Vulnerability exploits are up, and other findings from the X-Force Threat Intelligence Index

Friday, February 27, 2026

Today's top story, from reporter Patrick Lucas Austin:

Cyberattacks caused by the exploitation of public-facing applications grew by 44% in 2025, according to the new IBM X-Force Threat Intelligence Index. Threat actors doubled down on undiscovered vulnerabilities and insecure credentials, taking advantage of the kinds of everyday security gaps that too often go unaddressed.

The surge in credentials-based attacks is a sharp reminder that cybersecurity fundamentals—fixing misconfigurations, enforcing risk-based access controls and continuously testing for weaknesses before someone else does—still matter. It also underscores the growing reality for enterprises that human and non-human identities alike must be monitored with equal rigor. In a digital world where AI agents can execute tasks and monitor activity, and attackers grow nimbler by the day, preparedness and transparency are more important than ever.

That's where the Threat Intelligence Index comes in. The 2026 report, released earlier this week, highlights the evolution of security threats year over year, so that organizations—and the people who defend them—are better equipped in the face of an attack. Here are some of the report's most illuminating findings on the cyberthreat landscape today:

All (attackers') eyes on manufacturers. Manufacturing is still attractive to cyberattackers, and for the fifth year in a row was the most targeted industry in 2025, at 27.7%. Claire Nunez, Creative Director of IBM X-Force Cyber Range, emphasized the importance of due diligence for manufacturers, as supply chain disruptions can have costly consequences. "It takes time and money to fully do risk assessments on some of your supply chain partners," she said on the latest Security Intelligence episode. "And the speed of business is not always the speed of security."

AI as a tool for bad and good. 2025 saw the use of AI in cyberattacks skyrocket, making security fundamentals critical. With adversaries adopting generative AI to scale phishing campaigns and accelerate malicious code development, defenders must rely on tested processes, adhere to cybersecurity best practices, and leverage AI-driven tools to shorten the time between threat detection and response.

Why hack in when you can log in? Credential theft was another popular 2025 cyberattack tactic, functioning as an initial access vector in 32% of all cybersecurity incidents. The reason? It works. "Treating identity as critical infrastructure requires centralized governance, continuous risk-based access controls and AI-specific defenses to counter increasingly advanced threats," said Limor Kessem, IBM X-Force's Global Lead for Cyber Crisis Management, in a recent blog post.