FS-ISAC

Community Institution & Associations Risk Summary Report

Week of 11 December | 2023 Edition | Vol. 208

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).

Fake LinkedIn profiles target Saudi workers for information leakage and financial fraud. Researchers have discovered nearly a thousand fake profiles created with the intention of reaching out to companies in the Middle East. These profiles, often difficult to distinguish from real ones, have been successful in their campaigns. (Dark Reading)

Security automation gains traction, prompting a "shift everywhere" philosophy. According to Synopsys, the use of automated security technology is on the rise, as organizations increasingly embrace the "shift everywhere" philosophy to improve the effectiveness and reduce the cost of security activities.. (Help Net Security)

US healthcare giant Norton says hackers stole millions of patients' data during ransomware attack. Norton Healthcare, which runs eight hospitals and more than 30 clinics in Kentucky and Indiana, has admitted crooks may have stolen 2.5 million people's most sensitive data during a ransomware attack in May 2023. During the intrusion, the criminals accessed names, contact information, Social Security Numbers, and dates of birth, and also may have accessed driver's license and government ID numbers, financial account information, and digital signatures. (The Register)

Apache fixed critical RCE Flaw CVE-2023-50164 in Struts 2. The Apache Software Foundation has released security updates to address a critical file upload vulnerability in the Struts 2 framework, which could allow for remote code execution. (Security Affairs)

Cybersecurity training must not skip the C-suite. Ilia Sotnikov, Vice President of User Experience at Netwrix, notes that C-level executives are increasingly targeted in social engineering attacks due to their high-profile status and authority, making their access privileges exploitable by cybercriminals. To combat this, Sotnikov advises executives to participate in cybersecurity training, engage in regular discussions about cybersecurity with the CISO, and advocate for verifying suspicious activities through alternative communication channels. (Forbes)

50K WordPress sites exposed to RCE attacks by critical bug in backup plugin. The vulnerability tracked as CVE-2023-6553, can be exploited by unauthenticated attackers without user interaction. Although a patch has been released, almost 50,000 WordPress websites remain vulnerable to this critical security flaw. (Bleeping Computer)

Over 1,450 pfSense servers were exposed to RCE attacks via bug chain. Around 1,450 instances of pfSense, an open-source firewall and router software, are vulnerable to command injection and cross-site scripting flaws. These flaws, if exploited together, could allow attackers to execute remote code on the system. (Bleeping Computer)

Security Framework Guidance. The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Office of the Director of National Intelligence (ODNI), and industry partners have released a guide developed by the Enduring Security Framework, "Securing the Software Supply Chain: Recommended Practices for Managing Open-Source Software and Software Bill of Materials (SBOMs)." (CISA)

Threat Actor TA4557 targets recruiters with malware. The threat actor uses techniques such as sending URLs to fake resume websites or attachments containing instructions to visit the website, leading to the download of malicious files. (InfoSecurity Magazine)

This Week's Top Risks

Security is Everyone's Responsibility

Threats, Malware, Cybercampaigns, and Adversaries

- Agent Tesla
- Akira ransomware
- AtlasLion/Storm-0539
- BiBi ransomware
- Business email compromise and impersonation use of texts; credential pharming, harvesting, and validation scams.
- Carbanak (aka Anunak aka Sekur) Malware
- Crimson Kingsnake
- DarkGate Malware
- Diceloader
- Gh0st RAT
- GRANDOREIRO
- Lokibot
- Leonem/Phorpiex
- Mispadu
- Phorpiex
- Scattered Spider
- SectopRAT (aka ArechClient2)
- Snakelogger
- SorillusRAT
- TraderTraitor
- Ursa
- Xworm

Hardware & System Vulnerabilities (multiple)

- Adobe, Amazon, Apache, Apple, Atlassian, CA Database, Cygwin, Debian, Dell, Google, Hitachi, HP, Huawei, IBM, Lenovo, Linux, Microsoft, Mozilla, NetScout, nGeniusONE, Oracle, PAN-OS, Red Hat, SAP, SAPIU5, SUSE, Tableau, Ubuntu, and WordPress.

Themed Phishing Campaigns

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

Subject Keywords: Agent Change for my policy, Best Buy, Fidelity, Law office of, M365, Propertyfinder, Purchase Order, QR Code, RFQ CS2023-11, and Your Document #45.

Threats of the Week

Ransomware attack on CU provider and GuLoader highlight this week's risks

Ransomware Attack Impacts 60 Credit Unions

Summary

On 7 December, Ongoing Operations, a subsidiary of Trellance Cooperative Holdings, Inc., stated that they recently experienced an isolated cyber security incident, which is reportedly linked to outages at FedComp. Also on 7 December, CU Times reported National Credit Union Association (NCUA) Board Chairman Todd Harper did not hold back his feelings of frustration concerning the ransomware attack that has crippled approximately 60 credit unions around the country. Harper spoke publicly for the first time about the ransomware attacks during his quarterly media availability with reporters. He said, "All the affected credit unions are small institutions with $100 million or less in assets. Based on our estimates, approximately $912 million in aggregate assets and 93,000 members are affected by the FedComp outage."

On its website, Ongoing Operations said, "The nature of this ongoing investigation takes a substantial amount of time as the process of reviewing the files to determine what information may have been involved is lengthy and complex. We have made significant progress as we continue to re-establish services for customers. We are encouraged by our progress to date and remain confident our teams will be able to resolve the issue in a safe and secure manner." They provided the following notes that included:

- "On November 26th, 2023, Ongoing Operations experienced an isolated cybersecurity incident.
- Upon discovery, we took immediate action to address and investigate the incident, which included engaging third-party specialists to assist with determining the nature and scope of the event.
- We notified federal law enforcement. At this time, our investigation is currently ongoing, and we will continue to provide updates as necessary.
- As part of our response to this incident, we are reviewing the impacted data to determine exactly what information was impacted and to whom that information belonged.
- This incident is isolated to a segment of the Ongoing Operations network and our team is diligently working around the clock to minimize service interruptions wherever possible and to ensure the safety of information stored on the Ongoing Operations systems.
- We have notified all impacted customers and any who have not received a notice were not affected by this incident.
- The forensic investigation into the incident is still ongoing. We continue to make progress in re-establishing services for customers and we are notifying customers whose information was impacted. We will share more information as soon as there are updates.
- Ongoing Operations will assist impacted credit unions with member notification and will offer complimentary credit monitoring and identity restoration services to those who are impacted."

There have been no additional updates.

Remediation

We know that Information security and technology personnel wear many hats, and you want accurate and concise information to safeguard your credit union. The FS-ISAC community facilitates timely and sector-specific information sharing to put you in a better position to do just that. You can customize your access to FS-ISAC's intelligence alerts, reports, trends, strategic level trend reports for executive briefings, etc. to only receive what is critical for your IT management.

Additionally, every FS-ISAC member institution has a dedicated account manager who can provide individualized assistance to help you make the most of your membership and is available for consultation when it suits your schedule.

Problems Facing Credit Unions	FS-ISAC Solutions
1. Protecting data and operations from internal and external threats.	1. A community based on mutual trust and intelligence sharing housed in a robust secure intelligence platform.
2. Subject to a wide range of regulations and compliance requirements.	2. A document library with over 1,600 governance and operational risk management templates for use.
3. Limited resources and budget constraints.	3. Membership provides access to conferences, exercises, training, and a network of over 4,200 subject matter experts.
4. Information overload.	4. Concise daily reports and digests reduce "noise" and help you quickly identify information important to your credit union.

For a complete listing of available products and services by tier, please visit fsisac.com.

GULOADER Adds New Anti-Analysis Tactic to Arsenal

Summary

Cyware reports that security experts have unmasked a new trick adopted by the GULOADER malware (also known as CloudEyE) to evade detection by antivirus software. The highly evasive shellcode downloader malware, which typically spreads through emails bearing ZIP archives or links containing a VBScript file, has been found leveraging Vectored Exception Handler (VEH) capability to make analysis challenging.

According to Elastic Security Labs, the technique involves using a feature in Windows applications. GULOADER starts this process by adding the VEH using 'RtlAddVectoredExceptionHandler,' allowing the malware to intercept and handle exceptions during program execution. When these exceptions are triggered, the VEH checks for hardware breakpoints and subsequently deploys malicious payloads in the final stage.

Researchers note that while the technique is not new, the malware continues to add new exceptions over time as part of its anti-analysis tactics. Two of these exceptions, EXCEPTION_PRIV_INSTRUCTION and EXCEPTION_ILLEGAL_INSTRUCTION, were added to the malware in the last few months.

GULOADER employs a variety of sandbox evasion techniques, code obfuscation, and multiple layers of encryption to counteract antivirus products. While the core functionality of the malware has not changed drastically over the past few years, the updates in its obfuscation techniques indicate that GULOADER is under constant development. Coming to the latest anti-evasion tactic, organizations can leverage the latest YARA rules from Elastic Security to detect malware.

GULOADER is not the only malware with new evasion and anti-analysis techniques. The development comes days after researchers discovered a new variant of GootLoader, named GootBot, using custom-built bots in the late stage of the attack to avoid detection. This allowed the attackers to rapidly spread the malware throughout the network and deploy further payloads. In another instance, a malware loader known as WailingCrab used shipping-themed email messages to bypass security checks before being deployed onto the victims' systems.

FBI Guidance: Cyber Incidents on SEC Reporting Requirements

Reporting requirement goes into effect on 18 December

The FBI, in coordination with the Department of Justice, is guiding how victims can request disclosure delays for national security or public safety reasons. The FBI recommends all publicly traded companies establish a relationship with the cyber squad at your local FBI field office. This follows the Securities and Exchange Commission's new requirements for companies to disclose material cybersecurity incidents which takes effect on 18 December 2023.

Institutions can click on the buttons at the bottom of this page to read guidance on requesting a delay and providing necessary information to the FBI, to view the SEC Rule, and to read the FBI's Policy Notice about how victim requests are processed.

The FBI strongly encourages institutions and companies to contact the FBI directly or through the US Secret Service, CISA, or another sector risk management agency soon after a registrant believes disclosure of a newly discovered cybersecurity incident may pose a substantial risk to national security or public safety. This early outreach allows the FBI to familiarize itself with the facts and circumstances of an incident before the company makes a materiality determination. If the victim of a cyber intrusion engages with the FBI or another U.S. government agency, this engagement doesn't trigger a determination of materiality. However, it could assist with the FBI's review if the company determines that a cyber incident is material and seeks a disclosure delay. Please note that delay requests won't be processed unless they are received by the FBI immediately upon a company's determination to disclose a cyber incident via 8k.

'Tis The Season

Helping job-seeking customers avoid scams during the holiday season

Summary

This week concludes our second piece on holiday job scams. Scams can be hard to spot because they often look just like the real thing. That includes job scams. They crop up on real job sites, including places like LinkedIn. Scammers have even invited people to do things like 45-minute interviews, putting in the time so you let your guard down. So how do you tell a scam from the real thing?

Let's say you get a message from a recruiter. They say you're *just* what they've been looking for and schedule a virtual interview. The invitation has the company's logo and an official-looking job briefing guide describing the job's duties. Soon after the interview, you get the email: You got the job! The offer letter comes in — company logo and all — and everything seems promising. But what comes next? Here are some signs that the job offer may be a scam:

- **Scammy recruiters will email you from a personal email, not a company account.** Recruiters will generally email from their company (@companyname.com), not a personal email like @gmail.com or @yahoo.com.
- **Scammy recruiters push you for money.** They might send you a fake invoice for equipment (like a computer) or "training" that they'll supposedly order but tell you to pay for first — using mobile payment apps like Cash App, Zelle, or PayPal. They'll promise to reimburse you… but won't because it's a scam.
- **Scammy recruiters ask for your personal information upfront.** Before giving you any details about the job, they'll ask for your driver's license, Social Security, or bank account number to fill out "employment paperwork." But if you share it, they might steal your identity.

Not sure if you're dealing with a job scam? Contact the company using a phone number or website you know to be legitimate — not one you got from the "recruiter."

Report job scams to the FTC: ReportFraud.ftc.gov.