CROWDSTRIKE

# 2025 APJ eCRIME LANDSCAPE REPORT

# Table of Contents

# Executive Summary

A new era of cyber threats has emerged in the Asia Pacific and Japan (APJ) region, one marked by the rise of the enterprising adversary — a term introduced in the CrowdStrike 2025 Global Threat Report. This modern class of threat actor operates with business-like discipline, executing attacks with strategic precision, scalable infrastructure, and a clear focus on maximizing impact. Their methods reflect a calculated approach that mirrors corporate efficiency, enabling them to reach their objectives faster and with greater consequence.

In this environment, innovation is essential to stay ahead. Organizations across APJ must adopt advanced technologies and proactive threat hunting strategies to outpace adversaries that are constantly evolving their tactics. These threat actors exploit both technical and human vulnerabilities. They leverage social engineering tactics, often amplified by AI, and target unmanaged devices that fall outside traditional IT oversight. These blind spots offer attackers undetected entry points for data theft, lateral movement, or broader system compromise.

The CrowdStrike Counter Adversary Operations team has brought together industry-leading threat intelligence and best-in-class managed threat hunting with the AI-powered CrowdStrike Falcon® platform to detect, disrupt, and stop enterprising adversaries. Counter Adversary Operations comprises two closely integrated teams. The CrowdStrike Intelligence team provides actionable reporting that identifies new adversaries, monitors their activities, and captures emerging cyber threat developments in real time. The CrowdStrike OverWatch team uses this intelligence to conduct proactive threat hunting across customer telemetry to detect and address malicious activity. Together, these teams protect thousands of customers from the most sophisticated adversaries by providing the intelligence and threat hunting skills and resources that most organizations lack.

A diverse mix of regional and global eCrime threat actors is operating across the evolving APJ eCrime landscape. In addition to major ransomware groups that impact organizations globally, lesser-known threat actors are actively targeting the APJ region, especially through underground Chinese-language channels that support phishing, credential theft, and monetization campaigns. In Southeast Asia, financially motivated threat actors are zeroing in on high-value social media business accounts, reflecting a shift toward tailored, opportunistic targeting. These financially motivated cybercriminals are referred to as SPIDERs in CrowdStrike's adversary naming convention.

This report offers an in-depth view of the APJ eCrime threat landscape based on CrowdStrike Intelligence reporting from January 2024 to April 2025. It explores regional adversaries, underground economies, and malware trends across Central Asia, East Asia, Southeast Asia, South Asia, and Oceania to provide the context and clarity needed to defend against today's most enterprising adversaries.

# eCrime Overview

## Big Game Hunting

From January 1, 2024, to April 30, 2025, CrowdStrike Intelligence documented 763 APJ-based victims named on data extortion and ransomware dedicated leak sites (DLSs).[1] The five countries most represented on DLSs in this time frame are India, Australia, Japan, Taiwan, and Singapore (Figure 1). Although the APJ region represents more than half of the global population, victims based in this region constituted only 9% of 8,418 organizations named on DLSs globally.

Ransomware actors most frequently targeted the manufacturing, technology, industrials and engineering, financial services, and professional services sectors (Figure 1).

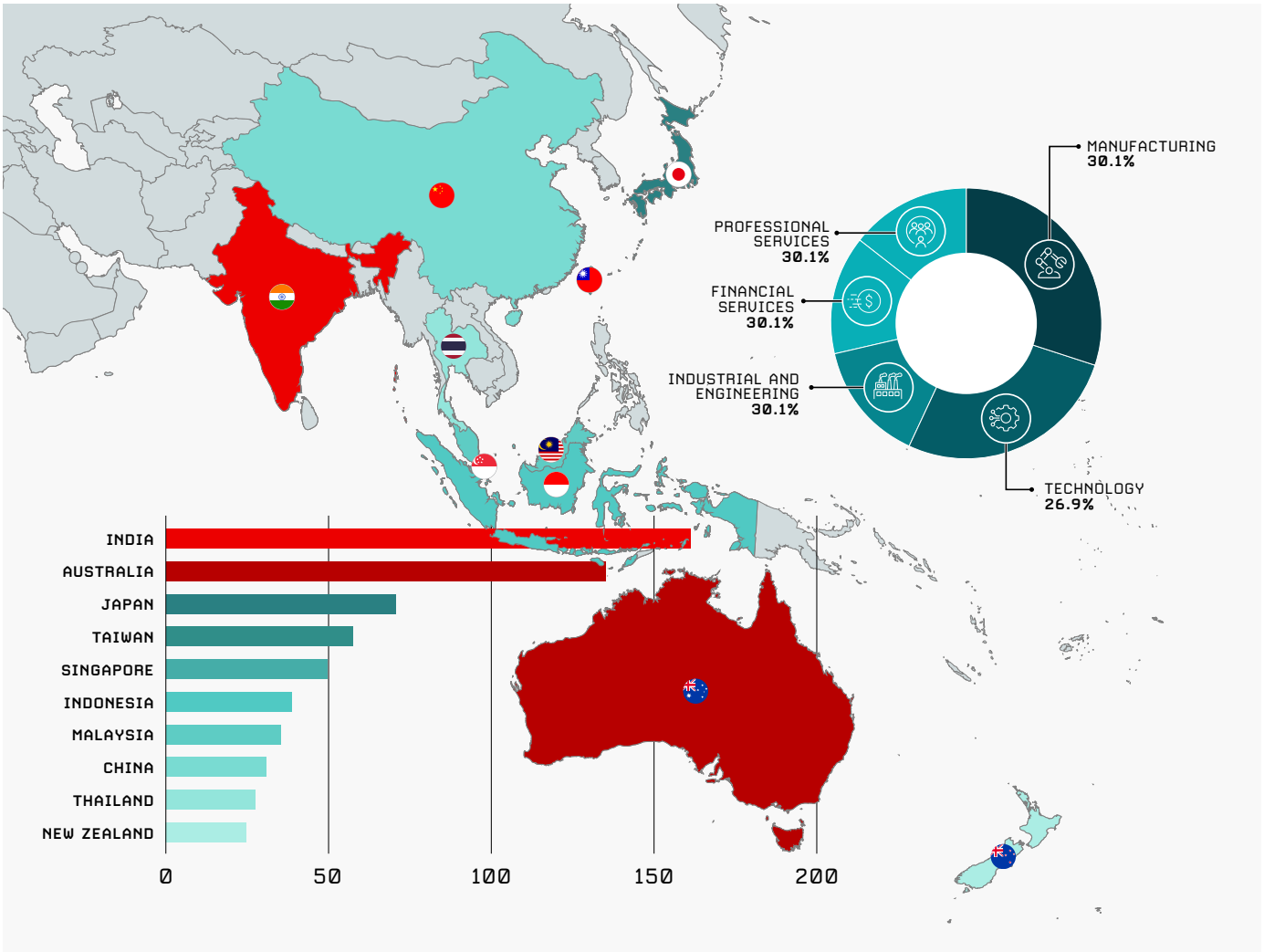


**Figure 1.** Data extortion and ransomware incidents in APJ by country and sector, January 2024-April 2025

1 This number represents only victims that refused to pay a ransom and consequently had data leaked

Based on the DLS data, OCULAR SPIDER, BITWISE SPIDER, BRAIN SPIDER, TRAVELING SPIDER, and PUNK SPIDER issued the most ransomware threats to the APJ region from January 2024 to April 2025 (Figure 2). These adversaries' regional victim proportions are similar to the overall APJ-based big game hunting (BGH) victim proportions, indicating the adversaries likely targeted relevant APJ-based entities opportunistically rather than with overall strategic intent.

These adversaries (except BITWISE SPIDER) did not list Chinese entities on their DLSs, even though China is both the world's second largest economy and second most populous country. OCULAR SPIDER — otherwise the most prolific adversary — explicitly prohibited affiliates from targeting China, the Commonwealth of Independent States (CIS), Cuba, and the Democratic People's Republic of Korea (DPRK). BGH adversaries prohibiting certain target areas is not uncommon, but such prohibitions are typically confined to CIS nations.

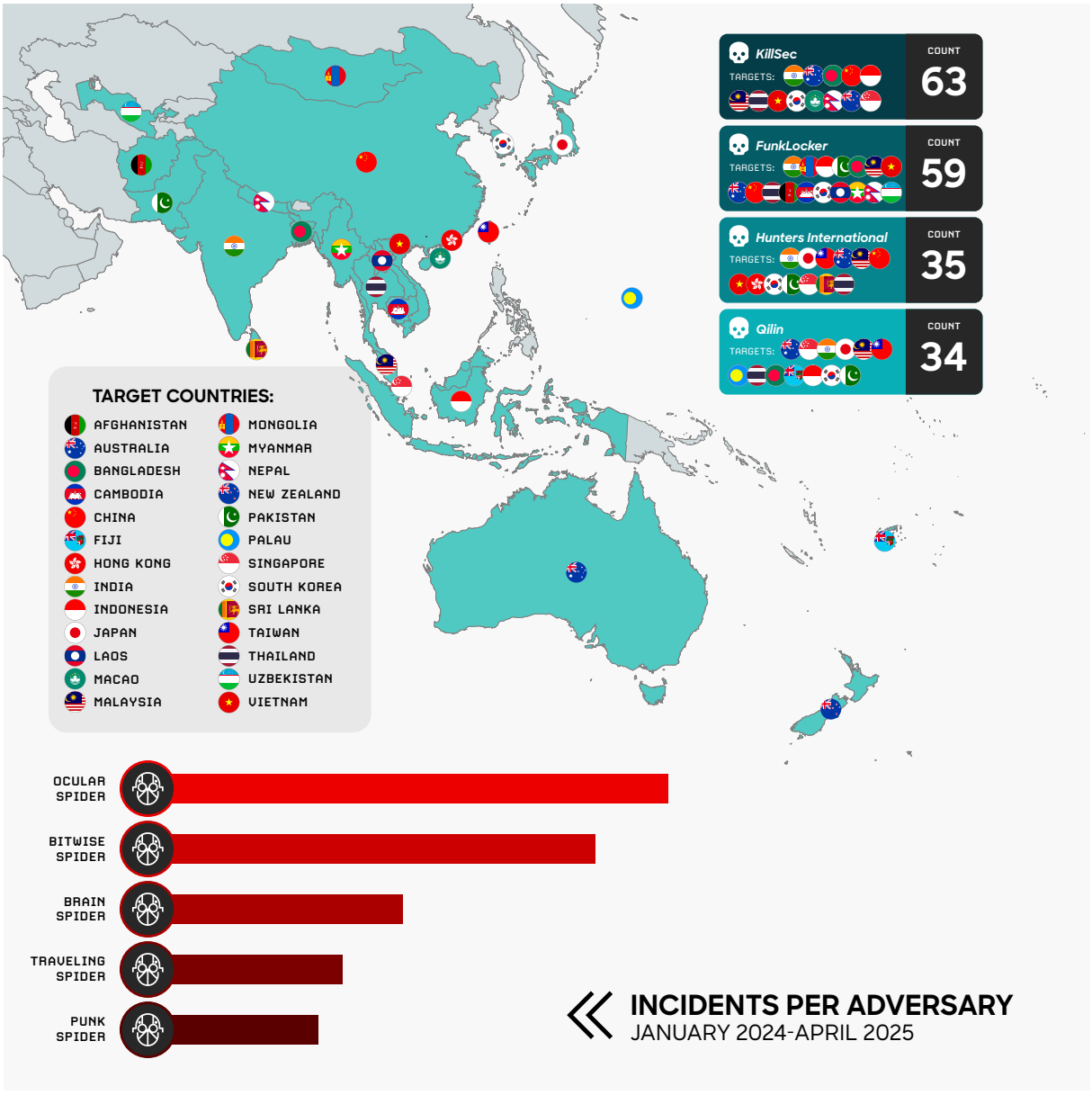


**Figure 2.** Prevalent ransomware threats and incident count in APJ, January 2024-April 2025

Ransomware as a service (RaaS) providers *FunkLocker* and *KillSec* named a disproportionate number of APJ-based victims on their DLSs, comprising 35% and 32% of their total victims, respectively. Of these victims, most were based in India (21% for *FunkLocker* and 33% for *KillSec*). CrowdStrike Intelligence cannot currently assess the threat actors' targeting goals; however, *FunkLocker* claimed in an interview that they target entities based on a combination of revenue and weak defenses. The group's leader, *Scorpion*, has historically also engaged in hacktivism.[2]

2 https://foresiet.com/blog/funksec-ransomware-architect-exclusive-interview/

# Underground Ecosystem

Despite the Chinese government's internet restrictions and eCrime crackdown, clearnet and darknet marketplaces remain prominent in the Chinese-language underground ecosystem. eCrime actors also maintain numerous Telegram channels on which they advertise and solicit criminal services. Likely in response to government control, Chinese-speaking eCrime actors have adopted unique tactics prioritizing operations security (OPSEC) and default anonymity.

The following sections describe the prominent Chinese-language marketplaces Chang'an, FreeCity, and Huione; historically, the now-defunct Huichan and Tea Horse Road were also prominent.

## CHANG'AN MARKETPLACE

Prominent Chinese-language criminal marketplace Chang'an (aka Chang'an Sleepless City or 长安不夜城) has been active since 2022. The site hosts numerous criminal services advertised in the marketplace's multiple sections (e.g., Data Resources, 数据资源; Carding CVV, 卡料CVV; Physical Goods, 实体物品; Technical Skills, 技术技能; and Services, 服务业务) as well as in a dedicated Telegram marketplace with more than 7,000 current members. Though most discussions occur on Telegram, Chang'an encourages members to conduct transactions using the marketplace's escrow service.

Likely due to the Chinese government's crackdown on eCrime, Chang'an emphasizes anonymity. Sellers' usernames are obfuscated by default in listings, which display only the first and last letters of each username. Similarly, the marketplace prohibits sellers from providing contact information in their listings. Instead, customers can leave a public message under the listing or contact the seller via Chang'an's private messaging function.

To further avoid law enforcement attention, Chang'an prohibits certain advertised content. In September 2024, Chang'an's administrator stated that content such as espionage, politics, and law enforcement is prohibited.

## FREECITY MARKETPLACE

Active since 2020, FreeCity (自由城) is a well-known Chinese-language criminal marketplace that also offers English, Russian, and Ukrainian user interfaces to attract users beyond the Chinese underground ecosystem (Figure 3). CrowdStrike Intelligence has identified individual non-Chinese-speaking FreeCity users. For example, since January 2025, the Russian-speaking user *Lord* has advertised *RMS Loader x3*, claiming Chinese forums offer many malware sales opportunities.


**Figure 3.** FreeCity main page, August 2025

FreeCity marketplace sections include:

- Data Intelligence (数据情报)
- CVV Combing (CVV 梳理)
- Physical Goods (实体物品)
- Private Guarantee (私人担保)
- QP/CP Only (QP/CP 专属)[3]
- Service Orders (服务接单)
- Virtual Resources (虚拟资源)

Similar to other Chinese-language eCrime marketplaces, FreeCity also has several associated Telegram channels that include the following:

- Chinese Community Channel (中文社区)
- Darkweb Tutorial Channel (暗网教程; this channel primarily explains how to use Tor and VPNs to bypass the Great Firewall)
- Fraudsters Exposure Channel (骗子曝光")
- Notice Channel (公告频道)

3 Chinese-speaking eCrime actors commonly use “QP/CP” as slang for sports gambling and lottery activities

# HUIONE/HAOWANG GUARANTEE MARKETPLACE

Huione Group is a Cambodia-based conglomerate that manages financial services, real estate, transportation, and insurance operations. In 2021, Huione Group launched the Telegram-based service Huione Guarantee, ostensibly a platform for buying and selling legitimate goods and services that was promoted on the website for Huione Group's online payment application, Huione Pay.[4]

Despite its purported intentions, Huione Guarantee rapidly became the most prominent eCrime marketplace for Chinese-speaking threat actors, which leveraged the service for money laundering, cashouts, escrow, and contraband sales. The platform became especially popular with operators of pig butchering scams — fraud campaigns, often carried out by individuals forced to work under duress, where victims are lured through social or dating platforms and manipulated into investing cryptocurrency that is ultimately stolen. Money laundering and pig butchering scams continue to be prevalent across Southeast Asia. Law enforcement agencies are actively combating these operations in Cambodia, Laos, Myanmar, Thailand, and Vietnam.


**Figure 4.** Huione main page, August 2025

Huione Guarantee operated a web of Telegram channels divided into two categories: the Public Group, which operated on a subscription model catering to threat actors with large sales volumes, and the Dedicated Group, designed for one-time transactions between two individuals. Huione Guarantee established a reputation for transparency and trustworthiness among eCrime actors and facilitated an estimated 27 billion USD worth of transactions, primarily in Tether, over its lifespan.[5]

On May 1, 2025, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a ruling naming Huione Group a financial institution of primary money laundering concern and moved to block its access to the U.S. financial system.[6] Around the same time, the service changed its name to Haowang Guarantee, but the new name was short-lived, as Telegram began shutting down the service's channels and banning administrators' accounts.

By mid-May 2025, Huione/Haowang Guarantee's Public Group services were discontinued. The group transferred remaining cryptocurrency assets to the eCrime marketplace Tudou Guarantee for customer settlements.[7] Telegram users associated with Huione/Haowang Guarantee have claimed that the Dedicated Group remains operational, but CrowdStrike Intelligence has not confirmed the service's current status.

4 https://www.elliptic.co/blog/cyber-scam-marketplace

5 https://www.elliptic.co/blog/elliptic-data-telegram-market-takedown

6 https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern

7 https://www.elliptic.co/blog/elliptic-data-telegram-market-takedown

# Targeted eCrime Threats

CrowdStrike Intelligence tracks four named active eCrime adversaries based in the APJ region: CHARIOT SPIDER, RADIANT SPIDER, SINFUL SPIDER, and SOLAR SPIDER (Figure 5). Apart from SOLAR SPIDER, these adversaries are mainly opportunistic and have not been observed targeting the region. eCrime adversaries (especially in Eastern Europe) sometimes prohibit targeting of their own region due to nationalistic loyalties or to avoid legal repercussions.

Though CrowdStrike Intelligence has not observed APJ eCrime actors explicitly prohibiting regional targeting, Chinese-speaking marketplaces' rules and emphasis on anonymity indicate they hope to avoid law enforcement attention.

Nonetheless, CrowdStrike Intelligence has identified likely Chinese-speaking eCrime actors using the remote access tools (RAT) *ChangemeRAT*, *ElseRAT*, and *WhiteFoxRAT* to target Chinese and Japanese speakers.

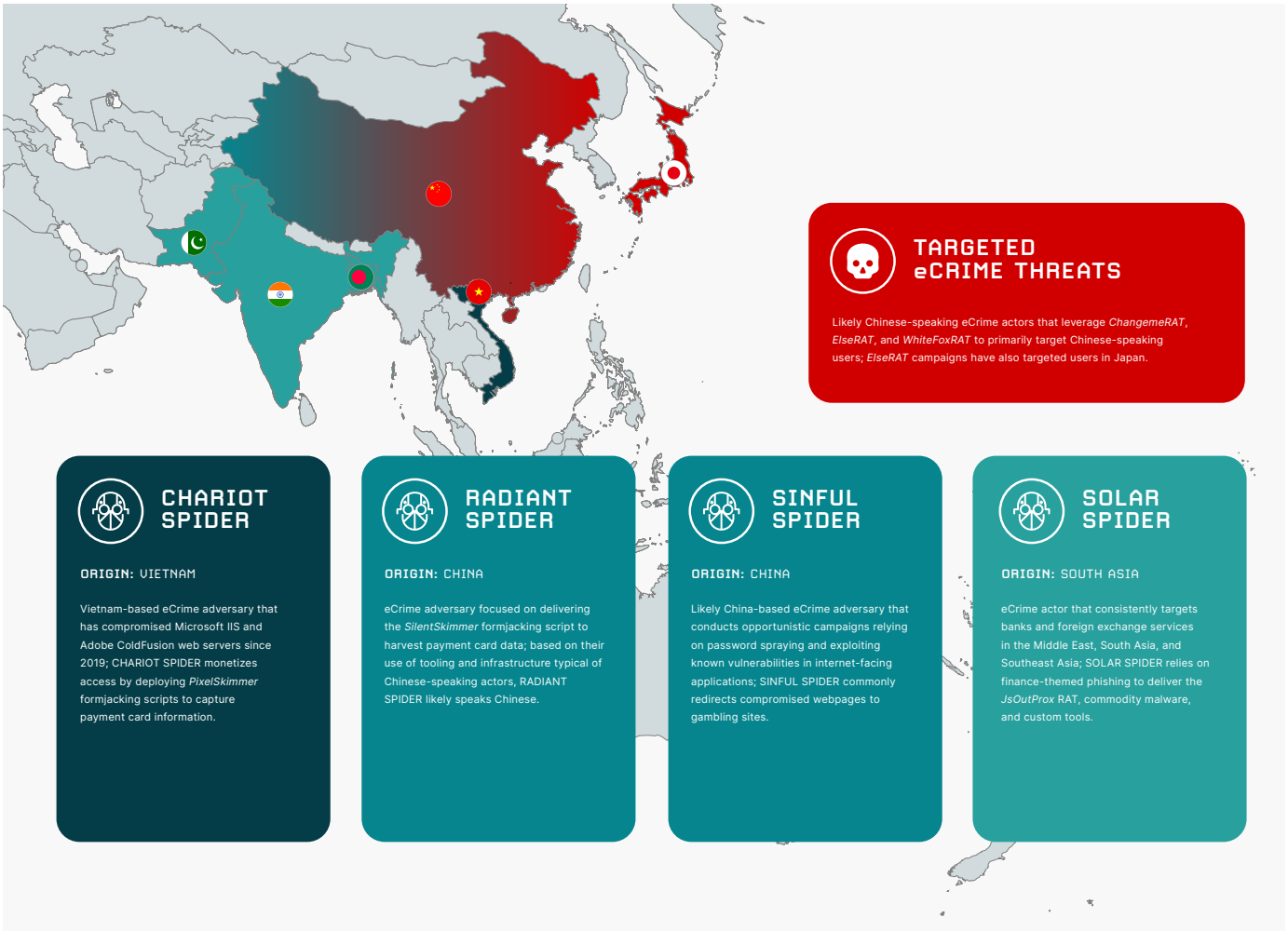


**Figure 5.** APJ eCrime adversaries and threats, January 2024-August 2025

## CHANGEMERAT

Since at least October 2024, an unidentified financially motivated threat actor has delivered *ChangemeRAT* to Chinese-speaking users, consistently delivering payloads via trojanized Microsoft Software Installer (MSI) files hosted on websites likely disseminated via search engine optimization (SEO) poisoning or malvertising.

In March 2025, CrowdStrike Intelligence identified a *ChangemeRAT* campaign impacting Chinese-speaking users in which payloads masqueraded as legitimate Chinese-language applications, including Youdao Dictionary and SiGua Instant Messaging.

The campaign leveraged multiple legitimate MSI binaries that sideload various malicious loader dynamic link libraries (DLLs) containing legitimate but invalid signatures. The invalid signatures suggest the threat actor likely modified legitimate DLLs to contain code that ultimately deploys the *ChangemeRAT* samples.

The DLL implements specific anti-analysis features, including checking for `ZhuDongFangYu.exe`, a process associated with the China-based security product 360 Total Security. This specific check suggests the DLL developer hopes to evade security products commonly used by Chinese speakers.

CrowdStrike Intelligence observed this campaign impacting a likely Chinese-speaking individual at a European entity, suggesting the threat actor likely targeted Chinese speakers across geographies.

## ELSERAT

Since at least January 2025, a Chinese-speaking eCrime actor has targeted users in China and Japan using *ElseRAT*, directing users to Chinese- and Japanese-language phishing pages that encourage them to download .docx files masquerading as purchase orders.

Each .docx file, typically named `document.docx`, contains English-language instructions and a ZIP archive named `document.zip` embedded as an Object Linking and Embedding (OLE) object that the user must extract. The ZIP archive contains a binary named `document.exe` that ultimately drops an *ElseRAT* sample (Figure 6).

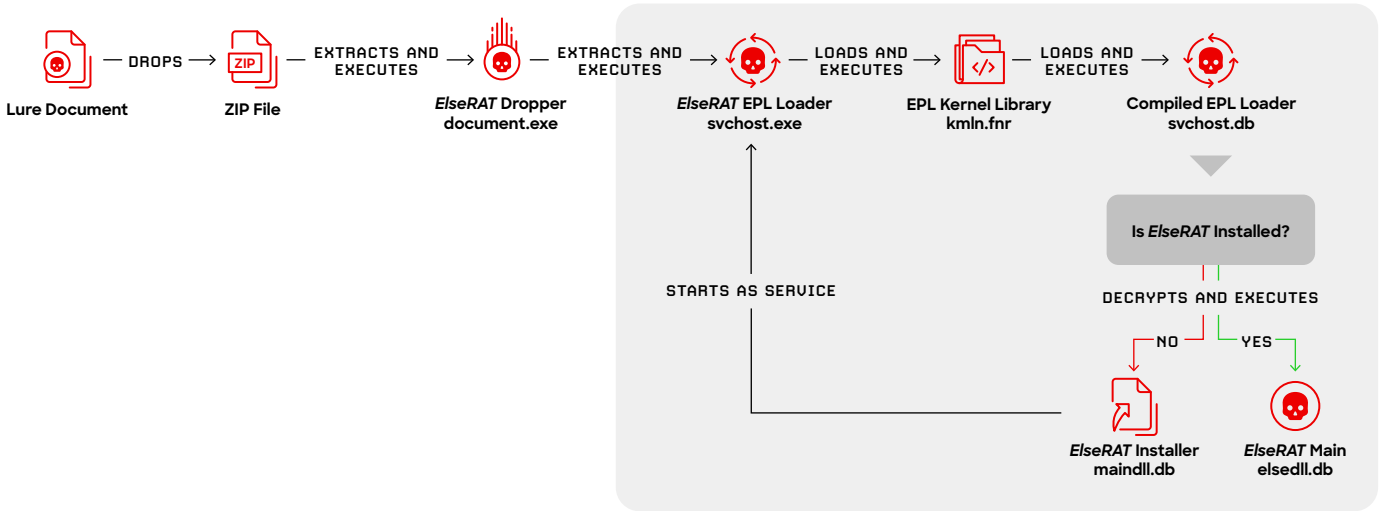


**Figure 6.** *ElseRAT* infection chain

The *ElseRAT* dropper, which contains a valid Tangshan Jimin Information Technology Partnership Enterprise signature, decrypts a further ZIP archive embedded in its resource section and extracts several payloads. The payloads include benign Ruby, AnyDesk, and TightVNC executables as well as an Easy Programming Language (EPL) loader and an encrypted *ElseRAT* installer and binary. The EPL loader loads the *ElseRAT* installer, which disables security controls and executes the ElseRAT binary.

This campaign's *ElseRAT* samples connect to three command-and-control (C2) domains that all resolve to an IP address owned by XNNET LLC, a U.S.-based hosting provider with no apparent social media presence and a one-page website providing no service or purchase details. The company is registered in Wyoming by a firm that acts as a proxy registrar for businesses wishing to obscure their true ownership.

## WHITEFOXRAT

From January 2024 through March 2025, CrowdStrike Intelligence identified several opportunistic eCrime campaigns delivering *WhiteFoxRAT*, primarily to Chinese-speaking users. A native Chinese speaker using the moniker *Brother Li* (李哥) developed *WhiteFoxRAT* and offers it for sale on a Chinese-language Telegram channel.

*Brother Li* also maintains *WhiteFoxRAT*'s distribution domains, which masquerade as legitimate software download sources. The developer claims to direct traffic to the domains via search engine bidding, in which threat actors place bids on specific search engine keywords that then appear as sponsored results when users search those keywords.

*WhiteFoxRAT* distribution targets Chinese-speaking users across multiple geographies; *Brother Li*'s distribution domains often leverage VPN-themed phishing lures, suggesting the threat actor also targets Chinese users operating outside China's restrictive internet parameters. Threat actors distribute the RAT via MSI and ZIP files masquerading as applications for Chinese speakers, including QuickQ VPN, Mei Qui AI, and WPS Office.

In one intrusion, CrowdStrike observed *WhiteFoxRAT* downloading a DLL that checks the system language and exits if the language is not set to Chinese, further demonstrating that *WhiteFoxRAT*'s operators likely focus on Chinese speakers.

### SOLAR SPIDER Targets APJ Financial Entities

Since their 2018 identification, eCrime adversary SOLAR SPIDER has consistently targeted financial entities in the Middle East, South Asia, and Southeast Asia. The adversary relies on financial transaction-themed phishing lures to deliver their *JsOutProx RAT* and commodity malware that includes *NetSupportRAT*, *STRRAT*, and *WSHRAT*.

Though SOLAR SPIDER's tactics, techniques, and procedures (TTPs) remained relatively consistent in 2024, the adversary began delivering novel custom and commodity malware at a heightened operational tempo in early 2025.

From January 2025 to May 2025, numerous SOLAR SPIDER campaigns targeted banks and foreign exchange services in Bangladesh, India, Japan, Malaysia, Nepal, the Philippines, the Republic of Korea, and Sri Lanka. The adversary leveraged Swift and Western Union transaction-themed phishing lures to deliver payloads hosted on GitHub and GitLab. As well as their typical payloads, SOLAR SPIDER delivered a likely new *Meduza Stealer* version and custom Java reconnaissance tools.

# Observed eCrime Service Providers

## CDNCLOUD BULLETPROOF HOSTING

Since July 2024, China-based bulletproof hosting provider CDNCLOUD has advertised its services on the Telegram channel "CDNCLOUD server — fangfang" (服务器—芳芳). The provider purportedly maintains offices in Thailand, Singapore, and the U.S. and offers its services to users in Singapore, Hong Kong, Japan, Taiwan, India, Vietnam, the Philippines, Malaysia, Indonesia, Cambodia, Mongolia, and Macao.

CDNCLOUD offers two data routes for its servers: ChinaNet Next Carrying Network (CN2) — a Chinese telecom network — and Border Gateway Protocol (BGP), which includes multiple interconnected routing protocols. Tether addresses that receive CDNCLOUD funds are likely associated with Huione Group escrow services.

## MAGICAL CAT PHISHING KIT

Since December 2023, threat actor Luck has operated three Chinese-language Telegram channels promoting their phishing as a service tool *Magical Cat*. With more than 4,200 members, the channels have conducted cryptocurrency transactions in excess of 790,000 USD with other known Chinese-speaking eCrime actors.

*Magical Cat* includes the *Dracula Suite*, a framework that clones legitimate websites for use as phishing pages. Luck also regularly shares prebuilt phishing templates in their Telegram channels, targeting organizations across multiple regions.

CrowdStrike Intelligence documented 29 distinct *Magical Cat* phishing domains targeting organizations across APJ (Figure 7). Domain registration patterns, campaign timelines, and targeting cycles analysis suggest these campaigns were conducted by multiple distinct threat actors leveraging the same phishing kit rather than as part of a single coordinated operation.

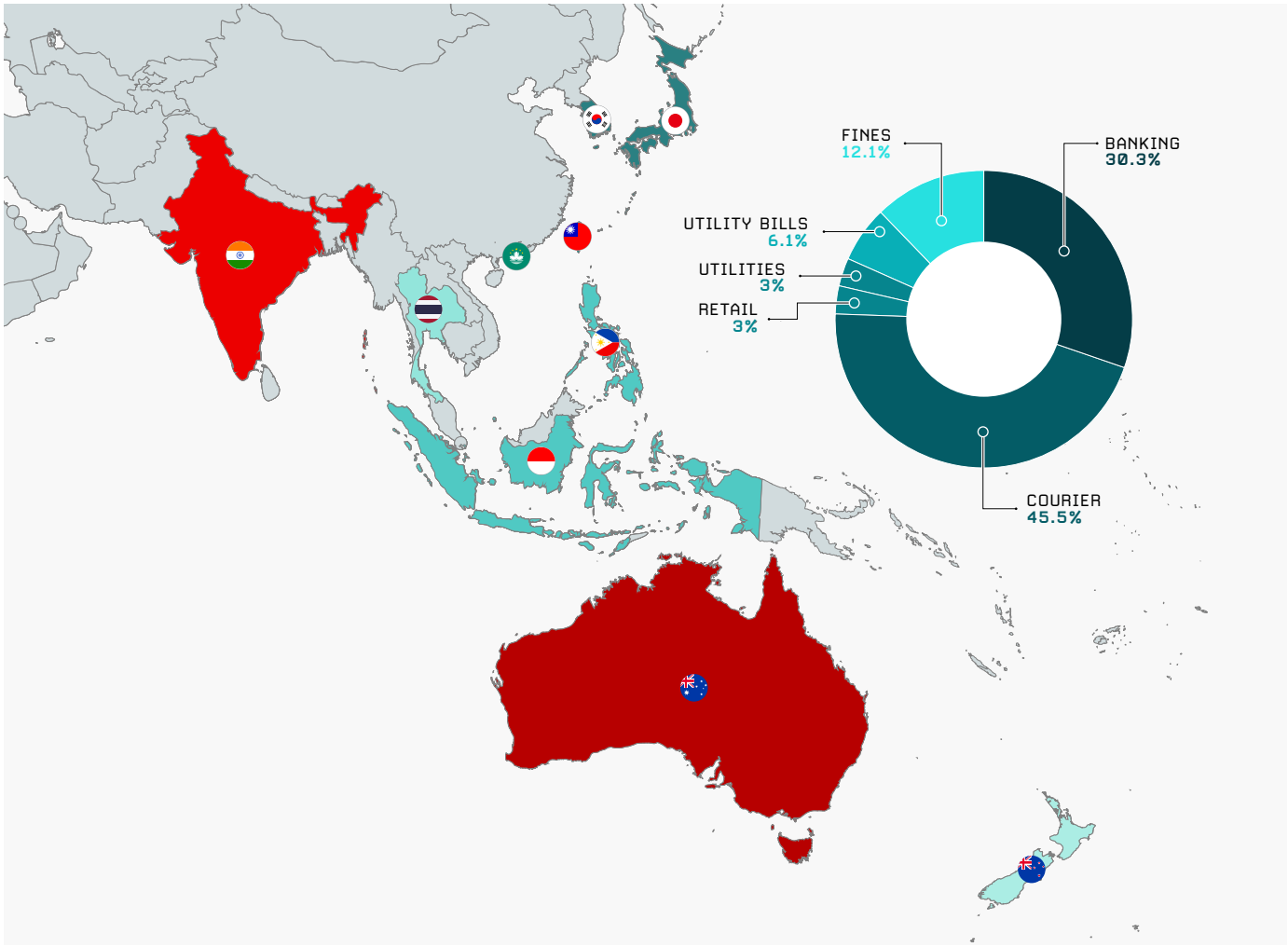


**Figure 7.** APJ *Magical Cat* phishing kit targets

## GRAVES INTERNATIONAL SMS

Graves International SMS (格雷福斯 国际短信), a global SMS spam service first advertised by *yongd02* on Telegram on April 11, 2025, includes a dedicated *Magical Cat* v3 phishing kit integration. Though the service operates independently, threat actor Luck specifically recommends it to *Magical Cat* users. The integration enables automated high-volume SMS distribution for *Magical Cat*'s phishing pages.

### ATO Campaigns Compromise Japanese Trading Accounts to Manipulate Stock Prices

In 2025, CrowdStrike Intelligence identified numerous account takeover (ATO) campaigns targeting users of Japanese services, particularly securities companies. The ATO campaigns reportedly leveraged compromised accounts to purchase China-based companies' thinly traded stocks (aka penny stocks) to artificially inflate prices and sell earlier positions.

One or more Chinese-speaking eCrime actors likely used the same phishing kit to conduct the campaigns. This assessment is made with high confidence based on Chinese comments in the phishing kit's code, reliance on China-based infrastructure, and sales of victim data on Chang'an.

# Vietnam-Based Threats

The Vietnamese eCrime ecosystem focuses particularly on social media business account compromise; threat actors target accounts with significant advertising budgets. In May 2024, Vietnamese authorities prosecuted more than 20 individuals for the development and distribution of information stealers, both domestically and internationally, that led to more than 20,000 compromised social media accounts.

Vietnamese-speaking malware developers have designed multiple information stealers specifically for social media credential theft. These include the recent threats *Ailurophile Stealer* and *FatStealer*, which both contain Vietnamese-language code strings.

## AILUROPHILE STEALER

Since August 2024, threat actor Ailurophile has advertised the information stealer *Ailurophile Stealer* on the underground forum `exploit[.]in`. This comprehensive stealer targets various Gecko- and Chromium-based browsers to steal usernames, passwords, and cookies as well as several cryptocurrency wallets and a social media site to steal cookies and ad balances.

*Ailurophile Stealer* includes several error messages and text-file messages in Vietnamese, suggesting its developer speaks Vietnamese. Further, Ailurophile's GitHub account is set to a time zone consistent with Vietnam, and their forum posting history occurs within Vietnamese work hours.

## FATSTEALER

Since March 2023, campaigns distributing the PHP-based information stealer *FatStealer* have used malvertising and SEO poisoning to distribute files masquerading as popular movies or legitimate software. Operators typically distribute *FatStealer* in ZIP archives and obfuscate the stealer with the legitimate commercial software ionCube.

# Conclusion

eCrime threats differ greatly across the APJ subregions and countries, likely due to a combination of factors, including relative degree of digitalization and economic activity as well as threat actor political affiliations.

Although ransomware and data extortion campaigns impact APJ-based organizations on a smaller scale than in Europe and North America, BGH adversaries will likely continue to pose the greatest eCrime threat to large regional economies, such as Australia, India, Japan, Taiwan, and Singapore. The ransomware operations that publicly named the most APJ-based victims between January 2024 and April 2025 largely overlap with the most prolific global ransomware operations in the same time frame, including OCULAR SPIDER's *RansomHub* RaaS, BITWISE SPIDER's *LockBit* RaaS, and the *Qilin* RaaS. Notable exceptions are the *FunkLocker* RaaS and *KillSec* RaaS, which have named a disproportionate number of APJ-based victims on their DLSs.

Likely APJ-based eCrime actors exhibit a variety of different monetization methods. Both China-based RADIANT SPIDER and Vietnam-based CHARIOT SPIDER have conducted long-running formjacking campaigns in which they inject malicious JavaScript to targeted websites to harvest payment data. An unidentified likely eCrime actor performed ATO campaigns throughout the first half of 2025 targeting consumer securities accounts to purchase penny stocks in China-based companies, likely with the intent to inflate those stocks' value.

Chinese- and Japanese-speaking users, including those based outside APJ, face targeted eCrime threats (e.g., *ChangemeRAT* and *WhiteFoxRAT*) that will likely persist, facilitated by the resilient and developing regional underground ecosystem. These campaigns are largely opportunistic, with users often directed to malicious sites via malvertising and SEO.

# Recommendations

## 1 Adopt agentic AI to scale security operations

As threat actors adopt AI to strike faster, scale operations, and evade detection, defenders face mounting pressure to keep pace. Security teams are already stretched thin, grappling with growing alerts, contending with skills shortages, and racing to respond at speed. To close these widening gaps, security teams should operationalize agentic AI — systems capable of reasoning, adapting, and acting autonomously within defined guardrails and organizational policies. These capabilities can scale intelligence-driven operations by using emerging threat intelligence and expertise to triage alerts, conduct investigations, and execute response actions. By offloading time-intensive, repetitive tasks, agentic AI empowers human analysts to focus on proactive threat hunting and hypothesis-driven investigation, elevating both strategic impact and operational efficiency.

## 2 Secure the entire identity ecosystem

Adversaries increasingly target identities using credential theft, multifactor authentication (MFA) bypass, and social engineering while moving laterally between on-premises, cloud, and software as a service (SaaS) environments via trusted relationships. This allows them to impersonate legitimate users, escalate privileges, and evade detection.

Organizations should adopt phishing-resistant MFA solutions, such as hardware security keys, to prevent unauthorized access. Strong identity and access policies are essential, including just-in-time access, regular account reviews, and conditional access controls. Identity threat detection tools must monitor behavior across endpoints and on-premises, cloud, and SaaS environments to flag privilege escalation, unauthorized access, and backdoor account creation. Integrating these tools with extended detection and response (XDR) platforms enables comprehensive visibility and a unified defense against adversaries.

Additionally, organizations should educate users to recognize voice phishing (vishing) and phishing attempts while maintaining proactive monitoring to detect and respond to identity-based threats.

## 3 Eliminate cross-domain visibility gaps

Adversaries' growing use of hands-on-keyboard techniques and legitimate tools makes detection and response more difficult. Unlike traditional malware, these methods allow attackers to bypass legacy security measures by executing commands and using legitimate software to mimic normal operations.

To counter this, organizations must modernize their detection and response strategies. XDR and next-gen security information and event management (SIEM) solutions provide unified visibility across endpoints, networks, cloud environments, and identity systems, enabling analysts to correlate suspicious behaviors and see the full attack path. Agentic AI-powered triage and investigations can extend these capabilities, autonomously analyzing signals across domains to surface high-fidelity insights and prioritize real threats.

Proactive threat hunting and threat intelligence further enhance detection by identifying potential attack patterns and providing insights into adversary TTPs. With real-time intelligence, organizations can stay informed about emerging threats, anticipate attacks, and prioritize critical security efforts.

## 4 Defend the cloud as core infrastructure

Cloud-focused adversaries are exploiting misconfigurations, stolen credentials, and cloud management tools to infiltrate systems, move laterally, and maintain persistent access for malicious activities like data theft and ransomware deployment.

Cloud-native application protection platforms (CNAPPs) with cloud detection and response (CDR) capabilities are critical to counter these threats. These solutions provide operators with a unified view of their cloud security posture, helping them rapidly detect, prioritize, and remediate misconfigurations, vulnerabilities, and adversary threats. Additionally, enforcing strict access controls — such as role-based access and conditional policies — limits exposure to critical systems while continuously monitoring for anomalies, including logins from unexpected locations.

Regular audits are also critical to maintaining security. Automated tools can uncover overly permissive storage settings, exposed APIs, and unpatched vulnerabilities. Frequent reviews of cloud environments promptly addresses unused permissions and outdated configurations.

## 5 Prioritize vulnerabilities with an adversary-centric approach

Adversaries are increasingly exploiting publicly disclosed vulnerabilities and using exploit chaining, combining multiple vulnerabilities to gain rapid access, escalate privileges, and bypass defenses. These multi-stage attacks often rely on public resources like proof-of-concept (POC) exploits and technical blogs, enabling adversaries to craft effective and hard-to-detect payloads.

To counter these threats, organizations must prioritize regular patching or upgrading of critical systems, especially frequently targeted internet-facing services like web servers and VPN gateways. Monitoring for subtle signs of exploit chaining, such as unexpected crashes or privilege escalation attempts, can help detect attacks before they progress.

Tools like CrowdStrike Falcon® Exposure Management, built with native AI prioritization, enable teams to reduce noise and focus on the vulnerabilities that matter most, specifically those affecting critical and high-risk systems. By adopting proactive security approaches, discovering exposures across the attack surface, and leveraging automation, organizations can mitigate sophisticated threats and limit adversary opportunities.

## 6 Know the adversary and be prepared

When a cyberattack unfolds in minutes — or even seconds — being prepared can be the difference between containment and catastrophe. An intelligence-driven approach enables security teams to move beyond reactive defense by understanding which adversary is targeting them, how they operate, and what their objectives are. With threat intelligence, adversary profiling, and tradecraft analysis, security teams can prioritize resources, adapt defenses, and actively hunt for threats before they escalate. CrowdStrike's threat intelligence doesn't just detect known threats — it anticipates new and evolving tradecraft, keeping defenders one step ahead. By seamlessly integrating intelligence into security workflows, organizations can accelerate response times, disrupt adversaries, and turn intelligence into action.

Though technology is critical to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. Organizations should initiate user awareness programs to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

# 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:** www.crowdstrike.com

**Follow us:** Blog | X | LinkedIn | Facebook | Instagram | YouTube

**Start a free trial today:** www.crowdstrike.com/free-trial-guide