CROWDSTRIKE
Investor Relations

2025 CrowdStrike Global Threat Report: China's Cyber Espionage Surges 150% with Increasingly Aggressive Tactics, Weaponization of AI-powered Deception Rises

February 27, 2025

The industry's preeminent source on adversary intelligence exposes a 442% increase in vishing as GenAI-driven social engineering attacks increase; DPRK insider threats spike

AUSTIN, Texas--(BUSINESS WIRE)--Feb. 27, 2025-- CrowdStrike (NASDAQ: CRWD) today released its 2025 Global Threat Report, exposing the growing aggression of China's cyber operations, a surge in GenAI-powered social engineering and nation-state vulnerability research and exploitation, and a sharp increase in malware-free, identity-based attacks. The report reveals that China-nexus adversaries escalated state-sponsored cyber operations by 150%, with targeted attacks in financial services, media, manufacturing and industrial sectors soaring up to 300%.

At the same time, adversaries worldwide are weaponizing AI-generated deception, exploiting stolen credentials and increasingly executing cross-domain attacks—exploiting gaps across endpoint, cloud and identity—to bypass security controls and operate undetected in the shadows. The shift to malware-free intrusions that exploit trusted access, combined with record-shattering breakout times, leaves defenders little room for error. To stop modern attacks, security teams need to eliminate visibility gaps, detect adversary movement in real-time and stop attacks before they escalate—because once they're inside, it's already too late.

CrowdStrike Global Threat Report Highlights

Tracking more than 250 named adversaries and 140 emerging activity clusters, CrowdStrike's latest research reveals:

- **China's Cyber Espionage Grows More Aggressive** : CrowdStrike identified seven new China-nexus adversaries in 2024, fueling a 150% surge in espionage attacks, with critical industries seeing up to a 300% spike in targeted attacks.
- **GenAI Supercharges Social Engineering**: AI-driven phishing and impersonation tactics fueled a 442% increase in voice phishing (vishing) between H1 and H2 2024. Sophisticated eCrime groups like CURLY SPIDER, CHATTY SPIDER and PLUMP SPIDER leveraged social engineering to steal credentials, establish remote sessions and evade detection.
- **Iran Utilizes GenAI for Vulnerability Research and Exploitation**: In 2024, Iran-nexus actors increasingly explored GenAI for vulnerability research, exploit development and patching domestic networks, aligning with government-led AI initiatives.
- **From Breaking In to Logging In – Surge in Malware-Free Attacks**: 79% of attacks to gain initial access are now malware-free while access broker advertisements surged 50% YoY. Adversaries exploited compromised credentials to infiltrate systems as legitimate users, moving laterally undetected with hands-on keyboard activities.
- **Insider Threats Continue to Rise**: DPRK-nexus adversary FAMOUS CHOLLIMA was behind 304 incidents uncovered in 2024. 40% involved insider threat operations, with adversaries operating under the guise of legitimate employment to gain system access and carry out malicious activity.
- **Breakout Time Hits Record Speed**: The average eCrime breakout time dropped to 48 minutes, with the fastest recorded at 51 seconds—leaving defenders little time to react.
- **Cloud Environments Under Siege**: New and unattributed cloud intrusions increased by 26% YoY. Valid account abuse is the primary initial access tactic, accounting for 35% of cloud incidents in H1 2024.
- **Unpatched Vulnerabilities Remain a Key Target**: 52% of vulnerabilities observed were related to initial access, reinforcing the critical need to secure entry points before adversaries establish persistence.

"China's increasingly aggressive cyber espionage, combined with the rapid weaponization of AI-powered deception, is forcing organizations to rethink their approach to security," said Adam Meyers, head of counter adversary operations at CrowdStrike. "Adversaries exploit identity gaps, leverage social engineering and move across domains undetected—rendering legacy defenses ineffective. Stopping breaches requires a unified platform powered by real-time intelligence and threat hunting, correlating identity, cloud and endpoint activity to eliminate the blind spots where adversaries hide."

CrowdStrike pioneered adversary-driven cybersecurity through the CrowdStrike Falcon® cybersecurity platform, which delivers AI-powered protection, real-time threat intelligence and expert threat hunting to secure identity, cloud and endpoint as the gold standard in cybersecurity. Leveraging innovative behavioral AI and machine learning trained on industry-leading threat intelligence and trillions of security events, CrowdStrike delivers real-time protection against advanced threats, providing comprehensive visibility and protection across the entire attack lifecycle.

Additional Resources:

- Download the 2025 CrowdStrike 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.

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/20250227012922/en/

Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike