FS-ISAC

Securities Industry Risk Group (SIRG) Newsletter

Week of 5 June 2023

Follow Us

TLP: 🟩

Global Cyber Threat Level: 🟩

AMERICAS: 🟩 EMEA: 🟩 APAC: 🟩

Contents

Upcoming Events

FS-ISAC Events - *NEW

APAC Summit
11-12 July 2023 | Singapore

FinCyber Today Summit
1-4 October 2023 | Orlando, FL

EMEA Summit
6-8 November 2023 | Amsterdam, NL

Cyber Range Exercises

Join Us on 22 June: Enabling and Securing Generative AI and ChatGPT

Our next SIRG meeting will be on 22 June at 11am EDT when we will have EY joining us to discuss the topic of *Enabling and Securing Generative AI and ChatGPT*. The invitation for the meeting has been distributed on the SIRG listserv, but please reach out to Michael Petrik if you have not received it.

SpinOK Spyware Infects Over 400 Million Android Devices

A recently discovered spyware labeled "SpinOK" by **researchers at Dr. Web** has been found embedded in over 101 Android apps, some of which are available on Google Play, and which have over 400 million downloads. SpinOK presents itself as an advertisement SDK which promises daily rewards through mini-games. Behind the scenes, the trojan SDK verifies sensor data of the Android device to ensure it is not in a controlled environment for monitoring potentially harmful apps. Then it has the ability to list files within directories, search for specific files, upload files from the device, or manipulate the contents of the clipboard by copying and replacing them. Additionally, it can steal account passwords, credit card information, or direct cryptocurrency payments to the threat actor's crypto wallet addresses.

FS-ISAC Board of Directors Elections Results

FS-ISAC is pleased to share the results of the 2023 Board of Directors election. The election broke participation records both in terms of applicants to the Nominating and Governance Committee as well as members who voted, illustrating our membership's strong engagement and interest in the future direction of FS-ISAC. FS-ISAC expresses our deep gratitude to all those who applied to be part of the board, our final slate of nominees who ran but did not win, and all who voted. We also extend our deep thanks to SIRG members **Meg Anderson** of Principal, who is exiting the board after the maximum two three-year terms, as well as **Gary Owen** of iCapital Network, for their years of service and contributions to our community.

Intelligence Exchange Refresher Sessions for New and Existing Members

[28 JUN](#)
[26 JUL](#)
[30 AUG](#)
[27 SEP](#)
[25 OCT](#)
[29 NOV](#)
[27 DEC](#)

Resources

FS-ISAC Intelligence Exchange (View)

SIRG PODCASTS (Listen)

SIRG CONNECT - Secure CHAT Channels:

Alternative Investor Council (AIC)

Asset Managers Council (AMC)

Broker-Dealer Council (BDC)

EMEA SIRG Channel (EMEA-SIRG)

Futures Commissions Merchants Council (FCMC)

Retirement Industry Council (RIC)

SIRG TAGS on SHARE

Product:SIRG Newsletter
Product:SIRG Podcast
Product:SIRG Surveys

Breach Found on Platform Used by SEC

A post on a dark web blog revealed that there has been a **breach in the legal technology platform** called Casepoint which is used by the United States Courts, the Security and Exchange (SEC) and the United States Department of Defense (DOD). Russian linked ransomware cartel **ALPHV/BlackCat** posted on their dark web blog that 2TB of sensitive data was stolen from the company. The post indicates that the thieves took company data, attorney files and other information. The blog post contains several screenshots of the alleged stolen data**,** including legal agreements and government IDs. Casepoint is used by legal departments, law firms and public agencies to organize and navigate data. Users upload to Casepoint's system where the input process is streamlined. ALPHV/BlackCat seems to be focused on professional service providers and claims to have breached the **Mazars Group**, an international audit, accounting and consulting firm.

2023 CAPS Registration is Open

The registration for the 2023 CAPS exercise for securities and investments 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 securities 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 securities and investment firm. 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.

Unmaintained SalesForce Sites Vulnerable to Threat Actors

SalesForce sites which are improperly deactivated and unmaintained are vulnerable to threat actors, according to research by **Varonis Threat Labs**. With SalesForce sites, you can create customized communities that allow partners and customers to interact with your SalesForce environment. When these sites are no longer needed, they can be left unmaintained, open to new vulnerabilities, and fail to receive updated security measures. The company may change the DNS record of the site domain, but will not remove the custom SalesForce domain or deactivate the site, allowing it to remain active and continue to pull information.

In these circumstances, threat actors can exploit these sites by changing the host header to trick SalesForce into thinking the site was accessed at the appropriate URL. The threat actors may not know the full internal URL, but they use tools that index and archive DNS records to identify these sites. These "Ghost Sites", as labeled by Varonis Threat Labs, have been found to host confidential data, such as PII and sensitive business data. The data is not limited to old records, and new records may be included if the sharing configuration settings in the SalesForce environment allows access for the guest user. The simple fix is to ensure any unused SalesForce Sites are deactivated and to track user permissions on these sites.

EMEA Summit Call for Presentations Closes 9 June

The Call for Presentations for the EMEA Summit will close on June 9. This is a great opportunity to share your best practices with the FS-ISAC community. **Submit your presentation here** to be considered for the EMEA Summit which will be held in Amsterdam from the 6 – 8 November.

Sphynx Ransomware Improved to Evade Detection

The threat actors behind the BlackCat ransomware have developed a new version, labeled ***Sphynx***, with an emphasis on speed and stealth to evade detection methods. *Sphynx* uses junk code, encrypted scripts, and will re-work the command line arguments passed to the binary. Additionally, it incorporates a loader to decrypt the ransomware payload which performs network discovery activities to search for additional systems, delete volume shadow copies, encrypt files, and leave the ransom note.