FS-ISAC Securities Industry Risk Group Global Cybersecurity Brief | **May 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), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI) and the Insured Retirement Institute (IRI).

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 Issues Notice to Firms About Imposter Websites

The Financial Industry Regulatory Association (FINRA) recently published a notice to the firms it oversees about imposter websites (**FINRA Notice**). The notice states that several member firms have recently notified FINRA that they have been victims of imposter websites, which were designed to mimic a firm's actual website with the end goal of committing fraud. FINRA also outlines steps firms can take such as:

- Report the attack to local law enforcement, the nearest Federal Bureau of Investigation (FBI) field office or the Bureau's Internet Crime Complaint Center, and the relevant state's Attorney General.
- Run a "WHOis" search (www.whois.net) on the site to determine the hosting provider and domain name registrar associated with the imposter website (which may be the same organization in some instances).
- Submit an abuse report to the hosting provider or the domain registrar asking them to take down the imposter website.
- Seek the assistance of a cybersecurity specialist attorney or consultant.
- Notify the U.S. Securities and Exchange Commission (SEC), FINRA or other securities or financial regulators.
- Consider posting an alert on your website and sending email notifications to warn clients of the imposter website(s) and the associated URL(s).

The notice also mentions utilizing their FS-ISAC membership to share about the attack so they can provide mitigation advice. In July 2018, this topic was discussed on the quarterly SIRG call, notes and a replay of the presentation can be found under the SIRG folder on the FS-ISAC portal (**FS-ISAC Portal**).

Government Warns of VPN Security Software Flaws

The US Department of Homeland Security (DHS) issued a warning on April 12, 2019 for VPN software from Cisco, Palo Alto and F5 that it may improperly secure tokens and cookies and thus allow hackers an opening to invade and take control over a user's system (***Network World***). DHS's Cybersecurity and Infrastructure Agency (CISA) warning comes after a notice from Carnegie Mellon's CERT that multiple VPN applications store the authentication and session cookies insecurely in memory of log files. The ***CISA report*** states that if an attacker has persistent access to a VPN user's endpoint or exfiltrates the cookie using other methods, they can replay the session and bypass authentication methods, thereby having access to the same applications the users had through their VPN sessions. Manufacturers listed in the CISA report have released or are working on releases to correct this software flaw. Firms are advised to review the CISA report, check with the manufactures of their VPN systems and apply the required security updates to their systems.

Fewer Businesses Reporting Breaches and Attacks Although Impact of Those Firms is Still Severe

A UK government report (***GOV.UK***) last week claimed that cyber breaches and attacks dropped last year, due to tougher data regulations including GDPR (***Forbes***). The report states that the institutions being hit by attacks are being hit more often and by the same attackers. The report also states that the wave of attacks is directed from Iran against part of the UK's national infrastructure. These attacks occurred in December of last year and are believed to have impacted private sector companies, including banks, and the theft of personal data of thousands of employees.

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**