

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

Week of 19 May 2025 | Issue 283

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 transfers
- Business Email Compromise

### System Vulnerabilities

[ABUP](#), Amazon, Apple, Arista, [Assured Telematics](#), Atlassian, [AutomationDirect](#), Cisco, [Danfoss](#), Debian, Dell, F5, GitLab, Google, IBM, [Ivanti](#), Lenovo, Linux, [Mdaemon](#), Microsoft, [Mitsubishi](#), Mozilla, [National Instruments Circuit Design Suite](#), Red Hat, [Siemens](#), [Schneider](#), Spring Security, [Srimax](#), SUSE, Ubuntu, [Vertiv](#), VMware, [Zimbra](#), and [ZKTeco](#).

### Themed Phishing and Smishing Campaigns

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

**Subject Keywords:** Adult Dating, BID - Vantagepoint Consulting, Confidential File Portal sent you ProposalReview\_and\_Approval for White Mountain, Consulting, Gift Card Request, Intuit, Law firm Documents available, Matsui Securities, Motivational Messages, Notification, Password Expiry, Payoff Statement, Payroll Diversion, Proposal, QuickBooks, Remittance/Invoice, Request for confirmation to continue using the service, RingCentral, SAP, SSA ScreenConnect, and You have recieved an important voice mail.

### 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
- Latrodictus
- MetaStealer
- Mispadu
- Nitrogen
- StilachiRAT
- SocGhosh
- SocksShell (aka Zapcat Supper)
- SparkRAT
- SQUIDGATE (TerraLoader)
- Venom Spider
- Xloader
- Xworm
- Zloader

## NEWS AND RISK INFORMATION

**FS-ISAC Navigating Cyber 2025 report is available.** FS-ISAC's annual [Navigating Cyber](#) report is available for download. The report highlights the top cyber threats challenging the financial services sector today, including surging fraud and scams enabled by generative AI (GenAI), attacks on suppliers that impact critical operations, more opportunities for threat actors to exploit geopolitical and economic conflict and uncertainty, and the increasing sophistication of long-established attack types such as distributed denial of service (DDoS) attacks and ransomware. The report also provides key predictions for 2025 and beyond, offering firms valuable insights to help strengthen their cybersecurity programs. ([FS-ISAC](#))

**Google Chrome data leakage bug confirmed as actively exploited.** "A Google Chrome vulnerability allowing the leak of OAuth codes was [added to the Known Exploited Vulnerabilities catalog](#) by the Cybersecurity & Infrastructure Security Agency (CISA) on Thursday. The flaw, tracked as [CVE-2025-4664](#), is due to insufficient policy enforcement in the Google Chrome Loader." ([SC Media](#))

**How the Signal knockoff app TeleMessage got hacked in 20 minutes.** "A critical breach of the TeleMessage Signal clone (TM SGNL) exposed sensitive data due to severe misconfigurations. Exploited in under 20 minutes, the breach compromised credentials, unencrypted chat logs, and encryption keys of users." ([Wired](#))

**LockBit leaks reveal drive to recruit ransomware newbies.** "Ransomware groups continue to find innovative new ways to shake down organizations large and small in their pursuit of ransom payoffs. For the LockBit group, one tweak was to debut a "lite" version of its ransomware portal that appears to have amassed dozens of very inexperienced business partners." ([Data Breach Today](#))

**New 'Defendnot' tool tricks Windows into disabling Microsoft Defender.** "A new tool named Defendnot demonstrates a critical method to disable Microsoft Defender on Windows systems by exploiting an undocumented Windows Security Center (WSC) API." ([Bleeping Computer](#))

**New Nitrogen ransomware targets financial firms in the US, UK, and Canada.** "Nitrogen ransomware, first publicly identified in September 2024, has emerged as a significant threat targeting organizations across the finance, construction, manufacturing, and technology sectors." ([Hack Read](#))

**Thousands of WordPress sites are at risk due to a critical Crawlomatic plugin vulnerability.** "A critical vulnerability ([CVE-2025-4389](#)) in the Crawlomatic Multisite Scraper Post Generator WordPress plugin allows unauthenticated attackers to upload arbitrary files, leading to remote code execution." ([The Cyber Express](#))

---

## THREATS OF THE WEEK

Russia's GRU attacks Western companies, and Scattered Spider targets US retailers, highlighting this week's risks.

### **Russian GRU Cyber Actors Targeting Western Logistics Entities and Tech Companies**

#### **Summary**

On 21 May, CISA issued a joint cybersecurity advisory highlighting a Russian state-sponsored cyber campaign. The threat actors are targeting Western logistics entities and technology companies, including those involved in coordinating, transporting, and delivering foreign assistance to Ukraine. Since 2022, Western logistics entities and IT companies have faced an elevated risk of targeting by the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (85th GTsSS), military unit 26165 — tracked in the cybersecurity community under several names (see [Cybersecurity Industry Tracking](#)).

Executives and network defenders at logistics entities and technology companies should recognize the elevated threat of Unit 26165 targeting, increase monitoring and threat hunting for known tactics,

---

techniques, and procedures (TTPs) and indicators of compromise (IOCs), and posture network defenses with a presumption of targeting.

## Scattered Spider Now Targeting US Retailers

### Summary

On 14 May, [Google Threat Intelligence Group told Bleeping Computer](#) it is monitoring ransomware and extortion operations against US retailers. The activity is possibly connected to Scattered Spider as the activity resembles that of Scattered Spider's recent exploitation of UK retailers.

John Hultquist, Chief Analyst, Google Threat Intelligence Group, stated, "The actor ... has a history of focusing their efforts on a single sector at a time, and we anticipate they will continue to target the sector in the near term."

Organizations with valuable data and critical availability needs are equally at risk.

### Remediation

Institutions and their retail customers should secure privileged accounts, implement phishing-resistant multi-factor authentication (MFA), and validate every Help Desk identity request.

## Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data

### Summary

On 21 May, the Federal Bureau of Investigation (FBI) and CISA released a joint cybersecurity advisory, [LummaC2 Malware Targeting U.S. Critical Infrastructure Sectors](#). This advisory details TTPs and IOCs linked to threat actors deploying LummaC2 malware. This malware is capable of infiltrating networks and exfiltrating sensitive information and poses a serious threat to vulnerable individuals' and organizations' computer networks across the US critical infrastructure sectors.

In May 2025, threat actors were observed using LummaC2 malware, underscoring the ongoing threat. The advisory includes IOCs tied to infections from November 2023 through May 2025. Organizations are strongly urged to review the advisory and implement the recommended mitigations to reduce exposure and impact.

On 21 May, the Justice Department [announced](#) the unsealing of two warrants authorizing the seizure of five internet domains used by malicious cyber actors to operate the LummaC2 information-stealing malware service.

[Read the entire alert.](#)

[Read the entire announcement.](#)

---

## THREAT INTELLIGENCE UPDATE

### Coinbase Breach

8-K report reveals soft dollar impact on restoring operations.

#### Summary

On 14 May, an [8-K](#) filing was released involving a security incident involving Coinbase. The report reveals that Coinbase received an email communication on 11 May 2025 from an unknown threat actor claiming to have obtained information about certain Coinbase customer accounts, as well as internal Coinbase

documentation, including materials relating to customer service and account management systems. The communication demanded money in exchange for not publicly disclosing the following information.

- Customer name, address, phone, and email
- Masked Social Security (last 4 digits only)
- Masked bank account numbers and some bank account identifiers
- Government ID images (e.g., driver's license, passport)
- Account data (balance snapshots and transaction history)
- Corporate data (including documents, training material, and communications available to support agents)

The threat actor did not compromise passwords or private keys or access customer funds. Coinbase believes the threat actor's assertions are credible and that the improper data access was part of a single campaign that succeeded in taking data from internal systems.

The threat actor appears to have obtained this information by paying multiple contractors or support role employees working outside the United States to collect information from internal Coinbase systems to which they had legitimate access. They did not, however, have a clear business need to do so.

Coinbase's security monitoring independently detected those instances and Coinbase immediately terminated the personnel involved. It also implemented heightened fraud-monitoring protections and warned customers whose information was potentially accessed to prevent misuse of any compromised information.

Coinbase has not paid the threat actor's demand and is cooperating with law enforcement's investigation.

### **Financial Impact**

Coinbase estimates *that* remediation costs and voluntary customer reimbursements will cost *\$180 million to \$400 million USD*. Further review of potential losses, indemnification claims, and potential recoveries could significantly change its estimate.

---

## **JUST FOR COMMUNITY INSTITUTIONS**

### **May CIAC Webinar Now Available in Video**

This month's webinar provides additional details on TeleMessage and more.

#### **Summary**

May's CIAC webinar is now available in the [CIAC Video Channel](#). Here's a brief snapshot of what our presenters shared:

- Janet West showed us how to use the COI Experience feature in IntelX, where you can register for events, join other Communities of Interest, and more.
- Miranda Dillon gave us this month's Threat Intel Briefing and shared information concerning the TeleMessage security incident, including assessment and remediation steps institutions can take.
- Greg Spicer and Craig Dellinger from Ostrich Cyber-Risk talked about risk assessment and how their tool assesses risk but assigns quantifiable financial risk/loss based on the individual risk category. This is a nice feature to help leadership teams understand the financial impact.

The next CIAC webinar will be held on 16 June 2025, 3:30 p.m. Eastern Time (12:30 p.m. Pacific Time), and will feature a presentation by Travelers.

---

## **FRAUD UPDATE**

### **April Fraud Trend Report Available**

## Summary

FS-ISAC's monthly fraud trend report is available to members.

During April, member sharing by region was composed of 91% AMER, 4% APAC, and 5% EMEA submissions related to fraud. In April, the insurance sub-sector again contributed the majority of fraud-related member reporting, with the securities and investments sub-sector experiencing the largest increase in alerts month-over-month.

Overall, FS-ISAC members reported a variety of attack patterns in April, the most prevalent being business email scam, manipulated invoice, and smishing.

[Read the entire report.](#)

---

## GOVERNMENT AND REGULATORY NEWS

### NCUA Charters African Diaspora Federal Credit Union

#### Summary

The National Credit Union Administration (NCUA) has granted a federal charter and National Credit Union Share Insurance Fund coverage to African Diaspora Federal Credit Union in St. Louis, Missouri.

[Read the Entire Press Release.](#)

### Board Briefed on NCUA's Voluntary Separation Program, Share Insurance Fund Performance

#### Summary

The NCUA Board held its third open meeting of 2025 and received a briefing on the agency's Voluntary Separation Program (VSP) and the performance of the National Credit Union Share Insurance Fund in the first quarter of 2025.

[Read the Entire Press Release.](#)

### NYDFS Urges Virtual Currency Customers to Protect Themselves from Cybercriminals

#### Summary

The New York State Department of Financial Services (NYDFS) is urging consumers to use caution before responding to outreach from individuals who may be falsely claiming to represent virtual currency entities.

Recent reports have indicated that criminals are using stolen personal and consumer account information to trick consumers into believing they are receiving legitimate calls, emails, and texts from a virtual currency company. Cybercriminals often steal sufficient information – Social Security and bank account numbers, images of government IDs, etc. — to credibly impersonate a communication from the consumer's service provider.

#### Risk

These cybercriminals request that customers transfer funds to a new account, tricking consumers into giving their assets to the criminals.

## Remediation

All customers should exercise caution when contacted regarding their accounts or when asked to provide sensitive information or transfer funds. If you receive unsolicited communications about your accounts, you should end the conversation. Do not use the contacts or links provided in these communications. Instead, directly reach out to the company using a contact on the company's public website or another trustworthy source.

Additional steps to protect yourself from scams can be found [here](#).

## Register Now for the Planning for Retirement with Credit Unions Webinar on 28 May

### Summary

May is Older Americans Month, and the National Credit Union Administration's Office of Consumer Financial Protection will host a webinar on the importance of preparing for retirement and how credit unions are helping their members get ready.

The one-hour webinar will take place on Wednesday, 28 May at 1 p.m. Eastern Time. [Registration for this webinar is now open](#).

---

## PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

### Recent Publications

- [Navigating Cyber 2025](#)
- [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

- 28 May | May CIAC Open Forum
- 28 May | Member Success Onboarding Session
- 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](#).