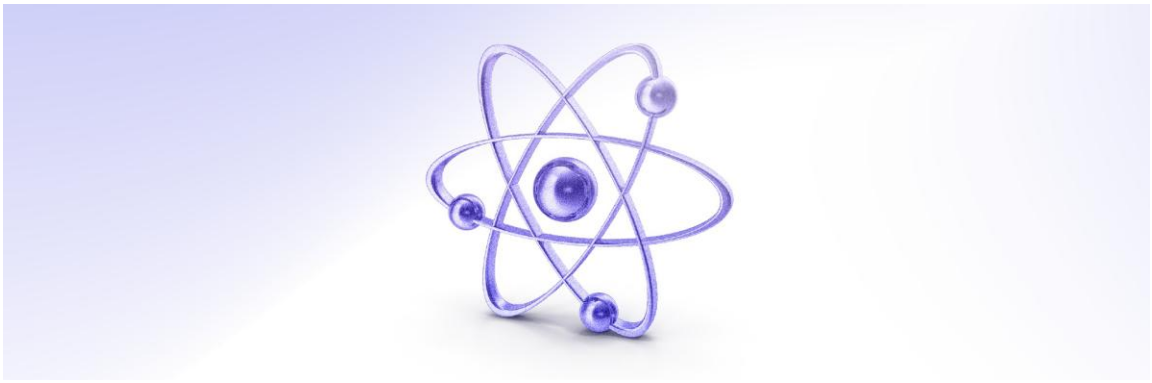
FS-ISAC | Executive Brief

Global Cyber Threat Level | Americas: EMEA: APAC: **October 2025**

We encourage you to share this brief with other senior executives of your organization or to incorporate this information in your regular reporting processes.



Threat Intelligence Update

On 25 September, Cisco disclosed the ongoing exploitation of certain Cisco Adaptive Security Appliance (ASA) 5500-X Series devices running Cisco Secure Firewall ASA Software with VPN web services enabled. Cisco also released security advisories for three vulnerabilities – CVE-2025-20333, CVE-2025-20363, and CVE-2025-20362 – to address weaknesses exploited in this activity.

The same day, the Cybersecurity and Infrastructure Security Agency (CISA) issued an Emergency Directive, and the UK National Cyber Security Centre (NCSC) released a technical analysis report.

- The CISA Directive urges US federal agencies to account for all Cisco ASA devices, assess potential compromise, address immediate risks, and collect forensic evidence via CISA-provided procedures and tools. Agencies are instructed to disconnect end-of-support devices and upgrade devices that remain in service.
- The NCSC report contained tactics, techniques, and procedures (TTP) mappings and detection rules for the identified malware, RayInitiator, a multi-stage boot kit, and LINE VIPER, a shell code loader for use on Cisco ASA devices.

FS-ISAC assesses Cisco devices running vulnerable software, especially those

that are near or at end-of-life, represent an immediate risk. We recommend remediation according to Cisco, CISA, and NCSC guidance. FS-ISAC published a Flash report and organized a Spotlight Call with members to provide messaging from the Cisco Information Security team regarding the activity.

Cisco assessed with high confidence that the threat actor behind the suspected state-sponsored “ArcaneDoor” campaign – uncovered in early 2024 – is the originator of this threat activity. In April 2024, Cisco reported initial campaign activity dating back to early November 2023 involving the compromise of unspecified government networks with identified actor-controlled infrastructure.

What's New at FS-ISAC

Security Advisories

FS-ISAC recently released two TLP GREEN Security Advisories, both available on SHARE. These Security Advisories give member firms detailed guidance on recent threat activities, preventative controls, and mitigation strategies.

Protecting CRM and SaaS Platforms

These token-centric integrations collapse security boundaries and allow attackers to “live off the API.” Enterprises can manage these threats within their environments with a defense-in-depth strategy that combines stringent technical controls with comprehensive visibility and proactive threat hunting.

The Security Advisory discusses FS-ISAC’s recommendations for CRM and SaaS defense, particularly regarding:

- Identity and Access Management (IAM) hardening
- Proactive monitoring/behavioral analytics
- Vendor and third-party management

Software Supply Chain Risk: Protecting Against NPM Software Dependencies

The “s1ngularity” and “Shai-Hulud” campaigns infect commonly used open-source packages with malware, including those integral to application development. The threat actors’ intent appears to be the discovery and exfiltration of various tokens, private keys, and cryptocurrency wallet funds. To help members defend their firms, this Security Advisory:

- Describes the stages of the s1ngularity compromise

- Outlines the attack chain and deployment of the Shai-Hulud malware
- Summarizes member reports of recent malicious npm package activity, likely related to these campaigns

A separate document lists the Indicators of Compromise (IOC) associated with these attacks and provides an FS-ISAC member's compilation of 520 identified malicious npm packages.

Industry News

Aspen Institute National Task Force Publishes Fraud Prevention Strategy

On 30 September, the Aspen Institute Financial Security Program released *United We Stand: A National Strategy to Prevent Scams*, published by the Institute's National Task Force on Fraud and Scam Prevention, of which FS-ISAC is an inaugural member. The report details a collaborative public/private, national strategy to combat fraud by making it less appealing, harder to execute, and riskier to attempt.

United We Stand includes input from the Task Force's working groups and subject matter experts, as well as the Institute's research. FS-ISAC, along with many of our members and fellow ISACs, assisted in the development of the report.

Security Lapse Exposes Data of 270,000 Bank Customers

A data spill from an unsecured Amazon S3 storage bucket exposed over a quarter million customer documents relating to bank transfers in at least 38 Indian banks and financial institutions.

According to TechCrunch, the data included account numbers, transaction figures, and customer contact information. The security lapse was discovered in August by cybersecurity firm UpGuard and was attributed to a configuration gap. Although the gap has been addressed, the incident reinforces the importance of strict configuration management, regular audits, and using the principle of least privilege.

Call for Comments on FinCEN Survey

On 29 September, the Financial Crimes Enforcement Network (FinCEN) requested comments from federal agencies and the general public on a proposed Survey of the Costs of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Compliance. FinCEN, a bureau of the US Department of the Treasury, hopes to determine the costs incurred by non-bank financial institutions – such as insurance companies, credit card systems, loan companies, and other businesses – to comply

with AML/CFT requirements, and learn how these expenses overlap with fraud monitoring and related costs. Comments will be accepted until 1 December 2025.

Knowledge

Practical Know-How from your Fellow Members

- The Timeline for Post Quantum Cryptographic Migration
- Leveling Up: A Cyber Fraud Prevention Framework for Financial Services
- Security Advisory: Protecting CRM and SaaS Platforms
- Software Supply Chain Risk: Protecting Against NPM Software Dependencies
- Hardening API Controls: A Three-Part Framework for API Risk Mitigation

See the full list of Knowledge resources

FS-ISAC FinCyber Today

Insights from Top Leaders in our Community

FinCyber Today Podcast Season 2 of 2025

- Meg Anderson: Lessons in Cyber Leadership From a Trailblazing CISO
- Jochen Friedemann: The Fun Side of Financial Services Cybersecurity
- Debbie Janeczek: How to Prepare for the Quantum Revolution
- Susan Koski: Managing the Move to the Post-Password Cyber Landscape
- Ariel Weintraub: Ensure Your Supply Chain Continuity - Even Under Pressure

FinCyber Today Podcast Season 1 of 2025

- 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

See the full FinCyber Today Podcast catalog

Subscribe