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.

FBI Alert: Ransomware on the Rise

Last week, the FBI released a new **public service announcement** regarding the ongoing ransomware epidemic, emphasizing that attacks are becoming more targeted since early 2018, with losses increasing significantly over time. The new PSA also lists common infection vectors; email phishing campaigns, Remote Desktop Protocol vulnerabilities and software vulnerabilities. The FBI is encouraging ransomware victims to report incidents to law enforcement, and suggests companies defend themselves by following best practices, including backing up data, emphasizing awareness and training, regularly patching, automatically updating AV and anti-malware solutions, disabling macros scripts and more. (FBI)

FS-ISAC and Europol Partner to Combat Cross-Border Cybercrime

On 19 September, FS-ISAC and Europol's European Cybercrime Centre (EC3) **announced** a partnership to combat cybercrime in the European financial services sector. FS-ISAC and EC3 signed a Memorandum of Understanding (MOU) that will facilitate and enhance the law enforcement response to financially motivated cybercriminals targeting financial institutions through a symbiotic intelligence sharing network. In response to the rise of sophisticated cyber-attacks impacting numerous countries at once in recent years, the partnership will help foster a pan-European approach to intelligence sharing to ensure cross-border cooperation for better detection, prevention and reduction of cybercrime. "Cybercriminals are increasingly targeting financial services and institutions to the cost of citizens and businesses across the EU" said Steven Wilson, head of EC3. "It is crucial to bring key stakeholders around the table to improve the coordinated response; this MOU with FS-ISAC builds a platform to allow us to do exactly that."

International Monetary Fund (IMF) Releases Paper on "Cybersecurity Risk Supervision"

The International Monetary Fund (IMF) recently released a paper on 'Cybersecurity Risk Supervision". The 55 page paper highlights the emerging supervisory practices that contribute to effective cybersecurity risk supervision, with an emphasis on how these practices can be adopted by those agencies that are at an early stage of developing a supervisory approach to strengthen cyber resilience. It discusses cyber risks facing financial institutions and actions that financial

supervisors should take to address cyber and resiliency risks. The paper discusses the importance of cybersecurity risk management practices at financial institutions, security testing exercises, and strong information sharing practices.

New Medusalocker Ransomware

Researchers have discovered and continue to analyze a new ransomware that is being distributed labeled '**Medusalocker**'. 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.

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.

Financial Services Information Sharing and Analysis Center

fsisac.com

Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – November 2019