Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – August 2020

SEC Issues Warning on Ransomware

Last month the Securities and Exchange Commission warned advisers and broker dealers about **a rise in phishing and ransomware attacks**. The commission's Office of Compliance Inspections and Examinations (OCIE) posted has observed an apparent increase in sophistication of ransomware attacks on SEC registrants, which include broker-dealers, investment advisers, and investment companies. The **risk alert** suggested that firms immediately review their cybersecurity controls, as well as other financial service market participants to monitor the cybersecurity alerts published by the Department of Homeland Security's Cyber Security and Infrastructure Agency (CISA), included an **updated alert** published on 30 June 2020 related to recent ransomware attacks. OCIE also encouraged registrants to share the updated CISA alert with their third-party service providers, particularly those that maintain client assets and records for registrants. Organizations are starting to bring their employees back into the office environment, raising questions on how to **securely transition** back to the 'next normal'. Devices that were not connected to a corporate network through a VPN may need to be validated prior to returning to the network. Targeted phishing campaigns could take advantage of a workforce that is in transition mode while returning to the office.

Cisco Small Business Switches Facing a High-Severity Flaw

Cisco recently warned that some of their small business switches are vulnerable to **high-severity flaws**, which could open the doors for remote, unauthenticated attackers to access the switches' management interfaces with administrative privileges. While some updates focus on fixing the flaws are available for some affected switches, those that have reached end of life (EOL) will not receive a patch. An attacker could manipulate a user's authentication for devices, obtain the user's privileges and ultimately take over the session account. The flaw (CVE-2020-3297) starts from the use of weak entropy generation for session identifier values.

Join our 2020 Virtual Summits

The Call for Presentations is now open for all events. Registration for events opens 28 July.

- Americas Fall Virtual Summit | 14-15 October | CFP closed | **Learn more**
- Europe Virtual Summit | 4-5 November | CFP closes 17 August | **Learn more**
- Asia Pacific Virtual Summit | 1-2 December | CFP closes 14 September | **Learn more**

FS-ISAC Intelligence Exchange

The FS-ISAC Intelligence Exchange is the new platform for members to utilize our services and collaborate with their fellow members. This will allow quicker, seamless access to all of FS-ISAC's capabilities, while also providing more control and customization of your engagement with FS-ISAC (**Learn more**).

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. Learn more at fsisac.com.