FS-ISAC Securities Industry Risk Group **August 2018**
Global Cybersecurity Brief **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**).

Same Ransomware, New Purpose

Researchers from Fortinet have discovered that the Jigsaw ransomware appears to be repurposed to steal Bitcoin by altering the addresses of wallets and redirecting payments into accounts owned by the attacker (**ZDNET**). Little of the source code of the malware has been changed so most security products will still identify the file locking malware.

The source code of Jigsaw has been available online for some time and anyone with knowledge of C# code could in theory tailor the malware to perform any malicious acts. Since this version of Jigsaw will be identified with most security products, firms should ensure that their software, network devices and appliances are updated and ensure they have mitigation plans in place in the event the malware attempts to install on their systems.

Worst Cyber Attacks So Far in 2018

As the first half of 2018 has come and gone, we look back at some of the worst cyber breaches so far in 2018. The number of global ransomware attacks and government leaks are fewer this year during the same time last year, which is good news (***WIRED***). Here are a few attacks that stand out so far in 2018:

- **Rampant Data Exposures** – A data exposure is when data is stored and secured improperly, such that it can be easily accessed by anyone anywhere. This often occurs when a database or other storage mechanisms are misconfigured**,** and requires minimal or no authentication to access it, such as using default passwords.

- **VPNFilter** – This attack is relatively recent; officials have warned about a Russian hacking campaign that has impacted more than 500,000 routers worldwide. VPNFilter can be used to coordinate the infected device and create a massive botnet; it can also directly spy and manipulate web activity on compromised devices. VPNFilter can infect dozens of popular router models. Authorities have been working to stop the botnet**,** while researchers are still trying to identify the full scope of this attack.

Based on these attacks alone, firms can learn to apply better techniques, develop or update polices, ensure devices are up to date and default passwords are not used to keep their networks and data more secure.

College Savings Accounts Stolen

Last month a state-run college savings trust reported that scammers stole $1.4 million. (**CNBC**). The Connecticut Higher Education Trust (CHET), which offers the state's 529 savings plan, announced the theft from 21 of its direct investors. The organization explained that the theft occurred by accessing the user's accounts online and making withdrawals. According to the state's deputy treasurer, the online activity occurred on accounts that previously had no online access. The lost funds for the affected customers have been made whole.

The facts known from this incident point to fraudsters having personally identifiable information of the account holders from a source other than CHET, using it to gain unauthorized access and illegally redirect payments.

Firms should review policies and procedures for managing online accounts, as well as accounts used by employees on internal systems. Firms should also investigate stronger password policies and utilizing a two-factor authentication system to help prevent illegal account takeovers.

DHS Hosts Cyber Summit and Announces New National Risk Management Center

On July 31, the US Department of Homeland Security (DHS) hosted a cybersecurity summit in New York City that included leaders from multiple government agencies and private sector leaders from the financial services, energy and telecommunications sectors. DHS announced a new National Risk Management Center. DHS also encouraged cross-sector cyber information sharing and exercises, announced efforts to focus on third-party risk, and signaled that the US Government will respond more aggressively, and collaborate more intensively to assist private sector companies in responding to and deterring against cyber adversaries. An FS-ISAC board member and senior

leaders from the FS-ISAC's Financial Systemic Analysis and Resilience Center (FSARC) participated on several panels that discussed the value of information sharing and systemic risk protection. FS-ISAC will be involved in several work streams with cross-sector partners resulting from the Summit.

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. Learn more and register (**Register Here**) for one of these upcoming sessions:

- August 29 | Federal Reserve Bank of St. Louis
- September 17 | Federal Reserve Bank of Chicago
- October 10 | Federal Reserve Bank of San Francisco
- October 24 | Federal Reserve Bank of Kansas City, MO

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.

Thank you,

FS-ISAC SIRG Team