

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

Week of 7 July 2025 | Issue 290

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
- Fake Invoice (Wire Fraud)
- IT/Tech Support
- Treasury Management Vishing
- Withdrawal Impersonation Fraud

System Vulnerabilities

Adobe, Amazon, Azure, Cisco, Cygwin, Debian, Dell, Emerson, F5, Fortinet, GNU C, Google, HP, Hitachi, IBM, Lenovo, Linux, Microsoft, Mitsubishi, Mozilla, Multi-Router Looking Glass, Nessus, Palo Alto Networks, PAN-OS, PHPMailer, Oracle, Red Hat, Redis, Ruby on Rails, Samsung, SAP, ServiceNow, Splunk, SUSE, Symantec, Synacor Zimbra, TeleMessage, Tenable, and Ubuntu.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: 3rd Quarter, Amy Smith has invited you to view a file, Bid Invitation, Car Payment, DD AUTH FORM, Desk Notification Service, Encrypted PDF, Gift Card, Google Ads, New encrypted PDF message, New Submission From Tom's Truck Center, Prize Claim, and RecipeLister.exe, Project Review, Renewal/Monthly Statement, SIGNUP FOR EARLY ACCESS.

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

- GolangGhost
- GorillaBot
- Grandoreiro
- Xworm
- ZAPCAT
- Zloader

NEWS AND RISK INFORMATION

Android TapTrap attack fools users with invisible UI trick. “A newly discovered Android attack technique, dubbed TapTrap, enables stealthy tapjacking by exploiting UI animation transitions. Unlike traditional overlay-based methods, TapTrap works even with zero-permission apps.” ([Bleeping Computer](#))

Critical Sudo bugs expose major Linux distros to local root exploits. “Researchers disclosed two vulnerabilities (CVE-2025-32462 and CVE-2025-32463) in the Sudo command-line utility for Linux and Unix-like operating systems. Local attackers can exploit them to escalate privileges to root on affected systems.” ([Security Affairs](#))

Ingram Micro confirms ransomware behind multi-day outage. “Ingram Micro, one of the world's largest distributors, has confirmed it is trying to restore systems following a ransomware attack ... The Safepay ransomware claimed to have accessed sensitive information, including financial statements, intellectual property, accounting records, lawsuits and complaints, personal and customer files, bank details, transactions, etc.” ([The Register](#))

New technique detects tampering or forgery of a PDF document. “Researchers from the University of Pretoria presented a new [technique](#) for detecting tampering in [PDF documents](#) by analyzing the file's page objects. The technique employs a prototype that can detect changes to a PDF document, such as changes made to the text, images, or metadata ... With the PDF format being used as a formal means of communication in multiple industries, it has become a good target for criminals who wish to affect contracts or aid in misinformation.” ([Help Net Security](#))

Researchers defeat content security policy protections via HTML injection. “Security researchers have demonstrated a method to bypass nonce-based Content Security Policy (CSP) protections using HTML injection, CSS-based nonce leakage, and browser cache manipulation.” ([gbhackers](#))

Researchers warn of exposed JDWP interfaces targeted for cryptomining attacks. “Since JDWP [Java Debug Wire Protocol] lacks authentication or access control mechanisms, exposing the service to the internet can open up a new attack vector that attackers can abuse as an entry point, enabling full control over the running Java process.” ([The Hacker News](#))

RondoDox Unveiled: Breaking down a new botnet threat. “RondoDox is a new botnet threat that exploits two critical vulnerabilities: CVE-2024-3721 (TBK DVR models) and CVE-2024-12856 (Four-Faith router models). These vulnerabilities allow remote attackers to execute arbitrary commands.” ([Fortinet](#))

THREATS OF THE WEEK

Shellter infostealer highlights this week's risk.

Helter “Shellter” Being Used as Infostealer by Adversaries

Summary

Shellter, once a legitimate security tool, is now being used by adversaries as an infostealer.

[Dark Reading](#) reports, “Shellter enables [red team operators](#) to more effectively deploy their command-and-control (C2) frameworks against contemporary anti-malware solutions. However, the same features that provide them with this capability can also allow attackers to evade detection, which is an unfortunate byproduct of such solutions.”

Specifically, the Shellter framework includes payload encryption using AES-128 CBC mode and compression via the [LZNT1](#) algorithm, and features a component designed to evade detection.

To help defenders, Elastic Security Labs reports that it is “releasing [a dynamic unpacker](#) for binaries protected by Shellter that uses a combination of dynamic and static analysis techniques to automatically extract multiple payload stages. Though the unpacker is not fully comprehensive, it does successfully process a large majority of tested samples.”

THREAT INTELLIGENCE UPDATE

NordDragonScan infostealer targets Windows with LOTL methods

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

Summary

[Fortinet reports](#) the discovery of a newly disclosed infostealer dubbed 'NordDragonScan' that executes stealthily on Windows machines using living-off-the-land (LOTL) techniques. The attack kicks off when users visit a site called secfileshare[.]com, which downloads a RAR archive designed to look like a Ukrainian government document.

A LNK shortcut within the archive invokes the Windows utility mshta.exe to retrieve and execute an HTML Application (HTA) script from the secfileshare[.]com domain, called 1.hta., that copies the legitimate PowerShell.exe binary to the Documents folder and renames to install.exe to hide its activity. It then downloads a benign decoy document, tricking the victim into believing this is the file they installed, while the malicious payload runs in the background.

The final NordDragonScan payload, named adblocker.exe to further hide its nature, communicates with a C2 server called kpuszkiev[.]com. It establishes persistence by creating a Windows registry key that ensures the malware will always run when the victim logs in to their machine.

Target and Impact

Data theft activities include collecting basic system and user information, taking screenshots, retrieving data from Chrome and Firefox browsers, and copying certain files from the Desktop, Documents, and Downloads folders.

The malware targets Microsoft Word documents and text files, PDFs, spreadsheets, and configuration files for OpenVPN and the Remote Desktop Protocol.

NordDragonScan scans for active network interfaces, extracts the IP address and subnet mask, calculates the CIDR range for the subnet, and probes each address to identify active connections. This allows it to create an inventory of potential targets for lateral movement across the local area network (LAN).

JUST FOR COMMUNITY INSTITUTIONS

How Bad Is Brand Impersonation?

Summary

A [Menlo Security Report](#) finds that nearly 51% of browser-based phishing attempts involve brand impersonation, in which cybercriminals build fake websites that closely resemble legitimate ones to scam victims into offering sensitive information and money. The report “identifies several key drivers behind the sharp rise in browser-based attacks, including AI-powered attacks, phishing-as-a-service (PhaaS), and zero-day vulnerabilities. The research reveals that a surge in generative AI-based threats has spurred a 140% increase in browser-based phishing attacks compared to 2023, and a 130% increase specifically in zero-hour phishing attacks.”

The News Isn't Great

According to [Security Magazine](#), the key findings from Menlo Security's State of Browser Security Report are:

- Cybercriminals create nearly 1 million new phishing sites each month, a 700% increase since 2020.
- Nearly 51% of browser-based phishing attempts involved some form of [brand impersonation](#).
- 75% of phishing links are hosted on good, trusted websites, with up to six days as the average window of exposure before legacy security tools begin blocking pages from zero-hour phishing attacks.
- Phishing attacks hosted on subdomain providers increased by 51%, representing 24% of all phishing attacks.
- Four of the top five hosting providers used by bad actors to host phishing attacks were based in the US, potentially reflecting the country's economic and political significance, high rate of digital transformation, remote work, and the growing reliance on US-based cloud services and SaaS platforms housing critical data and financial information.
- Instances of attackers exploiting cloud services to host malicious content, including phishing sites and ransomware, are on the rise. AWS and CloudFlare accounted for nearly 50% of all instances of abused cloud hosting in 2024.

Risk

Brand impersonation can negatively impact financial institutions, from customer confusion, loss of goodwill, legal ramifications, operational downtime, to name just a few in a long list.

Remediation

Protecting your institutions can be a complicated process, especially for small institutions with personnel handling roles. Some things you can do include:

- Select the right provider
- Ensure you have strong cybersecurity protocols (e.g., Use of DMARC, SPF, and DKIM email authentication, and SSL encryption for websites)
- Monitor for brand impersonation by detecting counterfeit websites.
- Prevent domain squatting, look for variations of your institution's web address.
- Provide education to your customers/members and provide resources for them to alert you.
- Quickly respond to incidents that include taking legal action. (e.g., cease-and-desist notification, domain takedown, etc.)
- Determine if the problem is widespread and if consumer transparency is warranted.
- Monitor social media activity involving your institution.
- Work closely with your public relations team.

Smaller institutions may require the assistance of a third-party provider to handle the day-to-day monitoring.

GOVERNMENT AND REGULATORY NEWS

Bank Secrecy Act/Anti-Money Laundering: Customer Identification Program, Tax Identification Number, Alternative Collection Method

Summary

An alert issued by the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA) and the Financial Crimes Enforcement Network (FinCEN) notified all institutions subject to the agencies' jurisdiction that they are exempt from the requirements of the [Customer Identification Program \(CIP\) Rule](#) for the collection of taxpayer identification numbers (TIN) from customers in the circumstances specified in the alert.

Read the [FDIC statement](#).

Read the [OCC statement](#).

FFIEC Publishes 2024 Data on Mortgage Lending

Summary

The Federal Financial Institutions Examination Council (FFIEC) recently published data on 2024 mortgage lending transactions reported under the Home Mortgage Disclosure Act (HMDA) by 4,908 US financial institutions in the [Snapshot National Loan-Level Dataset](#). The dataset contains the national HMDA datasets as of 19 May 2025.

The FFIEC released [several data products](#) to serve a variety of data users, including the 2024 Snapshot National Loan-Level Dataset, the HMDA Dynamic National Loan-Level Dataset, and Aggregate and Disclosure Reports. The One-Year National Loan Level Dataset for 2023 and the Three-Year National Loan Level Dataset for 2021 were released as well. Users can use the [Data Browser Dataset Filtering tool](#) to download customized reports based on the updated data.

NCUA Monitoring and Assisting Credit Unions Affected by Flooding in Texas

Summary

As the state of Texas recovers from damage caused by severe storms, straight-line winds, and flooding, the National Credit Union Administration is monitoring the situation closely and has resources available to help affected credit unions.

NCUA examiners have been working to stay in contact with credit unions in the areas affected, determine their status, and offer assistance as needed. Credit unions needing assistance should contact their regional offices.

[Read the entire press release.](#)

Request for Information on Potential Actions to Address Payment Fraud

Summary

The OCC, the Federal Reserve System's Board of Governors, and the FDIC seek public input on questions related to payment fraud.

This request for information offers the opportunity for interested stakeholders to identify ways that the OCC, the Federal Reserve System, and the FDIC could take actions collectively or independently to help consumers, businesses, and financial institutions mitigate check, automated clearing house (ACH), wire, and instant payments fraud.

Community banks regulated by the OCC can submit comments by visiting <https://www.regulations.gov>. Enter "Docket ID OCC-2025-0009" in the search box and click "Search." Public comments can be submitted via the "Comment" box below the displayed document information or by clicking on the document title and then clicking the "Comment" box on the top-left side of the screen.

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](#).