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.

Chinese State-Sponsored Hackers Target Crypto Firms

A report from cybersecurity firm FireEye reports that a Chinese state sponsored hacker group is attacking several companies including crypto firms (Finance Magnates). The hacking group is called APT41and has been involved in breaching video game companies for financial gain. The report shows that the hacker group recently moved away from financially-motivated crime toward espionage, targeting industries aligned with China's five-year economic development plans (FireEye). In its report, FireEye provided detailed evidence that APT41 targeted companies by sending phishing emails. The group has been targeting companies across the globe, and in particular those located in France, India, Italy, Japan, the Netherlands, Singapore, Switzerland, the United Kingdom, the United States and Hong Kong. The cybersecurity company also found code snippets previously used to target a US-based gaming development company in 2016. Firms should review the FireEye report, update Antivirus and Intrusion protection software and follow any other recommendations provided in the report.

SEC Cyber Chief Leaving This Month

Last week, the US Securities and Exchange Commission (SE) announced that Robert Cohen, Chief of the SEC's Division of Enforcement's Cyber Unit will leave after 15 years at the Commission. Mr. Cohen joined the SEC Enforcement Division in 2004 and was promoted to this current role in 2015 (Finance Magnates). The Cyber Unit, which is part of the SEC's Enforcement Division, was created two years ago to restore investor confidence in the SEC following a data breach. At the time, the breach was serious enough for the regulator to notify members of Congress about the hack before it was announced publicly. The division was initially created to target market manipulation and cyber-related threats to trading platforms, but then its role evolved to investigate violations in digital assets.

Researchers are Puzzled with BlueKeep Exploit

In mid-May of this year, Microsoft issued an alert for a remotely exploitable software flaw. The CVE-2019-0708 vulnerability known as BlueKeep, allows attackers to connect to Remote Desktop Protocol services (RDP) and issue commands which could steal or modify data, install malware and conduct other malicious activities (CVE Details). The vulnerability has a similar worm-like spreading function which powered the WannaCry ransomware outbreak in 2017, and affects computers running Windows XP, Windows 7, Windows Server 2003 and 2008 (ZDNet). The software company and the National Security Agency (NSA) consider this vulnerability dangerous enough that customers have been advised repeatedly to apply the patches (NSA).

Even today, researchers are puzzled by the lack of attacks forecasted by security firms (DarkReading). Researchers believe the lack of a public exploit is one reason for the lack of attacks, as it is difficult to create an exploit from scratch. Researchers also believe that there are people with less technical experience that could create a worm for this exploit and others would utilize the vulnerability in a stealthier manner, making it harder to detect. In early July 2019, researchers at BitSight found more than 800,000 computers with signs of the vulnerability. Firms should patch their vulnerable systems as soon as possible.

Source Code for LokiBot Malware Hidden in Images

A new variant of the LokiBot Malware has been released with this version having the ability to hide its source code in image files on infected machines (ZD Net). Steganography is the technique used to hide messages or codes within various file formations such as. txt, .jpg, .rtf and some video formats. This practice can be implemented for legitimate purposes such as the protection of files on intellectual property and copyright purposes; however, attackers use this method to include triggers to hide source code and malware functionality. The developers of the malware realized the potential of using steganography for concealment of their malicious code. During a recent campaign, the variant has hidden encrypted binaries in .png files found within malicious files attached to phishing emails. If a malicious file in the email is opened, a script will install the Lokibot malware. If installed successfully, the malware can steal information, act as a keylogger and establish backdoors in infected systems.

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