

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

Week of 21 July 2025 | Issue 292

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, Apache, Arista, Atlassian, Avaya, Cisco, CrushFT, Debian, Dell, DuraCom, F5, F5OS, Fortinet, Google, IBM, Lantronix, Lenovo, Matanbuchus, Microsoft, Mozilla, Oracle, Palo Alto, Red Hat, Samsung, Schneider Electric, SUSE, SysAid, Trend Micro, Ubuntu, and VMware.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Coinbase, Crissie Worsham shared, CRUCIAL REQUEST, FICB – 00725, For Sale Contract, Gift Card, HR, KINDLY TREAT AS IMPORTANT, login index, Matsui Securities, Netflix, Payroll Diversion, Personal member, Proforma Invoice, QR, Quick Response, Secure Message, Syncing Error, Tax Document, The Maintenance Team - Contract Proposal, Title Request, Title Order, Treat Urgently, Unauthorized Card, United HealthCare, Unlock Payment Details, Voicemail, and Yodobashi.

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
- GremlinStealer
- InterLock Ransomware (NodeSnake RAT)
- KongTuke
- Latroedectus
- MetaStealer
- Mispadu
- Nitrogen
- Oyster[Loader] (Broomstick)
- Pay2key Ransomware
- Rhysida Ransomware
- StilachiRAT
- SocGholish
- SocksShell (aka Zapcat Supper)
- SparkRAT

- FileFix
- FormBook
- GolangGhost
- GorillaBot
- Grandoreiro
- GravityForms
- SQUIDGATE (TerraLoader)
- Vanguard Stealer
- Xloader
- Xworm
- ZAPCAT
- Zloader

NEWS AND RISK INFORMATION

NoName057(16) Operations Disrupted. European and US law enforcement targeted the pro-Russian group [NoName057\(16\)](#) in a joint operation. The group has been accused of organizing pro-Russian hackers to conduct DDoS attacks against pro-Ukraine organizations and companies. Authorities stated the group was behind cyber attacks targeting President Zelensky's 2023 address to the Swiss Parliament and the Ukraine Peace Summit in 2024. The operation, which took place between 14 and 17 July, issued nine arrest warrants, notified thousands of suspected supporters of their legal liability, and took down the group's main infrastructure. (FS-ISAC GIO)

A new ransomware variant has been spotted. "Huntress has identified a new ransomware variant named "[Crux](#)," which claims affiliation with the BlackByte ransomware group. Crux ransomware encrypts files with a .crux extension and uses ransom notes named "crux_readme_[random].txt." The ransomware employs Remote Desktop Protocol (RDP) as one of its initial access vectors and uses legitimate processes like svchost.exe and bcdedit.exe for malicious activities." ([Huntress](#))

China imposes exit bans on a US Department of Commerce employee and a Wells Fargo banker. "The unidentified government employee's restricted travel was confirmed as Beijing revealed new information about a US-based Wells Fargo banker who has also been subjected to an exit ban." ([CBS News](#))

FIDO keys under siege. "[PoisonSeed](#) attackers have developed a method to bypass FIDO key authentication using adversary-in-the-middle (AiTM) phishing attacks. These attacks exploit the cross-device sign-in feature of FIDO keys by tricking users into scanning QR codes, granting attackers access to accounts. FIDO keys, though secure, are not immune to identity-based attacks, which made up 66.2% of incidents in Q1 2025." ([Expel](#))

GRF Ransomware Report. "Global Resilience Federation (GRF) analysts recently completed the semiannual ransomware report covering the first half of 2025. The report series tracks attacks based on public sources and conversations of threat actors in closed forums. Analysts compiled data on 2,940 successful attacks." ([Global Resilience Federation](#))

New CrushFTP zero-day exploited in attacks to hijack servers. "CrushFTP is warning that threat actors are actively exploiting a zero-day vulnerability tracked as CVE-2025-54309, which allows attackers to gain administrative access via the web interface on vulnerable servers." ([Bleeping Computer](#))

Ransomware groups weaponize RMM tools to infiltrate networks and exfiltrate data. "Ransomware groups are increasingly weaponizing Remote Monitoring and Management (RMM) tools—originally intended for legitimate IT operations—to conduct sophisticated cyber intrusions." ([GB Hackers](#))

Russia linked to new malware targeting email accounts for espionage. "Russian military intelligence (GRU)-linked threat actors have been using previously unknown malicious software to enable espionage against victim email accounts, the UK's National Cyber Security Centre (NCSC) has reported." ([Infosecurity Magazine](#))

THREATS OF THE WEEK

Microsoft ToolShell Exploitation and geopolitical tension highlight this week's risk.

Microsoft Exploitation via ToolShell Exploit

Summary

FS-ISAC has distributed a series of advisories concerning a remote code execution (RCE) vulnerability that enables unauthorized access to on-premises SharePoint servers. The scope and impact continue to be monitored and assessed. Below is a recap of the most recent events.

Event Timeline

- On **23 July**, an unauthenticated RCE chain ([ToolShell](#)) targeting on-prem SharePoint servers (via [CVE-2025-49706](#) & [-49704](#)) is being actively exploited in the wild. Microsoft is preparing a patch. Until then, [enable ASMI](#) or remove internet access to SharePoint servers.

FS-ISAC published an updated analytic assessment and more detailed accounting of the on-premises SharePoint Server “ToolShell” Zero-Days. This publication can be found here: <https://share.fsisac.com/webapp/user/myfeeds/532481ad>

- On **22 July**, Microsoft released [information](#) to correct the actively exploited Common Vulnerabilities and Exposures (CVEs), which have been confirmed as [CVE-2025-49706](#), a network spoofing vulnerability, and [CVE-2025-49704](#), a remote code execution (RCE) vulnerability.
 - Active exploitation of a spoofing and RCE vulnerability chain involving [CVE-2025-49706](#) and [CVE-2025-49704](#) enables unauthorized access to on-premise SharePoint servers. While the scope and impact continue to be assessed, the chain, publicly reported as “ToolShell,” provides unauthenticated access to systems and authenticated access through network spoofing, respectively, and enables malicious actors to fully access SharePoint content, including file systems and internal configurations, and execute code over the network.
 - “Microsoft, which has tied early exploitation activity to China, is rushing out emergency patches to help organizations blunt the exploit chain, dubbed ToolShell, being used. On-premises versions of SharePoint are at risk, but SharePoint Online in Microsoft 365 is not.” ([Data Breach Today](#))

Common Vulnerabilities and Exposures (CVE)

- [CVE-2025-49706](#), a network spoofing vulnerability
- [CVE-2025-49704](#), an RCE vulnerability
- [CVE-2025-53770](#) is a variant of the existing vulnerability
- [CVE-2025-49706](#) poses a risk to organizations

While not actively exploited, Microsoft has identified the following new CVEs that pose a potential risk:

- [CVE-2025-53771](#) is a patch bypass for CVE-2025-49706
- [CVE-2025-53770](#) is a patch bypass for CVE-2025-49704

Remediation

FS-ISAC members should report any active intelligence to our [Global Intelligence Office](#).

Recommended actions to reduce the risks associated with the RCE compromise include:

- Apply the [necessary security updates released by Microsoft](#).
 - Configure [Antimalware Scan Interface \(AMSI\)](#) in SharePoint as indicated by Microsoft and deploy Microsoft Defender AV on all SharePoint servers.
 - If AMSI cannot be enabled, disconnect affected products from service that are public-facing on the internet until official mitigations are available. Once mitigations are provided, apply them according to Cybersecurity and Infrastructure Security Agency (CISA) and vendor instructions.
 - Follow the applicable [BOD 22-01](#) guidance for cloud services or discontinue use of the product if mitigations are not available.
-

- For information on detection, prevention, and advanced threat hunting measures, see Microsoft's [Disrupting active exploitation of on-premises SharePoint vulnerabilities](#) and [advisory](#) for CVE-2025-49706. CISA encourages organizations to review all articles and security updates published by Microsoft on 8 July, 2025, relevant to the SharePoint platform deployed in their environment.
- Rotate [ASP.NET](#) machine keys, then after applying Microsoft's security update, rotate ASP.NET machine keys again, and restart the IIS web server.
- Disconnect public-facing versions of SharePoint Server that have reached their end-of-life (EOL) or end-of-service (EOS) from the internet. For example, SharePoint Server 2013 and earlier versions are end-of-life and should be discontinued.
- Monitor for POSTs to /_layouts/15/ToolPane.aspx?DisplayMode=Edit
- Conduct scanning for IPs 107.191.58[.]76, 104.238.159[.]149, and 96.9.125[.]147, particularly between 18-19 July 2025.
- Update intrusion prevention system and web-application firewall (WAF) rules to block exploit patterns and anomalous behavior. For more information, see CISA's [Guidance on SIEM and SOAR Implementation](#).
- Implement comprehensive logging to identify exploitation activity. For more information, see CISA's [Best Practices for Event Logging and Threat Detection](#).
- Audit and minimize layout and admin privileges.

Available Patches

A patch is now available for SharePoint 2019 Core: <https://www.microsoft.com/en-us/download/details.aspx?id=108286>

A patch is now available for SharePoint Server Subscription Edition: <https://www.microsoft.com/en-us/download/details.aspx?id=108285>

ToolShell Victim List

ToolShell victim information has been made available by this **non-FS-ISAC** resource:

- <https://theravenfile.com/2025/07/22/cve-2025-53770-toolshell-hunting-down-the-attacker-techniques-victims/>

Additional Resources

- FS-ISAC CIAC members were provided the **OCCIP Flash Alert – Exploitation of SharePoint Vulnerability**

Geopolitical Tensions Increase Risk to Undersea Cables

Summary

On 16 July, Recorded Future published a [report](#) highlighting increased risk to undersea cables amid geopolitical tensions. The cables carry nearly all international data traffic, and damage to them can lead to disruptions impacting financial operations. While cable damage due to accidents or natural causes is not uncommon, in 2024 and 2025, 44 publicly reported cable damage incidents occurred, with some attributed to Russian and Chinese-linked vessels.

One of these [incidents](#) occurred in February 2025 when Taiwan detained a Chinese vessel after it allegedly damaged an undersea cable connecting the main island with the Penghu Islands. Researchers assess that these acts of sabotage will likely increase, as these tactics have a serious impact on international communications without escalating to open conflict.

While these incidents have had little immediate impact on the financial sector so far, the report notes that “three primary factors – lack of redundancy, lack of diversity of cable routes, and limited repair capacity – very likely raise the risk of severe outages caused by damage to submarine cables.”

Remediation

Members are encouraged to consider risks associated with outages caused by undersea cable damage in resilience planning.

THREAT INTELLIGENCE UPDATE

Protecting Community Institutions Against Interlock Ransomware

The joint advisory provides current remediation recommendations.

Summary

A multi-agency advisory is available for community institutions concerning defensive strategies against the Interlock ransomware.

The advisory highlights known Interlock ransomware indicators of compromise and tactics, techniques, and procedures identified through recent Federal Bureau of Investigation (FBI) findings.

Background

The Interlock ransomware variant was first observed in late September 2024, targeting various businesses, critical infrastructure, and other organizations in North America and Europe. The FBI maintains Interlock threat actors target their victims based on opportunity, and their activity is financially motivated.

The FBI is aware of Interlock ransomware encryptors designed for both Windows and Linux operating systems; these encryptors have been observed encrypting virtual machines (VMs) across both operating systems.

The FBI observed threat actors obtaining initial access via drive-by download from compromised legitimate websites, which is an uncommon method among ransomware groups. The threat actors were also observed using the ClickFix social engineering technique for initial access, in which the threat actor pretends to fix an issue on the victim’s system but instead executes a malicious payload. The threat actors then use various methods for discovery, credential access, and lateral movement to spread to other systems on the network.

Interlock employs a double extortion model in which it encrypts systems after exfiltrating data, which increases pressure on victims to pay the ransom to get their data decrypted and prevent it from being leaked.

Remediation

Actions organizations can take today to mitigate Interlock ransomware threat activity include:

- Preventing initial access by implementing domain name system filtering and web access firewalls, and training users to spot social engineering attempts.
- Mitigating known vulnerabilities by ensuring operating systems, software, and firmware are patched and up to date.

- Segmenting networks to restrict lateral movement from initially infected devices and other devices in the same organization.
- Implementing identity, credential, and access management policies across the organization and then requiring multifactor authentication for all services to the extent possible.

North Korean Remote IT Worker Observables and Resources

Summary

Since March 2023, FS-ISAC members have been sharing intelligence on suspicious applications they believed were tied to North Korean remote IT Workers. (16 July 2025 - 23 July 2025)

In March 2025, after receiving several submissions from members, FS-ISAC published an [Intelligence Spotlight Report on North Korean Remote IT Workers](#). Since publishing the report, members have continued to share valuable information regarding impersonated and synthetic identities of North Korean IT workers.

[See Alert ID 3550bd22.](#)

FRAUD UPDATE

PayPal Leverages AI to Roll Out Dynamic Real-Time Fraud Alerts

Summary

PayPal Holdings Inc. announced the launch of an AI-powered fraud-detection system that provides PayPal and Venmo users real-time alerts before a payment is made.

The new feature, available to PayPal and Venmo users globally, is intended to protect them from sending payments that are not eligible for refunds, such as those that respond to scams originating on social media, PayPal says.

Quarterly Fraud Trends Report Now Available

Summary

The FS-ISAC Quarterly Fraud Trends Report - Q2 2025 is now available on SHARE!

<https://share.fsisac.com/webapp/user/myfeeds/a1d227c4>

The Quarterly Fraud Trends Report for Q2 covers the period from April 1 to June 30, 2025. It provides an overview of fraud trends by region, sub-sector, and attack pattern, with highlights from notable member submissions.

GOVERNMENT AND REGULATORY NEWS

NCUA Releases 2024 Ombudsman Annual Report

Summary

The National Credit Union Administration (NCUA) today released its [Office of the Ombudsman 2024 Annual Report](#). The report highlights information about the Ombudsman's core programs, which inform recommendations made by the Ombudsman to the NCUA Board. The report also details the activities of

the Ombudsman for 2024, such as engagement with examiners, results from independent reviews of agency processes, and feedback from the Post Exam Survey.

Additionally, the report notes that the Office of the Ombudsman:

- Processed 44 inquiries and complaints related to data breaches and cyber threats at federally insured credit unions
- Made one recommendation to the NCUA Board about the agency's consumer complaint process
- Resolved 598 inquiries during 2024

The NCUA Office of the Ombudsman is an independent, neutral, and confidential resource for credit union stakeholders to informally resolve matters regarding the agency's supervisory processes or conclusions.

[Read the entire press release.](#)

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

Members enroll to attend events in the Member Services app.

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