CrowdStrike 2026 Threat Hunting Report: AI is Now Embedded Across Modern Adversary Operations

August 3, 2026

Threat actors operationalize AI to exploit vulnerabilities within hours, target enterprise AI, and scale attacks across software supply chains

AUSTIN, Texas--(BUSINESS WIRE)--Aug. 3, 2026-- CrowdStrike (NASDAQ: CRWD) today released the 2026 Threat Hunting Report, revealing that AI is now embedded across modern adversary operations. China-nexus adversaries exploited critical vulnerabilities within 24 hours of public proof-of-concept (PoC) release, while DPRK-nexus adversaries poisoned 131 trusted AI framework packages, demonstrating how AI has become both an operational capability and a high-value target.

AI is now a tool, target, and force multiplier for adversaries. As enterprises embed AI across their business, adversaries are exploiting AI infrastructure, compromising software supply chains, abusing enterprise LLMs, and following AI workloads into the cloud. The result is a new operational reality: attacks move faster, scale more efficiently, and increasingly target the AI systems enterprises depend on.

CrowdStrike Threat Hunting Report Highlights:

Based on frontline intelligence from CrowdStrike's elite threat hunters and intelligence analysts tracking more than 290 named adversaries, the report reveals:

- **AI Is a Tool, Target, and Force Multiplier for Adversaries:** Threat actors used AI to generate payloads and shell commands, exploit AI infrastructure, and abuse enterprise LLMs – including one campaign that sent nearly 200,000 AI model requests in two minutes. CrowdStrike OverWatch also observed AI agent-triggered detection leads grew at 2.5x the rate of human-triggered leads, showing how AI is accelerating the volume and velocity of activity security teams must investigate.
- **The AI Ecosystem Is the Next Supply Chain Battleground:** DPRK-nexus STARDUST CHOLLIMA injected a malicious npm package into 131 trusted Mastra AI frameworks. During 1H 2026, 87% of identified software registry threats involved malicious npm packages. eCrime actor ALTERED SPIDER compromised more than 300 software dependencies in a single day to harvest credentials and pivot into cloud environments.
- **Exploitation Windows Collapse to Hours:** In 1H 2026, 88% of CrowdStrike-observed exploitation of vulnerabilities with a PoC occurred within 48 hours of release. China-nexus actors VAULT PANDA and GENESIS PANDA moved even faster, launching deliberate attacks within 24 hours of disclosure.
- **Adversaries Follow AI into the Cloud:** Cloud-conscious eCrime activity surged 171% as adversaries executed credential theft, cryptomining, LLM abuse, and digital financial asset theft.
- **Trusted Authentication Becomes an Attack Path:** Vishing intrusions increased by 2x in 1H 2026. eCrime groups CORDIAL SPIDER and SNARKY SPIDER compromised single sign-on (SSO) integrated SaaS applications for data exfiltration. In one incident, SNARKY SPIDER moved from account takeover to data theft in under five minutes. Monthly device code phishing attempts increased 15x in 1H 2026, reflecting growing abuse of trusted authentication workflows.

"AI is now embedded in modern adversary operations. It is changing how attacks are planned, executed, and scaled while expanding the attack surface organizations must defend," said Adam Meyers, head of counter adversary operations at CrowdStrike. "The organizations that succeed will secure AI as aggressively as they adopt it and use AI to defend at the speed of the adversary."

Additional Resources:

- Download the CrowdStrike 2026 Threat Hunting Report.
- Visit CrowdStrike's Adversary Universe for the internet's definitive source on adversaries.
- Listen to the Adversary Universe podcast to amplify security practices.
- To learn more about the 2026 Threat Hunting Report, read our blog.

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/20260803155652/en/

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

Source: CrowdStrike