

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

Week of 16 June 2025 | Issue 287

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
- Account Takeover
- Advance Fee
- Business Email Compromise
- CEO Impersonation
- Customer Impersonation ATO
- Fraud Department Impersonation
- Withdrawal Impersonation Fraud

System Vulnerabilities

Amazon, Apache, Apple, Atlassian, Aveva (3), CA OPS, Citrix, Crucial Reponse, Cygwin, Debian, Dell, Dover, F5, Fortinet, Fuji Electric, GitLab, Google, HP, HPE, IBM, Lenovo, Linux, LS Electric, Microsoft, Mozilla, Nessus Agent, OpenShift, Oracle, Palo Alto, PAN-OS, PTZOptics, Red Hat, Siemens (8), SUSE, TP-Link, Trend Micro, and Ubuntu.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Adult Dating, Bonita21 (ATO), dd100150 (ATO), FakeUpdate, EFT APAR Update, Follow-Up, For Review and Approval, Important Update, Law Office of Peter Sloan, APC, james129 (ATO), monyymoon (ATO), NEW PROPERTY OFFER, nshimmin (ATO), Online Enrollment, Packages Posing as Utilities Delete Project Directories, Passwords, Payment Proposal, Payworks Payroll, Rakuten, REQUEST FOR TITLE WORK, ServiceStar Capital MGT, Sign Here : DocuSign, support.viewyourstatementonline, You have received Contract Payment Proposal document via Onedrive -Assigned to.

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
- Grandoreiro
- GremlinStealer
- InterLock Ransomware (NodeSnake RAT)
- Latrodectus
- MetaStealer
- Mispadu
- Nitrogen
- StilachiRAT
- SocGholish
- SocksShell (aka Zapcat Supper)

- Direwolf Ransomware Group
 - FormBook
 - GolangGhost
 - GorillaBot
 - SparkRAT
 - SQUIDGATE (TerraLoader)
 - Xloader
 - Xworm
 - Zloader
-

NEWS AND RISK INFORMATION

GrayAlpha uses diverse infection vectors to deploy PowerNet Loader and NetSupport RAT. “Insikt Group has identified new infrastructure linked to GrayAlpha — a threat actor overlapping with the group commonly known as FIN7 — including domains utilized for payload distribution and additional IP addresses believed to be part of the threat actor’s infrastructure.” ([Recorded Future](#))

Multi-stage malware attack on PyPI: “chimera-sandbox-extensions” malicious package threatens Chimera sandbox users. “A malicious Python package named chimera-sandbox-extensions was discovered on PyPI [Python Package Index, a software library for Python programming], targeting developers using the chimera-sandbox environment. The package is designed to steal sensitive infrastructure-specific data.” ([jfrog](#))

SEC scraps proposed cybersecurity rules for investment advisers, market participants. “The Securities and Exchange Commission has withdrawn proposed cybersecurity regulations for [investment advisers](#) and [companies participating in securities markets](#). The decisions, announced on Thursday with no explanation, mark potentially significant reversals of the commission’s plans to subject major financial entities to cyber requirements for the first time.” ([Cybersecurity Dive](#))

Smartwatches tabbed as latest vehicle for air-gapped system attacks. “Researchers say that the latest vehicle for covert data extraction from secured systems could be sitting on your wrist. [A paper](#) published by the Ben-Gurion University of the Negev in Beer Sheva, Israel, details how a smartwatch could possibly be employed to lift secured data from [air-gapped machines](#) by intercepting electronic signals.” ([SCWorld](#))

Trend Micro patches four 9.8 bugs in encryption PolicyServer products. “The bugs were a series of remote code execution (RCE) and authentication bypass flaws in [Trend Micro’s] Apex Central and Trend Micro Endpoint Encryption (TMEE) PolicyServer products.” ([SC World](#))

THREATS OF THE WEEK

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

Phishing and Account Takeover Campaigns

Summary

FS-ISAC members report various phishing campaigns aimed at taking over existing financial accounts. Additionally, members report observing password spraying attempts — attacks applying a small set of commonly used passwords across multiple accounts to gain unauthorized access.

Frontline branch employees should be trained to “[know their customers](#)” and identify suspicious financial activity, such as large dollar deposits and withdrawals, excessive ATM cash withdrawals, wire transfers, etc.

Below are additional techniques institutions can use to identify account takeover:

- Instant verification validates real customers and improves the customer experience while reducing the opportunity for fraud
 - Real-time account verification compares data entered by a user with data collected from the website of the financial institution servicing the account
 - Trial deposit verification validates the external account with two small trial deposits while the account holder confirms the amount of the two deposits
 - Identity verification provides financial institutions access to multiple third-party data sources and the ability to verify a customer’s or member’s identity in real time
-

- Out-of-wallet questions are designed to trick the fraudster by asking questions only the legitimate customer could answer

Erie Insurance Cyber Attack

Summary

On 7 June, Erie Insurance [reported](#) that it experienced a cyber attack that caused widespread outages and business disruption. The company stated it took “protective action” to secure its systems, which included shutting down systems. Customers [have](#) not been able to log onto the customer portal and reported difficulties making claims or receiving company paperwork.

The full scope, impact, and nature of the attack are not yet known, but the insurer is cooperating with law enforcement and is conducting a forensic analysis. The insurer has warned customers it will not call or email to request payments during the outage.

THREAT INTELLIGENCE UPDATE

Ransomware Actors Exploit Utility Billing Software Provider

Institutions are urged to prevent ransomware activity.

Summary

Ransomware threat actors have been exploiting flaws in SimpleHelp remote support software to gain unauthorized access to systems and disrupt services in several utility companies. In an effort to combat cybercrime, the Cybersecurity and Infrastructure Security Agency (CISA) published the [advisory](#), “Ransomware Actors Exploit Unpatched SimpleHelp Remote Monitoring and Management to Compromise Utility Billing Software Provider.”

These actors likely exploited [CVE-2024-57727](#) to access downstream customers’ unpatched SimpleHelp RMM for disruption of services in double extortion compromises.

Third-Party Risk

Recommended mitigations for third-party vendors, vulnerable downstream customers, and end users should be implemented immediately.

Institutions should check if any service providers are using SimpleHelp and verify whether SimpleHelp is embedded or bundled in vendor-owned software or if a third-party service provider leverages SimpleHelp on a downstream customer’s network, then identify the SimpleHelp server version at the top of the file `<file_path>/SimpleHelp/configuration/serverconfig.xml`.

If version 5.5.7 or prior is found or has been used since January 2025, third-party vendors should:

1. Isolate the SimpleHelp server instance from the internet or stop the server process.
2. Immediately upgrade to the latest SimpleHelp version per SimpleHelp’s security vulnerability advisory.
3. Contact downstream customers to direct them to take actions to secure their endpoints and undertake threat hunting actions on their network.

Ransomware Impact

If a system has been encrypted by ransomware, CISA recommends the following actions:

1. Disconnect the affected system from the internet.
2. Use clean installation media (e.g., a bootable USB drive or DVD) to reinstall the operating system. Ensure the installation media is free from malware.

3. Wipe the system and only restore data from a clean backup. Ensure data files are obtained from a protected environment to avoid reintroducing ransomware to the system.

CISA observes that this incident reflects a broader pattern of ransomware actors targeting downstream organizations through unpatched versions of SimpleHelp RMM since January 2025.

All organizations using SimpleHelp RMM should review the advisory and implement the recommended actions immediately.

Additional remedial actions are recommended in the [CISA alert](#).

JUST FOR COMMUNITY INSTITUTIONS

CAPS Registration

Summary

Registration for Cyber Attack Against Payment Systems (CAPS) exercises for community institutions will open at the end of June. The exercises will run from 2 September through 17 October 2025.

Registered members receive an after-action report and aggregate unattributed data. Participating firms will evaluate their results in-house to gain insight into their resilience profile.

A quick note on what's new and exciting for 2025 CAPS:

- The exercise will be in one part, allowing us to streamline and tighten the material (while still making it enjoyable and useful), remove redundancies, and be more attractive to management and additional attendees.
- We are improving the survey and welcoming user feedback.
- We're introducing a big change in 2025: we intend to generate dialogue with AI voices vs. volunteer actors.
- We plan to offer a Spanish-language version.

Registrants will access all CAPS materials in one of three CAPS VIDEO channels. Q&A will be available in a separate Connect channel.

RESILIENCE UPDATE

Military Action in the Middle East

Summary

On 12 June, Israel [launched](#) attacks on Iran, targeting nuclear facilities and Iranian military officials. US Secretary of State Marco Rubio issued a [press release](#) stating the United States is “not involved in strikes against Iran” and that “Iran should not target US interests or personnel.”

On 13 June, Iran launched retaliatory attacks against Israel, firing multiple rounds of missiles towards Tel Aviv. Officials [stated](#) that the US military diverted Iranian missiles targeting Israel. Continued escalation of kinetic actions is likely to drive cyber activity by threat actors on both sides of the conflict and could impact financial institutions.

At the time of writing, the **direct cyber threat to the financial sector is unlikely to have risen significantly outside of the immediate conflict zone**. We have seen no intelligence to indicate an increase in an Iranian cyber threat to the financial sector. However, this remains a rapidly evolving situation; our assessments may change at short notice.

Considering intent and capability, **FS-ISAC assesses that Iranian cyber activities present a moderate cyber threat to the financial sector outside of Israel and regional opponents such as Saudi Arabia**.

The **primary Iranian threat to the financial sector pertains to the technology providers based in Israel as well as Israeli financial institutions**, which now face an increased cyber threat from pro-Iran hackers and Iranian state-sponsored cyber actors.

The full report is available in Share, [Iranian Cyber Threat Assessment for the financial sector, linked to the increased escalations between Israel and Iran.](#)

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- [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:](#)
 - [Ariel Weintraub: Ensure Your Supply Chain Continuity – Even Under Pressure](#)
 - [Debbie Janeczek: How to Prepare for the Quantum Revolution](#)
 - [Meg Anderson: Lessons in Cyber Leadership From a Trailblazing CISO](#)
 - [Susan Koski: How to Manage the Move to the Post-Password Cyber Landscape](#)
 - [Jochen Friedemann: The Fun Side of Financial Services Cybersecurity](#)
- [FinCyber Today Podcast Season 1:](#)
 - [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](#)
- 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

- 25 June | CIAC and COFFE Open Forum
- 25 June | Member Success Session
- 21 July | Monthly CIAC Webinar
- 30 July | CIAC and COFFE Open Forum
- 5-8 October | Americas Fall Summit [**Registration now open**]

[View all Americas events.](#)



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](#).