Cyber Threat Landscape Financial Services - 2025

March 2026

Prepared by

Asia Information Sharing & Analysis Center Limited

Prepared for

Corporate Members

Asia-ISAC

“**Cybersecurity is the foundation for our digital world.** It is at the heart of trust and will allow society to fully benefit from the transformations enabled by new technologies like AI and quantum.

But it’s not something one can do on their own. We have to come together, share intelligence globally and develop the skills.. “

Michael Miebach,
Chief Executive Officer,
Mastercard

Table of Contents

Disclaimer

This report is issued by Asia Information Sharing & Analysis Center Limited ("Asia-ISAC") for general informational and intelligence-sharing purposes only. The information, analysis, and attribution assessments contained herein are derived from sources believed to be reliable at the time of publication; however, cyber threat intelligence is inherently dynamic, may be incomplete, and remains subject to change without notice.

While reasonable care has been taken in the preparation of this report, Asia-ISAC makes no representation or warranty, whether express or implied, as to the accuracy, completeness, or reliability of the contents. This report does not constitute legal, regulatory, technical, or professional advice and should not be relied upon as such.

Asia-ISAC shall not be liable for any loss or damage arising directly or indirectly from the use of, or reliance on, this report.

Some incident details, financial estimates, and vulnerability references are based on aggregated intelligence, anonymized case studies, and modeled scenarios derived from multiple sources, and may not correspond to publicly disclosed incidents.

All assessments are based on Asia-ISAC analysis of incident data, partner intelligence, and open-source reporting as of the time of publication.

Asia-ISAC Overview

NO COMPANY IN ASIA SHOULD FACE CYBER THREATS ALONE

Vision

The Asia Information Sharing & Analysis Center (Asia-ISAC) is the region's first cross-industry, non-profit cyber intelligence network dedicated to trusted threat sharing and secure AI adoption. As cyberattacks grow more sophisticated and the cost of data breaches continues to rise, Asia-ISAC enables organizations to collaborate, share intelligence, and strengthen their collective cyber resilience.

Mission

- Enable secure, sustainable, and trusted information sharing
- Unlock business innovation and growth with secure AI
- Provide early warnings on emerging cyber threats
- Strengthen cyber resilience

Executive Summary

Asia Financial Services (FS) 2025

$8.0 Trillion

Customers served

2.7 Billion

FS Companies in Asia

70,000+

What this report covers

This Cyber Intelligence Report provides an overview of the cyber threat landscape targeting the financial services sector across Asia in 2025. The scope includes:

- Regional coverage across East Asia, Southeast Asia, South Asia, and Oceania.
- Impacts spanning financial services and their related supply chain environments, including financial losses, private data exposure, supply chain vulnerabilities, and service disruptions.
- Analysis of notable incidents, threat actors, malware families, and exploited vulnerabilities.

Key findings and highlights

The Asia financial sector experienced significant cyber threats in 2025. Ransomware attacks, Distributed Denial of Service (DDoS), credential theft, insider threats, and exploitation of supply chain vulnerabilities were among the most impactful challenges faced by organizations. Both cybersecurity-related financial losses and reputational impacts increased significantly, driven by highly active threat actors and evolving tactics.

State-sponsored entities like Lazarus Group and Salt Typhoon amplified espionage and financial fraud activity, targeting high-value financial institutions and cryptocurrency platforms. Vulnerabilities such as insecure APIs and third-party systems further enabled attackers to gain persistent access into sensitive environments. This report also provides insights into tactics and techniques observed, offering actionable recommendations.

Key findings include:

- Increasingly sophisticated ransomware campaigns (e.g. Toppan breach).
- State-sponsored activities targeting financial and cryptocurrency sectors.
- An escalating reliance on third-party vendors and cloud ecosystems.

Major attacks and business impact

The financial services sector in Asia continues to face an escalating wave of sophisticated cyber threats — ranging from ransomware and advanced persistent threats (APTs) to insider-enabled fraud. These attacks represent significant business risks, triggering significant financial losses, regulatory scrutiny, reputational damage, and deep erosion of customer trust.

Here are the major cyberattacks that resulted in significant business impact and losses.

- Toppan Ransomware Incident (Singapore) compromised printing vendor Toppan Next Tech and exposed customer data (~11,200 affected customers) from DBS Bank and Bank of China Singapore.
- Lazarus Group APT Attack on Cryptocurrency Platforms (UAE) resulted in losses of US$1.5 billion - largest ever cryptocurrency heist to date.
- Coinbase Insider Incident US$20 million ransom demand; US$400 million loss; stolen data of over 69,000 customers - involving overseas contractors.

In summary, these three attacks, while distinct in method and geography, share a common thread: they exploited trust — trust in vendors, trust in platforms, and trust in people.

Actionable intelligence in this report

This report provides actionable intelligence and insights to support a clearer understanding of the threat landscape and enable proactive risk mitigation.

- **Top threat actors** active against the financial services sector in Asia.
- **Malware used and evolving tactics & techniques** by these threat actors.
- **Vulnerabilities exploited** in the financial services sector.
- **Recommendations** mapped to observed threat behaviors to strengthen resilience.

Key Threat Landscape Insights

Threat Analysis

The cyber threat landscape for the financial services sector across Asia is rapidly evolving, with several key insights emerging on major threats, trends, and incidents observed in 2025.

Asia's financial services sector faced a persistent and highly sophisticated series of threats in 2025. Ransomware, DDoS, insider threats, and supply-chain attacks remain the critical vectors affecting business continuity, customer trust, and financial stability. Taken together, these threat vectors point to a threat environment that is broader in scope, deeper in impact, and harder to defend against than ever before.

59%

Y-o-Y Growth in Ransomware Attacks

KEY INSIGHTS:

- **Increasingly sophisticated ransomware campaigns:** Predominantly cybercriminal groups targeting APIs, supply chains, and leveraging DDoS-for-Hire services (Fog ransomware, Toppan breach, and others).
- **State-sponsored activities targeting financial and cryptocurrency sectors:** At least 3 state-sponsored APT groups focused on espionage and cryptocurrency theft.
- **An escalating reliance on third-party vendors and cloud ecosystems:** Growing impact from insider threats and third-party vulnerabilities with vulnerabilities being exploited to disrupt operations and exfiltrate data.

Addressing these threats for financial services companies requires urgent adoption of data-centric security, enhanced endpoint and API protections, and collaborative strategies between businesses, regulators, and governments worldwide.

Summary of Major Incidents

Summary of key cyberattacks for the financial services sector with the most severe impacts in terms of operational disruptions, financial losses, and/or private data compromises.

These cyber incidents can provide insights on the gravity of the cyberattacks including the business and economic impact of these incidents. Furthermore, the primary threat actor or hacking group that conducted the attack and attack details are indicated to get a better understanding of who conducted and how the attack was successful.

1. Toppan Ransomware Incident (Singapore)

- Date: April 2025
- Business Impact: Private data from financial institutions leaked; significant reputational damage to affected organizations.
- Financial Losses/Costs: Not disclosed; fines and recovery efforts.
- Attack Attribution: Cybercriminals targeting third-party vendors.
- Attack Type: Third-party ransomware breach.
- Techniques: Compromised printing vendor Toppan Next Tech, exposing customer data from DBS Bank and Bank of China Singapore. Approximately 11,200 affected customers (8,200 DBS, 3,000 Bank of China).
- Reference: 3

500	US$1.5M
Computers crashed	Ransom demand

2. Espionage and State-Backed APT Operations (East Asia)

- Date: Ongoing through 2025 (affected January-April 2025)
- Business Impact: Theft of sensitive financial sector data related to critical infrastructure.
- Financial Losses/Costs: Strategic intellectual property theft, future competitive disadvantage.
- Attack Attribution: State-backed actors (e.g., MirrorFace, Salt Typhoon).
- Attack Type: Multi-vector targeted espionage.
- Techniques: Multi-sector infiltration, including Japanese financial institutions; data exfiltration
- Reference: 2

3. DDoS Wave Against APAC Financial Institutions

- Date: 2024-2025
- Business Impact: Widespread service interruptions, significant loss of customer trust.
- Financial Losses/Costs: Difficult to quantify; indirect costs due to downtime and mitigation.
- Attack Attribution: Likely cybercriminal groups using DDoS-for-Hire services.
- Attack Type: Distributed Denial of Service (DDoS).
- Techniques: Focused on APIs, customer-facing websites, and regional financial services networks (38% of volumetric DDoS globally targeted APAC financial sectors).
- Reference: 1

4. APT Attack on Cryptocurrency Platforms

- Date: January-April 2025
- Business Impact: Major theft of cryptocurrency funds; damage to institutional trust in cryptocurrency.
- Financial Losses/Costs: estimated US$1.5 billion (largest ever cryptocurrency heist targeting a platform in ByBit, Dubai).
- Attack Attribution: Lazarus Group (APT state-aligned actor).
- Attack Type: Phishing, malware, and data exfiltration tactics.
- Techniques: Cryptocurrency wallets and exchanges through spear-phishing and advanced malware
- Reference: 3

5. Southeast Asia Spyware Surge

- Date: January-June 2025
- Business Impact: Private data compromises affecting individuals and financial organizations across Southeast Asia.
- Financial Losses/Costs: Indirect costs from privacy breaches and regulatory fines.
- Attack Attribution: Multiple spyware actors.
- Attack Type: Spyware attacks.
- Techniques: Detected across 427,265 incidents involving spyware linked to financial data exfiltration
- Reference: 5

6. Third-Party Vulnerabilities in Financial Supply Chains

- Date: Throughout H1 2025
- Business Impact: Continuous breaches through financial services' reliance on outsourced services; regulatory scrutiny.
- Financial Losses/Costs: Escalating response costs and potential fines under PDPC and other laws.
- Attack Attribution: Cybercriminal collaboration.
- Attack Type: Supply-chain compromise.
- Techniques: Exploitation of third-party data exchange systems in Southeast Asia
- Reference: 4

7. Insider Threat Incident at Coinbase

- Date: February 2025
- Business Impact: Breach of 69,461 user accounts; severe reputational harm.
- Financial Losses/Costs: US$20 million ransom demand; US$180-400 million in incident response costs; stock prices down 7%.
- Attack Attribution: Insider bribery and social engineering of overseas customer support agents.
- Attack Type: Insider threat (bribery/social engineering).
- Techniques: Extraction of sensitive user data.
- Reference: 3

8. DDoS & Ransomware Escalations (UAE)

- Date: January – June 2025
- Business Impact: Incident spike in financial sector services, outages disrupting banking and transaction flows.
- Financial Losses/Costs: Financial impact remains difficult to quantify; significant downtime and reputation hit.
- Attack Attribution: Likely financially motivated groups; includes some state-nexus actors (geopolitical adversaries).
- Attack Type: DDoS, ransomware, phishing.
- Techniques: Data/system exfiltration, ransomware monetization strategies.
- Reference: 6

9. API and Credential Theft Campaign (Malaysian Bank)

- Date: June 2025
- Business Impact: Unauthorized financial transactions; abuse of stolen credentials and compromised APIs.
- Financial Losses/Costs: Ongoing investigations into fraud costs and identity abuse.
- Attack Attribution: Cybercriminal organizations leveraging credential-theft campaigns.
- Attack Type: Credential theft.
- Techniques: Targeted banking APIs and digital credentials.
- Reference: 5

10. Fog Ransomware Attack on Unnamed Financial Institution

- Date: May 2025
- Business Impact: Severe disruption to operations; reputational damage; financial losses.
- Financial Losses/Costs: Undisclosed ransom amount; extensive recovery costs.
- Attack Attribution: Sophisticated ransomware group.
- Attack Type: Ransomware.
- Techniques: Targeted legitimate employee monitoring tools and open-source penetration testing tools to gain and maintain access.
- Reference: 3

Recommendations

Strengthen the cybersecurity posture

These recommendations are made based on lessons learned and key challenges faced in the incidents highlighted in the financial services sector.

The financial services sector continues to face an evolving threat landscape fueled by nation-state actors, ransomware operators, and sophisticated cybercriminal groups. As a critical engine of capital flow, financial services companies must adopt a proactive and layered cybersecurity approach to safeguard services, data, and customer trust.

By adopting these measures, financial services providers can significantly bolster their defenses against emerging malware tactics, targeted attacks, and supply chain vulnerabilities while ensuring compliance with regulatory mandates and industry standards.

Zero Trust Security Architecture

Enforce a Zero-Trust Framework and implement strict Identity and Access Management (IAM) solutions coupled with multi-factor authentication (MFA).

Supply Chain Risk Audits

Perform regular reviews of third-party vendors, especially to identify threats posed or weak controls. Engage vendors to comply with industry-standard cybersecurity guidelines (ISO and NIST).

Cyber Threat Intelligence

Partner with regional alliances, including Asia-ISAC, to obtain early indicators, TTPs, and mitigation playbooks for ransomware and APT campaigns.

Endpoint Detection and Response

Deploy next-generation endpoint protection tools with built-in capabilities to detect, isolate, and remediate ransomware, malware, and credential theft attempts.

Robust Cyber Crisis Response Plan

Conduct regular tabletop simulations and cyber crisis team exercises to improve effectiveness of your response plan.

Summary of Top Threat Actors, Malware, and Vulnerabilities

Top Threat Actors Targeting the Financial Services Sector

The financial services sector in Asia faces a complex and multi-dimensional threat environment in 2025 — one that is no longer defined by isolated incidents, but by a persistent, organized, and increasingly coordinated ecosystem of malicious actors.

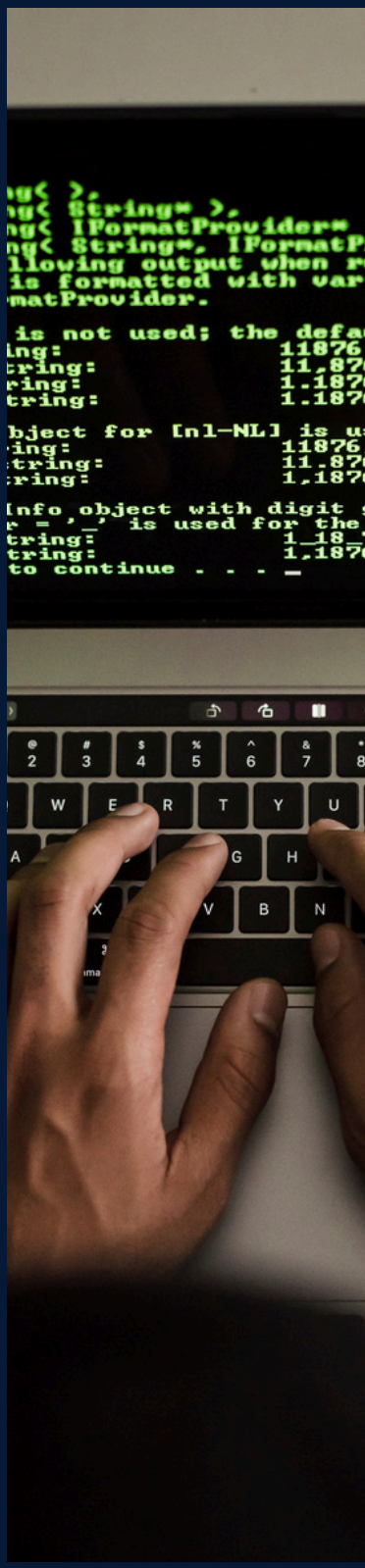
These threat actors span the full spectrum: from state-sponsored Advanced Persistent Threat (APT) groups executing long-term espionage and cryptocurrency theft campaigns, to organized cybercriminal syndicates deploying ransomware, DDoS-for-hire services, and supply chain exploits for financial gain, to insider threats enabled by social engineering and bribery.

What unites them is a shared and deliberate focus on the financial sector — its critical infrastructure, its vast customer data, its digital assets, and its systemic importance to national and regional economies. The top threat actors profiled below represent the most significant and consequential cyber adversaries targeting Asia's financial institutions today.

The following threat actors have aggressively targeted the financial services sector in Asia as identified across the Asia-Pacific, Australia, South Asia, Central Asia, and the Middle East regions in 2025.

These threat actors are identified based on Asia-ISAC analysis of incident frequency, operational impact, and intelligence reporting across the region.

This section profiles each actor, draws cross-incident patterns, and identifies four structural trends that will define threat actor behaviour against Asian financial services sector through 2026.



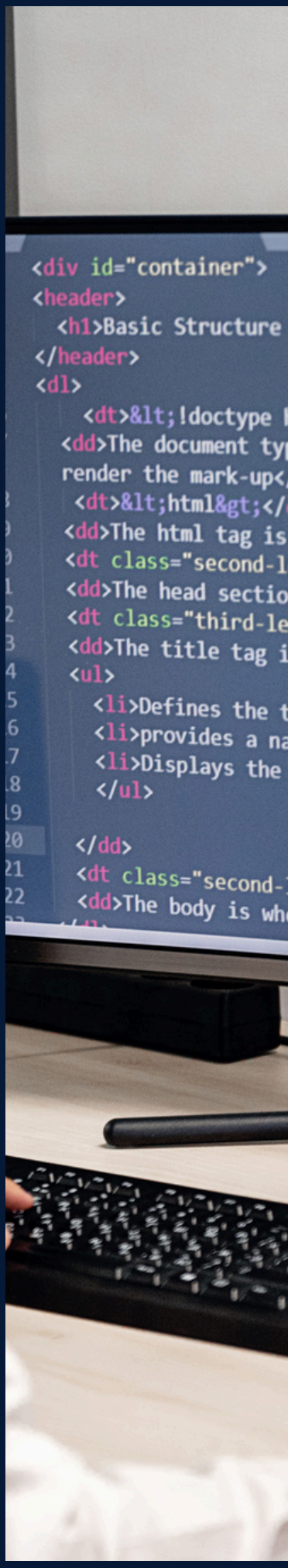
Key Observations

The Convergence of State-Sponsored and Cybercriminal Tactics: The traditional distinction between nation-state actors and organized cybercrime groups is rapidly dissolving. State-sponsored groups like Lazarus Group and MirrorFace are employing techniques — phishing, ransomware-adjacent malware, credential theft — that are commonly used by criminal groups like Fog Ransomware. Conversely, cybercriminal groups are achieving levels of operational sophistication, coordination, and persistence that were once the exclusive domain of state actors.

The Human Element and the Extended Enterprise Are Now the Primary Attack Surface: The most damaging incidents were not achieved by breaching hardened technical perimeters — they were achieved by exploiting people and third-party relationships. The Coinbase insider breach (bribed contractors), the Toppan supply chain attack (compromised vendor), the Malaysian API attackers (stolen credentials), and Spyware Operators (targeting individuals) all demonstrate that the human and vendor layers of an organization represent the path of least resistance for sophisticated adversaries.

Financial Impact Has Reached a Scale That Threatens Systemic Stability: The aggregate financial damage inflicted by these ten threat actors is staggering: US$1.5 billion stolen by Lazarus Group alone, US$400 million in total losses from the Coinbase insider incident, and millions more in remediation, regulatory penalties, and business disruption costs from ransomware and DDoS campaigns.

Threat Actor	Attack Type	Techniques	Impact
Fog Ransomware Group	Ransomware	Use of open-source penetration testing tools	Severe operational disruption; reputational damage
Toppan Attackers	Ransomware supply-chain attack	Exploited Toppan Next Tech's vulnerabilities	Data breach affecting 11,200 customers; financial losses
MirrorFace (APT)	Espionage and data exfiltration	Multi-vector: phishing, infiltration, data extraction	Theft of sensitive infrastructure and financial data
UAE DDoS & Ransomware Groups	DDoS, ransomware, phishing	Large-scale DDoS campaigns tied to extortion	Repeated service outages, business delays



Threat Actor	Attack Type	Techniques	Impact
DDoS-for-Hire Groups	Distributed Denial of Service	Volumetric DDoS attacks targeting APIs	Service outages
Lazarus Group	Crypto theft	Phishing, malware, wallet compromises	Largest theft in 2025: US$1.5 billion stolen from ByBit
Spyware Operators (Unnamed Multiple)	Spyware	Spyware targeting systems for financial data exfiltration	Widespread privacy breaches in Southeast Asia
Supply Chain Attackers	Supply-chain compromise	Exploiting third-party systems	Continuous breaches; high mitigation and regulatory costs
Insider Threat at Coinbase	Credential theft, insider attack	Insider social engineering, credential extraction	US$400M+ total cost, breach of 69,461 accounts

Top Vulnerabilities Targeted by Threat Actors

The financial services sector has remained a critical target for cyber threat actors, given its essential role in global industry and economic activities.

The vulnerabilities listed here represent high-impact risks affecting the financial services sector due to the nature of sensitive systems (e.g., APIs, cloud, databases, and mobile apps). Common threat vectors include credential theft, misconfigurations, code injections, and flawed third-party integrations.

This report profiles each vulnerability class, maps it to the threat vector, and identifies structural trends that will define vulnerability targeting through 2026.

Key Observations

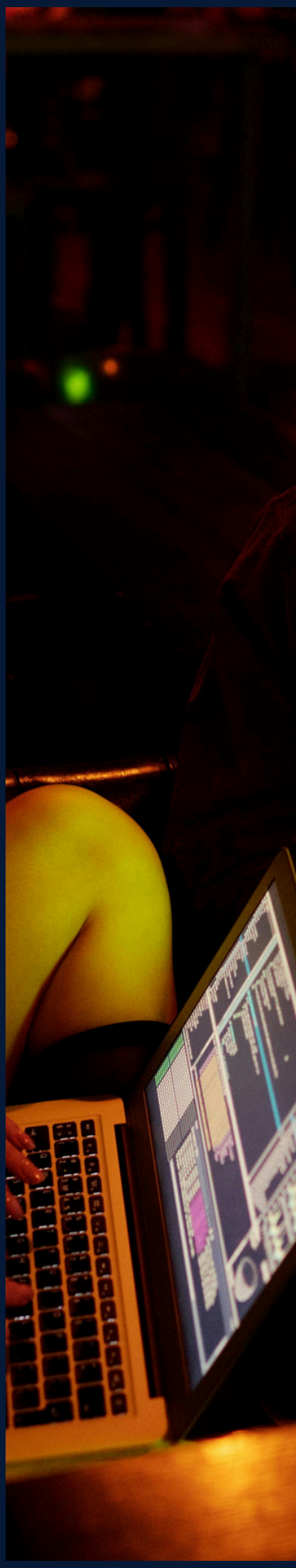
APIs and Digital Channels Have Become the Most Exploited Attack Surface: Of the ten CVEs profiled, four directly target APIs, web applications, and mobile banking channels — CVE-2025-10001 (open banking API escalation), CVE-2025-11235 (token bypass), CVE-2025-11601 (DDoS amplification via networking APIs), and CVE-2025-10567 (cross-site scripting in financial web apps). This concentration is not coincidental. The rapid acceleration of open banking mandates, mobile-first banking strategies, and API-driven fintech integrations has dramatically expanded the digital attack surface.

Legacy Technology Debt and Misconfiguration Are Amplifying Risk: A striking pattern is that many of the most critical vulnerabilities are not exotic zero-days — they are the consequence of known, preventable weaknesses: outdated Java libraries (CVE-2025-10239), encryption misconfigurations in mobile apps (CVE-2025-11689), weakly configured payment gateways susceptible to brute force (CVE-2025-11008), and improperly configured Kubernetes privileges in cloud environments (CVE-2025-11304). These vulnerabilities span every layer of the technology stack — from application code, to encryption protocols, to cloud orchestration infrastructure.

Third-Party and Infrastructure Vulnerabilities Enable Systemic Compromise: The most severe vulnerabilities in this profile — CVE-2025-11995 (RCE in financial databases), CVE-2025-10812 (backdoor injection via third-party vendor systems), and CVE-2025-11304 (Kubernetes privilege escalation) — share a defining characteristic: they do not just compromise a single application or data set; they enable complete, persistent, institution-wide control. Together, these vulnerabilities illustrate that the consequences of a single unpatched flaw in a critical system or trusted vendor can cascade into a catastrophic, enterprise-wide breach.

The vulnerabilities listed below represent commonly observed and high-impact vulnerability patterns based on aggregated threat intelligence and may include representative or modeled scenarios.

CVE	Description	Threat Vector	Impact
CVE-2025-11008	Payment gateway brute force exploit	Brute-forcing credentials or weakly configured payment gateways for unauthorized access.	Loss of customer payment information and fraudulent transactions
CVE-2025-11601	DDoS amplification abuse in networking APIs	Abuse of networking APIs for DDoS amplification attacks targeting public-facing systems.	Service disruptions due to amplified network load



CVE	Description	Threat Vector	Impact
CVE-2025-10001	Open banking API escalation vulnerability	Exploitation of improperly secured banking APIs by attackers escalating access rights	Unauthorized access to higher privilege APIs; potential fraud and information theft
CVE-2025-11235	Token bypass exposing sensitive customer transactions	Manipulation of token authorization mechanisms to bypass authentication layers	Transaction data leakage, exposing sensitive customer banking or financial data
CVE-2025-11995	RCE flaws in financial databases	Remote code execution vulnerabilities exploited within database servers hosting sensitive data	Complete system compromise with potential theft of critical financial transaction data
CVE-2025-10239	Java libraries exploited in banking apps	Vulnerable or outdated Java dependencies abused for unauthorized control	Remote code execution leading to theft, data breaches, and compromise of financial apps
CVE-2025-11689	Encryption misconfigurations in mobile banking apps	Misconfigured encryption protocols exploited to decrypt sensitive data in apps	Exposure of encrypted financial data leading to privacy breaches and fraud risks
CVE-2025-10812	Backdoor injection in third-party vendor systems	Exploitation of third-party vendor software vulnerabilities to inject persistent backdoors	Backdoor access enables remote control and data exfiltration from financial systems
CVE-2025-11304	Kubernetes privilege escalation in cloud hosting	Threat actors exploiting improperly configured Kubernetes privileges to escalate access	Unauthorized control of containerized applications hosting critical financial workloads

Top Malware Families Targeting the Financial Services Sector

The financial services sector, due to its critical role in global banking and financial infrastructure, has been a prime target for advanced malware campaigns in 2025. Below is a ranked list of the top 10 malware families used by the top threat actors targeting the Financial Services sector, along with their functionality, methods of exploitation, and their attributions.

This section profiles each malware family, draws cross-incident patterns, attribution, and identifies usage trends that will define the malware threat landscape through 2026.

Key Observations
Credential Theft Dominance: Most listed malware focuses heavily on credential harvesting for unauthorized access and financial fraud.
Advanced Evasion Techniques: Malware like AsyncRAT and Skuld employ robust anti-detection mechanisms, such as in-memory execution and sandbox evasion.
Phishing and Exploit Kits: A majority of malware dissemination relies on human error through phishing emails or vulnerabilities in popular systems.
Cryptocurrency Targets: Malware like Lumma and Skuld increasingly target crypto wallets and exchanges due to the rise of digital asset usage globally.

Insights & Trends:

- Many Remote Access Trojans (RATs) such as AsyncRAT, AgentTesla, and Remcos are instrumental in attack campaigns, emphasizing data exfiltration and espionage capabilities.
- Credential theft malware like Lumma Stealer and Formbook continues to rise, with primary targets including finance-specific credentials and cryptocurrency wallets.
- Ransomware and loaders facilitated by tools like Amadey are focused on delivering secondary payloads to financial systems.

Name	Functionality	Target	Attribution	Usage
AsyncRAT	Enables remote control of infected systems, keylogging, credential theft, file exfiltration, and desktop recording	Windows systems in financial services, finance, technology, and government sectors	Commonly used by amateur hackers to nation-state entities, prominent in Chinese cybercrime groups	Distributed via phishing emails, malvertising, and exploit kits
FakeUpdates	Deploys malicious browser updates to infect systems with malware and steal credentials	Targets browser users across all industries, focusing on Chrome and Edge users	Cybercriminal groups using fake software installers or browser updates as phishing payloads	Distributed via compromised websites, phishing emails, or malicious ads
AndroxGh0st	Python-scripted malware targeting .env files for credential harvesting, and exploits Laravel vulnerabilities	Targets cloud infrastructure (AWS, Office365, SendGrid) and financial services applications	Attribution linked to Xcatze malware group and potentially state-sponsored entities	Webshell deployment, credential harvesting from Laravel services, cloud system abuse
Remcos	Empowers attackers via remote control, credential harvesting, keylogging, and file monitoring	Focuses on business, government, and military sectors for espionage activities	Associated with organized cybercrime groups	Distributed via malvertising, phishing emails, and payload binders
Lumma Stealer	Steals data like credentials, cookies, credit card details, crypto wallets, and 2FA	Focuses on cryptocurrency wallets, 2FA extensions, and browser data	Attributed to a cybercriminal called “Shamel” who distributes Lumma via dark web forums	Phishing emails and fake software installers (e.g., VLC, game updates)

Name	Functionality	Target	Attribution	Usage
Formbook	Info-stealer designed to collect credentials, browser cookies, autofill data, and clipboard content	Targets businesses, government bodies, and small-medium enterprises	Often linked to cybercrime-as-a-service networks selling malware kits	Phishing campaigns, spyware loader for broader malware deployment
AgentTesla	Remote Access Trojan (RAT) for stealing credentials, keylogging, clipboard monitoring, and file exfiltration	Focuses on email systems, business networks, including IoT devices and industrial controls	Frequently used by entry-level cybercriminal groups and organizations	Distributed via phishing emails, fake invoices, and exploit tools
Amadey	Malware loader that distributes additional malicious payloads, focusing on spy modules and ransomware distribution	Business systems and non-targeted attacks across random industries, used for establishing loaders	Cybercriminal groups and malware resellers	Exploits vulnerabilities in web apps, generally spread via phishing and in bundled campaigns
ChromeKatz	Designed for browser credential theft specifically targeting Chromium-based browsers. Capable of stealing cookies	Finance, retail, and e-commerce platforms due to payment card theft	Used by cybercriminal groups leveraging point-of-sale data theft in browsers	Distributed via infected browser extensions/phishing emails aimed at financial theft campaigns
Skuld Stealer	Advanced info-stealer focused on cryptocurrency wallets, browser data, and gaming platforms	Crypto wallets like Metamask, gaming platforms, browser extensions, and financial apps	Possible attribution to cybercrime groups	Trojanized software, phishing payloads disguised as gaming cheats and crypto tools

References:

1. FS-ISAC and Akamai Report: DDoS Attacks on APAC Financial 11 Jun 2025 · In 2024, the Asia Pacific (APAC) financial services sector was the most targeted for volumetric DDoS attacks (38% of total).

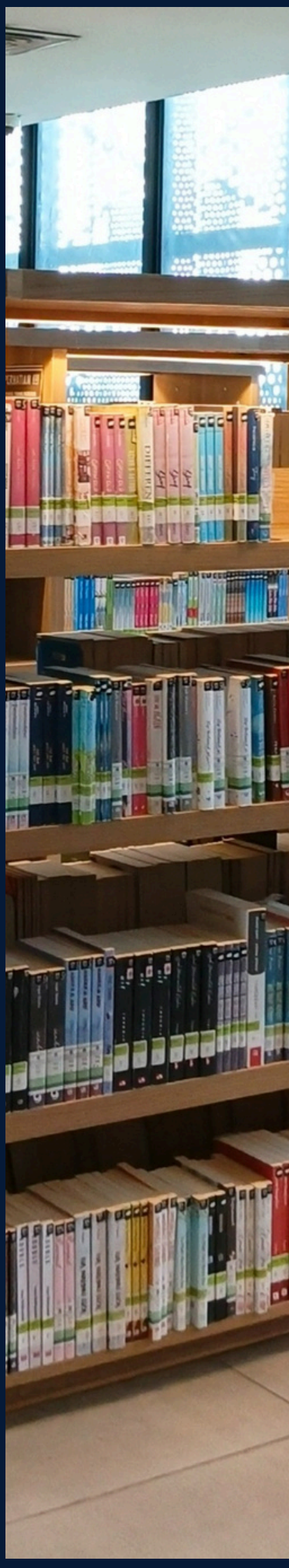
2. Cyber Espionage and Ransomware: East Asia's 2025 State-backed 19 Sept 2025 · Japan faced a surge in sophisticated cyberattacks throughout 2025, driven by a mix of state-sponsored espionage and regional disruption campaigns.

3. 2025 Global Cybersecurity Breach Analysis: Comprehensive Report A sophisticated Fog ransomware attack targeted an unnamed financial institution in Asia during May 2025, employing unusual toolsets.

4. Cyber Threats Are Rising Across Southeast Asia—Is Your Data 27 Oct 2025 · Cyber threats are intensifying across Southeast Asia, with data breach costs rising to $3.67M in 2025.

5. Cybersecurity firm reports a 70% spike in spyware attacks across 16 Nov 2025 · Kaspersky's enterprise solutions detected and blocked a total of 427,265 spyware attacks across Southeast Asia..

6. GCC Financial Crime, Cybersecurity Risks: Regulatory Responses 24 Dec 2025 · Financial institutions face sustained ransomware and DDoS campaigns, alongside large-scale data breaches.



Contact Us

Asia-ISAC

Website

www.asia-isac.org

Email

help@asia-isac.org

LinkedIn

www.linkedin.com/company/asia-isac