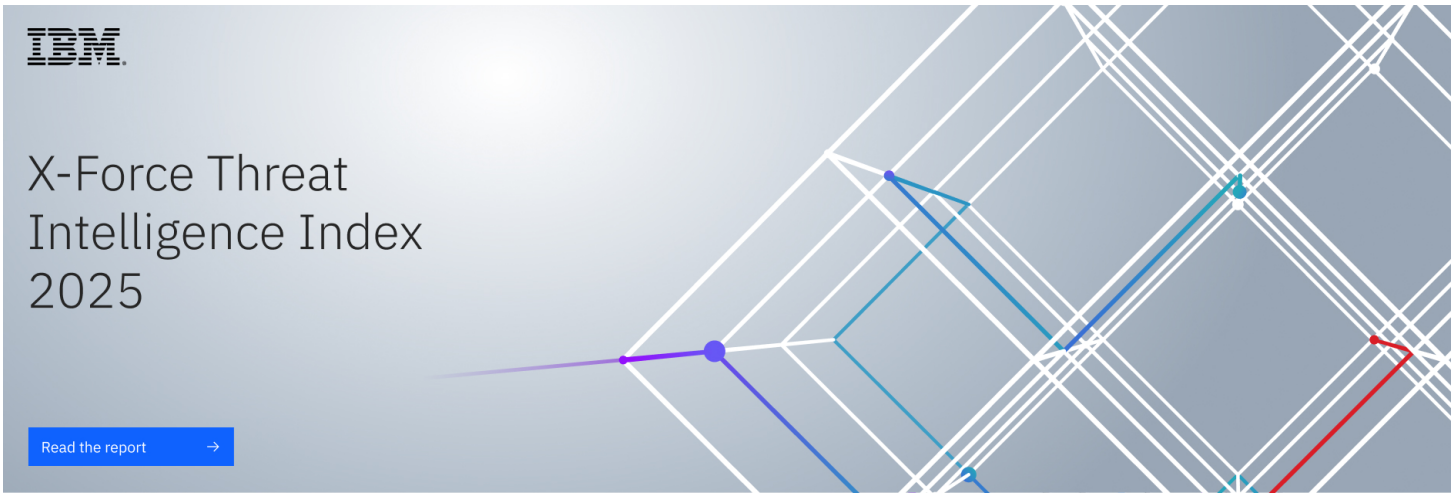
IBM Newsroom

2025 IBM X-Force Threat Index: Large-Scale Credential Theft Escalates, Threat Actors Pivot to Stealthier Tactics

- Nearly half of all cyberattacks resulted in stolen data or credentials

- Identity abuse was the preferred entry point

- Asia Pacific represented more than one-third of attacks in 2024



ARMONK, N.Y., April 17, 2025 /PRNewswire/ -- IBM (NYSE: IBM) today released the 2025 X-Force Threat Intelligence Index highlighting that cybercriminals continued to pivot to stealthier tactics, with lower-profile credential theft spiking, while ransomware attacks on enterprises declined. IBM X-Force observed an 84% increase in emails delivering infostealers in 2024 compared to the prior year, a method threat actors relied heavily on to scale identity attacks.

The 2025 report tracks new and existing trends and attack patterns – pulling from incident response engagements, dark web and other threat intelligence sources.

Some key findings in the 2025 report include:

- Critical infrastructure organizations accounted for 70% of all attacks that IBM X-Force responded to last year, with more than one quarter of these attacks caused by vulnerability exploitation.
- More cybercriminals opted to steal data (18%) than encrypt it (11%) as advanced detection technologies and increased law enforcement efforts pressure cybercriminals to adopt faster exit paths.
- Nearly one in three incidents observed in 2024 resulted in credential theft, as attackers invest in multiple pathways to quickly access, exfiltrate and monetize login information.

"Cybercriminals are most often breaking in without breaking anything – capitalizing on identity gaps overflowing from complex hybrid cloud environments that offer attackers multiple access points," said Mark Hughes, Global Managing Partner of Cybersecurity Services at IBM. "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."

Patching Challenges Expose Critical Infrastructure Sectors to Sophisticated Threats

Reliance on legacy technology and slow patching cycles prove to be an enduring challenge for critical infrastructure organizations as cybercriminals exploited vulnerabilities in more than one-quarter of incidents that IBM X-Force responded to in this sector last year.

In reviewing the common vulnerabilities and exposures (CVEs) most mentioned on dark web forums, IBM X-Force found that four out of the top ten have been linked to sophisticated threat actor groups, including nation-state adversaries, escalating the risk of disruption, espionage and financial extortion. Exploit codes for these CVEs were openly traded on numerous forums — fueling a growing market for attacks against power grids, health networks and industrial systems. This sharing of information between financially motivated and nation-state adversaries highlights the increasing need for dark web monitoring to help inform patch management strategies and detect potential threats before they are exploited.

Automated Credential Theft Sparks Chain Reaction

In 2024, IBM X-Force observed an uptick in phishing emails delivering infostealers and early data for 2025 reveals an even greater increase of 180% compared to 2023. This upward trend fueling follow-on account takeovers may be attributed to attackers leveraging AI to create phishing emails at scale.

Credential phishing and infostealers have made identity attacks cheap, scalable and highly profitable for threat actors. Infostealers enable the quick exfiltration of data, reducing their time on target and leaving little forensic residue behind. In 2024, the top five infostealers alone had more than eight million advertisements on the dark web and each listing can contain hundreds of credentials. Threat actors are also selling adversary-in-the-middle (AITM) phishing kits and custom AITM attack services on the dark web to circumvent multi-factor authentication (MFA). The rampant availability of compromised credentials and MFA bypass methods indicates a high-demand economy for unauthorized access that shows no signs of slowing down.

Ransomware Operators Shift to Lower-Risk Models

While ransomware made up the largest share of malware cases in 2024 at 28%, IBM X-Force observed a reduction in ransomware incidents overall compared to the prior year, with identity attacks surging to fill the void.

International takedown efforts are pushing ransomware actors to restructure high-risk models towards more distributed, lower-risk operations. For example, IBM X-Force observed previously well-established malware families including ITG23 (aka Wizard Spider, Trickbot Group) and ITG26 (QakBot, Pikabot) to either completely shut down operations or turn to other malware, including the use of new and short-lived families, as cybercrime groups attempt to find replacements for the botnets that were taken down last year.

Additional findings from the 2025 report include:

- **Evolving AI threats.** While large-scale attacks on AI technologies didn't materialize in 2024, security researchers are racing to identify and fix vulnerabilities before cybercriminals exploit them. Issues like the remote code execution vulnerability that IBM X-Force discovered in a framework for building AI agents will become more frequent. With adoption set to grow in 2025, so will the incentives for adversaries to develop specialized attack toolkits targeting AI, making it imperative that businesses secure the AI pipeline from the start, including the data, the model, the usage, and the infrastructure surrounding the models.
- **Asia and North America most attacked regions.** Collectively accounting for nearly 60% of all attacks that IBM X-Force responded to globally, Asia (34%) and North America (24%) experienced more cyberattacks than any other region in 2024.

- **Manufacturing felt the brunt of ransomware attacks.** For the fourth consecutive year, manufacturing was the most attacked industry. Facing the highest number of ransomware cases last year, the return on investment for encryption holds strong for this sector due to its extremely low tolerance for downtime.
- **Linux threats.** In collaboration with Red Hat Insights, IBM X-Force found that more than half of Red Hat Enterprise Linux customers' environments had not deployed a patch for at least one critical CVE in their environment, and 18% had not patched five or more. At the same time, IBM X-Force found the most active ransomware families (e.g., Akira, Clop, Lockbit and RansomHub) are now supporting both Windows and Linux versions of their ransomware.

Additional Resources

- Download a copy of the 2025 IBM X-Force Threat Intelligence Index.
- Sign up for the 2025 IBM X-Force Threat Intelligence webinar onTuesday, April 22nd at 11:00 am ET.
- Connect with the IBM X-Force team for a personalized review of the findings.
- Read more about the report's top findings in this IBM 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
mbrancati@ibm.com

SOURCE IBM

Additional assets available online: Photos

https://stage.mediaroom.com/ibmnewsroom/2025-04-17-2025-ibm-x-force-threat-index-large-scale-credential-theft-escalates,-threat-actors-pivot-to-stealthier-tactics