CROWDSTRIKE
Investor Relations

CrowdStrike 2026 Technology Threat Landscape Report: China Steals AI Capabilities It Can't Build

June 9, 2026

Technology is the world's most targeted industry as adversaries exploit the AI being built and the tools used to build it

AUSTIN, Texas--(BUSINESS WIRE)--Jun. 9, 2026-- CrowdStrike (NASDAQ: CRWD) today released the CrowdStrike 2026 Technology Threat Landscape Report, revealing that China-nexus adversaries are escalating espionage against technology organizations to steal the AI capabilities and intellectual property they cannot build fast enough on their own. With the world's most valuable AI assets concentrated inside technology firms, the sector is now the most targeted industry in the world, and China-nexus adversaries drove more than 58% of state-sponsored targeted intrusions against it.

At the same time, DPRK-nexus adversaries are accelerating fraudulent IT worker schemes to funnel revenue to the regime, while eCrime actors are weaponizing AI and turning the developer ecosystems behind it into attack vectors. The report makes it clear: the same innovation that makes technology valuable makes it the adversary's primary target.

CrowdStrike Technology Threat Landscape Report Highlights:

Based on frontline intelligence from CrowdStrike's Counter Adversary Operations tracking more than 280 named adversaries, the report reveals:

- **China-Nexus Adversaries Steal Technology to Fuel Beijing's AI Ambitions:** China-nexus adversaries – including MURKY PANDA, MUSTANG PANDA, OVERCAST PANDA, SUNRISE PANDA, and WARP PANDA – targeted technology more than any other industry. MURKY PANDA's password-spraying campaign alone impacted more than 340 U.S.-based entities.
- **DPRK Embeds Operatives Inside Tech Using AI:** FAMOUS CHOLLIMA used AI-enhanced personas and U.S. front companies to secure remote IT roles inside technology firms, accounting for 47% of all state-sponsored interactive intrusions against the sector and channeling illicit revenue directly to the regime's weapons programs.
- **Cybercriminals Accelerate Access for Extortion:** Financially motivated attacks accounted for 65% of all interactive operations against the sector. Initial access brokers advertised access to 277 technology organizations, a nearly 30% increase, while big game hunting adversaries named 572 technology entities on dedicated leak sites for extortion.
- **eCrime Groups Weaponize AI to Scale Attacks:** Adversaries used AI-generated scripts to dump credentials and erase forensic evidence at machine speed, collapsing the time defenders have to respond. Across the broader eCrime landscape, actors exploited surging AI adoption – distributing Skrawl, a novel macOS information stealer, through fake OpenClaw extensions and counterfeit download sites impersonating legitimate AI tools.
- **Adversaries Infiltrate Developer Supply Chains:** STARDUST CHOLLIMA compromised the Axios NPM package – downloaded 100 million times per week – likely exposing millions of downstream users, poisoning open-source supply chains. Separately, prior to CrowdStrike's disruption of the Glassworm botnet, malware operators compromised 350 GitHub repositories to inject malicious code into JavaScript and Python projects, targeting software development ecosystems.

"Technology organizations are building the most valuable and most targeted assets in the world. Every AI breakthrough creates a competitive advantage and new attack surface at the same time," said Adam Meyers, head of counter adversary operations at CrowdStrike. "China runs cyberespionage as industrial policy to try to close the AI innovation gap, demonstrating that AI capabilities are the prize adversaries are after. Whether you're building AI or adopting it, security has to be built in from the start."

Additional Resources:

- Download the CrowdStrike 2026 Technology Threat Landscape Report
- Listen to the Adversary Universe podcast for insights into threat actors and recommendations to amplify security.
- To learn more, 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/20260609239344/en/

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

Source: CrowdStrike