FS-ISAC Financial Services Information Sharing and Analysis Center

Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – December 2019

FS-ISAC on Cybersecurity Awareness

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

The information provided in this monthly newsletter highlights cybersecurity topics and emerging threats to the securities industry globally. It is intended to increase the cybersecurity awareness of an organization's end-users and to help them interact in a more secure manner.

This newsletter is not intended to replace the benefits of joining FS-ISAC's member-based organization and readers from organizations who are not already members are encouraged to (join) FS-ISAC.

For Our Birthday, #daretoshare

Over the last two decades, we've made cybersecurity intelligence sharing in financial services a global priority, growing our peer-to-peer network of trust to nearly 7000 member institutions around the world.

As we look to the next 20 years, we're doubling down on sharing, and calling on our community to do the same. On our 20th anniversary page, hear from our CEO on where FS-ISAC is focusing its efforts, and find resources for you to get involved and enlist your network to **#daretoshare**.

FS-ISAC releases new All-Hazards Framework and updated US Playbook Appendix

The ***TLP White*** *FS-ISAC All-Hazards Framework ("Framework")* outlines the key elements of trusted information sharing to evaluate and respond to physical and cyber crises. The Framework may be used to develop country, sector and event specific crisis information sharing Playbooks. The Framework is used to: identify sharing activities during exercises, develop Playbook appendices and identify sharing sources during a crisis event, and is **available to all financial institutions**. The updated ***TLP Green*** *US Playbook Appendix***,** provides US-based FS-ISAC members, their partners and critical infrastructure stakeholders a guide to evaluate, escalate, and communicate information and actions pertaining to disruptive cyber and physical threats and events. Obtain your free copy of the Framework here. Members of FS-ISAC should see Tracking ID: 951678 to obtain a copy of the Appendix.

Institutional Investors Targeted by Hackers

Two endowments and a hedge fund were hit by cyberattacks in late September and late October, respectfully, that has experts warning institutional investors to be on the lookout. Fraudulent emails were sent with the hopes of recipients clicking on a "Continue to email" link which could infect a recipient's computer with malware or allow the hackers entry into that target's account. While it does not appear the attackers were successful, the article highlights the dangers of high-profile executives' accounts getting hacked. Firms are reminded to continually to educate employees, ensure testing of systems is an ongoing process and have a response plan in place should an incident occur.

New York Enacts SHIELD Act

On 23 October 2019, the state of New York's 'Stop Hacks and Improve Electronic Data' Security Act' (SHIELD Act) went into effect. The **SHIELD Act** amends the state's current data breach notifications laws, imposing more expansive heightened data security and data breach notification requirements on companies, ensuring better protection for New York residents from data breaches of their private information. The act defines the boundaries, requirements, and consequences for companies of those failing under jurisdiction. Any company without security systems and practices will be forced to adopt and secure infrastructure in its entirety, and companies with a security system will now need to practice better testing and evaluation tools.

The SHIELD act explains what counts as a data breach and will include the ability to view data without being able to download or steal copies. The SHIELD act also refers to recent events such as the Equifax data breach. Some facts on SHIELD are:

- The deadline for data protection programs is March 21, 2020, but data breaches must be recorded starting October 23, 2019.
- This Act adds to the existing New York's data breach law.
- The SHIELD Act expands data elements to include not only social security number and driver's licenses, but to biometric information, bank account numbers, and payment information

FS-ISAC and Europol Announce Partnership

As part of our continued global expansion, FS-ISAC has teamed up with Europol to foster a pan-European approach to intelligence sharing, ensuring the cross-border cooperation necessary for the detection, prevention and reduction of cybercrime. In addition to facilitating information sharing, the agreement will also enable education and resilience through training exercises and informational summits (**Read More**).

New Medusalocker Ransomware

Researchers have discovered and continue to analyze a new ransomware that is being distributed labeled '**Medusalocker**'. The malware targets a few dozen running executables, including those belonging to G Data, Qihoo 360 and Symantec security products. The method of how this ransomware is distributed is still unknown. What has been reports is the ransomware performs the following activities:

- It first creates a Registry value 'EnableLinkedConnections' under a certain path and sets it to '1' to access mapped drives in UAC launched processes.
- Then, it has been observed to restart the LanmanWorkstation service to ensure that Windows networking is running. This also verifies that mapped network drives are accessible by the ransomware.
- Processes including DefWatch, wrapper, and tomcat6, among others, are terminated to shut down security programs. This enables all data files to be accessible for encrypting.
- As the final step, it clears Shadow Volume Copies of files, like most ransomware. This is to make sure that the files cannot be restored.
- Now, it scans files and ignores those with certain extensions such as .exe or .rdp. It also ignores files present in certain folders.
- All other files will be encrypted using AES encryption.

A ransom note called 'HOW_TO_RECOVER_DATA.html' is left in each file folder that it has encrypted on the victim's infected machine that contains an email address for instructions about payment.

FS-IAC and Independent Community Banker Association Educate CEOs on Business Email Compromise Threats

As part of National Cybersecurity Awareness Month, FS-ISAC and Independent Community Bankers of America collaborated on a webinar for community bank CEOs on Business Email Compromise (BEC) on October 15. The 60-minute presentation focused on how email-based scams target business customers impact banks and their communities, how to detect scams, coordination with law enforcement, legal risks, and actions banks can take to better protect banks and customers. FS-ISAC collaborated on a 7 page paper "Tips on Safeguarding Your Bank and Customers from Business Email Compromise" and a one page quick guide developed by ICBA, FS-ISAC, Federal Bureau of Investigation, and US Secret Service which are available by contacting FS-ISAC Member Services (admin@fsisac.com).

About FS-ISAC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is an industry consortium dedicated to reducing cyber-risk in the global financial system. 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 cyberthreats. FS-ISAC has nearly 7,000-member firms with users in more than 70 countries. Headquartered in USA, the organization has offices in the UK and Singapore. To learn more, visit www.fsisac.com. This newsletter is not intended to replace the benefits of joining FS-ISAC's member-based organization. Please consider joining if you're not already a member.

Thank you,

FS-ISAC SIRG Team

If you have any questions about this week's report, please contact the FS-ISAC SIRG.

This newsletter contains content developed by FS-ISAC as well as links to content developed by third-parties.

FS-ISAC makes no claims or warranties as to the accuracy of information provided by third-parties. All copyrights remain with their respective owners.

Financial Services Information Sharing and Analysis Center

fsisac.com