2025 CrowdStrike Threat Hunting Report: Adversaries Weaponize and Target AI at Scale

DPRK-nexus adversaries infiltrate 320+ companies using GenAI accelerated attacks; threat actors exploit AI agents, exposing autonomous systems as the next enterprise attack surface

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Aug. 4, 2025-- Black Hat USA 2025--CrowdStrike (NASDAQ: CRWD) today released the 2025 Threat Hunting Report, highlighting a new phase in modern cyberattacks: adversaries are weaponizing GenAI to scale operations and accelerate attacks – and increasingly targeting the autonomous AI agents reshaping enterprise operations. The report reveals how threat actors are targeting tools used to build AI agents – gaining access, stealing credentials, and deploying malware – a clear sign that autonomous systems and machine identities have become a core part of the enterprise attack surface.

CrowdStrike Threat Hunting Report Highlights

Based on frontline intelligence from CrowdStrike's elite threat hunters and intelligence analysts tracking more than 265 named adversaries, the report reveals:

- **Adversaries Weaponize AI at Scale:** DPRK-nexus adversary FAMOUS CHOLLIMA used GenAI to automate every phase of its insider attack program. From building fake resumes and conducting deepfake interviews to completing technical tasks under false identities – AI-powered adversary tradecraft is transforming traditional insider threats into scalable, persistent operations. Russia-nexus adversary EMBER BEAR used GenAI to amplify pro-Russia narratives and Iran-nexus adversary CHARMING KITTEN deployed LLM-crafted phishing lures targeting U.S. and EU entities.
- **Agentic AI Is the New Attack Surface:** CrowdStrike observed multiple threat actors exploiting vulnerabilities in tools used to build AI agents, gaining unauthenticated access, establishing persistence, harvesting credentials, and deploying malware and ransomware. These attacks demonstrate how the agentic AI revolution is reshaping the enterprise attack surface – turning autonomous workflows and non-human identities into the next frontier of adversary exploitation.
- **GenAI-built Malware Becomes Reality:** Lower-tier eCrime and hacktivist actors are abusing AI to generate scripts, solve technical problems, and build malware – automating tasks that once required advanced expertise. Funklocker and SparkCat are early proof points that GenAI-built malware is no longer theoretical, it's already operational.
- **SCATTERED SPIDER Accelerates Identity-Based, Cross-Domain Attacks:** The group resurged in 2025 with faster and more aggressive tradecraft – leveraging vishing and help desk impersonation to reset credentials, bypass MFA, and move laterally across SaaS and cloud environments. In one incident, the group moved from initial access to encryption by deploying ransomware in under 24 hours.
- **China-nexus Adversaries Drive Continued Surge in Cloud Attacks:** Cloud intrusions rose 136%, with China-linked adversaries responsible for 40% of increased activity, as GENESIS PANDA and MURKY PANDA evaded detection through cloud misconfigurations and trusted access.

"The AI era has redefined how businesses operate, and how adversaries attack. We're seeing threat actors use GenAI to scale social engineering, accelerate operations, and lower the barrier to entry for hands-on-keyboard intrusions," said Adam Meyers, head of counter adversary operations at CrowdStrike. "At the same time, adversaries are targeting the very AI systems organizations are deploying. Every AI agent is a superhuman identity: autonomous, fast, and deeply integrated, making them high-value targets. Adversaries are treating these agents like infrastructure, attacking them the same way they target SaaS platforms, cloud consoles, and privileged accounts. Securing the AI that powers business is where the cyber battleground is evolving."

Additional Resources:

- Download the 2025 CrowdStrike Threat Hunting 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 2025 CrowdStrike Threat Hunting Report, read our blog, visit us online, or stop by the CrowdStrike Black Hat booth #2733.

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 | Twitter | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

View source version on businesswire.com: https://www.businesswire.com/news/home/20250803570128/en/

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

Source: CrowdStrike, Inc.