FS-ISAC Securities Industry Risk Group **February 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**).

Account Takeovers Leveraging the SWIFT System

In 2017, cyber criminals conducted account takeover attacks against individual banks resulting in fraudulent transfers via the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system. For example, criminals attempted to steal $60 million from the Far Eastern International Bank (FEIB) of Taiwan in October. While most of the funds were recovered, two Sri Lankans were arrested for successfully withdrawing $500 thousand. A few weeks later, NIC Asia Bank in Nepal had more than $4 million fraudulently transferred out under similar circumstances. Many security analysts link this activity to the North Korean-associated Lazarus Group. SWIFT banned transactions from United Nations-sanctioned North Korean banks in March which may have prompted these attacks out of retribution and an effort to generate revenue for the regime. Regardless of attribution, it is believed this tactic has been used against the international banking system since at least 2015. Understanding this growing threat with severe consequences, SWIFT is promoting best practices and information sharing through its customer security program. FS-ISAC additionally provides reporting and guidance from SWIFT on our Portal (**FS-ISAC Portal**).

FS-ISAC Responds to Spectre and Meltdown

While vulnerability management is a core part of most financial institutions cybersecurity practices, FS-ISAC and our members continue to assess the actual risk and seek additional information about the vulnerabilities and their potential impact. The FI community takes all vulnerabilities seriously and takes proactive measures to ensure proper risk mitigation.

In addition to the security considerations raised by this design flaw, performance degradation is expected which could require more processing power for affected systems to compensate and maintain current baseline performance. Additional costs may also be a factor to maintain current system and application performance.

Even outside of the known performance hit, fixing kernel level vulnerabilities typically requires more testing than browser, office productivity applications and other patches due to the underlying direct link to the operating system. There will need to be consideration and balance between fixing the potential security threat vs the performance and other possible impact to systems. The current general thought is that the security risk will be lower on dedicated servers and end points (due to the expected exploit requirement to run code on an individual system) and higher on shared computers such as hosting and cloud services which use the same physical hardware (and processor) to share different (user) virtual machines.

FS-ISAC held a special members-only call on Tuesday 9 January and the ISAC Analysis Team provided that “Speculative Execution” is a CPU feature designed to accelerate program execution and ensure efficient CPU utilization. This allows a processor to execute code in advance even before it is certain it needs to be done, so the results are ready as quickly as possible if needed and simply ignored if not. However, security researchers have demonstrated that this feature could be taken advantage of by malicious actors to read system memory that should be inaccessible. In Intel’s x86-64 hardware it appears that programs may be able to speculatively execute code that would not have permission to run under normal circumstances, allowing carefully-constructed, malicious code to essentially read the kernel memory space without the proper permission. The potential impact of such an attack is unauthorized access to sensitive information including passwords or login files.

Android-Based Malware Targets Mobile Banking Apps

Researchers from Avast Software have disclosed a new Android based malware that can steal customer passwords and carry out fraud (**Avast**). The new malware is called ‘Catelites Bot’ that shares similarities to another malware named ‘CronBot’**,** which was discovered in May 2017. Both get installed on a device from fake apps available on third-party app stores or via a phishing website (**Security Week**).

Researchers also mentioned that the Catalite actors are linked to the CronBot actor and have seen one to two fake apps per week attacking Android devices to make users download the malware. Once downloaded the criminal uses sophisticated social engineering techniques to get the victim’s credit card and bank account information. The malware can pose as apps to over 2,200 financial institutions adopting the logos and application names of these firms.

Researchers suggest the following tips to mobile users:

1. Beware of any strange requests for admin rights: better still, always think twice about granting any admin rights request.

2. If you open your bank app and something doesn't look right, shut it down.

3. If you think you have the malware on your phone, boot your phone in safe mode and carefully follow the directions. Remove any suspicious apps as directed.

4. Only get your apps from reputable stores like Google Play.

5. Install security software on your phone to protect against this and other malware threats.

FS-SIAC Presents New Board Presentation Briefings

In the era of constant cyber-attacks and high-profile breaches, keeping top leadership abreast of both cybersecurity threats and best practices is a high priority for all financial institutions. FS-ISAC is offering a new presentation series for our members and designed for boards of directors.

Many boards of directors are asking for neutral third-party and independent briefings and discussions about cyberthreats that may impact their financial institution. They seek best practices to prevent, defend and respond to those threats.

With about 7,000 members, from regional community institutions through the world's largest financial firms and spanning business banking, commercial banking, insurance, brokerages, securities and more, FS-ISAC executives are experienced in providing boards of directors with sophisticated executive-level briefings and have made such presentations over the past few years.

Boards will walk away from this briefing with the following:

- Understanding the major threats affecting the financial services industry;
- Knowing threat actor motivations and tactics at a top level;
- Seeing the important role that the board of directors plays in managing cyber-risk;
- Learning best practices used by industry peers;
- Hearing about the importance of the executive team in overseeing prevention, detection and response to risks in relation to the enterprise and to customers/members; and
- Experiencing the importance of information sharing as one of many tools critical to combat cyber-attacks against your financial institution.

View a one-page overview of this program (**One-Page Overview**). Please note that there is a fee for this service and there are a limited number of briefings available. To schedule a session, please contact: **boardpresentation@fsisac.com**.

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**