

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

Week of 11 August 2025 | Issue 295

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

- Account Takeover
- Business Email Compromise
- Fraud Investment
- Fraudulent Withdrawal
- Transfers via Business Banking Spoofing & Impersonation

System Vulnerabilities

Adobe, Amazon, Apache, Apple, Ashlar-Vellum Cobalt, AVEVA, Azure, CA-OPS, Cisco, Debian, Dell, DHL, End-of-Train, F5, Fortinet, Google, HP, HPE, IBM, Intel, Juniper, Lenovo, Linux, Magneto, MegaSys, Microsoft, N-able, NVIDIA, Oracle, Palo Alto, Red Hat, Samsung, Santesoft, SAP, Schneider Electric, Siemens, SUSE, Trend Micro, Ubuntu, WinRAR, and Xerox.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: AAA Emergency Free Kit, ACH Receipt Notification, Approved RFP, Confidential Document, Employee-eFile, Greg Lee shared Gree_Contract_2 with you, Güralp Systems, Letter of Intent, O365, Payment Policy, Payroll Diversion, QuickBooks, Request for 2024 Employee W-2 Forms, SSA, StratFin, Unauthorized Transaction, and Zoom.

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
- Dark Crystal
- Direwolf Ransomware Group
- Duck Tail Malware
- Etelaat Infostealer
- FileFix
- InterLock Ransomware (NodeSnake RAT)
- Katz Stealer
- KongTuke
- Latrodectus
- Longwait Malware
- MetaStealer
- Mispadu
- Nitrogen
- Oyster[Loader] (Broomstick)
- Pay2key Ransomware
- Phantom Stealer
- Rhysida Ransomware
- SectopRAT
- StilachiRAT
- SocGholish

FormBook
GolangGhost (ICEBITE.WIN)
GorillaBot
Grandoreiro
GravityForms
GremlinStealer

- SocksShell (aka Zapcat Supper)
- SparkRAT
- SQUIDGATE (TerraLoader)
- Vanguard Stealer
- Xloader
- Xworm
- Zloader

NEWS AND RISK INFORMATION

After researchers unmasked a prolific SMS scammer, a new operation has emerged in its wake. “A new large-scale SMS phishing operation, dubbed Magic Mouse, has emerged following the takedown of the earlier scam campaign known as Magic Cat. Magic Mouse is now responsible for the theft of approximately 650,000 credit cards per month.” ([Tech Crunch](#))

From fake CAPTCHAs to RATs: Inside 2025’s cyber deception threat trends. “Between late 2024 and early 2025, the percentage of customers affected by security incidents nearly tripled, rising from 6% to 17%. Over half of these incidents began at the initial access stage [where the threat actor attempted or gained access to a host but not the tools to download or configure persistence].” ([HelpNet Security](#))

Juniper Networks security advisory (AV25-491). “On August 8, 2025, Juniper Networks issued Security Advisory AV25-491 to address multiple vulnerabilities in Juniper Secure Analytics (JSA). These vulnerabilities affect versions 7.5.0 up to but not including 7.5.0 UP12 IF03.” ([Cyber](#))

MedusaLocker ransomware group is looking for pentesters. “The MedusaLocker ransomware group, active since 2019 and operating under a Ransomware-as-a-Service (RaaS) model, has announced a recruitment drive for penetration testers via its Tor-based data leak site.” ([Security Affairs](#))

Royal and BlackSuit ransomware gangs hit over 450 US companies. “Homeland Security Investigations (HSI), DHS’s main investigative arm, which took down the group’s infrastructure in cooperation with international law enforcement partners, added that the cybercriminals also collected over \$370 million from their victims.” ([Bleeping Computer](#))

SAP patches three critical 9.9 S/4 HANA bugs. “SAP released 19 security notes — four of which were [previously released](#) — and three were patches to critical 9.9 bugs found on its [SAP S/4 HANA](#) ERP system. S/4 HANA is SAP’s flagship [ERP platform](#), widely deployed across Fortune 500 companies and critical industries, including manufacturing, finance, healthcare, and defense.” ([SC World](#))

ShinyHunters targeting Salesforce accounts. Google [disclosed](#) that one of its Salesforce instances was impacted in June by UNC6040 (aka ShinyHunters). Google reported that the data stolen was largely publicly available business information. Several [organizations](#), such as Qantas, LVMH, and Adidas, have disclosed they had data breaches through “a vendor platform used for managing customer data.” Bleeping Computer reported that ShinyHunters attempted to privately extort companies over email, threatening to leak stolen information unless a ransom was paid in bitcoin. ([Google](#))

Xerox FreeFlow Flaws Enable SSRF and Remote Code Execution. “Xerox has released critical patches for FreeFlow Core version 8.0.4 to address two high-severity vulnerabilities — CVE-2025-8355 and CVE-2025-8356 — that enable Server-Side Request Forgery (SSRF) and Remote Code Execution (RCE).” ([GB Hackers](#))

THREAT OF THE WEEK

North Korean threat group phishing with malicious LNK files highlights this week’s risk.

ScarCruft drops VCD Ransomware

Summary

The North Korean APT group ScarCruft is behind an advanced malware phishing campaign that camouflages itself as a postal code update notice. The group is noted for cross-language malware development and victim-specific ransomware. The campaign leverages PubNub, a real-time communication platform with instant data streaming and messaging functionality utilizing a global DSN

with at least 14 data centers for low latency and scalability, which complicates detection and mitigation. In an 11 August [Cyware](#) report, “Likely entry point is phishing emails with malicious LNK files in RAR archives. Nine distinct malware components were deployed, including NubSpy (Autolt/PowerShell backdoor), TxPyLoader (Python-based loader), LightPeek (PowerShell infostealer), FadeStealer (keylogger/audio recorder), and CHILLYCHINO (Rust-based backdoor). VCD ransomware encrypts files using RSA and AES-256-CBC, drops bilingual ransom notes, self-deletes after execution, and renames files with the .VCD extension.”

THREAT INTELLIGENCE UPDATE

UPDATE: Microsoft Releases Guidance on High-Severity Vulnerability (CVE-2025-53786) in Hybrid Exchange Deployments

CISA is “deeply concerned” about a Microsoft Exchange vulnerability.

Summary

12 August Update: The Cybersecurity and Infrastructure Security Agency (CISA) has updated this alert to provide clarification on identifying Exchange Servers on an organization’s networks and provided further guidance on running the Microsoft Exchange Health Checker.

7 August Update: CISA issued [Emergency Directive \(ED\) 25-02: Mitigate Microsoft Exchange Vulnerability](#) in response to [CVE-2025-53786](#).

CISA is aware of the newly disclosed high-severity vulnerability, [CVE-2025-53786](#), that allows a cyber threat actor with administrative access to an on-premise Microsoft Exchange server to escalate privileges by exploiting vulnerable hybrid-joined configurations. This vulnerability, if not addressed, could impact the identity integrity of an organization’s Exchange Online service.

While Microsoft has stated there is no observed exploitation as of the time of this alert’s publication, CISA strongly urges organizations to implement Microsoft’s [Exchange Server Hybrid Deployment Elevation of Privilege Vulnerability](#) guidance outlined below, or risk leaving the organization vulnerable to a hybrid cloud and on-premises total domain compromise.

1. Organizations should first inventory all Exchange Servers on their networks (organizations should leverage existing visibility tools or publicly available tools, such as NMAP or PowerShell scripts, to accomplish this task).
2. If using Exchange hybrid, review Microsoft’s guidance [Exchange Server Security Changes for Hybrid Deployments](#) to determine if your Microsoft hybrid deployments are potentially affected and available for a Cumulative Update (CU).
3. Install Microsoft’s [April 2025 Exchange Server Hotfix Updates](#) on the on-premise Exchange server and follow Microsoft’s configuration instructions [Deploy dedicated Exchange hybrid app](#).
4. For organizations using Exchange hybrid (or have previously configured Exchange hybrid but no longer use it), review Microsoft’s [Service Principal Clean-Up Mode](#) for guidance on resetting the service principal’s keyCredentials.
5. Upon completion, run the [Microsoft Exchange Health Checker](#) with appropriate permissions to identify the CU level of each Exchange Server identified and to determine if further steps are required.

Remediation

CISA highly recommends institutions disconnect public-facing versions of Exchange Server or SharePoint Server that have reached their end-of-life (EOL) or end-of-service from the internet. For example, SharePoint Server 2013 and earlier versions are EOL and should be discontinued if still in use.

Institutions should review Microsoft's blog [Dedicated Hybrid App: temporary enforcements, new HCW, and possible hybrid functionality disruptions](#) for additional guidance as it becomes available.

FRAUD UPDATE

Misuse of Credentialing Tools in Financial Fraud Schemes

Summary

Cyber criminals are using increasingly sophisticated tactics to pose as legitimate financial investment advisers in pig-butcherer scams – i.e., a faux relationship designed to entice victims into a fake investment opportunity. By exploiting publicly available credentialing tools intended to verify advisers' professional registration, cyber criminals are creating convincing but fake websites to support their personas and deceive investors into transferring funds — including cryptocurrency — to fraudulent accounts.

Background

Since at least 2023, malicious actors have exploited these services and other open-source information — such as advisers' LinkedIn profiles — to create convincing websites. Fraudulent personas and websites lure victims into believing they are investing with a reputable financial institution until the perpetrator disappears with the funds.

In this type of scam, fraudulent websites often share common characteristics, including:

- A domain name incorporating the impersonated adviser's full name (first, middle, and last name)
- URL characters in languages not associated with the advisor or Unicode to mimic regular ASCII characters
- A CRD number or a copied BrokerCheck report
- An atypical or single-product investment option
- A use of a personal, rather than firm-affiliated, email address

Remediation

To counter the growing threat, OCCIP recommends implementing the following measures as a part of routine cyber hygiene and customer communication. These measures aim to protect institutions and individuals alike, while supporting enforcement and takedown actions against fraudulent operations.

Verify credentials: Use Investor.gov's "Check Out Your Investment Professional" tool to confirm the contact information for the investment firm, adviser, or broker.

Avoid unsolicited communications: Distrust "advisers" who reach out via text message or social media platforms and suggest moving future communications to Voice-over-Internet-Protocol (VoIP) applications.

Monitor for copycat websites: Deploy automated tools that identify look-alike domains and detect mimicked branding assets.

Pursue website takedowns: Contact the fraudulent website's hosting provider to file a website takedown request.

Reporting Incidents

To report a suspected cybersecurity intrusion and request technical assistance, you can contact:

- CISA at central@cisa.dhs.gov or call 888-282-0870
- The Federal Bureau of Investigation (FBI), through a local field office, the FBI's Cyber Division at CyWatch@fbi.gov, or call 855-292-3937
- Any US Secret Service local field office

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- [Cross-Sector Mitigations: Scattered Spider | Guidance for Proactive Defense](#)
- [The Business Information Security Officer](#)
- [Quarterly Threat Trends Report - Q2 2025](#)
- [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](#)

[See the full list of Knowledge Resources](#)

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- [FinCyber Today Podcast Season 2](#)
- [FinCyber Today Podcast Season 1](#)

UPCOMING EVENTS

Americas

Members can enroll in the Member Services app to attend events.

- 18 August | Monthly CIAC Webinar
- 27 August | CIAC and COFFE Open Forum
- 27 August | Member Success Webinar
- 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](#).