FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 27 October 2025 | Issue 306

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, Apache, ASP, Avaya, Check Point, Dassault Apriso, Debian, Dell, F5, Google, Hitachi, HP, Jenkins, IBM, Lenovo, Linux, Microsoft, Motex, Oracle, Red Hat, Schneider Electronics, Ubuntu, Vertikal, and WatchGuard.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Advisory - Outstanding Bill, Aging Report, Best Contact Method, CompleteDocsOnline, Dassault Systèmes, Executive Bill, Florida Beef Council invoice, Loan Statement and Closing Doc, New Invoice, Payapp Document, and Special Invitation.

Threats, Malware, Cyber Campaigns, and Adversaries

- 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

AI browser risks are demonstrated by PoC sidebar spoofing attacks. “With the launch of OpenAI’s ChatGPT Atlas this week and Perplexity’s Comet earlier this year, AI browsers have been gaining steam and embedding the power of large language models (LLMs) more deeply into users’ online experiences. From a cybersecurity perspective, these browsers represent a new potential attack vector, with previous proof of concept (PoC) attacks showing how Comet could be manipulated to exfiltrate sensitive data or deliver malicious links.” (SC Media)

Baohuo Android malware hijacks Telegram accounts via fake Telegram X. “A new Android threat is spreading fast through fake versions of Telegram X, giving attackers complete control over users’ accounts. Security researchers at Doctor Web have named it Android[.]Backdoor[.]Baohuo[.]1[.]origin, describing it as one of the most advanced Android backdoors seen this year.” (HackRead)

Bots, bread, and the battle for the Web. “AI-powered malicious SEO is rapidly transforming the digital threat landscape, enabling threat actors to manipulate search engine algorithms at scale. This undermines the visibility of legitimate content, [and] erodes trust in online information.” (Unit 42)

Full Disclosure: Revive Adserver vulnerability. “A high-severity SQL injection vulnerability (CVE-2025-52664) has been identified in Revive Adserver version 6.0.0. The flaw resides in the admin-search.php script and is exploitable via the keyword parameter using either GET or POST methods.” (Seclist)

Have I Been Pwned: MyVidster (2025) data breach. “A significant data breach has impacted MyVidster, compromising the personal information of nearly 3.9 million users. The data was publicly posted on a hacking forum, increasing the risk of phishing and credential-based attacks.” (Have I Been Pwned)

Infostealers Running Wild? “The threat posed by information-stealing malware continues to rise, as it mass harvests ever-greater quantities of user credentials and offers them for sale across the cybercrime underground. Researchers have recently tracked 1.8 billion stolen credentials being sold across illicit marketplaces.” (Data Breach Today)

A new CoPhish attack steals OAuth tokens from Copilot Studio agents. “CoPhish abuses the flexibility of Microsoft Copilot Studio, which allows users to create and share chatbot agents hosted on copilotstudio[.]Microsoft[.]com. These agents can be customized using "topics" – automated workflows with login prompts.” (Bleeping Computer)

Ransomware Spotlight: DragonForce. “DragonForce introduced a “data analysis service” designed to assist affiliates, and pressure victims of ransomware/data leak attacks into paying. The "service" functions as a risk audit of both the targeted organization and the stolen data, generating materials such as extortion call scripts, drafts of letters to management, and pseudo-legal analysis and advice reports.” (Trend Micro)

THREAT OF THE WEEK

Windows server vulnerability and EtherHiding highlight this week’s risks.

Out-of-Band Security Update to Mitigate Windows Server Update Service Vulnerability Released

Summary

Microsoft released an update to address a critical remote code execution vulnerability impacting Windows Server Update Service (WSUS) in Windows Server (2012, 2016, 2019, 2022, and 2025), CVE-2025-59287, that a prior update did not fully mitigate.

Institutions should implement Microsoft’s updated Windows Server Update Service (WSUS) Remote Code Execution Vulnerability guidance, or risk an unauthenticated actor achieving remote code execution with system privileges.

Remediation

Institutions utilizing affected products should immediately:

1. Identify servers currently configured to be vulnerable to exploitation (i.e., affected servers with WSUS Server Role enabled and ports open to 8530/8531) for priority mitigation.
2. Apply the out-of-band security update, released on 23 October 2025, to all servers identified in Step 1. Reboot WSUS server(s) after installation to complete mitigation.
    - System administrators of institutions that are unable to apply the update immediately should disable the WSUS Server Role and/or block inbound traffic to ports 8530/8531, the default listeners for WSUS, at the host firewall. They are urged not to undo either of these workarounds until after they have installed the update.
3. Apply updates to remaining Windows servers. Reboot servers after installation to complete mitigation.

DPRK Actors Leverage EtherHiding Technique

Summary

Democratic People's Republic of Korea (DPRK) threat actors are leveraging 'EtherHiding' as a new technique in their 'Contagious Interview' campaign. Contagious Interview is an ongoing campaign in which threat actors pose as recruiters or employees from financial institutions, most often digital asset firms, for malicious purposes.

Contagious Interview cybercriminals are known to leverage the 'ClickFix' technique to trick targets into clicking on malicious links, e.g., clicking a link in a fake error message to "fix" a supposed computer problem. The link downloads malicious code.

What is EtherHiding?

EtherHiding is a technique that embeds the malicious payload associated with the ClickFix lure in a smart contract on a public blockchain instead of a command and control (C2) server. When the victim clicks the link sent by the actor, it downloads the payload from the smart contract. Leveraging a blockchain-based smart contract to act as a C2 server leaves cyber defenders with no infrastructure for targeted disruption. The malicious payload remains in place as long as the blockchain remains in existence.

Remediation

EtherHiding is designed to resist traditional response and mitigation practices, such as blocking known malicious IP addresses. Still, the US Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection recommends that network defenders take these steps to prevent and mitigate campaigns that leverage EtherHiding.

- Implement a restrictive download policy to prevent employees from downloading malicious files.
- Block access to public blockchain nodes unless required. If required, block public blockchain nodes identified as malicious in cyber threat reporting.
- Restrict access and permissions for running Windows Run and PowerShell.
- Monitor networks for unusual Web3 traffic, specifically network calls to blockchain application programming interfaces (API) and Remote Procedure Call (RPC) endpoints.

THREAT INTELLIGENCE UPDATE

AWS US-East Widespread Outage

Summary

On 20 October, Amazon Web Services (AWS) experienced a widespread outage due to a reported DNS resolution issue originating from its US-EAST-1 region. The alleged root cause was a defect within the AWS database service DynamoDB's automated DNS management service. The cascading issue resulted in technical issues across Amazon's Elastic Compute Cloud (EC2), Network Load Balancer (NLB), and other Amazon services.

Amazon issued a comprehensive statement indicating the event began at 11:48 p.m. Pacific Daylight Time (PDT) on 19 October and ended at 2:20 p.m. PDT on 20 October, with three distinct periods of impact. The outage affected many services relying on AWS, including streaming services (e.g., Netflix and Disney+), messaging services (e.g., WhatsApp and Signal), and several government websites (e.g., the UK's NHS).

As of Q2 2025, Amazon Web Services holds an approximate 30% worldwide market share of cloud infrastructure, with Microsoft Azure holding 20% and Google Cloud holding 13%. Despite the relatively short downtime and lack of malicious activity, the widespread impact of the AWS outage highlights the potential risks associated with relying on a single cloud service provider. Member firms should consider reviewing contingency plans for technical outages and compromises of essential infrastructure, including both critical systems and third-party providers.

JUST FOR COMMUNITY INSTITUTIONS

Protecting Employees Victimized by Cybercrime – and Their Employer

Summary

Work can be a haven for employees facing issues at home. But cyber stalkers or domestic abusers often harass their victims at their workplace, and no-contact orders don't always prevent it. Employers can take the following steps to help protect both the victim and the firm.

Policies to Protect the Institution

1. Develop and enforce clear cyber policies.
    - Have a zero-tolerance policy of cybercrime and file charges when appropriate.
    - Ask to see employees' no-contact orders to understand the depth and breadth of the situation.
2. Educate employees on the company's cyber policies and cybercrime prevention techniques.
    - Regularly remind employees about the risks and best practices for online safety, such as not opening suspicious links or files from unknown sources.
3. Prohibit the sharing of employees' location and direct contact information.
4. Provide a confidential outlet to report incidents.

Note that employees can be victimizers. Develop a comprehensive digital media policy that prohibits cyberstalking behavior and clearly outlines the consequences.

Corporate Security Actions

1. Secure company networks.
    - Implement and maintain security software and protocols, but please note that these are not a replacement for user awareness and good judgment.
    - Strengthen passwords and security.
    - Require strong, unique passwords for all accounts and enable two-factor authentication whenever possible.
2. Discuss security requirements with victims.
    - Document malfeasance with screenshots and save messages.
    - Warn abusers in writing to cease contact with employees, then stop all communication and report incidents to the police.

Security Measures for Employees

Employees should inform their employer if cyberstalking is work-related and/or affects their ability to perform their job duties, so their employer can provide support and take necessary action.

Those being harassed should document messages with screenshots and save messages, warn the stalker in writing to cease contact, refuse all communications, and report the incidents to the police.

Keep the entire workforce safer with reminders to:

1. Be alert to their surroundings when entering or leaving buildings. Those who feel endangered should:
   - Park near entrances.
   - Ask for an escort to and from their vehicles.
2. Use social media security measures, such as:
   - Avoid posting personal details, like home addresses, phone numbers, workplace matters, or usual travel routes.
   - Set profiles to "private" and limit posts to friends only.
   - Only accept friend requests from known people.
   - Do not use location tags in photos or posts.

These guidelines may not completely solve the problem, but they are effective security measures that keep employees and institutions safer.

FRAUD UPDATE

Mass Messaging Systems Target School District

Summary

FS-ISAC members have recently reported phishing campaigns targeting messaging systems in school districts and education organizations across the country. Additionally, fraudulent vishing and SMS texting have been reported by the parents of schoolchildren.

Tactics, Techniques, and Procedures

To date, common attack patterns include:

- Spoofing main toll-free numbers and schools to contact school employees.
- Using the school's short codes with a financial institution referenced in the message.
- Referring to the validation of transactions from large retailers.

FS-ISAC members should review Alert IDs ebbb4b55 and 6b3cb706 for TLP Amber details and to identify remedial action.

Protecting Consumers Across Channels: Building the Trust Network of the Future

Summary

Join FS-ISAC and Somos on 10 November from 12-1:30 p.m. Eastern Time for an educational webinar on telco-enabled phishing threats. We know that smaller community institutions will greatly benefit from the insights they'll gain to protect consumers across various channels.

You may register by visiting Somos's website.

REGULATORY AND GOVERNMENT UPDATES

Sector Financial Institution Letter and Other Announcements

FRB:

- Federal Reserve issues FOMC statement, 29 October
- Federal Reserve Board requests comment on proposals to enhance the transparency and public accountability of its annual stress test, 24 October
- Federal Reserve and FDIC release public sections of resolution plans for several large banking organizations, 23 October

NCUA:

- NCUA Announces New Date for Public Budget Hearing, 24 October.

OCC:

OCC 2025-35, Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches: Notice of Proposed Rulemaking, 27 October

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.

- 31 October | Member Success Webinar
- 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