FS-ISAC Securities Industry Risk Group
Cybersecurity Brief for North America **October 2016**

FS-ISAC Collaborates with IIAC and SIFMA on First Monthly Update

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is pleased to be working with the Investment Industry Association of Canada (IIAC) and the Securities Industry Financial Markets Association (SIFMA) to provide to you this monthly newsletter that highlights Cyber Security topics and emerging threats to the Securities Industry within North America.

The information provided in this Monthly Newsletter is intended to increase the cybersecurity awareness of an organization's end users and to help them behave in a more secure manner.

This newsletter is not intended to replace the benefits of joining FS ISAC's member based organization and IIAC and SIFMA members who have not already done so are encouraged to join FS ISAC.

Thank you,

Peter Falco and Richard Livesley

pfalco@fsisac.com rlivesley@fsisac.com

Stolen Data from Encrypted Web Traffic

Researchers in Belgium have discovered a new Web-based attack that used JavaScript to steal encrypted information from HTTPS traffic. The attack is called HEIST, which stands for **H**TTP **E**ncrypted **I**nformation can be **S**tolen through **T**cp-Window (**Softpedia**). The threat actor relies on a malicious JavaScript code on a web page, or through a JavaScript based ads. The attacker embeds the malicious code inside of an ad that is shown on a banking portal or social media site. Threat actors can easily execute attacks using HEIST. The attacker can decrypt information such as email addresses, social security numbers, and account numbers with ease (**Arstechnica**). *Researches advise that users should configure their web browser to disable support for third-party cookies or JavaScript execution.*

Mobile Vulnerability Discovered

Investigators have discovered that a company based in Israel called the NSO group, sells software that tracks a target's mobile phone. The software can read email and text messages, as well as track calls and contacts. It can even record sounds, collect passwords and know the location of the phone (**NYTIMES**). Executives from NSO have stated that their spyware worked like a 'ghost', leaving no traces of the targets they tracked.

*Apple has released a patched version of its mobile software, iOS 9.3.5. Apple iPhone owners can apply this update through a normal software update (**APPLE**). Firms should apply the latest software updates on mobile devices, as well as inform end users of this vulnerability and how to apply this update.* FS ISAC members can find additional info on the FS-ISAC portal (**Tracking ID #924118**).

2012 Hack Reveals More Than 68M Passwords Stolen

After a 2012 hack in which more than 68 million usernames and passwords were stolen, the online storage company Dropbox is forcing some of its users to reset their passwords (**WSJ**). Dropbox learned that people outside the company had obtained files containing credentials, thus forcing them to reset user's passwords. While Dropbox had previously disclosed the attack in 2012, they greatly underestimated its impact until files began to surface.

Although the breach occurred in 2012, the scale of it has become more apparent. The efforts by Dropbox to force users to reset their passwords is a positive one. Many people use the same passwords for multiple personal and business accounts. *Firms should encourage users to not use the same passwords for different accounts, as well as include a password policy that makes users change their passwords on a regular basis.*

Cyber Threats Continue for Bitcoin Exchanges

Last month the second largest cyber threat on a Bitcoin exchange called Bitfinex, where hackers stole $70 million dollars of the virtual currency. New data by Reuters find that a third of bitcoin exchanges have been hacked and nearly half have closed in the past 6 years (**Reuters**). Bitfinex is now up and running, but lost 36% of the assets they had on their platform and were compensated with token credits for the losses that have be converted into equity in its parent company.

In contrast, data from the Privacy Rights Clearinghouse, a non-profit organization, showed that of the 6,000 operational U.S banks, only 67 U.S. banks (*Approx. 1%*) experienced a publicly-disclosed data breach between 2009 and 2015.

Ransomware 101 Events

The FS-ISAC is teaming up with the National Health ISAC, Multi-State ISAC, Palo Alto Networks, Symantec, FBI, and US Secret Service to conduct 15 workshops across the US to build awareness on ransomware threats. Ransomware has been a continuing threat to financial institutions and organizations throughout the economy. This series of workshops will be designed for both small and large organizations at the C-Suite level to build awareness and describe mitigation techniques among healthcare, financial services and state/local government entities. In this half-day workshop, these experts in cybersecurity will:

- Describe ransomware;
- Cover the tactics, techniques and procedures used by the criminals;
- Provide the threat landscape;
- Discuss why situational awareness and information sharing are important;
- Offer strategies to help protect your organization from ransomware attacks;

*Click **here**, for more information on the upcoming free events and how to register. (This program is not delivered in Canada. Information on ransomware is posted by the federal government on its **GetCyberSafe website**.)*

2016 FS-ISAC Fall Summit

The 2016 FS-ISAC Fall Summit, taking place October 23-26 in Nashville, Tennessee, features nearly 70 member-vetted breakout sessions and multiple amazing networking opportunities. Enjoy the sights and sounds that only Nashville can offer in the company of some of the brightest minds in information security. **View the brochure** for full session descriptions and the agenda. Here are just two sessions from our amazing line-up:

- **Preparing for A Bad Day Through Cyber-Exercises** - Discuss what several banks have done and are doing when it comes to preparing its technical and executive staff through the implementation of cyber threat-based exercises.

- **Crowdsourcing Solutions Forum with Members** - Have a tricky problem that you want to know how other member companies are addressing? This session will focus on industry members and the FS-ISAC staff sharing approaches to solving or addressing tricky problems.

Learn more about the **2016 Fall Summit** or **register today** – the early bird registration ends September 23.

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.

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

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