FS-ISAC Securities Industry Risk Group **January 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 Cyber Security 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**).

Associations to Regulators: No New Cyber Rules Needed

A number of officials from different associations and outside experts continue to back the harmonization of existing regulations for cyberbreaches, rather than implementing new requirements for financial firms (**Think Advisors**). The consensus is that there are already numerous rules and guidance, and that regulators should work to harmonize existing requirements not impose new requirements which will add to the regulatory burden. Former US Securities and Exchange Commission (SEC) Deputy General Counsel Andrew Vollmer states "no strong case for new laws has been made." Mr. Vollmer goes on to say that new laws impose a significant cost for compliance, spawn a false confidence and reduce the flexibility of responding to new forms of attacks. He believes at this time that a new law is not justified. Vollmer also states that "Broker-dealers, public companies, and investment advisers are not resisting solutions to the threat of hacking; they are in favor of protecting against cyberintrusions. Cyberintrusions are very costly to businesses. They need cost-effective and workable solutions. If those existed, we have every reason to believe that regulated members of the securities markets would be prepared to adopt them without the compulsion of a law." Outside experts have shared the same concerns. They feel that simplicity is needed and that as soon as rules become more complex, loopholes can be easily exploited by the industry.

Doubts Raised About Group-IB Report

The Moscow-based cybersecurity software company Group-IB Security released a report last week asserting that a gang of criminals known as MoneyTaker had reportedly stolen more than $10 million from US and Russian banks (**The Hacker News**). According to the report, a successful attack would play out as follows:

- Actors first take over the bank's network to check to see if they can connect to the card processing system.
- They then legally open or buy cards of the bank whose IT system they hacked and provide those cards to money mules.
- Upon getting into the card processing system, the attackers removed or increased cash withdrawal limits for cards held by the mules and remove overdraft limits.
- The mules then withdrew the cash from the ATMs

Group-IB describes MoneyTaker as a group employing sophisticated TTPs. For instance, Group-IB claimed that MoneyTaker was able to create its own tools, regularly evolve their tactics and have a mature reconnaissance program that helps them avoid detection.

Notwithstanding these claims, which were widely reported in the media, the *American Banker* dug a little deeper and found that the claims in the report are misleading or unsubstantiated (**American Banker**). The *American Banker* included a statement from Gartner Vice President Avivah Litan, stating 'You couldn't have attacks on 16 community banks without FS-ISAC knowing about it'. The article also noted that the FS-ISAC recommends being part of an information-sharing network, and surveying peers to find out if they've seen an attack or been affected by it.).

Keylogger Function Found in Popular Laptops

HP issued a Security Bulletin regarding a keylogger function present in preinstalled Synaptics Touchpad software present on its laptops (**Business Insider**). According to HP, the keylogger function was built into the Synaptics software to help debug errors. Although disabled by default, an attacker accessing the computer could enable the function and harvest data. The issue impacts all Synaptics OEM partners which also includes Lenovo and Dell. At this time, HP is the only known manufacturer to provide a Security Bulletin in response (**HP Support**).

Over 1 Billion User Credentials Discovered on the Dark Web

Researchers at security firm 4iQ have discovered that over 1 billion unencrypted user credentials, such as usernames, email address and passwords have been leaked onto the dark web (**4iQ**). The researchers discovered a single database file containing user credentials in plain text, allowing anyone to easily read information (**ITPortal**). The database is a collection of over 250 many known breaches such as LinkedIn and Netflix. The database is alphabetized and indexed to allow for easy and quick access to credentials.

Firms are advised to review password policies and procedures with their end users and suggest to employees not to use common passwords that were found in the database such as '123456789','qwerty','password' and '111111'.

2018 FS-ISAC Annual Summit

The 2018 FS-ISAC Annual Summit will be held at the Boca Raton Resort & Club from May 20 - 23, 2018. FS-ISAC has reserved a block of rooms for its members at a group rate (More Details). Please make sure to reserve your room now, as the block will fill quickly. Reservation requests for the FS-ISAC Annual Summit will be accepted through Friday April 27, 2018. The block is available up to this date or until the block is full. Reservations requests received after April 27 are on space and price availability.

FS-ISAC Summits are a source of nutritional brain food and give you the energy to tackle your compliance, security and technical challenges. For more information on the summit or hotel reservations, please visit the summit site (**Summit Overview**).

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

If you have any questions about this report, please contact the **FS-ISAC**.

Financial Services Information Sharing Analysis Center **www.fsisac.com**