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

Patch Released for a Severe Bug Found in VPN Software

On January 29, 2018, CISO Systems announced a critical vulnerability in their Adaptive Security Appliance (ASA) devices and Firepower Threat Defense (FTD) software (**CISCO**). The vulnerability allows an unauthenticated, remote attacker to execute code or cause a system to reload. The vulnerability received a perfect 10.0 on the Common Vulnerability Scoring System (**CVSS**) which is a global standard run by the industry group FIRST.

In the announcement, Cisco explained that an attacker could exploit the vulnerability by sending multiple XML packets to a webvpn-configured interface on an affected system allowing the attacker to execute arbitrary code or obtain full control of the system (**Cyberscoop**). The affected products are popular tools for protecting corporate networks and data centers. Firms are urged to apply security updates that resolve the vulnerability.

Millions of Leaked Credentials for Fortune 500 Companies Found on the Dark Web

A recent report by VeriCloud found that email credentials for about 2.7 million Fortune 500 employees was found on the dark web (**VeriCloud**). The report included data from a three year period, that looked at 27 million Fortune 500 employees and found the stolen credentials in multiple locations on the dark web, thus increasing the possibility that it was bought and used by malicious actors (**SC Media**).

The availability of these passwords on the dark web creates vulnerabilities for a corporation to any number of potential cyberattacks including spear phishing, and attacks that lead to malicious actors having direct access to corporate networks. Firms are advised to review or implement a strong password policy and instruct employees of the potential threats if using the same passwords for both corporate and personal use.

More Patches and Software Released for SPECTRE Vulnerability

Companies such as Microsoft and Google have released patches to help resolve the SPECTRE Vulnerabilities (**SPECTRE**). Microsoft has issued an out-of-band patch to fix problems from a buggy update (**Info Security**). The fix was issued on January 29, 2018 and covers Windows 7(SP1), Windows 8.1 and all versions of Windows 10 (**Microsoft Support**). This update can be applied by downloading it from the Microsoft Update Catalog (**Microsoft Update Catalog**) or via a registry setting change for advance users.

Google has released its Chrome 64 browser for Windows, Mac and Linux (**Bleeping Computer**). The new browser provides stronger pop-up blocking to protect unwanted content through redirects of website and more mitigations for the SPECTRE Vulnerability that can be used against browsers.

Firms should review the updates and new browsers and apply them to help mitigate the SPECTRE vulnerability on all corporate machines.

FS-ISAC Unveils 2018 Cybersecurity Trends

Cybersecurity continues to be a top concern for financial institutions globally. To help leaders and businesses understand cybersecurity trends across the globe, the FS-ISAC unveiled results of its 2018 CISO Cybersecurity Trends (**FS-ISAC 2018 Trends**).

Most critical defense

CISOs surveyed were split on their top priorities for securing their organizations against cyberattacks. Most (35 percent) of CISOs surveyed said that employee training is a top priority for improving security posture in the financial sector. Infrastructure upgrades and network defense are also prioritized by (25 percent) CISOs; and breach prevention by 17 percent. CISOs reporting into a technical function like Chief Information Officer (CIO) prioritize infrastructure upgrades, network defense and breach prevention. CISOs reporting into a non-technical function like the Chief Operations Officer (COO) or the General Counsel prioritize employee training.

Frequency of reporting
While cybersecurity used to be handled in the server room, it is now a board room topic. The study found that quarterly reports to the board of directors were most common (53 percent) with some CISOs (eight percent) reporting more than four times a year or even on a monthly. In the era of increasing security threats and vulnerabilities, CISOs know that keeping top leadership and boards updated regularly on these security risks and effective defenses is a top priority

Most CISOs report to CIO, not CEO
As security has increasingly become a concern for financial institutions, the role of the CISO has been thrust into the organizational spotlight. The study found that the majority of CISOs don't report to the CEO; the top cyber chain of command is more likely to be the CIO; followed by Chief Risk Officer (CRO) and then COO. Sixty-six percent of CISOs report into the CIO, CRO and COO. Only eight percent of CISOs report into the CEO. The study found that the reporting relationship did not impact frequency of reporting to the board of directors on cybersecurity.

Recommendations for 2018
FS-ISAC recommends training employees should be prioritized for all CISOs, regardless of reporting structure because employees serve as the first line of defense. Employee training should include awareness about downloading and executing unknown applications on company assets, and in accordance with corporate policies and relevant regulations, and training employees on how to report suspicious emails and attachments.
FS-ISAC encourages more frequent and timely reporting to the board of directors to ensure businesses maintain an 'at the ready' risk posture and that cyber practices are transparent to board members.

As the threat landscape shifts, FS-ISAC recommends CISOs having expanded reporting responsibilities or dual-reporting responsibilities within the corporate structure to ensure critical information flows freely. Free and direct flow of critical information to the CEO and to the board of directors will help increase transparency and facilitate faster decision making.

All participants in the FS-ISAC CISO survey are FS-ISAC members, serving as current CISOs for their respective financial institutions around the world. This is the first year FS-ISAC conducted the CISO Cybersecurity Trends Study.

The FS-ISAC recently announced a new FS-ISAC Board Presentation Briefings service. An FS-ISAC executive can make an interactive presentation to your board of directors for a fee. (**FS-ISAC Board Presentation Briefings**).

2018 FS-ISAC Annual Summit

The 2018 FS-ISAC Annual Summit will be held at the Boca Raton Resort & Club from May 20 - 23, 2018. FS-ISAC has reserved a block of rooms for its members at a group rate (**More Details**). Please make sure to reserve your room now, as the block will fill quickly. Reservation requests for the FS-ISAC Annual Summit will be accepted through Friday April 27, 2018. The block is available up to this date or until the block is full. Reservations requests received after April 27 are on space and price availability.

FS-ISAC Summits are a source of nutritional brain food and give you the energy to tackle your compliance, security and technical challenges. For more information on the summit or hotel reservations, please visit the summit site (**Summit Overview**).

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**