IBM Newsroom

IBM 2026 X-Force Threat Index: AI-Driven Attacks are Escalating as Basic Security Gaps Leave Enterprises Exposed

ARMONK, N.Y., Feb. 25, 2026 /PRNewswire/ -- IBM (NYSE:IBM) today released the 2026 X-Force Threat Intelligence Index, revealing that cybercriminals are exploiting basic security gaps at dramatically higher rates, now accelerated by AI tools that help attackers identify weaknesses faster than ever. IBM X-Force observed a 44% increase in attacks that began with the exploitation of public-facing applications, largely driven by missing authentication controls and AI-enabled vulnerability discovery.

Some of the key highlights include:

- Active ransomware and extortion groups surged (49%) year over year, marking ecosystem fragmentation, while publicly disclosed victim counts rose roughly 12%.
- Large supply chain and third-party compromises nearly quadrupled since 2020, as attackers increasingly exploit environments where software is built and deployed or SaaS integrations.
- Vulnerability exploitation became the leading cause of attacks, accounting for 40% of incidents observed by X-Force in 2025.

"Attackers aren't reinventing playbooks, they're speeding them up with AI," said Mark Hughes, Global Managing Partner for Cybersecurity Services, IBM. "The core issue is the same: businesses are overwhelmed by software vulnerabilities. The difference now is speed. With so many vulnerabilities requiring no credentials, attackers can bypass humans and move straight from scanning to impact. Security leaders need to shift to a more proactive approach, using agentic-powered threat detection and response to identify gaps and catch threats before they escalate."

AI's Mounting Identity Problem

Infostealer malware led to the exposure of over 300,000 ChatGPT credentials in 2025, signaling that AI platforms have reached the same credential risk as other core enterprise SaaS solutions.

Compromised chatbot credentials create AI-specific risks beyond simple account access. Attackers can manipulate outputs, exfiltrate sensitive data or inject malicious prompts. This underscores the need to assess enterprise-wide AI adoption and

enforce strong authentication, and conditional access controls.

AI, Leaked Tooling Lower Barriers to Ransomware Ecosystem

In 2025, X-Force observed a 49% increase in active ransomware groups compared to the prior year, as smaller, transient operators whose low volume campaigns complicate attribution. This trend is accelerated by collapsing barriers to entry as threat actors reuse leaked tooling, rely on established playbooks and increasingly tap AI to automate operations. As multimodal AI models mature, X-Force expects adversaries to automate complex tasks like reconnaissance and advanced ransomware attacks, driving faster-moving, more adaptive threats.

Pressure on Supply Chains Poised to Grow

X-Force identified a nearly 4X increase in large supply chain or third-party compromises since 2020, mainly driven by attackers exploiting trust relationships and CI/CD automation across development workflows and SaaS integrations. With AI-powered coding tools accelerating software creation, and occasionally introducing unvetted code, the pressure on pipelines and open-source ecosystems is expected to grow in 2026.

This rise is also attributed to the blurring line between nation-state and financially motivated actors. As tactics and techniques spread across underground forums, and AI streamlines reconnaissance and exploitation, techniques once reserved for nation-state actors are now being adopted by financially motivated groups.

Additional findings from the 2026 report include:

- **AI accelerating attacker lifecycle.** Attackers are using AI to speed research, analyze large data sets and iterate on attack paths in real time. For example, North Korean IT worker schemes are using AI to scale operations, including AI-driven image manipulation for synthetic identities and translation tools to interact across global marketplaces.
- **Security fundamentals still lacking**. X-Force Red penetration tests reveal persistent weaknesses in credential hygiene and software configuration, with misconfigured access controls as the most common entry point for these engagements.
- **Manufacturing tops the target list for the fifth year.**The sector accounted for 27.7% of incidents observed by X-Force, with data theft being the most common.
- **North America emerged as the most-attacked region**. Accounting for 29% of total cases observed by X-Force, and up from 24% in 2024, North America became the most attacked region for the first time in 6 years.

Additional resources:

- Read the full IBM X-Force Threat Intelligence Index 2026.
- Sign up for the IBM X-Force Threat Intelligence 2026 webinar onMarch 17 at 11 am ET.
- Connect with the IBM X-Force team for a tailored review of the findings.
- Read more about the report's top findings in this blog.

About IBM

IBM is a leading provider of global hybrid cloud and AI, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain a competitive edge in their industries. Thousands of governments and corporate entities in critical infrastructure areas such as financial services,

telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's long-standing commitment to trust, transparency, responsibility, inclusivity and service. Visit www.ibm.com for more information.

Media Contact:
Michele Brancati
IBM Communications
Mbrancati@ibm.com

SOURCE IBM

Additional assets available online: Photos

https://newsroom.ibm.com/2026-02-25-ibm-2026-x-force-threat-index-ai-driven-attacks-are-escalating-as-basic-security-gaps-leave-enterprises-exposed?utm_source=openai