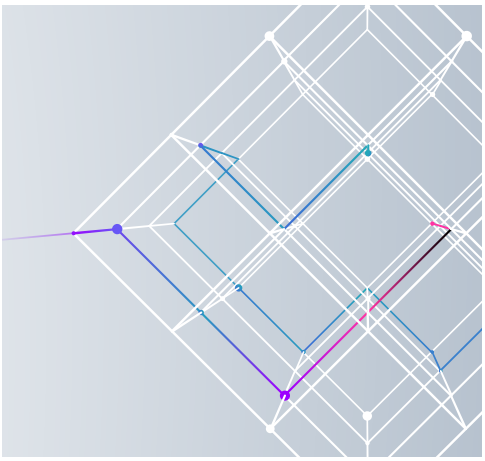
IBM X-Force 2025 Threat Intelligence Index

Transforming cyber defense into cyber resilience

As cyberattacks grow in scale and sophistication, organizations and ecosystem partners need to adopt a coordinated approach to prevent intrusions, enable rapid response, and mitigate impacts.



Manufacturing is the #1-targeted industry, four years in a row.

Manufacturers continued to experience significant impacts from attacks, including extortion (29%) and data theft (24%), targeting financial assets and intellectual property.

Asia-Pacific sees a 13% increase in attacks.

This region experienced the largest share of incidents in 2024 (34%), underscoring APAC's growing exposure to cyberthreats, likely due to its critical role in global supply chains and as a technology and manufacturing hub.

Number of infostealers delivered via phishing emails per week increases by 84%.

Year-over-year, there is a rise in infostealers delivered via phishing emails and credential phishing. Both result in active credentials used in follow-on, identity-based attacks.

Identity-based attacks make up 30% of total intrusions.

For the second year in a row, attackers adopted more stealthy and persistent attack methods, with nearly one in three observed attacks using valid accounts.

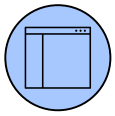
Ransomware makes up 28% of malware cases.

While ransomware made up the largest share of malware cases in 2024 at 28%, we observed a decline in ransomware incidents overall. This is the third year that ransomware incidents have declined.

Continued →

4 out of top 10 vulnerabilities most mentioned on the dark web are linked to sophisticated threat actors.

All top 10 vulnerabilities had publicly available exploit code or had been found being actively exploited in the wild, with 60% of these being actively exploited or having a publicly available exploit from less than two weeks after disclosure to a zero day.



25% of attacks exploit public-facing applications.

One in four attacks exploited vulnerabilities in common public-facing or internet accessible applications. Post-compromise, threat actors use active scanning to identify new vulnerabilities, gain additional access, and move laterally in compromised environments. Manufacturing is the #1-targeted industry, four years in a row. Manufacturers continued to experience significant impacts from attacks, including extortion (29%) and data theft (24%), targeting financial assets and intellectual property.

"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."

Mark Hughes,
Global Managing Partner for Cybersecurity Services, IBM

Threat actors are using AI to build websites, incorporating deepfakes in phishing attacks, and applying gen AI to create phishing emails and write malicious code.

IBM X-Force 2025
Threat Intelligence Index
April 2025

Download the full report here.

Visit the IBM Institute for Business Value
www.ibm.com/ibv

IBM Red Hat