

Global Cyber Threat Level 🚩 | Americas: 🚩 EMEA: 🚩 APAC: 🚩

Week of 2 June 2025 | Issue 285

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

- ACH Wire Fraud
- Fake New Brokerage/Investment Fraud

System Vulnerabilities

Amazon, Android, Apache, Apple, [ASUS \(2\)](#), Cisco, [Craft CMS](#), [ConnectWise](#), [CyberData](#), Cygwin, DameWare, F5, Google, [Hitachi \(5\)](#), HP, HPE, Lenovo, Linux, Mitsubishi, Mozilla, Oracle, [Qualcomm](#), Samsung, [Schneider \(2\)](#), SUSE, Trend Micro, and Xerox.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Account Access, Adult Dating, Appraisal, BMANAGER, Bank Change Request, ConsultDRB, Contract Agreement, DocuSign, Gift Card New: DRB Development Solutions, GlassTX, I just shared a file with you on OneDrive, Income Document, Legal Document, Notice of Payment, M365 Security Notice, Manipulated Invoice, Merrill Edge, New Voicemail, OS Update, Payment Application #0828, Request, Payment Request, Payroll Diversion, Phoenix Construction, Processing Payroll, QR Code, Quickbooks, Retain Access: Service Ref #0400849936, Scanned from a Xerox Multifunction, Secure Message, Shared Document, Splunk, Spring Cloud Gateway Server, Upcoming Task, URGENT EMAIL RESPONSE, Voice Business, and Xerox Multifunction Printer.

Threats, Malware, Cyber Campaigns, and Adversaries

- Acreed ransomware
- BeaverTail (InvisibleFerret)
- BitStep RAT
- Bumblebee (aka ShellSting, Shindig)
- CellikRAT V4.0 Malware
- ChainedDown malware
- ChainedRAT
- ClickFix/ClearFake
- ColdRiver Group
- FormBook
- GolangGhost
- GorillaBot
- Grandoreiro
- GremlinStealer
- InterLock Ransomware (NodeSnake RAT)
- Latrodectus
- MetaStealer
- Mispadu
- Nitrogen
- StilachiRAT
- SocGholish
- SocksShell (aka Zapcat Supper)
- SparkRAT
- SQUIDGATE (TerraLoader)
- Xloader
- Xworm
- Zloader

NEWS AND RISK INFORMATION

50,000+ Azure AD users exposed via unsecured API: BeVigil uncovers critical flaw. “A critical security vulnerability was discovered in an aviation company’s infrastructure. The flaw involved an unauthenticated API endpoint embedded in a JavaScript file, which issued Microsoft Graph tokens with elevated privileges.” ([Cloudsek](#))

ASUS router backdoors affect 9K devices, persist after firmware updates. “Thousands of ASUS routers have been compromised with malware-free backdoors in an ongoing campaign to potentially build a future botnet, [GreyNoise reported on 28 May](#). Initial access is gained through a combination of credential brute-forcing and exploitation of authentication bypass flaws, which are patched but have not been assigned CVEs, according to GreyNoise.” ([SC World](#))

Cisco IOS XE bug rated 10.0: ‘Waiting is not an option. “The details about a [10.0 Cisco IOS XE Wireless LAN Controller \(WLC\) flaw](#) that [Cisco patched May 7](#) have been made public, bringing the industry closer to a working exploit and prompting security pros to tell teams to patch right away.” ([SC World](#))

Cyber attack on ConnectWise believed to be a nation-state threat actor. “Remote monitoring and management (RMM) software provider ConnectWise reported that an undisclosed nation-state actor reportedly affected 45,000 managed service provider (MSP) customers.” ([SC Media](#))

Linux zero-day vulnerability was discovered using Frontier AI. “Large language models have taken a big step forward in their ability to help chase down code flaws, said a vulnerability researcher who successfully trained OpenAI’s o3 to review Linux kernel code, leading to the LLM - in an apparent first - discovering a new zero-day vulnerability in the code.” ([Data Breach Today](#))

US DOJ seizes 4 domains supporting cybercrime crypting services in global operation. “On 27 May 2025, a coordinated international law enforcement operation led by the Department of Justice (DOJ), in collaboration with Dutch and Finnish authorities, resulted in the seizure of four publicly disclosed domains—these include AvCheck[.]net, Cryptor[.]biz, Cryptor[.]live, and Crypt[.]guru.” ([The Hacker News](#))

What is Q-Day – and are you ready for it? “Quantum computing poses a transformative and potentially devastating threat to the entire financial sector. From retail banking and asset management to payment processing and digital identity verification, the industry depends on cryptographic systems to protect sensitive data and ensure secure transactions. As quantum computers develop the ability to break widely used cryptographic algorithms such as RSA and ECC (elliptic-curve cryptography), the core security mechanisms that underpin financial operations are at risk of becoming obsolete.” ([International Banker](#))

THREATS OF THE WEEK

Special risks to small institutions highlight this week’s risks.

Special Risks for Small Institutions

Summary

Within the US financial services sector’s “community institution” ecosystem lies a crucial base of community banks and credit unions. The most recent statistics show that the US has:

- 622 federally insured credit unions with at least \$50 million but less than \$100 million in assets ([NCUA](#))
- 921 federally insured banks with at least \$50 million but less than \$100 million in assets ([FRED](#))

These institutions may have a single branch and a limited number of staff to provide financial services to their communities. Although small, they can bring financial solutions that rival larger institutions.

Size, Complexity, and Risk

To some extent, small institutions' ability to offer such services requires partnerships with third-party suppliers. Those outsourced providers, while crucial, can create challenges and increase risks for small institutions, particularly related to technology and core systems.

Third-party providers are not directly part of the client's organization so have no access to their cybersecurity mechanisms. They may have a lower level of cyber maturity than their financial sector clients as well. This can impact critical areas such as patching critical systems, backing up data, testing, monitoring, and processing threat intelligence. Limited maintenance can result in uncertainty and other inefficiencies.

Financial institutions are required to maintain third-party management programs per regulatory guidelines, but a small firm – which may have a single person overseeing vendors – may have less robust oversight.

Regardless of size, financial institutions are obligated to comply with all regulatory guidelines. Institutions can outsource support; however, institutions cannot outsource the responsibility.

Institutions should refer to their regulator's guidelines regarding third-party risk Management.

Why Does Cyber Threat Intelligence Matter?

Cyber threat intelligence gives firms information on current threats and mitigation techniques. Providers that don't or can't ingest cyber threat intelligence due to a lack of expertise leave their customers at risk of data breaches, ransomware, and other cyber threats.

FS-ISAC members receive curated, current cyber threat intelligence, among other benefits, including:

- **Access to our Intelligence Exchange** platform and vast document library containing governance, program, and risk management guidance, and all-in-one toolkits that enhance your cybersecurity initiatives without huge time commitments.
- **Collective intelligence alerts** on current fraud, physical security, and cybersecurity vulnerabilities, incidents, and threats. Dedicated channels are used during outbreaks involving affected members.
- **Customizable intelligence feeds**, providing anyone at your credit union with information the way you need and want it.
- **Communication channels** linking members so you can find solutions to diverse topics that increase efficiency and operational goals.
- **FS-ISAC Communities of Interest**, which are groups of members with an interest in or subject matter expertise on issues that impact operations, strategy, threats, and more (e.g., CyberIntel, Fraud, Payment Risk, etc.). They connect regularly to discuss specific topics, brainstorm, and produce materials that benefit the sector, their firms, and their careers.
- **Monthly member-only and special event webinars**, featuring guest speakers discussing current events. These events provide information about industry-leading practices and solutions and provide a platform to explore them with their peers.
- **Education** through exercises and training with minimal time commitment and access to a series of member-only Tabletop Exercises.
- **Security awareness and education newsletters** that can be shared with employees and members to enhance regulatory obligations.

To learn more about FS-ISAC, visit [fsisac.com](https://www.fsisac.com).

THREAT INTELLIGENCE UPDATE

Vishing Campaigns

Customer relationship management systems are being targeted.

Summary

In early April 2025, FS-ISAC began tracking suspicious activity likely associated with the threat actor group known as Scattered Spider. Since then, FS-ISAC has published three alerts from members who were targeted in social engineering through voice phishing (vishing) attacks.

These submissions involved tactics, techniques, and procedures (TTPs) consistent with those used by Scattered Spider. The primary objective of these attacks is almost certainly the exfiltration of data from the organization's Salesforce environment. However, the purpose of the activity beyond this initial stage is unconfirmed.

The social engineering scam appears to follow the same pattern. First, the threat actor uses Mullvad VPN to conduct reconnaissance to determine if a potential target organization uses Salesforce. If the organization does, the threat actor calls the firm, using a phone number available to the public, posing as an internal IT helpdesk support staffer, requesting help from an employee to close out a ticket.

Then the threat actor tricks the employee into linking an external application, likely a modified Data Loader application, to the Salesforce tenant. Once the application is connected, the threat actor attempts to exfiltrate data.

Risk

Customer relationship management (CRM) systems like Salesforce are prime targets for threat actors due to their valuable company and confidential customer information.

Remediation

To prevent data exfiltration, institutions should use multi-factor authentication (MFA) configurations and IP restrictions.

FS-ISAC members may read the entire report [here](#).

JUST FOR COMMUNITY INSTITUTIONS

New Guidance for SIEM and SOAR Implementation

Summary

Community institution members frequently discuss Security Information and Event Management (SIEM) implementation within their organizations. On 27 May, the Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Australian Signals Directorate's Australian Cyber Security Centre and other international and US partners, released new guidance for organizations seeking to procure SIEM and Security Orchestration, Automation, and Response (SOAR) platforms.

This guidance includes the following three resources:

- **Implementing SIEM and SOAR Platforms – Executive Guidance** outlines how executives can enhance their organization's cybersecurity framework by implementing these technologies to improve visibility into network activities, enabling swift detection and response to cyber threats.
 - **Implementing SIEM and SOAR Platforms – Practitioner Guidance** focuses on how practitioners can quickly identify and respond to potential cybersecurity threats, leveraging these technologies to streamline incident response processes by automating predefined actions based on detected anomalies.
-

- **Priority Logs for SIEM Ingestion – Practitioner Guidance** offers insights for prioritizing log ingestion into a SIEM, ensuring that critical data sources are effectively collected and analyzed to enhance threat detection and incident response capabilities tailored for organizations.

Institutions should review the guidance to determine if implementation will strengthen their cybersecurity maturity.

For access to the guidance documents, please visit CISA's [SIEM and SOAR Resource page](#).

RESILIENCE UPDATE

CAPS is Coming!

Summary

The 18th annual CAPS exercise season is scheduled for 2 September through 17 October 2025. More to come on registration, promotions, email signature, materials, etc.

What is CAPS?

The CAPS exercise is conducted onsite, and FS-ISAC provides each participating firm with materials and guides. It challenges your institution's incident response team to evaluate a fictional organization's response to overcome a simulated attack against operations and processes. Participants practice mobilizing quickly, working under pressure, critically appraising information as it becomes available, and connecting the cyber-dots to defend against an attack. One individual registers and leads your internal team through the exercise. The exercise follows a realistic, timely scenario involving a fictional organization.

Registered members receive an after-action report and aggregate unattributed data, and results are evaluated by the organization.

A quick note on what's new and exciting for 2025 CAPS:

- The exercise will be in one part, allowing us to streamline and tighten the material (while still making it enjoyable and useful), remove redundancies, and be more attractive to management and additional attendees.
- We are improving the survey and welcoming user feedback.
- We're introducing a big change in 2025: we intend to generate dialogue with AI voices vs. volunteer actors.
- We plan to offer a Spanish-language version.
- Registrants will access all CAPS materials in one of three CAPS VIDEO channels. Q&A will be available in a separate Connect channel.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- [Navigating Cyber 2025](#)
- [Cyber Fraud Prevention Framework for Financial Institutions](#)
- [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

- [FS-ISAC Security](#). CIAC Director Jeffrey Korte discusses the value to small institutions
- [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

- 3 June 2025 | FinCyber Today Canada
- 16 June | May CIAC Meeting
- 25 June | June CIAC Open Forum
- 25 June | Member Success Session
- 5-8 October | Americas Fall Summit **[Registration now open]**

[View all Americas events.](#)

TLP GREEN 

© FS-ISAC 2025



12120 Sunset Hills Rd, Reston
VA 20190

To manage emails you may receive, please log in to the Member Services platform of the Intelligence Exchange to [update subscription preferences](#).