FINANCIAL SERVICES | Information Sharing and Analysis Center

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

Tips on How to Combat Ransomware Attacks

The Petya malware attacks on June 27 again highlight the need for good cyberhygiene practices, including upgrading operating systems and timely patch management as well as participating in information sharing. Security analysis of these attacks shows that the malware, with attributes of ransomware, permanently encrypts data, effectively destroying it. Members should ensure that they are protected against older vulnerabilities in certain Microsoft software products (**Microsoft**). The adversaries behind the attacks leverage tools released by the group known as the Shadow Brokers. Microsoft has released patches for these vulnerabilities. As a result of the new release of hacking tools that target closed networks as well as internet activity, FS ISAC recommends members review all published information related to these threats. This will help ensure they are protected, especially from campaigns using older vulnerabilities and targeting unsupported software. Security companies and governments are researching the adversaries behind these ransomware and data destruction attacks.

In addition to extensive reporting and information sharing, the FS-ISAC released a publicly available tip sheet on ransomware (**FS-ISAC**), including:

- Isolating infected systems from your networks
- Keeping operating systems and antivirus software up-to-date
- Testing backups in a real-world environment
- Reporting any ransomware to law enforcement within 72 hours

The FS-ISAC advises firms to download this tip sheet and share with other colleagues within their company as well as review and update their mitigation plans regarding ransomware.

New Low-Cost Password Stealing Malware Arises

Researchers at Proofpoint have discovered a new malware named 'Ovidiy Stealer' aimed at stealing user credentials (**Proofpoint**). The malware is an effective password-stealing tool that can snatch credentials from web browsers such as Opera and Google Chrome.

According to the researchers at Proofpoint the malware is distributed as executable email attachments (**FORBES**). The attacker, who goes by the name 'TheBottle', also gets access to a web-based dashboard that provides updates on attack campaigns, reviews log files from infected computers and tech support from the malware's hacker. Researchers state that the malware is not as advanced as others, but its low price of $13 USD gives it potential to be a much more widespread threat.

Firms should take measures to prevent this malware from invading their system - such as ensuring all software and hardware have the latest patches, improve password policy to include longer length passwords that contain a combination of letters, numbers and special characters; implement two-factor authentication on all user accounts and blacklist/block the 'ovidiystealer[.]ru' domain which is utilized by the malware.

Release of "Principles for Fair and Accurate Security Ratings"

A group of executives from financial services, energy companies, health, retail, and security vendors developed a set of voluntary "Principles for Fair and Accurate Security Ratings" to guide the use and development of cybersecurity ratings.

According to the principles, "Security rating companies use a combination of data points collected or purchased from public and private sources and proprietary algorithms to articulate an organization's security effectiveness into a quantifiable measure or score. As these ratings rely in part upon the quality and breadth of the data they use, the variety of sources and the dynamic nature of the environment create risks of producing ratings that can potentially be inaccurate, irrelevant or incomplete." The principles "promote fairness in reporting and enhance the value of security ratings across all industries" and are organized around six categories:

- Transparency
- Dispute, Correction and Appeal
- Accuracy and Validation
- Model Governance
- Independence
- Confidentiality

The companies that contributed to these principles view this as a first step at maturing the security rating industry and their use. The securities principles were released on June 20 by the US Chamber of Commerce and available on its website (**US. Chamber of Commerce**)

Cybersecurity: Top Compliance Concern in Recent Poll

In a 2017 poll conducted by the Investment Adviser Association, the ACA Compliance Group and OMAM, a global asset management company found that cyber security has been the top compliance topic for the 4th year in a row (**IAA Poll**). The poll found that 76% of respondents increased cybersecurity

testing over the past year. Firms have also continued to dedicate more resources to cybersecurity, with 44% having purchased cybersecurity insurance (**ThinkAdvisor**). Eighty six percent of firms said they have conducted cyber risk assessments while 72% have conducted network penetration tests.

FS-ISAC Outreach

The FS-ISAC is pleased to announce Securities Industry Risk Group – Europe-Middle East-Africa email distribution list (SIRG-EMEA). The distribution list was created to provide an information sharing forum for FS-ISAC member firms in the Securities/Investment Industry (such as asset managers, broker dealers, hedge funds, private equity firms) whose offices are based in the EMEA region who want to share information with other members in the region.

This email distribution list will allow the members in EMEA region to gain a more hands-on experience with their FS-ISAC membership, and have a new outlet for information sharing and asking questions related to cyber and physical threats, as well as regulatory cyber compliance. Members of this group will also be included in the FS-ISAC SIRG mailing list, so that they can communicate with other members in the SIRG as well as receive SIRG materials such as newsletters, invites to SIRG meetings and access to material in the SIRG folder on the 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**.

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