FINANCIAL SERVICES | Information Sharing and Analysis Center

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

US Treasury Report Calls for Cybersecurity Harmonization.

In a testimony before a House Appropriations subcommittee (**C-SPAN**), Treasury Secretary Steve Mnuchin said that 'One agency should be named as the lead agency and coordinate amongst all the rest of them' on cybersecurity (**Investment News**).

Treasury Secretary Mnuchin released a report that recommends federal and state regulators harmonize cybersecurity regulations and improve coordination on examinations. (**US Treasury Report**). The report mentions that financial institutions and regulatory agencies share the same goal of maintaining the safety and soundness of the financial system by mitigating and protecting institutions and the sector from cybersecurity attacks, and that better coordination on cybersecurity regulation is needed to achieve this goal.

The Financial Services Sector Coordinating Council (**FSSCC**) has been advocating for such regulatory harmonization on cyber-topics. Of the Treasury report. As written it could be misinterpreted as a FSSCC report it says, "Treasury recommends that further coordination should occur on two fronts. First, financial regulatory agencies should work to harmonize regulations, including using a common lexicon. Second, financial regulators should work to harmonize interpretations and implementation of specific rules and guidance around cybersecurity."

Currently, there may be a risk of overlap in requirements for the various sub-market segments where some financial regulatory agencies have each finalized differing cybersecurity requirements that impact the same financial institutions. Coordination around these two important aspects of cybersecurity regulation will enable additional efficiencies in staffing personnel and resources related to regulatory compliance and oversight.

FS-ISAC Outreach

On June 23, 2017, FS-ISAC's Peter Falco participated on a panel at the North American Securities Administrators Association's (**NASAA**) Cybersecurity Roundtable titled '***Scaling the Threat: Cybersecurity Basics for those on a Budget***'. Peter and other panel members discussed how small and mid-sized financial firms, that may be significantly budget-constrained, can access cybersecurity resources, including via the FSISAC. The primary target audience was state-registered Investment Advisors, but discussions were relevant to other small-sized financial firms as well.

DHS and FBI Warns Against North Korean Hackers

On June 14, 2016, the Department of Homeland Security (DHS) and the Federal Bureau of Investigations (FBI) issued a joint technical alert of attacks by North Korean government hackers known as Hidden Cobra (**NetworkWorld**). This group is also referred to as the Lazarus Group, who in 2014 targeted Sony Pictures Entertainment. In the alert published by US-CERT (**US-CERT: TA17-164A**) technical details were explained about the tools these actors used to target the media, aerospace, financial and critical infrastructure sectors in the United States and globally.

In the alert, the DHS and the FBI also release indicators of compromise (IOC) associated with the malware DeltaCharlie that the North Korean government hackers use to manage its DDoS (distributed denial of service) botnet infrastructure. The report describes a list of 633 IP addresses in the IOC that are being used by Hidden Cobra for network exploitation.

The group has been busy targeting victims for the last eight years with malicious tools such as DDoS botnets, keyloggers, remote access tools and wiper malware. The group targets machines running older and unsupported versions of Microsoft Windows as well as exploit vulnerabilities in Adobe Flash Player and Microsoft Silverlight.

The alert advises firms to replace machines using older unsupported versions of Windows, updated vulnerable software and block the list of 633 IP address from accessing their networks.

New SEC Co-chiefs See Cybercrime as Biggest Market Threat

On June 8, 2017, the Securities and Exchange Commission named Stephanie Avakian and Steven Peikin as co-directors of enforcement (**Reuters**). The U.S. regulators are starting to track cybercrimes more closely after an increase of hackers breaking into brokerage accounts to steal assets or make illegal trades or for insider trading. The commission has seen an increase in the number of investigations involving cybercrimes and brokerage account intrusions. The duo stressed that the enforcement efforts at the SEC will continue to be 'vigorous' and any conflicts will not impede the division's activities. The dual enforcement role can help prevent problems by allowing officials to recuse themselves when conflicts of interest may exist. The also expect the SEC will continue to weigh whether corporate penalties are appropriate in certain cases.

QakBot Trojan Capable of Locking Out Users

According to IBM's X-Force team, a new variant of the QakBot financial trojan are locking out Microsoft Active Directory (AD) system user (**eWeek**). The lockout attacks can occur in different ways such as malware assisting the lockouts, to threat actors using stolen credentials and accidently locking out accounts. Researchers have found that the malware is attempting to spread through an infected network, then utilizes the credentials of the affected user which triggers the AD lockout issues.

Researchers state that QakBot is a modular, multithread malware with various components to implement online banking credential theft, and has the ability to subvert antivirus tools (**Security Intelligence**). If a company has a poor password policy or if the malware can guess the admin password, its features can increase disabling security software running on desktops utilizing the stolen admin password.

There are several actions firms can take to mitigate and prevent infection with the malware, such as improving web browsing hygiene by disabling online ads, and filtering macro execution in files that are sent via email. Other suggestions are:

- enforce complex passwords that users are prompted to change regularly
- modify domain accounts to not perform job tasks that can launch the payload of the malware
- create an emergency domain admin account with a complex password for safety purposes

These simple steps can stop most of the brute force attempts by the malware, and allow admins to connect into the AD environment and unlock infected accounts.

Cost of Cybercrime Continues to Rise

Researchers at Juniper research project that by 2022, the cost of cyber-attacks will cost business around the world $8 trillion USD (**ITPORTAL**). The report states that due to higher levels of internet connectivity and inadequate security, the threshold will be hit very soon (**Juniper**). Researchers also report that the number of personal data records stolen in 2017 will be around 2.8 billion and by 2020, it is expected to hit 5 billion.

The report also highlights that the biggest problem exists when companies try to integrate legacy systems with a new system, and don't pay attention to the security on their networks.

Firms should commit to spending time, money and resources to help resolve any known or potential security risks, and update any systems with the proper software patches or replacements. These small steps now, will hopefully save a lot in the future.

FFIEC Cybersecurity Self-Assessment Tool Updated

The Federal Financial Institutions Examination Council (FFIEC) released an updated version of the Cybersecurity Assessment Tool, commonly referred to as the CAT, during the week of May

30. The FFIEC provided an updated tool (**FFIEC Tool**) and appendices to help financial institutions to "identify their risks and determine their cybersecurity preparedness."

FS-ISAC and the FSSCC developed an automated tool for member institutions to use to complete the 2015 version of the CAT. FS-ISAC has received the updated, 2017 version of the FFIEC CAT and is evaluating the changes in the new version and working with members to make an updated version of the automated CAT tool available for download soon.

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**