

2025 THREAT HUNTING REPORT

Adversaries are leveraging GenAI to scale operations and accelerate attacks. The CrowdStrike 2025 Threat Hunting Report exposes a sharp rise in malware-free intrusions, cross-domain threats, and AI-enabled attacks.¹ This infographic highlights the most urgent trends² and the insights you need to stop modern threats before they escalate.

Adversaries weaponize AI at scale



320+ organizations were infiltrated by AI-enabled adversary **FAMOUS CHOLLIMA** in the last year, a 220% increase.



Threat actors are increasingly using AI to exploit human trust and accelerate operations.

Malware-free intrusions are on the rise



81% of hands-on-keyboard intrusions in the last 12 months were malware-free.



Adversaries no longer need malware — they hide in plain sight using stolen credentials and legitimate tools.

Cloud environments are under siege



There was a 136% surge in cloud intrusions in the first half of 2025 compared to all of 2024.



The cloud remains a key battleground — CrowdStrike OverWatch observed a 40% year-over-year increase in China-nexus cloud intrusions.

GenAI powers social engineering



Voice phishing (vishing) is on track to double last year's volume by the end of 2025.



This is on top of the 442% increase in vishing attacks between the first and second half of 2024 reported in the [CrowdStrike 2025 Global Threat Report](#).

Cross-domain attacks are accelerating



SCATTERED SPIDER moved from account takeover to ransomware deployment in just 24 hours.



This rapid pace leaves defenders little time to respond, especially as intrusions span multiple domains.

Identity remains the primary target vector



5 of the top 10 most commonly used MITRE ATT&CK® techniques in the past 12 months were Discovery techniques.



After gaining access, attackers immediately map accounts and escalate privileges to quietly move laterally.

