FS-ISAC Securities Industry Risk Group **June 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 cybersecurity 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**).

CIO 100 Award Winners: FS-ISAC and Sheltered Harbor

On 2 May 2018, IDG's CIO (***CIO Magazine***) announced that Financial Services Information Sharing and Analysis Center (FS-ISAC) and Sheltered Harbor are each individual recipients of the 2018 CIO 100 Awards (**2018 CIO Awards**). The 31st annual award program recognizes organizations around the world that exemplify the highest level of operational and strategic excellence in information technology.

FS-ISAC's crucial innovation has created the first-ever centralized platform for cyberprofessionals to aid in combatting ever-increasing cyberthreats. Before FS-ISAC, evaluating the veracity of incident information was slow and time consuming with only local, decentralized resources to help. FS-ISAC members now benefit and contribute to having access to 24/7 global and local intelligence. Information is shared both digitally and in person via a trusted online network, emergency local or global threat calls, monthly regional member meetings, and at one of four annual Summits (**FS-ISAC Summits**). FS-ISAC further holds webinars on hot topics, offers cybersecurity training, hosts exercises and provides tools and resources to respond to incidents.

Sheltered Harbor, a subsidiary of FS-ISAC, is being recognized for its contributions to creating a safety net for consumers in a worst-case security scenario. Founded by 34 financial institutions,

industry trade groups and leaders, along with core processing providers, Sheltered Harbor's mission is to safeguard consumers and the financial sector from cyber and physical attacks (**SH Site**).

Retirement Industry Council Launch

The Financial Services Information Sharing and Analysis Center (**FS-ISAC**), in partnership with the SPARK Institute (**SPARK**) announced the creation of the Retirement Industry Council (RIC) to help promote voluntary information sharing and threat intelligence to members within the retirement industry that administer plans like 401(k), individual retirement accounts and pension funds (**FS-ISAC Press Release**).

The RIC was created to provide a forum for, and to assist firms involved in the $28 trillion* retirement investment community. Participants in the council will either be members of the FS-ISAC or members of the SPARK Institute's Data Security Oversight Board (DSOB). The RIC will share information about solving security challenges and focus on the combination of physical and cybersecurity threats faced by the retirement industry. Through collaboration, the council will also provide trusted best practices on security controls and priorities. "Information sharing of cyberthreats, vulnerabilities, and best practices is one of the most effective ways to stay ahead of cyberattacks," said Bill Nelson, chief executive officer of FS-ISAC. "Expanding FS-ISAC coverage to include retirement assets is yet another way to ensure the entire financial services sector can protect their customer accounts in every way and throughout each life stage."

The council is a subset of the FS-ISAC Securities Industry Risk Group (SIRG), with members sharing information related to solving challenges specific to organizations in the securities industry. The SIRG is comprised of more than 300 FS-ISAC members in various roles including chief information security officers, chief risk officers, information technology operations and corporate security. Members involved in the securities industry include asset managers, broker-dealers, hedge funds, private equities, securities exchanges, payments and transfer agents, banks and insurers. "Having SPARK partner with the FS-ISAC through the RIC helps our members connect and share information on cyberthreats for the industry," said Doug Peterson, the chair of SPARK's DSOB and the chief information security officer at Empower Retirement.

SPARK's DSOB is made up of 37 industry representatives with members from both the record keeping industry and plan consultants that serve the interest of plan sponsors. If you or someone within your firm is interested in learning more about the RIC, please contact the FS-ISAC SIRG Team (**FS-ISAC SIRG Team**).

Zero-Day Vulnerability Found in Office 365

A new zero-day vulnerability known as baseStriker, which bypasses the security systems on an Office 365 account to send malicious emails, was discovered by security researchers from Avanan (**Avanan**). The researcher noticed that baseStriker is able to penetrate Office 365 by essentially

confusing APT, Safelinks or other cyber defenses by splitting and hiding the malicious link using a <base> URL tag (***BleepingComputer***). Researchers said there is no fix for this problem, but recommends users implement two-factor authentication; the malware won't stop from being installed but could resist attempts as credential harvesting by malicious actors (***SC Magazine***). Firms should review the Avanan report to further understand the malware as well as consider implementing two-factor authentication on their systems or enforce a stronger password policy.

FS-ISAC CEO Testifies before Senate Banking Committee

On 24 May, Bill Nelson, CEO and President of FS-ISAC testified before the US Senate Banking Committee on cyber risks, efforts by the financial services industry to increase cyber readiness, and recommendations for the government to help protect companies' and consumer's information. (**Testimony**). Nelson conveyed three key points: 1) Despite a growing cyber threat environment, the financial sector has made a significant investment in cyber defenses; 2) The financial sector has come together as a community to back major resiliency efforts; and 3) The financial sector continues to benefit from strong public-private partnerships that enable cyber threat intelligence to flow to the sector and improve detection, prevention and response to cyber threats and other risks.

New Principles to Safeguard Customer Data Announced by SIFMA

On 12 April 2018, the Securities Industry and Financial Markets Association (SIFMA) released its Data Aggregation Principles (**SIFMA**) to protect member firms and their customers against potential security breaches and misuse of personal financial data by third-party aggregators. These principles are meant to provide customers with secure access to their financial information, while maintaining security and integrity of their member's systems. The four principles are:

Access

- Customers may use third parties to access their financial account data. SIFMA member firms believe that such access should be safe and secure.

Security and Responsibility

- Customers should not have to share their confidential financial account credentials (personal IDs and passwords) with third parties.

- Customers deserve assurances that anyone accessing their financial account data will keep it safe and secure, adopt the same data and security standards followed by regulated financial institutions, and take full responsibility for any data they receive and provide to others.

Transparency and Permission

- Customers should first receive a clear and conspicuous explanation of how third parties will access and use their financial account data, and then be able to consent affirmatively to this activity before it begins.

- Customers should be able to withdraw their consent easily and at any time with confidence that third parties will delete and stop collecting their financial account data and delete any access credentials or tokens.

Scope of Access and Use

- Customer information available to share with third parties typically includes financial account data such as holdings, balances, and transaction information, and does not include other non-public and confidential personal information.

- For customer protection, account activities such as third-party trading, money or asset movement, client verification, and other services that go beyond financial account data aggregation should be subject to separate agreements and require separate informed affirmative consent.

The above-mentioned principles will help customers who use these third-party aggregators via websites and mobile apps to access all of the finances on a real-time basis by reducing risks and potential fraud (**ThinkAdvisors**). SIFMA is encouraging member firms and aggregators to use application programming interfaces (APIs) or other secure technologies as a way for data aggregators to access customer data without using customer credentials. This method solution allows APIs and Aggregators to get access to data via an agreed upon connection with financial institutions. While SIFMA has not recommended any specific technology, SIFMA General Counsel Melissa MacGregor has suggested firms consider using a model API available from the FS-ISAC.

New Threat Campaign: Operation HaoBao

McAfee's Advanced Threat Research (ATR) analyst identified a new campaign, dubbed HaoBao. In January 2018, McAfee researchers observed financially motivated attacks and attributed the campaign to the North Korean threat actor known as the Lazarus Group (**McAfee**). The international cybercrime group Lazarus is targeting bitcoin users and global financial organizations, leveraging crafted emails that appear to be job recruitment advertisement.

On 15 January, McAfee ATR discovered a malicious document masquerading as a job recruitment for a Business Development Executive located in Hong Kong for a large multi-national bank. The document was distributed via a Dropbox account.

This is the mark of a new campaign, though it utilizes techniques, tactics and procedures observed in 2017. This document had the last author 'Windows User' and was created 16 January 2018 with Korean language resources. Several additional malicious documents with the same author appeared between 16-24 January 2018.

In this latest discovery by McAfee ATR, despite a short pause in similar operations, the Lazarus group targets crypto currency and financial organizations. Furthermore, the FS-ISAC observed an increased usage of limited data gathering modules to quickly identify targets for further attacks. This campaign is tailored to identifying those who are running Bitcoin-related software through specific system scans.

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**