FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 3 March 2025 | Issue 272

This report elevates this week's top risks to assist community institution information security and technology teams in proactively protecting their financial institution from dangers that can impair their ability to operate and avoid compliance, economic, legal, regulatory, and reputational impact.

This Week's Threats

Fraud Campaigns

- Account takeover (web)
- Business Email Compromise

System Vulnerabilities

Amazon, Android, Apache, CA Database, Debian, Dell, F5, Google. HP, IBM, Lenovo, Microsoft, Mozilla, Oracle, PAN-OS, Red Hat, Samsung, SUSE, Ubuntu, VMware, and Wireshark.

Themed Phishing and Smishing Campaigns

Please see the Phishing Daily Digest for all activities. Use keywords for AV blacklists.

Subject Keywords: Amazon, Available, Contract Termination, Fake CAPTCHA, Change Direct Deposit, Gift Card, HR Notification, Important Request, Job Opportunity, MyJCB, NAUPA (National Association of Unclaimed Property Administrators), Quick Check-In & Collaborative Request, Quick Task That Requires Attention, Request, Request for Assistance with Task, SAP Concur, and SARS LETTER OF DEMAND.

Threats, Malware, Cyber Campaigns, and Adversaries

- Astaroth
- AsyncRAT
- BeaverTail (InvisibleFerret)
- BitB
- BLACKWIDOW (aka Lotus)
- Bumblebee (aka ShellSting, Shindig)
- CellikRAT V4.0 Malware
- ClickFix/ClearFake
- CodeTail malware
- ConnectWise RAT
- Credential Pharming
- EvilGinx
- Fake Captcha
- Grandoreiro
- JavaGhost phishing campaign
- Latrodectus
- LandUpdate808
- LummaStealer
- MetaStealer
- Mispadu
- Nitrogen
- Safeplay Ransomware
- SocGholish
- SocksShell (aka Zapcat Supper)
- Social Engineering Attack via Microsoft Teams Impersonating IT
- SparkRAT
- SystemBC malware
- Typosquatting
- Umbral Stealer
- VenomRAT
- Xloader
- Xworm
- Zloader

NEWS AND RISK INFORMATION

Black Basta and Cactus ransomware groups add BackConnect malware to their arsenal. “Once infiltrated, [BackConnect] grants attackers a wide range of remote control capabilities, allowing them to execute commands on the infected machine. This enables them to steal sensitive data, such as login credentials, financial information, and personal files.” (Trend Micro)

Critical LDAP injection flaw in IBM TXSeries for Multiplatforms. “The vulnerability, identified as CVE-2022-46337, carries a CVSS score of 9.1, indicating its critical severity … This flaw could allow a remote attacker to bypass security restrictions by sending a specially crafted request.” (Cybersecurity News)

EncryptHub deploys ransomware and stealer via trojanized apps, PPI services, and phishing. "The financially motivated threat actor known as EncryptHub has been observed orchestrating sophisticated phishing campaigns to deploy information stealers and ransomware, while also working on a new product called EncryptRAT. Outpost24 KrakenLabs said the threat actor as (sic) a hacking group that makes operational security errors and as someone who incorporates exploits for popular security flaws into their attack campaigns." (Hacker News)

Fake CAPTCHA PDFs spread Lumma Stealer via Webflow, GoDaddy, and other domains. “Cybersecurity researchers have uncovered a widespread phishing campaign that uses fake CAPTCHA images shared via PDF documents hosted on Webflow's content delivery network (CDN) to deliver the Lumma stealer malware.” (Hacker News)

Hackers hijack 16 Google Chrome extensions for fraud. “These extensions were injected with obfuscated scripts designed to steal data, modify HTTP requests, and inject unauthorized advertisements.” (Cyber Express)

New PayPal scam tricks users with convincing ads and pages. “The scammers create ads that impersonate PayPal, often using hacked advertiser accounts. They exploit PayPal’s “no-code checkout” feature, designed for merchants to accept payments online or in person without needing a developer or coding knowledge.” (Security Online)

NYDFS updates regulated firms on upcoming cyber requirements. “Financial firms doing business in New York should be mindful of a recent e-blast sent by the state’s financial regulator concerning cybersecurity requirements that become effective in less than two months. The New York Department of Financial Services (DFS), in a “Cybersecurity Regulation Updates and Reminders” e-blast on Feb. 27, 2025, discusses annual compliance requirements under DFS’ cybersecurity regulation, 23 NYCRR Part 500 (Part 500), and alerts covered entities to new requirements under Part 500 taking effect on May 1, 2025, including requirements relating to access management, vulnerability management and protections against malicious code.” (JD Supra)

Over 49,000 misconfigured building access systems exposed online. “Researchers discovered 49,000 misconfigured and exposed Access Management Systems (AMS) across multiple industries and countries, which could compromise privacy and physical security in critical sectors.” (Bleeping Computer)

Ransomware attacks appear to keep surging. “Cybersecurity firm NCC Group counted 590 new victims in January, a 3% bump from the previous, also record-setting month. Threat-intelligence firm Cyble counted 518 newly disclosed victims in January, rising to 599 for the first 27 days of February, of which two-thirds targeted U.S.-based organizations. Other ransomware monitors also tracked increases in the overall quantity of victims over the past two months.” (Data Breach Today)

THREATS OF THE WEEK

Credential stuffing, DDoS attacks and threats against CEOs highlight this week’s risk.

Persistent Credential-Stuffing Attacks

Summary

FS-ISAC members reported persistent credential-stuffing attacks while Distributed Denial of Service (DDoS) attacks also continue.

Credential stuffing is a cyber attack method in which attackers use lists of compromised user credentials to obtain access to other systems and confidential information. Persistent, long-term attacks on a network or system are dangerous because they allow an threat actor to maintain access into a system even after disruptions.

Risk

The re-use of passwords across domains increases the potential for credential-stuffing attacks. The risks are significant — unauthorized access to sensitive data, account takeovers, financial losses due to fraudulent transactions, reputational damage to the organization, and potential legal consequences.

Remediation

To prevent unauthorized access, institutions should require:

- **Multi-factor authentication (MFA)** — multiple forms of identification to log in to an account
- **Strong, unique passwords** — different passwords for every account using a combination of uppercase and lowercase letters, numbers, and special characters
- **Regular password changes** — reminders or password management tools make this process easier
- **Rate limiting —** restricts the number of requests that a client can make to a server in a given time period
- **Tracking login success ratio** — a low login success ratio can indicate a credential stuffing attack
- **Web application firewall** — identifies and blocks access requests from known attackers
- **Education about security awareness** — to make users aware of the importance of protecting their personal information

Renewed CEO Threats

Summary

On 21 February, a gunman fired several bullets into the Lake Oswego, Oregon, home of Chip Terhune, CEO of State Accident Insurance Fund Corporation (SAIF). Terhune later announced that an individual claiming responsibility for the shooting had threatened other employees. None are known to have been endangered yet, and no arrests have been made.

Members responsible for the physical protection of institutional leaders and the institution's stability should begin assessing the tiered levels of enhanced security. Does your institution have:

- An executive protection program?
- Ransom fund?
- A process to scan emails for threats?

Thinking of the worst-case scenarios to prepare for extreme events is advisable.

THREAT INTELLIGENCE UPDATE

BianLian Ransomware Group

Unorthodox campaign casts doubt on attack legitimacy.

Summary

This week, FS-ISAC CyberIntel members are sharing intelligence regarding extortion attempts purported to be made by the BianLian ransomware group.

The victims say a letter was mailed to them stating that their corporate IT network had been compromised, and that sensitive data had been stolen. According to GuidePoint Security, victims were told that the stolen data would be leaked 10 days after receipt of the letter unless a ransom — demands have ranged from $250,000 to $350,000 USD — was paid. The letters include a Tor link to BianLian's data leak site.

The messages were delivered through the US Post Office, stamped with an American flag Forever stamp, and the return address is BIANLIAN GROUP, 24 FEDERAL ST, SUITE 100, BOSTON, MA 02110. Each envelope was marked "TIME SENSITIVE READ IMMEDIATELY."

Assessment

GuidePoint assesses, with a high level of confidence, that the extortion demands do not originate from the BianLian ransomware group. GuidePoint bases its rationale on multiple factors:

- The ransom demand is communicated via the postal service, unlike prior campaigns.
- The writer uses longer, more complex sentences and nearly perfect English. That is inconsistent with ransom notes observed from BianLian in the past.
- No contact information is provided in the letter — threat groups usually want to discuss their extortion threats with victims — and the content is unlike prior BianLian threats.
- The Bitcoin wallet addresses are all new and not connected with any known ransomware group, hiding the extortionist's identity and affiliation.

Remediation

Institutions that receive such letters should:

- Ensure their data is properly backed up, recoverable, and encrypted for additional security.
- Review their ransomware incident response plans.
- Notify executives of the existence of this threat.
- Tell employees what to do if they receive a ransom threat, whether it seems legitimate or not.
- Decide in advance how to respond to a ransomware threat.
- Share what you see with other FS-ISAC members.
- Report ransomware threats and incidents to your FBI field office and ic3.gov.

JUST FOR COMMUNITY INSTITUTIONS

FS-ISAC CIAC Video Channel Now Available

Summary

Monthly meeting and special webinar events are now available for CIAC members in FS-ISAC Video. These webinars are classified TLP Amber.

FRAUD UPDATE

ATM and Branch New Account Fraud BOLO

Summary

An FS-ISAC member reports new account openings for a potential money laundering scheme.

Tactics, Techniques, and Procedures Used

Fraud actors are reportedly opening multiple business accounts in New York and New Jersey using the same Chinese passport ID, making ATM cash deposits of $10,000 or less. Additionally, fraud actors are opening accounts using Cash App transactions ranging from $10,000 to $30,000.

After opening the accounts, fraudsters deposit large amounts of cash — hundreds of thousands of dollars — in automated teller machines (ATMs). Within days, sometimes the same day, the threat actors withdraw funds via cashier's check in a branch location.

Action to be Taken

- Scan for new accounts opened with Chinese passports that show no activity, then an influx of cash deposits of $10,000 or more through the ATM.
- Inform new account officers and ATM tellers about this fraud tactic and how to report similar activity to the appropriate internal department for investigation.
- Reconcile deposit activity promptly and look for deposit amounts like those noted above.
- Adhere to Suspicious Activity Reporting requirements.

GOVERNMENT AND REGULATORY NEWS

Enforcement of Corporate Transparency Act Suspended, FDIC and NCUA Rule Changes

Summary

The Treasury Department announced that it will not enforce the Corporate Transparency Act, nor any penalties or fines associated with the beneficial ownership information reporting rule under the existing regulatory deadlines, nor any penalties or fines against US citizens or domestic reporting companies or their beneficial owners after the forthcoming rule changes take effect.

FDIC Board of Directors Withdraws Four Outstanding Proposed Rules

Summary

The Federal Deposit Insurance Corporation’s (FDIC) Board of Directors approved the withdrawal of three outstanding proposed rules relating to brokered deposits, corporate governance, and the Change in Bank Control Act (CBCA). The FDIC is also withdrawing authority for staff to publish a proposed rule related to incentive-based compensation arrangements in the *Federal Register*.

View the entire press release.

Compliance Date Extension Amendments to FDIC Official Signs and Advertising Requirements

Summary

The FDIC is postponing the compliance date from 1 May 2025 to 1 March 2026 for the requirements under 12 CFR 328.5 related to the display of the FDIC official digital sign on an insured depository institution’s (IDI) digital channels, as well as analogous requirements related to IDIs’ ATMs and like devices under 12 CFR 328.4. This delay will allow the FDIC to propose changes to the regulation for public comment to address implementation concerns and potential sources of confusion.

View the entire press release.

FDIC Statement of Policy on Bank Merger Transactions

Summary

The FDIC is proposing to rescind the Statement of Policy on Bank Merger Transactions published in 2024 and reinstate its prior Statement of Policy on Bank Merger Transactions, which was in effect before the 2024 Statement.

View the entire press release.

NCUA Overdraft/NSF Fee Collection Announcement

Summary

The National Credit Union Administration (NCUA) will no longer publish overdraft and non-sufficient fund fee income for individual credit unions.

View the entire press release.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- More Opportunity, Less Risk: 8 Steps to Protect Financial Services Data with GenAI
- FS-ISAC 2024 Year-in-Review Report
- Stop the Scams: A Phishing Prevention Framework for Financial Services
- Ransomware Essentials: A Guide for Financial Services Firm Defense
- Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks
- Building Cryptographic Agility in the Financial Sector
- LockBit: Access, Encryption, Exfiltration, and Mitigation

See the full list of Knowledge Resources

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- Carsten Fischer: The Need for Speed in Threat Mitigation
- Stephen Sparkes: The Evolution of the CISO Role
- Lindsey Bateman: Keep Your Eyes On The Horizon For Emerging Threats – And New Solutions
- Burim Bivolaku: Financial Sector Collaboration Is Key To Third-Party Risk Management
- Beate Zwijnenberg: Can Cyber Risk be Quantified?
- Josh Magri: The CRI Profile – A Simplified Approach To Better Assessment

UPCOMING EVENTS

Americas

- 9-12 March 2025 | Americas Spring Summit
- 17 March | March CIAC webinar meeting
- 26 March | Member Success Session for New IntelX Users
- 30 April | CIAC Open Forum for Everyone
- 14 May | Member Community Connection, Los Angeles FBI

- 3 June 2025 | FinCyber Today Canada

View all Americas events.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190