FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 17 March 2025 | Issue 274

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
- Coinbase account takeover
- Counterfeit check deposits

System Vulnerabilities

Adobe, Amazon, AMI MegaRAC, Apache, Apple, Atlassian, CA Workload Automation (Apache), Cisco, Cygwin, Debian, Dell, Edimax, F5, F5OS-A Intel, Fortinet, HP, IBM, Kubernetes, GitRepo, Google, Lenovo, Microsoft, NAKIVO, Oracle, PAN-OS, PHP, Proofpoint, Red Hat, RSA, SAP, Schneider Electric, SMA, Spring Security, SUSE, Tomcat, Ubuntu, and Veeam.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Account Notification, Administrator authorized, AP Signed Docu: ID: 5405, D.D. Change Request, Migrate to Coinbase Wallet, Equipment Purchase (wire transfer), Fake Invoice, Final Request, Loan Payoff Quote, Masqueraded Files, Outstanding Invoice Reminder, Protest Notice/Invoice, Purchase Order, Rakuten, Requested Document, Sante PACS Server, scanned Document, Secure File, Sharepoint, SSA Impersonation, Support ID: #896531 - Advertising Restrictions: Advertising Restrictions: FTC Compliance Issue Detected, Undelivered Mail, and Updating Banking information.

Threats, Malware, Cyber Campaigns, and Adversaries

- Astaroth
- AsyncRAT
- BeaverTail (InvisibleFerret)
- BLACKWIDOW (aka Lotus)
- Bumblebee (aka ShellSting, Shindig)
- CellikRAT V4.0 Malware
- ChainedDown malware
- ChainedRAT
- ClickFix/ClearFake
- Cluster Phishing
- CodeTail malware
- ConnectWise RAT
- Credential Pharming
- MetaStealer
- Mispadu
- Nitrogen
- Safeplay Ransomware
- SocGholish
- SocksShell (aka Zapcat Supper)
- SEO Poisoning
- SocksProxyGo (aka PortStarter) Malware
- SparkRAT
- SystemBC malware
- Typosquatting
- Umbral Stealer

- DNS Flood Attack
- EvilGinx
- Grandoreiro
- Latrodectus
- VenomRAT
- Xloader
- Xworm
- Zloader

NEWS AND RISK INFORMATION

A new Steganographic campaign found distributing multiple malware variants. "The campaign was found distributing Remcos and AsyncRAT via phishing emails with malicious Excel files. These exploit vulnerabilities download disguised JPGs with encoded payloads and use process hollowing to steal data and maintain control." (Seqrite)

Bank customers want clearer communication on cybersecurity. "A recent poll from a global professional services firm found that 85% of bank customers say clear communication about cybersecurity practices is essential. However, 28% rate their bank highly when it comes to providing such clarity. Meanwhile, the majority of banks surveyed believe they're doing well in this area, revealing a discrepancy between how banks and their customers feel about banks' cybersecurity messaging." (Banking Dive)

ClickFix attacks increasingly lead to infostealer infections. Social engineering tactics designed to trick users into installing malware, often by "fixing" a fake problem, are becoming more common. Experts say most ClickFix — aka ClearFix or paste-and-run — attacks now lead to information-stealing malware infections. (Data Breach Today)

How financial institutions can minimize their attack surface. Sunil Mallik, CISO, Discover Financial Services, explained Discover's approach to defending the business and customers against social engineering attacks, payment fraud, and account takeover fraud, along with "insights on balancing compliance with agility, lessons from regulatory audits, and Discover's approach to risk management and workforce development." (HelpNet Security)

New Lockbit-linked ransomware group targets Fortinet vulnerabilities. The threat actor, tracked as Mora_001, has been using the LockBit 3.0-based strain dubbed "SuperBlack" in campaigns between late January and March 2025. Forescout reported that the group is targeting exposed Fortigate firewalls vulnerable to CVE-2024-55591 and CVE-2025-24472. (SCMedia)

Microsoft warns of new StilachiRAT malware used for crypto theft and reconnaissance. "While the malware (dubbed StilachiRAT) hasn't yet reached widespread distribution, Microsoft says it decided to publicly share indicators of compromise and mitigation guidance to help network defenders detect this threat and reduce its impact." (Bleeping Computer)

OctoV2 Android banking trojan masquerades as Deepseek AI in a phishing attack. "A new report from K7 Labs uncovered a sophisticated Android banking trojan campaign that is disguised as a popular AI chatbot to deceive users. The OctoV2 malware is being spread through deceptive websites that mimic Deepseek AI." (SecurityOnline)

OpenAI's Operator AI agent can be used in phishing attacks. "Just as attackers use social engineering to trick people, they can prompt AI agents into taking malicious actions … the real risk isn't AI itself, but the fact that organizations don't manage these non-human identities (NHIs) with the same security controls as human users." (SCWorld)

Sophisticated phishing campaign exploiting Microsoft 365 infrastructure. "By leveraging legitimate Microsoft domains and tenant misconfigurations, attackers conduct Business Email Compromise (BEC) operations, tricking users into providing information while maintaining a high degree of legitimacy." (Guardz)

THREATS OF THE WEEK

Apache vulnerabilities and GitHub compromise highlight this week's risk.

Apache Camel Vulnerability

Summary

A bypass/Injection vulnerability (CVE-2025-27636) in Apache Camel components affects Apache Camel under particular conditions.

This vulnerability is present in Camel's default incoming header filter. The vulnerability allows an attacker to include Camel-specific headers that can alter some Camel components' behaviors, such as exploiting the camel-bean component to call another method on the bean coded in the application.

Risk

Institutions with Camel applications directly connected to the internet via HTTP could be compromised by an attacker who includes malicious HTTP headers in the HTTP requests sent to the Camel application. All the known Camel HTTP components — such as camel-servlet, camel-jetty, camel-undertow, camel-platform-http, and camel-netty-http — would be vulnerable out of the box.

Remediation

Institutions should review the recommended remedial actions based on your environment.

Supply Chain Compromise of Third-Party GitHub

Summary

Popular third-party GitHub Action tj-actions/changed-files (that detects which files have changed in a pull request or commit) was compromised in an exploit that allows for information disclosure of secrets. Disclosures may include valid access keys, GitHub Personal Access Tokens (PATs), npm tokens, and private RSA keys, among others. This has been patched in v46.0.1.

The compromise is tracked as CVE-2025-30066. The Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2025-30066 to its Known Exploited Vulnerabilities Catalog.

Remediation

CISA strongly urges users to implement the recommendations to mitigate this compromise and strengthen security when using third-party actions.

Related Content

See the following resources for more guidance:

- GitHub: tj-actions changed-files through 45.0.7 allows remote attackers to discover secrets by reading actions logs
- GitHub: Security hardening for GitHub Actions - GitHub Docs
- GitHub: tj-actions/changed-files: :octocat: Github action to retrieve all (added, copied, modified, deleted, renamed, type changed, unmerged, unknown) files and directories
- StepSecurity: Harden-Runner detection: tj-actions/changed-files action is compromised
- Wiz: GitHub Action tj-actions/changed-files supply chain attack

Institutions should report incidents and anomalous activity to CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870.

THREAT INTELLIGENCE UPDATE

Campaigns Targeting Credit Unions Increase

Third-party infiltration, ransomware, and fraud exploits are on the rise.

Summary

Cyber attacks, particularly ransomware attacks, are increasing against credit unions. The National Credit Union Administration (NCUA) reported over 1,000 cyber incidents from September 2023 to August 2024 against service providers. Table 1 reflects some of the larger incidents gleaned from open-source channels, including privacyrights.org.

Table 1.

Date	Incident Type	Impact
11 March 2025	Vishing/Check Fraud	Fraud ring netted more than $3 million from 800 credit union member accounts
20 January 2025	Data Breach	An unauthorized party accessed parts of a CU's IT network of 240,000 CU member records
26 November 2024	Data Breach/Ransomware	Ransomware attack on a vendor caused outages in 60 credit unions
23 September 2024	Data Breach	Hackers compromised over 36,000 CU member records
5 September 2024	Ransomware	Ransomware attack carried out by the Nitrogen group involves 240,000 CU member records.
1 July 2024	Data Breach/Ransomware	Ransomware attack led to the proactive shutdown of several customer-facing banking systems
27 June 2024	Data Breach/Ransomware	The Meow ransomware group claimed to steal 99,000 CU members' social security numbers
31 May 2023	Third-Party Data Breach	MoveIT incident involving 500,000 stolen CU member records discovered on 30 July 2024

Why the Increased Focus?

Threat actors are learning that while credit unions (CUs) generally have lower assets than community banks, they are lucrative targets. Further, some CUs lack the technical staff to manage IT and auditing services, which could allow gaps in security postures.

America's Credit Unions, the National Credit Union Association, and FS-ISAC

Though many are vulnerable, no credit union is alone in the fight against cybercrime.

For instance, America's Credit Unions (ACC) advocates for legislation establishing a comprehensive federal data privacy and security standard.

The NCUA continues to develop updated information security examination procedures and provides a cyber resource center for its members. To report cyber incidents to the NCUA, including incidents involving a vendor or third-party provider, use one of the following channels within 72 hours of detection:

- Submit a cyber incident report
- Call the NCUA at 1.833.CYBERCU (1.833.292.3728)
- Send a secure email to cybercu@ncua.gov

FS-ISAC's role is to collect and share actionable, proactive threat intelligence to prevent cyber incidents. We host the Credit Union Council comprised of CU members who look after each other in a trusted

community to ensure privacy and confidentiality. In addition to this report, they have access to alerts, secure chat channels connecting them to communities of interest, and other communication channels.

Every member is supported by Account Managers and an Executive Sponsor to help them maximize FS-ISAC's tools and products. Learn more about joining our community here.

JUST FOR COMMUNITY INSTITUTIONS

Counterfeit Check Fraud

Summary

Several CUs in the American Northeast were victims of a reported $3M USD check fraud scam.

TTPs

- Fraudsters initiated a vishing campaign to trick consumers into sharing their account information.
- The information obtained was used to create counterfeit checks that were then deposited into the CU member accounts.
- Funds were allegedly abstracted.

Remediation

- Institutions should work with internal stakeholders to raise awareness about vishing and phishing campaigns with their members, front-line associates, and deposit and retail operation departments.
- Institutions should "Know Their Customer" and discreetly inquire about abnormal deposits to identify potentially suspicious deposits.
- Partner with fraud departments for further investigation action.
- Institutions should "Know Their Recourse" and place applicable holds on deposits as per their policy and regulatory guidelines.

RFI

If your institution is experiencing similar fraud activity, please report it to intelligence@fsisac.com.

What FS-ISAC is Doing

FS-ISAC continues to monitor the situation and will provide updates once they have been confirmed.

FRAUD UPDATE

FS-ISAC Monthly Fraud Trends Report

Summary

The FS-ISAC Monthly Fraud Trends Report - February 2025 is now available on SHARE. This report provides an overview of fraud trends for FS-ISAC members.

Download the report.

Video Recording of Scam Compounds Spotlight Call

Summary

FS-ISAC held a TLP Green Spotlight Call on Scam Compounds featuring Erin West as our guest speaker. West is a former Deputy District Attorney and currently the president of Operation Shamrock, a non-profit organization committed to combating transnational organized crime.

In this Spotlight Call, West briefed on the following:

- The scam compounds that are currently operating
- The latest developments in their operations
- How the financial sector and other key stakeholders can more effectively identify and combat this highly damaging activity

Key takeaway: Awareness is paramount — financial institutions should enhance training for frontline staff to better identify red flags during withdrawals.

The Spotlight Call is available for members in FS-ISAC's IntelX Videos App. West's presentation is available under Share Alert ID dbe23ecf.

GOVERNMENT AND REGULATORY NEWS

Bank Supervision: Removing References to Reputation Risk

Summary

The Office of the Comptroller of the Currency (OCC) has commenced removing references to the bank's reputation risk from its *Comptroller's Handbook* booklets and guidance issuances. Concurrently, the OCC has instructed its examiners to no longer examine reputation risk.

The OCC has never used reputation risk as a catch-all justification for supervisory action. Rather, the OCC has focused primarily on the risks to a bank's current or projected financial condition and resilience arising from negative public opinion. Nonetheless, the OCC believes removing references to reputation risk will improve transparency and confidence in the supervisory process. For handbooks and guidance issuances issued jointly with other regulators, the OCC will work with those regulators to expeditiously remove references to banks' reputation risk.

The OCC expects banks to engage in sound risk management practices, operate safely and soundly, and comply with applicable laws and regulations.

Read the entire bulletin.

NCUA Releases 2024 Annual Report

Summary

The NCUA recently released its 2024 Annual Report, documenting the NCUA's performance in meeting its goals and objectives as detailed in its strategic plan and annual performance plan. The report contains the audited financial statements for the agency's four funds, which earned unmodified or "clean" opinions for 2024. It also provides assurances of the agency's compliance with federal financial management guidelines, regulations, and relevant laws.

View the entire press release.

Q4 2024 State-Level Credit Union Data Report

Summary

According to the latest Quarterly US Map Review released by the National Credit Union Administration, federally insured credit unions experienced growth in shares and deposits at the median over the year ending in the fourth quarter of 2024, while loans outstanding remained unchanged. The median delinquency rate rose.

View the entire press release.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- Leveling Up: A Cyber Fraud Prevention Framework for Financial Services
- Charting the Course of AI: Practical Considerations for Financial Services Leaders
- 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

- FinCyber Today Podcast Season 1:
  - Olivier Nautet: Infobesity - How Much Data is Too Much?
  - Karl Schimmeck: Data Security in a Demanding Regulatory Environment
  - Claus Norup: Governance - What a CISO Needs to Succeed
  - Matt Harper: The Convergence of Business and Cyber-Risk Management Through a Bigger Lens

- 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

- 26 March | Member Success Session for New IntelX Users
- 21 April | April CIAC webinar meeting
- 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.

12120 Sunset Hills Rd, Reston
VA 20190