2026 CrowdStrike Global Threat Report: AI Accelerates Adversaries and Reshapes the Attack Surface

AI-enabled attacks surge 89% as breakout time falls to 29 minutes; AI tools and development platforms are actively exploited

AUSTIN, Texas--(BUSINESS WIRE)--Feb. 24, 2026-- CrowdStrike (NASDAQ: CRWD) today released its 2026 Global Threat Report, revealing that AI is accelerating the adversary and expanding the enterprise attack surface. The average eCrime breakout time fell to just 29 minutes in 2025, with the fastest observed breakout occurring in only 27 seconds. Adversaries are also actively exploiting AI systems themselves, injecting malicious prompts into GenAI tools at more than 90 organizations and abusing AI development platforms. The Global Threat Report makes clear that as innovation accelerates, adversary exploitation follows.

AI-enabled adversaries increased operations by 89% year-over-year, weaponizing AI across reconnaissance, credential theft, and evasion. Intrusions now move through trusted identities, SaaS applications, and cloud infrastructure, blending into normal activity while compressing defenders' time to respond. AI is both the accelerant and the target.

CrowdStrike Global Threat Report Highlights:

Based on frontline intelligence from CrowdStrike's elite threat hunters and intelligence analysts tracking more than 280 named adversaries, the report reveals:

- **AI Is the New Attack Surface – Prompts are the New Malware:** Adversaries exploited legitimate GenAI tools at more than 90 organizations by injecting malicious prompts to generate commands for stealing credentials and cryptocurrency. They also exploited vulnerabilities in AI development platforms to establish persistence and deploy ransomware, and published malicious AI servers impersonating trusted services to intercept sensitive data.
- **Fastest Breakout Time on Record:** As AI accelerated attacks, the average eCrime breakout time fell to 29 minutes – a 65% increase in speed from 2024 – with the fastest observed breakout ever occurring in just 27 seconds. In one intrusion, data exfiltration began within four minutes of initial access.
- **Nation-State and eCrime AI Use Accelerates:** AI-enabled adversaries increased their activity by 89%. Russia-nexus FANCY BEAR deployed LLM-enabled malware (*LAMEHUG*) to automate reconnaissance and document collection. eCrime actor PUNK SPIDER used AI-generated scripts to accelerate credential dumping and erase forensic evidence, and DPRK-nexus FAMOUS CHOLLIMA leveraged AI-generated personas to scale insider operations.
- **China- and DPRK-Nexus Operations Surge:** China-nexus activity increased 38% in 2025, with the logistics vertical having the greatest increase in targeting up 85%. 67% of all exploited vulnerabilities by China-nexus actors delivered immediate system access, while 40% targeted internet-facing edge devices. DPRK-linked incidents rose more than 130% as FAMOUS CHOLLIMA activity more than doubled. PRESSURE CHOLLIMA's $1.46B cryptocurrency theft was the largest single financial heist ever reported.
- **Zero Day and Cloud Exploitation Grows:** 42% of vulnerabilities were exploited before public disclosure as adversaries weaponized zero days for initial access, remote code execution, and privilege escalation. Cloud-conscious intrusions rose by 37% overall, with a 266% increase from state-nexus threat actors targeting cloud environments for intelligence collection.

"This is an AI arms race," said Adam Meyers, head of counter adversary operations at CrowdStrike. "Breakout time is the clearest signal of how intrusion has changed. Adversaries are moving from initial access to lateral movement in minutes. AI is compressing the time between intent and execution while turning enterprise AI systems into targets. Security teams must operate faster than the adversary to win."

Additional Resources:

- Download the CrowdStrike 2026 Global Threat Report.
- Visit CrowdStrike's Adversary Universe for the internet's definitive source on adversaries.
- Listen to the Adversary Universe podcast to glean insights into threat actors and recommendations to amplify security practices.
- To learn more about the 2026 Global Threat Report, read our blog or visit us online.

About CrowdStrike

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/
Follow us: Blog | X | LinkedIn | Instagram
Start a free trial today: https://www.crowdstrike.com/trial

View source version on businesswire.com: https://www.businesswire.com/news/home/20260224017260/en/

Media Contact
Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike