FS-ISAC | Risk Summary Report

Global Cyber Threat Level 🛡 | **Americas:** 🛡 **EMEA:** 🛡 **APAC:** 🛡

Week of 15 September 2025 | Issue 300

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

- ACH Wire Fraud
- Business Email Compromise
- Fraudulent Withdrawals (Call Center)
- SEO Poisoning

System Vulnerabilities

Adobe, Amazon, Apple, Atlassian, Avaya, Azure, BMC Control, Cisco, Cognex, Cygwin, Daikin, Dassault Systèmes, Debian, Dell, Delta Electronics, Dover, End-of-Train & Head-of-Train, F5, GitLab, Google, HP, Hitachi, HPE, IBM, Ivanti, Jenkins, Lenovo, Linux, Microsoft, Mozilla, Oracle, Red Hat, Samsung, SAP, Schneider Electric, Siemens, Spring Security, SUSE, Symantec, Ubuntu, WatchGuard, and Westermo Network Technology.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: 2024 Employee W-2 Forms Request, 2025 Employee Account information, Account Request, Adobe, Appraisal Details, Account on hold, Adult Dating, Amazon, AppleID, Cryptocurrency, Daiwa Securities, Document Signature, Download your Statement, Fake Calendar Invitations, Fake Calendar Invitations, Fake Invoice, Fake Updates, FedEx, Final Reminder: Benefits Enrollment, Gift Card, Microsoft 365 security: You have messages in quarantine, New VoiceMail Notification, messages-noreply (RingCentral voicemail), RFQ, Palmer & Cay.WAV, Palmera Consulting, Payment Pending Review, Payroll (HR), Purchase Order, QR Code, Quotation/Shipment, Unauthorized Transaction, Updated Document: Revised Salary & Benefits Chart Structure – Secure Access, Southeastern Lighting Solutions, Time to Close the Loop – Invoice [U0857] Past Due, Updated Employee Package: Salary Increase, Benefits, Voicemail, You Received a New Document, and Your video is not available for all users.

Threats, Malware, Cyber Campaigns, and Adversaries

- AdaptixC2
- Amatera Stealer
- Astaroth
- Agent Tesla
- AsyncRAT
- Aura Stealer
- BeaverTail
- BitStep RAT
- CHILLYHELL
- LummaStealer
- MultiRat
- Netsupport RAT
- Nitrogen Loader
- NotDoor
- Oyster
- Rhadamanthys Stealer
- Remcos
- SHADOWPAD

- Dark Crystal
- GolangGhost
- GULoader
- HardHat RAT
- ICEBITE.PYTHON
- KeyPlug
- KongTuke Malware
- LAMEHUG
- Latrodectus
- SocGholish
- SocksShell
- SparkRAT
- SquidLoader
- Vanguard Stealer
- VMScape
- Xloader
- Xworm
- ZynorRAT

NEWS AND RISK INFORMATION

AI-forged military IDs used in North Korean phishing attack. “The phishing campaign involved emails impersonating a South Korean defense-related institution, claiming to manage ID issuance for military personnel. These emails contained malicious attachments.” (Information Security)

AI-powered Villager pen testing tool hits 11,000 PyPI downloads amid abuse concerns. “Villager’s AI-driven architecture enables large-scale, parallelized exploitation … The fact that Villager is available as an off-the-shelf Python package means it offers attackers an easy way to integrate the tool into their workflows.” (Hacker News)

Akira ransomware affiliates continue breaching organizations via SonicWall firewalls. “Over a year after SonicWall patched CVE-2024-40766, a critical flaw in its next-gen firewalls, ransomware attackers are still gaining a foothold in organizations by exploiting it … The July 2025 surge in attacks was, according to SonicWall, facilitated by the fact that organizations had migrated from Gen 6 to Gen 7 firewalls but did not reset local user passwords (as advised by the firewall maker).” (Help Net Security)

EvilAI operators use AI-generated code and fake apps for far-reaching attacks. “EvilAI is a sophisticated malware campaign leveraging AI-generated code and social engineering to distribute trojans disguised as legitimate applications. These fake apps feature professional interfaces and valid digital signatures.” (Trend Micro)

Google, Microsoft account takeover made easy via VoidProxy. “VoidProxy is a PhaaS platform actively used by multiple cybercriminal groups to hijack Microsoft and Google accounts. It targets a wide range of victims, from SMBs to large enterprises, and facilitates real-time theft of credentials.” (The Register)

Scattered Spider resurfaces with financial sector attacks despite retirement claims. “Cybersecurity researchers have tied a fresh round of cyber attacks targeting financial services to the notorious cybercrime group known as Scattered Spider, casting doubt on their claims of going "dark." Threat intelligence firm ReliaQuest said it has observed indications that the threat actor has shifted their focus to the financial sector. This is supported by an increase in lookalike domains potentially linked to the group that are geared towards the industry vertical, as well as a recently identified targeted intrusion against an unnamed US banking organization.” (Hacker News)

THREAT OF THE WEEK

Phishing campaigns and VoidProxy highlight this week’s risks.

Phishing campaigns exploit RMM tools for access

Summary

For the past three weeks, threat actors have initiated various phishing campaigns to install malware.

Use of RMM Software

Red Canary reports, “malicious actors are increasingly using phishing campaigns to install RMM software on victim machines. These campaigns exploit various lures, including fake browser updates that prompt users to download the ITarian RMM tool, misleading meeting invites that install Atera or PDQ software, and deceptive party invitations that deliver RMM tools via trusted domains like Cloudflare R2. Additionally, government forms such as W-9s and tax returns are used to entice victims into installing malicious software … threat actors leverage compromised websites and malicious domains to manage large-scale malware campaigns.”

VoidProxy: New Phishing Threat Bypasses MFA

Summary

A new Phishing-as-a-Service (PhaaS) platform named VoidProxy, which controls Adversary-in-the-Middle (AitM) tactics, is crossing the horizon.

VoidProxy is designed to compromise Microsoft and Google user accounts by bypassing multi-factor authentication.

According to Cybersecurity News, “Early email lures originate from compromised legitimate Email Service Provider (ESP) accounts to evade spam filters and include multiple redirects through URL shortening services.

Before loading any page, victims must pass a Cloudflare CAPTCHA challenge to confirm human interaction. Automated scanners or security tools receive a generic welcome page, effectively neutralizing most analysis platforms.

Once the victim passes the challenge, the browser communicates with a Cloudflare Worker service responsible for filtering traffic and loading the appropriate phishing portal.”

AitM Attacks

- First, threat actors position their device as a server proxy between a user and a legitimate website.
- Then they steal information when the user attempts to log in using their credentials.
- Finally, the session is hijacked, and the threat actor gains access with a stolen session cookie, bypassing the need to re-authenticate or use MFA.

Risk

VoidProxy’s AitM engine's prowess can intercept session cookies and session tokens in real time.

Remediation

Institutions should implement targeted detection rules and enforce stronger resistant authentication methods.

THREAT INTELLIGENCE UPDATE

Data Theft and Extortion - Cybercriminal Groups UNC6040 and UNC6395

FBI releases a Flash Alert related to Salesforce.

Summary

On 12 September, the FBI issued a Flash Alert regarding cybercriminal groups targeting Salesforce platforms for data theft and extortion. The FBI identified two groups, UNC6040 and UNC6395, using different initial access methods to compromise Salesforce instances to conduct data theft and extortion.

- Since October 2024, UNC6040 threat actors have obtained initial access by leveraging social engineering attacks, in particular voice phishing (vishing), to gain access to organizations’ Salesforce accounts. To do so, UNC6040 threat actors commonly call victims’ call centers posing as IT support employees, addressing enterprise-wide connectivity issues. Under the guise of closing an auto-generated ticket, UNC6040 actors trick customer support employees into taking actions that grant the attackers access or lead to the sharing of employee credentials, allowing them access to targeted companies' Salesforce instances to exfiltrate customer data.

- UNC6040 threat actors have utilized phishing panels, directing victims to visit from their mobile phones or work computers during the social engineering calls. After obtaining access, UNC6040 threat actors have then used API queries to exfiltrate large volumes of data in bulk.
- UNC6040 threat actors have also directly requested user credentials and multifactor authentication codes to authenticate and add the Salesforce Data Loader application, facilitating data exfiltration.
- In August 2025, UNC6395 exploited compromised OAuth tokens from the Salesloft Drift application to access Salesforce instances. Following the incident, Salesloft and Salesforce revoked all active tokens to terminate unauthorized access.

The Flash Alert lists specific IP addresses and URLs associated with both groups, advising organizations to investigate these indicators before taking action.

Remediation

Institutions should train employees to recognize phishing attempts and implement phishing-resistant multi-factor authentication. Other defenses include:

- Enforcing the Principle of Least Privilege for user accounts.
- Monitoring API usage for unusual behavior.
- Regularly reviewing third-party integrations.
- Rotating API keys and credentials to enhance security.

Read the entire Flash Alert.

JUST FOR COMMUNITY INSTITUTIONS

Q4 Commercial Services Security Newsletter

Summary

FS-ISAC's Commercial Services Security Newsletter will be available to members via email or download in CONNECT on 3 October.

About the Newsletter

Small and midsized businesses face the same cyber and security risks as larger organizations, but don't have the staffing larger institutions do. The Commercial Services Security Newsletter offers security awareness content to community institutions, treasury management, and commercial service teams to share with their clients in smaller businesses.

The Commercial Services Security Newsletter not only helps small-business owners understand the changing cyber threat landscape, but it also provides FS-ISAC members with a way to connect with their commercial clients around banking services that enable those clients to bank more securely.

The Commercial Services Security Newsletter is TLP Green and can be shared with your employees and commercial clients. It cannot be posted on public-facing websites.

FS-ISAC also produces a Security Tips Newsletter, which is distributed on the first Friday of each month via email, CONNECT, and SHARE. The Security Tips Newsletter can be freely shared amongst employees, customers/and members.

Members can join the CIAC by visiting the Member Services app within IntelX and making additions using the Member Experience link.

REGULATORY AND GOVERNMENT UPDATES

The FDIC, OCC, and NCUA Provide Updates

FDIC

- FIL-42-2025 - The FDIC Updates its Enforcement Actions Manual regarding Minimum Standards for Termination of Cease-and-Desist and Consent Orders

NCUA

- NCUA Releases Q2 2025 State-level Credit Union Data Report. Read the entire press release.
- NCUA Board Briefed on Share Insurance Fund. Read the entire press release.

OCC

- OCC 2025-23 - Protecting Customer Financial Records
- OCC 2025-22 - Licensing and Community Reinvestment Act: Consideration of Politicized or Unlawful Debanking

FRAUD UPDATE

SEO Poisoning

Summary

GhostRedirector is a previously unknown and possibly China-based hacker group that has compromised up to 65 worldwide Windows servers, according to an article in The Record.

Using fraudulent search engine optimization (SEO), the scheme is likely aimed at promoting gambling websites. While these may be opportunistic attacks, customers and members using their debit cards could potentially file a Reg E claim, which can impact departments handling those claims operationally.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- 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
- The Business Information Security Officer
- Quarterly Threat Trends Report - Q2 2025
- From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector
- 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

See the full 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.

- 2 September-17 October | CAPS for Community Institutions
- 24 September | CIAC and COFFE Open Forum
- 24 September | Member Success Webinar
- 5-8 October | Americas Fall Summit
- 20 October | Monthly CIAC Webinar

View all Americas events.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190