

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

Week of 26 May 2025 | Issue 284

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 their ability to operate and avoid compliance, economic, legal, regulatory, and reputational impact.

This Week's Threats

Fraud Campaigns

- ACH Wire Fraud
- Business Email Compromise

System Vulnerabilities

Amazon, Apache, CA OPS/MVS Event Management, [Consilium](#), Cygwin, Google, [Instantel](#), [Lantronix](#), Lenovo, Linux, Mozilla, [Rockwell Automation](#), [Samsung](#), [Santesoft](#), and [Siemens](#) (2).

Themed Phishing and Smishing Campaigns

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

Subject Keywords: A TASK DETAILS, ACH/Wire Request, Action Required: Update Direct Deposit Info, Adult Dating, Ascend File, BUILDER INVESTMENT GROUP, Business Coach, Compensation Review, Confidential File Portal Sent, Daniel Green, Fake Investment, Gift Card Request, Missed a Call – Voicemail Available, MST, Password Expiration, Paycheck Adjustment Request, Payment Order, Payroll Diversion, Payoff Statement, Please help sort this, Proposal, Rakuten, Sent you a file 7947493839383939, ShareFile Attachment, Staff Documentation, Threatening (gmail), Voigt Law Group, and You have received a secure message.

Threats, Malware, Cyber Campaigns, and Adversaries

- Astaroth
- AsyncRAT
- BeaverTail (InvisibleFerret)
- BitStep RAT
- Bumblebee (aka ShellSting, Shindig)
- CellikRAT V4.0 Malware
- ChainedDown malware
- ChainedRAT
- ClickFix/ClearFake
- ColdRiver Group
- FormBook
- GolangGhost
- GorillaBot
- Grandoreiro
- GremlinStealer
- Latrodectus
- MetaStealer
- Mispadu
- Nitrogen
- StilachiRAT
- SocGholish
- SocksShell (aka Zapcat Supper)
- SparkRAT
- SQUIDGATE (TerraLoader)
- Venom Spider
- Xloader
- Xworm
- Zloader

NEWS AND RISK INFORMATION

AI-Generated TikTok videos used to distribute infostealer malware. “A new campaign is exploiting TikTok’s vast user base and viral content model to distribute information-stealing malware, including Vidar and StealC. It uses AI-generated videos to socially engineer users into executing malicious PowerShell commands.” ([InfoSecurity Magazine](#))

Decentralized crypto platform Cetus hit with \$223 million hack. “Cetus, a decentralized cryptocurrency exchange operating on the Sui blockchain, suffered a significant cyber attack on Thursday, 22nd May, resulting in the theft of approximately \$223 million.” This is the second crypto firm incident in a single week. ([The Record](#))

Fake CAPTCHA attacks deploy infostealers and RATs in a multistage payload chain. “A recent wave of phishing campaigns is exploiting fake CAPTCHA pages to trick users into executing malicious commands via the Windows Run dialog. These attacks deliver multistage payloads using obfuscated JavaScript embedded in MP3 or PDF files.” ([Trend Micro](#))

The fintech sector faces mounting third-party security breach risks. “Almost 42% of data breaches impacting top fintech companies can be traced back to third-party vendors, with a further 12% linked to fourth-party exposures. The findings, drawn from an analysis of 250 leading fintech firms worldwide, highlight the systemic risks facing the financial sector’s supply chain despite robust internal cybersecurity practices.” ([Business Wire](#))

Hackers target Coinbase users in an advanced targeted social engineering hack. In a follow-up from last week’s news, GB Hackers reports, “A sophisticated social engineering campaign has been actively targeting Coinbase users since early 2025, resulting in over \$300 million in annual losses and \$45 million in a single week in May.” ([GB Hackers](#))

KrebsOnSecurity hit with huge DDoS attack via Aisuru botnet. “KrebsOnSecurity, a prominent cybersecurity blog, was recently targeted by a massive, distributed denial-of-service (DDoS) attack peaking at 6.3 Tbps. The attack, attributed to the Aisuru botnet, is one of the largest recorded to date.” ([HackRead](#))

Naughty AI: OpenAI o3 spotted ignoring shutdown instructions. “Holding down a misbehaving device’s power button to forcibly turn it off and on again remains a trusted IT tactic since the dawn of the digital age. Enter a new challenge: artificial intelligence tools that refuse to comply with shutdown requests when they conflict with goals they’ve been set.” ([Data Breach Today](#))

THREATS OF THE WEEK

Cyber threat targeting Commvault, highlighting this week’s risks.

Cyber Threat Activity Targeting Commvault’s SaaS Cloud Application

Summary

Threat actors may have accessed client secrets for Commvault’s (Metallic) Microsoft 365 (M365) backup software-as-a-service (SaaS) solution, hosted in Azure. Commvault is monitoring the activity that may have allowed unauthorized access to Commvault’s customers’ M365 environments, where application secrets are stored by Commvault.

The Cybersecurity Infrastructure and Security Agency (CISA) believes the threat activity may be part of a larger campaign targeting various SaaS companies’ cloud applications with default configurations and elevated permissions.

Action to be Taken

1. Monitor Entra audit logs for unauthorized modifications or additions of credentials to service principals initiated by Commvault applications/service principals.
 - Handle deviations from regular login schedules as suspicious.
 - For more information, see NSA and CISA's [Identity Management guidance](#), as well as CISA's [Identity, Credential, and Access Management \(ICAM\) Reference Architecture](#) report.
2. Review Microsoft logs (Entra audit, Entra sign-in, unified audit logs) and conduct internal threat hunting in alignment with documented organizational incident response policies.
3. For single-tenant apps, implement a conditional access policy that limits authentication of an application service principal to an approved IP address that is listed within Commvault's allow-listed range of IP addresses.
 - **Note:** A Microsoft Entra Workload ID Premium License is required to apply conditional access policies to an application service principal and is available to customers at an additional cost.
4. Customers who have control over Commvault's application secrets should rotate their application secrets and credentials on Commvault Metallic applications and service principals [available between February and May 2025](#).
 - If applicable, customers should establish a policy to regularly rotate credentials at least every 30 days.
5. Review the list of Application Registrations and Service Principals in Entra with administrative consent for higher privileges than the business needs.
6. Implement general M365 security recommendations outlined in CISA's [Secure Cloud Business Applications \(SCuBA\) Project](#).

Precautions for On-Premise Software Versions

1. Where technically feasible, restrict access to Commvault management interfaces to trusted networks and administrative systems.
2. Detect and block path-traversal attempts and suspicious file uploads by deploying a Web Application Firewall and removing external access to Commvault applications [CSA-250502].
3. Apply the patches provided and monitor activity from unexpected directories, particularly web-accessible paths.

For additional information, visit [Notice: Security Advisory \(Update\)](#).

THREAT INTELLIGENCE UPDATE

Deepfake Threats

It's time to talk about deepfake scams.

Summary

As technology continues to improve, deepfakes are harder to identify. Criminals use deepfaked images, voice, or video for:

- Phishing scams
- Data breaches
- Hoaxes
- Reputation smearing
- Election manipulation
- Social engineering
- Automated disinformation attacks
- Identity theft (synthetic ID)
- Financial fraud
- Blackmail

Creating Realistic Deepfakes

There are more than sufficient videos and software applications on the internet to help beginners, intermediates, and experts create deepfakes.

- To create a deepfake video, you only need an image editor (e.g., Deepfake Studio, Face Swap, Face App, etc.), 20 minutes of quality video of the person you are trying to deepfake, and a video generator. With some practice, you'll achieve a convincing deepfake video.
- To create a deepfake voice, you'll need an application (e.g., Speechify, WellSaid, etc.) and a 30-second voice recording of the person you want to clone. Follow the application prompts, then type what you want the cloned voice to say in the dialogue box. That's all it takes to deepfake a voice.

It must be noted that deepfakes aren't necessarily malicious. Financial institutions may create a deepfake for legitimate business purposes, such as training or marketing. But the technology that allows financial firms to make deepfakes for reputable uses is also available to threat actors looking to scam you.

Spotting Deepfakes

In November 2024, FinCEN released an [alert](#) recommending some red flags for financial institutions. Take precautions when:

- A customer's photo is internally inconsistent (e.g., looks altered) or is inconsistent with their other identifying information (e.g., the date of birth indicates that the person is much older or younger than the photo would suggest).
- A customer presents multiple identity documents that are inconsistent with each other.
- A customer uses a third-party webcam plugin during a live verification check. Alternatively, a customer attempts to change communication methods during a live verification check due to excessive or suspicious technological glitches during the remote verification of their identity.
- A customer declines to use multifactor authentication to verify their identity.
- A reverse-image lookup or open-source search of a customer's identity photo matches an image in an online gallery of generative artificial intelligence (AI)-produced faces.
- A customer's photo or video is flagged by commercial or open-source deepfake detection software. Generative AI-detection software spots the potential use of AI-produced text in a customer's profile or responses to prompts.
- A customer's geographic or device data is inconsistent with the customer's identity documents.

Take the Quiz

Now that you have obtained information about deepfakes, test your knowledge by taking these quizzes from the BBC and iProov, below.

- BBC [Celebrity Quiz](#)
- iProov [Image and Video Quiz](#)

What if You've Been Scammed?

It's important to include deepfake scams in your Incident Response and security awareness programs so that employees are aware of deepfake threats, understand how they work, and know to whom they should report incidents. If your institution is the victim of a deepfake:

- Notify local police: File a police report if the deepfake involves criminal activity like fraud, harassment, or defamation.
- Notify the FBI's Internet Crime Complaint Center (IC3): Report deepfakes used in financial scams or other cybercrimes.
- Use a cybercrime reporting portal: If applicable, report to a national or regional cybercrime reporting portal.
- Preserve digital evidence: Maintain copies of all digital evidence.
- Provide evidence: Include details about the deepfake, how it was used, and any potential harm it caused.

Resources

[Contextualizing Deepfake Threats to Organizations](#), a cybersecurity information sheet authored by the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and CISA.

JUST FOR COMMUNITY INSTITUTIONS

AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems

Data security guidance for Artificial Intelligence.

Summary

CISA, the NSA, the FBI, and international partners released *AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems*.

This guidance highlights the critical role of data security in ensuring the accuracy, integrity, and trustworthiness of AI outcomes. It outlines key risks that may arise from data security and integrity issues across all phases of the AI lifecycle, from development and testing to deployment and operation.

[Download the document.](#)

FRAUD UPDATE

Cyber Fraud Prevention Framework for Financial Institutions

Summary

Were you aware of FS-ISAC's Cyber Fraud Prevention Framework for financial institutions?

The Framework provides an actionable model to strengthen collaboration between cybersecurity, fraud, financial crime, and anti-money laundering (AML) teams. Organizations can leverage the Framework's fraud response protocol to identify vulnerabilities earlier in the attack lifecycle, enhancing threat visibility and strengthening fraud controls.

The Framework breaks the lifecycle of a cyber-fraud attack, i.e., fraud conducted on cyber channels, into **five phases**:

1. **Reconnaissance:** Threat actors gather intelligence, set up infrastructure, and plan for attempted fraud.
2. **Initial Access:** Attackers gain a foothold for fraud against a consumer, financial services institution, or other entity, such as a third-party vendor.
3. **Positioning:** Threat actors manipulate account information, credentials, or payment details to prepare for fraud execution.
4. **Execution:** Stolen data is monetized through unauthorized transactions or fraudulent fund transfers.
5. **Monetization:** The stolen funds are transferred to the threat actor.

Download your [free copy](#).

GOVERNMENT AND REGULATORY NEWS

NCUA Invites Stakeholder Feedback on Operations and Initiatives

Summary

National Credit Union Administration Chairman Kyle S. Hauptman invited stakeholders to provide suggestions and feedback on the agency's operations and initiatives to aid in developing the NCUA's 2026–2030 Strategic Plan, which guides the agency's operational and budgetary priorities.

Review [NCUA's 2022–2026 Strategic Plan](#).
[Read the entire press release](#).

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- [Navigating Cyber 2025](#)
- [Cyber Fraud Prevention Framework for Financial Institutions](#)
- [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 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

- 3 June 2025 | FinCyber Today Canada
- 16 June | May CIAC Meeting
- 25 June | June CIAC Open Forum
- 5-8 October | Americas Fall Summit

[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](#).