FS-ISAC

Community Institution & Associations Risk Summary Report

Week of 14 August | 2023 Edition | Vol. 191

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).

Chinese RedHotel spy group linked to hacks in 17 countries. A Chinese state-sponsored spy group called RedHotel has emerged as a dominant espionage agent against government entities of at least 17 countries worldwide. Researchers said the motives and operations of the group closely link it to China's Ministry of State Security. (Data Breach Today)

**Groups urged to go passwordless to fight LAPSUS$**. The Cybersecurity and Infrastructure Security Agency (CISA) is urging organizations to use passwordless authentication and zero trust to prevent attacks by the LAPSUS$ hacking group. Social engineering and spear phishing are two methods favored by hackers. (IT Pro)

The brains behind the malware-friendly AI chat service 'WormGPT'. WormGPT, a private new chatbot service advertised to use Artificial Intelligence (AI) to help write malicious software without all the pesky prohibitions on such activity enforced by ChatGPT and Google Bard, has started adding restrictions on how the service can be used. Faced with customers trying to use WormGPT to create ransomware and phishing scams, the 23-year-old Portuguese programmer who created the project now says his service is slowly morphing into "a more controlled environment." The large language models (LLMs) made by ChatGPT parent OpenAI or Google or Microsoft all have various safety measures designed to prevent people from abusing them for nefarious purposes — such as creating malware or hate speech. In contrast, WormGPT has promoted itself as a new LLM that was created specifically for cybercrime activities. (Krebs on Security)

Intel x86 vulnerability — "Downfall". New research presented at Black Hat finds that several generations of Intel's x86 processors rely on a technique that increases performance but also introduces a vulnerability. The x86 architecture uses a small "register buffer" to store data. Different applications share this buffer, and when the CPU executes a "gather" command, it can read data left in the register by another application and forward it to an attacker. The vulnerability, called "Downfall," could allow an attacker to use one application to steal sensitive information like encryption keys or passwords. However, Intel commented that a practical attack "would be very complex to pull off." (FS-ISAC GIO)

Intel addresses 80 firmware, software vulnerabilities. The most serious of the patched flaws, based on their CVSS score, are 18 high-severity issues allowing privilege escalation or, in a few cases, denial-of-service (DoS) attacks. (Security Week)

New Windows malware QwixxRAT appears in the threat landscape. According to the experts, QwixxRAT is meticulously designed to steal a broad range of information, including data from browser histories, credit card details, screenshots, and keystrokes. (Security Affairs)

New Whirlpool backdoor used in Barracuda ESG campaign. CISA has released a new advisory detailing the malware, dubbed "Whirlpool." It claimed the backdoor established a TLS reverse shell to a command-and-control (C2) server. (Infosecurity Magazine)

Researchers discover new sophisticated info-stealing malware called Statc Stealer. Researchers observed that Statc Stealer can steal user's cookies data, web data, local state, data preferences, login data, various wallet information, FileZilla, browser auto-fills, AnyDesk, ronin_edge, MetaMask, and Telegram data. (Security Affairs)

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

Hardware & System Vulnerabilities (multiple)

- Adobe, Amazon, Atlassian, Cisco, Clam Antivirus, CrushFTP, Debian, Dell, F5, GNU, Google, HP, HPE, IBM, Intel, Lenovo, Linux, Microsoft, Mozilla, Oracle, Red Hat, Samsung, SUSE, Ubuntu, Xerox, and z/OS.

Themed Phishing Campaigns

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

Subject Keywords: Direct Cell#, DocuSign, Excel Documents, Mortgage, MFA, My Direct Deposit Modification, New Order, Okta, Pending Review, Proof of Payment, Shared RFP Invitation, RFP_#SSW567-BID Shipment, Notification, USPS, and Voice Mail.

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

Cl0p vengeance and EvilProxy highlight this week's risks

Cl0p Threatens Companies That Did Not Pay

Summary

There are currently 260 companies listed on Cl0p's data leak site with hundreds more affected by third- and fourth-party vendors. As a result of the attack on the MOVEit transfer service, it is estimated that the ransomware group has stolen data including personal details for at least 41 million individuals. The number of individuals is expected to rise as many organizations are still assessing the impact. Financial institutions are included in the list of top 10 organizations with the most victims. In some cases, Cl0p created dedicated websites for hosting the stolen data on the clear web. However, the cleared sites are easy for law enforcement to take down, and Cl0p recently changed tactics. To avoid law enforcement and takedowns, this week Cl0p began using torrents on the dark web to distribute stolen data. The ransomware group set up a new Tor site with instructions on how to use torrent clients to download the data. Torrents use peer-to-peer transfer among different users, and the transfer speeds are much faster. This distribution method is more efficient and much harder for law enforcement to take down. Companies that had torrents created include victims in the financial service industry, although not every company has had these sites created. Also, this week, Cl0p posted an update saying that any company that had refused to negotiate had until 15 August contact them and discuss payment otherwise the companies' stolen data would be leaked. On the eve of 15 August Cl0p posted additional torrents but nothing since. FS-ISAC continues monitoring the situation.

EvilProxy Phishing Attack Surges in Last Five Months

Summary

Cyware reports the EvilProxy phishing service continues to gain popularity as a tool for targeting Microsoft 365 accounts that are protected by Multi-Factor Authentication (MFA). Research conducted by Proofpoint reveals a significant increase in successful cloud account takeovers in the past five months, particularly impacting high-ranking executives. According to Proofpoint, the campaign supported by EvilProxy utilizes brand impersonation, bot detection evasion, and open redirections. The brands impersonated in the campaign include Adobe, DocuSign, and Concur.

If victims click on the embedded links in the phishing emails, they are redirected to various websites before landing on an EvilProxy phishing page that mimics the Microsoft 365 login page. Once a Microsoft 365 account is compromised, the threat actors add their own MFA method (via Authenticator App with Notification and Code) to establish persistence. The attackers used encoding techniques and hacked legitimate websites to hide user email addresses and create tailor-made phishing pages. Over a hundred organizations were targeted with 120,000 phishing emails to steal Microsoft 365 accounts. The attack impacted the accounts of 39% of C-level executives, 9% of CEOs, 17% of chief financial officers, and employees with access to financial assets or sensitive information.

Reverse proxy tools like EvilProxy remain potent threats in today's dynamic threat landscape. The significant rise in such phishing kits exposes crucial gaps in organizations' defense strategies. As these attacks are launched via emails, organizations must enhance their email and web security to defend against advanced hybrid threats.

The Clock is Ticking Towards Credit Union Cyber-Incident Reporting Rule

On 27 September 2023, the new reporting rule goes into effect

Summary

Credit unions are anticipating the 27 September effective date for the Cyber-Incident Reporting rule, but many CUs question what incident type requires reporting. The proposed rule defined a reportable cyber incident as any substantial cyber incident that leads to one or more of the following: a substantial loss of confidentiality, integrity, or availability of a network or member information system that results from the unauthorized access to or exposure of sensitive data, disrupts vital member services, or has a serious impact on the safety and resiliency of operational systems and processes; a disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities; and/or a disruption of business operations or unauthorized access to sensitive data facilitated through or caused by, a compromise of a credit union. Below is a list of reportable incidents.

- Ransomware attacks impacting critical systems or data.
- Unauthorized access to an information system containing a substantial amount of sensitive member information.
- Data breach exposing a substantial amount of employee personally identifiable information.
- Distributed denial of service attack causing significant downtime.
- Phishing attacks result in the successful installation of malware.
- Theft or loss of unencrypted device(s) containing sensitive information.
- Compromise of online banking platform or mobile application.
- A computer hacking incident disrupted a federally insured credit union's operation.
- A detected, unauthorized intrusion into a network information system.
- Discovery or identification of zero-day vulnerability in a network or information system.
- Internal breach or data theft by an insider.
- Sensitive data exfiltrated outside of the federally insured credit union or a contracted third party in an unauthorized manner, such as through a flash drive or online storage account.
- Member information was compromised because of card skimming

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.

- Social engineering attack leading to fraudulent wire transfers.
- Unauthorized alteration or destruction of financial data.
- Third-party notification to a federally insured credit union that the third party has experienced a breach of a credit union's sensitive member information.

at a credit union's ATM.

- Misconfiguration of information system(s), such as application programming interfaces, databases, and storage accounts, exposing a substantial amount of sensitive member information.

Just For Community Institutions

New York State Unveils New Cybersecurity Strategy

Please remember to patch routinely exploited vulnerabilities

Summary

On 11 August, Governor Kathy Hochul announced New York's first-ever statewide cybersecurity strategy; the goal of which is to protect the State's digital infrastructure from evolving cyber threats.

This strategy unifies New York State's cybersecurity services, functions, and operations to better protect our critical infrastructure, personal information, and digital assets from malicious actors. It also provides a framework for aligning the actions and resources of both public and private New York stakeholders so that we can collectively work toward a shared vision for protecting New York. Key among those stakeholders is county and local governments, which are often the primary interface between New York's residents and many government services. The strategy is organized into the following sections:

1. A Convergence of Cyber Threats
2. New York's Approach: Unification, Resilience, and Preparedness
3. Critical Stakeholders
4. Strategic Pillars: Operate, Collaborate, Regulate, Communicate, and Grow

The aggressive program will focus on upgrading networks, providing free cybersecurity tools, and considering new regulations. It also includes calls for the state to work with county governments and federal agencies on cybercrime investigations and information sharing.

Additional Member Benefits That May Be Available to You



FS-ISAC produces a daily phishing report. We do!

The Daily Phishing and Spearphishing Report provides a consolidated list of TLP Amber, Green, and White information.

Members must log into the IntelX platform to download the attached Excel spreadsheet indicated by the red circle.

In the search bar, add the alert name to obtain the report. (e.g., Alert ID a85b7228)

If already logged in, simply click the VIEW ALERT hyperlink near the bottom of the report to go directly there. If you need assistance, please contact Member Services by opening a Case in the Member Services app.



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 from your institution 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.