FS-ISAC

Community Institution & Associations Risk Summary Report

Week of 21 August | 2023 Edition | Vol. 192

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).

Chip manufacturers urged to collaborate on cybersecurity. The semiconductor industry is interdependent and complex and faces an increased risk of cyberattacks. Chip manufacturers could reduce the threat by collaborating, according to security leaders at Semicon West. Agreeing to security standards and holding suppliers to assessments can help, and SEMI is promoting industrywide collaboration through its Cyber Security Consortium. (Semiconductor Engineering)

Exploitation of Citrix ShareFile. Exploitation attempts targeting a remote code execution flaw in Citrix's ShareFile product have spiked just as the US Cybersecurity and Infrastructure Security Agency (CISA) added it to its Known Exploited Vulnerabilities Catalog. Tracked as CVE-2023-24489, the shortcoming has been described as an improper access control bug that, if successfully exploited, could allow an unauthenticated attacker to compromise vulnerable instances remotely. Citrix announced the availability of patches for the bug on 13 June, and exploitation started in late July. Researchers warned that there had been between 1,000 and 6,000 internet-exposed ShareFile instances. (FS-ISAC GIO)

New BlackCat ransomware variant leverages Impacket for lateral movement. Microsoft Threat Intelligence has observed a new version of the BlackCat ransomware being used in recent campaigns based on the open-source communication framework tool Impacket, which threat actors use to facilitate lateral movement in target environments. In a post on 17 August on X, (formerly Twitter), the Microsoft researchers said Impacket has credential dumping and remote service execution modules that attackers could use for broad deployment of the BlackCat ransomware. This BlackCat version also has the Remcom hacktool embedded in the executable for remote code execution. (SC Media)

Patched Citrix NetScaler devices still contain backdoors. Online scans conducted by Delft-based Fox-IT and the nonprofit Dutch Institute for Vulnerability Disclosure show more than 1,200 patched NetScaler devices containing a backdoor inserted by hackers. Attackers appear to have automated exploitation of a flaw allowing them to execute arbitrary commands through a web shell, "even when a NetScaler is patched and/or rebooted." (Data Breach Today)

TunnelCrack attacks a risk to VPN. Researchers have identified multiple vulnerabilities in VPN products that allow attackers to read user traffic, steal user information, or even attack user devices. These vulnerabilities are collectively known as TunnelCrack, and they are categorized within four CVEs. Two of the CVEs require a LocalNet (such as a rogue network), and the other two attack a ServerIP (a malicious ISP for instance). All of the vulnerabilities trick the victim into sending traffic outside the VPN, which allows an adversary to intercept it. Interestingly, the researchers state that Apple devices are the most vulnerable, while Android devices are the most secure. (FS-ISAC GIO)

Update: Companies respond to 'Downfall' Intel CPU vulnerability. AWS said its customers' data and cloud instances are not affected by Downfall and no action is required. The cloud giant did note that it has "designed and implemented its infrastructure with protections against this class of issues". (Security Week)

WinRAR flaw lets hackers run programs when you open RAR archives. A high-severity vulnerability that can allow attackers to execute commands on a computer simply by opening an archive has been fixed in WinRAR, the popular file archiver utility for Windows used by millions. (Bleeping Computer)

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
- DarkGate Malware
- Ducktail Malware
- EvilProxy
- Formbook
- GRANDOREIRO
- IceID
- JsOutProx RAT
- Lokibot
- Netsupport
- NJRAT/Rhysida
- Qbot/QakBot
- Redline
- Remcos (GuLoader)
- SectopRAT (aka ArechClient2)
- SOCGHOLISH
- SolarMarker (aka Jupyter) Malware
- TrueBot
- Xloader
- XWorm (churchxx, freshinxworm)

Hardware & System Vulnerabilities (multiple)

- Apache, Atlassian, Avaya, Check Point, Debian, Dell, F5, Google, HP, Huawei, IBM, Ivanti, Juniper, Juno, Lenovo, Linux, Microsoft, Mozilla, Oracle, Red Hat, SUSE, and Ubuntu.

Themed Phishing Campaigns

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

Subject Keywords: Clive Morgan, Completed Scan Date Doc Copy, Delivery, DHL, Download, FIS, Incoming Document, LinkedIn, MASS TRAIDING DELIVERY, Proposal Spreadsheet, Quick Request, Refinitiv Eikon, Remittance, Shared the folder, Terminus Roofing, View Completed Documents Loan, Wallet frozen, Woodall Heating & Cooling, you have a new message, and Your attachment.

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

LinkedIn, cloaked malvertising, and targeted Zimbra phishing highlight this week's risks

LinkedIn Accounts Hacked in Widespread Campaign

Summary

A widespread global campaign is targeting LinkedIn users, with threat actors taking over accounts and attempting to extort victims. Many users are now locked out for security, or their accounts are hijacked by attackers. Affected users have taken to X (formerly Twitter) to complain about their inability to resolve problems through LinkedIn support. Some users are being pressured into paying a ransom to regain control, or the threat actor threatens to delete the account. The attackers appear to use leaked credentials or brute force in an attempt to take over a large number of accounts. For users that use strong passwords and two-factor authentication, multiple account takeover attempts trigger a temporary lock from LinkedIn security as a protection measure. Owners of these accounts are then prompted to verify ownership by providing additional information and updating their passwords before they are allowed to sign in again. When hackers take over the account, they swap the associated email address with one from "rambler.ru." Rambler is a Russian search engine and one of Russia's largest web portals. Given the prevalence of LinkedIn use by individuals in the financial sector, it is recommended users review the security measures they have implemented and activate 2FA along with using a strong password. LinkedIn accounts are lucrative to hackers, allowing them to create social engineering, phishing, and job offer scams that can lead to multi-million-dollar cyber thefts. FS-ISAC has distributed the following TLP Amber reports for member review.

https://share.fsisac.com/webapp/user/myfeeds/16984b85

https://share.fsisac.com/webapp/user/myfeeds/54c75cbd

https://share.fsisac.com/webapp/user/myfeeds/bd596109

https://share.fsisac.com/webapp/user/myfeeds/5463406a

Cloaked Malvertising: Unmasking Complex Fingerprinting and Evading Detection

Summary

In an escalating digital arms race, malvertisers have unveiled a new wave of sophisticated tactics that employ an advanced cloaking technique to evade detection. Threat actors are targeting specific IT programs, such as remote access tools and scanners, by creating malicious ads that appear on popular search engines such as Google, revealed security experts at Malwarebytes.

The malvertising campaign involves creating ads for legitimate-sounding domains. The ads lead to pages that employ multiple layers of checks, including server-side IP checks and client-side fingerprinting, to ensure that the victim is not a researcher or using a virtual machine. The fingerprinting process collects various browser properties, time zone information, rendering capabilities, and other data. If the victim passes these checks, they are redirected to a malicious landing page where they can download the malware payload. The use of advanced cloaking techniques in malvertising campaigns allows threat actors to evade detection and maintain their malicious infrastructure online for longer periods. The tactic, furthermore, impacts takedown actions as platforms may need to validate reports before suspending advertising accounts.

The use of advanced cloaking techniques and sophisticated fingerprinting processes allows malicious ads to remain undetected and deliver malware payloads to unsuspecting victims. To safeguard against ever-evolving malvertising tactics, security experts must prioritize regular website security audits, robust traffic analysis, and anomaly detection. Continuous monitoring for unauthorized code injection is crucial to thwarting the persistent malvertising menace.

Ongoing Phishing Campaign Targets Zimbra Credentials

Summary

Cyware reports, that ESET researchers have discovered an ongoing phishing campaign targeting users of the Zimbra Collaboration software platform. The campaign, which started at least in April 2023, aims to collect Zimbra account users' credentials.

The campaign uses different social engineering lures such as an email server update, account deactivation, or similar issues to deceive recipients. The phishing email appears to come from an email server administrator and contains an HTML file that directs the user to a fake Zimbra login page. In some cases, the attackers have also been found using compromised Zimbra accounts to send subsequent waves of phishing emails. The submitted credentials are then collected and sent to a server controlled by the attacker. Despite not being highly sophisticated, the campaign is still successful, owing to the wide usage of the Zimbra Collaboration suite across multiple organizations, thus making them lucrative targets for adversaries.

The targets of the campaign include small and medium businesses as well as governmental entities. The countries most affected by the campaign are Poland, Ecuador, and Italy.

The campaign examined by ESET relies solely on social engineering tactics and user engagement. However, note that this may not always be the situation. In a previous campaign disclosed by Proofpoint in March 2023, the APT group Winter Vivern (also known as TA473) exploited the CVE-2022-27926 vulnerability to target webmail portals of military, government, and diplomatic entities in European countries. Another instance reported by Volexity in February 2022, involved a group called TEMP_Heretic extracting emails from European government and media organizations by taking advantage of another vulnerability (CVE-2022-24682) in Zimbra Collaboration's Calendar feature. In the most recent reference, EclecticIQ researchers examined a campaign resembling the current campaign. The primary distinction is that the HTML link leading to the fraudulent Zimbra login page is directly embedded within the email itself.

Since the current campaign heavily relies on phishing emails, security teams are advised to implement necessary email security controls to stay safe. Additionally, it is recommended to apply the latest security updates and look at the IOCs associated with the campaign to block the indicators at the endpoints.

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

Is Your Institution Retaining Too Many Documents?

Holding onto documents for too long may not be good for your institution

Summary

The one thing community institutions have is documents whether they are electronic or hard copy. Data retention laws define how your institution stores and manages records produced from everyday business. Some of these records include personally identifiable information, financial data, tax documents, intellectual property, and other relevant information. Additionally, institutions must consider federal retention laws (e.g., BSA Record Retention Requirements; for comprehensive and current BSA record retention requirements, refer to U.S. Treasury/FinCEN regulations found at 31 CFR Chapter X), and each state may also have data retention laws. These laws dictate the types of data that must be retained and for how long. There are also other considerations that include the European Union's General Data Protection Regulation.

Institutions should adopt a defensive structure regarding the documents they generate. This defensive structure includes an effective data retention policy, in compliance with data retention laws, which can prepare you for potential lawsuits, and which ensures an improvement in the overall efficiency of your institution's operation. Leading practices include understanding retention laws, encouraging collaboration within your institution, and identifying data retention periods, storage requirements, available technological solutions, authority structure, and protocols for policy or process violations.

Record Nations provides links to applicable document retention laws by state.

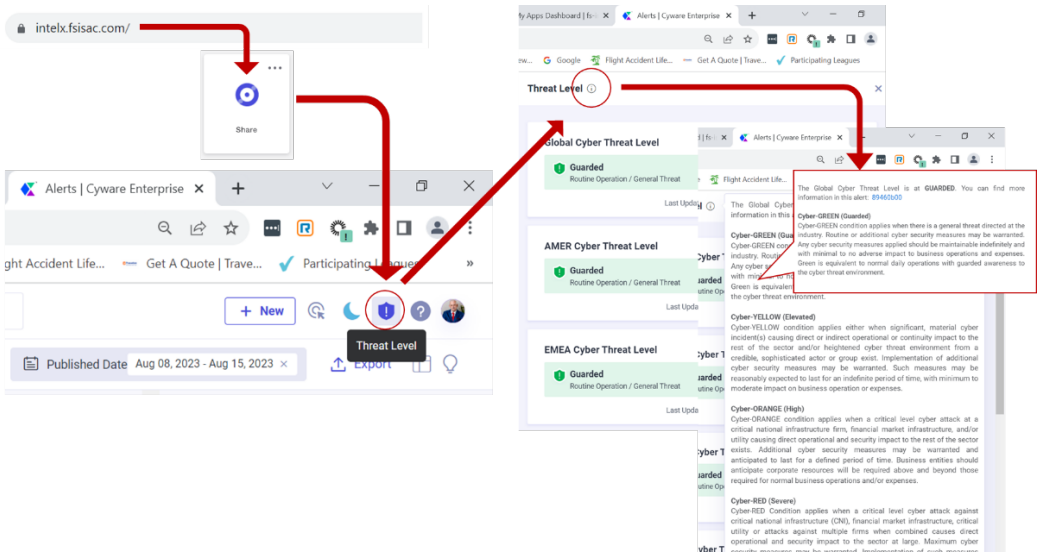
Additional Member Benefits That May Be Available to You

DID YOU KNOW?

You can check the threat status with the click of a mouse. You Do!

FS-ISAC members use the Cyber Threat Levels to keep their leadership situationally aware concerning any region around the globe.

1. Log into the IntelX platform.
2. Select the Share App
3. Select the Alert icon from the lefthand menu bar
4. Click on the shield icon in the upper right corner to expand the threat level box.
5. Click the information icon to learn more about each level and alert information justifying the current level.



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.

FinCyber Today Summit Registration is now open for our 2023 FinCyber Today Summit to be held 1 – 4 October in Orlando, FL. Registration is complimentary for all member tiers. To register, log into your IntelX account at intelx.fsisac.com. From there, go to your Member Services application and click Events/Training, located at the top of the website. The link for registration is "FS-ISAC 2023 FinCyber Today Summit 1OCT23."

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.