FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 20 October 2025 | Issue 305

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 its ability to operate and avoid compliance, economic, legal, regulatory, and reputational impact.

This Week's Threats

Fraud Campaigns

- Business Email Compromise
- CEO Impersonation
- Customer Impersonation (Call Center)
- Fraudulent Mobile Remote Check Deposits

System Vulnerabilities

Adobe, Amazon, Apple, Atlassian, ASKI Energy, AutomationDirect, Avaya, CA OPS/MVS, Danz Monitoring, Debian, Dell, Delta Electronics, F5 (BIG-IP), Fortinet, F5OS, GitLab, Google, Hitachi, IBM, ISC BIND, JD Edwards, Kentico, LanScope, Lenovo, Linux, Microsoft, Motex, Mozilla, MySQL, NIHON KOHDEN, OpenJDK, Oracle, Red Hat, Raisecomm, Rockwell Automation, SAP, Schneider Electronics, Siemens, TP-Link, Ubuntu, Veeder-Root, and WatchGuard.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: 1st New Home, Adult Dating, Costco, Digital Confirmation, DocuSign, Documents Pending eSign Review, E*TRADE, Fake Contract, Follow The Instructions!, Fundraising Event, Help Desk, Indelpower Request Ack, Invoice, J Black and Associates Inc, Jordan Black shared, Kristin Teffeau shared, LEGAL BID TRANSCRIPT FOR YOU, LinkedIn, Miles Mediation And Arbitration, Online Statement, Outstanding Payment Notice, Oxford Nanopro, Payment Request, Payroll Diversion, Quick Follow-Up, Revised Approved Statement, REVISED CONTRACT PROPOSAL, Sharefile, SharePoint, Tax Administration Service, UNITED WAY OF NEW YORK COUNTY DOCUMENTT, Urgent, Voicemail Message From Directmedicalinc, WhatsApp, You were invited to sign and review the following document, and Zimbra.

Threats, Malware, Cyber Campaigns, and Adversaries

- Amatera Stealer
- Astaroth
- Agent Tesla
- AsyncRAT
- Aura Stealer
- BeaverTail
- DarkCloud
- Dark Crystal
- GolangGhost
- GULoader
- Netsupport RAT
- NitroBunnyDownloader
- Oyster
- Rhadamanthys Stealer
- Remcos
- SHADOWPAD
- Snakeloader
- SocksShell
- Vanguard Stealer
- WarmCookie

- Latrodectus
- LummaStealer
- Metamorfo
- Xloader
- Xworm
- ZgRAT
- ZPHP

NEWS AND RISK INFORMATION

A critical WatchGuard Fireware flaw could allow unauthenticated code execution. ”The vulnerability is an out-of-bounds write issue that affects Fireware OS versions 11.10.2–11.12.4_Update1, 12.0–12.11.3, and 2025.1 … This vulnerability ticks all the boxes ransomware actors crave: remote code execution on a perimeter device, exposure via a public-facing VPN service, and pre-auth exploitability, making it a high-priority target for exploitation and urgent to patch.” (Security Affairs)

ConnectWise fixes Automate bug allowing AiTM update attacks. “ConnectWise released a security update to address vulnerabilities, one of them with critical severity, in Automate product that could expose sensitive communications to interception and modification.” (Bleeping Computer)

New phishing emails pretend to offer jobs to steal Facebook logins. “Targets are lured with fake job postings, mainly for Social Media Manager roles … the methodology remained the same across all emails, which suggests the scammers used a template or an LLM (Large Language Model) to quickly launch a varied wave of attacks.” (HackRead)

North Korean hackers combine BeaverTail and OtterCookie into Advanced JS Malware. “The North Korean threat actor linked to the Contagious Interview campaign has been observed merging some of the functionality of two of its malware programs, indicating that the hacking group is actively refining its toolset.” (Hacker News)

PolarEdge targets Cisco, ASUS, QNAP, and Synology routers in expanding botnet campaign. “PolarEdge was first documented by Sekoia in February 2025, attributing it to a campaign targeting routers from Cisco, ASUS, QNAP, and Synology with the goal of corralling them into a network for an as-yet-undetermined purpose.” (Hacker News)

Russian hackers evolve malware pushed in "I am not a robot" captchas. “The Russian state-backed Star Blizzard hacker group has ramped up operations with new, constantly evolving malware families (NoRobot, MaybeRobot) deployed in complex delivery chains that start with ClickFix social engineering attacks.” (Bleeping Computer)

THREAT OF THE WEEK

Windows SMB flaw and CAPI backdoor vulnerability highlight this week’s risks.

Windows SMB Flaw Under Active Attack

Summary

“The Cybersecurity Infrastructure and Security Agency (CISA) has reported that threat actors are actively exploiting a high-severity Windows SMB vulnerability (CVE-2025-33073). This flaw, which allows attackers to gain SYSTEM privileges on unpatched systems, affects all versions of Windows Server, Windows 10, and Windows 11 (up to version 24H2). Microsoft patched the vulnerability in June 2025, attributing its cause to improper access control. CISA has added the flaw to its Known Exploited Vulnerabilities (KEV) Catalog and mandated that federal agencies patch their systems by November 10, 2025.” (Cyware)

Phishing Campaign Unleashes CAPI Backdoor

Summary

“A new .NET malware, CAPI Backdoor, targets the Russian automobile and e-commerce sectors via phishing emails with ZIP files. The ZIP files contain a decoy Russian document and a malicious Windows shortcut (LNK) file that triggers the malware. The malware leverages a legitimate Microsoft binary (rundll32.exe) to execute its payload stealthily. CAPI Backdoor collects system information, steals browser data, takes screenshots, and exfiltrates data to a remote server.” (Cyware)

Remediation

Institutions should include the following preventive and remedial measures for a CAPI Backdoor infection:

- **Filtering email:** Implement advanced email filtering to block spear-phishing attempts.
- **Security awareness training:** Share current phishing exploits and advise employees where to report incidents.
- **Threat monitoring:** Use FS-ISAC threat intelligence feeds to raise protective shields and monitor for network connections to known indicators of compromise.
- **Endpoint security:** Deploy Endpoint Detection and Response (EDR) tools to detect and block suspicious processes and behaviors.
- **Restricting execution:** Block the execution of unauthorized .NET binaries and restrict the use of living-off-the-land (LotL) binaries from temporary paths.
- **Patching systems:** Maintain updates for all antivirus software and operating systems.

THREAT INTELLIGENCE UPDATE

Pixnapping Leaks Information Displayed On The Screen

Summary

Researchers have found that a new class of attacks called “pixnapping” allows a malicious Android app to stealthily leak information displayed by other Android apps or websites. A pixnapping attack against Google Authenticator, conducted by researchers, allowed malicious apps to steal two-factor authentication codes in less than 30 seconds. Pixnapping exploits Android Application Programming Interfaces (APIs) and a hardware side channel that affects nearly all modern Android devices.

Android Versions Impacted

Pixnapping affects five devices running Android versions 13 to 16 (up until build id BP3A.250905.014): Google Pixel 6, Google Pixel 7, Google Pixel 8, Google Pixel 9, and Samsung Galaxy S25 are vulnerable. It is not known whether Android devices from other vendors are affected by pixnapping. However, the core mechanisms enabling the attack are typically available in all Android devices.

Vulnerable Information

When the target app is open, the malicious app can steal any images onscreen – including chat messages, two-factor authentication codes, email messages, etc. – using pixnapping. It is unknown if pixnapping is being used in the wild.

Remediation

End users should apply current patches.

Resources

A pixnapping paper will appear in the 32nd ACM Conference on Computer and Communications Security (Taipei, Taiwan; 13-17 October 2025). A preliminary report on pixnapping can be read at https://www.pixnapping[.]com.

JUST FOR COMMUNITY INSTITUTIONS

An Alert for Mid-Sized Credit Unions

Summary

During the recent FS-ISAC Fall Americas Summit, Nate Wright, Threat Intelligence Analyst at SECU, presented on credit union (CU) breaches, revealing that medium-sized CUs have been breached more frequently than any other size CU. Wright provided detailed information going back to 2022, compiled from credible and high-confidence resources (e.g., notifications, state reporting, class action lawsuits, etc.).

Determining Asset Size

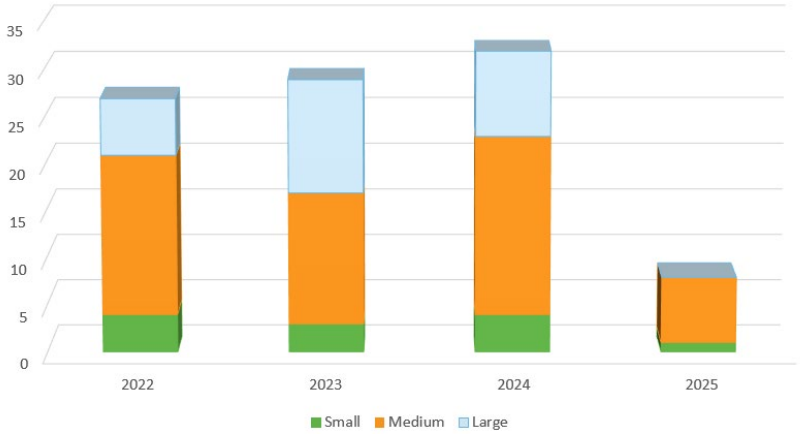
The National Credit Union Association qualifies small CUs as those with assets below $50M and large CUs as those with assets above $10B. Medium-sized CUs lie between the two.

Breach Increase Since 2022

The table below reveals that breaches have consistently increased year by year, with a noticeable uptick over the past 12 months (18% increase from 2022 to 2024). Because small CUs claim only 1% of all assets, they are probably less attractive to threat actors than medium-sized CUs, which have a broader footprint and are a more lucrative target for threat actor campaigns.

Breaches by CU Size Since 2022

- Small CUs = 13%
- Medium CUs = 59%
- Large CUs = 28%



Threat Actor Groups

Of the 96 successful breaches in the research, analysis linked 31 incidents to 22 different threat actor groups (TAG).

Most of the CUs were breached by TAGs established after 2021. Twenty of the 22 TAGs emerged since 2021, nine of which formed in 2023. That means at least nine TAGs have conducted a CU breach within two years of being established. Both old and new groups successfully breached medium-sized CUs at a high rate.

The increase in attributed breaches year over year could be due to the rise in the number of breaches overall. It is also possible that reporting to media and state/federal agencies – which is often mandatory – has increased.

The Rest of the Story

- New TAGs conduct breaches against CUs at a higher rate.
- Older TAGs stick with small- to medium-sized CUs.
- Newer TAGs attack larger CUs at a higher rate.
- Both old and new TAGs actively target medium-sized CUs.
- Increase in newer TAG activity correlates with older TAG disruptions.

Key Takeaways From the Presentation

- It's essential to understand the threat landscape.
    - It informs you about current threat activity.
    - It helps you understand common tactics, techniques, and procedures.
    - It gives you a broader perspective than your own environment.
    - Sharing threat intelligence enables you to adjust security controls to meet active threats.
- The sector needs more reporting around breaches.
    - More information clarifies risks and threats.
- Each institution's posture and needs are different.

FS-ISAC members can watch the entire presentation in the CIAC Video Channel.

REGULATORY AND GOVERNMENT UPDATES

Sector Financial Institution Letter and Other Announcements

FRB:

- Federal Reserve Board denies application by Canandaigua National Corporation, 17 October.
- Agencies announce withdrawal of principles for climate-related financial risk management, 16 October.

FDIC:

- FIL-49-2025, Rescission of Principles for Climate-Related Financial Risk Management for Large Financial Institutions, 16 October.

NCUA:

- NCUA Proposed Rulemaking Takes Further Action to Solidify Removal of Use of Reputation Risk, 20 October.

OCC:

- OCC 2025-34, Risk Management: Rescission of Principles for Climate-Related Financial Risk Management for Large Financial Institutions, 16 October.

RESILIENCE UPDATE

AWS Outage

Summary

A prominent Amazon Web Services (AWS) outage caused widespread internet disruptions on 20 October, taking down dozens of popular apps, games, and websites, including Signal, Roblox, Canva, Duolingo, and Ring.

The issue appeared to be related to DNS resolution of the DynamoDB API endpoint in US-EAST-1. This issue also affected other AWS Services in the US-EAST-1 Region. Global services or features that rely on US-EAST-1 endpoints, such as IAM updates and DynamoDB Global tables, experienced service disruptions. AWS continues to recover and resolve the issue.

The latest updates on the recovery can be viewed on the AWS Health Dashboard. If your company is experiencing impacts or challenges from the AWS outage, please share in the AMER BRC CONNECT channel.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- 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.

- 29 October | CIAC and COFFE Open Forum
- 31 October | Member Success Webinar
- 12 November | Executive Protection Council Meeting
- 17 November | Monthly CIAC Webinar
- 19 November | CIAC and COFFE Open Forum

View all Americas events.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190