FS-ISAC

Community Institution & Associations Risk Summary Report

Week of 6 November | 2023 Edition | Vol. 203

Follow Us

TLP GREEN | Americas Cyber Threat Level: Guarded | DHS Terrorism Threat Level: Elevated

In This Issue

Threats of the Week

News and Risk Information

Summary

Below are some top news and risks the Financial Services Information Sharing Analysis Center (FS-ISAC) has observed this week for community institutions (CIs).

Microsoft overhauls cyber strategy to finally embrace security by default. The Secure Future Initiative includes implementing secure default settings out of the box and using automation, AI, and memory-safe languages to develop software that is secure by design and default. (Cybersecurity Dive)

Russian reshipping service 'SWAT USA Drop' exposed. The Russia-based criminal reshipping service SWAT USA Drop was hacked, exposing its operations and revealing the involvement of over 1,200 people in reshipping stolen goods purchased with stolen credit cards. (Krebs on Security)

Small businesses must be on guard for cyberattacks. Small businesses may already be on alert for cybersecurity attacks, which affect 1 in 4 small businesses according to a new Shred-it report, but many are unaware of the costs that come along with data breaches. Across all businesses in the US, data breaches cost over $9.4 million. (Help Net Security)

Tougher NY regulations put cybersecurity onus on CISOs. New York is updating its cybersecurity regulations and making them stiffer than those recently released by the federal government, with a focus on ransom payments and board oversight. Chief information security officers are responsible for compliance and enforcing internal policies under the new rules. (Wall Street Journal)

Cisco patches 27 vulnerabilities in network security products. The most severe vulnerability, CVE-2023-20048, is a command injection bug in the Firepower Management Center (FMC) that could allow authenticated attackers to execute configuration commands on targeted devices. (Security Week)

New DarkGate variant uses a new loading approach. DarkGate is a versatile malware that includes features such as keylogging, information stealing, and downloading and executing other payloads. The DarkGate malware has been involved in multiple campaigns and continues to evolve. (Netskope)

Kinsing actors exploiting recent Linux flaw to breach cloud environments. Attackers are also extracting credentials from cloud service providers, marking the first documented instance of Looney Tunables exploitation. The group has a history of quickly adapting its tactics to exploit newly disclosed vulnerabilities. (Hacker News)

Nearly 5K employees affected in latest Okta breach. Okta was hit with another data breach and the sensitive information of thousands of employees was exposed through a third-party vendor. The incident follows a cyberattack on Okta's support management system. An unknown threat actor had accessed files after an employee signed in to a personal Google profile on the Chrome browser of an Okta-managed laptop (IT Pro)

Socks5Systemz proxy botnet infects 10,000 systems worldwide. The botnet uses a domain generation algorithm (DGA) to connect with its command-and-control server and can be instructed to establish backconnect server connections, allowing infected devices to be used as proxy servers. (Bleeping Computer)

Unmasking new AsyncRAT infection chain. AsyncRAT is being distributed through a malicious HTML file and uses various file types like PowerShell, WSF, and VBScript to bypass detection. The infection chain begins with a spam email containing a malicious URL to download the HTML file. (McAfee)

This Week's Top Risks

Security is Everyone's Responsibility

Threats, Malware, Cybercampaigns, and Adversaries

- Agent Tesla
- AsyncRAT
- Business email compromise and impersonation use of texts; credential pharming, harvesting, and validation scams.
- CageyChameleon (New)
- DarkGate Malware
- Diceloader
- DogeRAT
- Easy Stealer
- EvilProxy
- Formbook
- GRANDOREIRO
- IceID
- Lumma Stealer
- njRAT
- Parallax RAT
- PikaBot
- .RAR Malspam
- Rogue Raticate
- Scattered Spider
- SOCGHOLISH
- SorillusRAT
- XLoader

Hardware & System Vulnerabilities (multiple)

- Amazon, Android, Brocade, CA OPS/MVS, Cisco, Citrix, Debian, Dell, F5, Google, Hitachi, Huawei, IBM, Juniper, Lenovo, Linux, Microsoft, Nessus, Oracle, Proofpoint, Red Hat, Samsung, SUSE, Ubuntu, VMware, and z/OS.

Themed Phishing Campaigns

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

Subject Keywords: 404 TDS URLS, Compromised Websites, Apply for KYC Verification !, AVAILABLE ?, Computer Refresh, Document(s): Salary Amendment, FIS, IMPORT & EXPORT PERMIT, Microsoft 365, Order Your New Computer, returning message to sender, and TODAY.

Threats of the Week

Confluence, Turla hacking group, and deposit delays highlight this week's risks

New Critical Confluence Vulnerability

Summary

Atlassian has issued an alert to administrators, indicating that a critical Confluence security vulnerability, designated as CVE-2023-22518, now has a publicly available exploit. This exploit can be employed in data destruction attacks, specifically targeting Confluence instances that are both exposed to the internet and remain unpatched. This vulnerability, rated at 9.1 out of 10 in terms of severity, is identified as an improper authorization vulnerability. It impacts all versions of Confluence Data Center and Confluence Server software. In an update to the initial advisory, Atlassian emphasized the discovery of a publicly accessible exploit, significantly elevating the risk level for publicly available instances. "There are still no reports of an active exploit, though customers must take immediate action to protect their instances. If you already applied the patch, no further action is required." the company said.

Risk and Remediation

- Although malicious actors can utilize this vulnerability to erase data on affected servers, it should be noted that it cannot be leveraged to exfiltrate data from vulnerable instances. Additionally, Atlassian has confirmed that Atlassian Cloud sites accessed via the atlassian.net domain remain unaffected.
- Institutions should update their software. In cases where immediate upgrading is not possible, they should implement mitigation measures, such as creating backups for unpatched instances and restricting internet access to servers that have not yet received the necessary updates until the updates can be applied.

New Version of Kazuar Backdoor Discovered

Summary

Cyware reports that the Russian-linked Turla hacking group has been observed using a new version of Kazuar backdoor to expand its attacks. The new findings come from Palo Alto Networks Unit 42, which has been tracking the adversary under the name Pensive Ursa.

According to researchers, the malware has been spotted in the wild after years of hiatus and shows significant improvement in its code structure and functionality. The new version of the Kazuar backdoor supports over 40 distinct commands, half of which are previously undocumented. These commands can enable attackers to steal sensitive data from various browsers, take screenshots from victims' systems, get system information, manipulate files, and execute VBScript and PowerShell scripts. Other notable features include robust code and string obfuscation techniques, a multithread model for enhanced performance, and a range of encryption schemes used during the transmission of pilfered data to C2 servers. It is, further, noted that the malware leverages a function called 'named pipes' to establish peer-to-peer communication between Kazuar instances.

Kazuar malware first appeared in 2017 and made its comeback in July as Ukraine-CERT shared details of a phishing campaign that used the backdoor along with the Capibar malware to target the Ukrainian military. In the campaign, Kazuar performed credential theft while Capibar was used for intelligence gathering.

Risk and Remediation

The upgraded version of Kazuar reveals that Turla APT is making consistent efforts to operate in stealth mode and thwart analysis. As the threat actor group expands its arsenal to launch high-profile attacks, with some of them recently launched against international government agencies, organizations must exercise caution in detecting and blocking threats targeting their critical assets and infrastructures.

Ransomware Self-Assessment Tool

Financial institutions can now access the webinar rolling out the updated version of the Ransomware Self-Assessment Tool (R-SAT). The document provides executive management and the board of directors with an overview of the institution's preparedness towards identifying, protecting, detecting, responding, and recovering from a ransomware attack. It may also assist other third parties (such as auditors, security consultants, and regulators) that might review your institution's security practices.

- Ransomware Self-Assessment Tool, Version 2.0
- Report: Ransomware Lessons Learned by Banks That Suffered an Attack
- Webinar Recording – 24 October 2023
- Webinar Slides [PDF]

Additional Resources:

- Non-bank Ransomware Self-Assessment Tool
- Cybersecurity 101 for Bank Executives

US Banks Hit By Deposit Delays

Summary

On Friday, several US banks encountered deposit delays due to an error at a payment processing network, as reported by the Federal Reserve. The Federal Reserve informed banks on Friday afternoon that the issue stemmed from a "processing problem" at the private-sector entity responsible for operating the Automated Clearing House (ACH), a nationwide network for transaction processing. The Fed said an "error" in a batch of payments delayed the processing of payments. The Clearing House, which serves as the private-sector operator for ACH, confirmed to CNN that it had indeed experienced a processing problem with a batch of bank transactions.

'Tis The Season

Charity Scams steal money and trust

Summary

For many, the holiday season is a time for cheerful giving. But charity scammers ruin the mood by trying to cash in on your goodwill. If you're supporting a charitable cause this winter, make a donation plan that includes spotting and avoiding scams.

Charitable giving goes up near the end of the year and scammers know it. Your year-end giving has the best chance of reaching the organizations you want to reach — and not scammers — when you:

- Check out a charity before you give. Most organizations use heart-warming messages to inspire you to give. But scammers might do that too. So before you donate to a charity, check them out on Better Business Bureau's (BBB) Wise Giving Alliance, Charity Navigator, Charity Watch, or Candid. If you find anything that worries you about the organization, find another way to give to the cause.
- Ask how much of your donation will go to the charity. If you donate through an online platform, the platform or another organization may keep part of the money as a fee before sending the rest to your chosen charity. That information should be clear and easy to find on the platform's website. If it's not, consider donating directly to the charity instead.
- Don't rush. Scammers pressure you to give right away. They don't want you to have time to research their claims or think them through. Honest charities always need your donations — but they won't rush you into donating immediately.
- Pay by credit card. It's your safest bet. Scammers often ask you to wire money through companies like Western Union and MoneyGram or buy gift cards. Or they might insist that you pay by cryptocurrency. If someone says it's the only way for you to donate, you know it's a scam.

Cybersecurity Leaders Should Have A Seat At Table For M&A

When organizations merge with or acquire businesses, there is a case to be made for cybersecurity leaders to be involved in the process to help integrate solutions and inherited risks. Robert Huber, chief security officer at Tenable, looks at the acquisition process he oversaw when Tenable recently acquired Ermetic, including due diligence, evaluation, and integration. (Information Week)

Members who want to discuss and understand best practices for mergers and acquisitions are welcome to join the M&A Working Group ("MAWG") for ongoing discussions regarding current challenges and solutions. All MAWG members can receive a copy of the cybersecurity white paper written by the group. Members can contact admin@fsisac.com to join or request further information.

Upcoming FS-ISAC Events

Learn. Connect. Collaborate. FS-ISAC offers a variety of opportunities for members to share knowledge, upskill teams, and build the trust critical to our community's continued success in protecting the global financial system, both online and in-person around the globe at fsisac.com/events.

CIAC Meeting
13 November 2023
3:30 PM ET

Interactive Incident Response Workshop
21 November
12:00 PM - 2:00 PM EST
Register

CIAC Meeting
11 December 2023
3:30 PM ET

Full-Stack Cyber Competency Americas
13 December 2023
9 AM - 4 PM EST
Register

2024 Summit
3 - 6 March
San Diego, CA
Submit a Proposal

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is the only global cyber intelligence sharing community solely focused on financial services. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate, and respond to cyber threats. Headquartered in the US, the organization has offices in the UK and Singapore. Member financial institutions represent over $35 trillion in assets under management, with 15,000 users in more than 70 countries. To learn more, visit fsisac.com.