

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

Week of 14 July 2025 | Issue 291

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
- Business Email Compromise
- Check Fraud (High dollar)
- Commercial business targeted
- Crypto Scams
- IT/Tech Support
- Pump-and-Dump Brokerage fraud
- Treasury Management Vishing
- Withdrawal Impersonation Fraud

System Vulnerabilities

ABB, Advantech, ALE OmniAccess, Amazon, Apache, Atlassian, CA Database, CA Workload Automation, Cisco, Citrix, CyberArk, Cygwin, Debian, Dell, Delta Electronics, Ecovacs Deebot, gdk-pixbuf Heap-Based Buffer Overflow, Google, GnuTLS, Hitachi, HP, IBM, IDEC, Ivanti, JD Edwards, Johnson Controls, Kunbus, Lenovo, Leviton, Linux, LITEON, Microsoft, MySQL, NVIDIA, OpenJDK, Oracle, Panoramic, PeopleSoft, Red Hat, Schneider, Siemens, SUSE, Trend Micro, Ubuntu, VMware, WatchGuard, and Wing FTP Server.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Apple ID, Accenture, Account Issue, Activate And Confirm, Agreement For Agreement For, CAPTCHA, Complete with Docusign, Contract Agreement For, Documents Ready For Review #3450723, Fake Adobe, File # Review Closing Title Package, Mailbox Password Expired, ntt-docomo & matsu, pay-with-featured, Request, Salt Lake Dental, and WhatsApp.

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
- GremlinStealer
- InterLock Ransomware (NodeSnake RAT)
- KongTuke
- Latroectus
- MetaStealer
- Mispadu
- Nitrogen
- Pay2key Ransomware
- StilachiRAT
- SocGhosh

- Dark Crystal
- Direwolf Ransomware Group
- FileFix
- FormBook
- GolangGhost
- GorillaBot
- Grandoreiro
- GravityForms
- SocksShell (aka Zapcat Supper)
- SparkRAT
- SQUIDGATE (TerraLoader)
- Vanguard Stealer
- Xloader
- Xworm
- ZAPCAT
- Zloader

NEWS AND RISK INFORMATION

AMD warns of new Meltdown, Spectre-like bugs affecting CPUs. “AMD has disclosed four new side-channel vulnerabilities, collectively termed Transient Scheduler Attacks (TSA), affecting a broad range of its CPUs. Successful exploitation of the TSA vulnerabilities could lead to information disclosure.” ([The Register](#))

AsyncRAT evolves as ESET tracks its most popular malware forks. “ESET identified several prominent AsyncRAT forks actively used in cyber attacks, including DcRat, VenomRAT, and SilverRAT. DcRat offers an expanded feature set, while VenomRAT includes even more advanced capabilities.” ([Help Net Security](#))

Bitcoin Depot breach exposes data of nearly 27,000 crypto users. “The breach exposed sensitive personal information typically collected during Know-Your-Customer (KYC) verification processes,” and victims are advised to “maintain high alertness for signs of fraud, monitor their account statements, and consider placing a security freeze on their credit report.” ([Bleeping Computer](#))

Browser extensions turn nearly 1 million browsers into bots that scrape websites. “A recent investigation uncovered that 245 browser extensions—installed on nearly 1 million devices—are covertly turning users' browsers into web scraping bots. These extensions, available on Chrome, Firefox, and Edge, embed the MellowTel-jsx library.” ([ARS Technica](#))

Critical Bluetooth protocol vulnerabilities expose devices to RCE attacks. “Security researchers have uncovered a critical set of Bluetooth vulnerabilities, dubbed PerfektBlue, in OpenSynergy's BlueSDK framework. These flaws affect millions of devices, including in-vehicle infotainment systems ... The vulnerabilities can be chained together to achieve [remote code execution](#) (RCE) with minimal user interaction, requiring only device pairing to launch successful attacks.” ([GB Hackers](#))

Federal agencies have 24 hours to patch 'Citrix Bleed 2' bug. According to the [Cybersecurity and Infrastructure Security Agency \(CISA\)](#), “the insufficient input validation bug in Citrix NetScaler ADC and Gateway systems — [CVE-2025-5777](#) — poses a “significant, unacceptable risk” to the security of the federal civilian enterprise.” ([SC Media](#))

McDonald's AI hiring bot exposed millions of applicants' data to hackers who tried the password '123456.' “A critical security vulnerability in McDonald's AI-powered hiring platform, McHire.com, exposed the personal data of millions of job seekers. The breach was caused by the use of the weak password “123456” for administrative access.” ([Wired](#))

WordPress Gravity Forms developer hacked to push backdoored plugins. “A supply-chain attack has compromised the popular WordPress plugin Gravity Forms, affecting manual and composer installations of versions 2.9.11.1 and 2.9.12 downloaded between July 10 and 11, 2025.” ([Bleeping Computer](#))

THREATS OF THE WEEK

Android Trojan Anatsa highlights this week's risk.

Anatsa Trojan Targeting North America

Summary

ThreatFabric researchers discovered the [Anatsa banking trojan](#) being used against mobile banking customers in North America.

Anasta has been active since 2020 and has begun targeting financial institutions and Android mobile banking apps.

The Trojan steals financial data through overlay and keylogging, although it can also conduct fraudulent transactions remotely. To evade detection, the threat actors typically establish a user base with a legitimate application before deploying the malicious payload as an update.

In this case, they delivered the payload as a fake “PDF update” for a file reader application in the Google Play Store. The detected campaign was observed between 24 and 30 June, and the app had over 50,000 downloads.

Risk

Anasta steals banking credentials, logs keystrokes, and carries out fraudulent transactions directly from infected devices using remote-access tools.

Remediation

Institutions should review Cyber Threat Intelligence (CTI) and assess potential risks or impacts on their customers and systems. Institutions should share what they observe with other FS-ISAC members.

THREAT INTELLIGENCE UPDATE

Spotlight Report: India-Pakistan Cyber Warfare

FS-ISAC Spotlight Report shares insight on conflict.

Summary

On 22 April 2025, gunmen killed 26 Hindu tourists in Pahalgam, the India-administered region of Kashmir. As a result of the attack, tensions rose between two nuclear-powered countries. India blamed Pakistani-backed militants for the attacks and retaliated by striking Pakistani-based terrorist infrastructure through Operation Sindoor. However, the most intense battle occurred not across borders, but through cyber space, with threat actors and hacktivist groups on both sides trying to control the online narrative.

FS-ISAC’s Intelligence Spotlight Report: India-Pakistan Cyber Warfare Activity focuses on the cyber warfare activity conducted against India and Pakistan during this period, provides an assessment of the impacts on the financial sector, and elaborates on the potential for conflict escalation.

[Read the entire report.](#)

JUST FOR COMMUNITY INSTITUTIONS

Cybersecurity Awareness Month is Coming Soon

Summary

Before too long, October will be here — and that means Cybersecurity Awareness Month.

Cybersecurity Awareness Month raises awareness about online safety and rouses individuals and businesses alike with information to protect them from cybercrime. According to the National Cybersecurity Alliance, “This year’s theme, **Stay Safe Online**, is all about the simple ways to protect

yourself, your family, and your business from online threats. Small actions can make a big difference. That's why they're focusing on the **Core 4.**"

The Core 4 are four easy steps anyone can take to boost their online safety:

- Use strong passwords and a password manager
- Turn on multifactor authentication
- Recognize and report scams
- Update your software

Plan on getting involved now! For additional information, visit the National Cybersecurity Alliance [website](#).

FRAUD UPDATE

Threat Actors Targeting Commercial Customers

Summary

Using publicly available data from the [Paycheck Protection Program \(PPP\) database](#) and HELOC loans, fraudsters are targeting financial institutions' commercial clients using social engineering techniques.

State	Loan Amount	Business Name	Address	City	ZIP Code	Industry (NAICS Code)	Ra
AK	\$9,538,531.00	Kakivik Asset Management, LLC	5015 Business Park Blvd	Anchorage	99503	541990: All Other Professional, Scientific, and Technical Services	Ur
AK	\$7,666,768.00	Arctic Slope Native Association, Ltd.	7000 Uula St	Barrow	99723	813920: Professional Organizations	Ur

How They Do It

- Fraudsters query the PPP database — as they do many open source datasets to profile their intended target(s) — to get all the data they need to launch campaigns over a wide geographical area.
- Using common phishing techniques (email, VoIP, QR codes, using SIM boxes, etc.), the fraudster contacts the bank client.

Note: A SIM box (also called a SIM bank) is a device used as part of a [VoIP gateway](#) installation. It contains many [SIM cards](#), which are linked to the gateway but housed and stored separately from it. A SIM box can have SIM cards of different mobile operators installed, permitting it to operate with several [GSM gateways](#) located in other places.

- Fraudsters launch campaigns indiscriminately, hoping to hit a business that has lax security and employees with little security training.
- The attacker can implement a range of fraud tactics, including unauthorized withdrawal and account takeover.

Remediation

Institutions should alert commercial clients to advise them of this type of fraud activity and:

- Recommend training employees to spot social engineering tactics and what to do when confronted by an apparent attack.
-

-
- Intensify internal controls and approval processes, such as out-of-band confirmation and know your customer.
 - Evaluate the PPP loan portfolio against account activity and proactively research any potential threat trends.
 - Instruct commercial clients to describe their legitimate communications to their customers so they know what to expect — and what to suspect.
 - Share tools provided by FS-ISAC to bolster their loss prevention activity.
 - [Download the Cyber Fraud Prevention Framework for Financial Services.](#)
 - [Download the Phishing Prevention Framework.](#)

FS-ISAC produces a quarterly [Commercial Services Security Newsletter](#) that institution personnel can share with their customers concerning various security risks. Members must have an activated Share license to access the material.

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