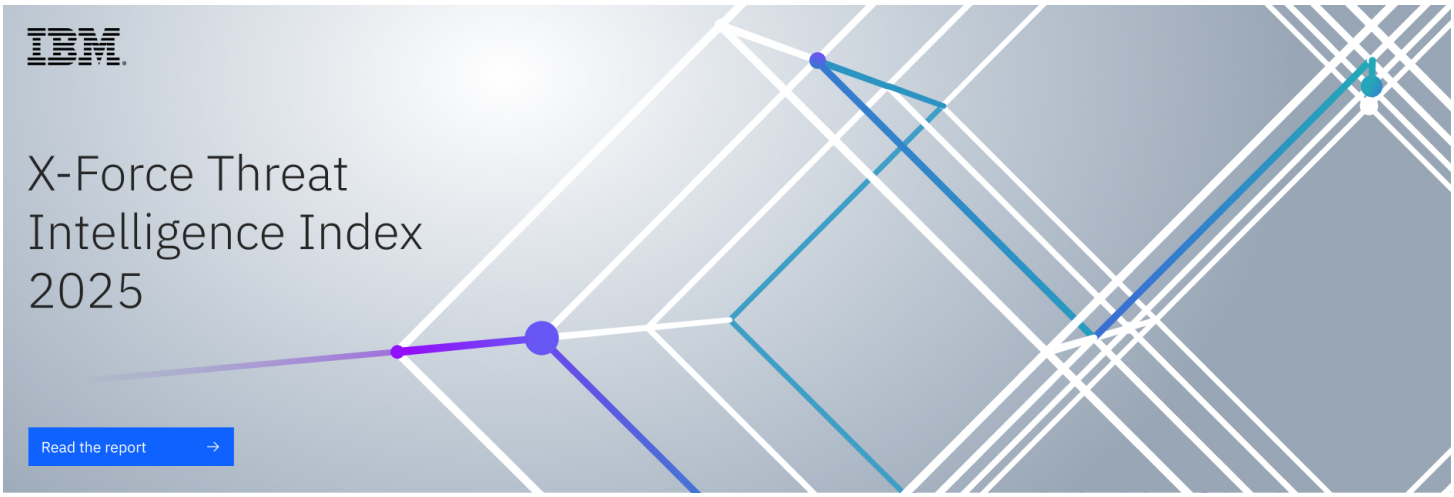
IBM Newsroom - Middle East & Africa

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

- Middle East was the fourth most-attacked region worldwide in 2024



Dubai, UAE, Apr. 17, 2025 -- 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.
- The Middle East was the fourth most-targeted region globally in 2024, accounting for 10% of attacks—up from 7% in 2023. Saudi Arabia and the UAE were the most impacted.
- The finance and insurance sector remained the most targeted industry, representing 61% of incidents, reflecting the Middle East 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%).

"As the Middle East continues to advance its digital transformation agendas, cybercriminals are adapting just as quickly- shifting to low-profile, identity-based attacks that are harder to detect," said Saad Toma, General Manager of IBM Middle East and

Africa. “With sectors like finance, energy, and government increasingly targeted, organizations in the region must invest in intelligence-led security strategies that prioritize identity protection, continuous monitoring, and rapid incident response.”

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 globally and in the Middle East, where exploitation of public-facing applications represented 33% of initial access methods.

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.

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. In the Middle East, malware-infostealers and recon/scanning tools each accounted for 50% of observed attacks, reinforcing a regional focus on stealth and information gathering. 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).

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 Resources

- Download a copy of the 2025 IBM X-Force Threat Intelligence Index.
- Sign up for the 2025 IBM X-Force Threat Intelligence webinar on Tuesday, 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.

---

https://mea.newsroom.ibm.com/ibm-x-force-announcement