FS-ISAC Securities Industry Risk Group Global Cybersecurity Brief | **March 2019 TLP: WHITE**

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 Securities Industry and Financial Markets Association (SIFMA), the Investment Industry Association of Canada (IIAC) and the International Council of Securities Associations (ICSA).

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.

FINRA Releases 2019 Regulatory Priorities Letter

On January 22, the Financial Industry Regulatory Authority, Inc. (FINRA) released its ***Annual Risk Monitoring and Examination Priorities Letter*** highlighting regulatory program points of emphasis for the coming year. "Risk Monitoring," is the process by which self-regulatory organizations initially identifies problem areas through surveillance, firm reporting, surveys, questionnaires and examination findings. The letter also mentions that FINRA will monitor firms' use of technological tools to catch any risks arising from supervision and governance systems, third-party vendor management, safeguarding customer data and cybersecurity.

Firms should use this letter and ***FINRA's 2018 examinations findings report*** to review compliance and supervisory procedures carefully and make any revisions.

New Council Serving the Futures Industry

FS-ISAC created the Futures Commission Merchants Council (FCMC) to better serve the futures industry. A subset of the Securities Industry Risk Group (SIRG), the FCMC will strengthen critical economic infrastructure by enabling dialog among FS-ISAC members in the alternative investment industry. Email **SIRG@fsisac.com** to learn more.

The mission of FCMC is to strengthen critical economic infrastructure by enabling dialog among FS-ISAC members in the alternative investment industry for Information Security and business resiliency leadership. Objectives include promoting rapid useful information sharing among participants, establishing rapport that reduces response time and hesitation to share during times of crisis, and serving as a unified platform to voice or receive dialog with external parties including intelligence sources, regulators, government, customers, vendors, and other sectors.

Hackers Use Google App Engine in Recent Attacks

Researchers at Netskope have reported that the hacking group 'Cobalt' has been using the Google App Engine for the delivery of malware through decoy PDF documents (***Security Week***). Since 2016, the Russia-based threat is known for attacks against financial institutions.

In recent assaults, the hackers use these decoy PDF files to point the victims to the malicious payload and uses the Google App Engine in an attempt to trick the victim into believing they are accessing a legitimate file from a trusted source. The attacker sends the malicious file to the victim via email messages using Adobe Acrobat 19. Once the malicious URL is accessed, the user is logged out of the *appengine.google.com*, an error is displayed and mentions the google site, which the user is then likely to allow and connect, thus redirecting the user to the malicious site.

The payload downloads a Microsoft Word document with an obfuscated macro code, which prompts the user to enable editing content. Once this happens, the macro is executed, and another stage payload is downloaded. Researchers state the recent attacks targeted more than 20 other banking, government and financial institutions globally.

Firms are advised to update their malware detection software, make employees aware of this attack and report back to IT staff immediately of any incident.

Letter Asks GAO to Examine Cybersecurity of Retirement Systems and Highlights the RIC

Sen. Patty Murray (WA) (ranking member of the Senate Committee on Health, Education, Labor and Pensions) and Rep. Bobby Scott (VA) (Chairman of House Committee on Education and Labor) sent a letter to Gene Dodaro, Comptroller General of the US Government Accountability Office (GAO), requesting that the GAO examine the cybersecurity of the retirement system (***Plan Sponsor***). The letter requests GAO to respond to 10 questions in response to increasing cyber risks and the growth in retirement savings. (***GAO Letter***). The letter mentions the FS-ISAC Retirement Industry Council (RIC) and the efforts by the council to disseminate actionable physical and cyber information for members in the retirement industry.

FS-ISAC Cyber-Range Ransomware Exercises

Cyber-range exercises offer FS-ISAC members a more technical, hands-on keyboard experience that provides greater interaction and sharing between members in a way that helps raise capability, maturity levels and resiliency across the sector. FS-ISAC has partnered with ManTech to build a network environment and facilitate

the event. For example, FS-ISAC conducted its second European cyber-range exercise in Zurich on March 1. The cyber-range exercise simulated a ransomware attack leveraging artificial intelligence. FS-ISAC partnered with UBS for an exercise that convened CISOs, CIOs, heads of security and security analysts from 14 leading financial services and trade associations from across Europe to take part in a WannaCry-style attack on a simulated bank network.

Upcoming Cyber-Range Exercises

- March19, 2018 | Federal Reserve Bank of Atlanta | **Register**
- April 2, 2018 | Federal Reserve Bank of Cleveland | **Register**
- July 25, 2018 | Federal Reserve Bank of Chicago | **Register**
- August 22, 2018 | Federal Reserve Bank of St. Louis, MO | **Register**

See ***FS-ISAC Exercises*** for additional details.

About the FS-ISAC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) helps assure the resilience and continuity of the global financial services infrastructure through sharing threat and vulnerability information; conducting coordinated contingency planning exercises; managing rapid response communications; conducting education and training programs; and fostering collaborations with and among other key sectors and government agencies. 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 report, please contact the **FS-ISAC**.

Financial Services Information Sharing Analysis Center **www.fsisac.com**