FINANCIAL SERVICES Information Sharing and Analysis Center

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

Surveys Show Threat Intelligence Key to Security

A recent survey of more than 1,000 IT and IT security practitioners found that 84% say threat intelligence is important to a strong security posture (**eSecurityPlanet**).. This is a 25% increase from last year. While many have found threat intelligence to be important for their firm's efforts to protect systems and data, others have found the it to be too voluminous and complex to integrate threat intelligence platforms with other security technology tools. While in its infancy threat intelligence is an integral part of a firm's security operations. Overcoming the challenges of large volume of data and alerts will help a firm become more cyber aware in the long run.

Impact of China's Cybersecurity Law on Foreign Firms

A recent report highlighted the broad powers given to the China Information Technology Evaluation Center (**CNITSEC**) by China's new Cybersecurity Law enacted on June 1, 2017. CNITSEC is part of the Ministry of State Security (MSS) rumored to be behind APT3 (**Recorded Future**). Under the Cybersecurity Law, the MSS could initiate investigations of foreign firms based on 'national security', and conduct software vulnerability tests or reliability checks on them via the CNITSEC. Presumably, the information collected by CNITSEC would be forwarded to the MSS as part of its bigger intelligence gathering effort. The concern from foreign firms is that such information could potentially be used by the MSS to conduct future state sponsored cyberattacks. The report also commented on the broadness of the law, where any "enterprises and institutions that provide services and conduct business activities through networks" are in scope. The vagueness of its language could also be used by the government to compel companies to disclose sensitive information. As a result, firms operating in China face a difficult choice between following the law or risk being excluded from operating in China. FS-ISAC members are encouraged to share any information on the law's impact to financial institutions.

Examinations Uncover Large Number of Vulnerabilities

At its annual conference last week, the North American Securities Administrators Association (NASAA) announce that nearly 700 cyber-related vulnerabilities were found after a coordinated exam on state-registered investment advisors (**Financial Advisor**). The examinations were held in 37 states and jurisdictions from January 2017 to June 2017. The vulnerabilities found no testing of cybersecurity vulnerabilities, and a lack of procedures regarding security of devices.

Firms should look at these findings as a good starting point for where to begin or continue to improve their cybersecurity readiness. For example, if a firm does not have cybersecurity insurance, the Financial Services Sector Coordinating Council (FSSCC) has a cybersecurity insurance buyers guide on their website (**FSSCC**). The FS-ISAC also has a wide range of information on its portal (**FS-ISAC Portal**) to help firms increase and improve their cybersecurity efforts as well as communities and groups such as the SIRG and its councils to ask questions and share information with members at the FS-ISAC.

Compromised Discovered in Utility Software

The software developer Piriform recently discovered that its CCleaner, has been compromised. Piriform immediately updated CCleaner Cloud with a newer, clean version. Businesses and consumers should immediately download CCleaner v5.34 from the Piriform website (**Piriform**).

Users of CCleaner v5.33 on any system should remove the malicious version immediately, reimage machines or restore from backup, change all privileged passwords to prevent the risk of compromised credentials and immediately update to CCleaner v.5.34. While there are elements of this attack that could not be avoided by users, firms should still review patch management processes and utilize automatic updates where possible. To help manage this process, firms should also sign up for industry and manufacturer alerts where possible to know immediately when this type of situation occurs. The FS-ISAC has posted information regarding this compromised (**Tracking ID: 933909**) for members to review and use as a resource to help mitigate the problem.

Keren Elazari, Author of "The Future of Cybersecurity – a Hackers Perspective", Keynotes EMEA Summit

Keren Elazari, internationally recognized expert and author of *The Future of Cybersecurity – a Hacker's Perspective*, will keynote the 2017 FS-SIAC EMEA Summit on 30 October-1 November in London). Elazari will discuss cybersecurity and hacker culture. You don't want to miss this keynote or the 40 quality sessions we have lined up, into four session tracks:

> **Governance and Resiliency:** Learn about and discuss upcoming legislation and regulatory mandates on the sector, including General Data Protection Regulation (GDPR), revised Payment Services Directive (PSD2) and mandatory reporting requirements. Topics related to external regulation, internal risk management and hearing a CISO case study. Meet the new EMEA Business Resiliency Council (BRC) at the Summit and hear about FS-ISAC's efforts in exercising with regional organizations.

Technology and Operations: Hear about the latest trends in using technology to deal with internal risks and external threats. Learn from FS-ISAC staff and members on how to deal with the tsunami of information overloading your teams and integrating operations with intelligence.

Testing and Security Assurance: Explore topics on testing internal applications in accordance with software development life cycle (SDLC) and open web application security project (OWASP), penetration testing and discussing the regional trend of mandatory penetration testing from the regulator like CBEST (Bank of England Cybersecurity Framework) and TIBER (Threat Intelligence Based Ethical Red Teaming). Contribute to ongoing member discussions on dealing with increased regulatory scrutiny on cybersecurity operations.

Threat Intelligence: Review the latest information on current and emerging threats hitting the financial sector. Meet the EMEA Threat Intelligence Committee (ETIC) members and hear from FS-ISAC's Global Intelligence Office (GIO) on how FS-ISAC's intelligence offering is evolving.

Learn more about *session tracks* and plan your content agenda.

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**