FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 15 December 2025 | Issue 313

This report highlights this week's top risks to support community institution information security and technology teams in proactively protecting their financial institutions from threats that can impair their ability to operate and avoid compliance, economic, legal, regulatory, and reputational impacts.

This Week's Threats

Fraud Campaigns

- Account takeover
- Call Center Identity impersonation
- CEO impersonation
- Fraudulent withdrawals

System Vulnerabilities

Android, Apple, Arista, ASUS, Atlassian, Avaya, AzeoTech, Cisco, Cygwin, Debian, Dell, F5, Fortinet, FreePBX, Fuji Electric, GeoServer, GitLab, Gladinet CentreStack, Google, Grassroots DICOM, Güralp Systems FMUS (Fortimus) Series and MIN (Minimus) Series, Hitachi, HP, IBM, Johnson Controls, JumpCloud, Lenovo, Linux, Microsoft, Mitsubishi, Mozilla, Nessus, .NET, OpenPLC, Oracle, OSGeo GeoServer, Red Hat, Samsung, SAP, Sierra Wireless, Siemens, SonicWall, SUSE, Ubuntu, and Varex Imaging.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Access Control MSG, Adult Dating, Amazon, December Bonus, DocuSign, Document Shared with you, Expense Reimbursement, Homes, Please Download, Q4 Salary Bonus, Refund Scheme, RSVP Required, SAU Insurance, and Trump Account.

Threats, Malware, Cyber Campaigns, and Adversaries

- AdaptixC2 Beacon
- Aisuru botnet
- Amatera Stealer
- Amadey
- Albiriox
- Astaroth
- Amadey
- AsyncRAT
- BeaverTail
- BianLian
- CastleLoader
- DarkCrystal
- DroidLock
- EdgeStepper
- Eternidade Stealer
- ModiLoader
- Oyster
- PoisonPlug
- Predator Spyware
- PureHVNC
- PureLogs
- PyStoreRAT
- Rhadamanthys Stealer
- Qakbot
- Remcos
- Rust
- SectopRAT
- Shadowpad
- ShadowRay
- ShriveledPeach Malware

- Formbook
- FvncBot
- GlassWorm
- GULoader
- HoldingHands RAT
- JsOUTProx
- LandUpdate808
- Latrodectus
- Lokibot
- Makop ransomware
- Metamorfo
- sLoad
- Snakeloader
- SocksShell
- TamperedChef
- VenomRAT
- Vidar
- Xloader
- XRed
- Xworm
- Zapcat
- ZgRAT

NEWS AND RISK INFORMATION

Askul confirms theft of 740K customer records in ransomware attack. “Askul Corporation, a major Japanese e-commerce company, suffered a ransomware attack by the RansomHouse group, resulting in the theft of approximately 740,000 customer records.” (BleepingComputer)

ClickFix attack spreads DarkGate malware. “A sophisticated social engineering campaign is exploiting a fake “Word Online” extension error message to distribute DarkGate malware. This attack utilizes the ClickFix technique, where users are tricked into executing malicious commands disguised as legitimate troubleshooting steps. Upon encountering a fraudulent message, victims are prompted to click a “How to fix” button, which triggers a malicious JavaScript snippet. This script decodes a hidden PowerShell command that downloads an HTA file named “dark.hta” from a compromised site. Once executed, the HTA file establishes communication with the attacker’s infrastructure, allowing for the deployment of additional malware and the theft of sensitive data.” (Cyware)

Data breach at credit check giant 700Credit affects at least 5.6 million. “A sophisticated adversary-in-the-middle (AiTM) phishing campaign has been identified, targeting Microsoft 365 and Okta users. The campaign bypasses multi-factor authentication (MFA) by hijacking legitimate single sign-on (SSO) authentication flows.” (TechCrunch)

Experts found an unsecured 16TB database containing 4.3B professional records. “An unsecured 16TB MongoDB database containing 4.3 billion professional records was discovered, posing a significant risk for large-scale AI-driven social engineering attacks. The database included LinkedIn-style data.” (Security Affairs)

Featured Chrome browser extension caught intercepting millions of users' AI chats. “A Chrome extension, Urban VPN Proxy, with over six million users, has been found intercepting and exfiltrating user data from AI chatbots like OpenAI ChatGPT and Microsoft Copilot.” (Hacker News)

The Incident Reconnection Framework for the Financial Services Sector has been updated. On 16 December, the Financial Services Sector Coordinating Council (FSSCC) and the Securities Industry and Financial Markets Association (SIFMA) published an updated version of The Financial Services Sector Reconnection Framework, designed for use by financial services firms that have been compromised by a cyber incident. (FSCC/SIFMA)

New PyStoreRAT malware targets OSINT researchers through GitHub. “PyStoreRAT is a newly identified malware targeting OSINT researchers and IT professionals through GitHub. It is distributed via fake OSINT tools and other software, leveraging AI to build trust and evade detection.” (Hack Read)

Trump administration issues new AI Executive Order. On 11 December, “the Trump Administration announced a new executive order with the intention “to remove barriers to United States AI leadership.” The order asserts the US is in “a race with adversaries” for AI dominance, and the presence of “cumbersome regulation” impedes the nation’s progress — particularly, state regulation.” (Security Magazine)

THREAT OF THE WEEK

Ransomware and malware highlight the risks of this week.

Supply Chain and the Ransomware Factor

Summary

The cybersecurity and resilience of the financial services sector are among the most robust among infrastructure industries. That does not make the sector invulnerable. Threat actors are increasingly targeting the sector's supply to steal data – and a favored tactic is ransomware extortion.

These attacks rely on various techniques, often social engineering, that enable cybercriminals to access data and release it for a price (though there's no guarantee). Artificial intelligence makes these attacks more sophisticated, effective, and frequent.

In this threat environment, firms must have a ransomware prevention and protection plan – FS-ISAC recommends the following checklist to defend your firm against ransomware.

Does your organization have regularly scheduled backups?	Determine if these backups are disconnected from your network, either via cloud storage systems or air-gapped USBs/hard drives.
Are any nonessential devices connected to your organization's network?	If so, assess if they can be moved to other networks that do not house sensitive data.
Does your organization understand the regulatory and legal risks involved with paying a ransom?	Get legal guidance on the laws applicable to the jurisdictions in which you do business.
Does your organization regularly update its software and systems?	Inventory the current update schedule and, ideally, automate software and system updates.
Does your organization have a plan for how to deal with a ransomware attack and the loss of valuable data?	Develop a robust incident response and vendor oversight playbook.
Does your organization have a cyber insurance policy? If so, how does that plan apply to ransomware attacks?	Speak with your carrier. Some plans explicitly prohibit ransom payments, while others cover the cost if payment is part of the policy.

Investing in Real-Time Protection

- Invest in anti-malware protection systems that adapt to new threat intelligence in real time.
- Evaluate the security of all devices connected to networks that house sensitive or essential information. Connect all nonessential systems to a separate network.
    - Be particularly careful when bringing IoT or "smart devices" (e.g., Alexa, Google Nest, medical sensors, etc.) into your workspaces, because these systems often have weaker or nonexistent security systems and can be targeted as access points to essential systems.
    - Consider the security of remote work setups. Ensure security tools work off the network to monitor all web traffic.
- Promote employee education around phishing attacks and the necessity of strong password protections.
- Consider implementing MFA across your organization if feasible.
- Keep all systems and software regularly updated. Change settings to allow for automated updates if possible.
- Develop an incident response and crisis management plan for how to deal with a ransomware attack and the loss of valuable data.

- Prepare an external communication plan in the event of a ransomware attack that includes relevant stakeholders, authorities, and industry peers.

Data Backups

- Invest in secure, regularly updated backup systems that keep your data protected.
    - If using USBs or hard drives, physically disconnect these devices from networked computers after backups are complete.
    - If using cloud storage, equip the server with high-level encryption and MFA.
- Create a read-only copy of the general ledger for worst-case disaster recovery.
- Develop systems that perform automated data recovery and remediation.
- Develop scenarios to assess how long it will take to recover critical data and business services.

Though the sector's cybersecurity and resilience are uniquely mature, the supply chain will always present vulnerabilities. Develop a ransomware plan now, so you can marshal the necessary response when a threat actor attacks a vendor – and ultimately, your firm.

Just In Time For The Holidays: SantaStealer Malware

Summary

This in from Rapid7: "A new MaaS called SantaStealer is being promoted on Telegram and hacker forums, operating in memory to avoid detection. This malware is a rebranding of BluelineStealer and is offered in two subscription tiers: Basic, priced at $175/month, and Premium, priced at $300/month.

SantaStealer utilizes 14 data-collection modules, each running independently to extract information from browsers, cryptocurrency wallets, and messaging apps, including Telegram and Discord. It exfiltrates stolen data in chunks to a hardcoded command-and-control endpoint.

Despite claims of advanced evasion techniques, current samples have revealed vulnerabilities and are easily analyzed, indicating poor operational security on the part of the developers. The exact distribution methods for SantaStealer remain uncertain, but it may involve tactics like phishing and malicious software downloads."

THREAT INTELLIGENCE UPDATE

React2Shell Exploitation in the Wild

Summary

On 8 December, Wiz.io reported the active exploitation of CVE-2025-55182, a remote code execution vulnerability disclosed by React on 3 December.

Wiz noted opportunistic exploitation as part of crypto mining and credential harvesting campaigns. Additionally, the company noted at least one campaign using the Sliver post-exploitation framework. So far, at least one FS-ISAC member has observed scanning for vulnerable React2Shell components and reported relevant indicators of compromise.

Risk

On 15 December, Microsoft's Research Team shared an update regarding the incident, saying the "vulnerability presents a significant risk" due to:

- Vulnerable default configurations that require no special setup or developer error.
- Readily available public proof-of-concept exploits, with almost perfect reliability.
- User authentication is not required.
- The ability to exploit the vulnerability with a single malicious HTTP request.

Remediation

CVE-2025-55182 represents a high-impact, low-friction attack path against modern React Server Components deployments. Rapid patching combined with layered Defender monitoring and WAF protections provides the strongest short-term and long-term risk reduction strategy.

Microsoft's Research Team recommends that users:

1. **Patch immediately**
    - React and Next.js have released fixes for the impacted packages. Upgrade to one of the following patched versions (or later within the same release line):
        - React: 19.0.1, 19.1.2, 19.2.1
        - Next.js: 5.0.5, 15.1.9, 15.2.6, 15.3.6, 15.4.8, 15.5.7, 16.0.7
    - Because many frameworks and bundlers rely on these packages, make sure your framework-level updates also pull in the corrected dependencies.
2. **Prioritize exposed services**
    - Patch all affected systems, starting with internet-facing workloads.
    - Use Microsoft Defender Vulnerability Management (MDVM) to surface vulnerable package inventory and to track remediation progress across your estate.
3. **Monitor for exploit activity**
    - Review MDVM dashboards and Defender alerts for indicators of attempted exploitation.
    - Correlate endpoint, container, and cloud signals for higher confidence triage.
    - Invoke the incident response process to address any related suspicious activity stemming from this vulnerability.
4. **Add WAF protections where appropriate**
    - Apply Azure Web Application Firewall (WAF) custom rules for Application Gateway and Application Gateway for Containers to help block exploit patterns while patching is in progress. Microsoft has published rule guidance and JSON examples in the Azure Network Security Blog, with ongoing updates as new attack permutations are identified.

JUST FOR COMMUNITY INSTITUTIONS

2025 CWE Top 25 Most Dangerous Software Weaknesses

Summary

According to IBM, unpatched vulnerabilities remain a massive business risk, driving a significant portion of cyber attacks – 78% of breaches involve known, unpatched flaws. Verizon found that a fifth of all attacks start with exploited software vulnerabilities, and 32% of ransomware originates from them, reports Sophos.

In fact, the most severe and prevalent weaknesses total 39,080 system flaws. The sheer volume of new flaws (around 130 daily in 2025) can overwhelm your teams, leading to a backlog where critical issues linger for months, making them prime targets for attackers who exploit well-documented weaknesses.

Uncovering the root causes of these vulnerabilities serves as a powerful guide for investments, policies, and practices to prevent these vulnerabilities from occurring in the first place — benefiting both industry and government stakeholders.

The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Homeland Security Systems Engineering and Development Institute (HSSEDI), operated by the MITRE Corporation, has released the 2025 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses. This annual list identifies the most critical weaknesses adversaries exploit to compromise systems, steal data, or disrupt services.

Prioritizing the weaknesses outlined in the Top 25 is integral to CISA's Secure by Design and Secure by Demand initiatives, which promote the development and procurement of secure technology

solutions. CISA and MITRE encourage organizations to review this list and use it to inform their respective software security strategies.

The 2025 CWE Top 25:

- **Supports vulnerability reduction**: By focusing on the Top 25, organizations can prioritize lifecycle changes, adopt safer architectural decisions, and reduce high-impact vulnerabilities related to injection, access control, and memory safety defects.
- **Drives cost efficiencies**: Eliminating weaknesses early reduces downstream remediation; addressing them before deployment is more efficient and cost-effective than patching, reconfiguring, or responding to emergency incidents.
- **Strengthens Customer and Stakeholder Trust**: Transparent efforts to identify, mitigate, and monitor weaknesses demonstrate commitment to Secure by Design principles. Organizations that prioritize eliminating recurring weaknesses contribute to a safer software ecosystem.
- **Promotes Consumer Awareness**: The Top 25 empowers consumers to understand underlying causes of common vulnerabilities, supports more informed purchasing decisions, and encourages adoption of products that follow robust security engineering practices.

Recommendations for Stakeholders:

- **For Developers and Product Teams**: Review the 2025 CWE Top 25 to identify high-priority weaknesses and adopt Secure by Design practices in development.
- **For Security Teams**: Incorporate the Top 25 into vulnerability management and application security testing to assess and mitigate critical weaknesses.
- **For Procurement and Risk Managers**: Use the Top 25 as a benchmark when evaluating vendors and apply Secure by Demand guidelines to ensure investment in secure products.

Action to Be Taken

If you discover that you have legacy, vulnerable flaws in your institution, what are the practical steps you can take to begin resolving them?

Step 1: Identify and prioritize risk
Step 2: Migrate what's high-risk and critical first
Step 3: Find/Develop A Solution For Continuous Protection

Remember, the goal is to ensure that you protect your institution by maintaining long-term resilience and continuing compliance, which helps you free up time to devote energy to other business objectives.

REGULATORY AND GOVERNMENT UPDATES

Sector Financial Institution Letter and Other Announcements

CISA

- Cybersecurity Performance Goals 2.0 for Critical Infrastructure, 11 December

FDIC

- FIL-60-2025, Notice of Final Rulemaking on Establishment and Relocation of Branches and Offices, 16 December
- FIL-59-2025, Notice of Proposed Rulemaking to Establish GENIUS Act Application Procedures for FDIC-Supervised Institutions Seeking to Issue Payment Stablecoins, 16 December
- FIL-58-2025, Interim Final Rule on Special Assessment Collection, 16 December

FRB

- Agencies announce dollar thresholds for smaller loan exemption from appraisal requirements for higher-priced mortgage loans, 15 December
- Agencies announce dollar thresholds for applicability of truth in lending and consumer leasing rules for consumer credit and lease transactions, 15 December

NCUA:

- NCUA Board to Hold Meeting on December 18, 11 December

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks
- Deepfake Threats, Controls, and Mitigations: A Practitioner's Guide
- FS-ISAC Deepfake Threat Taxonomy: Threats and Controls for Detection Models and Watermarks
- Security Advisory: Software Supply Chain Risk: Protecting Against NPM Software Dependencies
- The Timeline for Post Quantum Cryptographic Migration
- Security Advisory: Protecting CRM and SaaS Platforms
- The Business Information Security Officer: Actionable Advice from Practitioners in Four Industries
- Navigating Cyber 2025
- Define the Role, Limit the Risk: The Roles and Responsibilities of AI Usage in Financial Services
- Cross-Sector Mitigations: Scattered Spider | Guidance for Proactive Defense
- From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector
- Leveling Up: A Cyber Fraud Prevention Framework for Financial Services

See the complete list of Knowledge Resources

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- FinCyber Today Podcast Season 2
- FinCyber Today Podcast Season 1

UPCOMING EVENTS

Americas

Members can enroll in the Member Services app to attend events.

- 15 December | Monthly CIAC Webinar
- 17 December | CIAC and COFFE Open Forum
- 30 January | Member Success Session

View all Americas events.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190