FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Securities Industry Risk Group **April 2017**
Global Cybersecurity Brief **TLP: WHITE**

FS-ISAC Collaborates 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 Advisory of 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**).

Apache Struts Vulnerability

Last week, the Canadian government shut down their websites for filing federal taxes after a hack, preventing any attempts of stealing data (**Reuters**). The hack was due to a vulnerability in software known as Apache Struts 2. This software is commonly used in websites of governments, banks, and other organizations.

This vulnerability (**CVE-2017-5638**), allows a remote attacker to inject operating system commands into a web application through the "Content-Type" header.

The FS-ISAC is monitoring developments about widespread scanning and exploitation that was reported on March 9, 2017, and continues to be reported by various sources involving "Struts." The Struts Framework is a popular framework for developing Java-based web applications. Since the release of the vulnerability, FS-ISAC members have observed aggressive scans and attempted attacks. The FS-ISAC continues to monitor this incident and work with our members to aid in the successful detection and mitigation of this vulnerability.

Ransomware Attacks Dutch Parliament Websites

On March 28, 2017, the website of the Dutch Parliament's was attacked by ransomware (**Business Insurance**). A Dutch internet security firm, Fox-IT reviewed the attacks and believed that they were conducted by Turkish hacking groups. The Dutch news agency ANP reported that Turkish hacking groups are targeting the Netherlands in a potential political retaliation. The news agency also reported that the Dutch parliament took 'appropriate measures' to respond to the attack, but declined details.

Security Gaps Found in US Federal Agencies

Despite efforts by the US government to thwart cybersecurity threats, hackers continue to attack federal agencies. A report to the Department of Homeland Security (DHS) shows that 30,899 cyber incidents have been reported in 2016, including 16 breaches where personal data was compromised (**Bloomberg**).

The incidents included thousands of email phishing attacks, violations of policies by authorized users, loss or theft of devices and media, as well as attacks from a website and web-based applications. Of the 16 breaches, 10 resulted with employees taking personal information or other sensitive information. As mentioned in the report, the US State Department does not have 'an effective organizations-wide information security program'.

Firms should take the lessons learned from these incidents and consider improving their own cyber maturity by reviewing their data loss protection efforts, increase user training and implementing multifactor authentication.

Recent Bank Attacks Linked to North-Korean Based Hacking Group

Symantec has linked a recent cyber campaign targeting organizations in 31 countries to the Lazarus hacking group based in North Korea (**Reuters**). In a Symantec Blog post, researchers have uncovered digital evidence suggesting that the Lazarus group was behind the campaign (**NY Times**).

The campaign targets victims using a 'loader' software to install malicious programs to stage these attacks. The attackers exploited 'watering holes' to infect machines from certain areas (**SecurityAffairs**). The malware was programmed to infect visitors whose IP showed they were from 104 specific organizations based in 31 countries. The largest numbers were in Poland, the Brazil, Chile, Mexico and the United States. Polish banks confirmed their systems were infected after their staff visited the site of the Polish Financial Supervision Authority. Authorities made the decision to take down the infected site to avoid spreading the malware and 'secure evidence'.

Firms should take the lessons learned from these incidents and update anti-virus and malware software, educate users to be aware of possible attacks, and block known sites from which malicious codes can be executed.

Regulatory Items of Interest

The FS-ISAC participated on a panel with leaders from Commodity Futures Trading Commission (CFTC) at the CFTC's International Regulators Meeting in Boca Raton, Florida. The panel simulated a major cyber-attack affecting the futures industry, and how the futures exchanges and market participants, FS-ISAC and US and international regulators would respond. About 50 participants from 17 countries participated in the meeting which preceded the Futures Industry Association (FIA) meeting.

Registration Now Open for the APAC and Annual Summits

Registration is now open for both the Asian Pacific **APAC Summit**(3-4 April, 2017 in Singapore) and **Annual Summit** (30 April-3 May, 2017 in Lake Buena Vista, FL)! Don't miss your chance to attend!

The FS-ISAC Summits are focused around peer-to-peer networking and building relationships or circles of trust with financial services organizations. We invite you to attend and see what new sessions and exciting innovations are developing around information sharing amongst financial institutions and threat intelligence practices.

Register for the APAC Summit | **Register for the Annual Summit**

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,

Peter Falco and Richard Livesley

pfalco@fsisac.com rlivesley@fsisac.com

If you have any questions about this report, please contact the **FS-ISAC**.

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