

FS-ISAC | Risk Summary Report

Global Cyber Threat Level  | Americas:  EMEA:  APAC: 

Week of 23 June 2025 | Issue 288

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
- Call Center ATO
- Account Takeover
- Advance Fee
- Business Email Compromise
- CEO Impersonation
- Customer Impersonation ATO
- Fraud Withdrawals
- Property Sales
- Withdrawal Impersonation Fraud

System Vulnerabilities

Amazon, Apache, Apple, Atlassian, Clam AV, Cisco, Citrix, ControlID, Cygwin, D-Link, Debian, Dell, Delta Electronics, F5OS-A, Fortinet, GitLab, Google, Hitachi, IBM, Kaleris, Lenovo, AMI MegaRAC, Microsoft, Microsens, Mitsubishi, Mozilla, NVIDIA, Oracle, Palo Alto, PAN-OS, Parsons AccuWeather, Red Hat, Schneider, Serv-U, Splunk, SUSE, TrendMakers, Trend Micro, Ubuntu, and Velociraptor.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: 20250618 CBCM Global, Administrator Review, Adult Dating, b20999, CONFIRM MOBILE CELL, Document Review, DocuSign, Employee Handbook, Fake Invoice, FOLLOW UP ASAP!, Geek Squad, Gift Card, IMPORTANT REQUEST!!, Important Update, Indeeal, Intuit E-Commerce Service, INV. 00-Z564, Mailbox Full, Meis CPA'S, Notification, O365, Outstanding Payment Notice, pay-with-featured, Please Review and Sign: Contract / Statement of Work Enclosed, POC available for CVE-2025-49144, QR Code, Relax Rentals, Request for Updated Information!, Review of Social Security Benefit Determinations, Sales Contract, Shared via SignFlow, Social Security Record Accuracy, Social Security Processing, SSA Review, Treasury Management/Corporate Client, Treat with urgency, Uphold Address Verification, Voicemail Notification, and WhatsApp.

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
- GremlinStealer
- InterLock Ransomware (NodeSnake RAT)
- Latrodectus
- MetaStealer
- Mispadu
- Nitrogen
- StilachiRAT

- ChainedRAT
- ClickFix/ClearFake
- ColdRiver Group
- Direwolf Ransomware Group
- FormBook
- GolangGhost
- GorillaBot
- Grandoreiro
- SocGholish
- SocksShell (aka Zapcat Supper)
- SparkRAT
- SQUIDGATE (TerraLoader)
- Xloader
- Xworm
- ZAPCAT
- Zloader

NEWS AND RISK INFORMATION

Cloudflare blocks record DDoS attack. Cloudflare [commented](#) that it automatically blocked the largest distributed denial-of-service (DDoS) attack ever recorded. The mid-May 2025 attack, which hit a peak of 7.3 terabits per second, [exceeds](#) the previously largest recorded DDoS attack, which peaked at 6.5 terabits. The unknown threat actor [targeted](#) a hosting provider, which represents a recent trend of threat actors targeting critical internet infrastructure through DDoS attacks. Nearly all of the attack traffic was categorized as a UDP flood, which sends a high volume of packets to the target's IP addresses. Firms can protect themselves through smart rate-limiting and dropping unwanted traffic. See our latest report written with Akamai, [From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector](#), for more proactive guidance. (FS-ISAC)

Critical authentication bypass vulnerability in Teleport (CVE-2025-49825) affects SSH and Git proxy setups. “Teleport security engineers have discovered a critical vulnerability affecting Teleport versions earlier than 17.5.2. This flaw allows remote attackers to bypass SSH authentication on servers running Teleport SSH agents, OpenSSH-integrated deployments, and Teleport Git proxy setups. Exploiting this vulnerability could enable unauthorized access to Teleport-managed systems by circumventing standard authentication controls.” ([Fortinet](#))

NCSC issues alert on 'UMBRELLA STAND' malware targeting Fortinet FortiGate firewalls. “The National Counterintelligence and Security Center (NCSC) issued an alert regarding a newly discovered malware dubbed UMBRELLA STAND, which targets internet-facing Fortinet FortiGate 100D firewalls. This malware is designed to establish persistent access to embedded network devices.” ([gbhackers](#))

NotePad++ vulnerability (CVE-2025-49144). “A severe privilege escalation vulnerability has been discovered in Notepad++ version 8.8.1, potentially exposing millions of users worldwide to complete system compromise. The flaw, designated CVE-2025-49144, allows attackers to gain SYSTEM-level privileges through a technique known as binary planting, with a proof-of-concept demonstration now publicly available. The vulnerability affects the Notepad++ v8.8.1 installer released on May 5, 2025.” ([Cybersecurity News](#))

Resurgence of the Prometei botnet. “This malware family, which includes both Linux and Windows variants, allows attackers to remotely control compromised systems for cryptocurrency mining (particularly Monero) and credential theft ... Prometei is under active development, incorporating new modules and methods into its capabilities.” ([Palo Alto Networks](#))

Scattered Spider targeting IT teams. On 17 June, Google Threat Intelligence Group (GTIG) [stated](#) that Scattered Spider is now targeting major insurers, a shift from the group's recent cybercrimes against US and UK retailers. In an email to Hacker News, GTIG noted that the threat actor tends to focus campaigns sector-by-sector. For the insurance industry, GTIG stated the threat actor is focusing its social engineering – a common Scattered Spider technique – on IT helpdesks and call centers. Three insurance companies [recently](#) disclosed cyber attacks, with one attack reportedly using social engineering. It is not yet confirmed if Scattered Spider was behind the attacks. (FS-ISAC)

Threat actors abuse the signed ConnectWise application as a malware builder. “A new malware campaign tracked as EvilConwi is actively abusing ConnectWise's ScreenConnect software to distribute signed malware. This follows earlier exploitation of CVE-2024-1708 and CVE-2024-1709 in February 2024.” ([gdatasoftware](#))

THREATS OF THE WEEK

Phishing and account takeover campaigns highlight this week's risks.

Phishing and Account Takeover Campaigns

Summary

Each week, the Risk Summary Report team gathers the current malicious threats, malware, cyber campaigns, adversaries, and subject lines so that you can proactively block potentially harmful emails. Additionally, FS-ISAC produces daily phishing and CYBERA fraud reports. This data enables FS-ISAC members to prevent the problems associated with the various campaigns.

Adversaries and criminal organizations are using many different subject lines as lures to distribute their malicious software. Many leverage credential spraying techniques to facilitate account takeover and withdraw funds from customer accounts. Adversaries are also impersonating customers to trick call center personnel.

Recommendations

- Provide customer-facing employees with information about threat actors' tactics and what you want employees to do if they observe them.
- Regularly update your network defenses and antivirus software and use intelligence from FS-ISAC reports to bolster prevention efforts.
- If you see something, tell us. FS-ISAC collects and analyzes threat information (e.g., indicators of compromise, URL addresses, malware type, etc.) and uses the intel to support the global financial services sector's cyber defense.

New Guidance Released for Reducing Memory-Related Vulnerabilities

Summary

The Cybersecurity Infrastructure and Security Agency (CISA), in partnership with the National Security Agency (NSA), released a joint guide on [reducing memory-related vulnerabilities in modern software development](#).

Memory-safe languages (MSLs) – such as Rust, Go, Java, C#, Swift, Python, and JavaScript – are safer and prevent programming errors such as [buffer overflows](#) and [dangling pointers](#). Languages like C and C++ are not MSLs and require careful manual memory management.

Memory safety vulnerabilities pose serious risks to national security and critical infrastructure. Adopting MSLs offers the most comprehensive mitigation against this class of vulnerabilities and provides built-in safeguards that enhance security by design.

The joint guide outlines key challenges to adopting MSLs, offers practical approaches for overcoming them, and highlights important considerations for institutions seeking to transition toward more secure software development practices.

Remediation

Public and private sector institutions are encouraged to review this guidance and support the adoption of MSLs.

THREAT INTELLIGENCE COMMUNITY INSTITUTION UPDATE

Military Action Sparks Concerns for Cyber Attacks

Military action leads to post-ceasefire DDoS attacks by pro-Iranian groups.

Summary

Following last week's military action between Israel and Iran, the following events have transpired:

- The ongoing Iran conflict is causing a heightened threat environment in the United States. On 22 June, the US government issued a Terrorism Advisory stating that:
 - > Low-level cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian government may conduct attacks against US networks.
 - > The likelihood of violent extremists in Iran independently mobilizing to violence in response to the conflict would likely increase if Iranian leadership issued a religious ruling calling for retaliatory violence against targets there.
- The US military conducted strikes against sites alleged to be nuclear enrichment installations.
- Iran responded by missile strikes against US military installations in Qatar.
- The FS-ISAC EMEA and Americas Threat Intel Committees raised the cyber threat to Elevated. This condition applies in response to evidence of a:
 - > Significant, material cyber incident(s) causing direct or indirect operational or continuity impact to the sector, and/or
 - > A heightened cyber threat environment from a credible, sophisticated actor or group.

Implementation of additional cybersecurity measures may be warranted. Such measures may be expected to last for an indefinite period, with a minimum to moderate impact on business operations or expenses.

- On 23 June, a total cease-fire was announced, which was followed by simultaneous missile fire from the combatants.

This Just In

In retaliation for the US strikes on Iran, pro-Iran hacktivist groups started targeting the websites of US banks, the military, and others – some of them using purported stress-testing services for DDoS attacks

A Graphika report reveals that at least five influential hacktivist groups – the Bengali Mysterious Team and Sylhet Gang, the North African Keymous+, the Moroccan Mr Hamza, and the Iraqi 313 Team – were behind the DDoS attacks on US websites. The Cyber Jihad Movement and other groups teased their own US attack campaigns. FS-ISAC members can view the entire report in [Alert ID 2ae9eec8](#), including threat indicators and indicator confidence scores.

Why It Matters

We assess these cyber attacks as having limited impact, but they illustrate a growing trend: hacktivists partnering with external stressor services to increase the potential for impact on critical infrastructure. They also demonstrate how some groups hijack international events for notoriety, as well as ideology.

Remediation

- Considering Iran's history of cyber attacks, community institutions should remain vigilant against social engineering and phishing exploits. Any institution may be a target at any time.
- Smaller credit unions outsourcing network security should advise their vendors of the elevated risk and carefully monitor their key perimeter(s).
- FS-ISAC's [Connect Channel](#) is available for institutions to obtain and share information.
- FS-ISAC members can view [Alert ID 7526df3d](#), which provides a comprehensive list of helpful resources.

For smaller institutions seeking best practice guidance, IndusFace published a list of [17 best practices to prevent DDoS attacks](#).

If you are a smaller credit union and are not a member of FS-ISAC, consider joining our community at [fsisac.com](#) to have access to TLP Amber content and remain informed of cyber incidents.

Additional References

[FS-ISAC and Akamai's analysis of 2024 DDoS attacks](#) in the financial sector revealed an evolution in attack strategies, with potentially serious implications for customer trust and business operations. Key findings include:

- DDoS attacks on the financial sector are surging. Attacks are increasing dramatically in both the number of attacks and volume of traffic.
- The financial services sector is the top target of DDoS attacks designed to overwhelm systems.
- DDoS attacks are more difficult to detect. A growing number target complex vulnerabilities in digital infrastructure and mimic legitimate traffic.
- Threat actors are increasingly sophisticated and precise, showing clear patterns of reconnaissance and strategic adaptation to financial firms' business models.

Resources

- [FS-ISAC Intelligence team](#) (email)
- [CISA](#)
- [National Threat Evaluation and Reporting \(NTER\) Program Office](#)
- [See Something, Say Something](#)
- [FBI Field Office](#)
- [DHS Fusion Center](#)
- [US National Terrorism Advisory](#)

FRAUD UPDATE

FS-ISAC Monthly Fraud Report - May 2025

Summary

FS-ISAC's [monthly fraud report](#) is now available. This report provides an overview of fraud trends for the month of May, categorized by region, sub-sector, and attack pattern, with highlights from notable member submissions.

GOVERNMENT AND REGULATORY NEWS

Simplified CECL Tool Updated for June 2025

Summary

The National Credit Union Administration has released the June 2025 update of its Simplified CECL Tool. The update provides the latest life-of-loan — or Weighted Average Remaining Maturity — factors. For credit unions currently using the Simplified CECL Tool, the June 2025 release facilitates calculating the credit loss expense on loans and leases for the period ending 30 June 2025.

The Simplified CECL Tool was developed primarily for small and non-complex credit unions as an option for estimating the allowance for credit losses on loans and leases. Credit unions with assets of less than \$10 million may also consider using the Simplified CECL Tool, as it could provide a more accurate measure of credit losses and serve as an additional tool for loan portfolio management.

To get the latest version, please visit [The Simplified CECL Tool](#) page and click on “Download the Latest Simplified CECL Tool.” To ease your use of the Simplified CECL Tool, please review [Frequently Asked Questions](#), the [User Guide](#), and the [Model Development Document](#) located on [The Simplified CECL Tool](#) page.

The NCUA updates the Simplified CECL Tool quarterly to enable credit unions to use the Tool when closing their books and submitting their quarterly NCUA Call Report.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- [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](#)
- [Stop the Scams: A Phishing Prevention Framework for Financial Services](#)
- [Ransomware Essentials: A Guide for Financial Services Firm Defense](#)
- [Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks](#)
- [Building Cryptographic Agility in the Financial Sector](#)
- [LockBit: Access, Encryption, Exfiltration, and Mitigation](#)

[See the full list of Knowledge Resources](#)

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- [FS-ISAC Security. CIAC Director Jeffrey Korte discusses the value to small institutions](#)
- [FinCyber Today Podcast Season 2](#)
- [FinCyber Today Podcast Season 1](#)
- Carsten Fischer: [The Need for Speed in Threat Mitigation](#)
- Stephen Sparkes: [The Evolution of the CISO Role](#)
- Lindsey Bateman: [Keep Your Eyes On The Horizon For Emerging Threats – And New Solutions](#)
- Burim Bivolaku: [Financial Sector Collaboration Is Key To Third-Party Risk Management](#)
- Beate Zwijnenberg: [Can Cyber Risk be Quantified?](#)
- Josh Magri: [The CRI Profile – A Simplified Approach To Better Assessment](#)

UPCOMING EVENTS

Americas

- 21 July | Monthly CIAC Webinar
- 30 July | CIAC and COFFE Open Forum
- 30 July | Member Success Session
- 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](#).

