FS-ISAC Securities Industry Risk Group **December 2017**
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**).

US SEC: New Guidelines on Reporting Data Breaches Coming

In a recent *Wall Street Journal* report, senior staff at the United States Securities and Exchange Commission (SEC) state that public companies will soon face new guidelines for how they report cybersecurity breaches to investors (**WSJ**). The commission will look into updates directions that it had given to companies six years ago before high-profile breaches such as Equifax Inc., and one on their own systems (**Morningstar**).

William Hinman, the SEC's Director of the Division of Corporation Finances, also stated that the commission should update the guidance on describing the level of cyber-intrusion that demands public disclosure. Mr. Hinman also advised companies to examine their own policies for insider trading following a cyberbreach.

Denmark Ramps Up Cyber Efforts

The Denmark government plans to release a strategy early next year to boost efforts to prevent cyber-attacks (**Reuters**). Part of the strategy would be to expand the early warning system with sensors that detect when Danish companies or authorities are under attack from malware or ransomware. The government also wants to increase the preventive capacity at the Danish Centre for Cyber Security to improve its ability to better catch and inform about imminent cyber threats.

The government also would like a deeper cooperation between authorities and private companies to battle or prevent cyberattacks, such as one of Denmark's largest companies Maersk, which caused one of the biggest disruptions in global shipping.

Sheltered Harbor: Building a Stronger Cyber Defense

The FS-ISAC helps financial institutions learn from each other about the cybersecurity threats facing the industry. But what happens when hackers hit your firm and customers' data is compromised inaccessible.

Sheltered Harbor (SH Site), was established following a series of cybersecurity simulation exercises, called the Hamilton Series, which were conducted by the Financial Services Sector Coordinating Council (FSSCC), in coordination with the US Dept. of the Treasury and with support from FS-ISAC. Sheltered Harbor is the industry's response for one of these vulnerabilities: to ensure business continuity for retail banking customers if an attack happens and all defenses fail. The organization partners with member banks to ensure their customers' accounts are safe, should a cyberattack damage the bank's data, and if a bank is unable to recover from such an attack in a timely manner. If the worst should occur, the bank's customers would still be able to access their account through another member financial institution via a restoration at another member bank or through a service provider. The data is encrypted and remains private, and service continuity for the customer is assured.

Like FS-ISAC, financial institutions are working together to ensure the safety of consumer data. Membership fees are determined by the size of the financial institution. So far already 63 percent of US retail bank and brokerage accounts are members – are you?

Two feature articles appeared this week in the Wall Street Journal (**WSJ**) and Bloomberg (**Bloomberg Technology**). For more about Sheltered Harbor, please visit their site (**Join SH**) or contact them at: **info@shelteredharbor.org**.

UK Banks Weather DDoS Attacks

Unknown threat actors have turned again to distributed denial of service (DDoS) attacks to cause disruption to business networks. Members in the United Kingdom report recurring DDoS attacks in the months of October and November. While these attacks have had relatively low impact to business operations and website availability, it has caused an increased operational tempo by security teams needing to adapt to the changing attacks. Other European members also report sporadic attacks; however, it is not currently known if any of these attacks are related to the persistent campaign in the UK. This is not believed to be linked to the DDoS extortion gang --the Armada Collective-- demonstrating attacks against finance-related firms in Europe as none of the other attacks were associated with a ransom demand. FS-ISAC is coordinating cross-border public-private partnerships to determine if there are any links.

Security researchers at Corero Network Security revealed new data suggesting that, as a whole, businesses are seeing a significant increase in DDoS attacks in the third quarter of 2017. Corero estimates that businesses see eight attempted DDoS attacks daily. DDoS using botnets of internet of things (IoT) devices may be partially responsible for increase. One such botnet that recently gained notoriety for its potential threat is the IoTrooper, also known as the Reaper botnet. It leveraged vulnerable internet-connected webcams, security cameras, and digital video recorders (DVRs) to grow in size, however, initial estimates of its power by security researchers at Check Point were found to be overstated. Members should consult their DDoS mitigation providers and work with their internal

response teams to ensure that they are implementing best practices. FS-ISAC does have DDoS mitigation documentation available on the portal. Some members have also reported DDoS extortion attacks but FS-ISAC largely considers these to be low threat and lacking credibility, as threat actors seldom follow through with their posed threats.

2018 SEC Priorities Letter Expected to Focus on Cybersecurity

While the 2018 version of the Securities and Exchange Commission (SEC) examination priorities letter is not yet released, many believe that cybersecurity will be main focus, especially after recent breaches such as the commission's Edgar system. While the commission's priorities list is a roadmap the Office of Compliance and Inspections and Examinations (OCIE) it will likely to be release in January with many believing to have a focus on cybersecurity.

FS-ISAC and MAS to Strengthen Cyber Information Sharing Across Nine Countries

The Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Monetary Authority of Singapore (MAS) today launched the FS-ISAC Asia Pacific Regional Analysis Centre's office and operations in Singapore. The setting up of the Regional Centre in Singapore shows the growing collaboration between the two organizations to fight cybercrime. The Centre currently supports 49 financial institutions across nine Asia Pacific countries. The nine Asia Pacific countries are Australia, India, Japan, Malaysia, New Zealand, Singapore, South Korea, Taiwan and Thailand.

"Information sharing remains one of the most effective ways to stay ahead of cybercrime. Strengthening local intelligence capabilities and cyber-resilience is critical at both a regional and a global level," said Bill Nelson, President and CEO, FS-ISAC. "Strengthening our presence in Asia Pacific helps build the resilience of the entire global financial services sector."

Sopnendu Mohanty, Chief FinTech Officer of MAS, said "Against the backdrop of increasingly complex and sophisticated cyber-attacks, it is even more important for countries to stay engaged, foster stronger relationships and exchange information and expertise freely. The Centre's operations and the regional intelligence reports it produces will help Asia Pacific countries to deal better with cross-border cybercrimes."

To help its Asia Pacific members stay ahead of cybercrime in the region, the Centre provides 24/7 local and global coverage with threat information sharing, actionable intelligence, as well as tools and resources to respond to incidents. Members also benefit from regional meetings, regionally-focused monthly threat calls, webinars on hot topics, cybersecurity training and summits.

To meet the growing need for cybersecurity talent, FS-ISAC signed a memorandum of understanding with Temasek Polytechnic to provide internship opportunities for the Polytechnic's students. Students will be exposed to real world cyber threats to build up their skills in cybersecurity. This initiative supports the financial services industry transformation map initiative to build a local pipeline of specialized IT talent for the financial services sector, including in the area of cybersecurity.

The next FS-ISAC AP Summit will take place in Singapore from July 17-18, 2018 (**FS-ISAC APAC Summit**) and includes member meetings, workshops and simulated exercises.

GIBON Ransomware Spread Via Malspam

Researchers have provided further information in relation to the GIBON ransomware, which is available for sale on a dark web forum back in May 2017 (**SC Media**). Initially GIBON was first discovered and reported by Proofpoint researchers, who gave the name GIBON, because it appeared in two places, once in the user agent string and once in the Admin panel. GIBON is spread via malspam containing a malicious document attached to the message; once activated it will down-load and install the GIBON ransomware on the victim's device. Once it has first executed, GIBON will connect to the Command and Control (C2) server and register a new victim by sending a base64 encoded string that contains the timestamp, version of Windows, and the 'register' string. Once contacted, the C2 server will then respond with a base64 encoded string that will be used by the GIBON ransomware as the ransom note. Once the victim machine is registered with the C2 server, it will locally generate an encryption key and send it to the server as a base64 encoded string. The malware will use the key to encrypt all files on the victim computer and leave a ransom note in each folder containing encrypted files. There has been a decryptor released (**Bleeping Computer**), and FS-ISAC would encourage members to share any information they see regarding GIBON via their Listservers and FS-ISAC portal.

FS-ISAC and JHU APL Partner to Advance Cybersecurity Automation in Financial Sector

On November 13, the FS-ISAC and Johns Hopkins University Applied Physics Laboratory (JHU APL) announced an effort to operationalize the Integrated Adaptive Cyber Defense (IACD) framework (**IACD Site**). The IACD framework guides implementation of commercially available automation technology to improve cybersecurity orchestration and information sharing. Tests of the IACD have shown a reduction in investigation and response time from 11 hours to 10 minutes. The IACD also enables an operations team handling 65 events per day to automatically process up to 95 events at the same time. Through this partnership, FS-ISAC will support greater adoption of the framework within the financial sector and JHU APL will provide technical assistance to FS-ISAC and member organizations that adopt the IACD. The US Department of Homeland Security is providing funding to JHU APL for this initiative.

Trojan Attacks Steal Data and Disrupt Service to Financial Institutions Globally

Throughout November, FS-ISAC has released alerts and reports about several trojan attacks targeting or impacting the financial industry. The names of these trojan attacks include FALLCHILL, Volgmer, IcedID and Silence and are designed to steal data or disrupt service. For example, FALLCHILL, Volgmer, IcedID and Silence have been discovered on systems throughout the world targeting financial institutions for the purpose of data theft or service disruption. FALLCHILL and Volgmer are remote access trojans (RAT) likely used by the North Korean hacking group Hidden Cobra. The US Department of Homeland Security and Federal Bureau of Investigation released threat detection and risk mitigation guidelines for these trojans in their joint Technical Alert earlier this month. The IcedID and Silence trojans both infiltrate systems using spear phishing campaigns and can be mitigated with employee training to avoid malicious emails, enabling protected view for email attachments and ensuring anti-virus programs are fully updated on all systems. FS-ISAC released Technical Analysis Reports (TAR) for both IcedID and Silence which can be found through the FS-ISAC Portal.

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**.

This newsletter contains content developed by FS-ISAC as well as links to content developed by third parties. FS-ISAC makes no claims or warranties as to the accuracy of information provided by third parties. All copyrights remain with their respective owners.

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