FS-ISAC

Community Institution & Associations Risk Summary Report

Week of 28 August | 2023 Edition | Vol. 193

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

How, why to bring more women into supply cybersecurity. When increasing cybersecurity efforts, procurement officials should know that "[d]iverse teams are 87% better at making decisions and 35% more likely to outperform their competitors," but "less than one-quarter (24%) of the entire cybersecurity workforce are gender diverse," Katie Owston of Glocomms writes. Supply chain leaders should promote their field and the cybersecurity subset by working to interest schoolgirls in STEM, "communicating and rewarding the skillsets needed," highlighting career paths, offering free seminars, and mentoring employees, says Owston, who details ways to do more. (SDC Supply & Demand Magazine)

International Cyber League Financial Cup 2023. This entirely virtual tournament, organized in partnership with Cyberbit, is a perfect opportunity to test your technical skills in a friendly competition simulating a real-life end-to-end attack. The International Cyber League Financial Cup allows cybersecurity professionals to experience live-fire challenges, which mirror real-life scenarios. Test your skills as a cyber defender, so you are better prepared for an attack in a live environment. This is a virtual tournament, which will have two rounds. The first round will require up to an hour of your time. The finals will require up to three hours of your time. Learn how to participate. View (FS-ISAC)

Nearly 1,000 organizations, 60 million individuals impacted by MOVEit hack. During 14-15 August, the cybercriminals leaked nearly 1 TB of information allegedly stolen from 16 victims, Resecurity said. These victims include UCLA, Siemens Energy, Cognizant, Norton LifeLock, and Netscout cybersecurity firms. (Security Week)

Vendors training AI with customer data is an enterprise risk. Zoom received some flak recently for planning to use customer data to train its machine-learning models. The reality, however, is that the video conferencing company is not the first, nor will it be the last, to have similar plans. (Dark Reading)

Android banking trojan MMRat carries out bank fraud via fake app stores. The Trend Micro Mobile Application Reputation Service (MARS) team discovered a new, fully undetected Android banking trojan, dubbed MMRat (detected by TrendMicro as AndroidOS_MMRat.HRX), that has been targeting mobile users in Southeast Asia since late June 2023. The malware, named after its distinctive package name com.mm.user, can capture user input and screen content and remotely control victim devices through various techniques, enabling its operators to carry out bank fraud on the victim's device. (Micro Trend)

Leaseweb reports cloud disruptions due to cyberattack. Dutch infrastructure-as-a-service and cloud solutions provider Leaseweb shut down some critical systems last week due to a cyberattack. They detected unusual activity on 22 August, but the company said impacted systems should now be restored. The company's status page does not mention any issues at the time of writing. Leaseweb provides cloud, CDN, managed hosting, colocation, bare metal servers, and other services to more than 17,000 customers, including SMBs and enterprises. (Security Week)

PoC for unauthenticated RCE on Juniper Networks firewalls released. Researchers have released additional details about the recently patched four vulnerabilities affecting Juniper Networks' SRX firewalls and EX switches that could allow remote code execution (RCE), as well as a proof-of-concept (PoC) exploit. (HelpNet Security)

This Week's Top Risks

Security is Everyone's Responsibility

Threats, Malware, Cybercampaigns, and Adversaries

- Agent Tesla
- ASYNC RAT
- Business email compromise and impersonation use of texts; credential capture, pharming, harvesting, and validation scams
- CosmicRust Malware
- DarkGate Malware
- Ducktail Malware
- EvilProxy
- Formbook
- GRANDOREIRO
- IceID
- JsOutProx RAT
- Lazarus Group
- Lokibot
- NJRAT/Rhysida
- Qbot/QakBot
- Redline
- Rhysida Ransomware
- Remcos (GuLoader)
- SectopRAT (aka ArechClient2)
- SOCGHOLISH
- SolarMarker (aka Jupyter) Malware
- vjw0rm (aka Vengeance Justice Worm) RAT Malware
- Xloader
- XWorm (churchxx, freshinxworm)

Hardware & System Vulnerabilities (multiple)

- Amazon, Apache, Apple, Arista, Avaya, Check Point, Cisco, Cygwin, Debian, Dell, F5, Google, IBM, Juniper, Lenovo, Linux, Microsoft, Mozilla, Oracle, Red Hat, SUSE, Trellix, Ubuntu, VMWare, Wireshark, and Xerox.

Themed Phishing Campaigns

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

Subject Keywords: COMPROMISED WEBSITES, Corporate eFax, Delivery, DUE INVOICE, Esther Mallard, iPhone, Mary Weathersbee shared, Microsoft, NEW Order 0928, Observe Messages, Order PO No, paid invoice, Payroll Submission, RFQ For Attached BOQ, Sharepoint, and Subscription Renewal.

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.

© 2023 FS-ISAC, Inc. | All Rights Reserved.

Threats of the Week

Barracuda, Lazarus, WinRAR, highlight this week's risks

Barracuda ESG is Still Vulnerable

Summary

The FBI has reported that Barracuda's Email Security Gateway previously exploited appliances are still vulnerable to attacks even after patches were published for CVE-2023-2868. NIST reports this vulnerability as a remote command injection vulnerability for versions 5.1.3.001-9.2.0.006 of Barracuda's Email Security Gateway related to incomplete input validation for .tar files. Mandiant reported in July that this vulnerability had been exploited by skilled actors, suspected to be linked to China. The Cybersecurity Infrastructure and Security Agency (CISA) separately published a report on the malware variants that were observed being used to implant backdoors in the appliance. On 29 August, Bleeping Computer reported US government email servers were hacked in Barracuda zero-day attacks. The attacks' motivation was espionage, with the threat actor (tracked as UNC4841) engaging in targeted exfiltration from systems belonging to high-profile users in government and high-tech verticals.

Remediation

FBI recommends the removal of Barracuda ESG appliances that have been compromised. Barracuda has notified affected customers.

We continue to be saddened by the terrible loss Hawaiians are continuing to endure for family, friends, colleagues, and victims in Maui. It's our sincerest wish that your resiliency be fueled by the love of your neighbor, your willingness to help, and the comfort you provide.

The Return of Lazarus

Summary

Cyware reports that the North Korean state-sponsored Lazarus APT group has initiated a fresh initiative aimed at internet backbone infrastructure and healthcare organizations situated in Europe and the US. Cisco Talos reported that the hackers commenced their attack by taking advantage of a vulnerability within ManageEngine ServiceDesk (CVE-2022-47966) as early as January, a mere five days after its disclosure.

The exploit was employed by Lazarus to establish initial access, prompting the immediate downloading and running of a malicious binary through the Java runtime process, thereby initiating the implant on the compromised server. This binary represents a modified version of the group's MagicRAT malware, dubbed QuiteRAT. The Lazarus Group APT has also introduced a fresh malware named CollectionRAT in this campaign. It functions as a RAT capable of executing arbitrary commands on a compromised system. Furthermore, security researchers could establish a connection between CollectionRAT and Jupiter/EarlyRAT, a malicious software previously associated with the Andariel APT faction, which operates under the umbrella of the Lazarus Group.

Similar to MagicRAT, QuiteRAT is constructed using the Qt framework, an open-source, cross-platform framework designed for crafting applications. It boasts functionalities such as arbitrary command execution. However, its file size is notably smaller, ranging from 4 to 5MB, in contrast to MagicRAT's 18MB. The analysis points out that this considerable difference in size can be attributed to the Lazarus Group's decision to incorporate only essential Qt libraries into QuiteRAT, as opposed to MagicRAT, where the entire Qt framework was integrated. Although MagicRAT integrates mechanisms for persistence by enabling the configuration of scheduled tasks, QuiteRAT lacks inherent persistence functionality. Instead, QuiteRAT relies on the C2 server to provide it with persistence instructions.

This marks the third officially documented campaign attributed to the Lazarus Group in the early months of 2023, and interestingly, this actor has consistently repurposed the same infrastructure across these operations. Cybersecurity teams are advised to track and analyze the threat for timely prevention of infection from QuiteRAT.

WinRAR Vulnerability Used to Target Traders

Summary

Last week we reported information about a Bleeping Computer story about a WinRAR flaw that lets hackers run programs when you open RAR archives (CVE-2023-40477). WinRAR is a popular data compression, encryption, and archiving tool; however, security researchers have identified a recently-patched vulnerability exploited as a zero-day as far back as April 2023. CVE-2023-38831 allows attackers to execute arbitrary code on a victim machine when the user attempts to view a benign file within a ZIP archive. The archive would have to contain a folder with a malicious executable that has the same name as the benign file, which would then be processed while attempting to access only the benign file. Additionally, the vulnerability allows actors to spoof a file extension, hiding malicious scripts in seemingly benign .jpg or .txt files. The attack was used to deliver a variety of malware families, including GuLoader, DarkMe, and Remcos RAT. The campaign identified by the researchers was targeted at traders, as they identified malicious archives hosted on at least eight popular trading forums with as many as 130 traders' devices being impacted globally. The actors would post the archives on forums where traders would share information, including files, with each other. After the compromise occurred, the actors were granted unauthorized access to the traders' broker accounts, allowing them to conduct illicit financial transactions and withdraw funds. As with many vulnerabilities that have since received patches, it is recommended to update your WinRAR instance to the current version, which at the time of this writing is 6.23.

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.

© 2023 FS-ISAC, Inc. | All Rights Reserved.

Just For Community Institutions

Your Toolkit for Synthetic Fraud Identification

Summary

The cybercriminal fraud toolkit contains a wide variety of instruments that fraudsters use, but were you aware synthetic fraud is often miscategorized as a credit loss and accounted for an estimated $20 billion in losses (Off-site) for US financial institutions in 2020? The Federal Reserve has produced a Fraud Mitigation Toolkit to educate and provide recommendations to reduce fraud loss. The toolkit contains 9 modules and is available at no charge.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While the use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each entity.

Additional Member Benefits That May Be Available to You

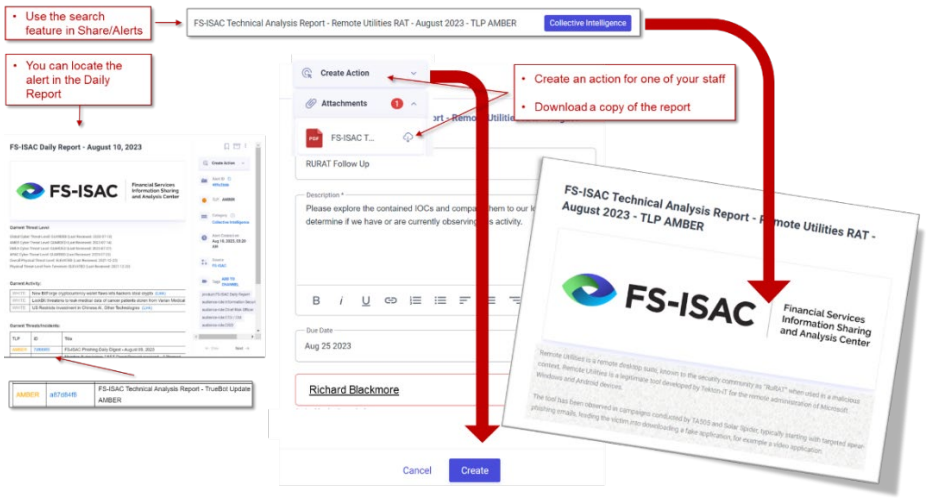
DID YOU KNOW?

You can sharpen your cyber intelligence teeth by reading FS-ISAC's Global Intelligence Office Technical Analysis Reports (TAR).

You can!

These reports cover a single topic and provide the who, what, and where on a variety of different items. There are many ways to obtain the report.

1. Log into the IntelX platform.
2. Select the Share App
3. Select the Alert icon from the lefthand menu bar



4. Go to the search field type Technical Analysis Report and select enter. Click on the desired report.
5. If you already received the FS-ISAC Daily Report, identify the report, and click on the report ID.
6. If you already receive Collective Intelligence Reports, open the TAR ID listed to access the IntelX and download it after authenticating.

EVENTS

Registration for the 2023 CAPS exercise for community institutions is now open on the FS-ISAC Intelligence Exchange, within the Member Services application. You'll register for the 2023 CAPS season, 4 September – 13 October, then conduct the exercise with your team over a day or two when best for your schedules. The CAPS virtual tabletop exercise challenges your incident response team to overcome a simulated attack against banking systems and processes. Participants practice mobilizing quickly, working under pressure, critically appraising information as it becomes available, and connecting the dots to defend against a cyber-attack on a fictional bank and credit union. One individual registers and leads your internal team through a two-part virtual exercise. The exercise follows a realistic, timely scenario involving a fictional organization.

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.

© 2023 FS-ISAC, Inc. | All Rights Reserved.