CROWDSTRIKE

Presented by:

VECTRA™
An ENSIGN Company

2026 FINANCIAL SERVICES THREAT LANDSCAPE REPORT

Table of Contents

Introduction

In 2025, financial services organizations faced a threat landscape defined by stealthy access, exploitation of vulnerable devices, and interactive intrusions designed to support theft, extortion, and intelligence collection. By Q1 2026, financial services ranked as the **fourth** most targeted sector, accounting for **12%** of total observed activity.

Globally, financial institutions experienced **43%** more hands-on-keyboard intrusions in 2025 than two years earlier. In North America, the trend was even more pronounced: Financial services organizations faced the highest level of targeting from both eCrime and state-sponsored adversaries, experienced a **48%** increase in interactive intrusions over the same period, and accounted for more than half of all Q1 2026 intrusions targeting the sector. These trends reflect the strategic value adversaries place on financial institutions and the need for defenders to detect and disrupt activity before access becomes impact.

Financial organizations remain attractive targets because they hold significant financial assets and high-value data, including cryptocurrency holdings, business intelligence, and customers' personally identifiable information (PII). They may also be perceived as more likely to pay a ransom because of the high availability requirements of financial operations. The rise in interactive activity further reflects adversaries' continued preference for hands-on-keyboard operations, which give them the flexibility to pursue theft, extortion, or intelligence collection after access is established.

AI-enabled social engineering may compound these challenges by helping adversaries craft more convincing lures, impersonate trusted users, generate realistic voice-based phishing attempts, and scale identity-based intrusion attempts across trusted access paths. At the same time, financial institutions' adoption of AI across customer support, fraud operations, software development, and internal workflows may expand the attack surface if these systems are not properly secured.

CrowdStrike observed a notable shift in eCrime activity targeting financial organizations in 2025 compared with 2024. Big game hunting (BGH) activity increased, reflected in a **27%** rise in financial services victims named on dedicated leak sites (DLSs), while initial access broker (IAB) activity advertising access to the sector declined. This drop may indicate stronger demand for access to other sectors or a growing preference for private partnerships between IABs and BGH operators, reducing visibility into these transactions.

MUTANT SPIDER was the most active threat to the financial services sector, driving the highest volume of intrusions and likely selling access to ransomware operators. CrowdStrike also observed SCATTERED SPIDER resume aggressive ransomware operations against insurance entities in Q2 2025, following a significant operational pause from December 2024 through March 2025. This activity marked a return to one of the group's historically common targeting patterns.

State-sponsored activity also remained persistent, driven largely by intelligence collection requirements. China-nexus adversaries posed the most significant intelligence collection threat to financial services organizations, particularly those in South and Southeast Asia. Their targeting likely reflects a priority to collect intelligence on economic conditions, PII, and data that can enable downstream espionage operations.

At the same time, Democratic People's Republic of Korea (DPRK)-nexus groups sustained operations targeting cryptocurrency and financial technology (fintech) entities. External blockchain analysts estimate DPRK-nexus groups stole **2.02 billion USD** in digital assets in 2025, a **51%** increase from 2024,[1] with stolen funds directly supporting the regime's military programs. In February 2025, PRESSURE CHOLLIMA conducted the largest single financial theft ever reported, stealing **1.46 billion USD** worth of cryptocurrency through trojanized software distributed via a supply chain compromise.[2] In Q4 2025, STARDUST CHOLLIMA tripled its operational tempo against financial entities, targeting individuals in cryptocurrency- and blockchain-adjacent roles across North America, Europe, and Asia.

These trends create acute operational risk for financial services organizations. Ransomware pressure on high-availability operations, sustained intelligence collection, and continued digital asset theft often unfold quickly across trusted access paths. As AI models continue to advance, adversaries are likely to increase the sophistication, scale, and speed of their operations. Defenders need intelligence-led visibility, continuous hunting, and the ability to act quickly with context.

CrowdStrike Counter Adversary Operations combines threat intelligence, managed threat hunting, and trillions of telemetry events from the AI-powered CrowdStrike Falcon® platform to detect, disrupt, and stop evasive adversaries. Counter Adversary Operations brings together two closely integrated teams: The CrowdStrike Intelligence team identifies new adversaries, tracks malicious activity, and captures emerging cyber threat developments in real time, and the CrowdStrike OverWatch team applies this intelligence through proactive threat hunting across customer telemetry to detect and disrupt malicious activity. Together, these teams deliver intelligence and hunting capabilities that help financial services organizations stay ahead of sophisticated adversaries.

The CrowdStrike 2026 Financial Services Threat Landscape Report presents analysis from the CrowdStrike Intelligence team covering activity observed from April 1, 2025, through March 31, 2026. The report details the key themes, trends, and events shaping the financial services threat landscape and provides anticipatory assessments to help organizations prepare for the continued evolution of eCrime and state-sponsored threats.

Explore the CrowdStrike Adversary Hub for the latest insights on adversaries, tradecraft, and activity.

1 https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/
2 https://www.ic3.gov/psa/2025/psa250226
https://www.elliptic.co/blog/bybit-hack-largest-in-history

ADVERSARY NAMING CONVENTIONS

BEAR	RUSSIA
BISON	BELARUS
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
HAWK	SYRIA
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SAIGA	KAZAKHSTAN
SPHINX	EGYPT
SPIDER	eCRIME
TIGER	INDIA
WOLF	TÜRKIYE

Sector Profile

The financial services sector comprises entities associated with currency management, including credit unions, banks, credit card companies, accountancy companies, consumer finance companies, stock brokerages, fintech entities, and investment funds. This sector connects with many adjacent industries and sectors, including insurance, cryptocurrency, financial management, and hedge funds.

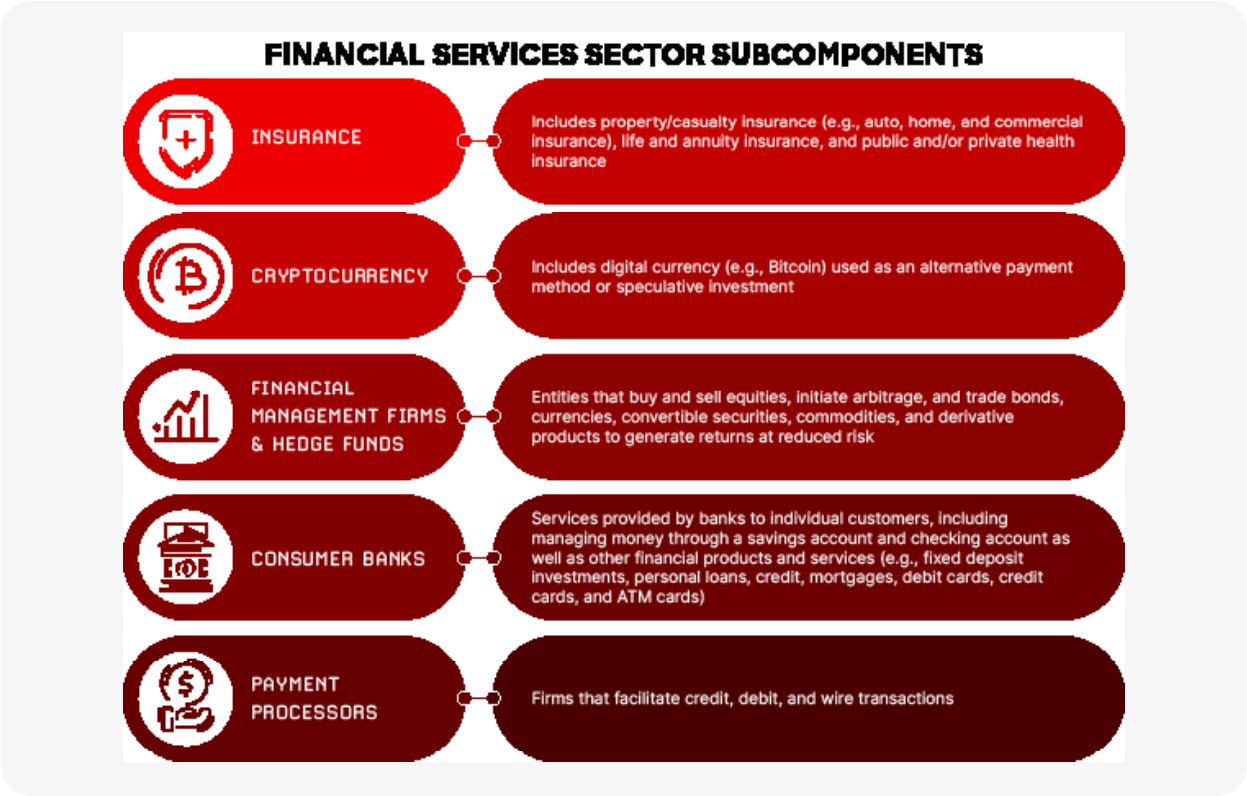

Figure 1. Financial services sector subcomponents

The financial services sector attracts threat actors of all motivations due to its unique convergence of valuable assets, strategic intelligence, and geopolitical significance:

- eCrime threat actors pursuing immediate financial gain target the sector through ransomware, data theft and extortion, credential harvesting, and cryptocurrency theft, exploiting the direct monetary value of banking credentials, payment systems, and digital assets.
- Targeted intrusion adversaries conduct intelligence collection and economic espionage to support governments' strategic objectives, gathering intelligence on economic policies, investment strategies, and market movements that inform geopolitical decision-making and secure competitive advantages. These adversaries also engage in financially motivated operations to evade international sanctions.
- Non-state threat actors, including hacktivists and ideologically motivated groups, target financial institutions to advance their political agendas, disrupt the economies of countries whose governments they oppose, or protest perceived injustices through distributed denial-of-service (DOS) attacks, data leaks, and reputational damage campaigns.

Collectively, these threats create a complex risk landscape. Financial institutions must defend against profit-driven criminals seeking immediate returns, sophisticated state-nexus threat actors pursuing long-term strategic intelligence objectives, and ideological threat actors weaponizing financial disruptions for political impact.

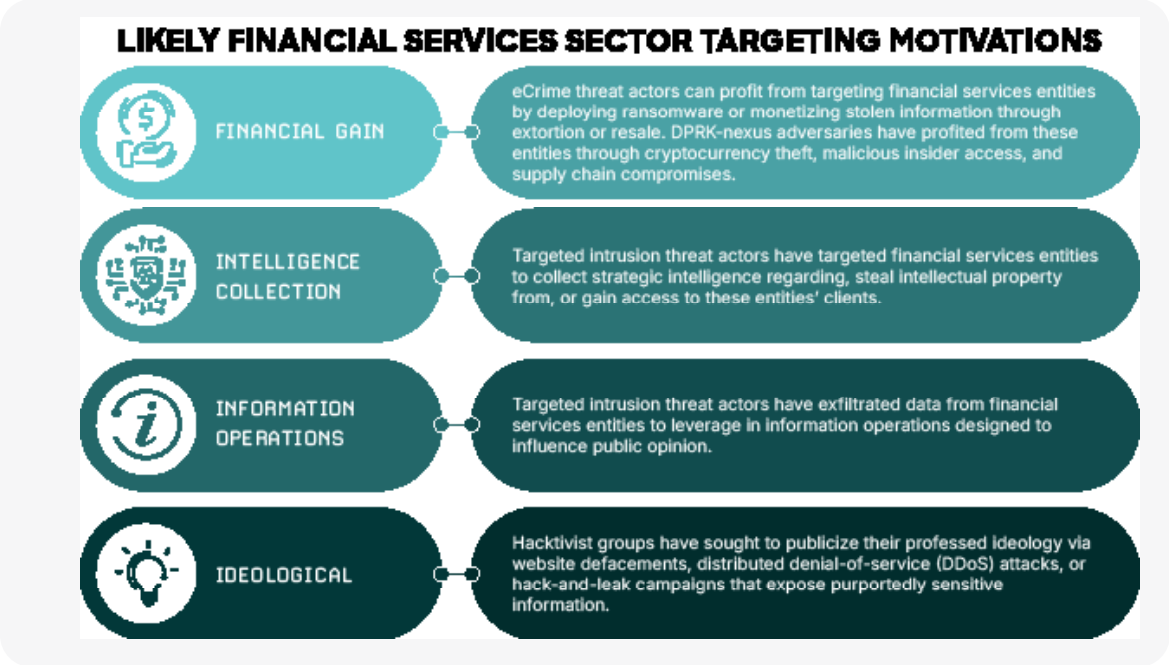

Figure 2. Motivations for targeting financial services entities

Data Snapshot

The intrusion breakdown for the financial services sector has remained consistent since 2023, with eCrime threat actors accounting for 75% of interactive intrusions and state-sponsored adversaries accounting for 25%. Three of the most prevalent malware families, *BeaverTail*, *BitStep RAT*, and *InvisibleFerret*, are used exclusively by FAMOUS CHOLLIMA, who conducts a high volume of sector-agnostic activity.

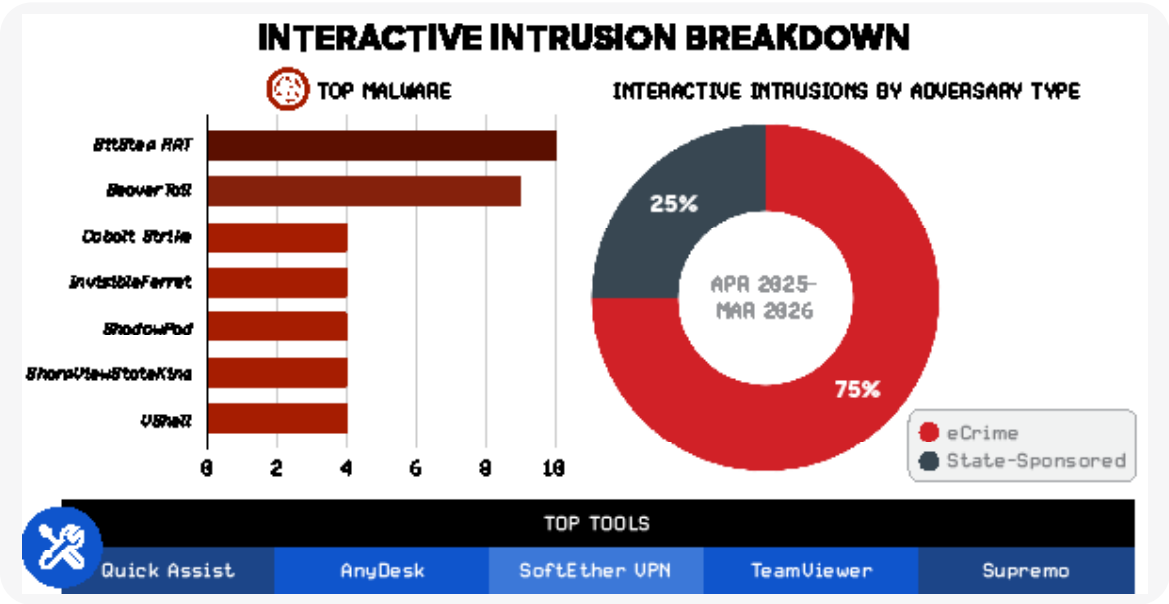

Figure 3. Financial services sector intrusion breakdown, April 1, 2025, to March 31, 2026

Adversary targeting remained global, but activity was concentrated around a defined set of priority countries. CrowdStrike Intelligence observed the highest volume of activity in Australia, Brazil, Canada, India, Indonesia, Israel, Ukraine, the United Kingdom, and the United States. This distribution reflects sustained adversary focus on major financial hubs and high-growth digital economies across North America, Europe, and Asia.

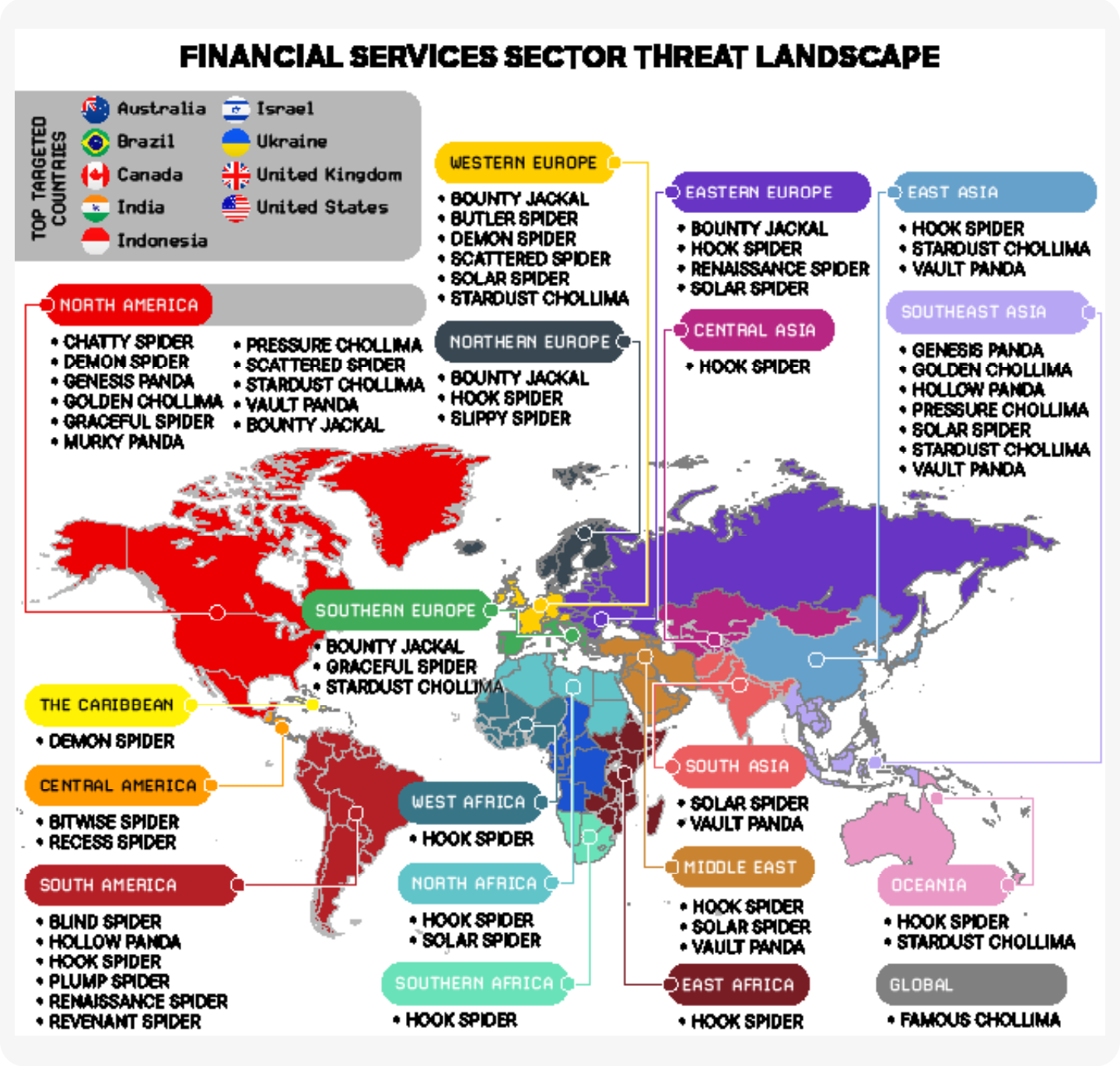

Figure 4. Financial services sector threat landscape, April 1, 2025, to March 31, 2026

Top Adversary Threats

During the reporting period, the adversaries highlighted in Figure 5 posed a persistent threat to the financial services sector. Based on analyzed targeting trends, these adversaries represent the most significant threats to the financial services sector for 2026. The following sections offer detailed analysis of these adversaries as well as additional adversaries who targeted financial services entities during the reporting period.

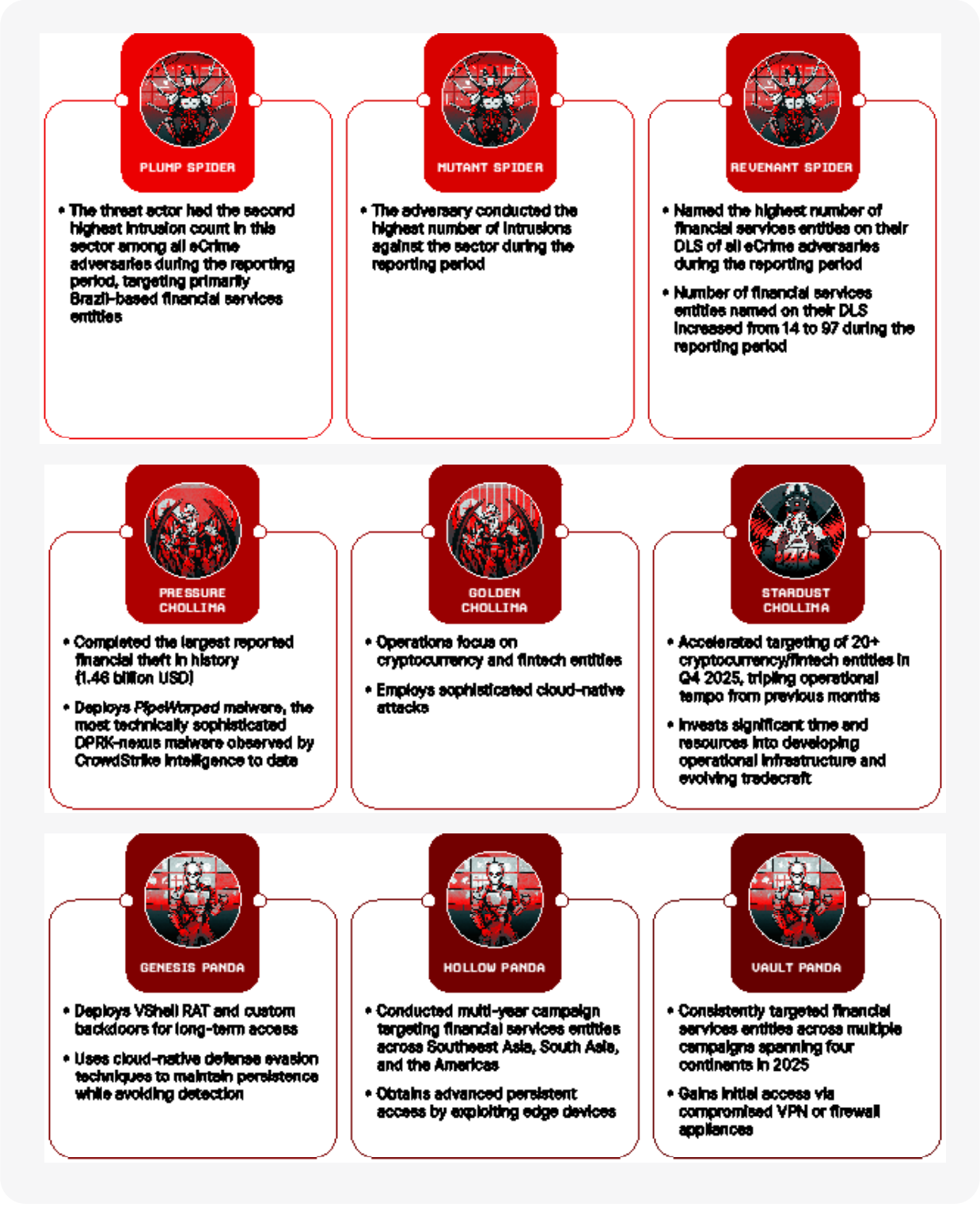

Figure 5. Top adversary threats to the financial services sector

eCrime

eCrime operations consistently target financial services entities due to the substantial amount of monetizable sensitive information that they possess, including Social Security numbers (SSNs) as well as customer names, addresses, and credit card details. CrowdStrike Intelligence has observed threat actors target the financial services sector directly in BGH operations and via enabling and commodity services.

Big Game Hunting

BGH adversaries gain initial access to victims via various techniques, including leveraging exploits, brute-forcing account credentials, and procuring network access from IABs. After gaining access, these adversaries often deploy ransomware, steal data, and threaten to publicly expose the stolen data on their DLSs, capitalizing on victims' desire to avoid the financial and reputational consequences of data leaks.

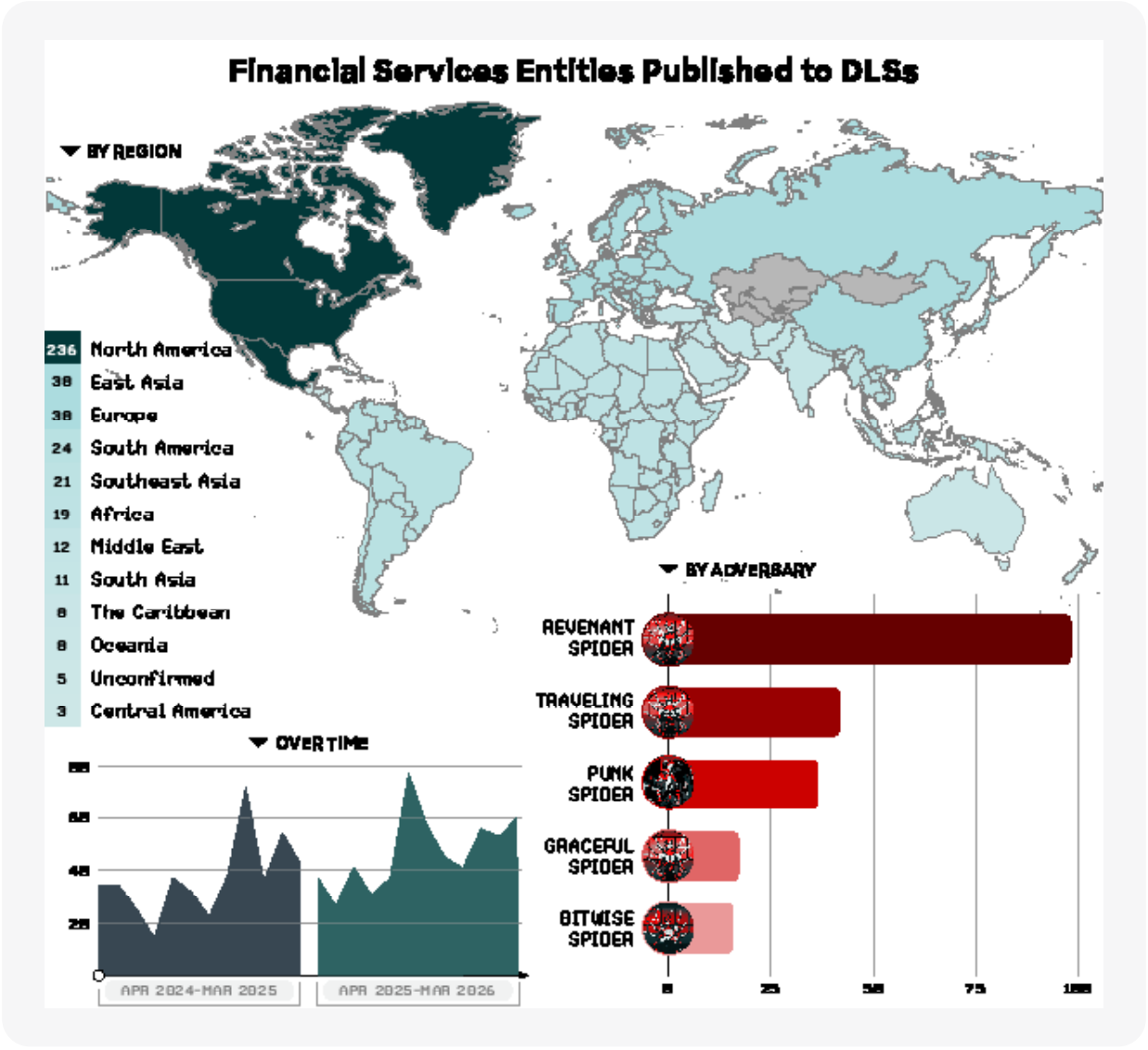

Figure 6. Top adversaries, top regions, and incident numbers for the financial services sector, April 1, 2025, to March 31, 2026

During the reporting period, BGH threat actors named 423 financial services entities on various DLSs, a 27% increase from the 334 financial services entities named to BGH adversary DLSs over the prior 12-month reporting period. This increase reinforces the sector's continued prioritization as a target for BGH operations.

Most organizations affected by BGH activity were located in North America, East Asia, and Europe. Figure 6 illustrates the most active BGH adversaries targeting the sector and the regions most frequently impacted from April 2025 to March 2026.

During the reporting period, the financial services sector was the sixth most targeted sector by BGH adversaries. REVENANT SPIDER, TRAVELING SPIDER, PUNK SPIDER, GRACEFUL SPIDER, and BITWISE SPIDER represent major threats to the financial services sector. These adversaries posted the most financial services entities to their respective DLSs. REVENANT SPIDER operates the *Qilin* ransomware as a service (RaaS); TRAVELING SPIDER operates the *INC*, *Lynx*, and *Sinobi* RaaS programs; and BITWISE SPIDER operates the *LockBit* RaaS. PUNK SPIDER operates *Akira* ransomware, and GRACEFUL SPIDER operates the *Clop* ransomware.

CrowdStrike Intelligence assesses that BGH operations will remain a significant threat to financial services entities over the next 12 months. This assessment is made with high confidence based on the following factors:

- Incidents impacting financial services entities increased 27% compared to the previous reporting period
- Over the last two years, the financial services sector has remained one of the ten most frequently targeted sectors by eCrime operations
- BGH operations are opportunistic and will target financial services entities whenever possible

eCrime Highlights

CHATTY SPIDER Sustains High-Tempo Data Theft and Extortion Campaigns Against Financial and Legal Organizations

In March 2025, CHATTY SPIDER continued to conduct high-tempo data theft and extortion campaigns, predominantly targeting legal and financial services entities. The adversary named and leaked data belonging to 41 victims on their DLS; among those victims, 14 were law firms and 10 were financial services entities, including accounting and insurance firms.

Following a mid-year hiatus from May 2025 to August 2025, CHATTY SPIDER resumed operations exclusively targeting law and insurance firms. The adversary continued to employ tactics, techniques, and procedures (TTPs) that have been observed in their operations since 2022: directly targeting users to establish a remote support session, downloading WinSCP to exfiltrate data from a single host, and threatening to leak stolen data on a clear web DLS unless their victim pays the demanded ransom.

CHATTY SPIDER will likely continue targeting financial services entities, including insurance entities, throughout 2026. This assessment is made with high confidence based on their high operational tempo throughout the reporting period and their historical target patterns.

International Law Enforcement Operation Dismantles Investment Fraud Network

On October 1, 2025, Spain's Policía Nacional disclosed details of a major international law enforcement operation conducted on September 17, 2025.[3] Coordinated by the European Union Agency for Criminal Justice Cooperation (Eurojust) with support from Europol, the operation successfully dismantled an eCrime network responsible for defrauding victims of more than 102 million EUR (approximately 120 million USD) through fraudulent online investment platforms since 2018.

The criminal organization operated through a network of shell companies and fraudulent investment platforms that promised victims unrealistic returns on their investments in cryptocurrencies, currencies, and technology products, enabling large-scale victimization across multiple jurisdictions.

In addition to arresting six individuals across four countries, authorities conducted multiple property searches, seized cryptocurrency and precious metal assets, and froze 83 bank accounts. The operation highlights eCrime threat actors' continued use of ostensibly legitimate investment platforms to facilitate fraud and convert stolen funds into cryptocurrency. At the same time, the operation demonstrates Spain's likely increasing capacity for and commitment to combating cybercrime.

SCATTERED SPIDER Aggressively Targets Insurance Entities, April 2025 to July 2025

The prolific eCrime adversary SCATTERED SPIDER has conducted various financially motivated operations since early 2022. CrowdStrike Intelligence assesses that the adversary's intent in these intrusions was to deploy ransomware on VMware ESXi infrastructure, reinforcing their continued focus on financial services and insurance organizations.

Throughout the reporting period, SCATTERED SPIDER employed the same tactics across their operations targeting insurance and retail victims, gaining initial access primarily through help desk social engineering by impersonating legitimate employees and claiming to require password and/or multifactor authentication (MFA) resets. After compromising the victim environments, SCATTERED SPIDER pivoted to integrated SaaS applications to search for data — including credentials and documentation — to support lateral movement or extortion.

In September 2025, the U.K.'s National Crime Agency (NCA) announced it had arrested and charged two SCATTERED SPIDER members — Thalha Jubair and Owen Flowers,[4] both of whom used adversary-associated monikers — for allegedly targeting the U.K.-based transport authority Transport for London in August 2024.

Enabling and Commodity Threats

Initial Access Brokers

IABs enabled eCrime operations by selling pre-compromised access, reducing the time and effort required by downstream threat actors to identify and compromise targets.

During the reporting period, IABs advertised 4,550 accesses on eCrime forums, a 10% increase from the 4,120 advertisements in the previous reporting period. Despite this overall increase, advertisements for financial services entities decreased 40%, from 155 to 93 listings.

3 https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=16674#
https://www.eurojust.europa.eu/news/eurojust-coordinates-action-halt-cryptocurrency-fraud-over-100-million-euros-across-europe

4 https://www.justice.gov/opa/pr/united-kingdom-national-charged-connection-multiple-cyber-attacks-including-critical

CrowdStrike Intelligence identified 41 IABs advertising access to financial services entities, a 31% decrease from 59 IABs in the previous reporting period. The 41 IABs targeted entities across 12 regions, continuing a geographically distributed pattern previously observed.

This decrease in IAB activity may reflect threat actors' formation of private partnerships with BGH operators, negating their need to publicly advertise accesses and reducing visibility into their sales.

Although financial services access represents a small share of advertised IAB listings, the risk to the sector remains disproportionate. A single foothold in a high-value environment is enough to enable ransomware deployment, data theft, and downstream fraud.

Figure 7 compares the number of IAB advertisements for financial services entities across the reporting periods and highlights the regions most frequently targeted. Most advertised financial services entities were either unconfirmed or located in the United States.

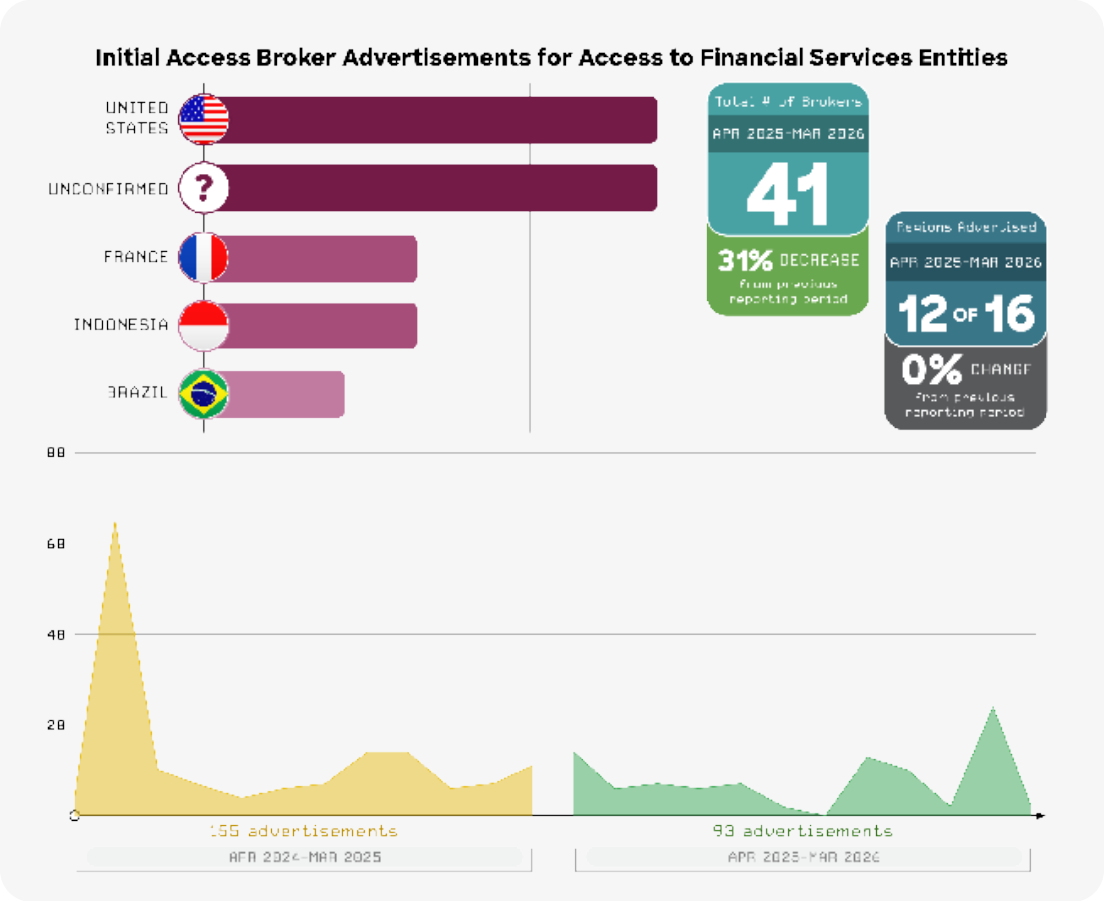

Figure 7. Summary of IABs targeting financial services entities, April 1, 2025, to March 31, 2026

Throughout the reporting period, advertised asking prices for access to financial services entities ranged from 100 USD to 1,000,000 USD. The average price was 23,252.41 USD, and the median price was 920.25 USD.

CrowdStrike Intelligence assesses that IABs will likely continue to opportunistically target financial services entities over the next 12 months. Despite the decline in the number of financial services entities advertised during the reporting period, this assessment is made with high confidence given eCrime threat actors' continued use of IAB services to access victim networks.

Commodity Malware and MaaS Threat Actor Highlight: MUTANT SPIDER

eCrime threat actors often access victim networks via commodity malware, distribution services, or malware as a service (MaaS) offerings.

MUTANT SPIDER was the most active threat to the financial services sector during the reporting period, with the highest volume of intrusions across the sector. This eCrime adversary likely sells access to ransomware groups, enabling faster and more scalable attacks.

To gain initial access, the adversary primarily leverages voice phishing (vishing) campaigns over Microsoft Teams, often impersonating internal IT support to manipulate users into resetting credentials and MFA, a tactic that AI-generated voice and text may make more convincing. This technique enables the threat actor to bypass traditional email-based defenses and quickly establish access. Additionally, the group deploys various custom tools — such as *PrionFlaire*, *SocksLoader*, and *SleepyMutagen* — to support post-access activity.

MUTANT SPIDER's opportunistic targeting model does not limit impact. Their reliance on scalable vishing operations and repeatable access techniques supports sustained intrusion volume across sectors, including financial services. CrowdStrike Intelligence assesses with moderate confidence that this activity will continue, supported by increased vishing operations observed since October 2024.

MUTANT SPIDER poses a significant threat to financial services organizations, responsible for the highest volume of intrusion affecting the sector via vishing campaigns.

Targeted eCrime

SOLAR SPIDER Targets Financial Sector with RATs, Custom Java-Based Tooling, and Updated *Meduza Stealer*

Throughout the reporting period, SOLAR SPIDER continued to target financial institutions in Europe, the Middle East, South Asia, and Southeast Asia using financial transaction-themed lures to entice targets into downloading various remote access tools (RATs): *JsOutProx*, *SorillusRAT*, *STRRAT*, and *WSH RAT*. Notable activity includes:

- In April 2025, the adversary expanded targeting to banks and foreign exchange services across Europe and North America, building on their historical focus in Africa and Asia. Campaigns conducted during this period leveraged a previously unobserved version of *Meduza Stealer*.
- From mid-May 2025 to early July 2025, SOLAR SPIDER continued to deploy *JsOutProx* and *STRRAT* and introduced *NetSupport RAT* into operations. Additionally, the adversary experimented with various commodity tools, including using *HijackLoader* to deliver *SpectreRAT* in June 2025 and July 2025.

SOLAR SPIDER will likely remain a persistent threat to the financial services sector throughout 2026. This assessment is made with high confidence based on the adversary's sustained targeting of the sector since 2018 and their continual modification of their TTPs.

SOLAR SPIDER has persistently targeted financial institutions for nearly eight years, adapting their tooling and delivery methods to sustain operations.

PLUMP SPIDER Demonstrates How Regional Specialization Drives High-Impact Financial Fraud

PLUMP SPIDER is a Brazil-based eCrime adversary that has consistently targeted Brazilian financial entities since at least September 2023 by attempting to gain access to internal payment systems and conduct fraudulent transactions. This positions PLUMP SPIDER as a direct financial theft threat rather than a data theft or extortion threat actor.

Throughout the reporting period, PLUMP SPIDER combined social engineering with hands-on intrusion techniques to establish and maintain access. In March 2025, the adversary conducted vishing campaigns against Brazil-based financial institutions, leveraging a novel technique to download and install SoftEther VPN via an obfuscated batch script, and deployed a custom credential harvesting tool to obtain web browser credentials.

From mid-September 2025 to mid-October 2025, PLUMP SPIDER continued to leverage their typical IT support-themed phishing tactics against various sectors, including the financial services sector, to prompt users to download and execute various tools — including remote monitoring and management (RMM) tools, SoftEther VPN, and *Xworm* — hosted on compromised government domains. The adversary also continued to modify their delivery methods, delivering *Xworm* via DLL sideloading and using batch scripts to configure and install SoftEther VPN on victim systems.

In February 2026, PLUMP SPIDER shifted to email-based phishing campaigns, impersonating Brazilian law enforcement and using investigation-themed phishing lures to entice targets to open malicious links in PDF attachments. The links hosted Inno Setup installers deploying previously unobserved *Kapa* downloaders that PLUMP SPIDER used to deliver *HijackLoader*-packed *HijackRAT* payloads after intrusion.

This combination of targeted financial access, localized social engineering, and evolving delivery techniques reinforces PLUMP SPIDER's effectiveness as a regionally specialized threat. CrowdStrike Intelligence assesses with high confidence that this activity will continue through 2026 based on their consistent targeting scope, historical activity, and demonstrated ability to modify delivery methods.

Threat Actor Targets Japan Using New Phishing Kit to Compromise Trading Accounts and Manipulate Stock Prices

In early April 2025, one or more unknown threat actors conducted account takeover campaigns targeting user accounts of several Japanese online services, particularly securities companies. The threat actors then purportedly used compromised trading accounts to primarily purchase China-based companies' thinly traded stocks (aka penny stocks) to artificially inflate prices and cash out their earlier positions.

One or more Chinese-speaking threat actors highly likely conducted these campaigns, which commenced in November 2024, using the same phishing kit. This assessment is made with high confidence based on Chinese-language comments contained in the phishing kit's code, the campaign's predominant use of China-based infrastructure, and the fact that the targeted data was sold on the Chinese eCrime marketplace Chang'an.

Targeted Intrusion

In 2025, targeted intrusion activity against the financial services sector was driven by a range of strategic objectives, including revenue generation and intelligence collection, across multiple adversaries:

- **China-nexus adversaries** posed the most significant espionage threat, consistently exploiting edge devices to target financial institutions — particularly in South and Southeast Asia — for economic intelligence collection.

> **DPRK-nexus adversaries posed a major threat to financial services entities, stealing a record 2.02 billion USD in digital assets in operations targeting fintech entities.**[5]

- **Iran- and Russia-nexus adversaries** conducted comparatively limited activity, with Iranian adversaries primarily focusing on geopolitically motivated operations in conflict areas and Russian adversaries focusing on Ukrainian financial entities.
- **Non-state hacktivist groups** conducted widespread DDoS campaigns and data breach operations against financial institutions; this activity responded to various geopolitical conflicts and demonstrated these groups' increased coordination and sophistication.

5 https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/

China

Figure 8. China-nexus financial services sector threat landscape, April 1, 2025, to March 31, 2026

Throughout 2025, China-nexus adversaries conducted sustained operations against the global financial services sector, demonstrating both geographic breadth and tactical diversity. The following operations leveraged consistent China-nexus TTPs, including exploiting edge devices, conducting DLL search-order hijacking, using compromised infrastructure for command and control (C2) communications, and targeting cloud environments:

- HOLLOW PANDA targeted financial institutions in South America and Southeast Asia by exploiting Check Point VPN appliances and deploying *ShadowPad* malware.
- VAULT PANDA operated across multiple regions, deploying *KEYPLUG* malware via DLL search-order hijacking and targeting both financial institutions and supporting entities, including a Middle East fintech organization.
- GENESIS PANDA targeted a Southeast Asia-based financial entity and a North American fintech organization, deploying VShell implants and FScan utilities and leveraging infrastructure linked to prior China-nexus operations.
- MURKY PANDA deployed a unique Chinese operational relay box (ORB)[6] network to access Microsoft 365 email accounts from more than 150 IP addresses in 36 countries. The activity targeted 340 organizations across more than 30 sectors; financial services was among the adversary's most frequently targeted sectors.
- VERTIGO PANDA targeted organizations in the Philippines, deploying the *InstituteX* RAT via infected USB devices.

These intrusions likely reflect China-nexus adversaries' prioritization of financial services entities as sources of intelligence on economic conditions, PII, and data that can facilitate downstream espionage operations.

THESE ADVERSARIES' SUSTAINED FOCUS ON SOUTH AND SOUTHEAST ASIAN FINANCIAL SERVICES ENTITIES LIKELY DEMONSTRATES THEIR STRATEGIC INTEREST IN GAINING ACCESS TO REGIONAL FINANCIAL SYSTEMS AND ECONOMIC INTELLIGENCE ACROSS MULTIPLE DEVELOPING MARKETS.

6 An ORB network is a traffic relay system — generally composed of a mix of compromised devices and leased servers — used to obfuscate the origin and destination of malicious traffic.

HOLLOW PANDA Conducts Multi-Year Economic Espionage Campaign Against Global Financial Sector

Financial services organizations, particularly investment-focused companies and economic management entities, should remain vigilant in defending their environments against HOLLOW PANDA, a Chinese state-sponsored adversary who has systematically targeted the financial sector across Southeast Asia, South Asia, and the Americas since at least 2023. In 2025, the adversary conducted confirmed intrusions at financial institutions in the Philippines, Indonesia, and Brazil.

This adversary pursues intelligence collection and industrial espionage goals aligned with the Chinese Communist Party strategic objectives outlined in China's 14th and 15th Five-Year Plans, specifically targeting organizations whose financial data and investment strategies provide insights into economic management and resource allocation strategies.

HOLLOW PANDA likely exploits Check Point VPN appliances to gain initial access and subsequently deploys *ShadowPad* malware via DLL search-order hijacking. The adversary configures the malware to leverage DNS tunneling techniques, enabling covert C2 communications and long-term persistent network access.

Combined with their proven ability to maintain undetected access to victim systems for extended periods while exfiltrating data, HOLLOW PANDA's focus on China's near abroad and strategic investment corridors poses an ongoing threat to financial institutions operating in Asia Pacific markets or managing investments related to Chinese economic interests.

DPRK

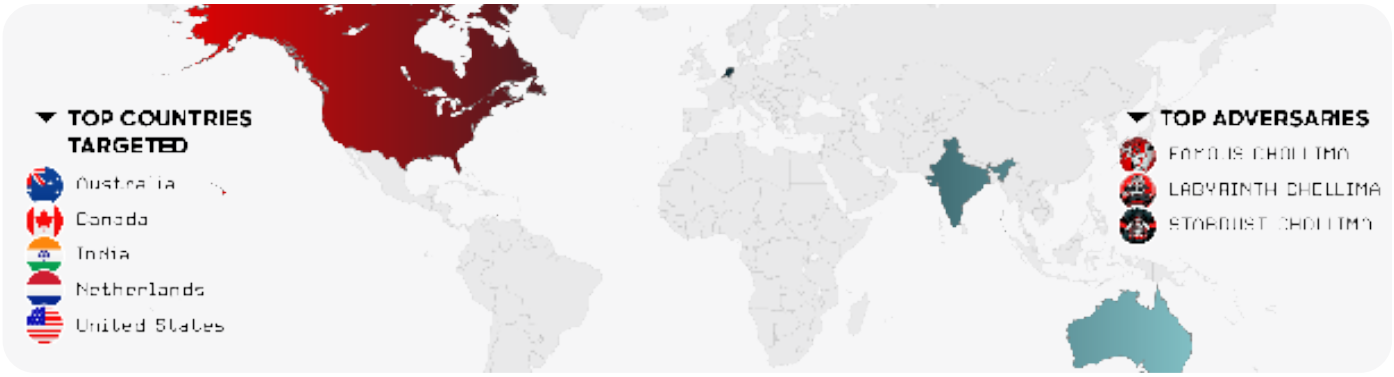

Figure 9. DPRK-nexus financial services sector threat landscape, April 1, 2025, to March 31, 2026

DPRK-nexus adversaries remained the most prevalent targeted intrusion threat to the financial services sector in 2025, with activity overwhelmingly focused on cryptocurrency and fintech organizations. With the exception of FAMOUS CHOLLIMA'S insider threat activity, these threat actors concentrated on digital asset ecosystems where theft can be executed and monetized at scale.

Based on blockchain tracking, DPRK-nexus adversaries stole the equivalent of 2.02 billion USD in digital assets in 2025, a 51% increase from 2024.[7] This figure represents the largest collective theft of digital assets among all tracked adversaries in 2025. Stolen proceeds are almost certainly laundered to fund the regime's military programs.

Compared to 2024, DPRK-nexus adversaries conducted fewer campaigns but achieved significantly higher returns by prioritizing high-value targets.[8] Targeting centered on Web3 companies, blockchain investment firms, cryptocurrency exchanges, and digital asset management platforms, where stolen funds can be cashed out more easily and with greater anonymity than within the traditional financial system.

PRESSURE CHOLLIMA represents the most acute threat within this group, possessing high intent and capability to execute large-sum theft. In February 2026, PRESSURE CHOLLIMA executed the largest single financial theft reported to date by compromising Safe{Wallet}, a digital asset management platform supporting cryptocurrency exchanges, to target funds held by the centralized cryptocurrency exchange Bybit. The adversary initially gained access to Safe{Wallet} systems by compromising a software developer's machine via a trojanized Python project (likely delivered using social engineering tactics) and exfiltrating development-related credentials.

7 https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/
8 Ibid

PRESSURE CHOLLIMA Deploys Advanced *PipeWarped* Malware Against Fintech Targets

In August 2025, PRESSURE CHOLLIMA began deploying the first observed instances of *PipeWarped* malware — the most technically advanced DPRK-nexus malware CrowdStrike Intelligence has observed to date — in operations targeting fintech entities.

PipeWarped is a highly sophisticated macOS malware family designed for flexibility and modularity. The malware supports numerous configurations, multiple network protocols, plugin loading, and comprehensive C2 capabilities. *PipeWarped* employs a sophisticated inter-process communication (IPC) architecture that orchestrates all malware operations and enables communication between components.

PRESSURE CHOLLIMA will highly likely continue to use this malware family against fintech targets in the long term. This assessment is made with high confidence based on *PipeWarped*'s increased sophistication compared to previous DPRK-nexus malware families and the resources PRESSURE CHOLLIMA likely invested to develop it.

STARDUST CHOLLIMA conducted nearly three times as many operations in October 2025 compared to previous months. Between November and December 2025, the threat actor targeted at least 21 cryptocurrency and fintech organizations across North America, Europe, and Asia. These operations relied on sophisticated social engineering tactics, including impersonation of recruiters on LinkedIn and Telegram, delivery of malicious coding challenges disguised as technical assessments, and the use of staged inauthentic video conferencing environments using images and videos of legitimate cryptocurrency professionals. AI tools can make these tactics more efficient and harder to detect by helping adversaries scale convincing engagement across languages and platforms.

GOLDEN CHOLLIMA complemented these efforts by delivering the *SnakeBaker* and *NodalBaker* malware families to fintech companies in Southeast Asia and Canada through recruitment-themed lures, successfully diverting cryptocurrency funds and accessing targets' cloud environments.

FAMOUS CHOLLIMA, the most active DPRK-nexus adversary in 2025, doubled their operational volume compared to 2024 while continuing to opportunistically target cryptocurrency exchanges, fintech platforms, and traditional banking institutions across North America, Europe, and the Asia Pacific region. Their malware-driven campaigns, publicly tracked as Contagious Interview campaigns, frequently target blockchain developers through fake freelance job postings. Rather than initiating contact with potential victims, the adversary engages victims once they apply for an advertised position. For example, FAMOUS CHOLLIMA has obtained access to enterprise environments via *BeaverTail* activity that highly likely resulted from a victim using corporate assets to apply for these freelance positions.

The 2025 campaigns underscore DPRK-nexus adversaries' substantial operational evolution from 2024, characterized by increased operational tempo, higher-value thefts, more advanced social engineering tradecraft, expanded geographic reach, and a sustained focus on cryptocurrency and blockchain ecosystems. These operations will likely continue to intensify in 2026, as international sanctions against the DPRK and the country's need to fund its military activities continue to drive aggressive cyber-enabled revenue generation activity.

Iran

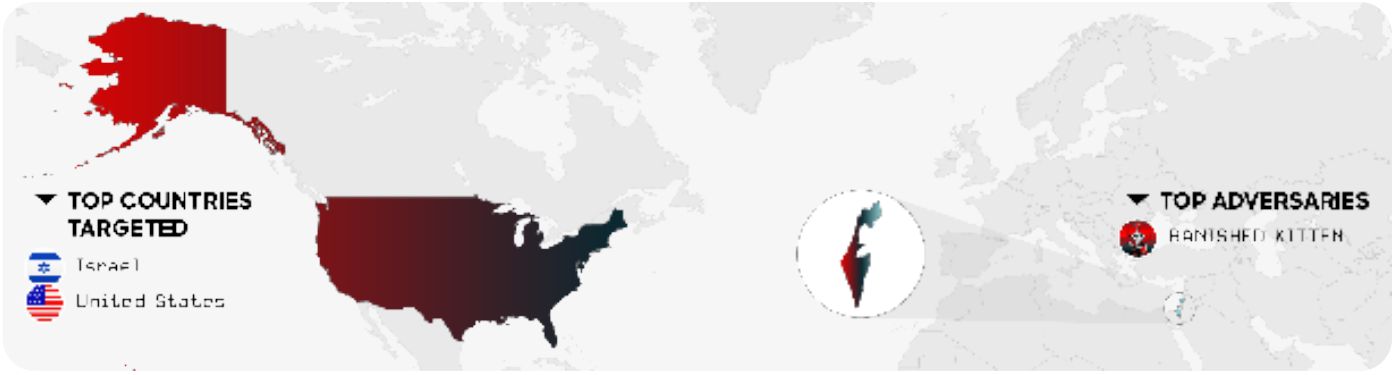

Figure 10. Iran-nexus financial services sector threat landscape, April 1, 2025, to March 31, 2026

CrowdStrike Intelligence observed limited Iran-nexus activity targeting the financial services sector in 2025, indicating a low baseline threat to the industry; however, Iran will likely continue to employ selective opportunism in targeting Western and Gulf entities. This could include broadened cyber efforts against Western organizations across various industries, including the financial sector, in the near to intermediate term; however, this will almost certainly be highly dependent on changing conflict dynamics.

Iran-nexus adversaries will likely continue conducting broad intelligence collection activities aligned with Iran's national interests, including activity targeting Western entities and their Gulf allies.

Russia

CrowdStrike Intelligence observed very limited Russia-nexus targeting of the financial services sector in 2025. However, Russia-nexus adversaries targeted adjacent sectors (e.g., the technology sector), likely to pursue long-standing intelligence collection objectives.

In mid-December 2025, FANCY BEAR likely targeted a prominent Ukrainian investment and financial services company using a malicious Microsoft Office document tailored to the company. The document contained a macro that delivered *FrameLoader*, a steganographic loader extracting its next stage payload from a PNG file container dubbed *EvilFrame*. The chain ultimately delivered a custom *Covenant Grunt* payload. Previously, in 2023, FANCY BEAR and VOODOO BEAR likely targeted this same Ukrainian entity in various phishing campaigns.

CrowdStrike Intelligence assesses that Russia-nexus adversaries do not pose a significant threat to financial services entities geolocated outside of Ukraine, unless such entities directly connect to Russia's immediate sphere of interest. In 2026, Russia-nexus adversaries will likely continue to conduct limited operations targeting Ukraine-based financial services entities, especially those providing essential services or involved in the Ukrainian war effort. This assessment is made with moderate confidence based on the limited observations of Russia-nexus activity targeting the financial services sector and Russian intelligence services' historical and current intelligence collection priorities.

Rest of World

CrowdStrike Intelligence observed limited financial services sector targeting from rest-of-world adversaries in 2025 and none during the reporting period. However, activity in late 2024 and early 2025 provides context on the limited but highly targeted threat these adversaries may pose.

India- and Kazakhstan-nexus adversaries primarily targeted government and government-adjacent sectors, including military and defense, to fulfill regional intelligence collection requirements. Financial targeting was rare and largely confined to state-linked institutions. For example, Kazakhstan-nexus adversary COMRADE SAIGA targeted Kyrgyzstan's Ministry of Finance and the state-run National Bank of the Kyrgyz Republic between late 2024 and early 2025. They used spear-phishing campaigns to deliver archive files containing decoy documents and malicious executables, including the unique *JLORAT* implant and open-source red-team tools. This activity suggests an expansion into financial governance targets to gain insight into national economic systems.

Private sector targeting was even less frequent. In January 2025, India-nexus adversary OUTRIDER TIGER targeted two Bangladesh-based organizations — including a private bank — using *Havoc*, an open-source post-exploitation framework, and a likely compromised Bangladeshi government email account. No follow-on activity was observed, and the objective remains unclear.

CrowdStrike Intelligence assesses that rest-of-world adversaries pose a limited threat to financial services entities in 2026. Targeting will likely remain focused on government-operated financial institutions in countries of immediate geopolitical interest. Private financial institutions face minimal risk unless they operate in regions aligned to these adversaries' intelligence collection priorities, such as Bangladesh for India-nexus threat actors or Kyrgyzstan for Kazakhstan-nexus threat actors. This assessment is made with moderate confidence based on limited observed activity and a consistent focus on government and defense sectors for regional intelligence collection.

Non-State

Figure 11. Non-state financial services sector threat landscape, April 1, 2025, to March 31, 2026

From April 1, 2025, to March 31, 2026, hacktivist groups conducted widespread DDoS campaigns and data breach operations against multiple sectors, including the financial services sector. These operations were primarily driven by geopolitical conflicts, including the Russia-Ukraine war, the Israel-Hamas conflict, the Cambodia-Thailand border tension, the India-Pakistan conflict, Sudan's civil war, and the U.S.-Israel-Iran conflict. Hacktivists demonstrated increased coordination, with groups amplifying each other's operations across social media, and conducted operations that combined ideological and financial motivations.

Pro-Russia hacktivist adversary BOUNTY JACKAL was among the most active threat actors, conducting extensive and near-daily DDoS campaigns against European entities, including financial services entities. Targeting focused on countries perceived as supportive of Ukraine through military or financial aid, those seen as aligned with the U.S. and Israel amid the U.S.-Iran conflict, and nations characterized by the adversary as Russophobic. This targeting was almost certainly largely opportunistic, as they leveraged their *DDoSia* attack toolkit to coordinate these campaigns with their global volunteer network. BOUNTY JACKAL also collaborated with like-minded hacktivists, including *Z-Alliance* (aka *Z-Pentest*, *Z-Pentest Alliance*), to target European financial services entities.

Numerous BOUNTY JACKAL campaigns were almost certainly timed to coincide with ongoing elections or protests in Europe, highlighting the adversary's broader anti-EU motivation and efforts to amplify disruption and influence public sentiment alongside technical impact. From October 2025 to November 2025, pro-Russia hacktivist groups *Killnet* and *Beregini* conducted a large-scale cyberattack against six Ukrainian insurance companies, exfiltrating PII and demonstrating both ideological and financial motivations in their attempts to sell the stolen data.

Hacktivist coalitions also emerged in 2025, with hacktivist groups *Keymous+*, *Ghilan Legion*, and *Hezi Rash* launching coordinated DDoS attacks against United Arab Emirates (UAE)-based financial entities under the #Stand_With_Sudan and #OpUAE campaign banners. Additionally, *Holy League* coordinated multi-group campaigns targeting Israeli financial services during the two-year anniversary of the October 7, 2023, Hamas attacks against Israel.

BOUNTY JACKAL's Persistent DDoS Threat to Western Financial Institutions

Financial services organizations — particularly those conducting business in Europe, in North America, or with entities that appear to support Ukraine — should remain vigilant against attacks from BOUNTY JACKAL. This pro-Russia hacktivist group was the most active DDoS adversary during the reporting period, claiming responsibility for attacks against hundreds of government and private sector entities, including financial services organizations.

In Q4 2025, BOUNTY JACKAL claimed to conduct DDoS attacks impacting French postal service La Poste and the company's banking provider, La Banque Postale. The activity caused limited disruptions to several services; however, La Banque Postale stated that payments, interbank transfers, cash withdrawals, in-store purchases, transfers, and online payments were not impacted.

Though BOUNTY JACKAL is primarily motivated by their ideological opposition to Western support for Ukraine, the group conducts opportunistic DDoS campaigns using their custom *DDoSia* toolkit, which is deployed by cryptocurrency-compensated volunteers. These campaigns target entities in countries providing military or economic aid to Ukraine, and such entities frequently include financial services firms due to their role in sanctions enforcement and economic support mechanisms.

Despite a July 2025 Europol-led operation (Operation Eastwood) that resulted in arrest warrants and temporary disruptions to *DDoSia* infrastructure, within days, BOUNTY JACKAL announced they had resumed operations. The adversary continues to coordinate multi-vector DDoS campaigns designed to cause website outages and service disruptions with other pro-Russia hacktivist groups, including *Z-Alliance*.

Financial institutions should anticipate continued DDoS activity from BOUNTY JACKAL — particularly during periods involving announcements of Western aid packages to Ukraine, international summits addressing the Russia-Ukraine war, or sanctions-related events — and should engage DDoS mitigation services, monitor for unusual traffic spikes, and implement incident response plans to ensure rapid service restoration following attacks.

Outlook

The financial services sector faces a sustained and multidimensional threat environment in 2026, driven by profit-motivated eCrime threat actors, state-sponsored adversaries pursuing strategic intelligence objectives, and hacktivists seeking to advance an ideological cause.

eCrime activity will remain the most consistent and operationally disruptive threat. CrowdStrike Intelligence assesses with high confidence that BGH adversaries will continue targeting financial institutions to obtain and monetize sensitive data. This assessment is supported by the sector's continued position among the ten most frequently targeted sectors by BGH operations globally and a 27% increase in financial services entities posted to DLSs compared to the previous reporting period. IABs will also highly likely continue enabling these operations despite reduced public advertising as access sales increasingly shift to private channels. Together, these trends sustain ransomware and data extortion risk, with direct implications for business operations and reputation.

Among targeted intrusion threat actors, China-nexus adversaries will likely remain the greatest intelligence collection threat to the financial sector globally. Their activity is driven by sustained interest in economic intelligence, PII, and data that supports downstream espionage, with financial entities in South and Southeast Asia — particularly India and Taiwan — likely to remain priority targets.

DPRK-nexus adversaries will continue to pose a serious threat, particularly to cryptocurrency and fintech organizations. Their operational success in 2025, combined with the regime's ongoing military funding requirements, will likely sustain aggressive theft activity in 2026. Though the risk is greatest for fintech, FAMOUS CHOLLIMA insider threat activity will likely continue to affect other parts of the financial services sector.

Russia- and Iran-nexus adversaries are not currently assessed to pose a significant threat to the broader sector. Russian activity is expected to remain focused on Ukraine and adjacent strategic interests, and Iranian activity will likely remain opportunistic and tied to geopolitical tensions involving Western and Gulf-aligned entities. Both could shift their focus in response to changes in the geopolitical environment.

Hacktivist activity will likely continue throughout 2026, driven by major geopolitical conflicts and characterized by coordinated, event-driven DDoS, defacement, and hack-and-leak operations. Though these campaigns typically do not match the destructive impact of ransomware or state-sponsored intrusions, they can create meaningful operational disruption and reputational damage, particularly during politically sensitive periods.

The 2026 threat landscape for financial services is defined by persistence and diversity of intent. The financial sector's unique position in the global economy makes it an attractive target for profit-driven criminals seeking immediate returns, mission-oriented state-nexus threat actors pursuing long-term intelligence objectives, and ideological threat actors weaponizing financial disruptions for political impact. AI will likely compound this challenge as adversaries use it to improve the efficiency and effectiveness of attacks, while financial institutions' own AI deployments expand the attack surface through new systems, workflows, and data paths that require protection. The overall trajectory points toward a threat environment that demands continuous, intelligence-driven defense rather than reactive posture.

Recommendations

1 Defend against social engineering and identity-based access abuse

Social engineering, help desk impersonation, phishing, and MFA reset abuse remain effective paths into financial environments because they exploit the trusted access workflows institutions rely on to support users and manage accounts. As adversaries adopt more scalable tools, including AI-assisted content generation and impersonation techniques, these attacks may become more convincing and harder to detect. Organizations should strengthen identity verification for password and MFA resets, remote support, contractor access, and privileged accounts. Phishing-resistant MFA, tighter controls on SaaS and cloud identities, and monitoring for anomalous authentication and session activity can help stop hands-on-keyboard intrusions before adversaries reach sensitive systems or data.

2 Prioritize edge device and perimeter patching and monitoring

Financial sector intrusions increasingly begin with the exploitation of vulnerable edge devices, VPN appliances, internet-facing systems, and virtual infrastructure that give adversaries a foothold for persistence and lateral movement. Organizations should prioritize rapid triage and patching of perimeter technologies and externally exposed services, while extending logging and detection coverage to virtualization platforms and other high-risk infrastructure. Reducing blind spots across these environments can help security teams uncover stealthy activity earlier and contain intrusions before they disrupt critical business services.

3 Strengthen resilience around high-value systems

For financial institutions, the impact of intrusion often extends beyond downtime to include theft of customer data, payment information, business intelligence, and other high-value records that can enable fraud, extortion, or downstream targeting. Organizations should strengthen data access governance, segment payment and transaction systems, monitor access to sensitive data stores, and test incident response and recovery plans against disruptive scenarios. These measures can help reduce operational, legal, regulatory, and reputational impact when attacks affect high-availability financial operations.

Recommendations

4 Secure digital asset and trusted software workflows

Cryptocurrency, fintech, and adjacent software ecosystems remain prime targets because they combine direct access to digital assets with trusted developer, vendor, and cloud administration workflows that adversaries can abuse at scale. Organizations should harden developer environments, validate software dependencies and verify code provenance, secure wallet and cloud administration processes, and apply stronger controls to third-party software and service providers. Financial institutions with digital asset exposure should also monitor for recruitment-themed lures, malicious coding challenges, and trojanized software designed to compromise trusted access paths.

5 Prioritize intelligence-led defense and proactive hunting

The financial services sector faces sustained targeting from eCrime, state-sponsored, and ideologically motivated adversaries pursuing theft, extortion, intelligence collection, and disruption. An intelligence-led approach helps organizations focus on the adversaries, access paths, and systems most likely to be targeted instead of spreading defenses too broadly. By applying threat intelligence through proactive hunting across identities, cloud and SaaS environments, payment systems, internet-facing assets, and high-value data stores, teams can detect interactive intrusions earlier and respond before business impact escalates.

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

Placeholder space.
Partner's logo can be inserted here.
Please replace this dotted box with logo.