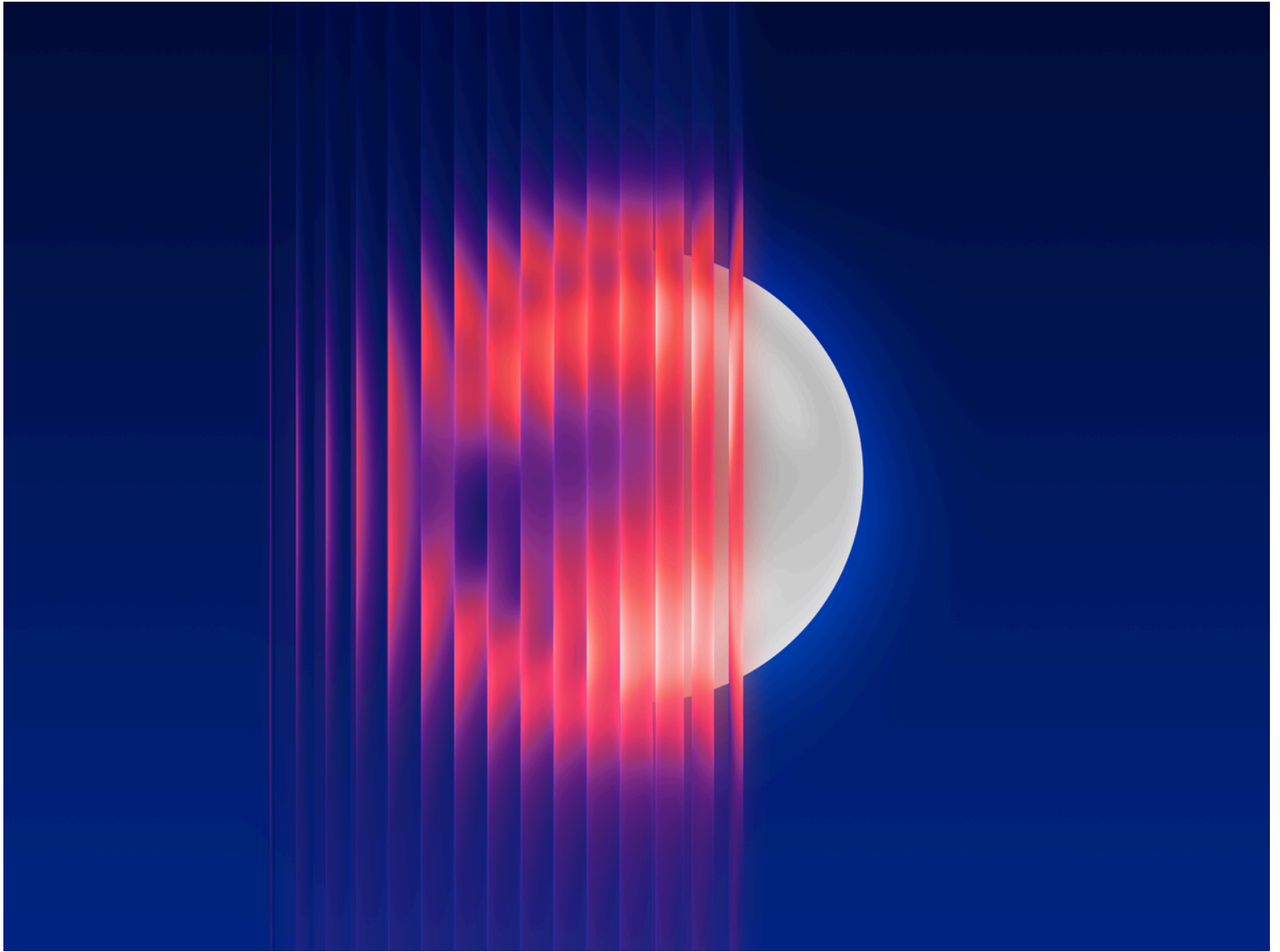


X-Force Threat Intelligence Index 2026

Published 25 February 2026



Executive summary

The biggest trends the IBM X-Force team observed in 2025 were a surge in broad-based exploitations of exposed systems, weaknesses in software supply chains and growing systemic dependencies across cloud and application ecosystems.

Last year, attackers refined their techniques for infiltrating software distribution channels, cloud services and open-source ecosystems. By doing this, they demonstrated how a single weak point in an interconnected environment can enable large-scale or high-privilege access.

X-Force, which pulled data from incident response and penetration tests, the dark web and other threat intelligence sources for this report, identified the leading initial access vector: the exploitation of public-facing applications. The team noted the growing number and complexity of software vulnerabilities—combined with misconfigurations in applications—and AI adoption broadened the attack surface for intrusions. Many vulnerabilities didn't require authentication at all, highlighting the critical need for stronger access controls, rigorous patching and secure deployment practices.

X-Force also found credential theft remained at the center of many prominent campaigns. Meanwhile, the rapid adoption of AI chatbot platforms for consumers and workplace users introduced a new layer of exposure; credentials tied to these chatbots increasingly surfaced in underground marketplaces, driven largely by infostealer infections on end-user devices.

Threat actors often publicly exaggerate their reach and successes, which can inflate the perceived scale of these compromises. That said, the underlying trend X-Force identified is a clear warning for security leaders: organizations are accumulating sensitive authentication data on systems that may not be adequately secured. Law-enforcement takedowns managed to disrupt portions of the infostealer ecosystem in 2025, but these malware families continue to offer adversaries easy and effective means of gathering high-value credentials.

The ransomware ecosystem also shifted in 2025, becoming more fragmented and volatile, with many small groups conducting lower volume but widespread attacks. Data extortion, supply-chain compromise and opportunistic targeting of smaller organizations remained prominent trends as well.

The tactics between nation-state actors and cybercriminal groups continued to converge. X-Force noted tools, techniques and operational patterns increasingly overlapped between these threat communities, complicating attribution and potentially delaying appropriate response actions. In several instances, activity that initially appeared mundane later proved to be part of highly sophisticated, persistent operations.

Overall, 2025 highlighted a clear message: identity protection, secure configuration and visibility across applications, development pipelines and cloud environments are increasingly central to cyber resilience.

Artificial intelligence also continued to reshape attacker operations in 2025. While AI has not changed playbooks, it has dramatically increased the speed, scale and efficiency of those operations. Adversaries are now using generative AI to shrink decision cycles, scale social engineering and iterate on attack paths in real time. As multimodal models mature, the barrier to entry will shrink further, allowing lower-

skilled workers to automate reconnaissance, privilege escalation and lateral movement, resulting in faster-moving, and more adaptive threats.

Despite these evolving trends and sometimes sophisticated threats, basic lapses in cybersecurity hygiene contributed to many compromises; X-Force incident response and penetration testing engagements found misconfigured access controls, weak authentication practices, incomplete logging and insufficient vulnerability management as recurring issues. These foundational weaknesses continued to provide attackers with opportunities that are far easier to exploit than advanced or novel techniques.

Overall, 2025 highlighted a clear message: identity protection, secure configuration and visibility across applications, development pipelines and cloud environments are increasingly central to cyber resilience. As attackers continue to refine credential-driven and supply-chain-focused operations, strengthening these fundamentals remains the most effective defense.

The IBM X-Force Threat Intelligence Index 2026 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. X-Force offers these insights as a resource to IBM clients, cybersecurity researchers, policy makers, the media and the broader community of security professionals and business leaders. Through the work of our global team, we aim to deliver a data-driven view of the current threat landscape. It's our intent to keep all parties informed of the current threat landscape so they can make the best decisions for reducing risk.

[NEXT: Report highlights](#) →

X-Force Threat Intelligence Index 2026

Report highlights

44% increase in the exploitation of public-facing applications

X-Force observed a rise in the exploitation of public-facing applications as an initial access vector in 2025 due to an increase in supply-chain attacks targeting development ecosystems and trusted infrastructure.

56% of disclosed vulnerabilities did not require authentication to successfully exploit

The number of vulnerabilities tracked by X-Force approached 40,000 in 2025 and over half didn't require authentication for an attacker to successfully exploit. This finding may reflect gaps in secure-by-design implementation as attackers are finding success without using credentials, MFA bypass or even end user interaction.

>300K ChatGPT credentials observed for sale on the dark web

In 2025, infostealer malware enabled the exposure of over 300,000 ChatGPT credentials, demonstrating that AI platforms have reached the same credential risk as other core enterprise SaaS solutions. While none of the credentials posted were still valid, the credentials consistently corresponded to infostealer infections and leaked credentials collections observed in 2024 and earlier.

X-Force tracked nearly 40,000 vulnerabilities in 2025. Over half didn't require authentication for an attacker to successfully exploit.

~4x increase in the number of major supply chain or third party breaches over 5 years

Adversaries increasingly exploited developer trust and identity integrations to steal credentials, pivot into cloud environments and maintain persistence across interconnected systems. Sprawling third-party dependencies create hard-to-secure attack surfaces—where one weak link can expose many targets. Once largely confined to nation-state actors, these supply chain attack techniques are now being adopted by financially motivated and other criminal threat groups, reflecting a clear trickle-down of advanced tactics.

49% increase in active ransomware groups compared to 2024

Fragmentation continues in the space, with 109 different ransomware extortion groups identified by X-Force in 2025. Up from 73 groups in 2024, this fragmentation reflects a lower barrier to entry: threat actors frequently reuse leaked tooling, follow established playbooks or shift between group identities, enabling many small operators to conduct opportunistic, low-volume attacks.

Manufacturing was the top-targeted industry for the fifth year in a row

The sector accounted for 27.7% of incidents, up only slightly from 26% last year. This figure is only a few tenths of a percent higher than the finance and insurance sectors, which accounted for 27% in 2025 and 23% in 2024.

29% of attacks targeted North America

The region accounted for nearly one third of total cases. Up from 24% in 2024, North America became the most attacked region for the first time in 6 years. Conversely, Asia Pacific saw a decrease from 34% to 27%.

[NEXT: Top initial access vectors](#) →

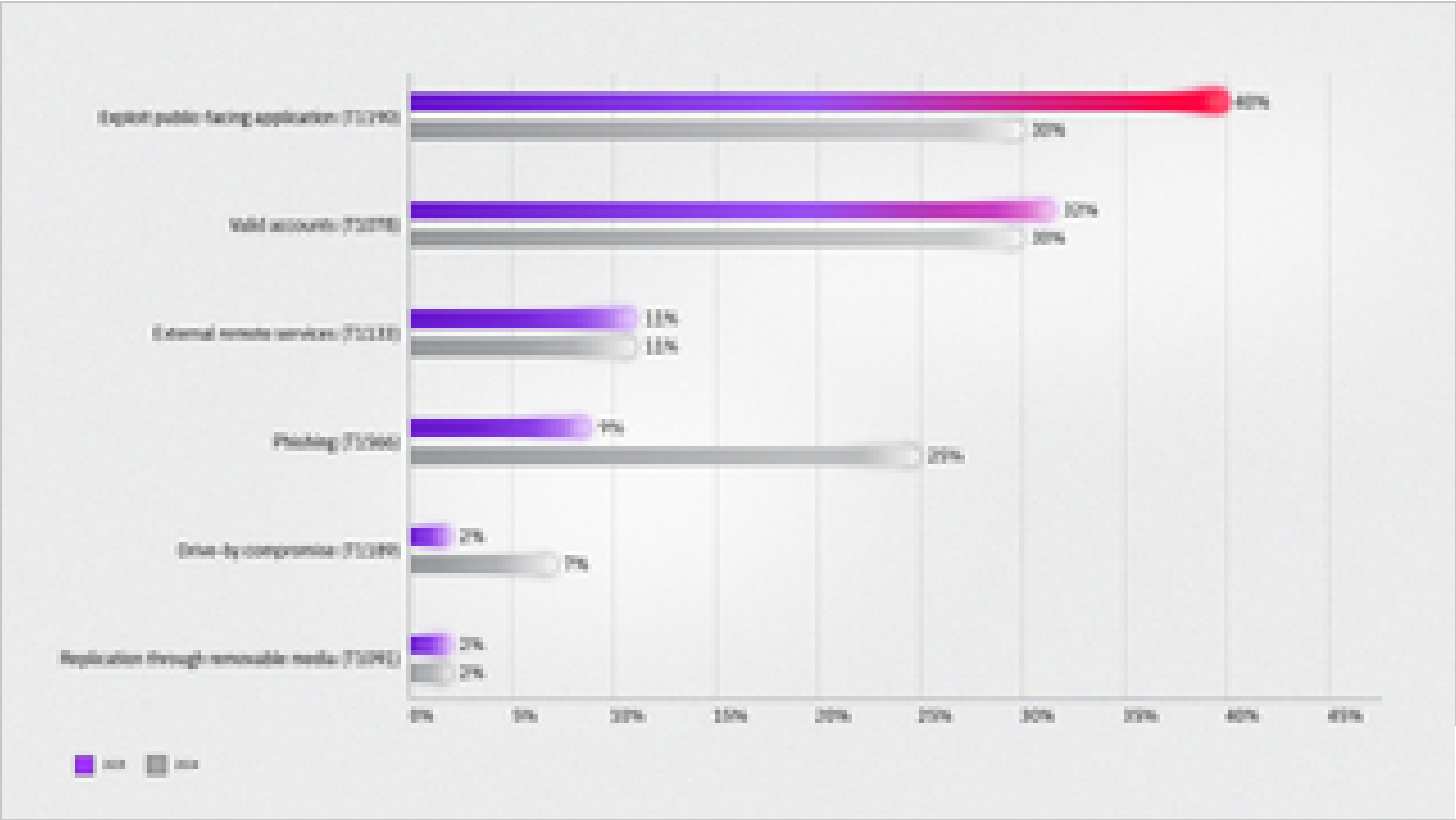
X-Force Threat Intelligence Index 2026

Top initial access vectors

Rise of vulnerability exploitation

For the past 2 years, X-Force reported on the abuse of valid credentials as a top initial access vector used by adversaries across industries and regions.

The appeal of using legitimate credentials to gain access to infrastructures has drawn attackers in for its relative simplicity and high success rate. However, in 2025, X-Force observed a dramatic shift in this trend. We witnessed a 44% increase in incidents caused by the exploitation of public-facing applications. This increase accounted for 40% of cases, whereas use of valid credentials made up only 32% of cases. Public-facing applications are subject to exploitation through vulnerabilities or misconfigurations associated with application deployment, configuration, or both.

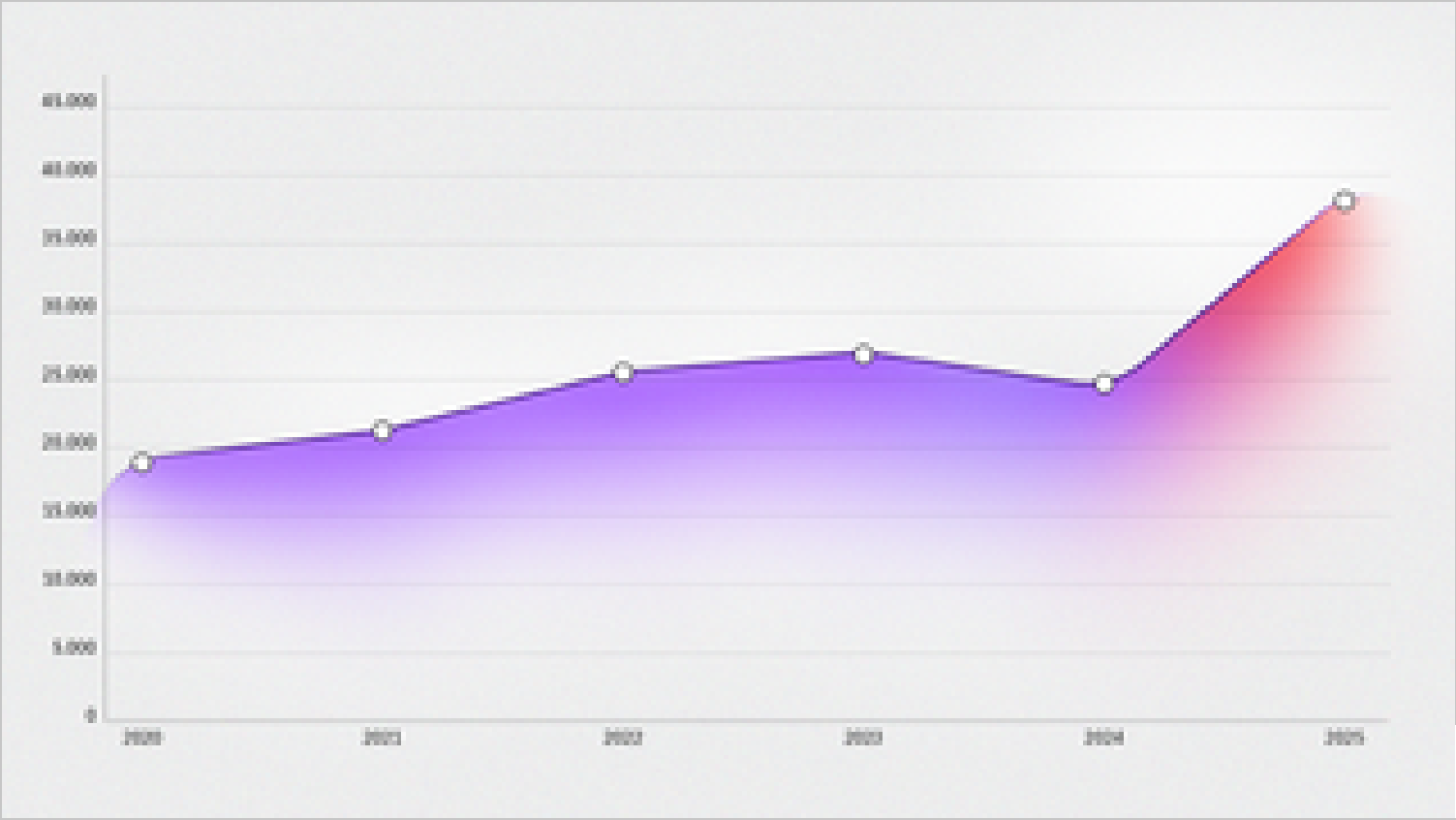


Top initial access vectors X-Force observed in 2025 and 2024. Source: IBM X-Force.

This trend was compounded by a rise in supply-chain attacks increasingly targeting development ecosystems and trusted infrastructure—meaning vulnerabilities were being exploited earlier in the software lifecycle and at a

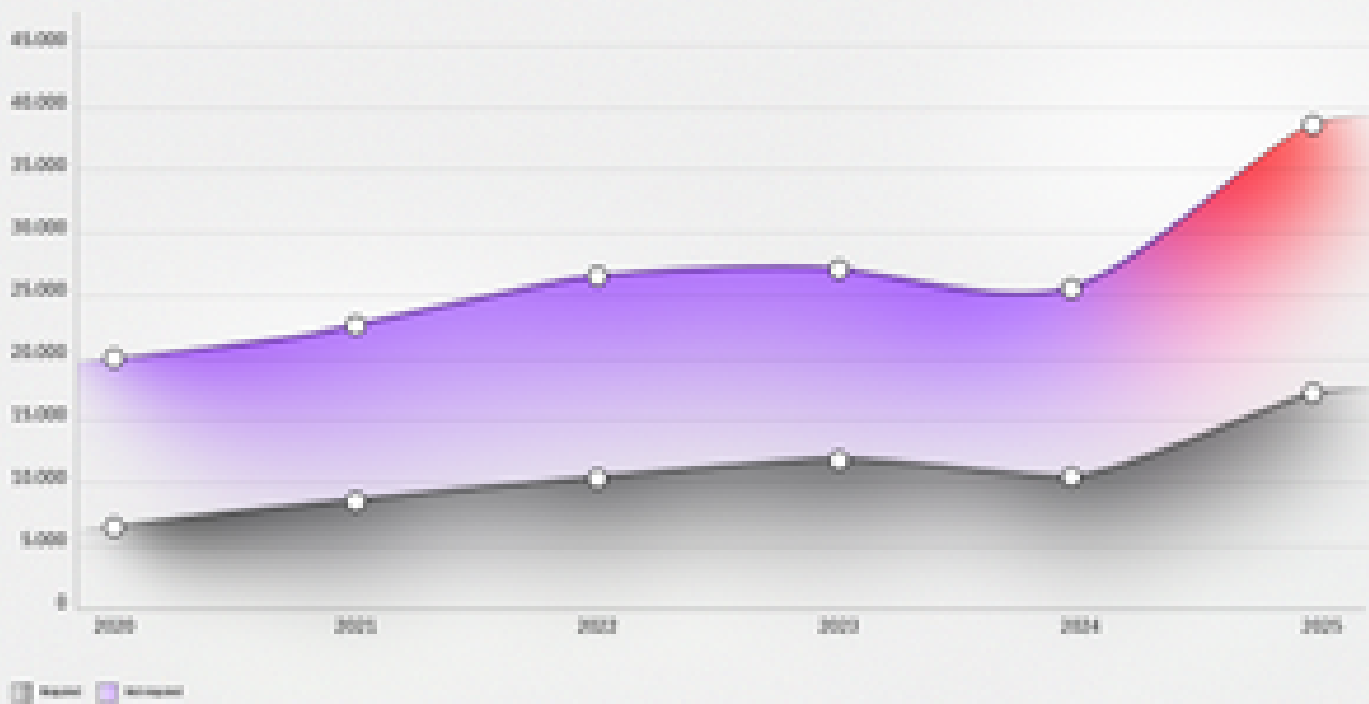
much larger scale. This shift may also be connected to weaknesses in client environments observed by X-Force Red (described later in this report), where misconfigurations, weak authentication and insecure code—identified by [Common Attack Pattern Enumeration and Classification's](#) CAPEC-180, CAPEC-49 and CAPEC-242—consistently provided easy entry points. Together, the systemic fragility in supply-chain ecosystems and the prevalence of these foundational CAPEC weaknesses significantly accelerated the exploitation of vulnerabilities throughout 2025.

In addition, we observed heightened discovery and reporting efforts in 2025. X-Force maintains a database tracking vulnerabilities over time, and our data indicated a notable upward trend, year over year, for new vulnerabilities. This trend marks the growing complexity of software ecosystems and available attack surface to include AI systems. It's also plausible this increase in vulnerability reporting could result in part from both researchers and attackers using AI and machine-learning tools to identify vulnerabilities.



The growth of vulnerabilities since 2020. Source: IBM X-Force.

Additionally, the tracked vulnerabilities can be placed into two categories determined by whether authentication was required for exploitation. The data reveals most (56%) vulnerabilities could be exploited without authentication, significantly increasing the potential attack surface. This trend underscores a critical security concern. Systems lacking authentication controls are more susceptible to unauthorized access and exploitation, making it essential for organizations to implement robust authentication mechanisms and enforce strict access policies.



Most vulnerabilities tracked in 2025 did not require authentication to exploit. Source: IBM X-Force.

Continued use of valid credentials

Although no longer the leading initial access vector, the misuse of valid accounts represented nearly a third of the cases, indicating a continued reliance on legitimate credentials. Legitimate credentials remain one of the preferred entry points for attackers because they eliminate the need for exploits and let adversaries blend seamlessly into the normal authentication process. This theme is clear across multiple IBM X-Force investigations.

Campaigns built around credential theft as the enabling step show the same pattern:

Hive0145’s 2025 operation against German organizations delivered [Strela Stealer](#) specifically to harvest Microsoft Outlook and Mozilla Thunderbird logins. Once obtained, those real credentials allowed attackers to access mailboxes and impersonate users.

Similarly, the [France-focused spear-phishing wave](#) used leaked ISP customer data to lure victims into entering their Amazon credentials on a fake login page, enabling immediate account takeover without any technical exploitation.

Together the system fragility in supply chain ecosystems and the prevalence of foundational CAPEC weaknesses

significantly accelerated the exploitation of vulnerabilities throughout 2025.

Beyond phishing credential-theft campaigns, attackers also target systems that store or manage high-value credentials. Our X-Force Red Adversary Services team [published research](#) around SCCM (Microsoft's System Center Configuration Manager) credential-decryption. Analysts showed once an attacker gains a foothold on a Configuration Manager site server, they can extract and decrypt service-account passwords stored in the SCCM database. They can then use those valid credentials to pivot across the environment with the same trust and reach as the organization's own management infrastructure. The attacker doesn't need an exploit at that stage—they simply "log in" with SCCM accounts that automate software deployment and have broad network permissions, turning a single compromised server into enterprise-wide access.

The use of legitimate credentials—either phished or stolen—can allow attackers to shift from outsider to authorized user, bypassing controls and gaining persistent, low-visibility access.

Understanding how valuable credentials are to attackers, it's not surprising these are some of the most sought-after items within cybercriminal marketplaces. Our analysis found credential harvesting topped the list of impacts experienced by victim organizations in 2025.

AI chatbot credentials

The proliferation of AI chatbots in business operations created a new attack vector for cybercriminals utilizing infostealer malware. As organizations increasingly integrate AI chatbot technologies into their workflows, the risk of infected systems with stored credentials for these platforms has emerged. Furthermore, the theft of AI chatbot credentials that enable access to other systems—illustrated by the [Salesloft/Drift incident](#), where attackers stole Drift OAuth tokens and used them to break into multiple Salesforce environments—shows chatbot-token-based access into other systems is already happening and may be occurring more widely.

The top 5 platforms—ChatGPT (OpenAI), Microsoft Copilot, Google Gemini, Perplexity and Claude AI (Anthropic)—were reviewed for accounts for sale on the dark web containing credentials for the platforms. Visibility varies significantly from platform to platform included in the dataset. Ones that use third-party providers—such as SSO, Apple, Google or Microsoft—do not have platform-specific credentials stored and cannot be identified in credential data. In 2025, over 300,000 ChatGPT credentials were observed for sale.

Additionally, in February 2025, a threat actor posted example ChatGPT credentials on BreachForums and claimed to have stolen over 20 million accounts. While none of the example credentials posted were still valid, the credentials consistently corresponded to infostealer infections and leaked credentials collections observed in 2024 and earlier. This illustrates how large-scale credential theft from past infostealer activity can resurface as renewed criminal leverage, transforming previously compromised data into fresh opportunities for exploitation.

While 2025 saw considerable takedowns of infostealer malware infrastructure—such as with Lumma and Rhadamanthys—the use of infostealer malware remains an easy method for threat actors to gain access.

As with the adoption of other new technologies, companies should first assess policies and adoption of AI chatbots within their organization. Next, they should prioritize cybersecurity awareness education and enhancements to credential protection—such as the use of multi-factor authentication and passkeys, detection of abnormal login patterns and monitoring of credential exposure.

[Next: Supply chain and third party compromises](#)

X-Force Threat Intelligence Index 2026

Supply chain and third party compromises

Throughout 2025, supply chain and third-party compromises took the form of coordinated, multi-stage campaigns targeting the core of modern open-source ecosystems, CI/CD platforms and cloud infrastructure. These attacks exploited developer trust, automation workflows and cloud interfaces. They enabled adversaries to infiltrate development environments, harvest credentials, exfiltrate sensitive data and maintain persistence across environments, often pivoting into cloud services.

IBM X-Force has been tracking an increase in attacks against developer platforms such as GitHub, GitLab and npm, alongside growing intrusions into cloud service providers and high-value SaaS platforms. These supply chain compromises in 2025 highlight a clear shift: attackers are targeting the environments where software is built—and increasingly the SaaS ecosystems that support those workflows—rather than traditional endpoints. These campaigns exploit trust relationships and automation within development workflows, often beginning in open-source registries or CI/CD platforms and extending into cloud infrastructure. By leveraging stolen credentials and configuration data, adversaries achieve persistence and lateral movement across interconnected systems, amplifying the impact of a single compromise.

Supply chain attack vectors

The software supply chain is no longer a single link, but an interconnected stack of dependencies, automation and identity. Modern supply chain compromises increasingly exploit this interconnectedness.

Open-source registries such as npm and PyPI packages remain high-risk due to their scale and decentralized governance—a single compromised account can propagate malicious updates across thousands of projects. Attackers often embed payloads in post-install scripts or build hooks, leveraging weak package signing and complex dependency chains to accelerate propagation.

There has been a nearly 4-fold increase in major supply chain or third-party compromises over the last 5 years. Often, a single breach at a trusted supplier spread to many downstream customers, leading to widespread infiltration, disruption or data theft.

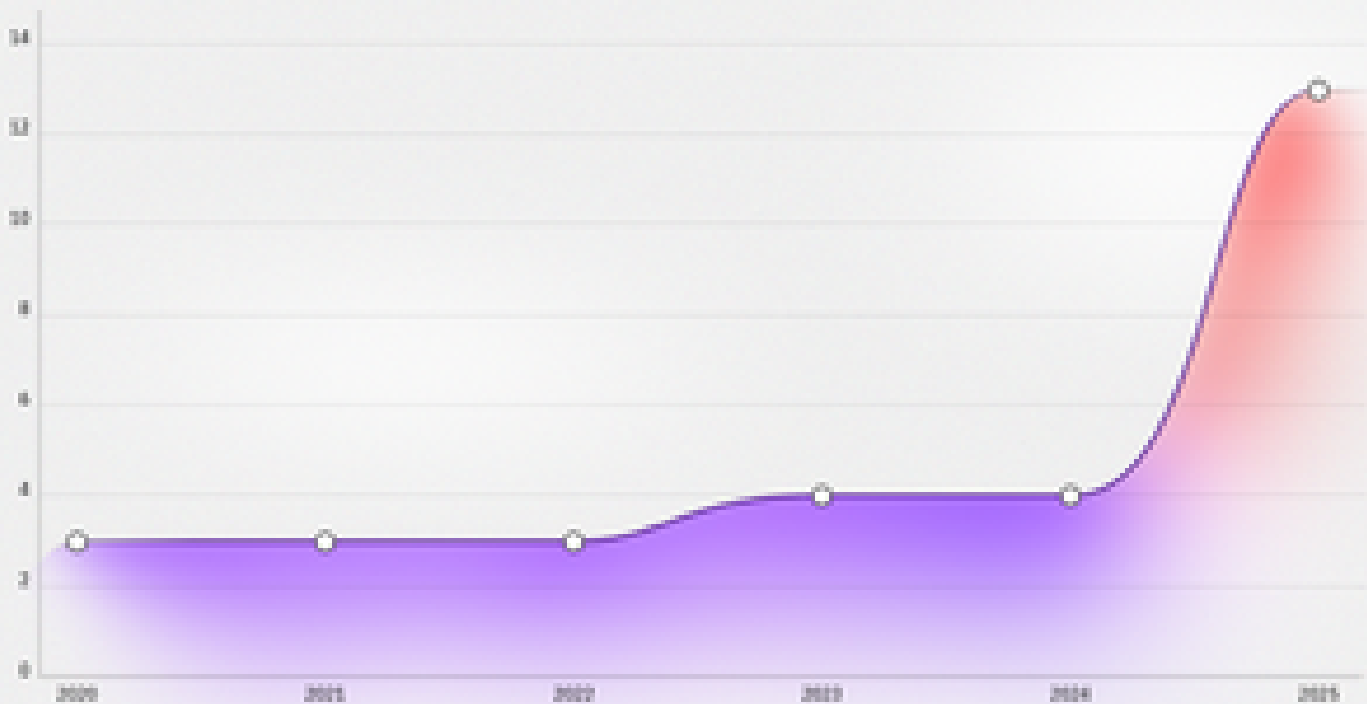
CI/CD platforms like GitHub Actions and GitLab CI have become prime targets for credential theft and workflow abuse. Malicious automation scripts harvest tokens, API keys and cloud credentials directly from build developer pipelines, while compromised personal access tokens provide long-term access across repositories and cloud environments. The deep integration of these cloud platforms with registries and cloud services indicates a single breach can expose the entire development lifecycle.

Cloud environments broadly represent the ultimate objective for many threat actor campaigns. Once attackers obtain developer or CI/CD credentials, they can easily pivot into cloud platforms using legitimate API calls to enumerate assets, create unauthorized admin accounts and extract sensitive data. Misconfigured IAM roles and exposed backups amplify this systemic risk, turning service providers into second-order supply chain targets while escalating overall impact across entire customer environments.

Implications

Supply chain attacks no longer rely solely on zero-day exploits or endpoint compromise. Instead, adversaries manipulate software delivery, deployment and management processes independently, exploiting trust and automation at scale. This evolution underscores a critical reality that the supply chain is now an interconnected stack of dependencies and identity rather than a single link, making integrity across these layers foundational to operational resilience.

Notably, there has been a nearly 4-fold increase in major supply chain or third-party compromises over the last 5 years. These compromises created a largescale, cascading impact: a single breach at a trusted supplier spread to many downstream customers, often leading to widespread infiltration, disruption or data theft. Once reserved for highly sophisticated nation-state campaigns, these supply-chain attack techniques are now increasingly leveraged by financially motivated and other criminal threat groups, contributing to the rise observed over the last several years.



The growth of major supply chain or third-party compromises since 2015 (see Appendix for details).
Source: IBM X-Force.

Notable threat actors

The X-Force team observed cybercriminal campaigns looking to exploit supply-chain and third-party vendor relationships in 2025. Three of the more prolific groups are Scattered Spider, LAPSUS\$ and ShinyHunters. Each represent well-documented, high-impact criminal actors whose tactics heavily influenced today’s supply-chain and third-party threat landscape.

- [Scattered Spider](#) is confirmed in multiple industry and government reports as a social-engineering-driven intrusion crew that exploits help desks, identity providers and cloud access pathways—allowing them to compromise not just a primary target but also downstream customers through federated IAM and managed service relationships.
- [LAPSUS\\$](#) is widely reported as an extortion group that targets telecoms, outsourcing firms and identity providers, using MFA reset abuse and insider recruitment to pivot into interconnected organizations reliant on those vendors.
- [ShinyHunters](#) is consistently profiled as a prolific data-theft collective breaching SaaS platforms and consumer services, stealing large datasets that are later weaponized for credential-stuffing, account takeover and secondary compromises across the victim’s customer ecosystem.

Together, these groups highlight how modern cybercrime leverages identity weaknesses, vendor trust relationships and SaaS interconnectivity to cause cascading supply-chain and third-party risk. In mid-2025, the

three groups [formed an alliance](#), signaling a new level of organization in cybercrime. This development combined advanced social engineering, data theft and extortion tactics into coordinated, multi-stage attacks against high-value enterprise targets.

[NEXT: Actions on objective](#)

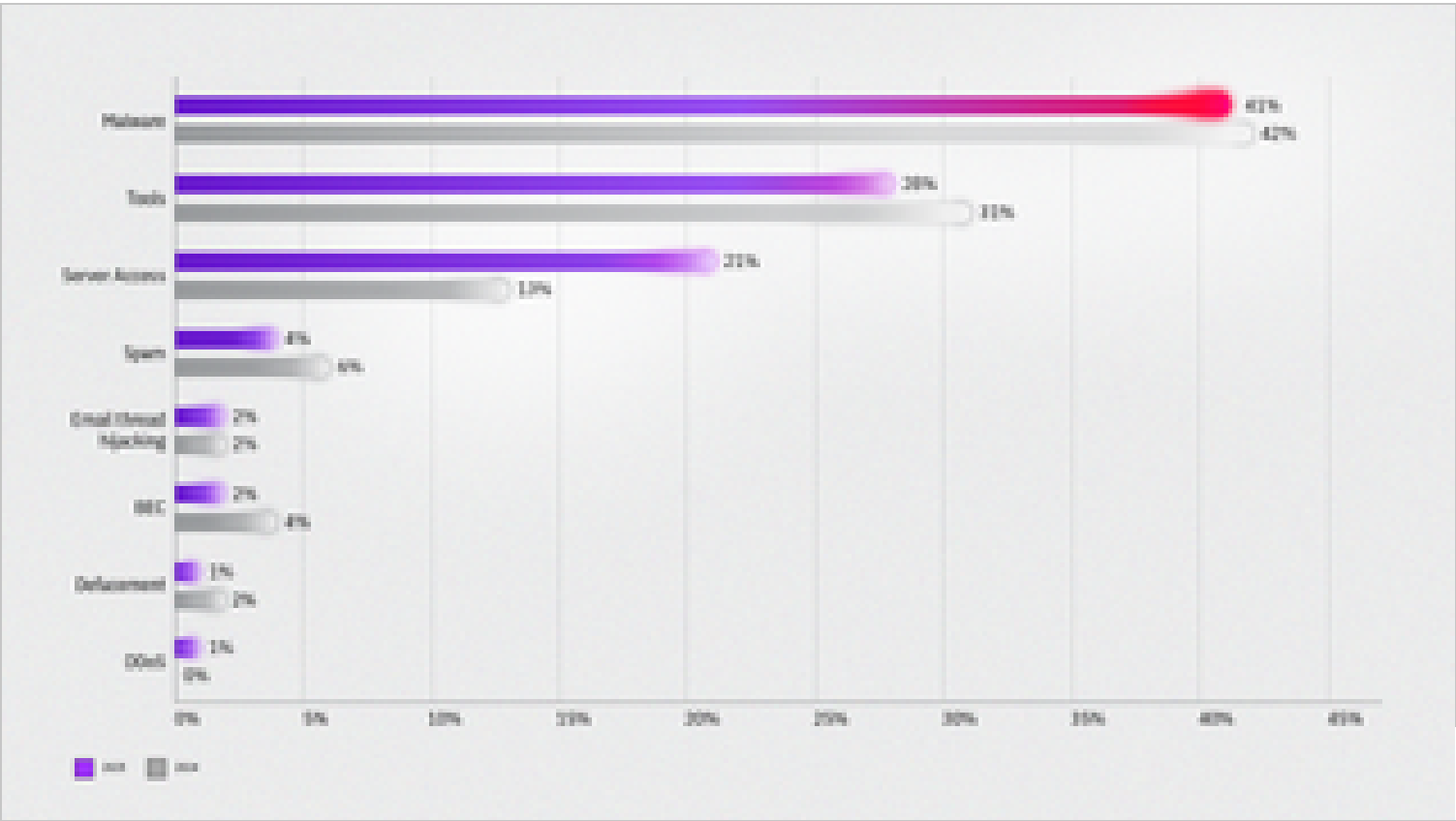
X-Force Threat Intelligence Index 2026

Actions on objective

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 41% of cases. Of all the malware cases, 18% included the deployment of ransomware, while another 18% deployed webshells. Infostealers and backdoors both made up 10% of malware cases.

The next most observed action on objective was the use of legitimate tools for malicious purposes, accounting for 28% of cases. This finding reflects utilization of hands-on-keyboard post-exploitation efforts and the deployment of utilities that allow for follow-up activities such as lateral movement and privilege escalation.



Top actions on objectives observed in 2025 compared to 2024. Source: IBM X-Force.

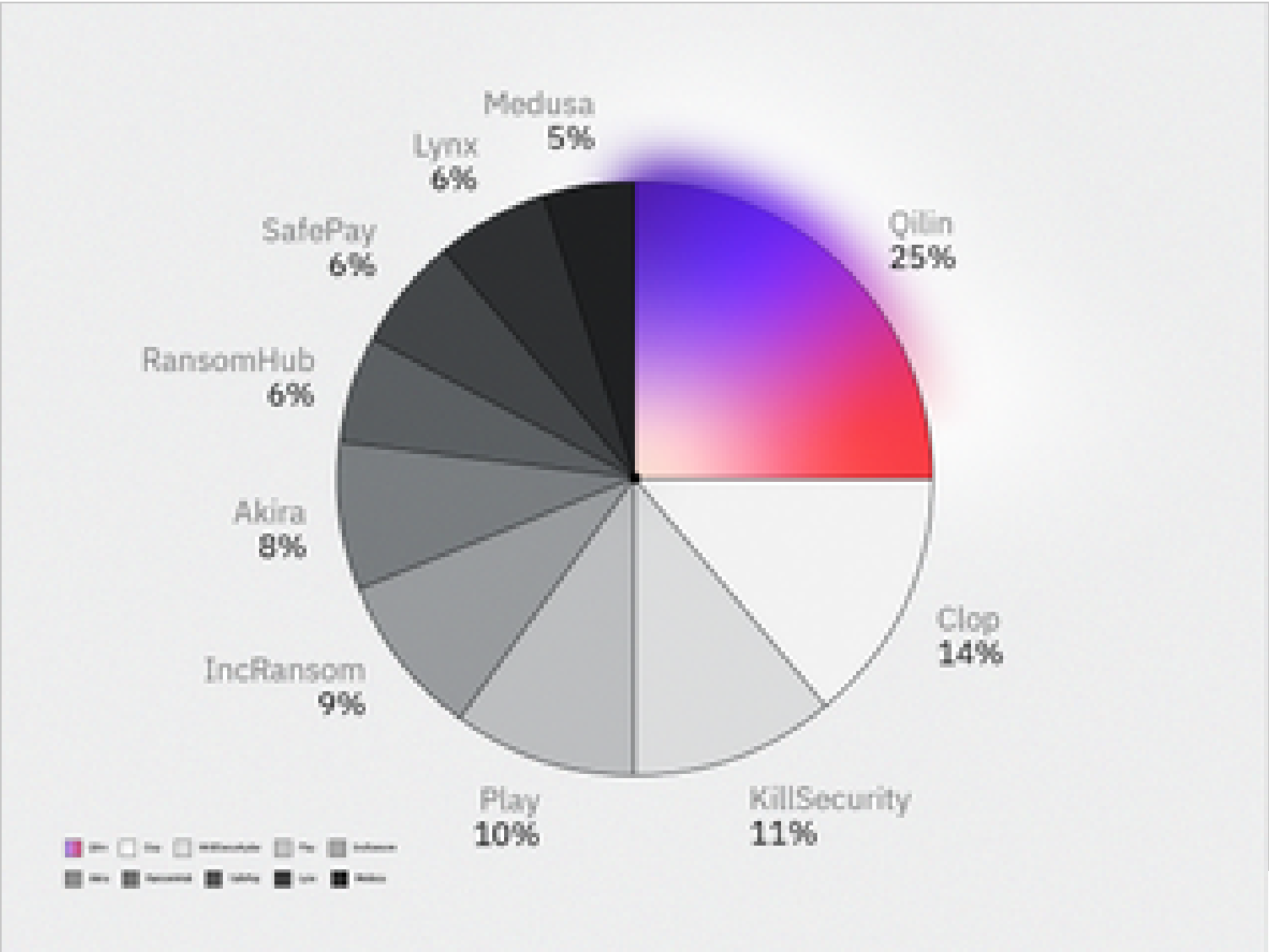
Ransomware landscape

The X-Force team’s review of dark-web activity indicated that Qilin, Clon, KillSecurity, IncRansom and Play were among the most active ransomware families over the past year. In 2025, Qilin was associated with the largest

share of discussed ransomware events, followed by Clop. A ransomware event on the dark web refers to an instance in which a threat actor claims to have impacted an organization.

The 2025 ransomware ecosystem has become highly fragmented and decentralized. We identified 109 active ransomware or extortion groups, with rapid turnover and an increasingly small portion of victims attributed to the top 10 groups. This fragmentation reflects a lower barrier to entry: actors frequently reuse leaked tooling, follow established playbooks or shift between group identities, enabling many small operators to conduct opportunistic, low-volume attacks. Victim counts on ransomware leak sites increased approximately 12% year over year.

Tactically, data extortion has become central, with groups exfiltrating sensitive information and threatening leaks alongside file encryption. Supply-chain intrusions are also rising, with compromised vendors driving widespread downstream impact. Small and mid-sized organizations are increasingly targeted due to weaker defenses and higher likelihood of operational disruption. Although law-enforcement takedowns disrupt major operations, they have not reduced overall activity. Smaller groups quickly fill the gaps, and several actors have reconsolidated into larger conglomerates—indicating a temporary shift from competition to cooperation within the ransomware ecosystem.



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. Source: IBM X-Force.

Infostealer landscape

The X-Force team continued to observe significant activity across both established and emerging infostealer families in 2025. Well-known stealers such as Lumma, RisePro, Vidar, Stealc and Rhadamanthys remained widespread, while newer families like Acreed expanded their presence in underground markets.

Although we observed an overall decrease in the number of infostealer events, this decline appears to be driven primarily by changes within Russian Market—a key forum for selling and distributing stolen credentials. Since November 2024, Russian Market-related activity dropped from 20,000–50,000 daily posts to roughly 9,000. This reduction reflects changes to the market’s own operations rather than a true decline in infostealer activity. Since February 2024, there have been intermittent spikes reaching 30,000 posts per day, but gaps in collection persist.

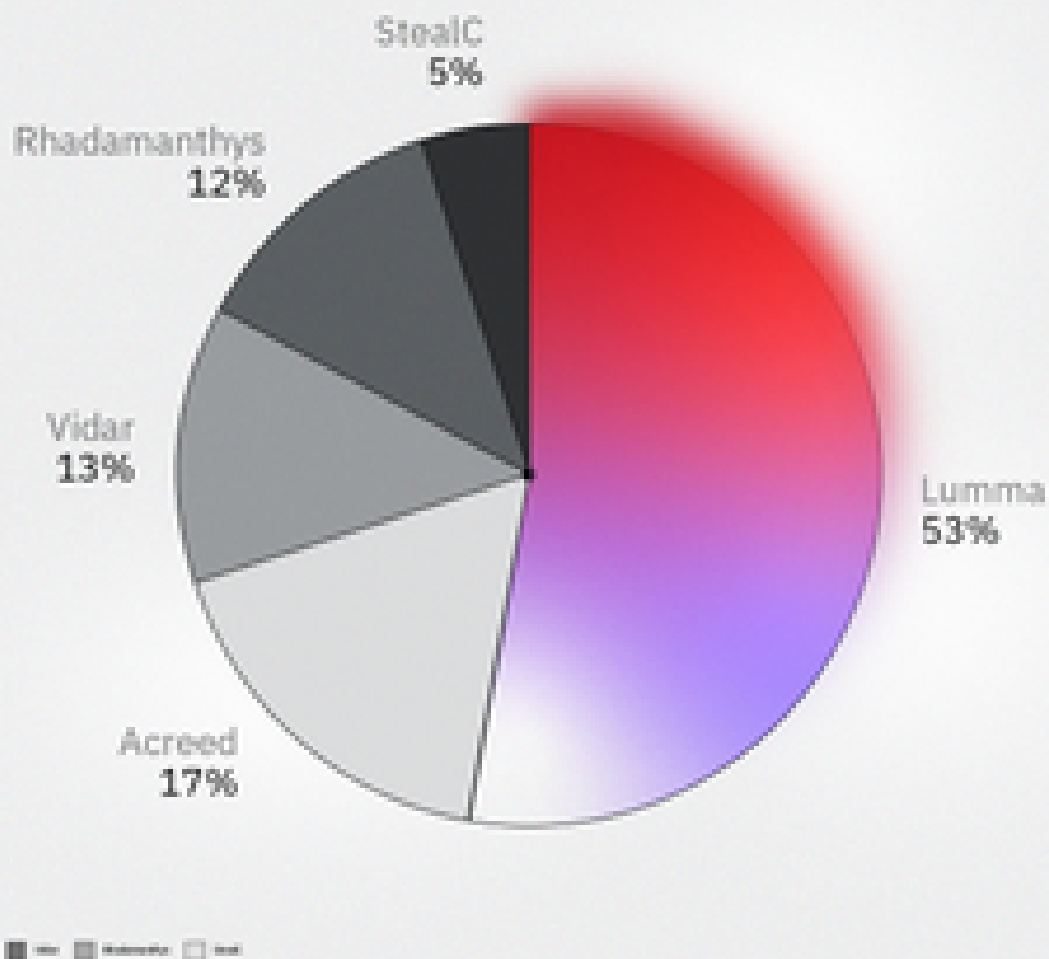
We observed several notable shifts in infostealer market share in 2025:

Lumma continued to dominate the ecosystem, maintaining roughly 50% of all observed activity.

Acreed and Rhadamanthys experienced significant growth, rising to approximately 16% and 11% of the market, respectively.

In contrast, Stealc’s share declined compared to 2024. This drop is likely tied to the timing of Acreed’s rapid expansion—Acreed gained visibility across major Telegram “malware-as-a-service” and trafficker recruitment channels just as Stealc’s distribution networks were weakening.

Instability within Russian Market favored stealers with diversified log-resale channels. Families like Acreed, which integrated directly with smaller credential marketplaces and private Telegram resale groups, were better positioned to capture market share amid these disruptions.



Top 5 infostealers seen on dark web forums based on credentials for sale. Source: IBM X-Force.

NEXT: The convergence of advanced persistent threats (APTs) and cybercriminal techniques

X-Force Threat Intelligence Index 2026

Blurring lines: the convergence of APT and cybercriminal techniques

Cybercriminals and nation-state actors are two distinct groups that conduct their operations based on each group's motivation. In addition to motivation, analysis of their campaigns often revealed distinct tools and techniques—combined with victimology—which often led to the attribution to one of the plethora of threat groups.

For the past several years, however, the traditional distinctions between nation-state groups and cybercriminals are becoming increasingly blurred as tactics, techniques and procedures (TTPs) from each respective group are being used by others:

North Korea nation-state actors are using [information stealers](#), once thought to be used largely by cybercriminals.

Silver Fox (also known as [Void Arachne or The Great Thief of Valley](#)), a China-based nation-state group, conducts both intelligence and [financially motivated](#) operations.

Russian cybercriminal groups have long thought to be in the employ of the Russian government, [according](#) to U.S. government officials.

This blurring presents a significant challenge for security professionals, as the similarities in TTPs muddies the evidence gathered when responding to an incident, and may lead organizations to miss opportunities to take appropriate actions.

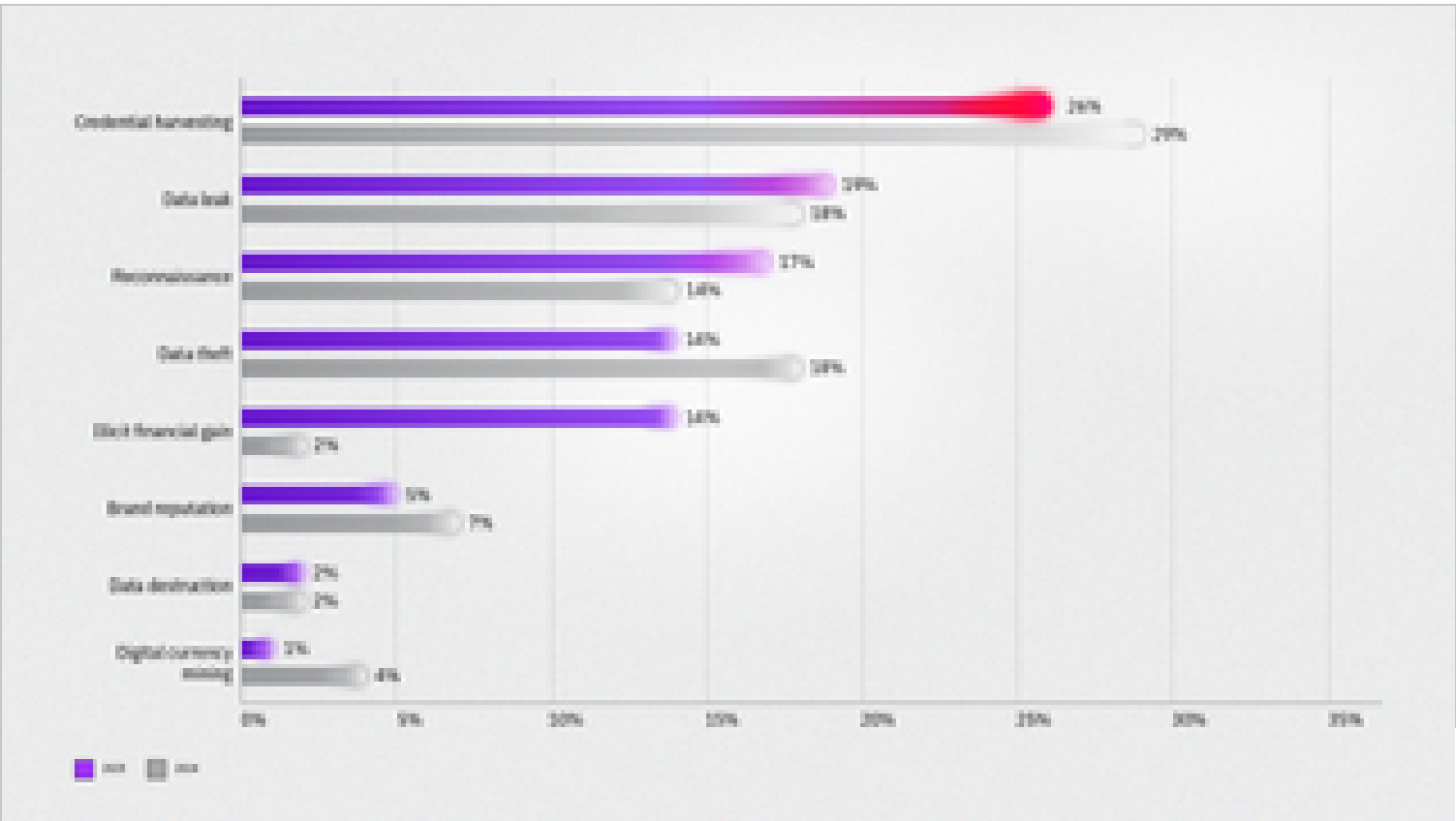
These missed opportunities may have dire consequences. X-Force observed network alerts triggered by seemingly commodity malware, which later turned out to be part of an advanced persistent threat (APT) operation. In the age of AI and automation, focusing solely on artifacts or alerts without consideration to broader context or insights may result in missed attribution or worse: a breach may go undetected as APT actors will often persist.

[NEXT: Impact](#)

X-Force Threat Intelligence Index 2026

Impact

The distribution of cybercrime impacts reveals most attacks are driven by data-centric and credential-focused objectives rather than direct system disruption.



Top impacts X-Force observed in incident response engagements in 2025 vs. 2024 (more than 1 response permitted). Source: IBM X-Force.

Credential harvesting (26%) and data leaks (19%)

Credential harvesting and data leaks lead the way, indicating attackers primarily seek to gain access to sensitive systems and exfiltrate valuable information. This trend underscores the persistent exploitation of weak identity management and insufficient data protection controls.

Reconnaissance (17%)

Reconnaissance suggests a significant portion of activity involves preparatory stages, where adversaries map networks and identify vulnerabilities before launching more damaging attacks.

Illicit financial gain (14%) and data theft (14%)

The presence of illicit financial gain and data theft highlights ongoing monetization motives, whether through resale of stolen data or direct financial fraud.

Brand reputation damage (5%), data destruction (2%) and digital currency mining (1%)

These impacts are less frequent, but still carry severe consequences when they occur.

These figures imply organizations must prioritize identity security, data protection and threat detection capabilities. Strengthening authentication mechanisms, monitoring for data exfiltration and improving visibility into reconnaissance behaviors can significantly reduce exposure. Moreover, the relatively lower but still impactful instances of reputation damage and data destruction emphasize the need for robust incident response and business continuity planning to minimize long-term fallout when breaches do occur.

[NEXT: Security 101: still lacking](#)

X-Force Threat Intelligence Index 2026

Security 101: still lacking

Organizations continue to face security incidents not due to sophisticated adversary techniques, but because foundational security controls are often inconsistently implemented or poorly maintained.

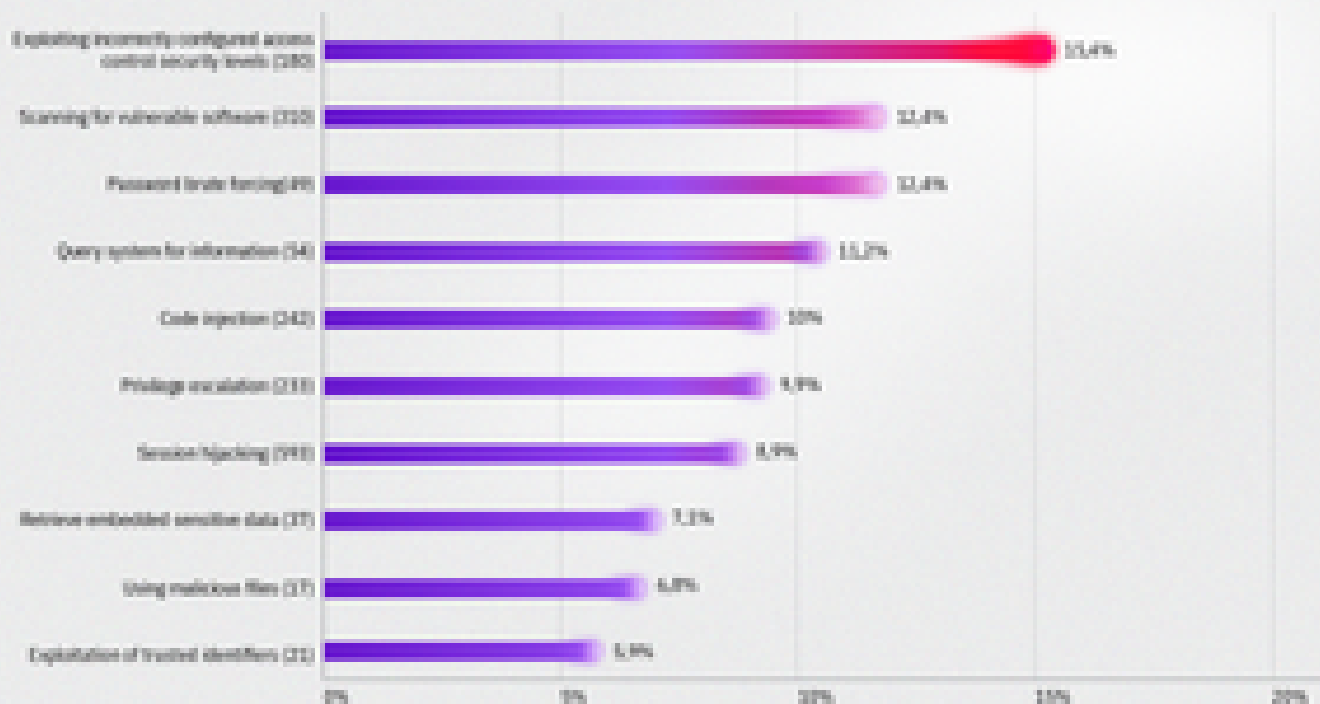
Basic measures such as comprehensive logging, timely patching, proper access management and secure configuration of deployed technologies are often neglected or only partially enforced. In some cases, critical security tools are installed without proper tuning, leaving misconfigurations and visibility gaps that undermine their intended effectiveness. These operational shortcomings rather than advanced threat capabilities can provide adversaries with the opportunity to establish and maintain access. Strengthening adherence to core cybersecurity hygiene remains essential to reducing overall risk.

Understanding how these issues are exploited in practice requires insights from real-world adversarial testing. X-Force Red, an elite team of hackers and researchers, conducts exercises which provide a glimpse into many of the methods that attackers can use to exploit vulnerabilities in victim environments. To best organize the findings, we have categorized the results of their penetration testing engagements into the MITRE Corporation's Common Attack Pattern Enumeration and Classification (CAPEC) framework.

Organizations continue to face security incidents not due to sophisticated adversary techniques, but because foundational security controls are often inconsistently implemented or poorly maintained.

CAPEC was designed to standardize how to describe, analyze, and reason about attacker behavior. It provides a public, structured catalog of attack patterns that adversaries repeatedly use to exploit systems, people and processes. The goal is to capture how attacks work at a conceptual and operational level, independent of any specific vulnerability, exploit or campaign.

The following chart lists the top ten attack patterns discovered by X-Force Red in 2025.



Top 10 attack patterns discovered by X-Force Red in 2025. Source: IBM X-Force.

The frequency of these CAPEC attack patterns highlights significant systemic weaknesses in access control, credential management and software configuration.

The high occurrence of exploiting incorrectly configured access control security levels (CAPEC-180) suggests misconfigurations remain a primary entry point for attackers, indicating persistent gaps in governance and enforcement of security policies.

The prominence of password brute forcing (CAPEC-49) and scanning for vulnerable software (CAPEC-310) reflects widespread exposure due to weak authentication practices and insufficient vulnerability management.

Frequent instances of query system for information (CAPEC-54) and code injection (CAPEC-242) reveal ongoing issues with information disclosure and insecure coding, which can facilitate further compromise.

Patterns such as privilege escalation (CAPEC-233) and session hijacking (CAPEC-593) demonstrate once attackers gain a foothold, they are able to move laterally and maintain persistence, amplifying the impact of initial breaches.

Collectively, these trends indicate organizations face compounded risks from both preventable technical flaws and operational oversights. This finding underscores the need for stronger configuration controls, proactive vulnerability management and secure development practices to mitigate recurring exploitation paths.

[NEXT: AI in offensive cybersecurity](#)

X-Force Threat Intelligence Index 2026

AI in offensive cybersecurity

Artificial intelligence is no longer an emerging concept in cybersecurity. It's a force multiplier actively used by both defenders and adversaries. Threat actors are already applying generative AI to scale phishing operations, accelerate malicious code development and enhance social engineering through improved language quality and realism. At the same time, defenders are using AI-driven analytics to process vast volumes of telemetry, identify anomalous behavior and shorten detection and response timelines.

However, it's important to acknowledge AI has not changed the fundamentals of cyberattack campaigns. Attackers still rely on unpatched vulnerabilities, valid credentials and misconfigurations to accomplish their goals. What AI has changed is the speed, scale and efficiency of these attacks, which serve to make rapid detection and decisive response more important than ever.

In the near term, AI is reshaping attacker operations by compressing decision cycles and enabling faster experimentation during active intrusions. Adversaries increasingly use AI to accelerate research, analyze large data sets and iterate on attack paths in real time, allowing them to adjust tactics as conditions change rather than relying on static, preplanned actions. This operational flexibility increases dwell-time risk and places greater strain on security teams that depend on fixed rules, signatures or delayed analysis to detect malicious activity.

What starts with AI-assisted impersonation and language manipulation often escalates into something far more consequential. Multimodal systems have the ability to extend these advantages beyond social engineering into technical intrusion workflows. As multimodal AI models mature, adversaries will be able to automate increasingly complex tasks—including reconnaissance, privilege escalation and lateral movement—creating faster moving, more adaptive threats.

The most substantive transformation underway is not the creation of brand new attack methods, but the democratization of advanced capability, where less experienced or poorly resourced groups can now execute operations that previously required deep expertise.

AI also provides advantages to attackers through asymmetric adoption. Adversaries face fewer constraints related to governance, safety and accountability, potentially allowing them to adopt and operationalize new capabilities faster than most enterprises. As a result, defensive use of AI does not automatically provide an advantage. Without high-quality data, mature processes and clear integration into security operations, AI-driven defenses can struggle to keep pace with adversaries who can rapidly test, discard and refine techniques without oversight.

[NEXT: Geographic trends](#)

X-Force Threat Intelligence Index 2026

Geographic trends

A regional analysis of X-Force Incident Response engagements reveals where cyber vulnerabilities are most prominent across the globe. North America emerges as the most affected region, representing 29% of all incidents to which X-Force responded. This metric reflects the region's economic scale, concentration of high-value industries and continued targeting by both financially motivated and state-sponsored threat actors.

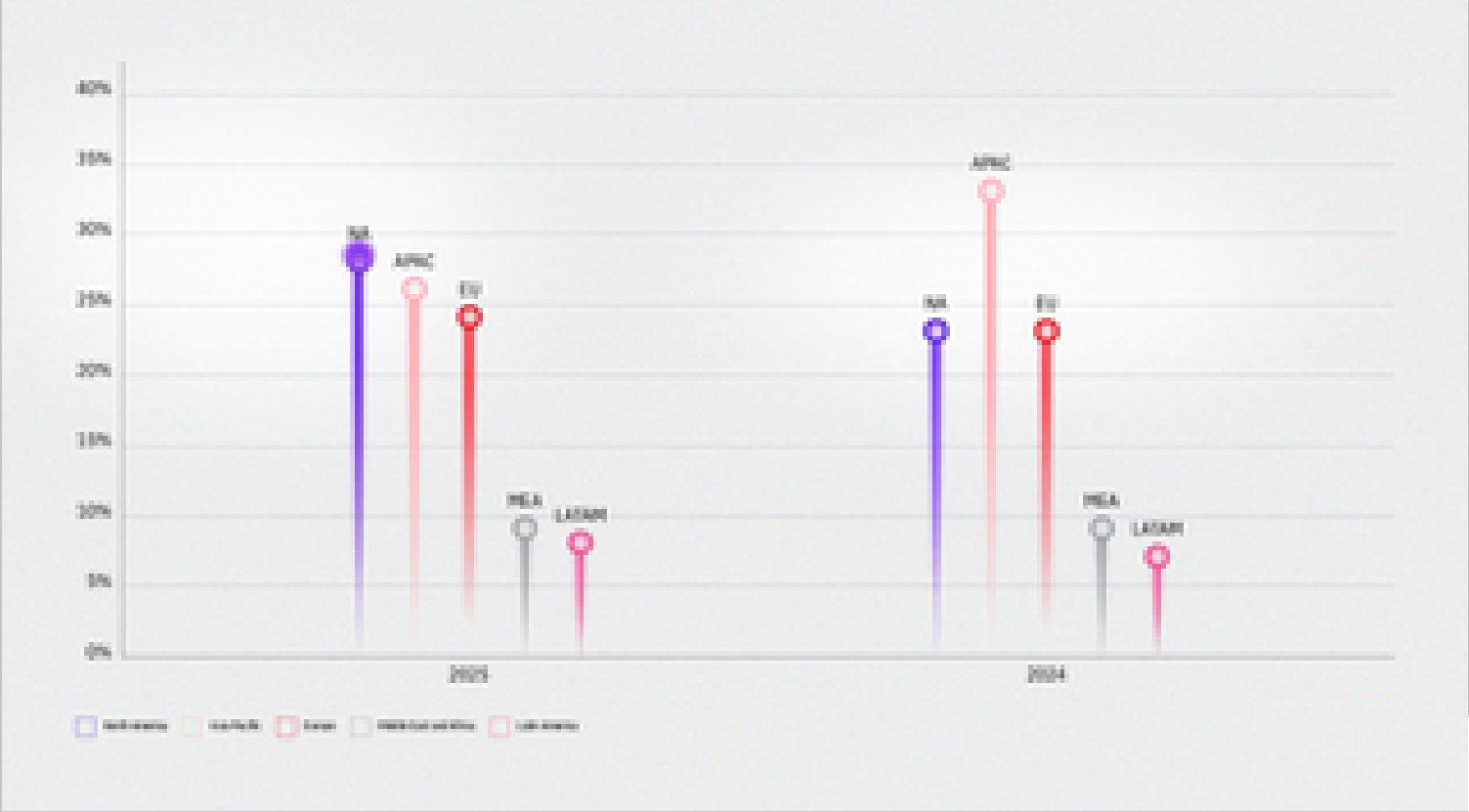
Asia-Pacific follows at 27%, reflecting the region's role as a nexus of global manufacturing, logistics and technological innovation. Its rapid digital expansion—paired with ongoing geopolitical tension—makes it an attractive environment for threat actors seeking strategic, financial or disruptive outcomes.

Europe, representing 25% of incidents, remains a consistent focal point. Its advanced economic landscape and concentration of essential sectors—from finance to industrial operations—create a diverse attack surface that continues to appeal to sophisticated adversaries.

The Middle East accounts for 10% of incidents, illustrating the pressures faced by a region balancing ambitious digital transformation efforts with persistent regional conflict. These dynamics contribute to recurring exposure to advanced threats, including espionage-focused campaigns and targeted attacks on critical infrastructure.

Latin America, at 9% of incidents, shows a slightly increasing share of global cyber activity. As organizations across the region expand their digital capabilities, they often do so in environments where cybersecurity practices are still maturing, creating openings frequently exploited by opportunistic and financially driven attackers.

Together, these regional patterns offer a global perspective on how threat actors distribute their efforts and underline the importance of region-specific intelligence, stronger international cooperation and ongoing investment in cyber resilience.



Share of incidents by geographic region in 2025 and 2024. Source: IBM X-Force.

North America – 29%

In 2025, the North America region ranked first in terms of incidents investigated, accounting for 29% of incidents. The most common actions on objective included malware and the use of legitimate tools (33% each), and server access (26%), signaling attackers’ focus on system control and persistence. The primary initial access vector was exploitation of public-facing applications (28%), followed by exploitation of valid accounts - local (22%).

When looking at regional impacts, credential harvesting (43%) dominated incidents, followed by data theft and data leaks (29%). The manufacturing sector was the most targeted, representing 21% of all incidents investigated, while wholesale (19%) and the finance and insurance sector (17%) followed behind, also facing significant threats.

Asia-Pacific – 27%

The Asia-Pacific (AP) region ranked as a close second, accounting for 27% of global incidents. Attackers frequently employed malware (45%), spam (15%), legitimate tools (15%), and server access (10%) as their

primary actions on objective. The extensive reliance on exploitation of public-facing applications (50%) and valid accounts (30%) as initial access vectors underscored vulnerabilities in AP's digital infrastructure.

Key impacts in the region included data theft (14%), brand reputation (14%) and credential harvesting (7%), reflecting the sector's susceptibility to attacks targeting sensitive data and operational disruption. The manufacturing sector remained the most targeted industry, representing 65% of incidents, followed by finance and insurance (17%) and transportation (7%).

Europe – 25%

Europe ranked as the third most targeted region in 2025, accounting for 25% of incidents. Malware (43%), legitimate tools (26%) and server access (26%) were the most common actions on objectives observed, with attackers leveraging exploitation of public-facing applications (40%) as the leading initial access vector.

Credential harvesting (40%) was the dominant impact, followed by data leak (27%) and data theft (13%), showcasing the attackers' continued focus on monetizing sensitive information. The finance and insurance sector led with 39% of incidents, followed by professional, business, and consumer services (18%) and retail (13%).

Middle East and Africa – 10%

The Middle East and Africa region accounted for 10% of global incidents, maintaining its position as the fourth most targeted region. Attackers predominantly employed malware (34%), legitimate tools (34%), and server access (17%), reflecting a focus on achieving stealthy persistence and leveraging existing system capabilities to expand access while minimizing detection.

The leading initial access vector was exploitation of public-facing applications (50%), highlighting vulnerabilities in exposed infrastructure across the region. Phishing or spear phishing attachment (15%) also played a significant role, underscoring the continued reliance on social engineering to compromise systems.

The finance and insurance sector remained the most-targeted industry, representing 38% of incidents, reflecting the region's growing financial landscape and associated risks. Additionally, the energy industry (38%) tied for the most-targeted industry in the region.

Latin America – 9%

Latin America accounted for 9% of incidents in 2025. Attackers frequently used legitimate tools (33%), server access (11%) and malware;ransomware (11%), reflecting a focus on maximizing disruption and financial gain.

The four initial access vectors observed (25% each) were exploitation of public-facing applications, valid accounts, external remote services and supply chain compromise.

The leading impact was credential harvesting (40%), with brand reputation damage (20%) also observed. The finance and insurance sector led with 47% of incidents, followed by energy (27%).

[NEXT: Industry trends](#)

X-Force Threat Intelligence Index 2026

Industry trends

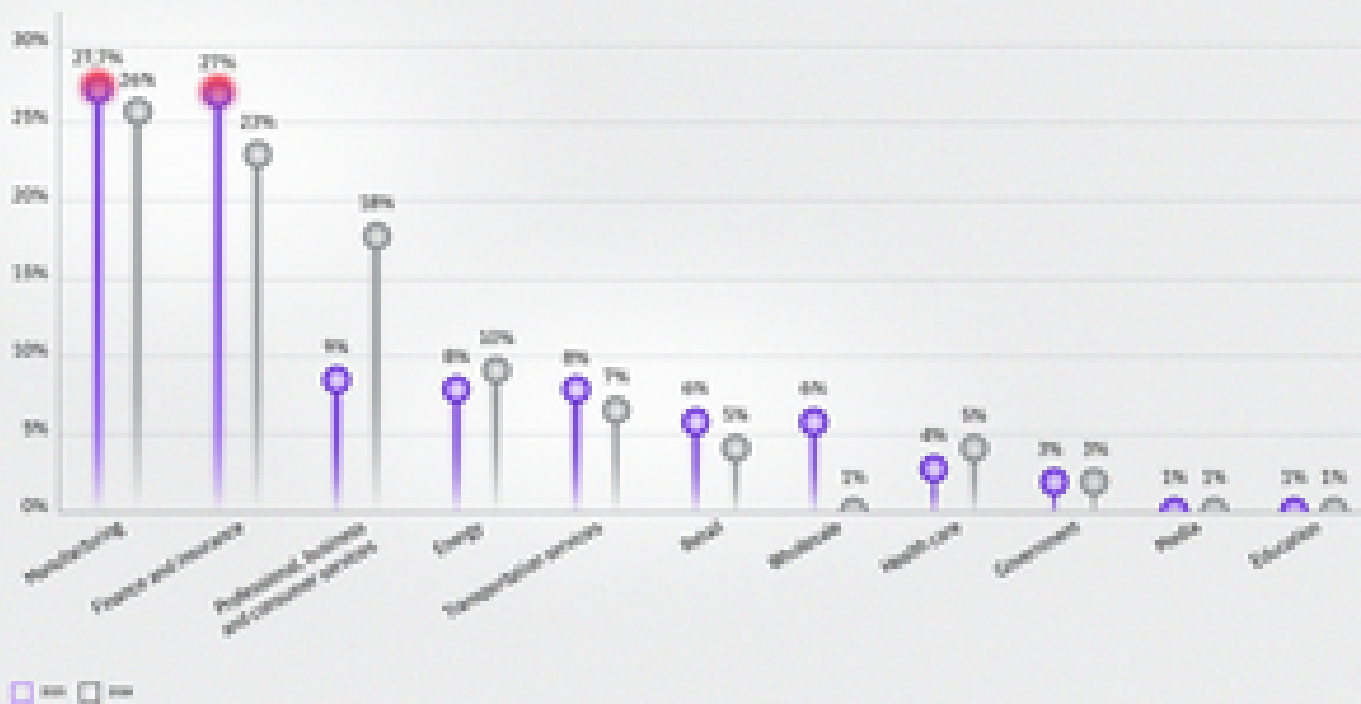
An analysis of X-Force Incident Response engagements highlights the industries most impacted by cyberattacks in 2025.

Manufacturing remained the most-targeted sector, representing 27.7% of all incidents. Its reliance on interconnected supply chains, valuable intellectual property and complex operational technology environments continues to make manufacturing a prime focus for threat actors.

Following close behind, the finance and insurance sector accounted for 27% of incidents, reflecting persistent adversary interest in financial data, capital access, and extortion opportunities.

Professional, business, and consumer services accounted for 9% of incidents, reflecting growing exposure tied to third-party service operations, supply chain integration and customer-facing platforms. Both the energy and transportation services sectors each represented 8% of incidents, underscoring persistent risks to critical infrastructure, industrial control systems and logistics networks, as these industries continue to digitize core operations.

These patterns illustrate how threat actors gravitate toward industries with valuable data, operational complexity and opportunities to create financial or strategic disruption. Addressing this landscape requires organizations to implement tailored risk assessments, enhance security investments aligned to industry needs and strengthen cooperative defense efforts across partners and supply chains. By doing so, critical sectors can better withstand emerging threats and build more durable cyber resilience.



Share of incidents by industry in 2025 and 2024. Source: IBM X-Force.

Manufacturing: 27.7%

For the fifth consecutive year, the manufacturing sector remained the most attacked industry, representing 27.7% of all incidents within the top industries. This ongoing targeting reflects 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 (32%) emerging as the most common vector. Valid accounts (domain) (16%) and external remote services (11%) were also prominent, reflecting attackers’ reliance on exploiting misconfigured or insufficiently secured access points.

After gaining access to manufacturing environments, attackers focused on establishing control, compromising systems or exfiltrating valuable data. Malware accounted for 45% of observed actions on objective, indicating a strong emphasis on operational disruption and financial extortion. The use of legitimate tools (31%) also stood out, showcasing the value of compromised access in enabling further attacks.

Manufacturing organizations experienced significant impacts from these attacks. Data theft (40%) was the most prevalent, targeting both financial assets and intellectual property such as trade secrets. Credential harvesting (10%) further increased risks, enabling persistent attacker access. The sector also faced

challenges with brand reputation damage (20%), which underscores the broader business and social consequences of cyber incidents.

The Asia-Pacific region continued to be the epicenter of manufacturing-related incidents, accounting for 68% of attacks. North America (23%) followed as the second most impacted region, reflecting the economic significance of its manufacturing operations. Europe (5%) and Latin America (2%) also faced activity, with a slight decrease over the past year.

Manufacturing remained the most-targeted sector at 27.7%, but finance and insurance was a close second at 27%.

Finance and insurance: 27%

The Finance and insurance sector ranked as the second most attacked industry for the fifth year in a row—trailing only manufacturing—and accounted for 27% of all incidents in 2025. The sector continued to be a high-value target given its critical role in the global economy and the significant value of its financial data and assets.

Attackers primarily breached finance and insurance systems through exploiting public-facing applications (36%). Valid accounts (domain) (14%) and external remote services (14%) were also common tactics, highlighting the need for robust credential and access management practices, as well as monitoring remote access vulnerabilities.

Once attackers were inside, the focus was on reconnaissance and data exfiltration. The most observed action on objective was the deployment of malware (54%) and the use of legitimate tools (29%).

The sector faced substantial impacts from these incidents. Credential harvesting (46%), and data leaks (31%) were the most common, with attackers focusing on stealing and leaking sensitive information and compromising account credentials. Other impacts, such as brand reputation (15%), highlighted additional attempts to tarnish brand identity and overall reputation within the sector.

Regionally, Europe experienced the highest volume of incidents (35%), likely driven by the region’s concentration of major financial institutions, regulatory complexity across jurisdictions and its central role in global financial markets. The Asia-Pacific (19%) region followed, driven by its economic growth and expanding digital footprint. North America (19%) also remained a major target this year, tying the Asia-Pacific region. Latin America (16%) faced notable activity with fewer cases compared to the prior year, while the Middle East and Africa only experienced 12% of incidents in 2025.

Professional, business and consumer services: 9%

The professional, business, and consumer services sector ranked as the third most attacked industry for the second year in a row, accounting for 9% of all 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 its reliance on sensitive data and operational dependencies.

Attackers employed varied tactics to achieve their objectives, with malware (50%) emerging as the most common action observed. Server access (25%) and email thread hijacking (25%) were also prominent, reflecting attackers' interest in establishing control and enabling further malicious activity.

Exploiting public-facing applications (33%), external remote services (33%) and drive-by compromise (33%) were the three initial access vectors affecting this industry.

The primary impact of these incidents was data theft (33%), emphasizing the attackers' intent to exfiltrate and monetize sensitive data. Credential harvesting (17%), data leak (17%), extortion (17%) and data destruction (17%) also highlighted the financial and reputational risks posed to organizations in this sector.

Regionally, Europe experienced the highest volume of incidents, accounting for 50% of cases, followed by North America (21%) and Asia-Pacific (14%). Activity in the Middle East and Africa (7%) and Latin America (7%) was lower, reflecting regional disparities in targeting and attacker focus.

Energy: 8%

The energy sector—which includes electric utilities, oil and gas companies, and related industries—ranked as the fourth most targeted industry, accounting for 8% of all incidents. Energy infrastructure remained a persistent target due to its critical role in sustaining global operations and the outsized impact even limited disruptions can cause.

Attackers employed a diverse range of tactics, with server access (29%) and malware (29%) among the most observed actions on objectives. Additional techniques included business email compromise, defacement and use of legitimate tools (14% each), showcasing a broad spectrum of strategies aimed at gaining access and control, stealing data and monetizing breaches.

The primary initial access method used was exploitation of public-facing applications (50%). There was also an equal distribution across additional access vectors such as trusted relationships, supply chain compromise (software supply) and phishing (spearphishing) (17% each). This distribution highlights attackers' adaptability and their focus on exploiting human error and vulnerabilities in exposed systems.

Concerning the impact on the energy industry, there is an equal split between credential harvesting and data leaks.

The Asia-Pacific region experienced the highest volume of incidents, accounting for 27% of cases, with Europe following behind in second place at 22%. Other regions, including Latin America (17%), North America (17%) and the Middle East and Africa (17%), saw an even distribution of attacks, emphasizing the global nature of threats to energy infrastructure.

Transportation: 8%

The transportation sector was the fifth most-attacked industry in 2025, accounting for 8% of all incidents. This finding reflects the sector's critical role in global logistics, commerce, and infrastructure, making it a target for both financially motivated attackers and those seeking to disrupt operations.

Malware (60%) was the most important action on objective for the industry, followed by a tie for second place by spam and business email compromise (20% each).

The two attack vectors observed for this industry were exploitation of public-facing applications and valid accounts (50% each).

The transportation sector faced significant impacts, with data leaks (100%) being the sole impact observed, reflecting attackers' interest in monetizing sensitive information.

Regionally, Europe experienced the highest volume of incidents, accounting for 42% of attacks, followed by Asia-Pacific (25%), North America (25%) and Latin America (8%). The concentration of incidents in Europe reflects the region's growing prominence in global transportation and logistics, as well as its expanding attack surface.

Retail: 6%

The retail sector accounted for 6% of incidents in 2025, a very slight increase from the prior year. Retailers' heavy reliance on digital infrastructure to store consumer data and process transactions continued to make the sector an attractive target for financial gain or operational disruption.

Attackers employed a range of tactics, with server access and the use of legitimate tools (38% each) as the most observed actions. Email thread hijacking and malware (13% each) followed. These methods highlight attackers' focus on both accessing and exploiting sensitive systems for further financial or operational gain.

The primary initial access vector was exploitation of public-facing applications (43%), underscoring the importance of securing internet-exposed services and promptly remediating vulnerabilities to prevent unauthorized access. Additional notable initial access vectors include valid accounts (cloud), valid accounts (local), valid accounts (default) and external remote services (14% each). Credential harvesting (100%) also dominated the impact on this sector, showing the increase in attackers monetizing stolen data.

Regionally, Europe (50%) experienced the highest proportion of retail-related incidents, followed by North America (40%) and Asia-Pacific (10%). This distribution underscores the concentration of threats in regions with a large volume of retail activity and digital infrastructure.

Wholesale: 6%

The wholesale sector accounted for 6% of incidents in 2025, representing a six-fold increase over the previous year. 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.

Server access (29%) was the most common action on objective, closely followed by the abuse of legitimate tools and malware (28% each). Attackers employed two primary initial vectors in wholesale incidents: valid accounts (local) (50%) and phishing (spearphishing via service) (50%), highlighting a focus on diverse and potentially tailored attack methods.

Credential harvesting was the sole impact observed affecting this industry directly. Regionally, incidents were only observed in North America (100%), underscoring a geographically concentrated threat landscape within this sector.

Healthcare: 4%

The healthcare sector accounted for 4% of all incidents, dropping from seventh place last year to eighth this year. Despite its lower ranking, the sector remains a high-value target due to its dependence on sensitive patient data, the need for uninterrupted operations and the prevalence of legacy systems.

Attackers predominantly focused on malware (50%) as well as server access and legitimate tools (25% each) 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 sole initial access vector observed was exploitation of public-facing applications (100%), emphasizing the risks posed by exposed systems and the urgent need for robust vulnerability management practices.

Regionally, North America (57%) experienced the highest volume of healthcare-related incidents, followed by Asia-Pacific, Europe and Latin America (14% each), indicating a significant concentration of threats in regions with advanced healthcare infrastructure.

Government: 3%

The government sector accounted for 3% of all incidents in 2025. Despite the sector’s lower incident rate, 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 server access (50%) and tool (credential acquisition) (50%) as their primary actions on objective, reflecting a focus on exploiting vulnerabilities and obtaining authentication data to expand their foothold within targeted environments. These techniques highlight the sector’s ongoing exposure to methods that enable unauthorized access and facilitate subsequent operational disruption or data theft. The two observed initial access vectors were evenly split between valid accounts (local) and phishing (spearphishing attachment) (50% each), showcasing attackers’ ability to exploit credential mismanagement and human error to infiltrate systems.

Regionally, North America (80%) experienced the highest volume of government-related incidents, followed by the Middle East and Africa (20%), reflecting the strategic importance of government entities in these regions and their prominence as targets for cybercriminals and nation-state actors.

[NEXT: Recommendations](#)

X-Force Threat Intelligence Index 2026

Recommendations

Cyber adversaries continue to achieve scale and impact by exploiting fundamental weaknesses in identity, access control and credential management, rather than relying on highly sophisticated or novel techniques. While attack tooling and automation have advanced, the underlying conditions enabling compromise remain largely unchanged.

Once access is established, attackers consistently pursue credential harvesting, privilege escalation and session hijacking, enabling lateral movement across hybrid, cloud and SaaS environments. This activity was further amplified—according to this year’s report data—by the fact that more than half of vulnerabilities disclosed required no authentication, allowing attackers to gain footholds without bypassing identity controls altogether.

What’s more, the exposure of AI chatbot credentials on underground markets demonstrates AI platforms have rapidly become part of the enterprise identity attack surface. Although the credentials observed were no longer valid, their consistent association with infostealer malware underscores the growing risk posed by unmanaged credentials and poor identity hygiene across SaaS and AI ecosystems.

At the same time, a nearly 4-fold increase in major supply-chain and third-party breaches over the past 5 years reflects adversaries’ increasing reliance on compromised identities, shared credentials and over-trusted integrations to gain access and maintain persistence.

Given these trends, how should organizations respond, and where should they start? And how can they turn security into a true business advantage, and not just a risk mitigation effort?

Prepare for AI-accelerated attacks—where speed, scale, and automation break traditional defenses

As threat actors use AI to put pressure on security teams—scaling their phishing campaigns, speeding up malicious code creation and fine-tuning social engineering—security leaders need a proactive rather than reactive approach to these threats. They should future-proof their organizations with AI-driven, end-to-end security.

This “shift left” strategy—from a reactive, tactical response to a proactive plan—means first gaining a holistic view of the rapidly evolving threat landscape, incorporating the latest threats and the broader context and insights into their plan.

These insights can be provided by security partners, using [agentic-AI powered threat detection and response](#), and preparing for [post-quantum threats](#). This shift-left action must also include a strong foundation of risk management, assessment and posture. With AI Security Posture Management (AISPM), organizations can gain greater

visibility and protection for AI-powered applications across cloud environments, enabling organizations to monitor and govern AI assets while safeguarding deployments against threats such as data poisoning and adversarial attacks.

Shifting left should also take into account an organization's business context—and its risk appetite. It should prioritize securing critical assets and data by business impact, [understanding adversary motivations and capabilities](#), and identifying and actively managing supply-chain and third-party dependencies.

The recent rise of [autonomous security operation centers](#), which use agentic AI to augment the roles of security workers, can orchestrate multiple agents to work across the entire threat lifecycle—from threat hunting to remediation—giving organizations the tools they need to detect and mitigate increasingly complex AI-generated attacks.

Monitor human and non-human identities—and detect threats—with AI

For organizations, protecting identities has always posed a challenge. It's about to get harder. As attackers fine-tune their credential-driven operations, IT and security leaders must turn to AI to help them gain visibility into identity-based risks and threats across their IT landscape. By combining AI-powered [identity threat detection and response](#) (ITDR) and [identity security posture management \(ISPM\) services](#) and solutions, organizations can move more quickly and efficiently to identify vulnerabilities and prevent attacks from happening.

If it still needs saying: identity must be treated as critical infrastructure. Security leaders who haven't already should elevate their identity systems to the same level of resilience, governance and monitoring as core infrastructure components.

If it still needs saying: identity *must* be treated as critical infrastructure. Given the sensitivity of AI-driven data and agentic workflows, security leaders who haven't already should [elevate their identity systems](#) to the same level of resilience, governance and monitoring as core infrastructure components. They should centralize identity access management and governance across workforce, customer, partner and machine identities.

They should also apply continuous, risk-based access controls informed by context such as user behavior, device posture and workload characteristics. This shift will also require specialized threat-hunting capabilities, AI-specific protections and infrastructure-level security controls to defend against increasingly sophisticated external attacks.

Embed identity controls in application and API security

Beyond the risk of compromised credentials, the rise in vulnerabilities not requiring authentication shows the importance of integrating identity [directly into application architectures](#).

To secure those architectures, security teams should provide strong authentication and authorization enforcement for public-facing and internal applications, APIs and service-to-service communications. Identity-aware access policies should be used to limit exposure and prevent application-level exploits from escalating into broader compromise.

Test and hunt for vulnerabilities

There's nothing attackers like more than an overlooked or ignored vulnerability. Fortunately, security leaders know how to handle this—by getting back to foundational, first principles. That means adopting a continuous, proactive approach to identifying weaknesses across environments, such as looking for:

- Insecure code
- Weak or reused credentials
- Misconfigurations
- Unauthorized changes
- Insecure defaults
- Risky user behavior
- Missing patches

If an attacker does break through, here are three things that can help prevent an initial exploitation from progressing into credential harvesting or data exfiltration: proactive remediation, strong configuration hygiene and continuous monitoring of application behavior.

Regular [penetration testing](#) across the full technology stack—including applications, networks, cloud infrastructure, AI models, mainframes, hardware and even personnel—is also needed to uncover vulnerabilities and configuration gaps that could lead to unauthorized access or exposure of sensitive systems and data.

Prioritize AI platform security

AI chatbots and agentic workflows must be secured and governed with the same—or even greater—rigor as other enterprise SaaS platforms. Too often, in the high-pressure rush to deploy, this is not what happens. That's a problem because the risks and threats from AI present significant challenges for organizations.

Agentic AI has [introduced new risks, and amplified others](#). Security leaders need a comprehensive AI governance solution to scale AI with trust and transparency, and in a way that generates value. To avoid vendor lock in, the solution should be open, hybrid and platform-agnostic, meaning organizations can use the right model for the right use case, and deploy their AI where it makes the most sense.

[Model governance](#) allows for evaluation of underlying AI, to test for performance, accuracy and safeguard against inappropriate behavior. Keeping up with regulations that pertain to the use of AI is critical to maintain compliance and reduce risk.

Organizations should assess AI adoption across the enterprise, including enforcing strong authentication and conditional access controls, securing AI systems, protecting AI service credentials and tokens, and monitoring for abnormal access patterns or credential exposure.

Map your footprint and track the signals that attackers watch

Security misconfigurations, data breaches, and plain old human error can lead to the public exposure of an organization's valued brand, domain, IP addresses or client-specific assets. This highlights the risk that resides outside your network perimeter's control. Security teams should work with a trusted partner to [identify the exposure](#) of these valuable assets across the public-facing surface web, the unindexed deep web and black-market sites on the dark web. These specialized services include monitoring capabilities for credential theft, suspicious domains, CVEs and security bulletins.

Accelerate data security

As data and AI play an increasingly vital role in today's digitized organizations, and across our digital economy, security leaders must innovate and adapt at the speed of AI-driven change. To do this, they and their teams should make sure they have the right [data protection controls](#)—such as encryption, access controls, data loss prevention, monitoring and auditing, and secure data classification—to secure the organizational data and manage what data is being fed into AI to prevent inadvertent exposure of sensitive data.

While data security has always been important, it gains even more importance in the AI world—discovering where the sensitive data lives, understanding how it's used and exposed, prioritizing data risks based on context and using proactive controls—all while meeting the stringent compliance requirements such as GDPR, CCPA, PCI-DSS and many more.

[NEXT: About us](#)

X-Force Threat Intelligence Index 2026

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 →](#)

Contributors

Alejandro Solano
Austin Zeizel
Benjamin Shipley
Christopher Caridi
Cole Robbins
Colin Connor

David McMillen
Evan Babwah
Jeff Kuo
Joshua Chung
Kaila Washington
Kelsey Oliver

Michelle Alvarez
Omari Jones
Sandra Hill
Sophie Cunningham

About IBM

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | February 2026

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.

Amazon is a trademark or registered trademark of Amazon.com, Inc. or its affiliates in the United States and other countries.

Anthropic and Claude AI are trademarks or registered trademarks of Anthropic PBC in the United States and other countries.

AnyDesk is a trademark or registered trademark of AnyDesk Software GmbH in Germany and other countries.

Apple is a trademark or registered trademark of Apple Inc. in the United States and other countries.

ASUS is a trademark or registered trademark of ASUSTeK Computer Inc. in Taiwan and other countries

Cisco and Duo are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and other countries.

Codecov is a trademark or registered trademark of Codecov, LLC in the United States and other countries.

ConnectWise is a trademark or registered trademark of ConnectWise, LLC in the United States and other countries.

Docker is a trademark or registered trademark of Docker, Inc. in the United States and other countries.

Fortra GoAnywhere is a trademark or registered trademark of Fortra, LLC in the United States and other countries.

Gainsight is a trademark of Gainsight, Inc. in the United States and other countries.

GITHUB is a registered trademark owned by GitHub, Inc. It is registered in the United States and other countries,

GitLab is a registered trademark owned by GitLab Inc.

Google and Gemini are trademarks of Google LLC.

Kaseya is a trademark or registered trademark of Kaseya Limited in the United States and other countries.

Kiteworks is a trademark or registered trademark of Kiteworks, Inc. in the United States and other countries.

LastPass is a trademark or registered trademark of GoTo Group, Inc. in the United States and other countries.

“npm” is a registered trademark of npm, Inc.

Okta is a trademark or registered trademark of Okta, Inc. in the United States and other countries.

OpenAI and ChatGPT are trademarks or registered trademarks of OpenAI OpCo, LLC in the United States and other countries.

Oracle is a trademark or registered trademark of Oracle Corporation and/or its affiliates in the United States and other countries.

Perplexity is a trademark of Perplexity AI, Inc.

Progress MOVEit is a trademark or registered trademark of Progress Software Corporation in the United States and other countries.

Python and PyPI are trademarks of the Python Software Foundation in the United States and other countries.

Salesforce is a trademark or registered trademark of Salesforce, Inc.

Salesloft is a trademark or registered trademark of Salesloft, Inc.

Snowflake is a trademark or registered trademark of Snowflake Inc. in the United States and other countries.

SolarWinds is a trademark or registered trademark of SolarWinds Worldwide, LLC in the United States and other countries.

SonicWall is a trademark or registered trademark of SonicWall Inc. in the United States and other countries.

Tyler Technologies is a trademark or registered trademark of Tyler Technologies, Inc. in the United States and other countries.

Wipro is a trademark or registered trademark of Wipro Limited in India and other countries.

3CX is a trademark or registered trademark of 3CX Ltd. in Cyprus and other countries

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.

[NEXT: Appendix](#)

X-Force Threat Intelligence Index 2026

Appendix

Table 1:
Major supply chain or third-party compromises since 2015

Year	Incidents
2015	XcodeGhost
2016	MeDoc (pre-NotPetya malicious updates)
2017	CCleaner compromise NotPetya via MeDoc
2018	ASUS Live Update compromise EventStream NPM compromise
2019	Wipro vendor breach Docker Hub credential leak
2020	SolarWinds Orion Accellion FTA Tyler Technologies
2021	Kaseya VSA CodeCov Bash Uploader Accellion FTA fallout
2022	Okta/Sitel breach (LAPSUS) GitHub OAuth tokens NPM/PyPI package poisoning
2023	MOVEit (Clop) GoAnywhere MFT 3CX (Lazarus) LastPass

2024	XZ Utils backdoor Snowflake credential compromise Cisco Duo/SMS provider breach Microsoft/Midnight Blizzard OAuth theft
2025	ConnectWise ScreenConnect AnyDesk compromise Salesforce OAuth token compromise Salesloft S3 exposure Salesforce Gainsight GitHub Action Shai-Hulud Worm Oracle Cloud SSO/LDAP Sonicwall Firewall Configuration Breach Shai-Hulud Worm 2.0 react2shell

Source: IBM X-Force. All links in table reside outside ibm.com.