FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 10 March 2025 | Issue 273

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, Apache, Apple, Arista, Avaya, Azure, Cisco, Debian, Dell, F5, HP, HPE, Gitlab, Google, IBM, Ivanti, Juniper, Lenovo, Microsoft, Mozilla, Oracle, Palo Alto, PAN-OS, Red Hat, SAP, SCADA, SUSE, Ubuntu, VMware, and WhatsApp.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: 2025 Q1 Staff Pay Adjustment Handbook, Confirm a charge, Credential Pharming, Direct Deposit, DocuSign, Employee Handbook, Gift Card, Mass QR Code, New Vmail From +1(902), and Vendor Payment.

Threats, Malware, Cyber Campaigns, and Adversaries

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

NEWS AND RISK INFORMATION

AI-Assisted fake GitHub repositories fuel SmartLoader and Lumma Stealer distribution. “Trend Research uncovered a campaign that uses fake GitHub repositories to distribute SmartLoader, which is then used to deliver Lumma Stealer and other malicious payloads.“ (Trend Micro)

Critical PHP vulnerability under widespread cyber attack. “Exploitation of CVE-20 24-4577, which affects all versions of PHP installations for Windows devices, can enable remote code execution on targeted systems. While recent attacks on the PHP vulnerability first appeared limited to Japan, GreyNoise said that is not true. Attack attempts have been observed across multiple regions, with notable spikes in the United States, Singapore, Japan, and other countries throughout January 2025.” (Cybersecurity Dive)

EByte Ransomware: A new Go-based threat with advanced encryption techniques. “This malware leverages advanced cryptographic methods, combining ChaCha20 for encryption and ECIES for secure key transmission … A decryption tool (EByte-Rware-Decryptor) is available but requires the attacker-controlled ECIES private key.” (Cybersecurity News)

FIN7, FIN8, and others use Ragnar Loader for persistent access and ransomware operations. “Ragnar Loader, also referred to as Sardonic, was first documented by Bitdefender in August 2021 in connection with an unsuccessful attack carried out by FIN8 aimed at an unnamed financial institution located in the US … The core functionality of Ragnar Loader is its ability to establish long-term footholds within targeted environments, while employing an arsenal of techniques to sidestep detection and ensure operational resilience.” (Hacker News)

Large-scale fraud operation "PrintSteal" generates fake KYC documents through spoofed sites. “Operating under a network of impersonating websites, the scheme has exploited Common Service Centre (CSC) platforms to produce and distribute fake Aadhaar cards, birth certificates, PAN cards, and other identity documents.” (Security Online)

Majority of orgs hit by AI cyber attacks as detection lags. “Most (87%) security professionals have reported that their organization has encountered an AI-driven cyber attack in the last year … with only 26% expressing high confidence in their detection abilities.” (Infosecurity Magazine)

Malvertising op targets almost 1M devices via malicious GitHub repos. “Microsoft Threat Intelligence on 6 March posted a blog that said that a large malvertising campaign aimed at stealing sensitive information that leverages malicious GitHub repos affected nearly 1 million devices globally on a wide range of consumer and enterprise machines. The attack originates when users access illegal streaming websites embedded with malvertising redirectors. This leads them to an intermediary webpage, where they are then redirected to GitHub, Discord, and Dropbox.” (SC Media)

Millions of stalkerware users exposed again. “As reported by TechCrunch, researchers found a vulnerability in three very similar stalkerware apps called Spyzie, Cocospy, and Spyic. The bug not only exposes the data from the victim’s device like messages, photos, and location data, but also allowed the researcher to collect 518,643 unique email addresses of Spyzie customers, 1.81 million email addresses of Cocospy customers, and 880,167 email addresses of Spyic customers.
Apparently, the bug is so easy to exploit that TechCrunch, and the researcher found it not advisable to reveal any details, since anyone would have been able to exploit it.” (Malwarebytes)

New Chirp tool uses audio tones to transfer data between devices. “A new open-source tool named 'Chirp' transmits data between computers (and smartphones) through different audio tones … Other microphone-equipped computers running Chirp may capture the sound and translate the message back into text.” (Bleeping Computer)

THREATS OF THE WEEK

Cybercriminals take advantage of the political landscape; phishing and malware highlight this week’s risk.

Apache Multiple Server Vulnerabilities

Summary

Apache announced several traffic server flaws. Cybercriminals can exploit malformed requests and access control list (ACL) issues, posing serious security risks to users. Institutions using the suite of products should investigate the CVE alerts and take appropriate action.

Related Content

The vulnerabilities are CVE-2024-38311, CVE-2024-56195, CVE-2024-56196, and CVE-2024-56202.

Geopolitical Landscape and More

Summary

Phishing remained the most reported attack pattern despite a slight decrease in volume compared to last month. Phishing reports noted a variety of evolving tactics, including the use of the Tycoon 2FA phishing kit and Callback Phishing campaigns leading users to download malware.

Malware varieties have increased since January, with 28 unique variants observed. The most frequently reported malware was SocGholish, Astaroth, and AsyncRAT.

Mass Exploitation of Critical PHP-CGI Vulnerability

Summary

The Cyber Center is aware of reports of ongoing and increased exploitation of CVE-2024-4577, a critical remote code execution (RCE) vulnerability in the PHP-CGI implementation of PHP on Windows. Windows-based PHP installations configured to use PHP-CGI are specifically at risk as the vulnerability exploits Unicode processing in the CGI module.

Threat actors are actively using this vulnerability. The Cyber Center is not aware of any Canadian victims from this increased activity, but systems in Canada remain vulnerable, though the exploit's proof-of-concept has been available since June 2024.

Remediation

Organizations should determine if they are at risk by verifying whether they are running vulnerable versions of PHP installed on Windows. Organizations are advised to update to the following versions of PHP [4]:

- PHP 8.3 - update to 8.3.8 or later
- PHP 8.2 - update to 8.2.20 or later
- PHP 8.1 - update to 8.1.29 or later

Organizations should also review and implement the Cyber Centre's Top 10 IT Security Actions [5] with an emphasis on the following topics:

- Consolidating, monitoring, and defending Internet gateways
- Patching operating systems and applications
- Isolate web-facing applications

Medusa Ransomware Advisory

Summary

The Cybersecurity and Infrastructure Security Agency (CISA), in its role as the National Coordinator for Critical Infrastructure Security and Resilience, partnered with the Federal Bureau of Investigation (FBI)

and Multi-State Information Sharing and Analysis Center (MS-ISAC) to publish a joint Cybersecurity Advisory #StopRansomware: Medusa. This advisory provides known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with Medusa ransomware actors identified through FBI investigations.
Medusa is a ransomware-as-a-service (RaaS) variant first identified in June 2021. As of December 2024, Medusa developers and affiliates have impacted over 300 victims from a variety of critical infrastructure sectors with affected industries including medical, education, legal, insurance, technology, and manufacturing. The Medusa ransomware variant is unrelated to the MedusaLocker variant and the Medusa mobile malware variant.

Recommended mitigation actions include ensuring operating systems, software, and firmware are patched and up to date; segment networks to restrict lateral movement from initial infected devices to other devices; filter network traffic by preventing users from unknown or untrusted origins from accessing remote services on internal systems.

Organizations are encouraged to review the advisory and implement recommended mitigations to protect against the ransomware threat actor. Organizations are also encouraged to visit stopransomware.gov, a whole-of-government approach with one central location for no-cost U.S. ransomware resources and alerts, to access an updated joint #StopRansomware Guide.

THREAT INTELLIGENCE UPDATE

Spearwing Claims 40+ Victims in 2025

Ransomware incidents by the Medusa group are spiking.

Summary

The Symantec Threat Hunter Team reported the Medusa ransomware group has hit nearly 400 victims since it first emerged in January 2023. “The Medusa ransomware is reportedly operated as a ransomware-as-a-service (RaaS) by a group Symantec’s Threat Hunter Team tracks as Spearwing,” says Symantec, and that Spearwing has claimed over 40 attacks in 2025.

Spearwing and other ransomware groups emerged after Noberus and LockBit were disrupted by law enforcement in the past two years.

Spearwing’s Medusa ransomware is distinct from the older MedusaLocker ransomware and is believed to gain access to victim networks by exploiting unpatched vulnerabilities in public-facing applications, such as Microsoft Exchange servers, and using legitimate accounts, possibly purchased from initial access brokers.

Medusa’s attacks involve a mixture of living-off-the-land and dual-use tools, especially the remote management and monitoring software PDQ Deploy. Attacks also consistently involve the bring-your-own-vulnerable-driver (BYOVD) technique to disable security software.

The consistency of TTPs suggests Spearwing conducts attacks themselves, has a small number of affiliates, and/or provides affiliates with an attack playbook.

The group and its affiliates typically carry out double extortion attacks, stealing victims’ data and encrypting their networks to pressure them into paying a ransom, which has ranged from $100,000 to USD 15 million.

Risk

Ransomware campaigns create a wide range of risks, including compliance, financial, regulatory, and reputation risks, and can threaten an institution’s ability to operate.

Remediation

Preparing for a ransomware incident begins with assessing the institution's risk and vulnerability. Institutions with limited resources will benefit by using the Ransomware Self-Assessment Tool, and by reviewing the 2023 edition of the #StopRansomwareGuide.

JUST FOR COMMUNITY INSTITUTIONS

Three Good Reasons to Share Threat Intelligence

Summary

At the Spring Summit in New Orleans, a cyber expert at an FS-ISAC member firm mentioned that though he read and acted on other members' reports, he had never shared one. When asked why, he said he thought his writing skills were under par compared to others, and he wasn't sure his institution permitted him to share threat information at all.

His points were reasonable — but perhaps mistaken.

The power of sharing intel

Cybercriminals are very clever and quick. Once they detect that an institution has moved to block an attack, bad actors simply select a new victim. If your institution is successfully rebuffing attacks but failing to tell others, adversaries just pivot to another attack. But when everyone shares what they are seeing, the financial services sector's defensive shields can be raised. That benefits the entire membership and each institution in it.

Writing posts with — or in — confidence

Some members are insecure about creating posts, so fail to alert the membership on the threats and mitigations that affect their firms.

That's unfortunate. All intel-sharing is good — it benefits everyone — and FS-ISAC is a trusted community that values its members' experiences. If that doesn't give you confidence, remember that posts can be made without attribution in SHARE. You can even ask your Community of Interest director to post for you while you stay anonymous.

Are you sure you can't share?

Some members assume their institution prohibits sharing intel but have never asked their legal department. Similarly, some legal counsels don't really understand how sharing with FS-ISAC works.

For example, your legal counsel may not know that:

- Members cannot share personally identifiable information on FS-ISAC communication channels.
- The valuable information shared in FS-ISAC by your peers includes a high-level summary of an incident, exploit type (i.e., malware, phishing, etc.), malware or phishing subject name, indicators of compromise or fraud, domain names, etc. This information doesn't damage the firm, but it does help defend the global financial system.
- Members can share information securely and without attribution.

Sometimes misunderstandings can be cleared with a simple conversation about the benefit of shared information and the desire to be a good corporate citizen by sharing.

Ultimately, there may be no reason to be reluctant to post and plenty of good reasons to do it.

FRAUD UPDATE

New Cyber Fraud Prevention Framework Released

Summary

FS-ISAC's Cyber Fraud Prevention Framework Working Group released its Cyber Fraud Prevention Framework in March 2025. The Framework helps firms coordinate all the teams that deal with fraud — from cyber to AML — and spot the tactics, techniques, and procedures a criminal may be using to steal money, credentials, account information, etc. With that vital information, teams can collaboratively stop the fraud and prevent others from happening.

Download your copy.

Fraudulent US Savings Bonds

Summary

An FS-ISAC member reports recently seeing a trend where individuals will enter branch locations requesting to redeem fraudulent US Savings Bonds, and in some cases deposit the proceeds of the fraudulent bonds.

Tactics, Techniques and Processes

- Most fraudulent bonds have been presented by new customers (less than one year).
- There are noticeable irregularities in the texture, feel, or appearance of the bond.
- The word "GIFT" appears at the bottom of the payee section (see examples below)
- The bond stamp is "FEDERAL RESERVE BANK JUNE, 19 1992 KANSAS CITY MO 10 2999" (see examples below).
- Customer profile and account level address may differ.
- Most fraudulent items presented in multiple states are payable to payees with Illinois addresses.
- Face values of $1,000 and $10,000 (see examples below).

Action To Be Taken

Institutions should:

- Share this intelligence with fraud and loss prevention teams
- Consider sharing this information with branch personnel and deposit operation teams for additional security awareness
- Provide direction on reporting these events to appropriate internal departments and how to report them.

Report incidents to FS-ISAC's Fraud Intelligence working group.

New FTC Data Show a Big Jump in Fraud Losses

Newly released Federal Trade Commission data show that consumers reported losing over USD 12.5 billion to fraud in 2024, representing a 25% increase over the prior year. In 2023, 27% of people who reported a fraud said they lost money; in 2024, that figure jumped to 38%.

Consumers reported losing more money to investment scams — $5.7 billion — than to any other fraud category in 2024. That amount represents a 24% increase over 2023. Losses to imposter scams came in second with $2.95 billion reported stolen. In 2024, consumers reported paying fraudsters with bank transfers or cryptocurrency more than all other payment methods combined.

Read the entire press release.

GOVERNMENT AND REGULATORY NEWS

Bank Activities: OCC Issuances Addressing Certain Crypto-Asset Activities

Summary

The Office of the Comptroller of the Currency (OCC) issued Interpretive Letter 1183, which rescinds OCC Interpretive Letter 1179 (18 November 2021) (IL 1179).

The OCC's 7 March 2025 Bulletin 2025-2 states, "These actions are intended to reduce burden, encourage responsible innovation, and enhance transparency. The OCC will examine the activities described in IL 1170 (addressing crypto-asset custody services), 1172 (addressing holding deposits that serve as reserves backing stablecoins), and 1174 (addressing the use of stablecoins and distributed ledger technology to facilitate payments) as part of its ongoing supervisory process.

As with all activities, banks must conduct crypto-asset activities in a safe, sound, and fair manner and in compliance with applicable law. New activities should be developed and implemented consistently with sound risk management practices and align with banks' overall business plans and strategies."

Read the entire bulletin.

Fourth Quarter Credit Union Report

Summary

According to the latest financial performance data released today by the National Credit Union Administration, total assets in US federally insured credit unions rose by $52 billion, or 2.3%, to $2.31 trillion over the year ending in the fourth quarter of 2024. Insured shares and deposits grew $58 billion, or 3.4%, to $1.78 trillion. The delinquency rate at federally insured credit unions was 98 basis points in the fourth quarter of 2024, up 15 basis points from one year earlier.

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

- 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

- 17 March | March CIAC webinar meeting
- 26 March | Member Success Session for New IntelX Users
- 12 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.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190