FS-ISAC

Community Institution & Associations Risk Summary Report

Week of 2 October | 2023 Edition | Vol. 198

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 the Financial Services Information Sharing Analysis Center (FS-ISAC) has observed this week for community institutions (CIs).

Booking.com customers hit by phishing campaign delivered via compromised hotel accounts. The phishing attacks are highly convincing, using personalized messages and a meticulously crafted phishing page that mimics the Booking.com interface, leading victims to unknowingly provide their credit card or bank information. (Perception Point)

DHS investigating whether floor plans and other security information were exposed in a ransomware attack. Senior Department of Homeland Security officials are working to determine if a ransomware attack on government contractor Johnson Controls International has compromised sensitive physical security information such as DHS floor plans, according to internal DHS correspondence reviewed by CNN. (CNN)

City of Fort Lauderdale, Florida, taken for $1.2m in an email scam. The payment, intended for a new police headquarters building, was made to a scammer who posed as the legitimate contractor, Moss Construction. The incident underscores the need for increased cybersecurity measures against process controls for vendor payments business email compromise. (Statescoop)

Don't let zombie Zoom links drag you down. Many organizations — including several Fortune 500 firms — have exposed web links that allow anyone to initiate a Zoom video conference meeting as a valid employee. These company-specific Zoom links, which include a permanent user ID number and an embedded passcode, can work indefinitely and expose an organization's employees, customers, or partners to phishing and other social engineering attacks (KrebsOnSecurity)

Eye on fraud. It's a sobering part of the daily payments arena—fraud is unending and always evolving. That's why payments and anti-fraud companies continue to create new services to keep up with the latest scams. Visa on Monday said it would make managed detection and response services from Expel Inc. available to its clients. McAfee Corp., best known for its antivirus software, added artificial intelligence capabilities that could help improve the detection of phishing attempts. (Digital Transactions)

Malicious ads infiltrate Bing AI Chatbot in malvertising attack. The Bing AI chatbot labeled the malicious website as the official website of an IP scanner provider and recommended users to visit it, despite its involvement in the malvertising attack campaign. In the wake of OpenAI's ChatGPT's soaring success, Microsoft's Bing AI Chatbot emerged as a challenging player in the world of artificial intelligence, boasting over 100 million active users. While this achievement underscores the growing influence of AI, it has also attracted the attention of cybercriminals seeking to exploit this massive user base. (Cybersecurity Now)

MOVEit maker warns of new critical bug affecting thousands. Progress Software, the company behind the MOVEit Transfer tool which hackers exploited to breach thousands of businesses, said its WS_FTP Server software needs to be patched for a maximum severity bug. The company recently disclosed vulnerabilities affecting the WS_FTP Server secure file transfer software's interface and Ad hoc transfer module. According to Progress' advisory, attackers could "leverage a .NET deserialization vulnerability in the Ad Hoc Transfer module to execute remote commands on the underlying WS_FTP Server operating system." (Cyber News)

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 capture, pharming, harvesting, and validation scams.
- CageyChameleon (New)
- Carbanak (aka Anunak aka Sekur) Malware
- Clearfake
- DarkGate Malware
- Daveloader
- EvilProxy
- Formbook
- GhostSec
- GRANDOREIRO
- JsOutProx RAT
- Lumma Stealer
- Minodo Backdoor Malware
- Redline
- Remcos (GuLoader)
- SOCGHOLISH

Hardware & System Vulnerabilities (multiple)

- Android, Apple, Arista, Atlassian, Avaya, CA OPS/MVS Event Management, Chromecast, Cisco, Cygwin, Debian, Dell, EXIM, F5, GNU, Hitachi, Lenovo, Linux, Microsoft, Mozilla, Oracle, Pan-OS, RackSpace, Red Hat, Samsung, SUSE, Ubuntu, Wireshark, Xerces-C++, and X.Org libX11.

Themed Phishing Campaigns

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

Subject Keywords: Additional Microsoft Security Verification, Contract Agreement, Crypto Themed, DBF | Notice of Distribution, Google, Incoming document from, McAfee, Payment, QR, Shipment, Support Team, User Registration Agreement, We the People, and Your Parcel.

Threats of the Week

libwebp vulnerability, Budworm, and EvilProxy highlight this week's risks

libwebp vulnerability - CVE-2023-4863

Summary

Google's recent decision to reclassify a vulnerability in the libwebp image library has brought significant attention to an issue initially described as a Chrome weakness. Tenable provides a clear overview. The vulnerability resides within the Huffman coding algorithm used by libwebp for lossless compression. Exploiting this weakness enables attackers to execute out-of-bounds memory writes by employing maliciously crafted HTML pages. Such exploits can lead to severe consequences, including system crashes, arbitrary code execution, and unauthorized access to sensitive information due to it initially going unnoticed as a potential security threat for numerous projects using libwebp, including 1Password, Signal, Safari, Mozilla Firefox, Microsoft Edge, Opera, and the native Android web browsers. However, different vendors filing different CVEs may be responsible for a library issue contributing to confusion and people not realizing the severity / potential impact of the vulnerability. CISA has warned that the vulnerability is already being actively exploited in the wild. The exploit chain is likely BLASTPASS, a zero-click vulnerability found in early September by Citizen Lab. The exploit was being used to deliver NSO Group's Pegasus spyware. While the scale of this vulnerability is not clear, many are drawing comparisons to the Log4j (CVE-2021-44228) vulnerability of 2021.

Budworm Strikes Again: Updated SysUpdate Targets Government and Telecom Sectors

Summary

The Budworm APT group is evolving its cyber arsenal. In the latest discovery, Symantec's Threat Hunter Team identified that Budworm has adapted and upgraded one of its primary tools. Two significant entities, an Asian government, and a Middle Eastern telecommunication firm, were targeted with this renewed strategy. In August 2023, Budworm, also known as LuckyMouse, Emissary Panda, and APT27, launched an attack deploying an updated SysUpdate backdoor - SysUpdate DLL inicore_v2.3.30.dll. The group combined this with a mix of custom malware, along with several living-off-the-land and publicly available tools. The primary aim of the attackers was credential harvesting to attacks, blending malicious tools with legitimate ones to avoid suspicion. Tracing back to 2013, Budworm's endeavors have primarily targeted entities in defense, government, and technology sectors, particularly in Southeast Asia, the Middle East, and the US. APT27's victim profile, such as the recent targeting of an Asian government and a Middle Eastern telecom firm, aligns with its intelligence-gathering objectives. The latest version of SysUpdate affirms the group's ongoing toolset development. Organizations should proactively update and patch their systems to counter known vulnerabilities exploited by tools like SysUpdate. Advanced threat intelligence and monitoring solutions can help identify and counteract unusual activities, especially those associated with known threat actors such as Budworm.

EvilProxy Phishing Attack Abusing Indeed

Summary

Recent research from Menlo Labs has uncovered a sophisticated phishing campaign aimed at executives employed across industries, such as banking, insurance, property management, real estate, and manufacturing. The US-based organizations have been the primary targets. The phishing campaign began in July and abused an open redirection vulnerability on the job search platform Indeed[.]com. The campaign employed the EvilProxy phishing kit against potential targets. The phishing pages masquerade as Microsoft, as part of the Adversary in the Middle (AiTM) phishing method. This kit operates as a reverse proxy, standing between the client and the legitimate website, dynamically fetching content from legitimate login sites to appear legitimate. The one sign to the user that the proxy login page is not the real one is the URL. When the victim logs in, EvilProxy can allow the attacker to intercept server communications and steal session cookies, enabling them to impersonate victims and bypass MFA. The open redirection vulnerability in Indeed plays a critical role in this malicious scheme, allowing users to be redirected to an untrusted external domain. This flaw can exploit the trust users have in the original source, misleading them into believing they're accessing a legitimate site when they are, in reality, being directed to a malicious one. This campaign highlights the escalating threats that organizations face from threat actors due to the use of sophisticated tools and trusted platforms to hoodwink their targets. To mitigate such threats, it is recommended to educate employees through regular training sessions, implement robust security protocols, continuously monitor network traffic, and maintain updated threat intelligence to identify and counteract emerging threats.

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 Breakfasts

1-4 October
Asia 1

Ransomware Exercise

11 Oct. 2023
Register

CIAC Meeting

23 Oct. 2023
3:30 PM ET

Top 2023 Domain Impersonations

17 October
Member Only Virtual

Just For Community Institutions

Two or More Ransomware Variants Impacting the Same Victims and Data Destruction Trends

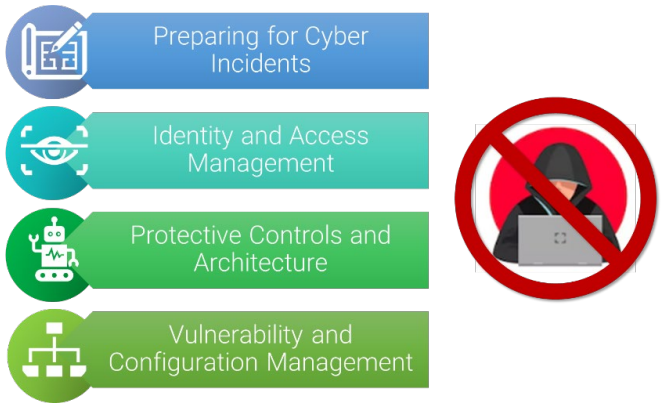
Summary

As of July 2023, the FBI noted two trends emerging across the ransomware environment and released a notification for industry awareness. These new trends included multiple ransomware attacks on the same victim in close date proximity and new data destruction tactics in ransomware attacks. In early 2022, multiple ransomware groups increased the use of custom data theft, wiper tools, and malware to pressure victims to negotiate. In some cases, new code was added to known data theft tools to prevent detection. In other cases, in 2022, malware containing data wipers remained dormant until a set time, then executed to corrupt data in alternating intervals.

The FBI noted a trend of dual ransomware attacks conducted near one another. During these attacks, cyber threat actors deployed two different ransomware variants against victim companies from the following variants: AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum, and Royal. Variants were deployed in various combinations. This use of dual ransomware variants resulted in a combination of data encryption, exfiltration, and financial losses from ransom payments. Second ransomware attacks against an already compromised system could significantly harm victim entities.

Remediation

- Institutions should follow mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise by ransomware.
- Report information concerning suspicious or criminal activity to their local FBI field office or ic3.gov. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.
- Access the FBI Private Industry Notification to obtain additional baseline practices.



Additional Member Benefits That May Be Available to You

DID YOU KNOW?

The Document Library is available to all community banks and credit unions.

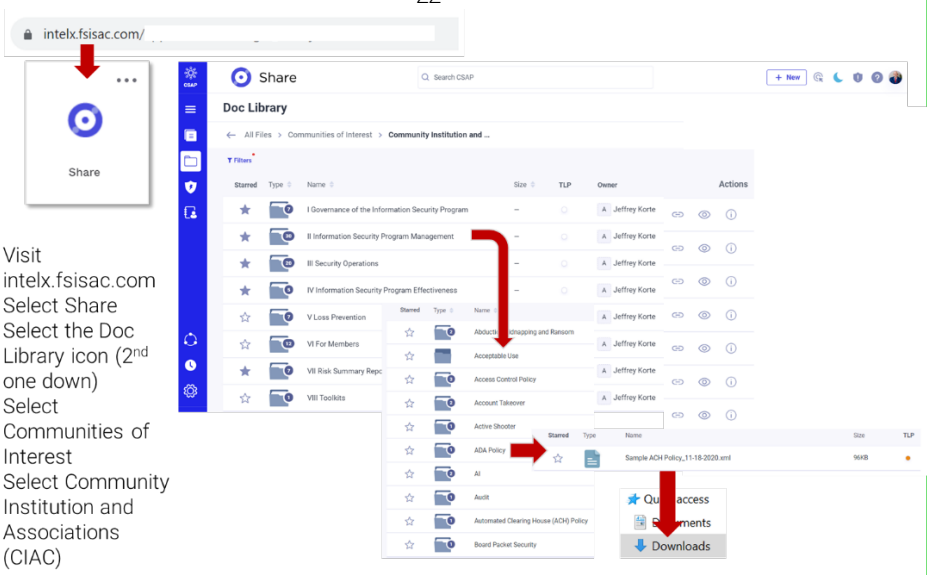
It is!

The Doc Library contains over 1,600 different documents that you can download, modify, and seek internal approval from your leadership.

These documents help reduce your research, development, approval, and implementation.

After logging into the IntelX platform and navigating to the CIAC section (see right), select the II Information Security Program Management folder and advance to the Policy, Programs, Procedures, and Planning folder. Note, there is a bar at the bottom to view other pages.

ZZ



1. Visit intelx.fsisac.com
2. Select Share
3. Select the Doc Library icon (2nd one down)
4. Select Communities of Interest
5. Select Community Institution and Associations (CIAC)

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.