Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – July 2020

Returning to the Office Securely

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.

Fake Ransomware Decryptor Double Encrypts Victims Files

A fake decryptor advertised to stop and decrypt files that have fallen victim to the STOP Djvu Ransomware doesn't do as promised, but rather encrypts the affected files a second time **making the situation even worse** for the victim. With over 600 submissions a day to the **ID-Ransomware** ransomware identification service, the STOP Djvu ransomware is the most actively distributed ransomware over the past year. Software companies have previously released decryption tools for older versions of the STOP Djvu variants, but these have proven ineffective against the new instance. The ransomware mostly affects home users whose computers are infected through adware bundles or pretending to be software cracks. Many who are infected simply cannot afford to pay $500 for a ransom decryption tool

Ransomware Operators Lurk in Network Before Attack

When a company falls victim to a ransomware attack, the assumption is the attacker quickly deployed the ransomware and then leaves the system so not to get caught, although **apparently that is not the case**. Ransomware attacks are conducted over time, ranging from a one-day attack to a month-long campaign snooping around corporate networks before encrypting files and folders. These breaches are done through exposed remote desktop services and vulnerabilities. Once access is gained, the malicious actor will use tools to gather login credentials and connect into the network, gaining access to computers, servers, and files on the network to deploy the ransomware attack.

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.