

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

Week of 28 July 2025 | Issue 293

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

- Account Takeover
- Business Email Compromise
- IT/Tech Support
- Withdrawal Impersonation Fraud

System Vulnerabilities

Adobe, Amazon, Apple, Cisco, Debian, Dell, Delta Electronics, F5, Fuji Electric, GitLab, GNU, HP, Honeywell, IBM, ICONICS, Johnson Controls, Lenovo, LG Innotek, Linux, Medtronic, Microsoft, Mitsubishi, Mozilla, National Instruments, Network Thermostat, NVIDIA, Oracle, Palo Alto, PaperCut, Red Hat, SharePoint, Samsung, SolarWinds, Splunk, SUSE, Tableau Server, Ubuntu, and VMware.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Authenticate Message, Bid Request, Bonus Disbursement, e-Tax, Fake Updates, Frontier Fiber Static Important Request, IP setup help, Hishing, Important Account Update, Intellectual Property Rights Violation Notification, LinkedIn Follow Up, NEW DIRECT DEPOSIT DETAILS, NF-e 41142646, Outstanding Payment, Payment Received, PayPal, Payroll Change, Payroll Diversion, Proposal Document, Quick Task, Teammates sent 2 messages to your chat, and Total SBA.

Threats, Malware, Cyber Campaigns, and Adversaries

- Acreed Ransomware
- Arkana Ransomware Group
- BeaverTail (InvisibleFerret)
- BitStep RAT
- Bumblebee (aka ShellSting, Shindig)
- CellikRAT V4.0 Malware
- Chaos RAT
- ChainedDown malware
- ChainedRAT
- ClickFix/ClearFake
- ColdRiver Group
- Dark Crystal
- Direwolf Ransomware Group
- Duck Tail Malware
- Etelaat Infostealer
- InterLock Ransomware (NodeSnake RAT)
- Katz Stealer
- KongTuke
- Latrodectus
- Longwait Malware
- MetaStealer
- Mispadu
- Nitrogen
- Oyster[Loader] (Broomstick)
- Pay2key Ransomware
- Phantom Stealer
- Rhysida Ransomware
- SectopRAT
- StilachiRAT
- SocGholish

- FileFix
 - FormBook
 - GolangGhost
 - GorillaBot
 - Grandoreiro
 - GravityForms
 - GremlinStealer
 - SocksShell (aka Zapcat Supper)
 - SparkRAT
 - SQUIDGATE (TerraLoader)
 - Vanguard Stealer
 - Xloader
 - Xworm
 - ZAPCAT
 - Zloader
-

NEWS AND RISK INFORMATION

FS-ISAC Quarterly Threat Report now available. The Q2 Threat Trends Report focuses on member submissions – delivered via FS-ISAC’s SHARE portal, CONNECT channels, and other sources – along with actionable intelligence from government and third-party partners. It offers a comprehensive analysis of prevalent attack vectors, malware trends, and emerging threats observed in the last three months, and elaborates on geopolitical and technological trends to give context for the evolving cyber threats and capabilities targeting the financial sector. ([FS-ISAC](#))

A critical Cisco ISE bug exploited in attacks. “A critical unauthenticated RCE vulnerability in Cisco ISE has been actively exploited in the wild. The issue was later split into two CVEs: CVE-2025-20281 (command injection) and CVE-2025-20337 (unsafe deserialization).” ([Bleeping Computer](#))

Gunra ransomware introduces a Linux strain. “Gunra ransomware has introduced a Linux variant that significantly enhances its encryption capabilities, allowing it to run up to 100 encryption threads in parallel and enabling partial file encryption. This development marks a strategic shift towards cross-platform targeting, expanding the group’s reach beyond its original focus. Since its emergence in April, Gunra has victimized various sectors, including healthcare, manufacturing, and IT, across multiple countries. Unlike its Windows counterpart, the Linux variant does not drop a ransom note, prioritizing quick and efficient encryption instead. It renames encrypted files with a .ENCRT extension and offers attackers the option to store RSA-encrypted keys separately, showcasing its advanced and flexible approach to ransomware attacks.” ([Trend Micro](#))

Hackers exploit IIS servers with web shell. “Hackers are exploiting IIS servers using a complex web shell script named UpdateChecker.aspx, which allows full remote control of compromised systems. This script, disguised as a legitimate ASPX page, employs heavy obfuscation techniques, encoding method names and strings to evade detection. It processes commands via HTTP POST requests, requiring encrypted payloads structured as JSON objects. The web shell is organized into modules that enable reconnaissance, arbitrary command execution, and extensive file system manipulation. Attackers can gather server information, execute Windows commands, and perform a variety of file operations, such as creating, modifying, and deleting files.” ([Fortinet](#))

PyPI warns of an ongoing phishing campaign. “PyPI issued a security warning about a phishing campaign targeting Python developers, where project maintainers are tricked into revealing their credentials via a spoofed domain. The phishing email impersonates PyPI with a deceptive address (noreply@pypj[.]org), directing users to a fake login page, forwarding their credentials to the real PyPI portal to create a false sense of legitimacy. PyPI confirmed that the attack is not due to a platform breach but is an opportunistic campaign targeting maintainers whose emails are listed in package metadata.” ([PyPI](#))

Romance scam drops malware. “A recent attack campaign targeting German speakers employs romance-themed scam emails to deliver malware through the Keitaro TDS. These emails contain malicious URLs that lead to a 300MB ISO file, which is designed to evade detection by inflating its file size. The ISO includes an executable named “lovely_photos.exe” that prompts users for a password, enabling the extraction of additional malicious files. The malware utilizes obfuscated batch scripts and AutoIT scripting to bypass antivirus detection, modifying system variables and creating a scheduled task to ensure persistence.” ([Sublime](#))

THREATS OF THE WEEK

Security vulnerabilities and Scattered Spider highlight this week’s risk.

Multiple Security Vulnerabilities Identified in the Niagara Framework

Summary

Community institutions using Tridium's [Niagara Framework](#) should be aware that more than a dozen security vulnerabilities have been identified in the Niagara Framework, which could allow attackers on the same network to compromise systems if misconfigured, disabling encryption. Severe Common Vulnerabilities and Exposures (CVEs) include [CVE-2025-3936](#), [CVE-2025-3937](#), [CVE-2025-3938](#), [CVE-2025-3941](#), [CVE-2025-3944](#), and [CVE-2025-3945](#), all with high Common Vulnerability Scoring System (CVSS) scores.

Exploitation could lead to root-level remote code execution, enabling attackers to intercept tokens, perform Cross-Site Request Forgery (CSRF) attacks, and gain elevated permissions for persistent backdoor access. Attackers could download private keys to conduct adversary-in-the-middle attacks, compromising both the Station and Platform components of the Niagara system.

Remediation

Institutions should review the CVE advisories to ascertain risk and implement the recommendations provided.

Scattered Spider Advisory Update

Summary

Scattered Spider presents a real threat, and financial services firms must remain diligent as it and other threat actors innovate and scan for new exploits. To help firms across sectors mount an effective defense, members of the National Council of ISACs – including the Financial Services, Information Technology, Food and Agriculture, Health, Aviation, Automotive, Retail and Hospitality, and Maritime Transportation System ISACs – shared their expertise to produce the recently released [Cross-Sector Mitigations: Scattered Spider Guidance for Proactive Defense](#).

Their analysis details Scattered Spider's observed activity and tradecraft as of May 2025, providing:

- Background on Scattered Spider so that firms can better scope their threat surface
- Technical procedures and cultural practices to thwart Scattered Spider attacks
- Analysis of ISAC and FBI intelligence, and corresponding MITRE ATT&CK® mitigations

Scattered Spider threat actors have been known to use various ransomware variants in data extortion attacks, most recently including DragonForce ransomware. While Scattered Spider often changes tactics, techniques, and procedures (TTPs) to remain undetected, it frequently employs social engineering techniques – such as phishing, push bombing, and SIM swap attacks – to obtain credentials, install remote access tools, and bypass multi-factor authentication.

Additionally, the FBI, CISA, Royal Canadian Mounted Police, Australian Signals Directorate's Australian Cyber Security Centre, Australian Federal Police, Canadian Centre for Cyber Security, and the UK's National Cyber Security Centre jointly produced [Cybersecurity Advisory Scattered Spider](#), providing updated TTPs obtained through FBI investigations conducted through June 2025.

Remediation

The Recommendations section of [Cross-Sector Mitigations: Scattered Spider Guidance for Proactive Defense](#) provides critical infrastructure organizations and commercial facilities mitigation suggestions to strengthen their defenses.

THREAT INTELLIGENCE UPDATE

Protecting Community Institutions Against Interlock Ransomware

Hacktivist groups use Distributed Denial of Service campaigns.

Summary

FS-ISAC affiliate partner Graphika reports that several pro-Russia and pro-Palestine hacktivist groups claimed to have launched distributed denial of service (DDoS) and industrial control system (ICS) attacks against Germany and other European targets in retaliation for Europol's Operation Eastwood, which disrupted the operations of the pro-Russia hacktivist group NoName057(16).

- Starting 16 July, the pro-Russia Z-Alliance claimed it conducted a DDoS attack against Norway's National Cyber Crime Centre, a German non-profit organization supporting Ukrainian refugees, a Czech online safety educational website, and the European Cyber Security Organization. The group later claimed ICS attacks against multiple Italian water management, delivery, and purification companies and a Czech wastewater management system. Z-Alliance used #??NONAME057(16), which translates to "ForNoName057(16)," to promote its alleged attacks.
- On 17 July, the pro-Russia group Server Killers cited Operation Eastwood and used obscene hashtag references to Eastwood while claiming DDoS attacks against the websites for German government ministries, several regions and cities, and transportation services.
- The same day, the pro-Palestine group Keymous+ announced DDoS attacks against multiple German cities' websites "in support for our russian [sic] friends," and against two chemical and road safety companies.
- Despite stating "Bye Bye Germany" in a Telegram post, the pro-Palestine group Team Fearless listed several already inactive or insecure US and French websites that it allegedly disrupted.
- The pro-Palestine group Dark Storm Team claimed it conducted DDoS attacks on Germany's defense and justice ministries, without mentioning Operation Eastwood.

While these groups expressed support for NoName057(16), their activities have been limited and appear uncoordinated, highlighting how hacktivist alliances and actions remain fragmented, as is their willingness to back members targeted by law enforcement.

FS-ISAC members can read the entire alert, which includes threat indicators. [View](#)

JUST FOR COMMUNITY INSTITUTIONS

What is Hishing?

Summary

Hishing refers to the characteristic misspellings found in phishing campaigns. Though not yet a widely used term in cybersecurity, financial services firms should be aware that hishing can signal a social engineering campaign conducted via email (phishing) or text (smishing).

Though poorly worded messages may be benign, they are a hallmark of threat actors operating in non-native languages or with minimal information about a target, like the correct spelling of a name. Employees should be trained to question spelling mistakes against their knowledge of the sender, the probability that the sender would request the information or activity in the message, and the likelihood of being targeted in a social engineering campaign.

If not done already, institutions should add hishing to their security awareness training and testing to ensure employees remain current with the tools adversaries use.

GOVERNMENT AND REGULATORY NEWS

Bank Activities: Crypto-Asset Safekeeping Services

Summary

The Comptroller of the Currency (OCC) has issued guidance for banking institutions that hold crypto-assets on the behalf of customers – specifically that they conduct that safekeeping in a sound manner, and in compliance with applicable laws and regulations. As with all new products, services, and activities, firms should carefully consider potential benefits and risks, including risks associated with using third-party service providers, before offering crypto-asset safekeeping.

The crypto-asset safekeeping statement discusses how existing laws, regulations, and risk-management principles apply to this activity and does not create any new supervisory expectations.

[Read the entire bulletin.](#)

Federal Bank Regulatory Agencies Seek Further Comment on Interagency Effort to Reduce Regulatory Burden

Summary

US federal bank regulatory agencies announced their fourth notice requesting public comment to reduce regulatory burden. The Economic Growth and Regulatory Paperwork Reduction Act requires the agencies to review their regulations at least once every 10 years to identify outdated, unnecessary, or unduly burdensome regulatory requirements for their supervised institutions.

The agencies will hold outreach meetings where interested parties may comment on applicable regulatory requirements directly to the agencies. Information about the outreach meetings will be publicized as details are finalized.

[Read the entire bulletin.](#)

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- [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 enroll to attend events in the Member Services app.

- 18 August | Monthly CIAC Webinar
- 27 August | CIAC and COFFE Open Forum
- 2 September-17 October | CAPS for Community Institutions **[Registration now open]**
- 5-8 October | Americas Fall Summit **[Registration now open]**

[View all Americas events.](#)

TLP GREEN 

© FS-ISAC 2025



12120 Sunset Hills Rd, Reston
VA 20190

To manage emails you may receive, please log in to the Member Services platform of the Intelligence Exchange to [update subscription preferences](#).