CrowdStrike 2026 Financial Services Threat Landscape Report: North Korean Adversaries Steal Billions in Digital Assets

May 14, 2026

China-nexus espionage and ransomware pressure on the financial sector intensify as adversaries weaponize AI to compress the time from access to impact

AUSTIN, Texas--(BUSINESS WIRE)--May 14, 2026-- CrowdStrike (NASDAQ: CRWD) today released the CrowdStrike 2026 Financial Services Threat Landscape Report, revealing that DPRK-nexus adversaries stole billions in digital assets in 2025 while industrializing cybercrime with AI-powered deception. Hands-on-keyboard intrusions against financial institutions spiked 43% globally and 48% in North America over the past two years, as adversaries exploited trusted identities and SaaS applications to evade legacy defenses.

CrowdStrike Financial Services Threat Landscape Report Highlights:

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

- **Digital Asset Theft Hits Record Levels:** DPRK-nexus actors drove a 51% year-over-year increase in digital asset theft in 2025, stealing a reported $2.02 billion across the sector. PRESSURE CHOLLIMA conducted the largest financial theft ever reported: $1.46 billion in cryptocurrency through trojanized software distributed via a supply chain compromise. GOLDEN CHOLLIMA used recruitment-themed lures to divert cryptocurrency funds and access cloud environments at fintechs in Southeast Asia and Canada.
- **DPRK Scales Deception with AI:** DPRK-nexus actors used AI to scale operations against the sector. FAMOUS CHOLLIMA doubled its operations using AI-generated identities to infiltrate cryptocurrency exchanges, fintech platforms, and consumer banks. STARDUST CHOLLIMA tripled its operational tempo, deploying AI-generated recruiter personas and synthetic video conferencing environments to target fintechs across North America, Europe, and Asia.
- **China-Nexus Espionage Scales Globally:** China-nexus adversaries posed the most significant intelligence collection threat. HOLLOW PANDA conducted intrusions at financial institutions in the Philippines, Indonesia, and Brazil. MURKY PANDA deployed an operational relay box network across more than 150 endpoints in 36 countries, targeting 340 organizations across more than 30 sectors, with financial services among the most frequently targeted.
- **eCrime Pressure on the Sector Intensifies:** 423 financial services organizations appeared on dedicated leak sites marking a 27% increase year-over-year. MUTANT SPIDER drove the highest intrusion volume through vishing campaigns, then sold access to ransomware groups, enabling faster and more scalable attacks. In the first half of 2025, SCATTERED SPIDER resumed aggressive ransomware operations against insurance entities after a four-month pause.

"Financial services organizations face threats from every direction and AI is making each of them harder to stop. The cost to create convincing identities, automate reconnaissance, and accelerate credential theft is near zero," said Adam Meyers, head of counter adversary operations at CrowdStrike. "Adversaries are using AI to compress the time from initial access to impact, moving through trusted paths faster than legacy defenses can respond. To close that gap, defenders have to meet AI with AI – pairing intelligence with hunting to outpace the adversary."

Additional Resources:

- Download the CrowdStrike 2026 Financial Services 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/20260514027026/en/

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

Source: CrowdStrike