FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 3 November 2025 | Issue 307

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
- CEO Impersonation

System Vulnerabilities

Advantech, Amazon, Android, Apache, Apple, Atlassian, Avaya, Broadcom, CA OPS, Cisco, CWP, CyberArk, Debian, Dell, Delta Electronics, Elastic, F5, Fuji Electric, Gladinet CentreStack and Triofox, Google (and Workspace), Hitachi, HP, IBM, IDIS, International Standards Org., Lenovo, Linux, Microsoft, Mozilla, .NET Core, Oracle, Progress, Proofpoint, Radiometrics, Red Hat, Samsung, Survision, Ubia FLXeon, Ubuntu, VMWare, WordPress, XWiki, and z/OS.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Adobe Acrobat Reader, Audit Compliance, eTrade, Fake Invoice, Gift Card, New Submission, Project Review, Proposal Invitation, QR Code Outlook Invitation, SendGrid, and Teams Call.

Threats, Malware, Cyber Campaigns, and Adversaries

- AdaptixC2 Beacon
- Amatera Stealer
- Astaroth
- Agent Tesla
- AsyncRAT
- Aura Stealer
- BeaverTail
- ColdRiver
- CodeTail
- DarkCloud
- Dark Crystal
- DeskRAT
- GolangGhost
- GULoader
- ICEBITE (PylangGhost)
- Latrodectus
- LummaStealer
- Metamorfo
- Netsupport RAT
- NitroBunnyDownloader
- Oyster
- Rhadamanthys Stealer
- Remcos
- SHADOWPAD
- Snakeloader
- SocksShell
- Vanguard Stealer
- WarmCookie
- Xloader
- Xworm
- ZgRAT
- ZPHP

NEWS AND RISK INFORMATION

Bronze Butler exploits Lanscope zero-day. “The China-linked Bronze Butler (Tick) threat group exploited a zero-day vulnerability (CVE-2025-61932) in Motex LANSCOPE Endpoint Manager to gain unauthorized access and steal confidential information. This vulnerability enabled attackers to execute arbitrary commands with SYSTEM privileges. The group utilized Gokcpdoor malware, which established a command-and-control connection, and the Havoc C2 framework for remote access. Additionally, they employed legitimate tools like goddi, remote desktop applications, and 7-Zip for lateral movement and data exfiltration, leveraging cloud storage services for their operations.” (Cyware)

China-linked hackers exploit Windows shortcut flaw to target European diplomats. “A China-affiliated threat actor known as UNC6384 has been linked to a fresh set of attacks exploiting an unpatched Windows shortcut vulnerability to target European diplomatic and government entities between September and October 2025.” (Hacker News)

Cloud identity exposure is 'a critical point of failure.' “Attackers keep hammering cloud-based identities to help them bypass endpoint and network defenses, logging in using inadvertently exposed credentials - or ones harvested through infostealers - then escalating access thanks to over-permissioned accounts, experts warn.” (Data Breach Today)

EU to propose Quantum Act to govern and scale quantum capabilities. “The European Union is actively shaping the digital future of its financial sector through a series of landmark regulatory initiatives. While the Digital Operational Resilience Act (DORA) and the Artificial Intelligence (AI) Act are already major focuses for banks, the upcoming Quantum Act signals a new, strategic dimension to technological governance.” (Moody’s)

Financial services can’t shake security debt. “Researchers analyzed data from more than 1.3 million applications and 126 million security findings. Financial institutions perform better than average at preventing severe vulnerabilities, but they are slower to fix them and carry more long-term security debt than most other sectors.” (Help Net Security)

Leak site ransomware victims spike 13% in a year. “A review of data leak sites over the period September 2024-August 2025 revealed a double-digit annual increase in European victims, to 1,380. After the UK, Germany, Italy, France, and Spain were the most targeted nations.” (Information Security)

New infostealer claims to extract 99% of credentials in 12 seconds. “Advertisements for the malware-as-a-service (MaaS) known as logins[.]zip were first observed by Hudson Rock researchers this month ... Logins[.]zip targets a wide range of credentials by combining both Windows DPAPI and browser exploits, potentially putting login details, cookies, and payment card details at risk.” (SC Media)

Ribbon discloses breach. Ribbon Communications, a leading US-based provider of cloud services, communications software, and network solutions, publicly disclosed a data breach by an unspecified nation-state threat actor. Unauthorized access was discovered in September 2025, and initial access may have occurred as early as December 2024. Ribbon Communications noted finding no evidence to date that intruders accessed customer systems. However, according to the disclosure, unspecified customer files on two laptops, which were saved outside of Ribbon’s main network, were accessed. While the investigation is ongoing, impacted customers have reportedly been notified. (FS-ISAC)

US Homeland Security Committee warns of rising cyber threats, as federal shutdown and lapsed law hamper defenses. “The US House Committee on Homeland Security published an updated ‘Cyber Threat Snapshot,’ outlining the heightened threats posed by malign nation-states and criminals to US networks and critical infrastructure since 2024. The Homeland Security Committee snapshot identified that this gap in federal cyber capacity comes at a moment when cyber actors affiliated with the People’s Republic of China (PRC) are expanding their targeting of US networks.” (Industrial Cyber)

THREAT OF THE WEEK

Airstalk and Microsoft Azure highlight this week’s risks.

Airstalk Malware

Summary

It is suspected that nation-state actors are distributing a new malware dubbed Airstalk.

What is Airstalk?

Palo Alto's Unit 42 has compiled the most current intelligence about this new malware, stating it abuses the legitimate AirWatch API for mobile device management (MDM) to create a covert command-and-control (C2) channel and exfiltrate sensitive data.

Unit 42 reports that Airstalk "disguises C2 traffic as legitimate MDM communications, making it difficult to detect with traditional network monitoring tools. The malware uses the custom device attributes feature as a 'dead drop' to pass messages between the infected host and the attackers."

Risk

The malware targets cookies, browsing histories, bookmarks, credentials, screenshots, and list files on Google Chrome, Microsoft Edge, and the Island Browser (the .NET variant) and exploits trusted third-party integrations and legitimate enterprise tools for malicious purposes.

Remediation

Network defense, good cyber hygiene, and awareness are strongly encouraged. It is also recommended that financial services firms institute:

• Patch management • Multifactor authentication • Endpoint security protection • Network security and segmentation • Mobile device management	• Behavior monitoring and threat hunting • Browser security • End-user awareness • Data backup • Incident response plan review • Isolation of compromised devices

Microsoft Azure Front Door Outage

Summary

Microsoft reported that starting approximately 15:45 UTC on 29 October, services leveraging the Azure Front Door (AFD) cloud content delivery network experienced latencies, timeouts, and errors.

Microsoft confirmed that an inadvertent configuration change triggered the event. The AFD impact was confirmed as mitigated by 00:05 UTC on 30 October. Widespread outages were reported for companies accessing Azure and Microsoft 365 services across all industries worldwide.

During the initial stages of the outage, media outlets also reported disruptions to Amazon Web Services. However, Amazon confirmed no outage occurred, with erroneous reports likely due to misattribution or multi-cloud interdependencies.

THREAT INTELLIGENCE UPDATE

Microsoft Exchange Server Security Best Practices

Summary

The Cybersecurity Infrastructure and Security Agency (CISA) and the National Security Agency collaborated with international cybersecurity partners to develop Microsoft Exchange Server Security

Best Practices, a guide to help network defenders harden on-premises Exchange servers against exploitation by malicious actors.

Organizations with unprotected or misconfigured Exchange servers remain at high risk of compromise. Persistent threat activity has been observed targeting vulnerable Exchange servers, including versions that have reached end-of-life.

Best practices include a focus on hardening user authentication and access, ensuring strong network encryption, and minimizing application attack surfaces. Organizations that implement these practices can significantly reduce their risk from cyber threats.

JUST FOR COMMUNITY INSTITUTIONS

Akira Ransomware

Summary

The ransomware-as-a-service (RaaS) Akira has been targeting three credit unions and Apache OpenOffice since July. Four weeks ago, Industrial Cyber reported that “Akira ransomware attacks escalated worldwide, primarily targeting SonicWall SSL VPN devices.”

Validate Security Controls

In addition to applying mitigations, the Federal Bureau of Investigation (FBI), CISA, the European Cybercrime Centre (EC3), and the National Cyber Security Centre for the Netherlands (NCSC-NL) recommend exercising, testing, and validating security programs against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework.

Prevention and Remediation

The top three leading practices:

1. Prioritize remediating known exploited vulnerabilities.
2. Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, virtual private networks (VPN), and accounts that access critical systems.
3. Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.

Additional action items:

- Revisit incident response and recovery plans.
- Ensure password guidelines adhere to industry best practices (i.e., those of the National Institute of Standards and Technology).
- Consider network segmentation.
- Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.
- Filter network traffic.
- Install, regularly update, and enable real-time detection for antivirus software on all hosts.
- Review domain controllers, servers, workstations, and active directories for new and/or unrecognized accounts.
- Audit user accounts with administrative privileges and configure access controls according to the principle of least privilege.
- Disable unused ports.
- Consider adding an email banner to emails received from external senders.
- Disable hyperlinks in received emails.
- Disable command-line and scripting activities and permissions.
- Maintain offline backups of data and ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization’s data infrastructure.

FRAUD UPDATE

FBI Holiday Fraud Scam Warning

Summary

Fraudsters exploit the holiday season to scam busy, distracted shoppers. The FBI has issued a press release to help consumers avoid fraud, which firms may want to share with their customers or members.

The release details several kinds of fraud, including:

- **Non-delivery scams:** goods are paid for but not shipped
- **Non-payment scams**: goods are shipped to the purchaser, but not paid for
- **Auction fraud:** misrepresentation of a product on an auction site

Protection Recommendations

- Practice good cybersecurity hygiene
- Be sure the merchant (or buyer) is legitimate
- Use safe payment methods.
- Monitor the shipping process.

Read the entire FBI press release for more information.

Quarterly Fraud Trends Report - Q3 2025

Summary

The FS-ISAC Quarterly Fraud Trends Report - Q3 2025 is now available on SHARE. The Report covers the period from 1 July to 30 September 2025 and provides an overview of fraud trends by region, sub-sector, technique, and sub-technique, with highlights from notable member submissions.

REGULATORY AND GOVERNMENT UPDATES

Sector Financial Institution Letter and Other Announcements

FDIC

- FIL-51-2025 | Supervisory Relief to Help Financial Institutions and Facilitate Recovery in Areas of Alaska Affected by Severe Storms, Flooding, and Remnants of Typhoon Halong, 6 November

FRB:

- Federal Reserve Board finalizes changes to its supervisory rating framework for large bank holding companies, 5 November

NCUA:

- Reminder | NCUA Currently Accepting CDRLF Grant Applications Through Mid-December, 3 November

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.

- 10 November | Protecting Consumers Across Channels: Building the Trust Network of the Future
- 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