

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

Week of 4 August 2025 | Issue 294

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
- Fraud Investment
- Fraudulent Withdrawal
- Transfers via Business Banking Spoofing & Impersonation

System Vulnerabilities

Adobe, Amazon, Apple, Cisco, Cygwin, Burk Technology, D-Link, Debian, Dell, Delta Electronics, Dreame Technology, HP, EG4 Technology, IBM, Instantel, Lenovo, Linux, Microsoft, Mitsubishi, Mozilla, Packet Power, Oracle, Red Hat, Rockwell Automation, SonicWall (Gen 7 Firewalls), SUSE, Trend Micro, Ubuntu, and Yealink.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: 504 Loan Commitment DMC, ANA, Business Banking Spoofing & Impersonation, DHL, Internal Revenue Service, KP TRUCKING LLC, New Messages, Order Receipt, Proposal Document, Robin Lloyd & Associates, Smart EX, UCC Closing #5245081-S-FL-CR, W-8BEN Form, Work Order, You have received a secure message from, and Your Payment.

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
- Latroductus
- Longwait Malware
- MetaStealer
- Mispadu
- Nitrogen
- Oyster[Loader] (Broomstick)
- Pay2key Ransomware
- Phantom Stealer
- Rhysida Ransomware
- SectopRAT
- StilachiRAT
- SocGholish

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

NEWS AND RISK INFORMATION

Akira Ransomware targets SonicWall VPNs in likely zero-day attacks. “Akira ransomware is exploiting a likely zero-day vulnerability in SonicWall SSL VPNs, targeting even fully patched devices with multifactor authentication (MFA) and rotated credentials. Multiple intrusions were observed in late July 2025.” ([Security Affairs](#))

The average cost of a data breach in the US has shot to a record \$10 million. “For the first time in five years, the average costs associated with a data breach globally have fallen, dropping to \$4.4 million, according to data from IBM; however, they also estimate that the average cost of a data breach is more than \$10 million due to rising detection system expenses and regulatory penalties.” ([The Record](#))

Google tweaks its vulnerability disclosure. “Security experts laud Google for trying out a new approach to publicizing flaws found by its in-house bug hunters, meant to get patches more rapidly into end users' hands. Under a trial policy effective immediately, Google's Project Zero team will publish a general alert to the public within seven days.” ([Data Breach Today](#))

Mozilla warns of phishing attacks targeting add-on developers. “Mozilla issued a warning about an active phishing campaign targeting developers on its official add-on repository. Mozilla's add-on platform hosts over 60,000 browser extensions and more than 500,000 themes.” ([Bleeping Computer](#))

PXA Stealer: Evasive cybercrime campaign. “Researchers uncovered an ongoing infostealer campaign using the Python-based PXA Stealer. The campaign has infected systems in over 62 countries, exfiltrating 200,000 passwords, hundreds of credit card records, and millions of browser cookies. The attackers are linked to Vietnamese-speaking cybercriminal circles, monetizing stolen data through a Telegram-powered subscription ecosystem. Delivery methods include sideloading legitimate signed software (e.g., Haihaisoft PDF Reader, Microsoft Word 2013) with concealed malicious DLLs. The malware targets a wide range of browsers, cryptocurrency wallets, VPNs, and applications, as well as specific financial and cryptocurrency-related websites.” ([SentinelOne](#))

Ransomware gangs are now expanding to physical threats in the real world. “Cybersecurity researchers Semperis claim that over the past 12 months, in 40% of ransomware incidents, the CEOs of the affected company were also physically threatened, which rises to 46% among US-based organizations. But even paying up may not be enough, as the research found more than half (55%) of organizations that paid a demand did so multiple times, with nearly a third (29%) of those firms paying three or more times, and 15% were not even sent decryption keys, or received corrupted keys.” ([Cybersecurity Review](#))

THREATS OF THE WEEK

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

New Attack Surface?

Summary

Sonatype researchers reported that North Korean hackers are conducting an ongoing [campaign](#) to plant malicious code in open-source repositories. Many of the malicious packages used typosquatting and brand impersonation tactics and have impacted an estimated 36,000 developers. Because the code may never be verified, it may permit persistent backdoors.

This campaign appears to have specifically targeted developers in DevOps and CI/CD-heavy environments. Researchers attribute this latest campaign to the Lazarus Group, which intends to “[turn] open-source ecosystems into sophisticated delivery mechanisms for cyberespionage,” reports [Recorded Future](#).

While smaller institutions may have limited in-house development solutions, third-party service providers often rely on internal code development for the banking solutions they provide clients, which can touch restricted and confidential information.

Scattered Spider Update 3

Summary

On 30 July, members of the National Council of ISACs published a [report](#) on the criminal group Scattered Spider. The report provides an overview of the threat group’s activity and tradecraft, and offers key recommendations for mitigation.

This report coincides with the Cybersecurity Infrastructure and Security Agency’s (CISA) [updated](#) joint cyber advisory stating Scattered Spider’s social engineering tradecraft includes tricking IT employees into provide the threat actors with sensitive information so that they can transfer login credentials to their own devices. Furthermore, Scattered Spider was noted as monitoring internal incident response communications by creating false identities in target environments and subsequently creating fake social media profiles to backstop the false identities.

Scattered Spider was also reported as using RattyRAT, a Java-based remote access trojan (RAT) used for persistence and internal reconnaissance, and the DragonForce ransomware to encrypt the victims’ data. The report stated that, according to trusted third parties, the threat actor may have used DragonForce ransomware to encrypt VMware Elastic Sky X integrated servers in recent incidents.

The updated advisory underscores how Scattered Spider remains a threat to the financial sector. However, it is still uncertain whether the [10 July arrests](#) of suspected Scattered Spider members in the UK will have an impact on the group’s operational tempo.

THREAT INTELLIGENCE UPDATE

Improving Cyber Hygiene

Conducting proactive threat hunting yields lessons learned.

Summary

Last week, CISA issued a [joint cybersecurity advisory](#) following the conclusion of a proactive government threat hunt engagement – led by CISA with the support of US Coast Guard (USCG) analysts – at a US critical infrastructure organization.

During this engagement, CISA did not identify evidence of malicious cyber activity or threat actor presence on the organization’s network, but did identify cybersecurity risks, including:

- Insufficient logging
- Insecurely stored credentials
- Shared local administrator (admin) credentials across many workstations
- Unrestricted remote access for local admin accounts
- Insufficient network segmentation configuration between IT and operational technology (OT) assets
- Several device misconfigurations.

While no malicious activity was identified, critical infrastructure organizations are advised to review and implement the mitigations listed in the advisory to prevent potential compromises and better protect US infrastructure.

Remediation

CISA's report encourages all organizations to take proactive measures to enhance their cybersecurity posture, noting their recommendations can be used to inform other organizations' defense measures. The findings and general practices to strengthen cybersecurity for operational technology environments align with CISA and the National Institute of Standards and Technology's (NIST) [Cross-Sector Cybersecurity Performance Goals \(CPGs\)](#), with mitigations provided in the USCG Cyber Command's (CGCYBER) [2024 Cyber Trends and Insights in the Marine Environment \(CTIME\) Report](#).

[Download the report.](#)

JUST FOR COMMUNITY INSTITUTIONS

Automated File Analysis and Aggregated Results

Summary

Malicious cyber adversaries continue to develop, advance, and use complex malware that threatens to disrupt critical infrastructure and services Americans use every day. To combat these threats, cybersecurity analysts work to figure out how the malware operates, what artifacts it leaves behind, and how to prevent it in the future. Historically, this work is a manual effort.

CISA's [Thorium](#) is a no-cost, scalable platform for automated file analysis and aggregated results from multiple tools. Cybersecurity teams in large or small organizations across mission functions — from software analysis to digital forensics to incident response — may benefit by using Thorium.

Thorium allows cyber defenders to integrate their preferred tools into a single platform that orchestrates customized and automated analysis workflows at scale, analyzing large amounts of malware quickly. Users can add and remove tools quickly as malware threats evolve.

Analysts can use Thorium for:

- **Easy tool integration:** Integrate command-line tools as Docker images (free and open source software [FOSS], commercial off-the-shelf [COTS], custom, etc.). With additional configuration, they can integrate virtual machine (VM) and bare-metal tools.
- **Filtering:** Filter tool results using tags and full-text search.
- **Security:** Control how submissions, tools, and results are accessible through strict group-based permissions.
- **Scalability:** Scale with hardware using Kubernetes and ScyllaDB to meet workload requirements. Out of the box, Thorium is configured to ingest over 10 million files per hour per permission group and schedule over 1,700 jobs per second, while maintaining fast results queries.
- **Pipelining:** Define event triggers and tool execution sequences to automate workflows.
- **Workflow integration:** Fully control Thorium via RESTful API and get started using either a web browser or a command-line utility.
- **Result aggregation:** Aggregate and index tool outputs for further analysis or ingestion by downstream processes and external platforms.
- **Tool sharing:** Import and export tools for ease of sharing across cyber defense teams.

Example Use Cases

-
- **Malware analysis:** Triage files using static and dynamic analysis tools. Aggregate results from multiple tools to trigger further analysis and outputs.
 - **Host forensics:** Automatically process forensic artifact files (emails, memory images, disk images, etc.) and generate intermediate analysis results.
 - **Scaled tool testing:** Assess tool performance on benchmark datasets to speed up development and troubleshooting.

Prerequisites

Thorium requires a deployed Kubernetes cluster, block store, and object store. Familiarity with Docker containers and computing cluster management is also necessary for successful deployment.

Institutions can obtain a copy of Thorium and more detailed installation instructions at <https://github.com/cisagov/thorium>.

GOVERNMENT AND REGULATORY NEWS

NCUA Launches Webpage Providing Tips for the Examination Document Request Process

Summary

The National Credit Union Administration (NCUA) launched a [webpage on ncu.gov](#) that provides tips for how examiners and credit unions can coordinate and improve the efficiency and effectiveness of the examination document request process. The page was created in response to credit union post-exam survey feedback that raised concerns about examiners sending duplicate requests for documents that were already provided.

The webpage explains how an NCUA examiner-in-charge can promote a well-organized and effective examination during the exam notification and document request process. The site also includes tips for credit unions to consider when naming and organizing requested files based on the secure method they use to provide the documents.

The NCUA encourages credit unions to continue providing feedback through the post-exam survey. All feedback is reviewed and considered when determining if changes need to be made to the credit union examination process.

See: [Tips on Starting an Exam Efficiently](#).

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 can enroll in the Member Services app to attend events.

- 7 August | Fraud Threat Call
- 18 August | Monthly CIAC Webinar
- 27 August | CIAC and COFFE Open Forum
- 27 August | Member Success Webinar
- 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](#).