FS-ISAC

Community Institution & Associations Risk Summary Report

Week of 31 July | 2023 Edition | Vol. 189

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).

CoinsPaid Blames North Korea-Linked APT Lazarus for theft of $37M worth of Cryptocurrency. "On July 22nd, CoinsPaid experienced a hacker attack, resulting in the theft of USD 37.3M," reads the announcement published by the company. "We believe Lazarus expected the attack on CoinsPaid to be much more successful." (Security Affairs)

Fruity Trojan relies on deceptive software installers to spread Remcos RAT. Threat actors are creating fake websites hosting trojanized software installers to trick unsuspecting users into downloading a downloader malware called Fruity to install a remote trojan tool like Remcos RAT. (The Hacker News)

More malicious npm packages found in wake of JumpCloud supply chain hack. Two weeks after the IT management firm JumpCloud announced that it was the victim of a supply chain attack aimed at a small population of customers in the cryptocurrency industry, an investigation by ReversingLabs researchers has uncovered evidence of more malicious npm packages, with links to the same infrastructure that also appear to target cryptocurrency providers. (Reversing Labs)

Dark Power ransomware abusing vulnerable dynamic-link libraries in resolved API flow. The Dark Power ransomware exploits vulnerabilities in kernel-related APIs to quickly propagate through the cyber-kill chain. It also leverages DLLs such as kernel32.dll, bcrypt.dll, and ole32.dll to carry out its malicious activities. (Heimdal)

Exploitation of recent Citrix ShareFile RCE vulnerability begins. The vulnerability, tracked as CVE-2023-24489 (CVSS score of 9.1), was the result of errors leading to unauthenticated file upload, which could then be exploited to obtain RCE, says security firm Assetnote, which identified and reported the bug. (Security Week)

New high-severity Ivanti bug reported, second in a week. Days after it emerged threat actors exploited an EPMM software flaw to attack a dozen Norwegian government ministries, a new vulnerability has been identified in the same mobile device management solution. (SC Media)

Spynote Android spyware strikes financial institutions through smishing campaigns. The infection chain typically begins with a deceptive SMS message urging users to install a "new certified banking app," followed by a redirect to a seemingly authentic TeamViewer app, which is used for technical remote support. (Infosecurity Magazine)

Web Browsing is the primary entry vector for ransomware infections. Attackers have been spotted rotating different URLs/hostnames (75.5%) to host the same ransomware or using the same URL to deliver different ransomware. Some attackers do both things. Ransomware gangs are also fond of using popular public hosting, social media, and media-sharing services, as well as long-lived benign domains they've managed to compromise, for ransomware delivery. FS-ISAC members have daily access to a brand infringement report which can alert members to brand assault. (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.
- DarkGate Malware
- FLATDIRT (aka RedFlag aka Cur1Agent)
- Formbook
- GRANDOREIRO
- IceID
- JsOutProx RAT
- Lokibot
- Mirai
- NetWire RAT
- Qbot/QakBot
- Redline
- Remcos (GuLoader)
- SOCGHOLISH
- TrueBot
- Xloader
- XWorm (churchxx, freshinxworm)

Hardware & System Vulnerabilities (multiple)

- Apache, Apple, BMC Brocade, Control, Cisco, Cygwin, Debian, Dell, F5, Google, Hitachi, IBM, Ivanti, Lenovo, libarchive, Microsoft, Mozilla, Nessus, Oracle, Red Hat, SUSE, Ubuntu, and. Vmware.

Themed Phishing Campaigns

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

Subject Keywords: AWB Ref#, Invoice Files, Payment Advice, Payment Done, Project Plan, Proposal, Request for Quotation (Quote), and Zelle.

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.

Threats of the Week

Abyss Locker and DarkGate malware highlight this week’s risks

VMware ESXi Servers Face New Threat from Abyss Locker

Summary

Cyware reports, MalwareHunterTeam recently uncovered a new variant of Abyss Locker ransomware specifically designed to target Linux-based VMware ESXi servers. This variant is a part of the larger Abyss ransomware family, which has been active since 2019, targeting various platforms and systems. The Linux version of Abyss Locker utilizes sophisticated attack techniques to gain unauthorized access to VMware ESXi servers. It leverages SSH brute force attacks to exploit weak or compromised credentials to enter the system. Once the ransomware gains access to the VMware ESXi server, it proceeds to encrypt virtual machines, rendering them inaccessible and unusable. Post-encryption, the threat actors drop ransom notes demanding payment in cryptocurrency, typically Bitcoin, for the decryption key. The recent version of Abyss Locker is part of an ongoing trend of ransomware targeting Linux-based systems, once deemed less susceptible to such attacks. The ransomware actors claim to have pilfered data ranging from 35GB to 700GB from different companies. Researchers believe that the Abyss Locker Linux encryptor has some overlaps with the HelloKitty ransomware. According to Michael Gillespie of Bleeping Computer, the Abyss Locker Linux encryptor seems to be derived from HelloKitty, although the former uses ChaCha encryption. HelloKitty uses a combination of AES-256 and RSA-2048 or even NTRU+AES-128. It remains unclear whether the Abyss Locker variant is a rebranding of the HelloKitty operation or if another ransomware group obtained access to the encryptor's source code. The discovery of the Linux variant of Abyss Locker underscores the evolving nature of ransomware attacks. Moreover, the operators behind Abyss Locker are highly skilled and have a history of launching targeted attacks against high-value assets.

Remediation

System administrators for community institutions using VMware ESXi servers should review their security measures and implement best practices for securing SSH access and credentials. Members can access a TLP Green Technical Advisory Report in IntelX Share app.

DarkGate Malware Reemergence

Summary

FS-ISAC members report the recent reemergence of DarkGate malware. Originally reported in November 2018, DarkGate was described as a sophisticated malware that has both ransomware and cryptomining components. The malware also uses several advanced anti-analysis techniques, such as using vendor-specific checks, to evade detection. For additional information on recent activity, please visit the IntelX Alert f9037b43.

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."

SEC Ruling on Disclosure of Cybersecurity Incidents

Summary

The US Securities and Exchange Commission (SEC) approved new rules that require publicly traded companies to publicize details of a cyber-attack within four days of identifying that it has a "material" impact on their finances. Officials said the measure would help investors and the public understand who to trust with their money and their data. This ruling comes as the cost of cyber incidents in publicly traded companies continues to mount and the frequency of major hacking incidents continues to grow.

This marks a major shift in how computer breaches are currently disclosed.

The new rules mandate that companies report the incident's nature, scope, timing, and impact. The disclosures can be delayed for up to 60 days if the US Attorney General determines that the details would cause national security or public safety implications and the Commission is informed in writing of the risk. Companies are further required to disclose material information on their cyber security risk management strategy and governance. The SEC ruling describes that something is material if it is something the investor wants to know. The SEC further clarified writing, “Doubts as the critical nature of the relevant information should be resolved in favor of those the statute is designed to protect, namely investors.”

The rule is set to take effect 30 days after it is published in the Federal Register. The ruling also puts the responsibility on a company's board of directors and will also require registrants to describe the board’s oversight of risks from cybersecurity threats and management’s role and expertise in assessing and managing material risks from cybersecurity threats.

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.

TLP GREEN

Just For Community Institutions

Prepare Now: Cybersecurity Awareness Month

Helping customers, help you

Summary

October is not that far away – so, it is time to think about and participate in Cybersecurity Awareness Month, October 2023, and we know many of you are always looking for ways to engage with your customer/members.

October 2023 marks the 20th Cybersecurity Awareness Month, and CISA needs your help to amplify messaging throughout the month and year-round. This year will focus on four key behaviors everyone can take to reduce cyber risk:

1. Turning on MFA
2. Using strong passwords and a password manager
3. Updating software regularly
4. Recognizing and reporting phishing

Join CISA and the National Cybersecurity Alliance for a webinar on 9 August from 2-3:00 PM ET to learn how you and your organization can get involved. To register, click here.

Additional Member Benefits That May Be Available to You

DID YOU KNOW?

To meet the needs of our members, we have several Communities of Interest or COIs that serve various industries within the Financial Service Sector.

Each COI is led by knowledgeable subject matter experts from that industry. Many of these directors were members of the industry and bring their experience to assist you in making the most out of your FS-ISAC membership.

Because everyone processes information differently, we provide members with several products and services to help facilitate this. Common features of the COIs include:

- Monthly meetings
- Connect channels and mail lists
- Report newsletters
- Surveys and their results

Additionally, these directors are on various communication channels to provide their knowledge on a subject and share their recommendations.

Over the next few issues, we will provide additional information on each group. This information is also available in your Membership Guide in Share.

Americas Threat Intelligence Committee. (TIC) The Threat Intelligence Committee's goal is to facilitate the FS-ISAC's information-sharing mission through the planning, coordination, collection, processing, and dissemination of cyber threat intelligence for the financial services sector. This committee is open for Tiers 4-1.

Americas Business Resiliency Committee. (BRC) The BRC community enables business continuity and crisis response information sharing to communicate sector-level impact and needs during a crisis event. Through the All-Hazards Crisis Response Coordination Playbook, the BRC plans and exercises for the operational resilience of financial sector critical functions and technologies. The BRC is instrumental in assisting and coordinating information during cyber and physical events disrupting the financial sector or critical supply chains. This committee is open for Tiers 4-1.

Brand Protection Working Group. The Brand Protection Working Group discusses topics related to brand monitoring and domain infringement through regular monthly meetings.

Business Security Executives Forum. (BSEF) The BSEF is a trusted community of Business Information Security Officers (BISOs) and Deputy Chief Information Security Officers (CISOs) sharing best practices and intelligence regarding their roles and responsibilities. The BSEF is open to all tiers who are interested in discussing the topic of implementing a BISO program. Participants must have the title of Business Information Security Officer or equivalent.

Clearing House and Exchange Forum. (CHEF) The CHEF brings clearing houses and exchanges together to aggregate shared data and develop trusted information-sharing platforms for peer firms to reduce the risk of successful attacks. This group is open to all Tiers; however, participation is open to exchanges or clearinghouses and additional criteria are defined in the Membership Guide.

Compliance and Audit Council. (CAC) The CAC shares information on industry best practices, discusses the latest regulatory developments, and works to find out how peer organizations are handling the latest compliance, audit, legal and control issues. This group is available to all Tiers

Community Institution and Associations Council. (CIAC) The CIAC is the single largest community within the FS-ISAC, providing credit unions and commercial banks (within the CIAC, CBs make up 80% and CUs make up 20%) under $20B in assets. Peer CIs and associations working together identify new and current security threats, risks, and develop action strategies, industry best practices and working groups to mitigate these changing risks.

Insurance Risk Council. (IRC) The IRC addresses topics, challenges, and opportunities specific to the insurance sector and pertaining to various operational risk issues including information security, resiliency, regulatory, fraud, physical security, and privacy. The IRC aids in strengthening information sharing across the insurance sector as well as preventing, detecting, responding, and recovering from the myriad of threats faced by insurance companies each and every day. Members must have an insurance line of business.

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.