

FS-ISAC | Risk Summary Report

Global Cyber Threat Level  | Americas:  EMEA:  APAC: 

Week of 30 June 2025 | Issue 289

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
- Call Center ATO
- Account Takeover
- Advance Fee
- Business Email Compromise
- CEO Impersonation
- Customer Impersonation ATO
- Fraud Withdrawals
- Property Sales
- Withdrawal Impersonation Fraud

System Vulnerabilities

Amazon, Avaya, Citrix, Debian, Dell, F5, FESTO (4), HP, Hitachi (2), IBM, Google, Lenovo, Linux, Microsoft, Mozilla, Oracle, Red Hat, SUSE, Ubuntu, and Voltronic.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: 365, Biocompatibility Quotation, Completed: Invoice Payment Notification, ConnectWise, Digital Wallet Withdrawal, Experience Personnalité, Fw: INV #00-O311, Gift Card, High Priority, libarchive, Payroll, RE: Outstanding Invoice #102497, Remote Desktop Request, Request-Gift Purchase, SBI, Terrain Solutions, Inc, and Unauthorized Transaction Alert.

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
- Direwolf Ransomware Group
- FormBook
- GolangGhost
- GremlinStealer
- InterLock Ransomware (NodeSnake RAT)
- Latrodectus
- MetaStealer
- Mispadu
- Nitrogen
- StilachiRAT
- SocGholish
- SocksShell (aka Zapcat Supper)
- SparkRAT
- SQUIDGATE (TerraLoader)
- Xloader
- Xworm

- GorillaBot
- Grandoreiro

- ZAPCAT
- Zloader

NEWS AND RISK INFORMATION

Cyber Threat Level. The Global Cyber Threat Level (CTL) has been lowered to Elevated. The CTL and Operational Resilience Risk level for the Americas remains Elevated.

Bluetooth flaws could let hackers spy through your microphone. “Three Bluetooth vulnerabilities in Airoha chipsets affect 29 audio devices from 10 vendors: Beyerdynamic, Bose, Sony, Marshall, Jabra, JBL, Jlab, EarisMax, MoerLabs, and Teufel ... The security problems could be leveraged to take over a vulnerable product and on some phones, an attacker within connection range may be able to extract call history and contacts.” ([Bleeping Computer](#))

Could your AI technology partner be a security trojan horse? “The use of AI is proliferating rapidly among financial institutions, driven by the wide availability of SaaS [software-as-a-service] and PaaS [platform-as-a-service] AI solutions, which allow banks to deploy AI quickly without requiring the time and expense of their development. But in their rush to add AI capabilities to their offerings, many providers may not be sufficiently focused on the security vulnerabilities of their solutions. Those weak points become embedded in their customers’ systems, undetected.” ([The Financial Brand](#))

DOJ raids 29 ‘laptop farms’ in operation against North Korean IT worker scheme. “The Department of Justice (DOJ) launched a major crackdown on a North Korean IT worker scheme, conducting raids on 29 'laptop farms' across 16 states. These workers accessed sensitive data, including International Traffic in Arms Regulations (ITAR) information.” ([The Record](#))

RansomHub breach: Six-day attack leveraged RDP, RMM tools and Mimikatz for data exfiltration and ransomware. “A threat actor exploited RDP misconfigurations and password spraying to deploy RansomHub ransomware. The attacker used legitimate administrative tools and Windows features to maintain stealth and efficiency throughout the operation.” ([Cybersecurity Online](#))

TikTok videos promise pirated apps, deliver Vidar and StealC infostealers instead. “A sophisticated social engineering campaign is exploiting TikTok to distribute the Vidar and StealC information-stealing malware. The campaign uses pirated software themes such as Windows OS, Microsoft Office, CapCut, and Spotify to lure users.” ([Trend Micro](#))

THREATS OF THE WEEK

The geopolitical environment and CitrixBleed 2 highlight this week’s risks.

CISA Urges Organizations to Stay Vigilant in the Current Geopolitical Environment

Summary

The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Federal Bureau of Investigation (FBI), the Department of Defense Cyber Crime Center (DC3), and the National Security Agency (NSA), recently released a [fact sheet](#) urging organizations to remain vigilant against potential cyber operations by Iranian state-sponsored or affiliated threat actors.

Despite a declared ceasefire and ongoing negotiations towards a permanent end to hostilities, Iranian-affiliated cyber actors and hacktivist groups may still conduct malicious cyber activity.

Over the past several months, hacktivists and government-affiliated actors increased their malicious cyber activity, which may escalate due to recent events. These cyber actors are often opportunistic, selecting targets that use unpatched or outdated software with known Common Vulnerabilities and Exposures (CVEs) or that use default or common passwords on internet-connected accounts and devices.

At this time, no indicators of a coordinated campaign of malicious cyber activity in the US can be attributed to Iran. CISA, FBI, DC3, and NSA strongly urge critical infrastructure asset owners and operators to implement the mitigations recommended in the joint fact sheet, which include:

- Identifying and disconnecting operational technology and industrial control systems devices from the public internet.
- Protecting devices and accounts with strong, unique passwords.
- Applying the latest software patches.
- Implementing phishing-resistant multifactor authentication (MFA) for access to OT networks.

Review the joint [Fact Sheet: Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest](#), and act now to understand the Iranian state-backed cyber threat, assess and mitigate cybersecurity weaknesses, and review and update incident response plans to strengthen your network against malicious cyber actors.

CVE-2025-5777 New Citrix Flaw – CitrixBleed 2

Summary

On 25 June, Citrix published a [security bulletin](#) warning about two critical vulnerabilities that impact NetScaler ADC and Gateway. Cybersecurity researcher Kevin Beaumont dubbed one vulnerability “[CitrixBleed2](#)” as the flaw resembles the 2023 CitrixBleed vulnerability previously exploited by threat actors. The current flaw, [CVE-2025-5777](#), can allow attackers to access session tokens, credentials, and other sensitive data while bypassing multifactor authentication.

The following supported versions of NetScaler ADC and NetScaler Gateway are affected by the vulnerabilities:

- NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56
- NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-58.32
- NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP
- NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS

Citrix has not stated whether these flaws are actively exploited but advised users to promptly install the relevant updated versions for both ADC and Gateway devices.

Remediation

Cloud Software Group strongly urges affected customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions as soon as possible.

THREAT INTELLIGENCE UPDATE

Salt Typhoon Targeting Canada

Military action leads to post-ceasefire DDoS attacks by pro-Iranian groups.

Summary

The Canadian Centre for Cyber Security and the FBI published a [bulletin](#) stating that the Chinese threat actor Salt Typhoon is targeting Canadian telecommunications providers. [Salt Typhoon](#) previously hacked US telecommunications networks. The bulletin notes that during a February 2025 incident, Salt Typhoon exploited a critical Cisco IOS XE [vulnerability](#) to retrieve configuration files of three devices and modified at least one of the files to facilitate network traffic collection. Indicator overlap suggests Salt Typhoon is also targeting other sectors, though the specific sectors are not listed in the bulletin.

FRAUD UPDATE

Brushing Scams on the Rise

Summary

The US Postal Inspection Service (USPIS) issued a warning about “brushing” scams.

According to the [USPIS website](#), in a brushing scam, a fraudster sends the victim a package containing inexpensive items — socks, a key chain, or the like — that the target didn’t order. The package is addressed to the recipient, but either has no return address or has the return address of a retailer.

The sender of the item(s) is usually an international, third-party seller who has found the recipient's address online and has written positive online reviews of the merchandise in the victim's name, giving the impression that the recipient is a verified buyer. These fake reviews fraudulently boost or inflate the products' ratings and sales numbers, which the fraudster hopes will increase actual sales in the long run. Because the merchandise costs little to manufacture or ship, the scammers perceive the scheme to be profitable. These scams are often a red flag that cybercriminals know the victim's name and address and worse, can launch a broader attempt to exploit the victim's identity or financial accounts.

Another Twist

A new variation on the brushing scam has emerged — quishing. Quishing, short for QR code phishing, uses a QR code that directs the victim to a fake website, often a bank, government organization, or other institution. These websites look legitimate and seem to be official sites, but they are used by criminals to get personally identifiable information (PII).

To employ quishing in a brushing scam, the fraudster includes a QR code in the package, indicating that by using it, the victim will discover who sent the package. Instead, the QR code sends the target to a malicious website designed to steal PII or install malware.

Remediation

If you are wary of an unsolicited package, please follow the USPIS [suspicious mail](#) instructions. The USPIS recommends checking account statements to ensure they are not unauthorized transactions. The USPIS also recommends that targets:

- Don't pay for the merchandise
- Return to sender
- Throw it away
- Change their account passwords
- Closely monitor credit reports
- Notify the retailer

If the merchandise is organic (i.e., seeds, food, plants) or an unknown liquid or substance, notify the proper authorities and follow their instructions.

Victims do not have to return the contents of the package. By law, people may keep unsolicited merchandise and are under no obligation to pay for it.

GOVERNMENT AND REGULATORY NEWS

Agencies Issue Exemption Order to Customer Identification Program Requirements

Summary

The Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the National Credit Union Administration, with the concurrence of the Financial Crimes Enforcement Network, granted an exemption from a requirement of the Customer Identification Program (CIP) Rule implementing Section 326 of the USA PATRIOT Act. The order applies to accounts at all entities supervised by those agencies. The CIP Rule requires a bank or credit union to obtain taxpayer

identification number (TIN) information from its customer before opening an account, and the exemption permits a bank or credit union to use an alternative collection method to obtain TIN information from a third party rather than from the customer.

Since the CIP Rule was issued in 2003, the ways consumers access financial services have evolved significantly, as have reports of customer reluctance to provide their full TIN. That hesitation is due, in part, to concerns about data breaches and identity theft. Accordingly, this exemption provides flexibility to those entities supervised by the agencies that must comply with the CIP Rule. The exemption does not change the underlying requirement for banks and credit unions to have risk-based CIP procedures that enable them to form a reasonable belief that they know the true identity of each customer.

This exemption is optional, and entities are not required to use an alternative collection method to obtain a customer's TIN information.

[Read the entire press release.](#)

[Read the Exemption Order \(PDF\).](#)

Aldersgate Federal Credit Union Closes

Summary

The National Credit Union Administration (NCUA) today liquidated Aldersgate Federal Credit Union of Marion, Illinois. Member deposits are federally insured by the National Credit Union Share Insurance Fund up to \$250,000.

The decision to liquidate Aldersgate Federal Credit Union and discontinue operations was made after determining the credit union was insolvent and had no prospect for restoring viable operations. The credit union violated numerous provisions of the Federal Credit Union Act and NCUA Rules and Regulations, including operating in an unsafe and unsound manner.

[Read the entire press release.](#)

Butler Heritage Federal Credit Union Closes: Cincinnati Ohio Police Federal Credit Union Assumes Members and Shares

Summary

The NCUA facilitated a partial purchase and assumption between Butler Heritage Federal Credit Union (FCU) in Middletown, Ohio, and the Cincinnati Ohio Police Federal Credit Union (COPFCU). Butler Heritage FCU members should contact COPFCU. COPFCU members, including those members previously with Butler Heritage Federal Credit Union, will experience no interruption in services, and their accounts remain federally insured by the National Credit Union Share Insurance Fund.

COPFCU immediately purchased some assets and assumed Butler Heritage FCU's share accounts. Butler Heritage FCU was subsequently liquidated. COPFCU is a federally insured credit union with more than 10,000 members and assets of \$173 million, according to the credit union's most recent Call Report.

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
- 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](#).