SISA
SAPPERS

THREAT REPORT

H1 2025

DIGITAL FORENSICS
SISA
SAPPERS
UNVEILING THE TRUTH

Table Of Content

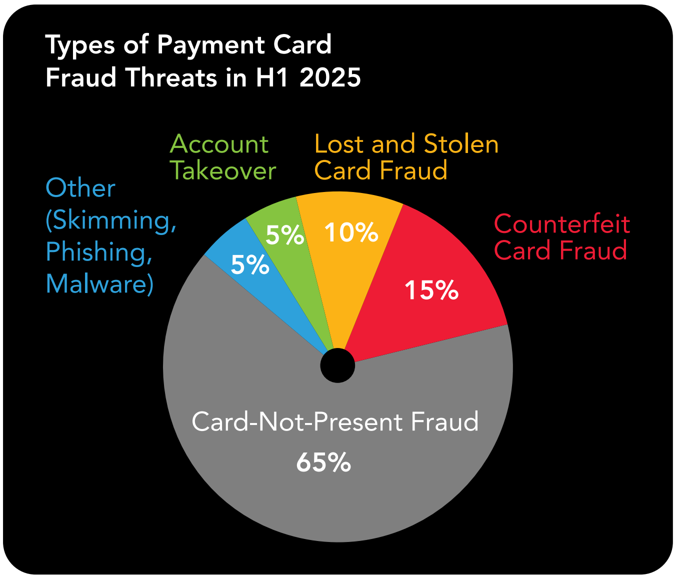
Table Of Content

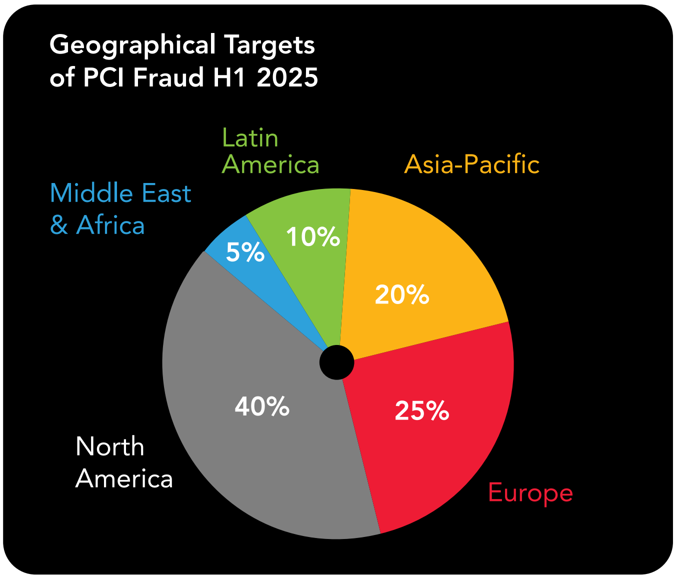
Executive Summary

In 2025, the global financial ecosystem confronts a dual-front cyber onslaught: on one side, sophisticated malware, ransomware-as-a-service outfits and nation-state actors,such as LockBit, Akira, Cl0p, and North Korea's Lazarus Group,are executing high-value data theft, double-extortion and multi-billion-dollar crypto heists; on the other, critical software vulnerabilities have been weaponized with unprecedented speed. Beyond stealer malware like AgentTesla and phishing kits like Cogui, five zero-day and high-severity flaws (including CVE-2025-22457 in Ivanti Connect Secure, sandbox escapes in Chrome's V8 engine, SAP NetWeaver deserialization (CVE-2025-42999), and a Mark-of-the-Web bypass in 7-Zip) were added to CISA's Known Exploited Vulnerabilities catalog and exploited in the wild. These vulnerabilities span enterprise VPN gateways, browser sandboxes, application deserialization, and archive handling,underscoring how attackers blend technical exploits with human-centric fraud. To stay ahead, BFSI institutions must not only deploy zero-trust architectures, endpoint segmentation, immutable backups, and AI-driven anomaly detection, but also implement a rigorous, real-time vulnerability management program: immediate patching of affected systems, thorough threat hunting on unpatched assets, and continuous compliance with KEV deadlines are now as critical as perimeter defenses.

BFSI-Specific Impact

The BFSI sector, particularly banks, mortgage firms, credit unions, NBFCs, and investment entities, faced targeted attacks leveraging stolen credentials, unpatched VPNs, phishing, and supply-chain vulnerabilities. Actor groups used specialized dark-web leak sites and negotiation portals to extort payment and showcase stolen data.





1.1 Emerging Trends

1.1.1 Japanese Digital-Skimming Campaign

Description: A long-running group exploited XSS vulnerabilities in Japanese eCommerce platforms. They submitted orders laced with malicious scripts that stole admin credentials, then injected JavaScript sniffer code to harvest PANs, CVVs, expiration dates, and billing addresses from real customer checkouts. Harvested data was stored in PNG files for covert exfiltration.

Why it matters: This multi-stage compromise, from XSS to credential theft to digital skimming, demonstrates how threat actors chain minor vulnerabilities into full data-theft campaigns.

1.1.2. Offline Transaction Fraud via HCE Apps

Description: Merchants misconfigure POS terminals to permit offline chip approvals. A malicious Android Host-Card-Emulation (HCE) app simulates a valid offline cryptogram (TC) to the terminal instead of forwarding the request online for issuer authorization. The terminal happily approves, then later sends the bogus transaction for clearing, leaving issuers on the hook.

Why it matters: This entirely in-store attack can evade real-time authorization controls. Only careful terminal configuration and velocity-based decline rules can stop it.

1.1.3 NFCGate ATM Relay Fraud

Description: Victims are phished into installing a spoofed "bank" app containing modified NFCGate code. They're instructed to place their contactless card under their phone and enter their PIN, thinking they're verifying identity. Behind the scenes, the app reads NFC data and PIN, relays to a co-conspirator's device, which then performs an ATM withdrawal via NFC on a compromised or collusive ATM.

Why it matters: Tapping into NFC's convenience feature subverts physical-POS and ATM controls, all through social engineering. Victims willingly hand over both data and PIN.

1.1.4 Contactless Purchase-Return Authorization (PRA) Fraud

Description: Fraudsters exploit the window between an approved Purchase Return Authorization (PRA) and its subsequent reversal. They buy high-value items with a debit card, then attempt a return using gift cards while feigning distraction (e.g., on a phone call). The initial full-value return fails, so they process multiple partial returns across several gift cards, each successful partial return boosts the issuer's Open-to-Buy (OTB) on the debit account. Finally, they cancel the returns and leave with the merchandise. Issuers, seeing only the interim successful partial credits, allow the customer to withdraw cash against the inflated balance before the final reversal posts.

Why It Matters:

- Exploits timing gaps in issuer systems
- Evades merchant reconciliation (offsetting credits)
- Cross-merchant coordination, from 10 to 120 miles, enables sustained OTB inflation
- Losses accrue at the issuer level, often undiscovered until after cash-outs occur

Recommendations:

- Real-Time Refund Monitoring: Detect repetitive partial refunds and flag multiple returns without matching original sales
- OTB Controls: Do not increase available balance until settlement arrives
- Settlement-First Posting: For single-message issuers, ensure PRAs post only after settlement, not at authorization
- Customer/Merchant Education: Warn that reversed credits may still be spendable briefly

1.1.5 Lenient Monitoring on VIP Accounts

Description: Issuers often exempt high-net-worth "VIP" accounts from standard fraud rules to minimize false declines. Attackers purchase compromised VIP PANs from underground shops and execute repeated high-dollar transactions, approved because these cards bypass real-time velocity and location checks.

Why It Matters

- VIP exemption creates a high-value blind spot
- Single transaction losses can exceed hundreds of thousands of dollars
- Reputation-driven rule-relaxation becomes exploitable

Recommendations:

- Inclusive Monitoring: Apply real-time fraud rules to all account tiers; adjust thresholds but never omit VIP cards

- Geolocation Analytics: Alert on implausible travel-speed transactions
- VIP Confirmation Protocols: Direct high-value alerts to dedicated VIP relationship managers for quick out-of-band verification

1.1.6 Token Relay Attacks

Description: Threat actors blend provisioning fraud with geographically distributed relay: 1) Provision a stolen PAN as a mobile token on Device A. 2) Co-conspirators at Stores B, C, D each run an NFC tap using a malicious app that relays authorization requests back to Device A. Valid ARQC cryptograms from Device A enable approved in-store transactions at each location, often for cashable gift cards.

Why It Matters

- Scales a single stolen PAN into multiple high-value purchases
- Exploits valid cryptograms, so risk systems see "legitimate" chip transactions

Recommendations:

- Provisioning Monitoring: Scrutinize device attributes, provisioning risk scores, and location anomalies at token issue time
- ATC-Based Risk Scoring: Use the Application Transaction Counter from chip messages to detect out-of-sequence or excessive uses
- Post-Provisioning Velocity: Impose tighter limits on the first few token transactions; gradually relax after establishing normal behavior

1.1.7 Chip-Shimming & Transaction Relay

Description: Shimming devices, thin interceptors inserted into EMV chip slots on unattended terminals (e.g., transit UATs), capture chip data and PIN. Attackers relay this to a receiver card, then use the harvested data at an ATM for immediate cash-out. The latest evolution even blocks legitimate chip reads at the POS, preventing detection by "follow-on" transaction rules.

Why It Matters

- Targets high-traffic areas (transit hubs) where users default to chip dip vs. contactless
- By blocking legitimate authorizations, it evades detection patterns that monitor ATM right after POS

Recommendations:

- Eliminate Plaintext Offline PINs: Enhanced security protocols phased out plaintext PIN storage on terminals as of Jan 2025
- Merchant Onboarding Rules: Flag new or sudden high-value, low-volume merchants, especially in tourist corridors, for enhanced due diligence
- Issuer Rules: Decline or alert on cross-border ATM cash-outs at maximum daily limits, especially in geographies inconsistent with typical cardholder behavior

1.2 Evolving Trends

1.2.1 AI-Driven

Attack Types Between January and July 2025, the Banking, Financial Services, and Insurance (BFSI) sector faced a surge in cyber attacks leveraging artificial intelligence (AI) and machine learning (ML) technologies. Attackers utilized AI to automate and enhance attack vectors, including phishing, ransomware, deepfake scams, and adversarial tactics, exploiting the sector's reliance on trust and sensitive data. This report provides a technical deep dive into these threats, their impact on BFSI, notable incidents, and AI-based defense strategies, encouraging reflection on how these technologies reshape cybersecurity.

1. Phishing and Spear-Phishing

Generative AI models have transformed phishing into a highly targeted threat. Advanced language models, such as GPT - 4.5 or similar, generate contextually relevant, grammatically flawless emails and messages that mimic trusted entities. In June 2025, an Iran - linked APT group (APT35) targeted BFSI executives in Israel with AI - crafted spear -phishing emails and WhatsApp messages, directing victims to fake login pages for banking platforms to harvest credentials. Industry data indicate that 83% of phishing emails targeting BFSI from September 2024 to February 2025 were AI - generated, a 54% year-over - year increase.

Technical Details:

- Models Used: Large language models (LLMs) like GPT - 4.5, capable of natural language generation with high contextual accuracy.
- Data Sources: Publicly available data from social media, corporate websites, and breached datasets, used to personalize messages.
- Attack Vector: Emails and instant messages with malicious links or attachments, often hosted on domains mimicking legitimate services.
- Detection Challenges: Signature-based detection fails against dynamic AI-generated content, requiring ML-based behavioral analysis to identify anomalies in message patterns or metadata.

2. Ransomware and Automated Malware

AI has been integrated into malware development, notably in ransomware. The FunkSec ransomware group, emerging in late 2024, targeted over 80 BFSI entities with its AI-assisted malware, FunkSec V1.5, written in Rust. The group used AI to generate code comments and automate target selection and ransom negotiations via an AI chatbot, enabling even low-skill attackers to deploy sophisticated Ransomware-as-a-Service (RaaS).

3. Deepfake Audio/Video Scams

AI-driven deepfake technology has enabled sophisticated fraud by cloning voices and faces. In January 2025, a Hong Kong merchant lost HK$145 million (~$18.5M) in a cryptocurrency scam where attackers used AI to clone a financial manager's voice on WhatsApp, convincing the victim to transfer USDT. Similarly, a U.S. insurance firm in May 2025 lost millions due to AI-generated voicemails impersonating a CFO.

Technical Details:

- Voice Cloning Process:
- Audio Collection: Scammers gather 3–30 seconds of audio from public sources (e.g., social media, interviews) or social engineering.
- AI Modeling: Deep learning models like WaveNet or Tacotron analyze vocal traits (pitch, tone, cadence) to create a voice profile.
- Voice Synthesis: Synthetic speech generated to mimic the target, deployable in real-time or pre-recorded scams.
- Application in Scams: Impersonation of trusted individuals to authorize fraudulent transactions or extract credentials.

Targeted BFSI Subsectors:

- Banking: Commercial and retail banks face AI-enhanced Business Email Compromise (BEC) and phishing campaigns. AI-crafted emails mimicking bank executives or vendors tricked employees into transferring funds or exposing credentials.
- Cryptocurrency Platforms: Crypto exchanges and traders were prime targets for deepfake scams and ransomware. The January 2025 Hong Kong crypto scam underscores the sector's exposure to AI-driven fraud.
- Insurance: Insurers were hit by AI-generated phishing and deepfake scams impersonating policyholders or executives, aiming to manipulate claims or authorize fraudulent payouts.
- Payment Systems: Fintech and payment processors face AI-powered attacks exploiting transaction systems, with automated bots testing for vulnerabilities in real time.

Notable Incidents in BFSI

- Jan 2025 – Hong Kong Crypto Scam: Attackers used an AI-cloned voice of a bank executive on WhatsApp to deceive a merchant into a fraudulent cryptocurrency investment, resulting in a HK$145M (~$18.5M) loss. Hong Kong police noted this as part of a broader wave of AI-assisted BFSI frauds costing over HK$200M in a single week.

- Jan 2025 – FunkSec Ransomware: Check Point reported that the “FunkSec” ransomware gang targeted 80+ BFSI entities, including banks and crypto platforms, using AI-generated code and an AI chatbot for target selection and ransom negotiations. The malware’s polished code comments, contrasting the group’s poor English, confirmed AI’s role in its development.
- May 2025 – U.S. Insurance Firm Deepfake Fraud: A U.S. insurer was defrauded of millions after attackers used AI-generated voicemails impersonating a CFO to authorize wire transfers. The incident prompted warnings about AI-driven vishing targeting BFSI executives.
- Jun 2025 – Iran-linked APT35 Campaign: An Iranian APT targeted Israeli BFSI professionals with AI-crafted spear-phishing emails and WhatsApp messages, directing victims to fake banking login pages. This campaign reflects AI’s role in nation-state attacks on financial systems.

Defense Strategies in BFSI

Strategy	Description
Behavioral Analytics	AI systems monitor user behavior to detect anomalies like unusual transactions or logins, and spot AI-generated phishing.
Deepfake Detection	AI tools detect manipulated audio/video to prevent fraud.
Automated Response Systems	AI-driven tools isolate/neutralize threats rapidly, reducing incident response times.
Employee Training	Staff are trained to detect AI-generated threats and phishing attempts.

1.2.2 Business Email Compromise (BEC) Incidents

Business Email Compromise (BEC) continues to be a top cyber-fraud threat in 2025. BEC schemes range from invoice and CEO impersonation scams to sophisticated vendor compromises, resulting in billions of dollars in losses (the FBI estimates ~$51 billion exposed globally). This report summarizes the types of BEC attacks, notable global incidents (Jan–Jul 2025), their financial/organizational impact, evolving attacker techniques/trends, typical victims, and defensive best practices.

Types of BEC Attacks and Threat Vectors

Attackers use various social-engineering techniques to trick employees into wiring funds or disclosing data. Key BEC scam types identified by the FBI include:

BEC Scam Type	Description / Tactics
False Invoice (Vendor Impersonation)	Fraudsters send fake invoices posing as legitimate suppliers. They often use a realistic template but change the payee bank details, so victims unknowingly pay the attacker's account.
Executive Impersonation (CEO/CFO Fraud)	The attacker spoofs a high-ranking executive's email, urgently instructing an employee (often in finance) to transfer funds or sensitive information. Exploiting authority and urgency, victims are tricked into wiring money (often overseas) or sharing confidential data.
Account/Email Compromise	A real corporate or vendor email account is hijacked (via phishing or credential theft) so that fraudulent payment requests come from a trusted sender. Victims receive seemingly normal invoices or payment requests, but the funds are diverted to the attacker's account.
Attorney/Legal Impersonation	Attackers pose as a company lawyer or legal representative, often citing confidentiality or urgency, to bypass normal approval. Employees (especially low-level staff) then follow the request (e.g. transferring money) without independent verification.
Data Theft	Some BEC schemes target finance or HR to steal valuable information (e.g. tax forms, employee PII) rather than immediate funds. Stolen data can be sold on the dark web or used for future attacks.

Other threat vectors and techniques include display-name spoofing and lookalike domains (e.g. buying a similar domain to mimic a real email address), compromised webmail accounts, and sometimes voice (vishing) calls to reinforce an email request. Rapid advances in technology (e.g. AI tools) are making fraudulent emails more convincing. In all cases, attackers rely on human trust (e.g. urgency, authority) to circumvent technical defenses.

1.2.3 Ransomware Actor's Exploitation of Blockchain- Based Payments and Tumblers Cryptocurrencies of Choice

Bitcoin: The Dominant Ransom Currency - Bitcoin remains the most prevalent cryptocurrency for ransomware payments, accounting for the vast majority of ransom demands due to its liquidity and universal acceptance. The Financial Crimes Enforcement Network (FinCEN) identified Bitcoin as the most common ransomware-related payment method, with over $5.2 billion in ransom payments made in Bitcoin alone. Despite its public nature, Bitcoin's widespread adoption and established infrastructure make it the preferred choice for ransomware operators seeking reliable payment processing.

Privacy Coins: Enhanced Anonymity - Privacy-focused cryptocurrencies, particularly Monero (XMR) and Zcash (ZEC), have gained significant traction among ransomware actors seeking stronger on-chain anonymity. A notable trend has emerged where ransomware groups offer dual payment options: Bitcoin with a premium surcharge or Monero at a discounted rate. For instance, the DarkSide group, responsible for the Colonial Pipeline attack, charged 10-20% higher prices for Bitcoin payments while accepting Monero at the base rate. This pricing strategy reflects the perceived value of enhanced privacy features.

In 2021, FinCEN identified 17 ransomware-related reports requesting payment in Monero, while research revealed at least 22 ransomware strains accepting only Monero and at least 7 strains accepting both Bitcoin and Monero. REvil ransomware notably switched to accepting only Monero in 2021, demonstrating the growing preference for privacy coins among sophisticated threat actors.

Emerging Tokens: Volatility Mitigation - Ransomware actors have begun experimenting with stablecoins such as USDT and USDC to reduce volatility risk during the payment and laundering process. This trend reflects the professionalization of ransomware operations and their desire to minimize financial exposure during extended negotiation periods.

Ransom Payment Mechanics

Ransom Notes and Digital Infrastructure - Modern ransomware operations have evolved beyond simple text-based ransom notes to include sophisticated payment portals. Attackers now embed QR codes and detailed cryptocurrency addresses directly into ransom demands, streamlining the payment process for victims. These portals often include real-time exchange rates, payment timers, and even customer support chat functions to facilitate transactions.

Payment Deadlines and Escalation Strategies - Ransomware groups employ sophisticated pressure tactics through escalation clauses. Typical ransom demands include deadlines of 24-48 hours, after which the ransom amount doubles. Some groups implement progressive pricing models where payments increase incrementally over time, creating urgency while maintaining negotiation windows. The average ransom demand has increased dramatically from $111,605 in 2019 to $5.2 million in 2024, representing a 4,559% increase.

Victim-Specific Wallet Management - To prevent cross-linking and enhance operational security, ransomware operators generate unique cryptocurrency addresses for each victim. This practice complicates blockchain analysis efforts and reduces the risk of exposing the broader payment infrastructure through a single compromised address.

Affiliate-Style Revenue Distribution

- **Ransomware-as-a-Service Business Models** - The RaaS ecosystem operates on various revenue-sharing models that mirror legitimate Software-as-a-Service platforms. The most common profit-sharing arrangements include:
- 70/30 split: Affiliates receive 70% of ransom payments, operators retain 30%
- 80/20 split: Affiliates receive 80%, operators retain 20% (used by LockBit)
- 90/10 split: Affiliates receive 90%, operators retain 10% (used by Ransom Hub and APT 73)

These arrangements often include performance-based adjustments, where more skilled affiliates with established infrastructure and proven track records receive higher commission rates.

Automated Payment Distribution - Advanced RaaS operations now employ smart contracts and automated scripts to distribute ransom payments immediately upon receipt. This automation reduces manual intervention and minimizes the risk of disputes between operators and affiliates while ensuring rapid profit distribution across the criminal ecosystem.

Mixing and Tumbling Services

Traditional Centralized Mixers - Centralized cryptocurrency tumblers have been extensively used by ransomware groups for laundering proceeds. Services like ChipMixer (shut down in 2023) processed over $3 billion in cryptocurrency and was used by prominent ransomware groups including LockBit, Conti, REvil, and Royal. These services typically charge 1-3% transaction fees while pooling funds from multiple users and redistributing them at random intervals to obscure transaction trails.

CoinJoin Protocols - Peer-to-peer privacy schemes such as Wasabi Wallet and Samourai's Whirlpool have gained popularity among ransomware actors seeking decentralized mixing solutions. These protocols enable users to coordinate mixing activities without relying on centralized services, reducing the risk of service seizures by law enforcement.

Smart Contract-Based Mixers - Ethereum-based mixers like Tornado Cash have become increasingly popular for ransomware laundering, processing over $7 billion in cryptocurrency since 2019. The service was used to launder more than $96 million from the Harmony Bridge heist and $7.8 million from the Nomad heist. Despite U.S. Treasury sanctions in 2022, Tornado Cash continues to operate, though at reduced volumes.

On-Chain Laundering Techniques

Chain Hopping - Ransomware groups have increasingly adopted "chain-hopping" strategies, moving funds across different blockchains to break transaction trails. This technique involves converting Bitcoin to Ethereum through DeFi bridges, then swapping for other tokens or stablecoins. The Conti ransomware group laundered approximately $29 million through RenBridge in Q4 2021, while Ryuk affiliates moved $35 million through the same service in Q2 2022.

Layering and Obfuscation - Sophisticated ransomware operations employ multiple successive mixing transactions, cross-chain bridges, and decoy transactions to create complex laundering networks. These layering techniques make it increasingly difficult for investigators to trace the ultimate destination of ransom payments.

Cash-Out Strategies - Ransomware operators utilize various cash-out methods including peer-to-peer over-the-counter brokers, gift card exchanges, and darknet marketplaces. Some groups have established relationships with complicit exchanges or use mule networks to convert cryptocurrency to fiat currency while maintaining operational security.

Blockchain Analytics Countermeasures

Blockchain Analytics Capabilities - Leading blockchain intelligence firms including Chainalysis, Elliptic, and TRM Labs have developed sophisticated tools for tracking ransomware payments. These platforms can cluster addresses, identify mixing patterns, and trace cross-chain transactions, providing law enforcement with unprecedented visibility into ransomware financial networks.

Regulatory Responses - The U.S. Treasury's Office of Foreign Assets Control (OFAC) has taken aggressive action against cryptocurrency mixing services, sanctioning Tornado Cash in 2022 and Blender.io previously. These sanctions make it illegal for U.S. persons to use these services and have resulted in significant volume reductions, though illicit usage percentages have increased

Financial Impact and Trends

Payment Volume Analysis - Ransomware payments reached approximately $813.55 million in 2024, representing a 35% decrease from 2023's record $1.25 billion. However, this decline masks concerning trends including larger individual payments and increased targeting of high-value victims. The median ransom payment soared from less than $199,000 in early 2023 to $1.5 million by June 2024.

Mixer Usage Statistics - Cryptocurrency mixers processed over $51.8 million worth of cryptocurrency daily at their peak, with illicit addresses accounting for 23% of mixer volumes, indicating growing sophistication in laundering techniques among cybercriminals.

2.1 Western Alliance Bank – Cleo File Transfer Breach 2025

Background: In March 2025, Western Alliance Bank, a major Arizona-based financial institution with over $80 billion in assets, disclosed that approximately 22,000 customer records were compromised through a breach involving a third-party managed file-transfer system. The attack exploited vulnerabilities in Cleo MFT software. Data was exfiltrated between October 12 and October 24, 2024, but the breach remained undetected until January 27, 2025. Exposed information included names, Social Security numbers, dates of birth, bank account and driver's license numbers, tax IDs, passport details, and in some cases, credit and debit card numbers, including CVV codes. The bank launched an investigation, notified regulators, and began informing affected customers, offering one year of complimentary identity-protection services. The breach highlights the risks posed by third-party applications, particularly in the BFSI sector.

Threat Actors: The breach was attributed to the CL0P ransomware and data extortion gang. Known for large-scale attacks on file-transfer systems such as MOVEit, Accellion, and GoAnywhere, CL0P exploited zero-day flaws in Cleo's managed file transfer platform and began listing victim organizations on its leak site. Western Alliance was named in late 2024. CL0P typically exfiltrates sensitive data and threatens public release unless ransom demands are met. The group is believed to operate out of Russia and frequently targets banking and financial organizations due to the sensitive nature of the data they handle.

Method of Attack: The attack leveraged two zero-day vulnerabilities in Cleo's file-transfer systems. In October and December 2024, Cleo patched critical remote code execution flaws in its LexiCom, VLTransfer, and Harmony products. Before these patches were widely implemented, CL0P deployed a Java-based backdoor, installed via a malicious Freemarker template. This backdoor provided access to a limited part of Western Alliance's infrastructure. Over a two-week period, attackers exfiltrated sensitive files containing personal and financial data. The breach only came to light after CL0P began leaking samples of the data online in early 2025.

Response - Once the breach was detected, Western Alliance Bank immediately notified law enforcement, regulators, and affected state authorities. Public disclosures were made through SEC filings and press releases. Impacted individuals were contacted directly and offered free access to identity theft protection services. The bank stated that, to date, no fraud had been detected using the stolen data. In parallel, the bank initiated a review of its security controls and removed vulnerable Cleo applications from its systems. Other organizations affected by the same Cleo vulnerability, including some of Western Alliance's partners, undertook similar actions to mitigate the threat.

Impact - The exposure of nearly 22,000 records containing sensitive PII and payment information presents serious regulatory and reputational risks. The compromised dataset included Social Security numbers, passport and driver's license details, and credit/debit card numbers with CVVs. Such data falls under the purview of PCI DSS, which strictly prohibits the storage of CVV codes and mandates encryption of PAN and cardholder data. Regulatory bodies, including federal and state banking authorities, may investigate whether the bank complied with relevant data protection standards. The breach could result in lawsuits, customer distrust, and intensified scrutiny of the bank's third-party risk management program. Though smaller in scale than earlier mega-breaches, the inclusion of regulated financial data significantly raises the breach's severity in the BFSI context.

How It Could Have Been Prevented - The breach highlights several key failings that could have been addressed through stronger compliance with PCI DSS and BFSI security standards:

Timely Patch Management

- Cleo released patches in October and December 2024, but the bank had not applied them before the breach window. A proactive vulnerability management program would have reduced the exposure window.

Data Encryption and Storage Controls

- Cardholder and personal data should be encrypted both in transit and at rest. PCI DSS mandates strong cryptographic protections, especially for payment data and identity documents.

Access Controls and Segmentation

- The compromised file-transfer application should have been segmented from critical systems. Least-privilege principles, multi-factor authentication, and network segmentation would have limited the attack's reach.

Third-Party Vendor Oversight

- PCI DSS requires formal agreements and regular assessments of third-party providers that handle cardholder or personal data. More stringent controls on Cleo's MFT deployment may have identified risks earlier.

Data Minimization

- Storing CVV codes is a direct violation of PCI DSS. Implementing tokenization and eliminating storage of unnecessary sensitive authentication data would have reduced the impact.

Incident Response Planning

- A well-drilled incident response strategy could have helped detect the breach earlier. Monitoring file transfers, conducting regular security audits, and employing intrusion detection tools would have shortened the breach dwell time.

By adhering more closely to PCI DSS requirements and BFSI security best practices, the risks posed by third-party software vulnerabilities can be substantially mitigated.

2.2 Insurance Sector Breach (Aflac, Erie, Philadelphia Insurance) – June 2025

Background: In mid-June 2025, a wave of breaches hit U.S. insurance companies. On June 12, 2025, supplemental insurance giant Aflac disclosed that its network had been infiltrated. Within days, filings and news reports revealed that Philadelphia Insurance Companies (PHLY) and Erie Insurance had also been attacked in the same campaign. This sequence of incidents came after Google's threat analysts warned that a cybercrime group was systematically targeting the insurance industry.

Threat Actors: Security researchers quickly tied these intrusions to Scattered Spider (a.k.a. 0ktapus or UNC3944), a sophisticated criminal gang known for targeting one industry at a time. Google's analysts had warned that "actors bearing the hallmarks of Scattered Spider" were pivoting from retail into insurance. The group's playbook involves heavy social engineering: call-center phishing, SIM-swap attacks, and help-desk credential theft. Aflac itself said the breach had the telltale signs of Scattered Spider, though it could not conclusively name the group. Scattered Spider operators (primarily English-speaking, believed to be based in the U.S. and U.K.) are known to impersonate employees, bypass multi-factor authentication (MFA), and abuse password-resets on helpdesk systems. No state actor was implicated, this was a financially motivated criminal campaign focused on data extortion.

Method of Attack - The intruders at Aflac and others apparently gained initial access through social-engineering. They tricked or coerced helpdesk and call-center staff into handing over credentials. Once inside the network, the attackers moved laterally, elevating privileges. Critically, they did not deploy traditional ransomware-encryption; instead their goal was data theft and extortion. Aflac reported “unauthorized access” to systems containing customer claims, health records, Social Security numbers and other PII. In one case analysts estimate the thieves extracted over a terabyte of files. The attackers then threatened to dump the stolen data on leak sites if ransoms weren’t paid. (PHLY and Erie Insurance reported system disruptions but similarly said no ransomware encryption had been detected) In short, this was an identity-based breach: abusing human trust to steal data, rather than a malware outbreak.

Response - Aflac and the other insurers sprang into action. Aflac’s SEC filing said the intrusion was identified on June 12 and “contained within hours,” with core insurance operations remaining functional. The company retained outside forensics experts and notified affected individuals. Erie Indemnity (Erie Insurance) reported unusual network activity on June 7 and immediately isolated affected systems. It engaged law enforcement and cyber specialists to investigate. Philadelphia Insurance’s parent (Tokio Marine/First Insurance of Hawaii) took deliberate outage measures on June 9 to halt the threat and rebuild systems. All three insurers worked to restore services (customer portals, email/phones, claims systems) while piecing together the breach. None of them confirmed paying any ransom. By late June, Aflac said only a review of accessed files remained, and PHLY/Erie were gradually returning to normal. Throughout, regulators (like state insurance departments and HIPAA officials) were informed, and the companies offered credit monitoring to potential victims.

Impact - These attacks exposed vast amounts of sensitive personal and health data. Aflac warned customers that claims information, medical details, Social Security numbers and related data were likely accessed. PHLY and Erie had to suspend online services – policyholders could not file claims or get billing info for days – causing operational headaches. While exact figures of stolen records were not published, the volume (over a terabyte at Aflac alone) implies hundreds of thousands of records were at risk. Beyond the immediate disruption, insurers now face costly fallout: forensic and recovery expenses, legal and regulatory scrutiny, and likely fines under HIPAA/insurance privacy laws. Share prices for insurers dipped on the news, and the sector’s cyber insurance premiums surged. The campaign demonstrated that even regulated, well-defended firms can fall victim to cunning, human-focused attacks.

How It Could Have Been Prevented

Lessons from these breaches suggest several defenses:

- Multi-Factor Authentication (MFA): Enforce MFA on all administrator and support accounts (especially remote access and helpdesk portals). This would have thwarted simple credential theft.
- Employee Training: Conduct regular, targeted phishing and social-engineering drills for IT, helpdesk, and call-center staff so they recognize imposter tactics.
- Zero-Trust Segmentation: Segment the network so that compromising one user or system (e.g. HR database) cannot give access to all others. Critical assets (claims systems, databases) should be on isolated VLANs with strict access controls.
- Continuous Monitoring/Threat Hunting: Deploy user and entity behavior analytics to flag anomalous logins or data flows (e.g. a helpdesk account downloading gigabytes at 3 AM). Early detection could limit dwell time.
- Data Loss Prevention (DLP): Use DLP tools to alert on large file transfers or unusual data exfiltration. This can detect mass download of personal data for review before it leaves the network.

By hardening identity controls and limiting lateral movement, the insurers could have greatly reduced the attackers' foothold and the amount of data stolen.

2.3 Victoria's Secret Cybersecurity Incident

Background - Over Memorial Day weekend, Victoria's Secret experienced a significant cybersecurity breach, timed during a period of reduced staffing and high digital activity, paralleling risks seen in BFSI during holiday transaction spikes or fiscal reporting cycles. The breach compromised public-facing websites and internal systems, exposing sensitive customer and operational data. The attack revealed architectural weaknesses and non-compliance with essential security standards, notably PCI DSS.

Threat Actors - The attack is attributed to Scattered Spider, a sophisticated threat group known for targeting retail and financial entities through identity-based attacks. Their modus operandi includes social engineering and lateral movement, tactics increasingly used against BFSI institutions to bypass traditional defenses.

Method of Attack

Social Engineering and MFA Bypass:

- The attackers exploited IT help desk workflows, using vishing/smishing to obtain credentials and bypass Multi-Factor Authentication (MFA), a critical vector relevant to high-value accounts in financial systems.

Internal System Exploitation and Lateral Movement:

- Post-access, the threat actors moved laterally across an inadequately segmented network, compromising email systems, backend databases, and internal apps, mirroring risks to BFSI data centers and shared infrastructure.

Holiday Timing Abuse:

- The breach occurred during Memorial Day weekend, a high-risk period of reduced monitoring, similar to known BFSI threat windows like fiscal close weekends or public holidays.

Response

Victoria's Secret launched incident response efforts covering containment, forensic analysis, and compliance engagement. However, the response was hindered by:

- Lack of automated post-deployment scanning
- Inadequate visibility across internal environments
- Deficient logging and alerting from critical assets

Key PCI DSS controls (e.g., segmentation, change management, post-implementation testing) were found to be violated or absent, triggering regulatory and legal scrutiny.

Impact -

- Data Exposure: Customer PII and operational data were compromised.
- Financial Losses: Incident response, regulatory fines, legal fees, and brand damage mirrored the financial and reputational risks common in BFSI post-breach scenarios.
- Operational Disruption: Core business systems were affected, analogous to transactional delays or service downtime in banking systems.
- Compliance Pressure: The firm now faces increased audits and regulatory attention due to PCI DSS failures.

How It Could Have Been Prevented

- Micro-Segmentation: Enforcing strict network segmentation (as required by PCI DSS and NIST) could have contained the attack and prevented lateral movement, paralleling BFSI best practices in data zone isolation.
- Robust Change Management: Implementing CI/CD pipelines with integrated security gates and mandatory pre/post-change scans would have blocked zero-days and configuration drift.
- Identity and Access Governance: Mandatory MFA across all access layers, Privileged Access Management (PAM) for admin users, and principle of least privilege would have reduced attack surface.

- Advanced Threat Detection and Response:
  - Deploying SIEM with EDR/XDR integration
  - Using UEBA to detect anomalous user behavior
  - Running purple team simulations quarterly
- Compliance Automation: Regular PCI DSS 4.0 audits, third-party risk assessments, and real-time policy compliance checks using GRC platforms are vital, especially for BFSI where audits are frequent and legally binding.

2.4 Marks & Spencer, Co-op, and Harrod Ransomware Incident

Background - Between April and June 2025, UK retailers Marks & Spencer (M&S), Co-op, and Harrods were hit by coordinated ransomware attacks. Attackers used social engineering tactics to trick third-party IT support into resetting employee credentials, leading to system compromise, exfiltration of personal data, and widespread disruption of services such as e-commerce, payments, and logistics. These incidents reveal systemic failures in vendor governance, authentication controls, and network segmentation, issues that directly map to PCI DSS violations and raise concerns for the broader BFSI sector.

Threat Actors -
The attacks were attributed to Scattered Spider (UNC3944), an English-speaking cybercrime group specializing in social engineering, operating in conjunction with the DragonForce ransomware-as-a-service platform. Their tactics involve credential theft, MFA abuse, lateral movement, and double extortion. Four individuals aged 17–20 were arrested in July 2025 for their roles in the attacks, indicating the threat posed by youthful, decentralized threat actors using commercially available tools and social engineering expertise.

Method of Attack -

- Initial Access: Impersonation of staff via calls/emails to third-party helpdesks, tricking agents into resetting passwords and MFA tokens.
- Persistence: Attackers registered rogue MFA tokens and federated identity providers into SSO systems.
- Privilege Escalation: Creation of unauthorized service accounts to gain domain admin access.
- Lateral Movement: Use of RDP, TeamViewer, ngrok, and other tools to traverse networks.
- Exfiltration & Encryption: Stole PII, order data, and encrypted hundreds of virtual machines (including payment systems) using DragonForce ransomware.

Response -

- Containment: Shut down online portals and isolated servers.
- Recovery: Gradual restoration of services over 4–6 weeks with limited functionality.
- Notifications: Informed the UK's NCSC, regulators, and customers; public statements issued.
- Law Enforcement: Four suspects arrested by the NCA; international law enforcement involved.

Impact -

- Financial: Over £800 million in combined operating losses across the three retailers.
- Operational: Multi-week outages affecting payments, inventory, and click-and-collect systems.
- Regulatory: Increased scrutiny of breach reporting and vendor controls.
- Reputational: Loss of customer trust, especially due to data breaches and prolonged outages.

How It Could Have Been Prevented

- Vendor Governance (PCI DSS 12.8): Enforce third-party security controls and reset verification protocols.
- Authentication Controls (PCI DSS 8.3, 8.5): Use phishing-resistant MFA and disable self-service resets.
- Network Segmentation (PCI DSS 1.2, 11.3): Isolate critical payment and identity systems.
- Monitoring (PCI DSS 10.1): Deploy SIEM and EDR for alerting on suspicious login and data movement.
- Incident Response (PCI DSS 12.10): Run ransomware-specific drills and improve recovery readiness.
- Least Privilege: Apply just-in-time access and regular privilege reviews.
- Encryption: Encrypt all sensitive data with external key vaults and restricted access.
- BFSI Compliance Integration: Align PCI DSS with NIST and FFIEC frameworks for unified protection.

2.5 Cork Protocol Hack: $11M Exploit via Uniswap V4 Hook Vulnerability

Background - Cork Protocol, a DeFi platform providing depeg insurance for stablecoins and liquid staking tokens, was exploited on May 28, 2025. The attack leveraged vulnerabilities in its integration with Uniswap V4 hooks, resulting in a loss of $11 million.

Threat Actors - The attacker created a rogue market and deployed a malicious hook contract to manipulate Cork Protocol's contracts and token reserves.

Method of Attack -

- Cross-Market Token Confusion: The attacker created a fake market using legitimate DS tokens as RA, violating the protocol's design.
- Exploitation of Uniswap V4 Hooks:
  - Missing Access Control: The CorkHook.beforeSwap function lacked proper access control, allowing arbitrary external calls.
  - Forced Deposits at Rigged Rates: The attacker manipulated reserves to deposit DS tokens at falsified rates.
- Token Extraction and Redemption: The attacker converted fake tokens back into real ones and redeemed them for wstETH, draining liquidity.

Response - Cork Protocol's co-founder announced collaboration with leading security firms for a thorough review and post-mortem analysis. The firms involved include @zeroshadowio, @HypernativeLabs, @Quantstamp, @Spearbit, @CertoraInc, and @hexagate.

Impact - The exploit resulted in a loss of $11 million, highlighting the risks associated with flexible DeFi architectures and the importance of rigorous validation.

How It Could Have Been Prevented

- Strengthen Access Control: Use onlyPoolManager modifiers on all hook functions to restrict access. Deploy hooks via CREATE2 to enable counterfactual addresses, allowing permissions to be pre-assigned to known addresses before deployment.
- Enforce Token Validation: Whitelist RA/PA/DS/CT types during market creation and validate token roles.
- Implement Pool Whitelisting: Restrict hooks to specific pools using allowedPools mappings.
- Audit Holistically: Ensure auditors review interdependent components (hooks, oracles, markets) together.
- Input Validation: Validate swap parameters and ensure reserve updates and token settlements match expected behavior and type roles.

This incident underscores the need for vigilance in balancing flexibility with security in DeFi protocols.

03 Top Threat Actors Targeting BFSI Sector

In 2025, the BFSI sector endures aggressive double-extortion and data-theft campaigns by five major actors: Akira, LockBit, Cl0p, and DPRK's Lazarus Group. Akira and LockBit maintain active leak sites targeting mortgage lenders, loan services, and government portals, while Cl0p exploits MOVEit vulnerabilities to expose hundreds of institutions. Lazarus Group executed a $1.5 billion crypto heist at Bybit. These actors leverage advanced loaders, AI-crafted lures, and custom malware alongside public leak portals to maximize pressure. BFSI organizations must enforce zero-trust segmentation, monitor legitimate-tool usage, whitelist cloud services, and maintain immutable backups to mitigate these evolving threats.

3.1. Akira

Background: Akira is a relatively new RaaS first seen in mid-2024, notable for focusing heavily on BFSI targets. It operates a dual-portal infrastructure: a public Tor "victim site" listing breaches and leaked files, and a separate Tor "comm portal" for private negotiations and affiliate management. Unlike some noisy ransomware gangs, Akira ran a lower-profile campaign, but its attacks spiked in summer 2025. Analysts note Akira borrowed tactics from LockBit-style operations, suggesting its operators may include ex-LockBit affiliates (some security blogs correlate Akira's encryption routines and ransom-note format to former LockBit 3.0 actors).

Motive: Standard financial extortion plus reputation-building. Akira encrypts or steals data to extort payment, but also seems intent on compiling a "portfolio" of high-value BFSI breaches. The group's Tor leak site showcases victims to attract affiliates and heighten pressure on each victim to pay.

Targeted BFSI Victims: Akira has struck a string of U.S. and global financial firms. On June 24, 2025 its leak site listed four new BFSI organizations in one day: three mortgage/financial services firms (Integrity Mortgage, Datrose, VS Associates) and one insurance broker (Patron Insurance Services). HookPhish reported Integrity Mortgage and Patron Insurance Services as Akira victims in June 2025. (Other tracked victims include credit unions, fintechs, and smaller banks.) In each case, Akira published sample exfiltrated data (e.g. loan records or policy information) on its site to prove the breach, then reached out via dark-web channels to negotiate ransoms.

Company Name	Discovery Date	Country
Pennant Park	2025-06-25	US
VS Associates	2025-06-24	US
Integrity Mortgage	2025-06-24	US
Access Financial	2025-06-24	-
Flagship Bank	2025-05-27	US
Patron Insurance Services	2025-06-12	US
Tufton Capital Management	2025-06-16	US

Recent Activity:

- June 24, 2025: Posted four new BFSI victims in a single day on their DLS, three mortgage/financial-services firms and one insurance broker.
- Ongoing: Weekly updates to victim roster; active negotiation threads visible in the comm portal.

Tactics, Techniques & Procedures (TTPs):

Akira's operators employ a mix of stealthy and brazen tactics. Key TTPs include:

- Selective encryption/exfiltration: Rather than crippling entire networks, Akira often encrypts only critical data stores (e.g. loan-processing databases) and exfiltrates business-critical records for maximum leverage.
- Dual Tor portals: A public leak portal (e.g. akirall2iz6…onion) is used to shame victims and host stolen files, while a separate private portal (e.g. akiralkzxz…onion) handles victim communications and affiliate recruitment.
- Ransom delivery via RDP: Akira affiliates typically deploy their ransom notes by logging into exposed RDP or administrative servers and placing text/HTML files with negotiation instructions. Victims find these notes on login, guiding them to the Tor portals.
- Affiliate-driven intrusion: Like other RaaS, Akira uses external affiliates for initial compromise. Common access vectors include stolen credentials, unpatched VPNs/ESXi servers, or phishing, after which the affiliate hands off to the core team for encryption/exfiltration.

Attribution -
Security researchers have linked Akira to a small cadre of cybercriminals that emerged from the collapse of LockBit 3.0. Multiple underground monitoring groups (e.g. LeakMonitor) have observed similarities in Akira's encryption routines and file-naming conventions to former LockBit affiliate strains. There is no public law-enforcement attribution naming individuals, but open-source tracking suggests Akira may be run by a tight-knit team formerly aligned with LockBit-like RaaS networks.

Risk Mitigation - Defending against Akira echoes general ransomware defenses. Critical steps include segmented backups and rapid patching. Maintain offline, immutable backups of databases and servers, and test recovery frequently. Require MFA on all remote-access and cloud services, and ban legacy (SMS-based) MFA methods. Proactively patch known vulnerabilities in webservers, VPNs, and virtualization platforms (e.g. VMware, ESXi) – Akira has exploited such holes in the past. Employ network segmentation (so a breach in a user zone cannot jump into core banking networks) and implement robust EDR/IDS monitoring to catch unusual RDP logins or data exfiltration patterns. Finally, train staff on phishing awareness, since initial access often begins via email. For companies negotiating with Akira, law enforcement generally advises against paying ransoms, and to report incidents immediately to authorities.

3.2. LockBit

Background
LockBit is one of the oldest and largest ransomware-as-a-service gangs, active since 2019 and responsible for many thousands of attacks. In late 2024 its developers rolled out LockBit 3.0 ("LockBit Black"), a faster, more stealthy encryptor. LockBit operates a massive affiliate program: any criminal can rent the ransomware, submit targets through LockBit's portal, and split ransoms with the core developers. The group's Tor leak site has very high traffic and lists hundreds of victims at any time. (Remarkably, in May 2025 LockBit's own infrastructure was breached and leaked by vigilantesen, but by mid-2025 the gang continued operating through mirror sites.).

Motive
Purely financial. LockBit's affiliates aim to extort big ransoms. Its standard model is double-extortion: encrypt networks and steal data, then threaten to leak the exfiltrated data if demands aren't met. LockBit has claimed responsibility for attacks on organizations of all sizes worldwide; it is often described as a "Walmart of ransomware", attacking "everyone" and generally focused on profit.

Targeted BFSI Victims

Although LockBit hits all industries, it has struck notable BFSI organizations. In 2025 it leaked data from at least three financial-sector victims: in February 2025 LockBit activists (using the handle LockBitSupp) published files claimed from the U.S. FBI's own systems(alleging exfiltration of FBI files). In April 2025 LockBit published data from AC Investment Management (acimfunds.com), a New York-based investment management firm. Also in April, LockBit published stolen records from Intelliloan, a U.S. financial services company. (These breaches appear on the LockBit leak site.) All three are finance-related organizations. In each case, LockBit shared customer/transaction records and loan files on its DLS after deadlines were missed.

Domain	Company Name	Discovery Date	Estimated Attack Date	Country
hennessyfunds.com	The Hennessy Funds	2025-05-09	2025-03-30	US
ehlers-inc.com	Ehlers, Inc.	2025-05-06	2025-04-16	US
pdcm.com	PDCM Insurance	2025-05-01	2025-04-28	US
acimfunds.com	ACIM Funds	2025-04-12	2025-03-09	LU
intelliloan.com	Intelliloan	2025-04-13	2025-04-03	US

Recent Activity

- Feb 25, 2025: Leaked compromised data from fbi.gov systems shortly after ransom deadline passed.
- Apr 23, 2025: Published ACIM Funds' customer and transaction records.
- May 9, 2025: Dumped Intelli Loan's proprietary loan-origination files.
- Tactics, Techniques & Procedures (TTPs)

LockBit 3.0 introduced a "stealth mode" that encrypts only selected file sets to evade detection by integrity-monitoring tools (rather than full-volume encryption). Affiliates still commonly gain access via vulnerable Remote Desktop (RDP) servers, exposed VPNs, or stolen credentialscisa.gov. After entry they spread laterally, harvest credentials (often with Mimikatz etc.), and then deploy the LockBit encryptor. The payload is typically delivered via scheduled tasks or command-line. LockBit's ransomware employs very fast encryption and can bypass some antivirus checks. Once encryption is done, a ransom note instructs the victim to visit LockBit's .onion negotiation portal. The group maintains a single high-availability Tor DLS which lists all victims and countdowns; if one domain is blocked, mirrors spin up within hours.

Attribution -
LockBit is attributed to a loosely-organized cybercriminal syndicate ("LockBit Team") rather than a nation. Law enforcement has indicted a few individuals (e.g. the developer "LockBitSupp"), but publicly it is simply tracked as a major criminal network. Industry analysts note that LockBit's brand was possibly founded by Russian-language criminals (though LockBit itself claimed "apolitical" and based in Netherlands. Regardless, there is no law-enforcement claim that it is state-sponsored. Its operations are monitored by US/CIS agencies; notably, in May 2025 a security breach exposed LockBit's internal chats and keys, which analysts found "really authentic", but the core crew remains at large.

Risk Mitigation -
Organizations should apply standard ransomware defenses. First, ensure offline, immutable backups of all critical systems and data – LockBit specifically instructs victims to restore backups if they cannot pay. Test restore procedures regularly. Enforce strong passwords and MFA, especially on any remote-access or admin accounts. Disable exposed RDP servers and Internet-facing admin consoles; if RDP is needed, restrict it behind VPNs with MFA. Keep all OS and applications up to date – promptly apply patches for remote-access tools (LockBit affiliates often used unpatched VPN and server flaws). Segment the network to contain breaches. Deploy comprehensive monitoring (EDR, log review) to spot the known indicators of LockBit activity (e.g. unusual Cobalt Strike beacons, high-volume file encryption). Finally, educate staff to recognize phishing and suspicious logins. The FBI/CISA warnings emphasize practicing incident response exercises and never relying solely on decryption keys(in fact, they "do not encourage paying ransom").

3.3. Cl0p

Background
Cl0p (often written "CL0P") is a long-running ransomware gang first seen in 2019 and tied to the notorious "TA505" cybercrime group. It recently became infamous for exploiting zero-day vulnerabilities in managed file-transfer (MFT) software (notably MOVEit in 2023). Unlike pure-encryption gangs, Cl0p heavily emphasizes data theft and extortion. In the first half of 2025 Cl0p continued a series of data leak campaigns, particularly impacting Indian BFSI companies. It is known for "encryption-less" extortion, often not encrypting systems at all if it can get data out quickly.

Motive

Cl0p's core goal is data extortion for profit. Attackers break in, steal sensitive information (customer records, transaction logs, etc.), and demand payment purely to prevent public release. This minimizes downtime for victims (no encryption) and accelerates payouts. Cl0p also sells or auctions stolen data if victims refuse, maximizing revenue. It reportedly earned over $75–100M from its 2023 MOVEit campaign alone

Targeted BFSI Victims

In 2025 Cl0p targeted several banking and finance organizations. Notably, its Tor leak site listed multiple Indian financial firms. Recent postings have included Indian commercial banks and finance companies (for example, government-regulated Federal Bank and Axis Bank, as well as NBFCs like Indiabulls) suffering data dumps of account and transaction records. Cl0p also hit international financial targets – for instance, security vendor Qualys (USA) was listed in early 2025 with screenshots of stolen Qualys customer info (from a breached file-transfer tool) to prove the hack. (Qualys publicly confirmed it was breached via an Accellion FTA exploit and had data exfiltrated.) In all cases Cl0p's leak site showed sample data (such as bank statements or account ledgers) and a ransom note threatening broader release.

Domain	Company Name	Discovery Date	Country
checkcity.com	CheckCity.com	2025-05-09	US
highbartrading.com	HighBar Trading	2025-02-27	-
ffl-group.com	FFL Group	2025-02-27	-
interfactura.com	Interfactura.com	2025-02-27	MX
morrisgroup.co	Morris Group	2025-02-12	CO
cassinfo.com	Cass Information Systems, Inc.	2025-02-10	CO

Recent Activity

2025 Q1–Q2: Multiple Indian BFSI institutions named on Cl0p's DLS, alongside a high-profile data dump from Qualys. Victim advisories included column-extraction samples to prove authenticity.

Tactics, Techniques & Procedures (TTPs)

Cl0p operators exploit zero-day flaws in file-transfer systems. In 2023 they used a SQL-injection in MOVEit (CVE-2023-34362) to deploy the "LEMURLOOT" web shell and steal files. Prior campaigns used zero-days in Accellion FTA (2020–21) and GoAnywhere MFT (2023). Once inside, Cl0p exfiltrates data through its C2 infrastructure but often does not deploy any ransomware payload – the victim's files remain intact. The stolen data is listed on its Tor DLS ("CL0P^_-LEAKS") with a countdown. Cl0p has a history of quadruple extortion: data theft, publication threats, plus DDoS and stakeholder harassment, but in practice the tech side is "stick a webshell, grab data, post leaks." Its toolkit includes off-the-shelf RATs (FlawedAmmyy, FlawedGrace), and it often uses highly credentialed phishing lures to gain initial access.

Attribution

Cl0p is widely attributed to the Eastern-European criminal group TA505. CISA and FBI note that Cl0p's operators are part of TA505, one of the largest phishing-and-malware syndicates globally. In fact, CISA calls Cl0p "TA505" when discussing its MOVEit campaigns. A known alias is "Graceful Spider" (per CrowdStrike). Analysts have linked Cl0p to sophisticated criminal networks with possible Russian-speaking members, but as with LockBit no intelligence agency has publicly blamed a specific country. U.S. advisories simply treat Cl0p as a top-tier ransomware gang (albeit one that often skips encryption).

Risk Mitigation

CISA/FBI have published specific guidance for Cl0p, focusing on the exploited MFT systems. Key mitigations include patching or isolating vulnerable file-transfer software (apply vendor fixes to MOVEit, Accellion, GoAnywhere, etc.). Limit exposure: if you must run MFT servers, avoid internet-facing deployments and monitor for any signs of compromise (unexpected IIS endpoints, novel web shells). In general, practice rigorous cyber hygiene: take inventory of all assets, whitelist only approved applications, and grant admin privileges sparingly. Segment the network so that even if an MFT server is breached, attackers cannot wander freely. Keep up-to-date network monitoring – log and alert on suspicious port usage and external communications. Maintain up-to-date patching and vulnerability scans. Continuously review and revoke any unknown accounts. And, as always, maintain secure offsite backups.

Security Note

Because Cl0p often publishes stolen data without warning, organizations should also consider data governance measures (e.g. encryption at rest of sensitive data, strict access controls) and be prepared for breach response even if encryption hasn't occurred. Victims should promptly involve law enforcement; FBI/CISA advisories contain IoCs for Cl0p breach campaigns.

3.4. Lazarus Group (APT38)

Background - The Lazarus Group, specifically its financially-focused subgroup APT38 (a.k.a. TraderTraitor in FBI parlance), is a North Korean state-sponsored cybercrime team that has been active since at least 2009. Operating under the DPRK's Reconnaissance General Bureau, APT38 conducts large-scale thefts from banks and cryptocurrency platforms to fund Pyongyang's nuclear and missile programs. Notoriously cunning, Lazarus employs both custom malware and human-intensive intrusion techniques.

Motive - State-directed fundraising. Lazarus's goal is to steal money (fiat or crypto) for the North Korean government's illegal weapons programs. This is espionage-motivated theft rather than personal gain. The group is sanctioned globally (OFAC designated Lazarus/ APT38 in 2019, and its cyber-heists are considered acts of economic warfare.

Targeted BFSI Victims - In 2025 APT38 scored several high-profile cryptocurrency heists. On February 21, 2025, the FBI publicly confirmed North Korean hackers stole ~$1.5 billion worth of cryptocurrency from Bybit – the largest crypto heist ever recorded. (The FBI bulletin identified "North Korea" – calling them "TraderTraitor" – as responsible for this massive breach Then on May 9, 2025, Taiwanese exchange BitoPro disclosed an $11.5 million loss to a hacker, publicly attributing it to the Lazarus Group. (BitoPro's forensic analysis found the attackers had compromised a cloud admin account and deployed crypto-stealer malware.) Both victims are crypto exchanges (BFSI-equivalent targets) handling large user funds. Lazarus has also historically hit conventional banks (SWIFT heists) and other financial infrastructure, though the 2025 incidents were all crypto-based.

Recent Activity -

- Feb 21, 2025: Conducted the largest crypto heist ever, stealing $1.5 billion from Bybit cold-to-hot wallet transfers; FBI confirmed Lazarus attribution and released 51 Ethereum addresses for sanctions blocking.
- May 9, 2025: Exploited a vulnerability in BitoPro's internal tooling to exfiltrate $11.5 million; BitoPro publicly confirmed the incident and invoked emergency forensics.

Tactics, Techniques & Procedures (TTPs) -

Lazarus uses highly targeted, multi-stage attacks. Typical elements include:

- Developer/cloud credential compromise: For Bybit, investigators reported that Lazarus hacked the exchange's developer environment and multisig wallet setup, allowing them to initiate fraudulent transactions from cold wallets. Similarly, BitoPro's breach began with social-engineering into a cloud engineer's AWS account, followed by malware that grabbed hot-wallet key. In short, they subvert the signing process for transactions.
- Custom malware and scripts: Lazarus deploys in-house tools (e.g. "FallChill" backdoors, "FastCash" trojans) tailored to financial networks. These backdoors give persistent access to exchange infrastructure.
- Layered laundering: After theft, Lazarus uses thousands of intermediate wallets and mixers to obscure the crypto trail. (The FBI even published a list of over 60 Ethereum addresses linked to the Bybit theft and urged providers to block them).
- No ransomware: Unlike the above actors, Lazarus's operations are pure theft, not extortion via encryption. There is no ransom note – they simply steal assets directly.

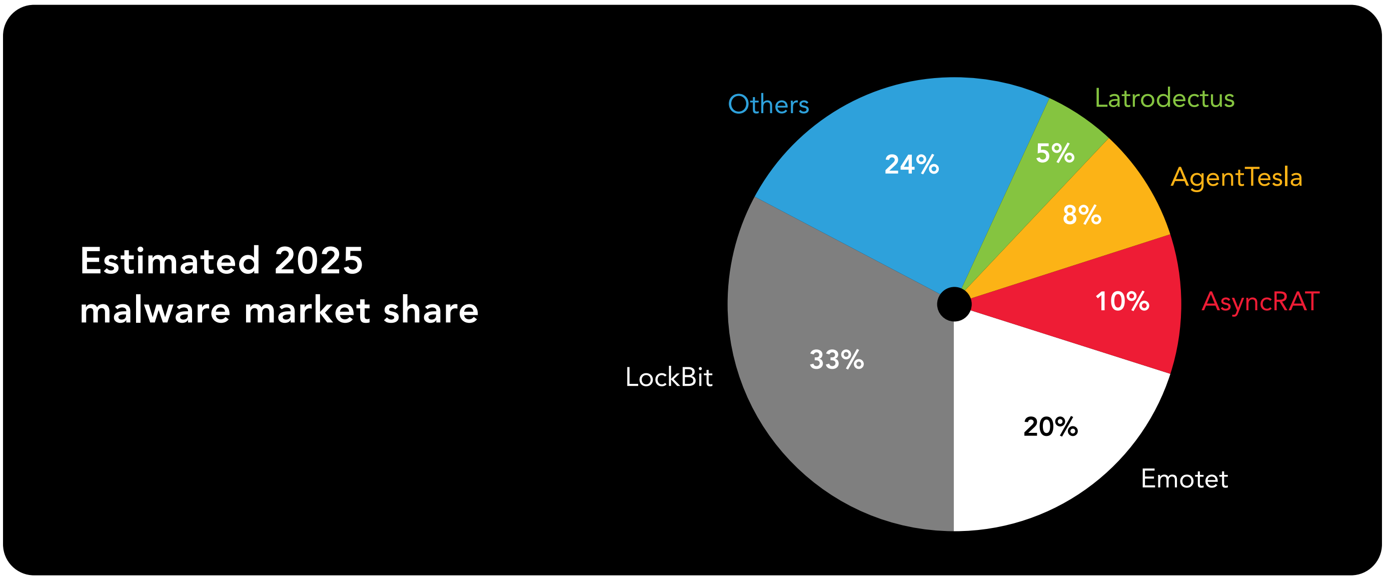
Attribution

Law enforcement unambiguously attributes these thefts to North Korea's Lazarus/APT38. The FBI's February 2025 alert explicitly names the DPRK and uses the code name TraderTraitor for this actor. Security news outlets likewise report that Lazarus was behind Bybit and BitoPro, citing FBI and independent analyses. The U.S. government long ago identified Lazarus as part of DPRK's Reconnaissance General Bureau (sanctioned as an "agency or instrumentality" of the DPRK).

Risk Mitigation

Defending against Lazarus requires both cybersecurity and financial controls:

- Protect wallet infrastructure: Enforce strict governance over cryptocurrency wallets. Use multi-signature cold wallets requiring multiple hardware keys. Keep private keys in Hardware Security Modules or physically air-gapped devices. Rotate and lock down keys after any suspected compromise.
- Harden development/devops environment: As Lazarus used stolen dev credentials in these incidents, secure the entire software development pipeline. Enforce MFA and strict access controls for all cloud accounts (e.g. AWS IAM), and regularly audit any privileged sessions. Limit third-party code and thoroughly vet any crypto software updates.
- Monitor blockchain activity: Use blockchain analytics to watch for suspicious movement of funds. The FBI has published dozens of crypto addresses linked to Lazarus thefts, exchanges and coin services should block or flag transactions involving these addresses. Proactively collaborate with regulators to trace and freeze illicit transfers.
- General security: Regularly patch and update all software, especially systems related to transactions. Employ network segmentation: isolate systems handling crypto wallet keys from general enterprise networks. Maintain comprehensive monitoring and incident response plans.
- Sanctions compliance: Ensure all financial dealings comply with international sanctions on DPRK. Report any contacts or transactions that may involve sanctioned individuals/addresses.



4.1. AsyncRAT

Behavior and Capabilities: A modular Windows remote-access trojan (RAT) first seen in 2019, now widely used in targeted campaigns. AsyncRAT is typically delivered via spear-phishing, often using obfuscated JavaScript or shortcut files. For example, recent attacks used malicious JScript (e.g. Lana_Rhoades_Photoos.js) and zipped LNK/BAT files hosted on trusted platforms (Dropbox, Cloudflare) to launch the RAT. Once running, it performs in-memory injection (e.g. into addinprocess32.exe) to evade disk detection. Its command channel often uses DNS tunneling or legitimate cloud services (e.g. Google Drive, paste.ee) for C2. AsyncRAT can exfiltrate system info, download plugins, capture screenshots, terminate processes, and update itself. It also uses WMI and nested PowerShell to bypass execution policies.

Attack Chain & Tactics: Typical chain: Initial Access via phishing (malicious script). Execution happens through script hosts (cscript/wscript) or PowerShell (T1059.001) that launch the RAT. It may create mutexes for Persistence (T1050) or use token manipulation for Privilege Escalation (T1134, e.g. enabling SeDebugPrivilege). Defense Evasion is achieved by injecting into other processes (T1055) and by masquerading as benign traffic (C2 over DNS/TLS). C2 Communication uses application-layer protocols (T1071.004) such as DNS or HTTPS channels (e.g. Google Drive URLs). Its broad toolkit maps to ATT&CK techniques like phishing (T1566), command-shell execution (T1059), injection (T1055), and DNS tunnel (T1071.004).

Tactic	Technique	MITRE ID
Initial Access	Phishing (malicious JScript)	T1566
Execution	Command-Line Interface (PowerShell, cscript)	T1059
Persistence	Create/Modify System Process (mutex)	T1050
Privilege Escalation	Access Token Manipulation (SeDebugPrivilege)	T1134
Defense Evasion	Process Injection	T1055
C2 (Command & Control)	Application Layer Protocol: DNS	T1071.004

Detection & Prevention:

- Network Rules: Block or monitor known AsyncRAT infrastructure, e.g. the IP 148.113.165.11 on port 3236 (observed in C2 traffic and domains like paste.ee used to stage payloads Inspect and block unusual DNS requests or cloud-storage URLs from endpoints.
- Endpoint Monitoring: Alert on script hosts (cscript.exe or mshta.exe) spawning PowerShell or unknown executables. Enforce PowerShell Constrained Language Mode and strict execution policies. Disable unused WMI subsystems and regularly audit for unexpected WMI/WBEM scripts.
- YARA/IOCs: Deploy YARA rules tuned for AsyncRAT payloads (e.g. known AsyncRAT function strings or loader patterns). Monitor for the creation of mutexes indicative of AsyncRAT (if known).
- User Education: Phishing awareness (e.g. don't click suspicious links/attachments) helps prevent the initial script download.

Usage & Targets:

AsyncRAT has been notably active in early 2025. It ranked #4 on Check Point’s Global Threat Index for Feb 2025. Analysts report it is especially used against IT, telecommunications, and education sectors. The malware’s use of trusted services (Dropbox, Cloudflare tunnels) makes detection challenging, so defenders should pay special attention to anomalous use of those services.

4.2. Latrodectus

Behavior and Capabilities - Latrodectus is a stealthy Windows loader/downloader first identified in late 2023. It often arrives via small downloader scripts or MSI installers (for example, a malicious MSI can spawn msiexec.exe, which then launches a hidden "NVIDIA Notification" process that loads the Latrodectus payload). Once running, it immediately self-deletes using an Alternate Data Stream (ADS) trick: the loader renames its own executable into an ADS (suffix like :wtfbbq) and schedules it for deletion via Windows APIs. This leaves little forensic trace. Latrodectus then fetches a secondary payload over HTTPS (typically on port 443) – often ransomware or an info-stealer. The loader persists by creating a registry Run key (HKCU\...\Run) to relaunch on login. Internally, Latrodectus uses string obfuscation (XOR/loops), dynamic WinAPI resolution, and sandbox checks (e.g. process count, ptrace detection) to hinder analysis.

Attack Chain & Tactics - A representative chain is: Initial Access via malicious email link or attachment that runs a JS/VBS/Msi script. Execution often involves a hidden window or script interpreter (T1059) launching msiexec or powershell to load the payload. Persistence is via the Run key (T1547.001) so it restarts at logon. Defense Evasion is shown by the ADS self-deletion (Indicator Removal T1070.006). C2 and payload download occur over standard HTTPS (non-standard ports are not really needed since 443 is standard; however, because traffic looks normal it's harder to flag). The malware's TTPs include Run key persistence, ADS deletion, and encrypted HTTP communication.

Tactic	Technique	MITRE ID
Defense Evasion	Indicator Removal on Host (ADS)	T1070
Persistence	Registry Run Keys	T1547.001
C2 Communication	Non-Standard Port (HTTPS/443)	T1571
Impact	Data Manipulation (payload download)	T1565

Detection & Prevention

- Network Filtering: Block or monitor known malicious domains and IPs used by Latrodectus affiliates (for example, agrahusrat[.]com or minrezviko[.]com have been observed). Use SSL/TLS inspection if possible to spot unusual downloads.
- Filesystem Monitoring: Alert on processes using low-level file APIs to manipulate ADS (e.g. calls to SetFileInformationByHandle with a stream name like ":wtfbbq"). Detect and log hidden-window executions where a download is immediately run.
- Registry/Startup: Monitor creation of new Run keys under HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
- YARA Rules: Use YARA signatures tailored for Latrodectus payloads or known obfuscation artifacts.
- Sandbox Evasion: Encourage use of behavior-based EDR; since Latrodectus uses sandbox checks, malicious samples might delay payload, so use longer observation windows in dynamic analysis.

Usage & Targets

Latrodectus emerged strongly in Q1 2025. It is frequently used as an initial loader for follow-on malware (ransomware, info-stealers). Reports indicate banking and corporate networks are common targets. Its stealth features (ADS deletion) make quick detection difficult, so organizations should watch for its characteristic behaviors (ADS file operations, hidden MSI executables).

4.3. Emotet

Behavior and Capabilities

Emotet is a notorious modular trojan/loader active since 2014, originally a banking trojan that evolved into a general-purpose loader. Emotet resurgence (post-2021) continues into 2025. It primarily spreads via malicious Office documents (Word or Excel) or even OneNote files. These documents contain macros or scripts that launch VBS/PowerShell payloads. For example, one variant drops a VBS (click.wsf) that runs a heavily obfuscated PowerShell to download an Emotet DLL into C:\ProgramData\*.dll, then executes it with regsvr32.exe. Once active, Emotet typically installs itself as a hidden Windows service (e.g. TnsZbP.dll) under System32, and also copies its core DLL (named like E.dll) to %AppData%\Local. It uses regsvr32.exe as a proxy (T1218.010) to sideload and execute its DLLs. Emotet deletes Zone.Identifier marks to evade SmartScreen, and often deletes volume shadow copies to prevent recovery. It uses elliptic-curve cryptography (ECDH/ECDSA) to secure C2 communications. Emotet modules can enumerate processes and network configuration, and even inject code into legitimate Windows tools (e.g. hollowing certutil.exe) to harvest credentials

Attack Chain & Tactics -
Emotet's chain is typically: Delivery via an email with an Office document (macro or script enabled) (T1566/T1204). Execution: macro drops and runs a script (VBS/WSF), which runs encoded PowerShell to fetch the Emotet payload Lateral Movement: After initial infection, Emotet may use stolen credentials or exploit SMB/RDP internally. Persistence: creates a new Windows service (T1050) and may set Run keys. Privilege Escalation/Evasion: uses regsvr32.exe (T1218.010) to run payloads invisibly, and can disable Defender or UAC if needed. Discovery: spawns systeminfo.exe and ipconfig.exe to gather host details. C2/Exfiltration: uses WinHTTP to connect to multiple hardcoded C2 servers over HTTPS (T1071). It downloads additional modules (Keylogger, banking trojans, etc.) via HTTP GET. Emotet's activities map to many ATT&CK techniques (new service T1050, hidden window T1143, process hollowing T1055.012, system/network discovery T1082/T1016, encrypted C2 T1071.001).

TTPs (MITRE ATT&CK)

Tactic	Technique	MITRE ID
Persistence	New Service	T1050
Defense Evasion	Hidden Window	T1143
Defense Evasion	Software Packing	T1045
Discovery	Process Enumeration	T1057
C2 Communication	Application Layer Protocols (HTTPS, custom ports)	T1071

Detection & Prevention -

- E-Mail Security: Filter inbound emails for malicious attachments, especially Office files with macros. Sandboxed detonation of suspicious attachments can catch the macro-initiated PowerShell.
- Blocklists: Block connections to known Emotet C2 IPs (e.g. 173.249.25.219, 212.83.184.188).
- Process Monitoring: Alert on unusual use of regsvr32.exe. For example, a Word process spawning regsvr32 /s *.tmp.dll is suspicious. Monitor for new services being created by non-privileged users.

- Execution Control: Disable or restrict use of regsvr32.exe and wscript.exe unless needed. Constrain Office macro execution policy (e.g. block or require user approval).
- YARA/Signatures: Deploy YARA rules targeting Emotet (e.g. rules looking for "EmotetFunctionStrings" used in its modules).
- Integrity Monitoring: Watch for changes to registry Run keys, hidden service DLLs, or deletion of VSS snapshots (indicative of ransomware follow-on).
- Network Monitoring: Use EDR/NDR to detect beaconing or unusual TLS connections to foreign IPs from regsvr32.exe.

Usage & Targets

Emotet remains among the most persistent loaders in 2025, rebuilding itself after takedowns. It predominantly targets financial services, government agencies, and education/healthcare. Global telemetry has shown Emotet campaigns hitting diverse industries worldwide. Its versatility (as a dropper for other payloads) makes it a widespread threat.

4.4. AgentTesla

Behavior and Capabilities

AgentTesla is a .NET-based credential-stealer RAT (also called OriginLogger) that has been continually updated through 2025. It's commonly sold on underground forums (subscription-based "MaaS"). Upon infection, it often installs itself as a Windows service and may disable User Account Control by setting the registry EnableLUA = 0 (bypassing UAC; MITRE T1088). AgentTesla hooks into processes by allocating large executable memory regions (RWX) for code injection (observed in jsc.exe or explorer.exe), allowing it to capture keystrokes and screenshots. It harvests stored credentials from browsers, email clients, FTP clients, and files (Credential Access T1081). Notably, AgentTesla uses multiple C2 channels for exfiltration: it frequently sends stolen data via SMTP (email), but also supports HTTP POST and even Telegram-based exfil. For example, a recent sample was observed sending data to finalrestingplace.net on port 587 (SMTP). Internally, AgentTesla may also gather network info (T1016) to profile the host.

Attack Chain & Tactics - Commonly distributed via phishing emails with malicious attachments (often malicious executables or PDFs). When run, it may drop files and modify the registry for persistence. Execution: the service or injected process runs AgentTesla's payload (T1059). Persistence: often via a new Windows service entry. Defense Evasion: bypasses UAC (T1088) and may elevate privileges (T1087). Discovery: performs local network and system enumeration (T1016). Credential Access: scans browser data and files for passwords (T1555.003/ T1081). Exfiltration: uses one-way outbound channels like SMTP, FTP, HTTP POST, or even encrypted messaging APIs (T1041). Because the data is typically exfiltrated to legitimate servers (e.g. mail providers or Telegram APIs), network defenders must rely on content inspection or detection of the AgentTesla message formats.

TTPs (MITRE ATT&CK)

Tactic	Technique	MITRE ID
Defense Evasion	Bypass UAC via Registry	T1088
Privilege Escalation	Enable Process Privileges	T1087
Discovery	Network Configuration Discovery	T1016
Credential Access	Credentials in Files	T1081
Execution	Windows Management Instrumentation	T1047

Detection & Prevention -

- Network Monitoring: Block/monitor outbound SMTP on unusual mail servers. For example, block traffic to finalrestingplace.net (108.179.232.90:587), a known AgentTesla SMTP host. Use Zeek/Suricata rules to look for AgentTesla-specific email patterns (Corelight's blog shows regex for its SMTP format). For HTTP, search for unusual POST to "*.php" endpoints carrying base64-encoded payloads. For Telegram C2, it is very hard to distinguish from normal Telegram SSL traffic, but monitoring for large encrypted uploads to Telegram might help.
- Registry/OS: Alert on changes to HKLM\...EnableLUA or similar UAC settings. Watch for creation of new services by non-standard processes.

- Memory/Process: Detect large RWX allocations or injector behavior in processes like jsc.exe or script hosts. Monitor for known AgentTesla strings (e.g. SMTP banner patterns) in memory.
- YARA Rules: Deploy YARA rules for AgentTesla signatures (many variants share core code).
- Email Gateway: As with others, block or sandbox suspicious attachments and disable macros/scripting where possible.
- Password Hygiene: Since AgentTesla targets credentials, enforce strong credential policies and use MFA to reduce impact.

Usage & Targets -
AgentTesla remains a daily active stealer in 2025. It's been found in campaigns against organizations of all sizes. Sector-wise, it often hits healthcare, manufacturing, and retail entities (where stolen creds and internal data are valuable). A Bitsight study notes that AgentTesla is prevalent worldwide and mainly spreads by email attachments. Its modular builder and frequent updates mean defenders must stay vigilant to new variants.

4.5. LockBit

Behavior and Capabilities: LockBit is a leading ransomware-as-a-service (RaaS) that first appeared as "ABCD" in Sept 2019 and rebranded to LockBit in 2020. It has since evolved (LockBit 2.0, 3.0/Black, 4.0, etc.) and remains highly prolific. LockBit's payload encrypts files system-wide with strong crypto (AES/RSA), appending randomized extensions (e.g. .wxacdzitl) to encrypted files. Upon execution, LockBit often replaces the desktop wallpaper and drops ransom notes (e.g. restore-my-files.txt). It aggressively deletes backups by wiping volume shadow copies (VSS) on Windows (Inhibit System Recovery, ATT&CK T1490). To spread in a network, affiliates frequently use stolen admin credentials and tools like Cobalt Strike to move laterally (ATT&CK T1021.002). LockBit's affiliates will often inject into explorer.exe or svchost.exe to locate and encrypt network shares. It also typically attempts to disable security software (e.g. forcibly terminating or uninstalling Windows Defender)

Attack Chain & Tactics: The chain may begin with phishing or exploiting a public-facing system to gain Initial Access. Privilege Escalation: stolen credentials grant domain admin rights. Discovery: scanning for file servers and drives (T1135) to maximize encryption. Lateral Movement: via SMB/Remote Services (T1021.002) as noted. Defense Evasion: stops security services, and obfuscates file names by random extensions (T1027). Impact: heavy data encryption (T1486) on local and mapped drives, effectively a ransomware wiper when combined with shadow-copy deletion (T1490). Unlike pure wipers, LockBit typically also exfiltrates data for double-extortion.

TTPs (MITRE ATT&CK)

Tactic	Technique	MITRE ID
Impact	Data Encryption	T1486
Discovery	Network Share Discovery	T1135
Defense Evasion	File Obfuscation (random extensions)	T1027
Credential Access	Credentials in Files	T1081

Detection & Prevention -

- File Monitoring: Look for sudden mass file changes or the appearance of novel extensions (e.g. many files renamed to *.wxacdzitl). Alert on large-volume file writes or encryption patterns.
- EDR/Process: Detect the characteristic process injection into explorer.exe/svchost.exe (LockBit often runs inside these processes) and scanning of network shares. Monitor for high CPU or file I/O on these processes.
- Service & VSS Monitoring: Watch for VSSAdmin commands deleting shadows. Alert if volume snapshot services stop.
- Access Controls: Strictly limit domain admin and service account privileges (principle of least privilege). Use dedicated jump servers for admin tasks. Network segmentation to prevent easy SMB lateral spread. Disable legacy protocols (SMBv1) and block SMB traffic where not needed.
- Backups: Maintain offline, immutable backups. Since LockBit removes online backups, offline copies are critical.
- Incident Response: If ransomware is detected (rapid encryption), isolate the affected system immediately.
- Awareness: Train users to avoid phishing and ensure timely patching of external systems (many LockBit infiltrations began with known exploits).

Usage & Targets -

LockBit has been the single most active ransomware group globally. In 2022 it was responsible for ≈50% of all ransomware incidents observed (often quoted as ~44%). It continues to dominate in 2025. The group targets healthcare and critical infrastructure prominently, as well as financial services, manufacturing, and government organizations. (LockBit's own rules even forbid attacks on critical power and post-Soviet countries.) Because of its scale and affiliate model, LockBit will remain a top threat into 2025.

4.6. Prilex POS Malware Variant

Description: A Brazilian-origin POS malware family, Prilex, has evolved to perform "ghost transactions." The installer (GB.exe) deploys multiple executables and scheduled tasks, registers malicious DLLs, and later injects into POS software to intercept live card transaction data. Upon detecting a transaction, it requests a fresh ARQC from the victim's card, captures PAN/CVV/expiry, then exfiltrates via HTTP to dynamic-DNS domains (amazoncrime-001-site1.htempurl[.]com).

Why It Matters

- Ghost transactions use legitimate cryptograms, evading authorization anomalies
- Physical installer vectors (social-engineered "POS update") bypass remote defense

Recommendations

- File Integrity Monitoring: Alert on unexpected new task-scheduler entries or suspicious DLL registrations
- Network Egress Controls: Block HTTP/S to known dynamic-DNS providers
- Script/Batch-File Auditing: Investigate VBS and BAT files creating persistence under %TEMP%

Latest Signatures / IoCs:

- File: GB.exe (v06.03.8080)
- AV Detection Name: HEUR:Trojan.Win32/64.Prilex
- C2 Domain: amazoncrime-001-site1.htempurl[.]com
- NFC Block String: "Contactless error, insert your card"

4.7. Cogui Phishing Kit

Description: Cogui is a Phishing-as-a-Service offering that sent over 580 million phishing emails between January and April 2025. It provides turnkey phishing kits, email templates, and a dashboard parsing campaign emails. The operation primarily targets Japan but also affects the United States, Canada, Australia, and New Zealand. Clients purchase access on Telegram, send phishing lures to targeted domains (email providers, banks), and harvest credentials for resale or immediate fraud.

Why It Matters

- Lowers operational barrier: no coding needed for large-scale credential theft
- Real-time dashboarding accelerates campaign optimization
- Volume represents the highest phishing campaign currently tracked by major security firms

05 Top 5 Vulnerabilities of 2025

Major new vulnerabilities discovered in early 2025 have been rapidly weaponized by attackers. Notably, an unauthenticated stack overflow in Ivanti Connect Secure (CVE-2025-22457) and a zero-day in Chrome's V8 engine (CVE-2025-5419) were both exploited in the wild. This report highlights five CVEs (January–July 2025) that were most frequently observed across threat intelligence sources and added to CISA's Known Exploited Vulnerabilities (KEV) catalog. Key risks include remote code execution bugs in enterprise appliances, browser engines, and deserialization flaws, as well as a security-bypass in a popular archiver. Immediate patching of affected products is strongly recommended to counter active attacks.

- Remote RCE in enterprise VPN/gateway appliances: Ivanti Connect Secure/Policy Secure/ZTA appliances have a critical stack-based overflow (CVE-2025-22457) allowing unauthenticated RCE.
- Chrome/Chromium sandbox escapes: Two critical Chrome flaws (CVE-2025-2783, CVE-2025-5419) enable remote code execution via malformed files or web content. These high-severity zero-days were actively exploited (e.g. by the "TaxOff" group) before patches were issued.
- SAP NetWeaver deserialization: A flaw in the Visual Composer uploader (CVE-2025-42999, CVSS 9.1) lets privileged users trigger deserialization and RCE on NetWeaver hosts. Onapsis reported it being chained with another SAP bug and abused in the wild.
- Trusted tool bypass (Mark-of-Web): 7-Zip's MotW protection was defeated (CVE-2025-0411) so that malicious archives run code without warnings. Attackers used this in phishing campaigns (e.g. delivering SmokeLoader malware via spear-phish) to stealthily execute malware.

CVSS Vector Key

- AV (Attack Vector): N = Network
- AC (Attack Complexity): L = Low
- PR (Privileges Required): N = None
- UI (User Interaction): R = Required
- S (Scope): U = Unchanged
- C (Confidentiality): L = Low
- I (Integrity): N = None
- A (Availability): N = None

Rank	CVE ID	Date Added	Affected Product	Brief Description
01	CVE-2025-22457	2025-04-04	Ivanti Connect Secure, Policy Secure, ZTA Gateways	Stack-based buffer overflow allowing unauthenticated RCE (remote code execution).
02	CVE-2025-2783	2025-03-27	Google Chrome (Mojo sandbox on Windows)	Sandbox escape via bad handle in Mojo (Chrome <134.0.6998.177) enabling remote code execution.
03	CVE-2025-5419	2025-06-05	Google Chrome/Edge (V8 JavaScript engine)	Out-of-bounds read/write in V8 (Chrome <137.0.7151.68) leading to heap corruption and RCE.
04	CVE-2025-42999	2025-05-15	SAP NetWeaver Visual Composer Metadata Uploader	Insecure deserialization (privileged user) enabling RCE on NetWeaver hosts.
05	CVE-2025-0411	2025-02-06	7-Zip	Mark-of-the-Web bypass (archive handling flaw) allowing execution of malicious files.

5.1. CVE-2025-22457

- About: A stack-based buffer overflow in Ivanti Connect Secure (<22.7R2.6), Policy Secure (<22.7R1.4) and ZTA Gateways (<22.8R2.2) permits remote, unauthenticated attackers to execute arbitrary code. This critical flaw (CVSS 9.8) was quickly exploited in the wild (Google/Mandiant ties it to China-linked actors). It was added to CISA's KEV on April 4, 2025.
- Risk Score: NVD 9.8 (Critical); Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.
- Exploit Status: Yes – active exploitation observed (CISA KEV, Mandiant). Full root RCE PoC was later demonstrated.
- Recommendation: Patch immediately. Upgrade Ivanti Connect Secure to 22.7R2.6, Policy Secure to 22.7R1.4, and ZTA Gateways to 22.8R2.2. CISA advises applying these patches by the April 11, 2025 KEV deadline and performing threat-hunting on any unpatched devices.

5.2. CVE-2025-2783

- About: A Chromium Mojo sandbox escape in Google Chrome on Windows (fixed in Chrome 134.0.6998.177) allows remote attackers to escape the browser sandbox via a crafted filen. The flaw arises from an incorrect handle being provided to Mojo, leading to privilege escalation. It was a zero-day exploited by the TaxOff group in March 2025 to deploy the Trinper backdoor. CISA added it to KEV on March 27, 2025 (due April 17).
- Risk Score: CVSS 8.3 (High).
- Exploit Status: Yes – used in active attacks (phishing>exploit chain) by APT (TaxOff).
- Recommendation: Update to Chrome/Chromium 134.0.6998.177 or later immediately (patch was released March 25, 2025). Until patching, avoid loading untrusted files and employ rigorous email/URL filtering to block the exploit.

5.3. CVE-2025-5419

- About: A critical out-of-bounds read/write flaw in Chrome's V8 JavaScript engine (affecting Chrome/Edge before 137.0.7151.68) enables remote heap corruption and code execution via a malicious web page. Google issued an emergency patch on June 5, 2025. This high-severity (CVSS 8.8) zero-day was actively weaponized in the wild. CISA's KEV lists it on June 5 (due June 26).
- Risk Score: CVSS 8.8 (High).
- Exploit Status: Yes – publicly confirmed in-the-wild exploitation (added to KEV). A public PoC also exists.
- Recommendation: Upgrade Chrome/Edge to version 137.0.7151.68 (or later) by June 26, 2025. As an interim measure, restrict untrusted HTML content or enforce strict Content Security Policies to mitigate exploitation.

5.4. CVE-2025-42999

- About: An insecure deserialization bug in SAP NetWeaver Visual Composer Metadata Uploader (fixed by SAP Security Note 3604119 on May 13, 2025) can be abused by a privileged user to execute arbitrary code on NetWeaver servers. This flaw (CVSS 9.1) was observed chained with another SAP zero-day (CVE-2025-31324) to give attackers unauthenticated RCE capability. CISA added CVE-2025-42999 to the KEV on May 15, 2025 (due June 5).
- Risk Score: CVSS 9.1 (Critical).
- Exploit Status: Yes – actively exploited (confirmed by CISA/Onapsis; used by ransomware/APT).
- Recommendation: Apply SAP Security Note 3604119 immediately to patch the deserialization flaw. Also review Visual Composer usage: disable it if not needed or restrict uploads to trusted administrators to reduce attack surface

5.5. CVE-2025-0411

- About: A "Mark-of-the-Web" bypass in 7-Zip (patched in version 24.09) fails to tag extracted files as untrusted. When a user opens a specially crafted archive, the extracted files execute as if coming from a trusted source. This allows malicious scripts or executables to run without warning, facilitating arbitrary code execution. Attackers have leveraged this in phishing campaigns (using Spoofed filenames) to deliver malware (e.g. SmokeLoader, ransomware). CISA added it to KEV on Feb 6, 2025 (due Feb 27).
- Risk Score: CVSS 7.0 (High).
- Exploit Status: Yes – actively exploited. Firms reported Spear-phish attachments exploiting this flaw to deploy malware without user suspicion.
- Recommendation: Update 7-Zip to v24.09 or later immediately (fix issued Feb 7, 2025). As a workaround, disable automatic MotW file extraction or enforce archive scanning via endpoint protections to block malicious archives.

Recommendations

- Universal 2FA: Wherever possible, enforce FIDO2/WebAuthn over SMS-based OTPs
- Email Authentication: Strict DMARC, DKIM, SPF enforcement at the domain level
- Phishing-Simulation Training: Regularly unannounced tests to reinforce user skepticism

5. Conclusion

The 2025 threat landscape makes clear that cyber resilience in the BFSI sector hinges on three pillars: rapid vulnerability response, layered defense, and collaborative intelligence sharing. As adversaries exploit everything from POS malware and phishing-as-a-service to zero-day flaws in widely used appliances and applications, organizations can no longer afford patch backlogs or siloed security teams. Proactive patch management, applying fixes for Ivanti, Chrome/Edge, SAP NetWeaver, 7-Zip and similar software within CISA's KEV timeframes, must be institutionalized alongside multi-factor authentication, network segmentation, immutable backups, and robust incident response playbooks. Only by marrying relentless vulnerability hygiene with threat-informed detection and cross-sector cooperation can financial institutions withstand the sophisticated, fast-moving attacks that define today's digital battlefield.

References

- https://www.trmlabs.com/resources/blog/lockbit-leak-provides-insight-into-raas-enterprise
- https://icoholder.com/en/news/crypto-heist-lazarus-group-steals-1-4b-from-bybit
- Victoria's Secret Security Incident Shuts Down Lingerie Giant's Systems - CPO Magazine
- https://threatprotect.qualys.com/2025/03/26/google-chrome-zero-day-vulnerability-exploited-in-the-wild-cve-2025-2783/
- https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/cve-2025-5419-out-bounds-readwrite-vulnerability-v8
- https://www.dbtsupport.com/2025/05/15/sap-netweaver-zero-day-cve-2025-31324-42999-exploited/
- M&S cyber attack: What we know about it and its impact
- https://www.cvedetails.com/cve/CVE-2025-5419/
- https://nvd.nist.gov/vuln/detail/CVE-2025-22457
- https://onapsis.com/blog/active-exploitation-of-sap-vulnerability-cve-2025-31324/
- https://cybelangel.com/banking-cybercrime-2025/
- https://www.techtarget.com/searchSecurity/news/366619872/FBI-Lazarus-Group-behind-15-billion-ByBit-heist
- https://www.quorumcyber.com/threat-intelligence/critical-chrome-zero-day-vulnerability-cve-2025-2783/
- https://cymulate.com/blog/akira-ransomware/
- https://www.picussecurity.com/resource/blog/akira-ransomware-analysis-simulation-and-mitigation-cisa-alert-aa24-109a
- https://cyberint.com/blog/dark-web/cl0p-ransomware/
- https://cybersecuritynews.com/cl0p-ransomware-attacking-telecommunications/
- https://gbhackers.com/cl0p-ransomware-launches-large-scale-attacks/
- https://foresiet.com/blog/cl0p-ransomwares-reign-of-cyber-extortion-analyzing-the-recent-cleo-software-exploits
- https://www.s-rminform.com/cyber-intelligence-briefing/cyber-intelligence-briefing-21-march-2025
- https://gbhackers.com/akira-ransomware-dominates-january-2025/
- https://icoholder.com/en/news/lazarus-hack-targets-bybit-stealing-1-4-billion-in-crypto
- https://coinmarketcap.com/academy/article/bybit-ceo-declares-war-on-lazarus-group-and-launches-dollar140-million-bounty-after-dollar14-billion-hack
- https://www.webasha.com/blog/unmasking-akira-the-global-impact-of-rising-cyber-threat
- https://www.linkedin.com/pulse/lockbit-ransomware-gang-announces-comeback-40-set-launch-amul-patel-n1uze

- https://en.wikipedia.org/wiki/LockBit
- https://www.bitcoininsider.org/article/268839/lazarus-group-heist-north-korean-hackers-steal-14b-bybit-exchange
- https://ubuntu.com/security/CVE-2025-0411
- https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/cve-2025-2783-google-chrome-sandbox-escape
- https://threatprotect.qualys.com/2025/06/03/google-fixes-third-zero-day-vulnerability-in-chrome-cve-2025-5419/
- https://www.rapid7.com/blog/post/2025/04/03/etr-ivanti-connect-secure-cve-2025-22457-exploited-in-the-wild/
- https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457
- https://www.cisecurity.org/advisory/a-vulnerability-in-google-chrome-could-allow-for-arbitrary-code-execution_2025-031
- https://arcticwolf.com/resources/blog/follow-up-cve-2025-42999/
- https://www.acaglobal.com/industry-insights/urgent-patching-required-address-7-zip-mark-web-bypass-vulnerability/
- https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/43999109/85e4cd3d-1034-417f-be87-3d45f5a230b0/paste.txt
- https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/43999109/7e1058d9-ed8d-4893-a43f-183ad3e5fb94/paste.txt
- https://en.wikipedia.org/wiki/Akira_(ransomware)
- https://gbhackers.com/cl0p-ransomwares-exfiltration-process-exposes-rce-vulnerability/
- https://fieldeffect.com/blog/second-zero-day-in-sap-netweaver-actively-exploited
- https://digital.nhs.uk/cyber-alerts/2025/cc-4610
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-5419
- May 28 2025 Exploit Post-Mortem - Cork
- https://www.reuters.com/business/insurer-aflac-discloses-cybersecurity-incident-2025-06-20/
- https://www.hipaajournal.com/erie-insurance-cyberattack/
- https://www.msdlegal.com/blog/2025/06/philadelphia-insurance-companies-cyberattack-class-action-investigation/
- https://www.insurancejournal.com/news/east/2025/07/02/830032.htm
- https://news.trendmicro.com/2025/06/21/aflac-data-breach/
- https://www.hindustantimes.com/cities/pune-news/fir-in-connection-with-fake-shaneshwar-devasthan-apps-duping-devotees-101752518765805.html
- https://www.businessinsider.com/return-fraud-amazon-shipping-retail-theft-wardrobing-online-shopping-2025-7
- Mastercard, VISA and American Express

SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and correctivecybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance

Payment Data Security

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance
- SWIFT

Strategy and Risk

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security
- HITRUST

Unified Audits

Managed Compliance

Security Testing

Application Security

- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Security Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Firewall Rule Review
- PCI ASV Scan

Phishing Simulation

Red Teaming Exercise

- Layer Security Testing

Cyber Defense

Managed Extended Detection and Response Solution - SISA ProACT

- 24x7 Monitoring
- UEBA
- Threat Intel
- Advanced Threat Hunting
- Breach & Attack Simulation
- SOAR
- Use-case Factory

Digital Forensics and Incident Response

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation
- Ransomware Simulation

Data Protection & Governance

Data Discovery and Classification

- PCI/PII/PHI Data Discovery
- Data Classification in Endpoint (Windows, Linux)
- Data Classification in O365, Metadata
- Dynamic Masking, Redact, Truncation
- Integration to DRM, DLP, SIEM

Data Privacy Professional Services

- Assessments (Unified Privacy Maturity, DPIA, 3rd Party Risk)
- Data Inventory, Mapping and Process flow, RoPA
- Data Privacy Framework - Policy, Notice, SoPs
- Consent and Notice Management framework
- Data Breach and Management
- Principal management
- Privacy by Design implementation guide
- Define Data Retention Guidelines and processes
- Technical/Organization measures
- Privacy Training/Awareness

Trainings & Certifications

Payment Data Security Training and ANSI Accredited Certification

- CPISI (2 Day Program
- CPISI (3 Day Program)
- CPISI- Advanced (3 Day Program)
- CPISI-D (Developers)
- CPISI Hybrid (4 Weeks)

Certification Program in Cybersecurity for AI – CSPAI

- CSPAI
- CSPAI - Developers

Forensic Briefing Sessions for Senior Management

Leading Tech Security

AI PRISM

- AI PRISM LLM Vulnerability Scanner Solution
- AI Risk Management and Governance Solution Framework
- AI Compliance and Governance Consulting Service

Hardware and IoT Security Testing

- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing
- MPOC/ PCI PTS

Quantum Security

- Quantum Cryptographic Consulting
- Quantum Security Risk Assessment
- Quantum Security Standards Compliance

For more Information visit us at www.sisainfosec.com
or
write to us at contact@sisainfosec.com

Follow us