CHECK POINT™

EXPOSURE MANAGEMENT

2025 FINANCE SECTOR LANDSCAPE REPORT

February 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The financial sector experienced a dramatic escalation in cyber threat activity throughout 2025, with total recorded incidents more than doubling year over year—from 864 in 2024 to 1,858 in 2025. This surge reflects the intensifying efforts of threat actors to compromise critical financial infrastructure, disrupt online services, and exploit sensitive customer and transactional data across global markets.

DDoS attacks, data breaches & leaks, ransomware, and defacement remained the dominant incident categories, each showing significant growth compared to the previous year. DDoS attacks nearly doubled, driven by highly coordinated hacktivist campaigns targeting banking portals, payment interfaces, and public facing financial services. Ransomware maintained its trajectory of steady expansion, with 451 incidents tied to increasingly sophisticated double and triple extortion models deployed by groups such as Qilin, Akira, and Clop. Data breach & leak cases rose sharply to 443, underscoring persistent weaknesses in identity governance, misconfiguration management, and third-party integrations. Meanwhile, defacement campaigns continued to proliferate, exposing vulnerabilities in web applications and amplifying reputational risk.

The United States remained the most targeted geography across all major attack vectors, reflecting its vast financial infrastructure, high digital interconnectedness, and attractiveness to financially motivated threat actors. Secondary concentrations of activity emerged across India, Indonesia, Brazil, South Korea, the U.K., and multiple LATAM markets—highlighting the global reach of both hacktivist and financially driven operations. These patterns demonstrate how adversaries continue to optimize their targeting strategies based on scale, geopolitical relevance, and systemic exposure.

Emerging trends—including AI-powered investment scams, deepfake-enabled identity bypass, advanced mobile banking trojans like Herodotus, and EMV cloning operations in LATAM—further expanded the threat landscape. Rapid commercialization of Phishing as a Service platforms, such as Spiderman, enabled low-skilled actors to launch highly effective, evasive credential-harvesting campaigns at scale. The evolution of these threats signals a growing reliance on automation, AI-driven deception, and cross-platform techniques that challenge traditional fraud and security controls.

Overall, the 2025 threat environment reinforces the urgent need for financial institutions to adopt proactive, intelligence-led security programs. Strengthened identity protection, enhanced DDoS resilience, improved ransomware preparedness, and advanced monitoring of external digital risks have become essential to maintaining operational continuity and reducing exposure to increasingly sophisticated global adversaries.

CYBER INCIDENT TRENDS: 2024–2025

The chart below compares year-over-year cyber incidents affecting the financial sector in 2024 and 2025. As shown, the sector experienced a significant increase in incident activity, with total reported cases rising sharply from 864 in 2024 to 1,858 in 2025. This more than two-fold increase reflects the growing pressure on financial institutions as threat actors intensify efforts to compromise critical services, customer data, and operational infrastructure.

For organizations operating in the financial domain, where trust, availability, and regulatory compliance are paramount, this upward trend is especially concerning. The data highlights not only a surge in overall incident volume but also significant shifts in the types of attacks most commonly observed. These changes offer valuable insights into the evolving behaviors of adversaries and emerging threats targeting banks, payment systems, and financial service providers.

The following key observations break down these trends and outline the most notable developments influencing the sector's threat landscape.

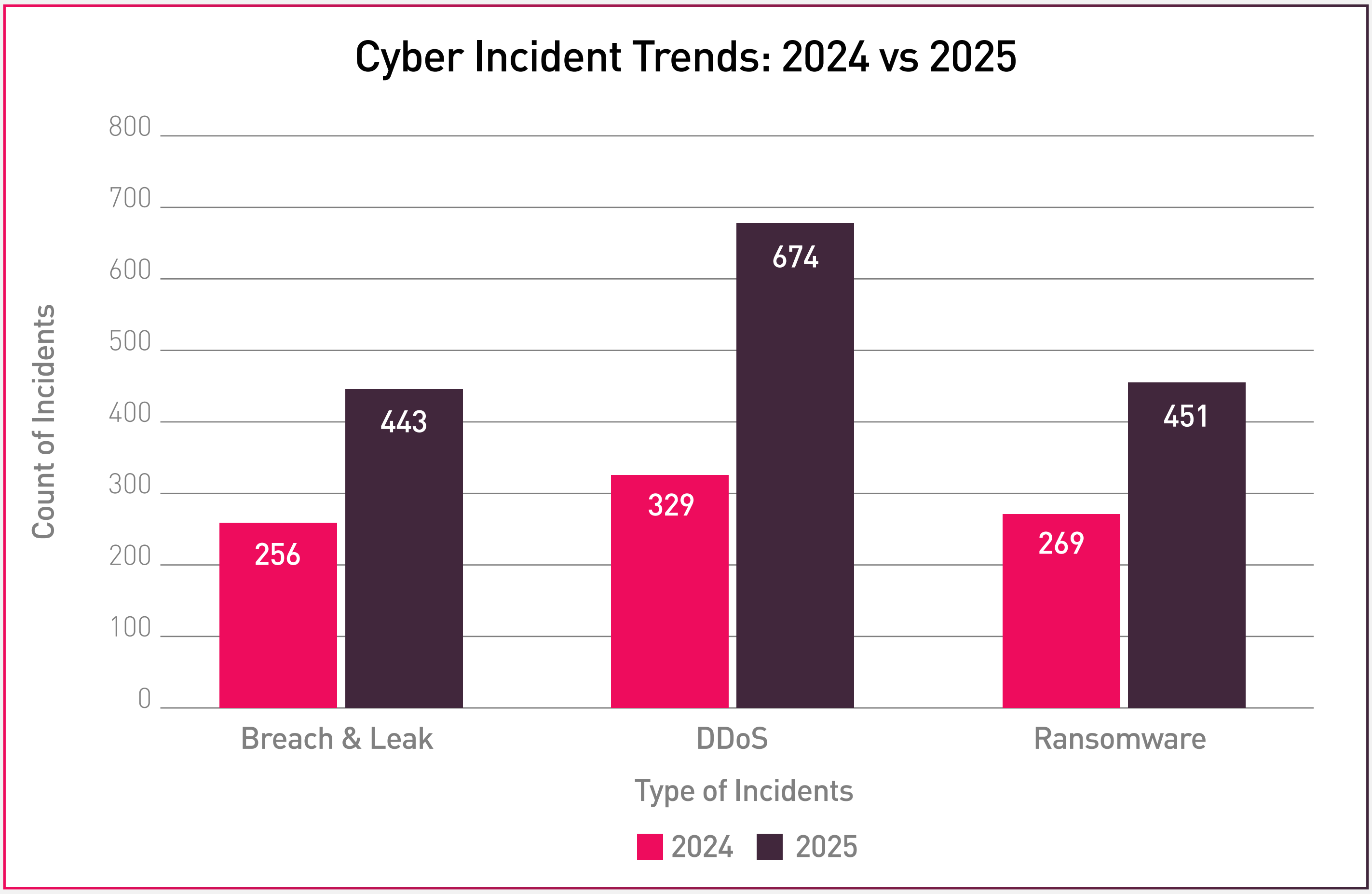
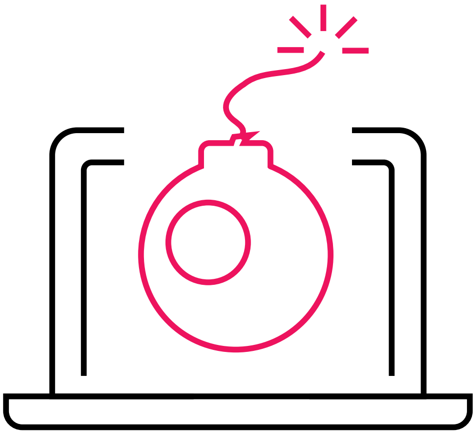


Figure 1: Comparison of the number of different attack vectors observed in 2024 versus 2025

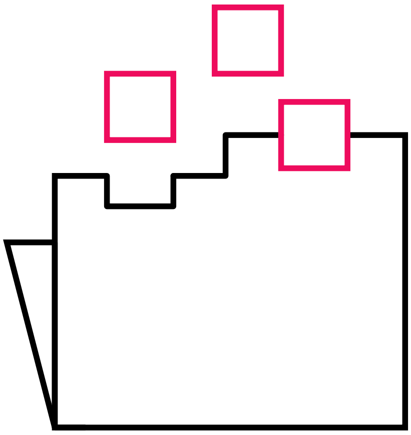
Key Observations

The financial sector experienced a substantial rise in cyber activity between 2024 and 2025, with every major incident category showing a clear upward trend. DDoS attacks remained the most significant contributor to overall volume, increasing from 329 incidents in 2024 to 674 in 2025. This doubling reflects threat actors' continued focus on disrupting the availability of online banking services, payment gateways, and financial platforms. For financial institutions—where uptime, reliability, and customer access are critical—the sustained rise in DDoS attacks underscores the need for stronger resilience, enhanced traffic scrubbing capabilities, and layered mitigation strategies.

Although not the fastest-growing category, ransomware incidents continued their steady rise, climbing from 269 in 2024 to 451 in 2025. This growth highlights attackers' ongoing focus on financial organizations as high-value targets with low tolerance for downtime. Beyond traditional encryption, modern ransomware campaigns increasingly involve data theft and extortion, putting additional pressure on affected institutions that must maintain confidentiality, integrity, and availability across critical systems while navigating regulatory and reputational fallout.



DDoS attacks **surged 105%**



Data breaches & leaks **jumped 73%**

Breach & Leak incidents also rose sharply, increasing from 256 in 2024 to 443 in 2025. This upward trend reflects persistent challenges in securing financial data, often stemming from misconfigurations, weak access controls, and vulnerabilities in third-party integrations. As financial institutions handle highly sensitive PII, PCI, and transactional data, the exposure or compromise of such information carries significant regulatory, operational, and reputational consequences.

At the same time, the continued frequency of these incidents indicates that adversaries are still successfully leveraging credential compromise, social engineering, and lateral movement to gain unauthorized access to financial systems. Although the growth in this category is less dramatic than in others, its persistence highlights the ongoing need for strong identity governance, privileged access monitoring, and rapid detection of abnormal activity across financial networks.

ATTACK VECTORS OBSERVED IN 2025

DATA BREACHES & LEAKS:

We analyzed global Data Breach & Leak incidents throughout 2025, leveraging intelligence collected from open, deep, and dark web sources. This combined category includes data leaks, breaches, and compromise events, reflecting the most impactful forms of unauthorized data exposure.

These incidents often involve large-scale exfiltration of sensitive information, either for financial gain, extortion, or ideological purposes. Unlike DDoS attacks, which aim for immediate disruption, Data Breach & Leak operations typically seek long-term leverage through stolen credentials, confidential records, and proprietary data. Many of these attacks are disclosed weeks or months after the initial compromise, underscoring the stealth and persistence of adversaries in this domain.

DATA BREACH & LEAK ATTACKS PER COUNTRY

Globally, Data Breach & Leak incidents show a strong concentration in regions with high digital footprints and valuable data ecosystems.

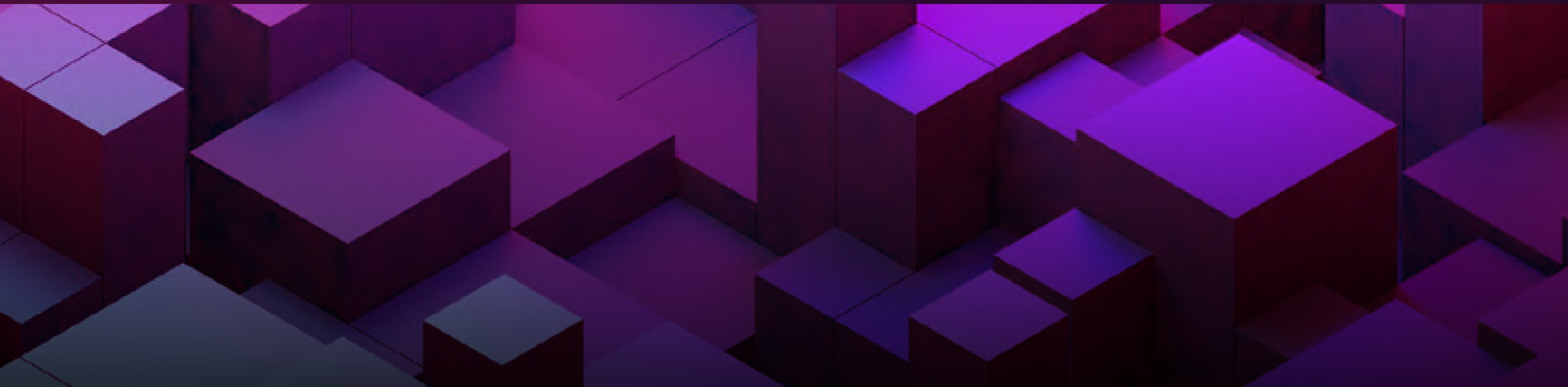
The dataset records 443 incidents in this category. The United States dominates with 177 incidents, accounting for 40 percent of all cases, reflecting its extensive enterprise infrastructure and attractiveness to financially motivated actors. India follows with 31 incidents, while Indonesia ranks third with 24 incidents, highlighting the growing exposure of emerging markets. Russia and France appear next with 16 and 15 incidents, respectively, and Israel registers 12 incidents, indicating persistent targeting of organizations with sensitive data.

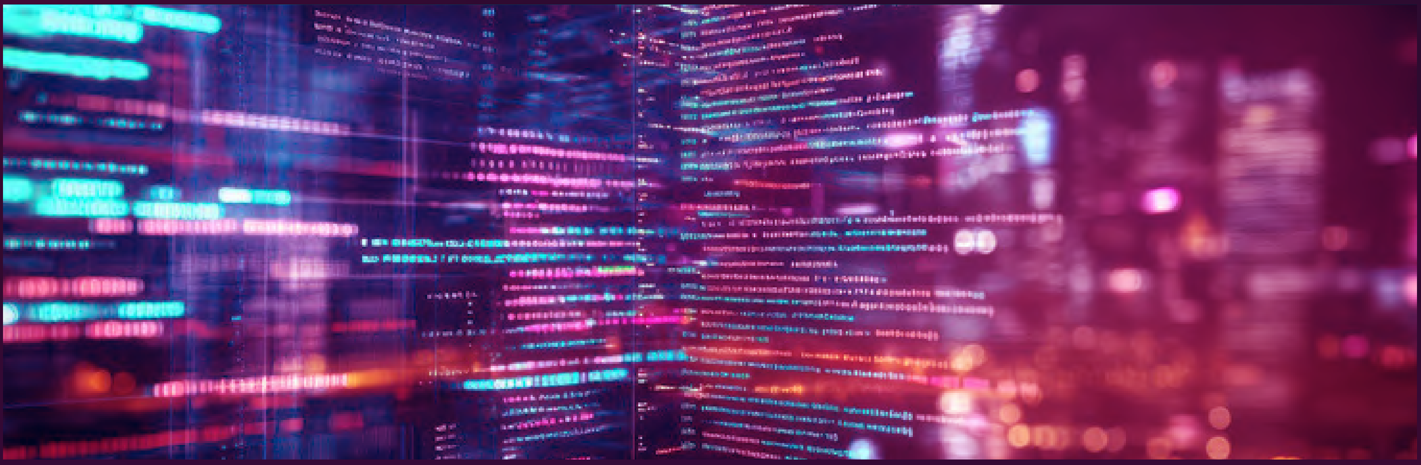
Other countries with notable activity include Spain, Mexico, Canada, and Thailand. A small portion of incidents is marked as Unknown, typically linked to multinational platforms or incomplete attribution. This distribution emphasizes the global nature of data compromise, with attackers prioritizing regions that offer both scale and strategic value.

Most targeted countries by data breach & leak attacks

USA	India	Indonesia	Russia	France
177	31	24	16	15
Israel	**Spain**	**Mexico**	**Canada**	**Thailand**
12	11	11	9	7

Figure 2: Most targeted countries by data breach & leak attacks





DATA BREACH & LEAK ATTACKS PER THREAT ACTOR

Attribution analysis reveals a fragmented but telling picture of threat actor behavior in data compromise campaigns.

The largest share of incidents – 145 cases (32.7 percent) – is attributed to Unknown actors, reflecting the covert nature of many breaches and the difficulty of linking operations to specific groups.
Among identified actors, BreachLaboratory stands out with 43 incidents, positioning itself as a major player in large-scale data theft and leak operations. Other actors such as ByteToBreach, DigitalGhost, and Sorb appear with smaller but consistent activity, each responsible for multiple breaches across diverse sectors.

While many of these groups operate quietly, their tactics often involve exploiting exposed services, purchasing initial access, and leveraging leak sites to monetize stolen data. The prevalence of Unknown attribution combined with the activity of specialized breach actors underscores the complexity of defending against these threats, which often blend opportunistic exploitation with structured extortion strategies.

Top 10 threat actors in data breach & leak attacks

Unknown	145
BreachLaboratory	43
ByteToBreach	6
DigitalGhost	5
Sorb	5
Panda	4
Lionishacker	4
CLOBELSECTEAM	4
N1KA	4
Cyber Toufan Operation	3

Figure 3: Top threat actors in data breach & leak attacks

More broadly, data breach and leak activity is characterized by a high degree of anonymity. In many cases, threat actors deliberately obscure their identities, operate under short-lived aliases, or avoid public attribution altogether, resulting in a substantial proportion of incidents remaining unattributed. This anonymity is often intentional, reducing operational risk while enabling actors to reuse infrastructure or shift personas across campaigns.

The primary motivation behind most data breach and leak operations is financial gain, whether through direct extortion of victims, the sale of stolen data on underground forums, or reputational leverage via public leak sites. Secondary motives include notoriety within cybercriminal communities and, less frequently, ideological signaling. Overall, these actors tend to prioritize low-risk, high-impact opportunities, exploiting exposed systems and weak access controls to rapidly monetize compromised data.

DDOS:

We analyzed DDoS attacks targeting global entities throughout 2025, drawing on intelligence collected from open, deep, and dark web sources. The analysis focuses on temporal patterns, geographic exposure by country, and the threat actors that shaped the worldwide DDoS landscape.

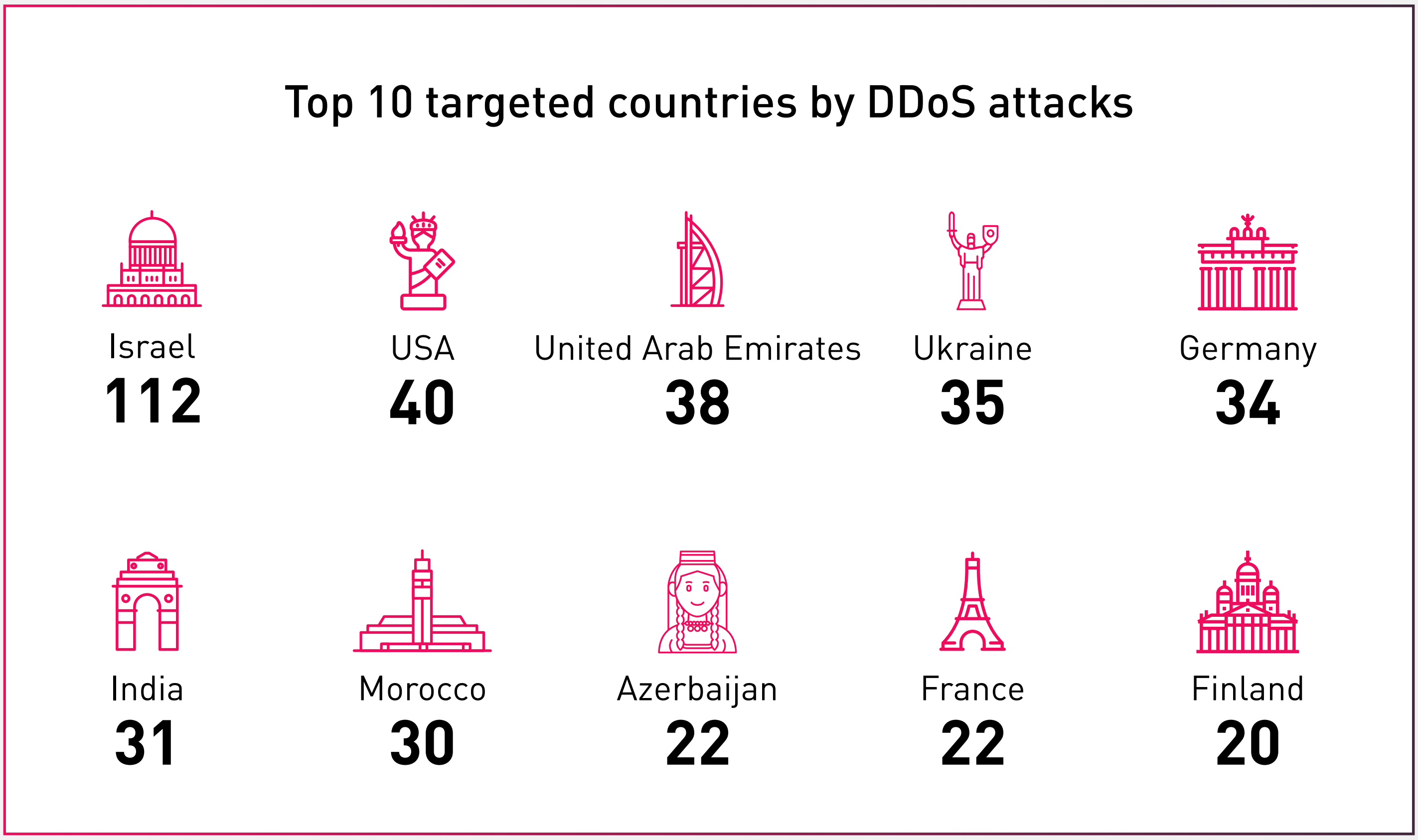
When interpreting overall DDoS activity, it is important to note that many events were executed as part of coordinated campaigns, where attackers launched dozens or even hundreds of short, successive hits against multiple targets during a single operation. This campaign style can inflate raw event counts while still reflecting the real operational pressure experienced by defenders.

DDoS Attacks Per Country

Globally, Data Breach & Leak incidents show a strong concentration in regions with high digital footprints and valuable data ecosystems.

The dataset records 443 incidents in this category. The United States dominates with 177 incidents, accounting for 40 percent of all cases, reflecting its extensive enterprise infrastructure and attractiveness to financially motivated actors. India follows with 31 incidents, while Indonesia ranks third with 24 incidents, highlighting the growing exposure of emerging markets. Russia and France appear next with 16 and 15 incidents, respectively, and Israel registers 12 incidents, indicating persistent targeting of organizations with sensitive data.

Other countries with notable activity include Spain, Mexico, Canada, and Thailand. A small portion of incidents are marked as Unknown, typically linked to multinational platforms or incomplete attribution. This distribution emphasizes the global nature of data compromise, with attackers prioritizing regions that offer both scale and strategic value.



Top 10 targeted countries by DDoS attacks

Israel	USA	United Arab Emirates	Ukraine	Germany
112	40	38	35	34
India	**Morocco**	**Azerbaijan**	**France**	**Finland**
31	30	22	22	20

Figure 4: Most targeted countries by DDoS attacks

DDOS ATTACKS PER THREAT ACTOR

Attribution in DDoS remains dominated by a small set of prolific hacktivist clusters that announce rapid, campaign-driven operations.

Keymous + is the most active group in the dataset with 121 claimed attacks (about 18.0 percent of all DDoS events), frequently conducting high-volume runs against multiple countries within short windows. NoName057(16) follows with 98 incidents (14.5 percent), reflecting its routine, politically timed disruption of government, media, and financial services targets in countries aligned with opposing geopolitical blocs. Dark Storm Team and Hezi Rash contribute 55 and 49 incidents respectively (8.2 and 7.3 percent), while SYLHET GANG and Mr Hamza add 33 and 28 incidents. Additional actors such as RABBIT CYBER TEAM, Hider_Nex, Red Wolf Team, and DieNet appear consistently across the year.

Taken together, the top 10 actors account for roughly 68.8 percent of recorded DDoS incidents, underscoring the concentration of capability and brand activity in a relatively small number of groups. Most of these operators rely on readily available infrastructure and coordination channels to scale impact quickly, which helps explain the bursty, campaign like patterns visible in the data.

Top 10 threat actors in DDoS attacks

Keymous +	121
NoName057(16)	98
Dark Storm Team	55
Hezi Rash	49
SYLHET GANG	33
Mr Hamza	28
Red Wolf Team	20
Hider_Nex	20
RABBIT CYBER TEAM	20
DieNet	18

Figure 5: Top threat actors in DDoS attacks

From a behavioral perspective, the majority of DDoS threat actors observed are ideologically and politically motivated, operating primarily within a hacktivist framework, for direct financial gain. These groups often align themselves with geopolitical narratives, national causes, or opposition to specific governments and institutions, selecting targets based on symbolic value and public visibility, rather than technical complexity.

Operations are typically designed to generate disruption and attention rather than long-term access, with actors prioritizing rapid execution, public claims of responsibility, and amplification through social media or messaging platforms. This ideological motivation, combined with low barriers to entry and shared tooling, enables recurring participation by the same groups across multiple campaigns, reinforcing the highly concentrated and cyclical nature of DDoS activity observed throughout the year.

RANSOMWARE:

Throughout 2025, Ransomware remains one of the most disruptive cyber threats to financial organizations, combining data encryption with extortion tactics to maximize impact. These attacks typically infiltrate networks through phishing, credential compromise, or exploitation of vulnerabilities, then encrypt critical files and demand payment – often in cryptocurrency – for decryption keys.

Beyond immediate operational paralysis, ransomware campaigns frequently involve data theft and public leak threats, amplifying reputational and regulatory risks. In 2025, ransomware actors continued to refine their methods, leveraging double- and triple-extortion schemes, targeting high-value financial institutions, and exploiting supply chain dependencies to broaden their reach.

RANSOMWARE ATTACKS PER COUNTRY

Viewed globally, activity concentrated most heavily in the United States, with meaningful secondary exposure in South Korea, the United Kingdom, and Canada.

Based on our records, 451 finance sector ransomware incidents in total were observed in 2025. The most targeted country is the United States: 196 incidents (43.5% of all events), after that, South Korea: 31 (6.9%); the United Kingdom: 22 (4.9%); and Canada: 16 (3.5%).

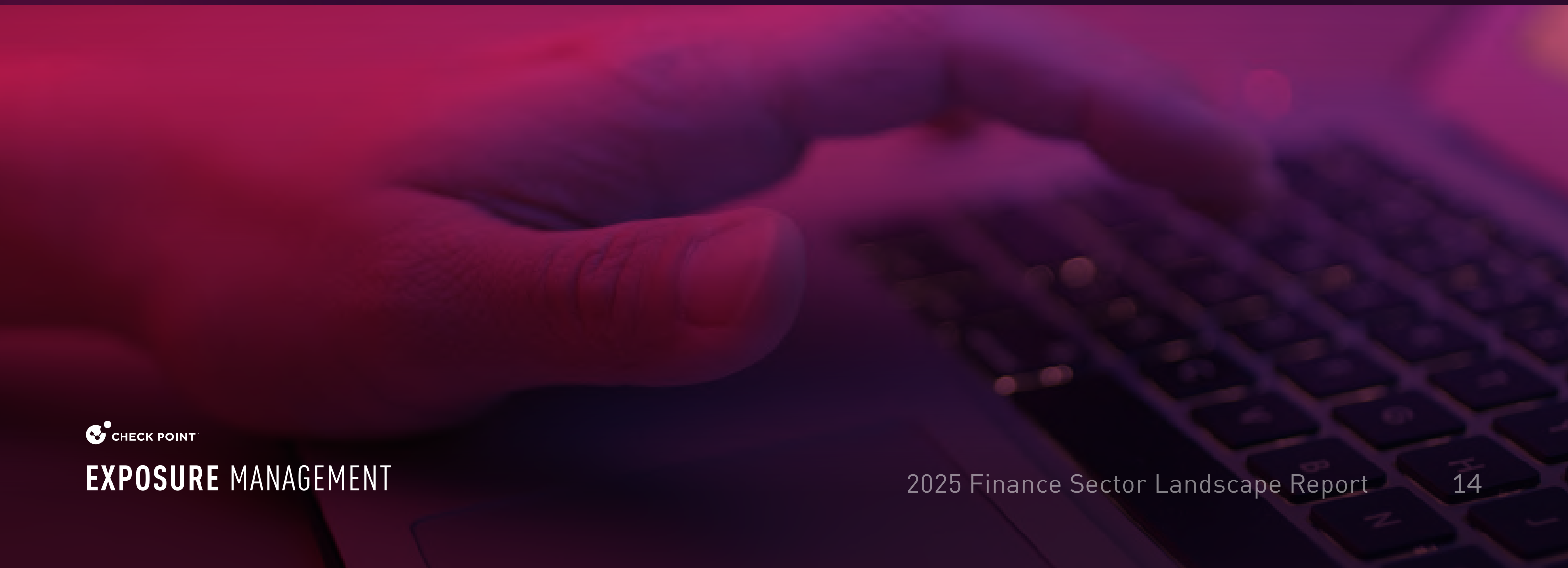
Additional notable activity spans Malaysia (10), India (10), Japan (9), Brazil (9), Spain (9), the Netherlands (7), and Argentina (6), with a smaller tail of "Unknown" geography where the victim's country could not be confidently derived.

This distribution indicates sustained focus on North American targets, alongside East Asian (especially South Korea) and European exposure – consistent with opportunistic campaigns against banks, insurance intermediaries, asset managers, and related financial services.

Top 10 targeted countries by ransomware attacks

USA	South Korea	UK	Canada	Malaysia
196	31	22	16	10
India	**Spain**	**Brazil**	**Japan**	**Netherlands**
10	9	9	9	7

Figure 6: Most targeted countries by ransomware attacks

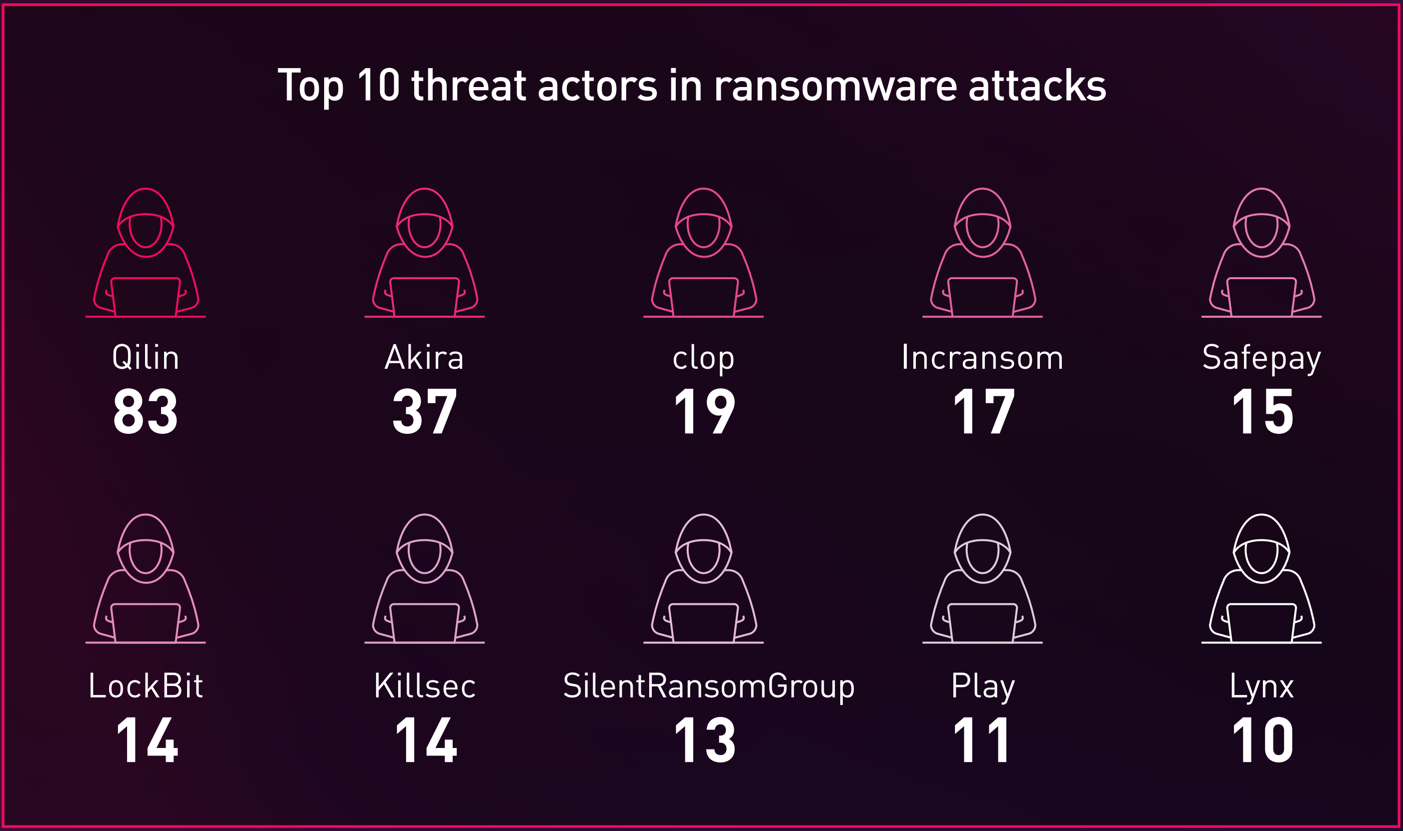


RANSOMWARE ATTACKS PER THREAT ACTOR

Attribution in ransomware remains dominated by a small set of prolific hacktivist clusters that announce rapid, campaign-driven operations.

Qilin is the most active ransomware group in the dataset with 83 incidents (≈ 18.4% of all recorded ransomware events), running opportunistic campaigns across multiple geographies. Akira follows with 37 incidents (≈ 8.2%), maintaining steady pressure on financial and professional services. Clop registers 19 cases (≈ 4.2%), while Incransom and Safepay contribute 17 (≈ 3.8%) and 15 (≈ 3.3%) incidents, respectively. LockBit and Killsec each account for 14 incidents (≈ 3.1% apiece). SilentRansomGroup appears in 13 cases (≈ 2.9%) and Play and Everest add 11 (≈ 2.4%) and 10 (≈ 2.2%) incidents.

Taken together, the top 10 groups represent ~51.6% of recorded ransomware incidents in your dataset, indicating a concentrated but diverse operator landscape. The leading actors largely rely on shared tooling and affiliate/RaaS models, which enable quick scaling and bursty, campaign like activity across sectors and countries—patterns that are visible in your data exports and charts.



Top 10 threat actors in ransomware attacks

Qilin	83
Akira	37
clop	19
Incransom	17
Safepay	15
LockBit	14
Killsec	14
SilentRansomGroup	13
Play	11
Lynx	10

Figure 7: Top threat actors in ransomware attacks

Ransomware operations are mostly financially motivated, with threat actors focusing on revenue generation through extortion rather than ideological signaling. Most of the groups observed operate within mature ransomware-as-a-service (RaaS) ecosystems, where affiliates are incentivized to maximize infection volume, target high-value organizations, and negotiate payments efficiently.

Target selection is typically opportunistic but economically driven, favoring sectors with lower tolerance for downtime and greater likelihood of payment, such as financial services, professional services, healthcare, and manufacturing. The reliance on shared tooling, access brokers, and standardized playbooks lowers operational friction and enables rapid campaign execution, contributing to the concentrated yet persistent ransomware activity reflected.

DEFACEMENT:

Throughout 2025, website defacement emerged as a persistent threat to financial organizations, aiming to disrupt trust and brand integrity through unauthorized alterations of public-facing content. These attacks typically exploit vulnerabilities in web applications or content management systems, allowing adversaries to replace legitimate pages with malicious messages, propaganda, or misleading information.

While the immediate impact may appear cosmetic, defacement incidents often signal deeper security weaknesses that could expose organizations to further compromise. In 2025, threat actors refined their tactics by automating large-scale campaigns, targeting financial institutions across multiple regions, and leveraging ideological or hacktivist motives to amplify visibility. The public nature of these attacks magnifies reputational damage, erodes user confidence, and underscores the critical need for robust web security and continuous monitoring of digital assets.

DEFACEMENT ATTACKS PER COUNTRY

Based on our records, 278 finance-sector defacement incidents in total were observed in 2025. Most targeted country is United States: 79 incidents (28.4% of all events), after that, India: 36 (12.9%); and United Kingdom: 23 (8.3%).

Additional notable activity spans Brazil (15), Indonesia (8), Islamic Republic of Iran (5), France (5), Canada (4), Nigeria (4), Netherlands (4), Israel (3), with a smaller tail of "Unknown" geography where the victim's country could not be confidently derived.

This distribution indicates sustained focus on North American targets, alongside East Asian and European exposure – consistent with opportunistic campaigns against banks, insurance intermediaries, asset managers, and related financial services.

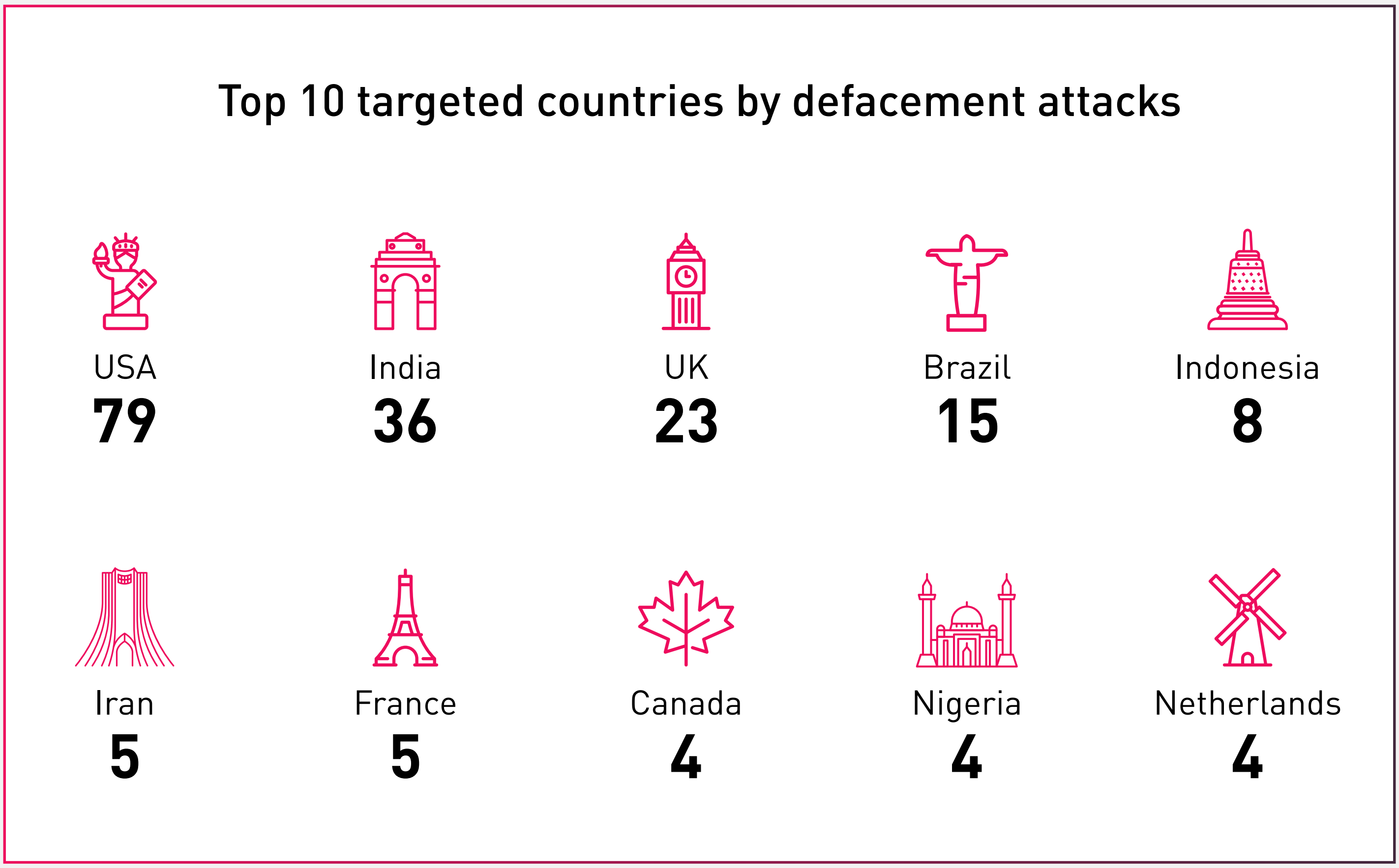


Figure 8: Most targeted countries by defacement attacks

DEFACEMENT ATTACKS PER THREAT ACTOR

Attribution in defacement remains dominated by a mix of hacktivist and opportunistic clusters executing campaign-driven operations.

chinafans is the most active defacement actor in the dataset with 40 incidents (≈14.4% of all recorded defacement events), running opportunistic campaigns across multiple geographies. Pharaoh's team follows with 24 incidents (≈8.6%), maintaining steady pressure on financial and professional services. Mr. BDKR28 registers 24 cases (≈8.6%), while XYZ and x7root contribute 15 (≈5.4%) each. TR0janX and Simsimi each account for 13 incidents (≈4.7% apiece). TheInternetJanitor appears in 7 cases (≈2.5%), and ChatLak and setupp.es add 7 (≈2.5%) and 6 (≈2.2%) incidents.

Taken together, the top 10 actors represent ~59.0% of recorded defacement incidents in your dataset, indicating a concentrated but diverse operator landscape. The leading actors largely rely on shared tooling and opportunistic exploitation, enabling quick scaling and bursty, campaign like activity across sectors and countries.

Top 10 Top threat actors in defacement attacks

chinafans	Pharaoh's team	Mr. BDKR28	XYZ	x7root
40	24	24	15	15
TR0janX	Simsimi	ChatLak	TheInternetJanitor	setupp.es
13	13	7	7	6

Figure 9: Top threat actors in defacement attacks

Defacement activity is primarily driven by visibility-seeking and symbolic motives rather than direct financial gain. Many of the actors involved operate within hacktivist or semi-opportunistic frameworks, using defacement as a low-barrier method to project ideological messages, gain notoriety within underground communities, or signal technical capability. In some cases, campaigns are loosely coordinated around geopolitical events or trending narratives, while others appear motivated by reputation-building and competitive posturing among peers.

Tactically, these actors tend to favor exposed web services, misconfigured content management systems, and recycled exploits, allowing rapid compromise with minimal investment. This combination of low operational cost, high public visibility, and short-lived impact explains the recurring, campaign-driven patterns observed in defacement activity and the sustained participation of a relatively small set of repeat actors.

TRENDS AND CAMPAIGNS

AI-POWERED TRUMAN SHOW SCAM: A NEW FINANCIAL THREAT

The OPCOPRO "Truman Show" scam is an AI driven investment fraud operation that traps victims inside a fully fabricated financial ecosystem. Attackers lure targets through SMS, ads, and messaging apps into WhatsApp or Telegram groups filled with AI generated experts and fake participants, all simulating an active trading community. Even the mobile apps victims are told to install look legitimate, but are merely WebView shells showing fabricated balances and trades.

By industrializing trust building and emotional manipulation, AI enables fraudsters to scale these schemes across languages and regions. Victims eventually hand over money and sensitive identity documents, resulting in financial loss and long term identity exposure. As investment fraud continues to dominate cybercrime, this scam highlights the growing threat of AI manufactured trust and the need for stronger scrutiny of financial apps and controlled online communities in 2025.

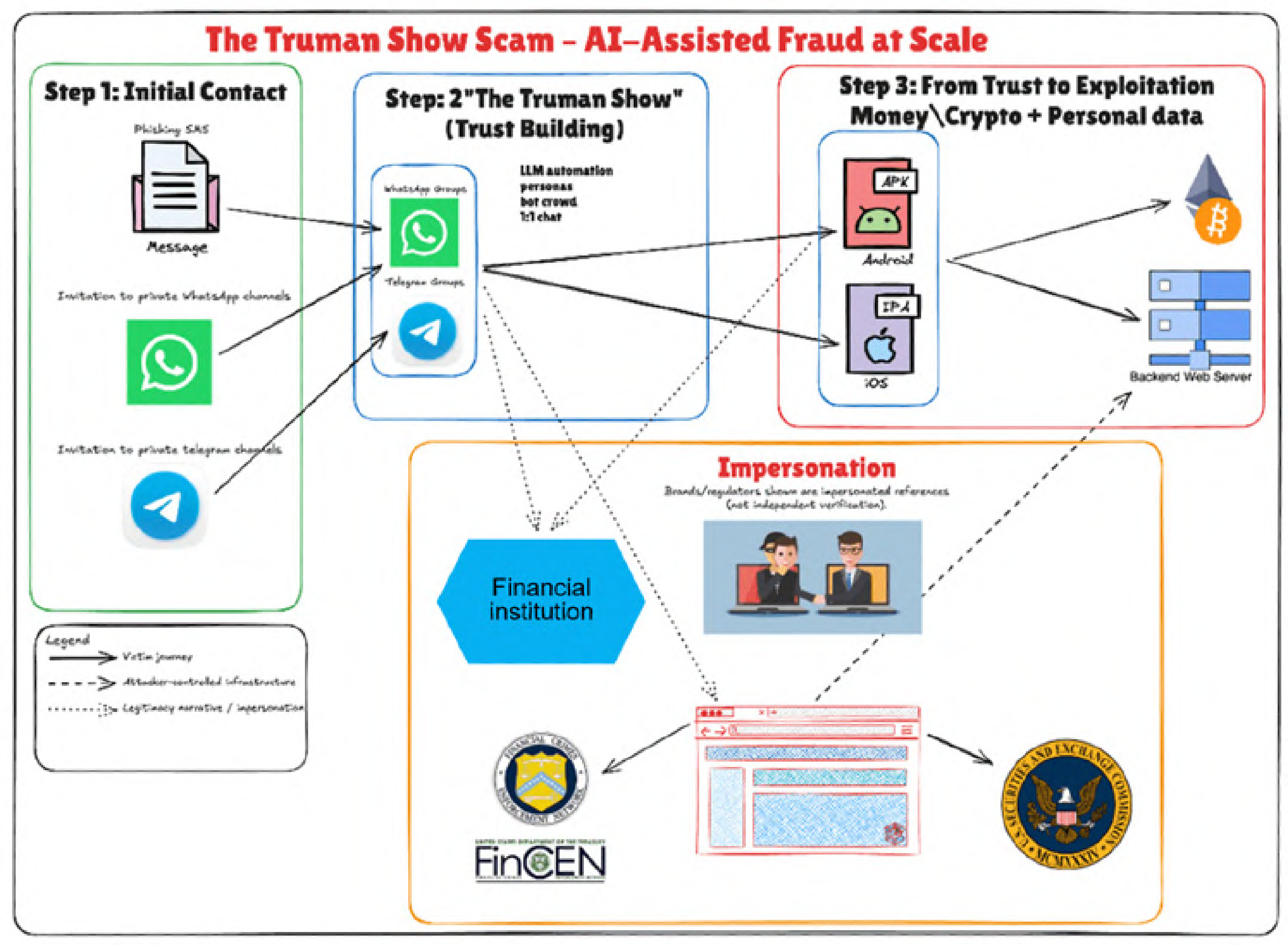

The Truman Show Scam – AI–Assisted Fraud at Scale
Step 1: Initial Contact
Phishing SMS
Message
Invitation to private WhatsApp channels
Invitation to private telegram channels
Step: 2"The Truman Show" (Trust Building)
WhatsApp Groups
Telegram Groups
LLM automation
personas
bot crowd
1:1 chat
Step 3: From Trust to Exploitation Money\Crypto + Personal data
APK
Android
IPA
iOS
Backend Web Server
Impersonation
Brands/regulators shown are impersonated references (not independent verification).
Financial institution
FinCEN
Legend
Victim journey
Attacker-controlled infrastructure
Legitimacy narrative / impersonation

Figure 10: Illustration of the "Truman Show" scam workflow

THE RISE OF PHISHING KITS IN 2025: THE SPIDERMAN PLATFORM AS A CASE IN POINT

The Spiderman platform emerged as a fully developed Phishing-as-a-Service operation that provides threat actors with ready-made phishing pages, anti-bot controls, domain management, and real-time credential harvesting. It is sold through dark web forums and encrypted channels, allowing even low-skilled actors to launch convincing phishing campaigns against banks and cryptocurrency platforms. HUMINT engagement confirmed that the seller actively maintains and customizes the platform for global targets, reflecting the growing accessibility of high-quality phishing infrastructure.

Spiderman also reflects the broader evolution of phishing in 2025, where phishing kits doubled, and 90 percent of large campaigns relied on PhaaS offerings. Reports from 2025 show that social engineering, mobile-first phishing, and AI-enhanced lures are becoming central features of modern attacks. Platforms like Spiderman, which mirror these trends with scalable tooling and realistic templates, illustrate how phishing in 2025 became more commercialized, more evasive, and significantly more difficult for financial institutions to defend against.

THE 2025 BANKING TROJAN LANDSCAPE: HERODOTUS AND BEYOND

In 2025, banking trojans grew more sophisticated, spreading beyond Windows to increasingly target Android and macOS devices. Android trojans used fake overlays, credential-stealing prompts, and advanced evasion techniques such as mimicking human typing to bypass anti-fraud systems. The financial sector saw over 1.3 million attacks, often delivered through messaging apps rather than traditional phishing emails. Classic trojans continued to use browser injections, keylogging, and spoofed banking pages to steal sensitive information.

A major development was Herodotus, an advanced Android banking trojan targeting Italy and Brazil. It mimicked human behavior with randomized keystroke delays, bypassed behavioral fraud detection, abused Android accessibility services to take control of devices, displayed fake banking screens, intercepted SMS two-factor codes, and read on-screen content. Herodotus expanded its reach to the U.S., Turkey, the U.K., and Poland, exemplifying the 2025 trend of mobile banking trojans becoming more human-like, automated, and capable of evading traditional defenses.

EMV CLONING CAMPAIGN TARGETING LATAM FINANCE INSTITUTIONS

In late 2025, Cyberint identified an emerging EMV cloning campaign circulating on underground carding forums and explicitly targeting financial institutions in Mexico, the Dominican Republic, Peru, and Colombia. The threat actor behind the campaign provides detailed operational guidance, including step-by-step cloning instructions, recommended tooling, and sources for acquiring full card "dumps" containing track data, PINs, and cardholder information. According to the actor's claims, the methodology remains effective due to persistent magstripe fallback acceptance, weak enforcement of chip and PIN protocols, and inconsistent terminal governance across the region.

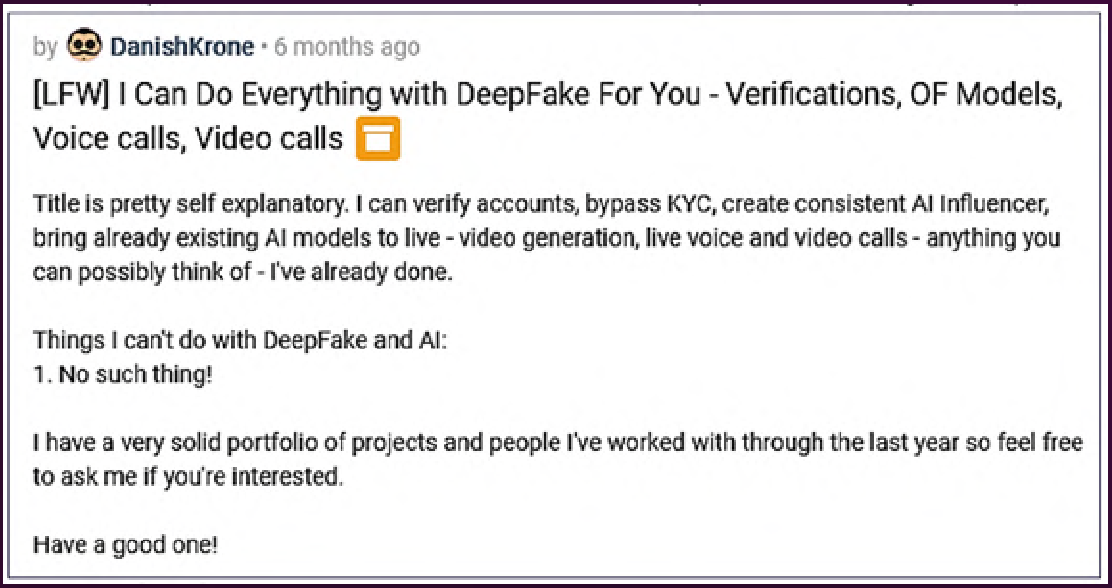
The campaign's success appears to rely on attackers writing stolen data onto JCOP chip cards using EMV personalization tools, then exploiting permissive fallback behavior at POS terminals and ATMs. Reported cash-out activity focuses on large retailers and select ATMs, with the actor boasting POS success rates of over 90% in the targeted geographies. While these claims cannot be fully validated, the described techniques align with known EMV ecosystem vulnerabilities in LATAM and highlight ongoing risks associated with outdated terminal configurations, offline approvals, and insufficient authentication controls.

This activity reflects a broader trend of organized fraud operations leveraging region-specific payment system weaknesses. Financial institutions in LATAM should prioritize tightening fallback rules, enforcing online PIN, enhancing transaction monitoring for fallback-driven approvals, and collaborating with acquirers and merchants to reduce exposure to EMV bypass techniques.

AI-DRIVEN FRAUD: HOW DEEPFAKES ARE RESHAPING FINANCIAL CRIME

In 2025, advances in generative AI and deepfake technologies have significantly increased risks across banking and financial services, particularly in identity verification and fraud prevention. AI-generated faces, voices, and documents are being used to bypass digital KYC controls, including facial recognition, liveness detection, and video-based onboarding, enabling the creation of synthetic or fully fabricated customer identities. These capabilities allow fraudsters to open accounts, access financial services, and move funds at scale while reducing the likelihood of detection.

Beyond onboarding, deepfake-enabled impersonation is affecting multiple areas of financial operations, including account takeover, social-engineering attacks against customers and employees, and executive impersonation during voice or video communications. The rise of high-quality synthetic identities has also facilitated money laundering and mule account networks, undermining transaction monitoring and customer due diligence processes. As a result, traditional rule-based and biometric-only defenses are increasingly insufficient, forcing financial institutions to adopt layered, AI-resilient controls that combine behavioral analysis, advanced fraud detection, and continuous identity verification to mitigate these evolving threats.



by DanishKrone • 6 months ago

[LFW] I Can Do Everything with DeepFake For You - Verifications, OF Models, Voice calls, Video calls

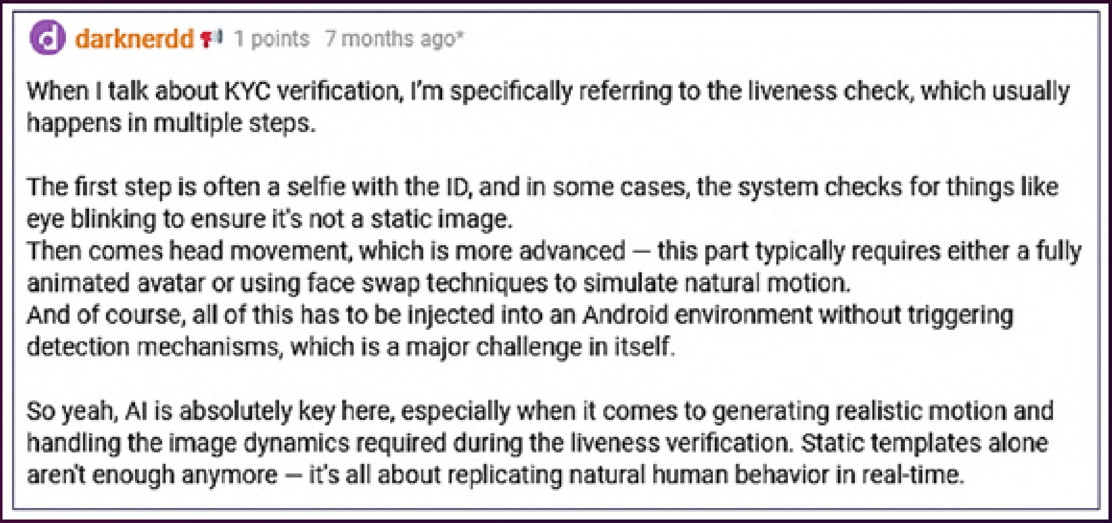
Title is pretty self explanatory. I can verify accounts, bypass KYC, create consistent AI Influencer, bring already existing AI models to live - video generation, live voice and video calls - anything you can possibly think of - I've already done.

Things I can't do with DeepFake and AI:
1. No such thing!

I have a very solid portfolio of projects and people I've worked with through the last year so feel free to ask me if you're interested.

Have a good one!

Figure 11: Dark forum user advertising deepfake creation services for various purposes



darknerdd 1 points 7 months ago*

When I talk about KYC verification, I'm specifically referring to the liveness check, which usually happens in multiple steps.

The first step is often a selfie with the ID, and in some cases, the system checks for things like eye blinking to ensure it's not a static image.
Then comes head movement, which is more advanced — this part typically requires either a fully animated avatar or using face swap techniques to simulate natural motion.
And of course, all of this has to be injected into an Android environment without triggering detection mechanisms, which is a major challenge in itself.

So yeah, AI is absolutely key here, especially when it comes to generating realistic motion and handling the image dynamics required during the liveness verification. Static templates alone aren't enough anymore — it's all about replicating natural human behavior in real-time.

Figure 12: Dark forum user explaining KYC verification processes and methods to bypass them

OVERVIEW OF THE EUROPEAN REGION

In 2025, Europe experienced a total of 345 recorded cyber incidents, reflecting a broad and geographically diverse threat landscape across the region. The United Kingdom accounted for the highest number of incidents (61), followed by France (47), Germany (42), and Ukraine (37), underscoring their continued attractiveness as targets due to the size of their financial sectors and the maturity of their digital infrastructure. Spain also saw elevated activity with 30 incidents, while Belgium (22), Finland (20), and Poland (20) reported moderate but notable levels of malicious activity. Additional incidents were observed in the Netherlands (18), Italy (14), Cyprus (13), Switzerland (11), and Lithuania (11). Lower yet persistent activity was recorded in the Czech Republic (8) and Greece (5), illustrating that cyber threats were not limited to a small number of countries but remained widespread across the European continent.

Incidents Per Country

UK	France	Germany	Ukraine	Spain
61	47	42	37	30
Belgium	**Finland**	**Poland**	**Netherlands**	**Italy**
22	20	20	18	14

Figure 13: Top targeted countries in the EU region

Monthly distribution of incidents shows relatively consistent pressure with distinct peaks in April (44), May (49), and December (44), months often associated with increased financial activity, operational strain, or seasonal targeting patterns by threat actors. The quieter periods occurred in February (15), March (18), and October (14), though none of the months saw a complete downturn, reflecting Europe's constant exposure to multi-vector cyber campaigns.

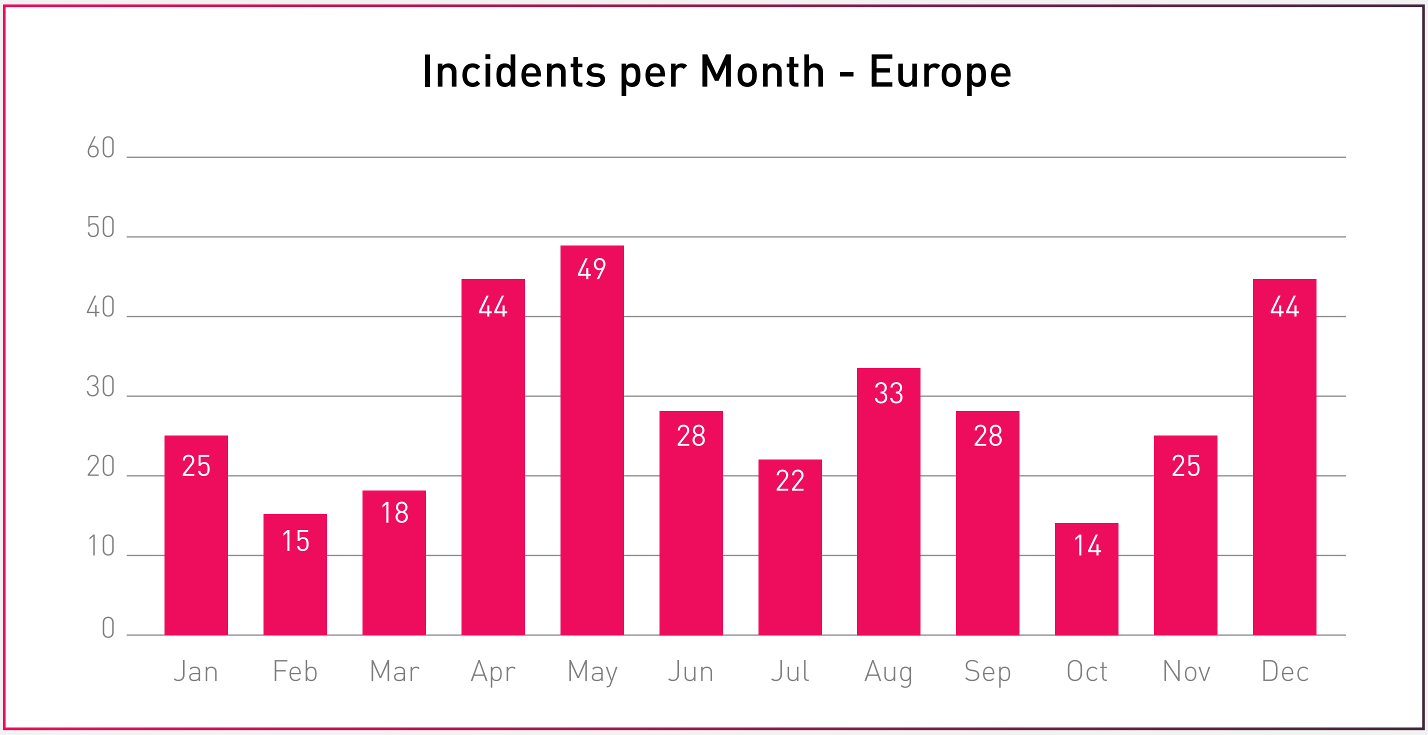


Figure 14: Breakdown of incidents per month in 2025

Across incident types, DDoS attacks were the dominant threat category, accounting for 179 of the 345 incidents. This continued emphasis on service disruption reflects adversaries' ongoing attempts to overwhelm online banking portals, payment processing systems, and digital financial services. Ransomware remained a significant concern, with 74 incidents, underlining the region's sustained vulnerability to extortion-driven campaigns targeting high-value financial assets and operational continuity. Defacement incidents (47) indicate persistent hacktivist or politically motivated activity, particularly targeting public-facing financial and governmental platforms. Meanwhile, Breach & Leak incidents (43) highlight ongoing risks associated with exposed systems, misconfigurations, credential compromises, and third-party weaknesses, issues that remain critical as financial institutions increase their reliance on cross-border digital services.

Overall, Europe's 2025 threat landscape remained highly active and diverse, driven largely by disruptive DDoS campaigns and financially motivated ransomware activity, with meaningful levels of data exposure and defacement. The broad geographic spread underscores the need for coordinated defenses, enhanced monitoring, and sustained investment in resilience across financial institutions throughout the region.

Incidents in the Europe Region

DDoS	Ransomware	Breach & Leak	Defacement
179	**74**	**43**	**47**

Figure 15: Breakdown of types of incidents in the EU region

OVERVIEW OF THE AMERICAS REGION

The Americas region recorded 628 cyber incidents in 2025, with activity distributed across North America, Central America, South America, and the Caribbean. The United States accounted for the overwhelming majority of observed incidents, reporting 493 cases, far surpassing those of any other country in the region. Canada followed at a distance with 32 incidents, while Brazil (29) and Mexico (15) were the most affected countries in Latin America. Other nations experienced comparatively lower volumes, with Argentina (12), Peru (9), Venezuela (7), Colombia (5), and several others reporting isolated events ranging from one to four incidents. This uneven distribution underscores the concentration of both threat activity and digital exposure in the region's largest financial and economic hubs.

Incidents Per Country

USA	Canada	Brazil	Mexico	Argentina
492	32	29	15	12
Peru	Venezuela	Colombia	Bolivia	Panama
9	7	5	4	4

Figure 13: Top targeted countries in the Americas region

From a temporal perspective, incident activity fluctuated throughout the year, with a clear upward trend in Q4. December recorded the highest number of incidents (92), followed by November (68) and March (62). Lower activity months included September (33) and July (40). This pattern reflects both seasonal threat cycles and increased end-of-year targeting, commonly observed in financial ecosystems due to heightened transaction volumes, holiday-driven fraud attempts, and opportunistic exploitation by threat actors during operational slowdowns.

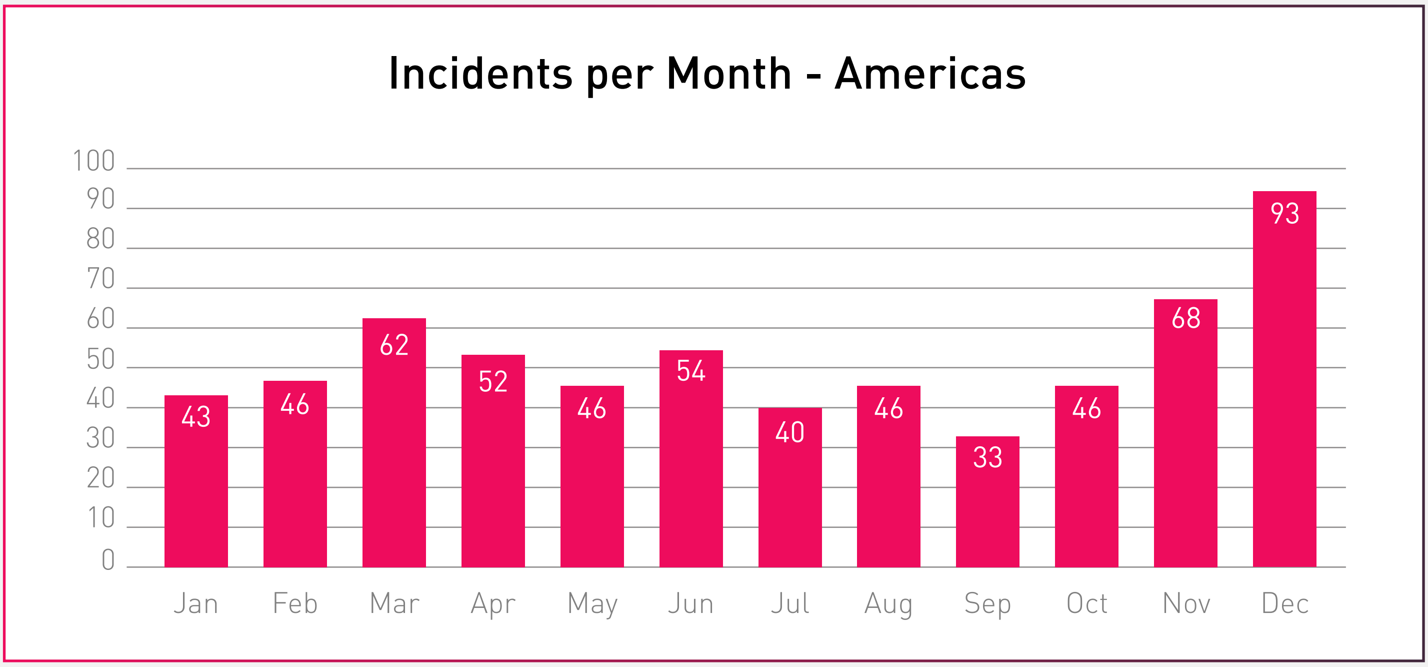


Figure 14: Breakdown of incidents per month in 2025

Across incident types, Ransomware remained the most dominant threat category, with 248 incidents, reflecting the financial sector's ongoing attractiveness to extortion-driven actors. Breach & Leak incidents followed closely at 218, highlighting persistent challenges around data exposure, access control weaknesses, and third-party vulnerabilities. Defacement incidents accounted for 111 cases, indicating continued hacktivist activity and opportunistic targeting of public-facing digital assets. Meanwhile, DDoS attacks (45) remained a smaller but strategically impactful portion of overall activity, often disrupting customer access to financial services and online platforms.

Overall, the 2025 threat landscape in the Americas reveals a region heavily impacted by high-volume ransomware, widespread data compromise, and geographically concentrated activity, with the United States driving the majority of incidents. Latin American countries, particularly Brazil, Mexico, Argentina, Peru, and Venezuela, also remain key targets, reflecting expanding digital infrastructures and persistent regional vulnerabilities. These trends emphasize the need for continued investment in resilience, monitoring, and coordinated defense across the financial sector throughout the Americas.

Incidents in the Americas Region

Ransomware	Breach & Leak	Defacement	DDoS
249	**223**	**112**	**45**

Figure 15: Breakdown of types of incidents in the Americas region

OVERVIEW OF THE APAC REGION

The APAC region experienced a significant volume of cyber incidents across all major attack vectors in 2025, reflecting its rapidly expanding digital financial ecosystem and the growing maturity of threat actors targeting banks, fintech platforms, payment processors, and mobile first financial services. Across the four primary incident categories:

- DDoS
- Ransomware
- Breach & Leak
- Defacement

APAC countries appeared consistently among the top 10 most targeted globally, underscoring the region's heightened exposure. India, Indonesia, South Korea, Japan, Malaysia, and Thailand represent the most frequently impacted economies, each showing persistent levels of attack activity driven by a combination of high population density, mobile centric financial activity, and diverse regulatory and infrastructure maturity across the region.

Ransomware and Breach & Leak incidents were particularly prominent across APAC. South Korea recorded 31 ransomware cases, making it the second most impacted country globally after the U.S., while India and Malaysia each registered 10 ransomware attacks, and Japan followed closely with 9 incidents.
Breach & Leak activity similarly showed strong regional concentration, with India (31) and Indonesia (24) ranking as the second and third most targeted countries worldwide for data compromise events. Thailand also appeared on the list with 13 incidents. These figures reveal persistent vulnerabilities tied to cloud misconfigurations, identity compromise, and the high-value customer datasets held by APAC financial institutions.

Disruptive attacks also played a major role in shaping the region's threat landscape. India appeared again among the top targets for DDoS, recording 31 incidents, placing it in the upper tier of globally targeted countries, particularly within prolonged hacktivist campaigns.

Defacement activity showed similar trends: Indonesia registered 8 defacement incidents, while India recorded 36, the second-highest number globally after the U.S. This pattern highlights APAC's dual exposure to both financial motivated threat actors and ideologically driven hacktivist groups.

Overall, the APAC region's 2025 cyber landscape demonstrates a mix of high volume data compromise, substantial ransomware pressure, and sustained disruptive activity, emphasizing the need for enhanced resilience, mobile first fraud defenses, and proactive intelligence capabilities across its financial sector.

PREDICTIONS FOR 2026

The financial sector is expected to face an even more challenging cyber landscape in 2026, shaped by the strong escalation of threat activity seen throughout 2025. The sharp rise in DDoS, breach and leak incidents, ransomware, and web defacement suggests that adversaries are becoming more capable and better equipped to exploit weaknesses across global financial ecosystems. These developments indicate that 2026 will bring continued growth in both volume and sophistication of attacks targeting banks, payment systems, and digital financial services.

DDoS attacks are likely to expand further as hacktivist groups continue using fast deployment models and accessible botnet infrastructure. The dramatic doubling of DDoS activity in 2025 signals that campaign-driven attacks tied to geopolitical events and public disruption efforts will remain common. Financial institutions should expect more high-frequency bursts aimed at online banking portals, payment platforms, and customer-facing systems.

Ransomware operations are also expected to evolve with more aggressive extortion tactics. Building on the steady growth observed in 2025, ransomware actors will likely strengthen their affiliate networks and improve their ability to target financial organizations through supply chain weaknesses. Data theft, service disruption, and pressure campaigns that target executives and customers will become increasingly common as groups like Qilin, Akira, and Clop refine their methods.

Breach and leak incidents will likely continue rising as attackers exploit cloud misconfigurations, weak access controls, and third-party integrations. The high number of attacks attributed to unknown actors in 2025 indicates that stealthier intrusion strategies will expand in 2026. Financial institutions should expect persistent identity-based attacks and quiet, long-term compromises of sensitive data environments.

AI-driven fraud will escalate significantly. Following the emergence of AI-powered investment scams and deepfake identity bypass in 2025, attackers will increasingly automate social engineering, KYC manipulation, and financial impersonation. Deepfake videos, synthetic voices, and fabricated documents will make identity fraud more scalable and harder to detect, challenging traditional onboarding and authentication systems.
Mobile threats are projected to grow as well. The evolution of Android trojans like Herodotus shows that attackers are moving toward more human-like interaction emulation and advanced device control. These techniques are expected to spread across more malware families, increasing risks for mobile-first financial interactions and authentication flows.

Payment fraud will also intensify, particularly in regions with outdated EMV implementations. The EMV cloning activity observed in LATAM during 2025 demonstrates that attackers are still exploiting magstripe fallback and permissive terminal configurations. These techniques are expected to expand into additional regions with similar structural weaknesses, putting pressure on financial institutions to enforce stricter payment controls.
Overall, 2026 is expected to bring increasing operational risk as adversaries become more automated, more coordinated, and more effective at exploiting digital and human vulnerabilities. Financial institutions that invest in adaptive, intelligence-led security programs will be better positioned to manage the rapidly evolving threat landscape.

CONCLUSIONS

The 2025 financial threat landscape underscores an alarming upward trajectory in both the frequency and sophistication of cyberattacks. Financial institutions worldwide faced multifaceted challenges, ranging from service disruption and extortion to large-scale data compromise and emerging AI-driven fraud. Europe, while comparatively less affected than the United States, showed significant exposure, particularly in the United Kingdom, France, and Germany, reinforcing the need for region-specific threat awareness and mitigation strategies.

Key takeaways include the persistence of DDoS attacks as a primary disruption vector, the growing scale and complexity of ransomware operations, the stealth and financial motivation behind breaches and leaks, and the rise of AI-powered schemes that exploit trust and human behavior. Mobile threats and payment fraud, including EMV cloning, further complicate the defensive landscape, demanding continuous innovation and vigilance.

To navigate the evolving environment, financial institutions must prioritize a combination of preventive, detective, and responsive controls. This includes strengthening resilience against DDoS and ransomware, enhancing identity governance, implementing AI-resilient fraud detection, securing third-party integrations, and maintaining robust monitoring across both IT and operational technology environments.

Ultimately, the 2025 trends signal that cyber risk in the financial sector will continue to intensify. Organizations that proactively leverage threat intelligence, adaptive security frameworks, and cross-border collaboration will be best positioned to withstand disruptions, protect sensitive data, and maintain trust in an increasingly complex and adversarial digital ecosystem.

RECOMMENDATIONS

Check Point Exposure Management recommends the following:

1 Strengthen Identity Security & Access Controls

Because breach & leak events rose significantly and were often driven by credential compromise:

- Enforce passwordless authentication (FIDO2/passkeys).
- Adopt strict Zero Trust identity governance (least privilege, continuous risk scoring).
- Monitor privileged accounts continuously, including 3rd party integrations.
- Deploy automated detection for abnormal lateral movement.

2 Enhance DDoS Resilience (Most Common Attack Type Overall)

DDoS volume more than doubled YoY and consistently targeted financial services.

- Use always-on mitigation instead of on-demand scrubbing.
- Segment critical customer services (banking portals, payment APIs) from public infrastructure.
- Adopt multi-CDN routing, DNS failover, and dynamic rate limiting.
- Create playbooks for hacktivist-driven bursts and politically timed campaigns.

3 Hardening Against Ransomware & Extortion Attacks

With 451 ransomware cases recorded in 2025:

- Implement EDR with strong behavioral analytics.
- Patch high-risk services routinely (VPNs, mail servers, perimeter devices).
- Maintain immutable, segmented, offline-capable backups.
- Adopt microsegmentation to limit blast radius.
- Test ransomware IR playbooks quarterly, including double- and triple-extortion scenarios.

4 Improve Cloud & Data Protection to Prevent Breach/Leak Events

Given sharp increases in global data compromise events:

- Continuously scan for misconfigurations (open S3 buckets, permissive firewall rules).
- Tokenize sensitive customer data at rest and in transit.
- Implement automated classification for PCI, PII, and financial data flows.
- Enforce strict access governance for cloud developers, contractors, and SaaS connectors.

5 Counter AI-Driven Scams, Deepfake Fraud & Synthetic Identity Abuse

The report highlights AI-generated personas used in investment scams and KYC bypassing.

- Add AI-resilient KYC checks: passive liveness, device behavior analysis, velocity rules.
- Deploy deepfake-detection solutions for voice, video, and document authentication.
- Educate employees and customers about AI-assisted social engineering techniques.
- Block non-official financial apps and sideloaded APKs on corporate devices.

6 Strengthen Anti-Phishing and Social Engineering Defenses

The surge in PhaaS (e.g., Spiderman platform) reflects increasingly sophisticated phishing.

- Deploy real-time phishing protection on endpoints (browser isolation, link rewriting).
- Use DMARC, SPF, and DKIM enforcement with continuous monitoring.
- Implement SMS phishing detection for mobile-first attacks.
- Train employees to identify AI-generated adversarial lures.

7 Fortify Mobile Banking Security

Banking trojans like Herodotus showed advanced evasion and device-control capabilities.

- Integrate mobile app hardening:
  - Accessibility abuse detection
  - Emulator/root detection
  - Anti-screenshot and anti-overlay measures
- Add behavioral biometrics to detect scripted or synthetic interactions.

  Monitor for rogue WebView-based apps impersonating banking platforms.

8 Improve Payment System Security (Especially EMV & Card Fraud)

EMV cloning campaigns exploited outdated fallback and terminal misconfigurations.

- Enforce online-PIN only for all card-present transactions where feasible.
- Reduce magstripe fallback acceptance across all terminals.
- Monitor for:
  - Unusual offline approvals
  - High-risk POS locations
  - Fallback-triggered transaction spikes
- Collaborate with acquirers and ATM operators to harden payment infrastructure.

9 Strengthen Digital Surface Monitoring & Early-Warning Capabilities

Across all incident types, early detection reduces impact.
Through this ongoing partnership, Check Point Exposure Management delivers:

- Continuous monitoring across:
  - Dark web forums for credential leaks
  - Hacktivist channels for DDoS planning and campaign chatter
  - Phishing kit deployments, domain registrations, and emerging fraud infrastructure
- Real-time tracking of impersonation domains, rogue applications, Telegram channels, and criminal marketplaces.
- End-to-end takedown support, enabling fast removal of:
  - Impersonation Websites
  - Social Media Impersonation
  - WhatsApp Impersonation
  - Exposed Documents

By maintaining and strengthening the collaboration with Cyberint, organizations ensure they remain protected by an always on threat intelligence operation that detects, investigates, and mitigates external risks before they escalate into impactful incidents.

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.
With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: checkpoint.com/exposure-management