FINANCIAL SERVICES Information Sharing and Analysis Center

FS-ISAC Securities Industry Risk Group
Global Cybersecurity Brief **February 2017**

FS-ISAC Collaborates for its first Global Monthly Update

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the International Council of Securities Associations (ICSA), the Investment Industry Association of Canada (IIAC) and the Securities Industry Financial Markets Association (SIFMA)

The information provided in this Monthly Newsletter highlights Cyber Security topics and emerging threats to the Securities Industry. 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 organizations who are not already members are encouraged to join. For information, please contact **FS-ISAC**.

Update from the FS-ISAC Analysis Team

Android Security Bulletin

January's Android Security Bulletin contained details of security vulnerabilities affecting Android devices. Impacts included distributed denial of service (DDoS), information disclosure, elevation of privileges, and system access. The most severe of these issues is a critical security vulnerability that could enable remote code execution on an affected device through multiple methods such as email, web browsing and MMS when processing media files.

2017 Cyber Security Predictions

To bring in the new year, various companies published their predictions of cyber security issues that will be notable in 2017. Trends in predictions across reports include further development and frequency of Internet of Things (IoT) attacks, targeting of industrial systems, and increase in attacks directed at corporations. Concerning the financial services industry, Palo Alto predicts that institutions will continue to adopt public cloud computing and adopt more multi-factor authentication (MFA) in light of stolen credentials and fraudulent fund transfers seen by SWIFT member banks. The company further

predicts that in 2017 attackers may target weaknesses in blockchain technology to compromise financial transactions.

New Ransomware Attacks

Researchers from Proofpoint discovered a new ransomware named the 'CryptoLuck' (**Malware Don't Need Coffee Blog**). The malware uses the RIG-Empire (RIG-E) exploit kit to distribute itself. The exploit kit is also new and is about a month old. The distribution uses malvertising, and visits to adult websites; however, it could begin to spread through compromised sites and other paths(**SecurityWeek**).

The malware infects computers by abusing the *GoogleUpdate.exe* and DLL hijacking (**BleepingComputer**). Once a computer is infected, the 2.1 bitcoin (~$1,500) ransom must be paid within 72 hours. Researchers have noticed that the ransomware perform a series of checks to see if the host to which it has attached is a virtual machine, if not, the malware scans all mounted drives and network shares for files that it can encrypt, and appends '*.[victim_id]_luck*' to the files it encrypts. Once the ransomware encrypts all files, a ransom note is displayed with instructions on how to download the decryptor. Once the decryptor is launched, detailed step by step instructions are provided to the user to make the ransom payment. Once payment is made, the files then automatically get decrypted.

Since the exploit kit is distributed by malvertising, individuals may be advised to practice general cyber awareness by thinking before clicking on advertisements or links, etc. In addition, given the vulnerabilities in Internet Explorer and Adobe Flash that RIG-E exploits, ensuring that this software applications and systems are up to date may also help prevent being affected by RIG-E and associated malware, including CryptoLuck.

Regulatory Update

While many regulatory discussions are underway, nothing has reached the level of publication this past month. There has been significant activity in the US.

Two U.S. regulators did publish examination priorities that may be of general interest. The Financial Industry Regulatory Authority (FINRA) has just released its 2017 Regulatory and Examination Priorities Letter (**FINRA**). Given the evolving nature and changes of cyber threats, FINRA will focus on firms' cybersecurity preparedness and approach to cybersecurity risk management. While FINRA recognizes there's no "one-size-fits-all" approach they will tailor assessments of firms' cybersecurity program based on factors such as business model, size and risk profile. Other areas that FINRA may review are a

firm's method for preventing data loss; understanding the flow of its data through the firm and possible vendors, including access controls firms use to monitor and protect this data.

The Securities and Exchange Commission (**SEC**) has also released their 2017 Examination Priorities Letter. The letter mentions cybersecurity as a priority for the commission, and that the SEC will continue their initiative to examine cybersecurity compliances, procedures and controls for firms, including testing the implementation of these procedures and controls.

The US financial services organizations are developing comment letters in response to an advanced notice of proposed rulemaking (**ANPR**) on "Enhanced Cyber Risk Management Standards". The Board of Governors of the Federal Reserve System (Federal Reserve), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) issued the ANPR in October 2016 and requested comments by February 17, 2017

Finally, the Trump Administration has promised to reduce regulatory burdens on financial institutions and businesses and focus on cybersecurity protections.

Registration Now Open for the APAC and Annual Summits

Registration is now open for both the Asian Pacific **APAC Summit**(3-4 April, 2017 in Singapore) and **Annual Summit** (30 April-3 May, 2017 in Lake Buena Vista, FL)! Don't miss your chance to attend!

FS-ISAC Summits are focused around peer-to-peer networking and building relationships or circles of trust with financial services organizations. We invite you to attend and see what new sessions and exciting innovations are developing around information sharing amongst financial institutions and threat intelligence practices.

Register for the APAC Summit | **Register for the Annual Summit**

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,

Peter Falco and Richard Livesley

pfalco@fsisac.com rlivesley@fsisac.com

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

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