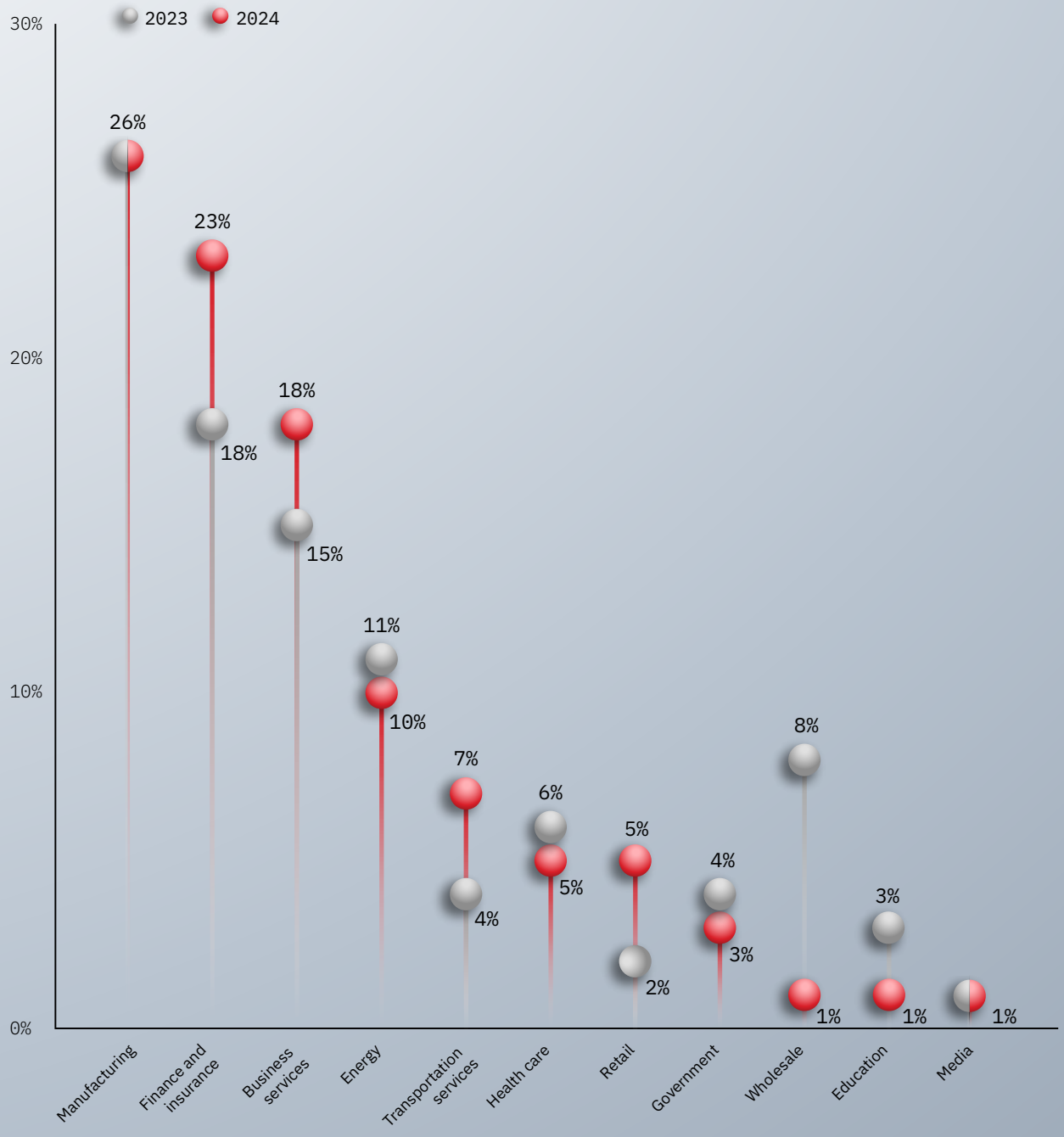
The professional, business, and consumer services sector emerges as another significant target, accounting for 18% of incidents.This reflects risks tied to third-party providers, supply chain operations, and organizations with consumer-facing vulnerabilities.

The energy sector placed fourth at 10%, as attackers continued to exploit its operational dependencies and critical infrastructure.

This distribution of incidents highlights a clear pattern of attackers prioritizing sectors with high-value assets, operational dependencies, and opportunities for financial or geopolitical leverage. To counter these evolving threats, organizations should adopt industry-specific risk assessments, prioritize enhanced cybersecurity investments, and foster collaborative defense strategies, such as industry or sector-specific ISACs, to safeguard these critical sectors and help ensure long-term resilience.

FIGURE 14

Share of attacks by industry, 2023-2024



Proportion of incident response cases observed by X-Force for the period 2023-2024. Source: IBM X-Force.

#1

Manufacturing – 26%

For the fourth consecutive year, manufacturing is the most attacked industry, representing 26% of all incidents within the top 10 industries. This ongoing targeting underscores its critical role in global supply chains and the high value of operational and intellectual property data.

Attackers leveraged several methods to breach manufacturing systems, with exploitation of public-facing applications (29%) emerging as the most common vector. Valid accounts-domain (21%) and external remote services (21%) were also prominent, reflecting attackers' reliance on exploiting misconfigured or insufficiently secured access points.

Once inside manufacturing environments, attackers frequently sought to establish control or exfiltrate valuable data. Server access (16%) and malware-ransomware (16%) were the most observed actions, emphasizing operational disruption and financial extortion as key objectives. The use of credential acquisition tools (13%) also stood out, showcasing the value of compromised access in enabling further attacks.

Manufacturing organizations experienced significant impacts from these attacks. Extortion (29%) and data theft (24%) were the most prevalent, targeting both financial assets and intellectual property. Credential harvesting (18%) further compounded risks, enabling persistent attacker access. The sector also faced challenges with brand reputation damage (12%), underscoring the business consequences of cyber incidents.

The APAC region continues to be the epicenter of manufacturing-related incidents, accounting for 56% of attacks. North America (22%) follows as the second most impacted region, reflecting the economic significance of its manufacturing operations. Europe (16%) and Latin America (7%) also faced notable activity.

#2

Finance and insurance –23%

For the fourth consecutive year, finance and insurance ranked as the second most attacked industry, trailing only manufacturing and accounting for 23% of incidents in 2024. The sector remains a prime target due to its critical role in the global economy and the high value of financial data and assets.

Attackers primarily breached finance and insurance systems through phishing / spearfishing attachments (30%)", leveraging human error to gain a foothold. Exploiting public-facing applications (20%) and using valid accounts-domain (20%) and valid accounts-local (20%) were also common tactics, highlighting the need for robust credential and access management practices. Additionally, external remote services (10%) reflected attackers' exploitation of remote access vulnerabilities.

Once inside, attackers focused on reconnaissance and maintaining control. Tool- recon/scanning (24%) and tool-remote access (18%) were the most observed actions on objectives, signaling a strategic focus on gathering intelligence and establishing persistence. The deployment of malware-infostealers (12%) further underscored attackers' intent to exfiltrate sensitive financial data.

The sector faced substantial impacts from these incidents. Espionage (20%), credential harvesting (20%), and data theft (20%) were equally common, with attackers focusing on stealing sensitive information and compromising account credentials. Other impacts, such as botnet activity (20%) and digital currency mining (20%), highlighted additional attempts to exploit compromised systems for broader campaigns or resource extraction.

Regionally, the Middle East and Africa experienced the highest volume of incidents, with 27% of cases targeting organizations in the region. This reflects the evolving financial landscape in emerging markets and attackers' interest in exploiting less mature cybersecurity defenses. APAC (24%) followed, driven by its economic growth and expanding digital footprint. North America (20%) and Europe (17%) remained significant targets, while Latin America (12%) saw fewer incidents.

#3

Professional, business, and consumer services – 18%

The professional, business, and consumer services sector ranked as the third most attacked industry in 2024, accounting for 18% of incidents. This diverse sector, comprising professional services such as consultancies, management companies, and law firms, business services such as IT, technology, and public relations firms, and consumer services such as real estate, entertainment, and recreation, remains a high-value target due to reliance on sensitive data and operational dependencies.

Attackers employed various tactics to achieve objectives, with server access (25%) emerging as the most commonly observed action. Malware-backdoor (13%), malware- web shell (13%), and business email compromise (13%) were also prominent, reflecting a focus on establishing control and enabling further malicious activity. Spam campaigns, malware such as worms and maldocs, and credential acquisition tools (6% each) underscored the wide array of techniques used against this sector.

The most common initial access vector was exploitation of public-facing applications (50%), demonstrating the sector's reliance on internet-exposed systems and applications. Phishing-spearphishing attachments (20%) ranked second, exploiting human error to gain access, while valid accounts (20%), both domain and cloud-based, were frequently used to infiltrate systems.

The primary impacts of these incidents were credential harvesting (45%) and data leaks (36%), emphasizing the attackers' intent to exfiltrate and monetize sensitive data. Extortion (9%) and data theft (9%) also highlighted the financial and reputational risks posed to organizations in this sector.

Regionally, Europe experienced the highest volume of incidents, accounting for 47% of cases, followed by North America (25%) and APAC (16%). Activity in the Middle East and Africa (6%) and Latin America (6%) was lower, reflecting regional disparities in targeting and attacker focus.

#4

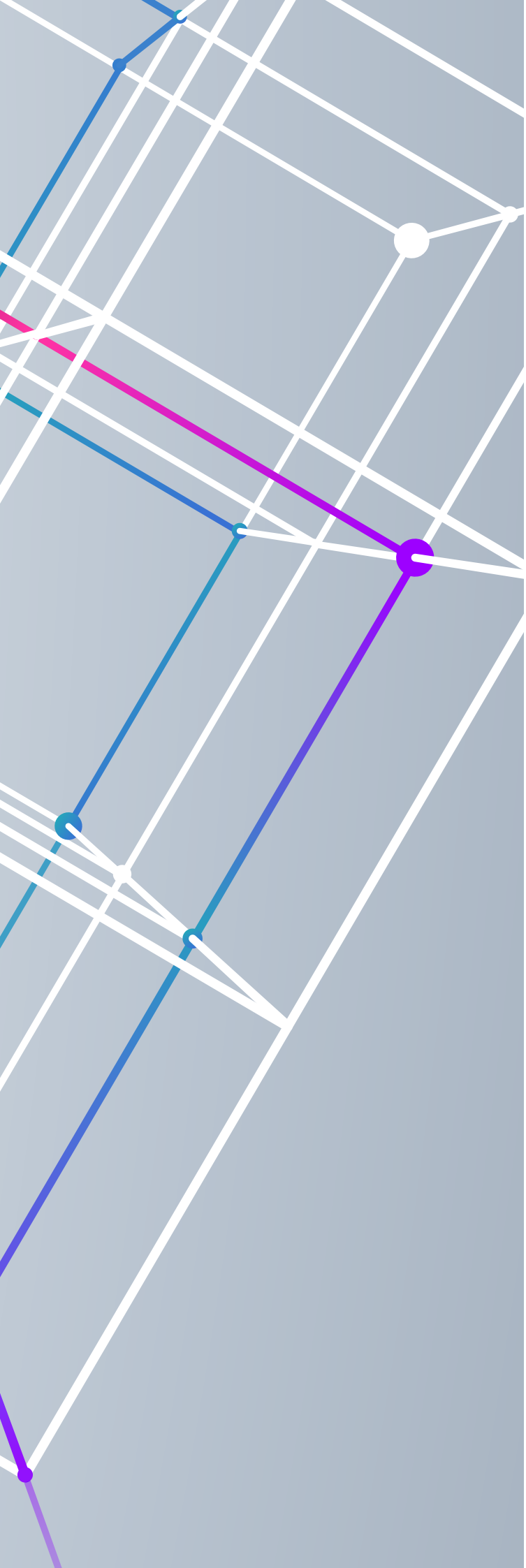
Energy 10%

The energy sector, encompassing electric utilities, oil and gas companies, and related industries, ranked as the fourth most targeted, accounting for 10% of incidents. The critical importance of energy infrastructure to global operations and its susceptibility to disruption makes it a persistent focus for attackers.

Attackers employed a diverse range of tactics, with server access (8%), malware- ransomware (8%), and malware-backdoor (8%) among the most observed actions on objectives. Additional techniques included malware-infostealer (8%), tool-credential acquisition (8%), and business email compromise (8%), showcasing a broad spectrum of strategies aimed at gaining control, stealing data, and monetizing breaches.

Initial access methods were evenly distributed across exploitation of public-facing applications (25%), phishing-spearphishing attachments (25%), external remote services (25%), and the use of valid cloud accounts (25%). This distribution highlights attackers' adaptability and their focus on exploiting vulnerabilities in exposed systems and human error.

Regionally, APAC experienced the highest volume of incidents, accounting for 33% of cases. Other regions, including Europe (17%), North America (17%), Latin America (17%), and the Middle East and Africa (17%), saw an even distribution of attacks, emphasizing the global nature of threats to energy infrastructure.



#5

Transportation services – 7%

Transportation rose to the fifth most attacked industry in 2024, accounting for 7% of incidents, up from eighth place last year. This increase reflects the sector's critical role in global logistics, infrastructure, and commerce, making it an attractive target for both financially motivated attackers and those seeking to disrupt operations.

The most common initial access vector observed was external remote services underscoring the sector's reliance on remote access solutions, which are often exploited by attackers to establish footholds within systems. This dependency emphasizes the importance of securing remote connections and monitoring for unauthorized access.

The transportation sector faced significant impacts, with data theft (67%) being the most common impact, reflecting attackers' interest in monetizing sensitive information. Extortion (33%) was also a prevalent outcome, showcasing the ongoing threat of ransomware campaigns targeting critical infrastructure.

Regionally, APAC experienced the highest volume of incidents, accounting for 54% of attacks, followed by Europe (23%), Latin America (15%), and the Middle East and Africa (8%). The concentration of incidents reflects the region's growing prominence in global transportation and logistics, and the expansive attack surface associated with interconnected suppliers and supply chains.

#6

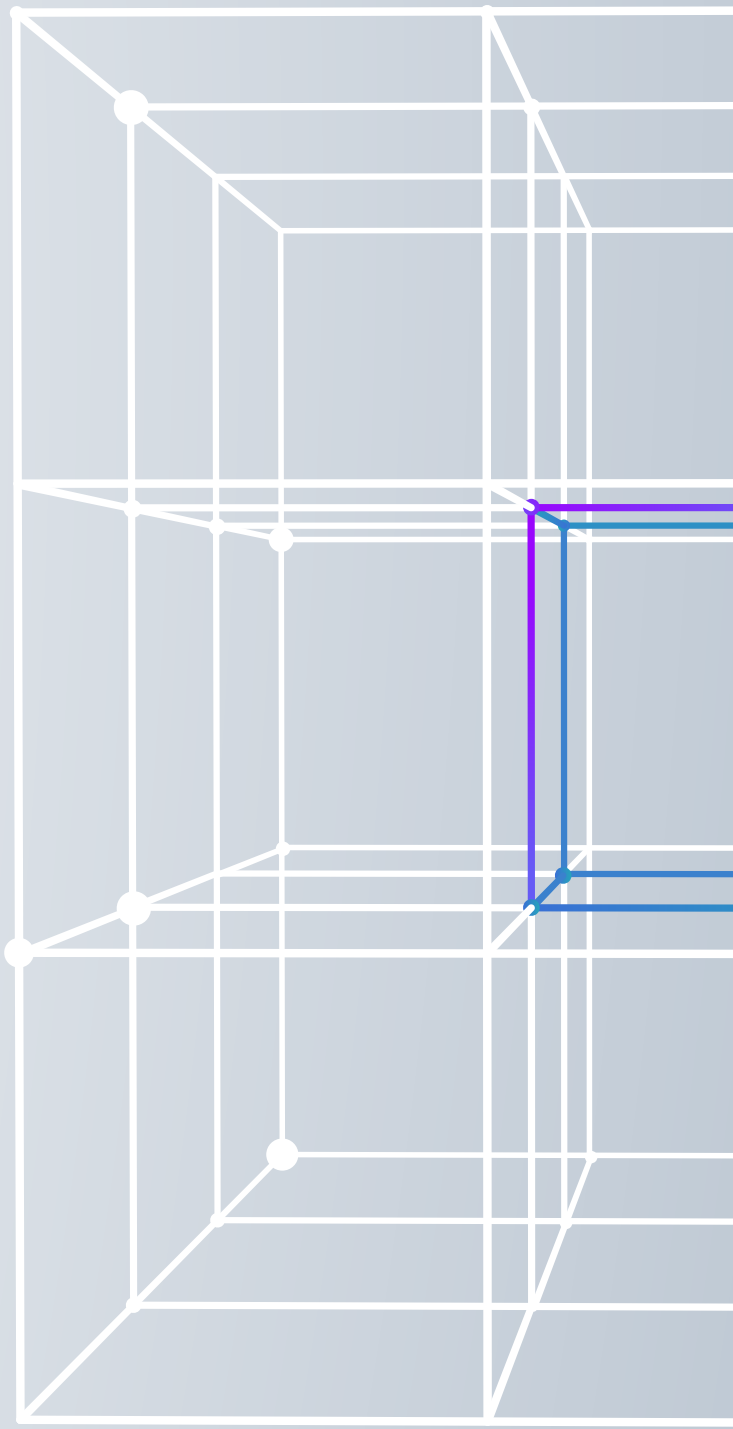
Retail sector – 5%

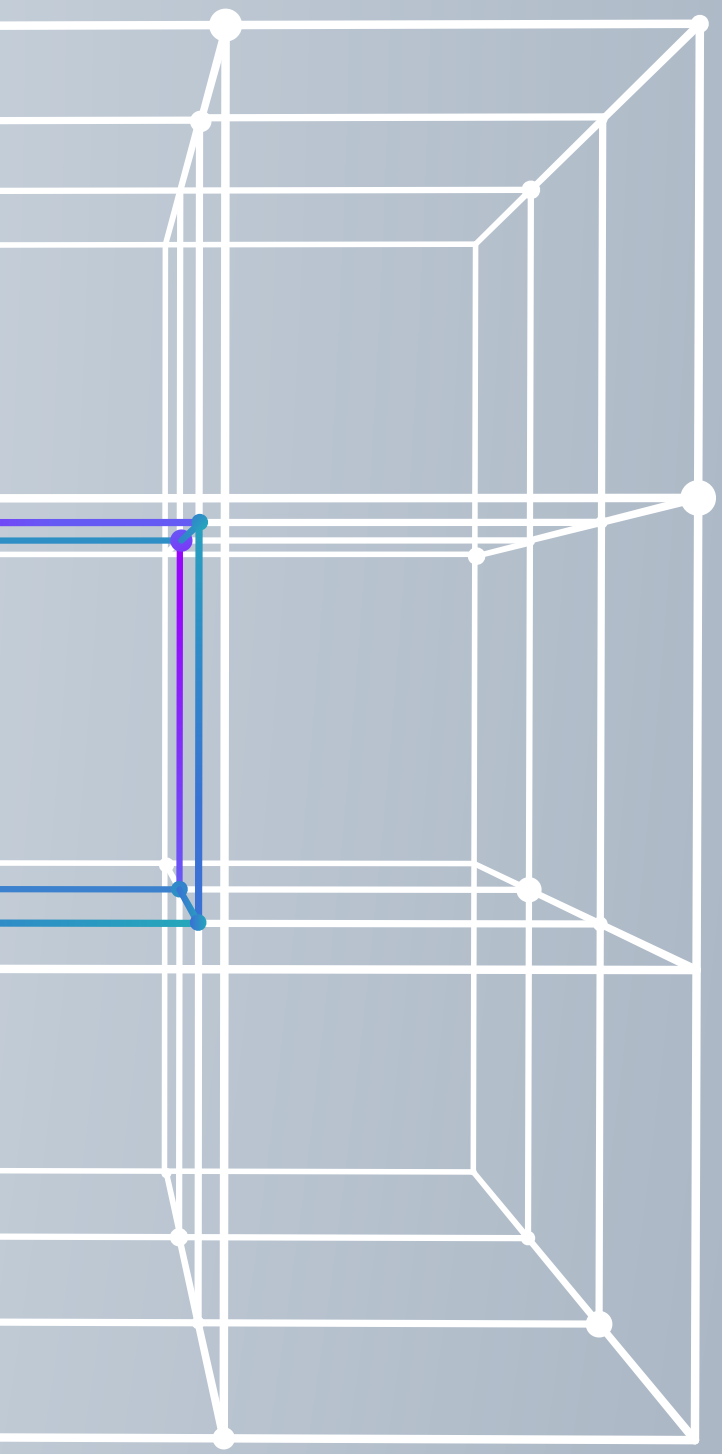
Retail accounted for 5% of incidents in 2024, reflecting its continued vulnerability to cyberattacks. As retailers rely heavily on digital infrastructure to manage consumer data and facilitate transactions, they remain an attractive target for attackers seeking financial or operational disruption.

Attackers employed a range of tactics, with business email compromise (25%), malware-backdoor (25%), email thread hijacking (25%), and malware-ransomware (25%) as the most observed actions. These methods highlight attackers' focus on both accessing and exploiting sensitive systems for further financial or operational gain.

The most observed initial access vector recorded was valid accounts-local, emphasizing the critical importance of managing and securing account credentials to help prevent unauthorized access. Interestingly, no direct impacts such as data theft, extortion, or financial loss were recorded in retail incidents this year. This could indicate a focus on reconnaissance or preparing systems for future exploitation rather than immediate disruption.

Regionally, North America (44%) experienced the highest proportion of retail-related incidents, followed by Europe (33%) and APAC (22%). This underscores threat concentrations in regions with extensive retail activity and infrastructure.





#7

Healthcare – 5%

Healthcare accounted for 5% of incidents in 2024, dropping from sixth place last year to seventh. Despite the decline, the sector remains a critical target due to its reliance on sensitive patient data, operational continuity requirements, and prevalence of outdated systems.

Attackers predominantly employed server access (67%) and malware-ransomware (33%) as their main actions on objective, reflecting a focus on both operational disruption and financial extortion. These actions highlight the sector's vulnerability to attacks that compromise systems and hold data or services hostage.

The most observed initial access vector was exploitation of public-facing applications, emphasizing the risks posed by exposed systems and the urgent need for robust vulnerability management practices. The primary impact of these attacks was credential harvesting, showcasing attackers' intent to obtain access credentials for broader campaigns or resale in underground markets. The comprehensive focus on credential harvesting reflects its importance as an enabler for follow-on attacks within this highly sensitive sector.

Regionally, APAC (44%) experienced the highest volume of healthcare-related incidents, followed by North America (33%) and Europe (22%), highlighting a significant concentration of threats in regions with advanced healthcare infrastructure.

#8

Government – 3%

Government accounted for 3% of incidents in 2024, dropping from seventh place last year to eighth. Despite the lower ranking, government entities remain high-value targets due to the vast amounts of sensitive data they manage, including state-level intelligence, classified assets, and personally identifiable information (PII).

Attackers predominantly used malware-other (67%) and spam (33%) as their primary actions on objective, reflecting a focus on spreading malicious content and exploiting vulnerabilities to gain system access. These tactics emphasize the sector's exposure to varied attack methodologies designed to disrupt operations and steal critical data.

Initial access vectors were evenly split between valid accounts-cloud (50%) and drive-by compromise (50%), showcasing attackers' ability to exploit both credential mismanagement and vulnerabilities in web-based resources to infiltrate systems.

The observed impact of credential harvesting underscored the attackers' focus on acquiring access credentials, which can enable follow-on attacks, espionage, or unauthorized access to classified systems. Regionally, North America (60%) experienced the highest volume of government-related incidents, followed by APAC (40%), reflecting the strategic importance of government entities in these regions and their prominence as targets for cybercriminals and nation-state actors.

#9

Wholesale sector – 1%

Wholesale accounted for 1% of incidents in 2024, reflecting its niche but ongoing presence as a target for cyberattacks. Wholesalers, responsible for distributing goods from manufacturers to retailers or directly to consumers, are critical links in the global supply chain, making disruptions to this sector impactful.

Attackers employed two primary tactics in wholesale incidents: tool-other (50%) and malware-other (50%), highlighting a focus on diverse and potentially tailored attack methods. No specific initial access vectors were identified this year, suggesting either indirect methods of compromise or secondary targeting via interconnected systems.

Similarly, no direct impacts, such as data theft or extortion, were observed in wholesale incidents for 2024. This absence may reflect attackers' focus on reconnaissance, supply chain infiltration, or other preparatory activities rather than immediate monetization or disruption.

Regionally, incidents were evenly split between APAC (50%) and North America (50%), suggesting a localized distribution of attacks across key regions for wholesale operations.

#10

Media – 1%

Media and telecommunications accounted for only 1% of incidents to which X-Force responded, coming in tenth place for the fourth 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, APAC, and Europe. In 2024-2025, the media sector remained a target for disinformation campaigns and espionage, particularly in the Middle East.

#11

Education – 1%

Education accounted for 1% of incidents in 2024, reflecting its continued position as one of the least targeted industries. Despite this low ranking, the sector remains vulnerable due to its reliance on sensitive student and staff data, often coupled with constrained cybersecurity resources.

Attackers exclusively utilized recon/scanning tools as the primary action on objective, highlighting a focus on gathering intelligence and identifying vulnerabilities within education systems rather than executing disruptive attacks. The drive-by compromise access vector emphasized the risks associated with users inadvertently accessing malicious websites or downloading harmful content.

All incidents in the education sector this year were recorded in North America, underscoring a geographically concentrated threat landscape within this sector.

Action guide

Threat management is the core of every successful cybersecurity program. Cyber risk and resilience practices go a long way towards improving security postures. For threats that do materialize, we need to evolve from ad hoc risk remediation and threat management to proactive, community-based measures such as threat intelligence sharing. Working together increases awareness and accountability across supply chains and ecosystems and raises collective resilience across the operations lifecycle.

01

Limit your exposure across the threat environment.

Know what the bad guys know about you. Monitor the dark web to gather real-world threat intelligence about your organization, employees, networks, and data on the dark web, before threat actors do.26

Keep your employees current on the most effective security practices. Educate your employees about the risks associated with phishing attacks and poor password hygiene and regularly update your people about ways to protect themselves and your organization.

Enhance ecosystem-wide incident response planning. Work with stakeholders in your organization and with partners across your ecosystem to develop and regularly update incident response plans that specifically address threats specific to your industry.

02

Embed and extend advanced security across all AI workloads and services.

Secure your AI development and deployment pipeline. Secure each stage of the AI pipeline including the data used to train, test, and tune models; the AI models themselves; and the responsible use of AI models to support robust infrastructure security.

Extend AI governance and ethics accountability. Robust governance is essential for trustworthy AI. Work with partners to set clear guidelines for AI usage; regularly audit AI systems for fairness, bias, and drift; and help ensure that AI outputs align with broader organizational values and ethics.

Use security frameworks to instill trust in AI systems. Use standardized frameworks that offer structured approaches to securing AI systems. These cover essential aspects such as data privacy, model integrity, usage controls, and ongoing monitoring. Protect credentials by reining in data and identity sprawl.

03

Protect credentials by reining in data and identity sprawl.

Implement robust data protection. Protect sensitive data wherever it resides, whether in on-premises, in the cloud, or in hybrid environments. To protect data in motion use encryption, implement strong access controls, and monitor data transfers.

Consolidate identity solutions. Work toward eliminating disconnected data and identity silos. This involves weaving identity management systems together into a unified, holistic framework—often referred to as an "identity fabric" approach.

Turn the tables on adversaries with AI-powered, proactive threat detection. As threat actors step up the use of AI to develop and scale credential-based attacks, step up the use AI and machine learning to detect threats faster and respond to attacks more effectively.

04

Patch authentication gaps before attackers can sneak in.

Significantly expand MFA use. Prioritize Multifactor Authentication (MFA) for all employees This provides an extra layer of protection for applications and network services, even if passwords are compromised.

Modernize identity strategy. Along with expanded MFA usage, develop and implement a comprehensive, adaptive, and scalable identity strategy. Align the strategy to changing operational and security requirements and improve it through regular audits.

Reduce IT and IS complexity. Growing IT and IS complexity hinders the effective administration of secure identities and slows down response to legitimate threats. To counteract complexity, invest in tools and technologies, such as identity fabrics, for simpler and more cohesive identity platforms.

Contributors

Michelle Alvarez

Manager, X-Force Strategic Threat Analysis. IBM Consulting

Christopher Caridi

Cyber Threat Analyst, X-Force Strategic Threat Analysis. IBM Consulting

Joshua Chung

Strategic Cyber Threat Analyst, IBM Consulting

Sophie Cunningham

X-Force Cyber Threat Intelligence Analyst, IBM Consulting

Michael Epley

Chief Architect and Security Strategist, Red Hat

Mohit Goyal

Senior Principal Product Manager, Red Hat Insights

Charlotte Hammond

Malware Reverse Engineer, IBM Consulting

Sandra Hill

Manager, X-Force Vulnerability Intelligence, IBM Consulting

Jeff Kuo

X-Force Engineer, X-Force Vulnerability Intelligence, IBM Consulting

Dave McMillen

Strategic Threat Analyst, IBM Security X-Force, IBM Consulting

Golo Mühr

Malware Reverse Engineer, X-Force Threat Intelligence, IBM Consulting

Gerald Parham

Global Research Leader, Security & CIO, IBM Institute for Business Value

Austin Zeizel

Threat Intelligence Consultant, IBM Consulting

Notes & sources

1. Francis, Joel. “Briefing 29: Implications of the Ongoing Salt Typhoon Campaign on Telecommunications and Space.” Kratos. January 15, 2025. https://www.kratosdefense.com/constellations/articles/implications-of-the-ongoing-salt-typhoon-campaign-on-telecommunications-and-space

2. Mühr, Golo, and Joe Fasulo. “Hive0137 and AI-supplemented malware distribution.” Security Intelligence. July 26, 2024. https://www.ibm.com/think/x-force/hive0137-on-ai-journey

3. “Combatting Cyber Threat Actors Perpetrating Living Off the Land Intrusions.” National Security Agency press release. February 7, 2024. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669159/combatting-cyber-threat-actors-perpetrating-living-off-the-land-intrusions/

4. “Cost of a data breach 2024.” IBM Security and Ponemon Institute. July 2024. https://www.ibm.com/reports/data-breach

5. Mühr, Golo, and Joe Fasulo. “Hive0137 and AI-supplemented malware distribution.” Security Intelligence. July 26, 2024. https://www.ibm.com/think/x-force/hive0137-on-ai-journey

6. IBM X-Force Threat Intelligence Index 2024. IBM Security. February 2024. https://www.ibm.com/reports/threat-intelligence

7. “Adoption of artificial intelligence among organizations worldwide from 2017 to 2024, by type.” Statista. May 2024. https://www.statista.com/statistics/1545783/ai-adoption-among-organizations-worldwide/

8. Merrill, Josh. “Smoltalk: RCE in open source agents.” Security Intelligence. February 14, 2025. https://www.ibm.com/think/x-force/smoltalk-rce-in-open-source-agents

9. Lumelsky, Avi, Guy Kaplan, and Gal Elbaz. “ShadowRay: First Known Attack Campaign Targeting AI Workloads Actively Exploited in the Wild.” Oligo. March 26, 2024. https://www.oligo.security/blog/shadowray-attack-ai-workloads-actively-exploited-in-the-wild

10. Hawkins, Brett and Chris Thompson. “Disrupting the Model: Abusing MLOps Platforms to Compromise ML Models and Enterprise Data Lakes.” IBM X-Force Red. January 6, 2025. https://www.ibm.com/downloads/documents/us-en/11630e2cbc302316?_gl=1*ndgdb2*_ga*MTYyOTYzMjEwMC4xNzE1ODc2MTkw*_ga_

11. Rodgers, Clarke, Moumita Saha, Dimple Ahluwalia, Kevin Skapinetz, and Gerald Parham. Securing generative AI: What matters now. IBM Institute for Business Value. May 2024. https://ibm.co/securing-generative-ai

12. Initial access: the adversary is trying to get into your network.” Mitre Att&ck. July 19, 2019. https://attack.mitre.org/tactics/TA0001/

13. Mühr, Golo, Joe Fasulo, and Charlotte Hammond. “Strela Stealer: Today’s invoice is tomorrow’s phish.” Security Intelligence. November 12, 2024. https://securityintelligence.com/x-force/strela-stealer-todays-invoice-tomorrows-phish/

14. Based on IBM X-Force telemetry. 2024.

15. Mühr, Golo and Joe Fasulo. “Hive0137 and AI-supplemented malware distribution.” Security Intelligence. July 26, 2024. https://securityintelligence.com/x-force/hive0137-on-ai-journey/

16. “Report on CVE-2024-24919: A Check Point Security Gateway Vulnerability.” Cybersixgill IQ. June 6, 2024. https://cybersixgill.com/news/articles/cve-2024-24919-vulnerability

17. “Detecting Compromise of CVE-2024-3400 on Palo Alto Networks GlobalProtect Devices.” Volexity blog. May 15, 2024. https://www.volexity.com/blog/2024/05/15/detecting-compromise-of-cve-2024-3400-on-palo-alto-networks-globalprotect-devices/

18. “BORN Group Supply Chain Breach: In-Depth Analysis of Intelbroker’s Jenkins Exploitation.” CloudSEK TRIAD. July 23, 2024. https://www.cloudsek.com/blog/born-group-supply-chain-breach-in-depth-analysis-of-intelbrokers-jenkins-exploitation

19. “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.” US Cybersecurity and Infrastructure Security Agency. February 7. 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

20. Hewitt, Nik. “The Rising Tide of Cybercrime as a Service (CaaS.” Cyber Defense Magazine. December 13, 2023. https://www.cyberdefensemagazine.com/the-rising-tide-of-cybercrime-as-a-service-caas/

21. “Qakbot Malware Disrupted in International Cyber Takedown.” U.S. Attorney’s Office, Central District of California press release. August 29, 2023. https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | April 2025