CrowdStrike 2025 APJ eCrime Landscape Report: Chinese Underground Marketplaces Drive Billions in Illicit Transactions; AI-accelerated Ransomware Surges

Chinese-speaking actors evade government restrictions and solicit criminal services through anonymized marketplaces; AI-accelerated ransomware operations signal next evolution of threats

AUSTIN, Texas & SINGAPORE--(BUSINESS WIRE)--Oct. 20, 2025-- **GovWare 2025** -- CrowdStrike (NASDAQ: CRWD) today released the 2025 APJ eCrime Landscape Report, exposing a thriving Chinese-language underground ecosystem and the rise of AI-enhanced ransomware operations. Despite the Chinese government's internet restrictions and eCrime crackdown, anonymized marketplaces remain central to cybercrime activity across Asia Pacific and Japan (APJ). This ecosystem provides a safe haven for Chinese-speaking actors to buy and sell stolen credentials, phishing kits, malware, and money-laundering services – processing billions in illicit transactions.

At the same time, AI is transforming the ransomware economy. From AI-enhanced social engineering to automated malware development, AI is accelerating every stage of the attack chain – representing a new wave of adversaries executing Big Game Hunting campaigns against high-value organizations across APJ.

APJ eCrime Landscape Report Highlights:

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

- **Chinese eCrime Marketplaces Evade Oversight:** Amid tightened restrictions, Chinese underground markets — including Chang'an, FreeCity, and Huione Guarantee — preserve anonymity across clearnet, darknet, and Telegram channels. This decentralized ecosystem remains a hub for Chinese-speaking actors focused on operational security (OPSEC), with Huione Guarantee alone processing an estimated $27 billion USD before its 2025 disruption.
- **AI Escalates Big Game Hunting Ransomware Campaigns:** AI-accelerated ransomware on high-value targets surged, with India, Australia, and Japan among the most impacted countries. Emerging Ransomware-as-a-Service providers *KillSec* and *Funklocker* – leveraging AI-developed malware – accounted for more than 120 incidents. Top targeted sectors included manufacturing, technology, and financial services, with 763 victims publicly named on dedicated leak sites.
- **Chinese-Speaking Actors Exploit Japanese Trading Accounts:** Coordinated account takeover (ATO) campaigns targeting Japanese securities platforms compromised users to artificially inflate the value of thinly traded China-based stocks. This pump-and-dump scheme, traced to Chinese-speaking threat actors, used shared phishing infrastructure to sell victim data on underground forums, including Chang'an Marketplace.
- **eCrime Service Providers Industrialize Attacks**: Providers such as CDNCLOUD (Bulletproof Hosting), *Magical Cat* (Phishing-as-a-Service), and Graves International SMS (Global Spam Service) enabled scalable phishing, malware distribution, and monetization operations throughout the region.
- **Remote Access Tools Target Regional Users**: Likely Chinese-speaking eCrime actors deployed tools like *ChangemeRAT*, *ElseRAT*, and *WhiteFoxRAT* to exploit Chinese- and Japanese-speaking users through SEO poisoning, malvertising, and phishing attacks masquerading as purchase orders.

"eCrime actors are industrializing cybercrime across APJ through thriving underground markets and complex ransomware operations. Simultaneously, AI-developed malware enables adversaries to launch high-velocity, high-volume attacks," said Adam Meyers, head of counter adversary operations at CrowdStrike. "Defenders must meet this new pace of attack with decisive action, powered by AI, informed by human experience, and unified in response."

Download the 2025 APJ eCrime Landscape Report to explore in-depth insights, adversary profiles, and expert strategies for defending against APJ's evolving cyber threats.

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/20251020946097/en/

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

Source: CrowdStrike