FS-ISAC Securities Industry Risk Group **April 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 cybersecurity 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**).

Massive DDoS Attacks Affect Thousands

On March 5, 2018 researchers discovered a massive Distributed Denial of Service (DDoS). The risk came by way of a vulnerability in Memcached, an open source utility designed to cache in RAM frequently used web pages (**DataBreach Today**). The utility was never designed to be internet-accessible and requires no authentication to access, but some instances such as Linux based servers have left TCP or UDP Ort 11211 open by default to internet-borne requests. Attackers have begun demonstrating how misconfigured servers can be attacked.

Researchers have also noted the Memcached flaw could be used for more than DDoS attacks (**BankInfoSecurity**). Security experts warn that open Memcached ports could be abused by attackers to reveal a firm's data, modify it and reinsert it into the cache without the Memcached owner knowing.

If firms are running the Memcached utility, they should review their server configurations, contact their internet service providers (ISP) to see if they are deploying exploitable port filters as well as look at their firewall rules and add the filters.

Phishing Campaign Targets SWIFT Users

Researchers at Comodo Threat Research Lab have discovered a new form of phishing attack that is targeting users of the SWIFT financial messaging services (**COMODO**). The report states that victims receive an email disguised as a message from SWIFT about a wire transfer to another bank account and are directed to click the attachment for more details of the fake transfer (**Media Post**).

The analyst's report that these types of messages are the '**Trojan.JAVA.AdwindRAT**' malware. Once this malware permeates into a user's systems, it modifies the registry, spawns many processes, checks for an antivirus installation and attempts to kill its process. The malware also checks for any instance of an anti-adware tool, then delivers the malicious executable files and makes a connection with a domain on the Tor network. The last step is the malware disables the Windows restore option and User Account Controls, which are used to prevent the installation of programs of which the user is unaware.

Firms are advised to review the researchers blog, understand how the malware can impact the desktop as well as warn and instruct end users of the phishing campaign

SEC Releases New Guidelines on Cybersecurity

On Wednesday February 21, 2018, US Securities and Exchange Commission (SEC) issued new guidelines on cybersecurity disclosures for publicly traded companies which included suggestions for adjusting insider trading policies to account for investigations into cyber breaches (**WSJ**). The guidance expands on 2011 guidance by emphasizing the importance of cybersecurity policies and how insider trading bans apply to a cybersecurity event (**Pensions & Investments**). The guidance also calls for greater clarity, more detailed information around cyber risks and breaches, and discourages companies from delaying disclosures due to continued investigations. Even with the new rules, companies are unlikely to disclose a breach to investors before it becomes public through other channels, such as media reports of state reporting requirements.

Firms should review the guidance that was issued (**SEC**) and compare it to their existing policies and procedures to ensure they explicitly account for information related to cybersecurity risks and incidents.

Software Patch Released to Fix Remote Desktop Vulnerabilities

Microsoft has released more than 70 patches, of which 15 are critical ones, related to an exploit authentication in the Microsoft Remote Desktop Protocol. The updates released for products such as ASP.NET, Core, >NET Core, PowerShell Chore, Office, Internet Explorer, Windows and Exchange Server (**SC Magazine**). One significant update was a vulnerability in the software company's Credential Security Support Provider protocol (CredSSP). This vulnerability could allow a hacker to gain control of a domain server and other servers within the network.

The CredSSP vulnerability affects all Windows versions starting with Windows Vista. Researchers found that an attacker could exploit the flaw in a man-in-the-middle attack that would allow them to abuse the protocol and remotely run code on the compromised server. While no attacks have been detected in the wild, the vulnerability is a big deal and firms should ensure workstations and servers are patched with the updated software

---

Six-Year-Old Malware Discovered

Researchers from Kaspersky Labs have discovered a malware named 'Slingshot' that is so stealthy that it has remained hidden for six years (**ARS Technica**). Slingshot received its name from text found inside some of the recovered malware samples. Researchers state the malware is the most advanced attack platform ever discovered and was likely developed on behalf of a well-resourced country.

Researchers still don't know how the malware infects all its targets, however the threat actors got access to routers made by MikroTick and planted the malicious code. Specifics on how the malware was loaded are still unknown, but researchers believe that the malware was loaded using the manufacturers configuration utility. Researchers also mentioned that Slingshot may have used other methods, including zero-day vulnerabilities to spread. Slingshot conceals itself in many ways, one way is the use of an encrypted virtual file system in an unused part of the hard drive. This method of segregating malware files from the file system of the infected computer increase its chances of not being detected by antivirus engines.

The main purpose of the malware seems to be espionage, where the malware logs desktop activity, clipboard contents, keyboard data, passwords and data of USB connected drives. Firms should review the Slingshot FAQ page (**SecureList**) to understand the malware and suggested methods to help mitigate it.

Horror Show for Victims of Annabelle Ransomware

Named after the horror film "Annabelle", this ransomware has been a horror show wreaking havoc of its own on infected computers, even though it was built on a version of the 'Stupid' Ransomware. Luckily this version of ransomware can easily decrypt files (**Bleeping Computer**). However, Annabelle negatively impacts the infected PC in other ways such as disabling Windows Defender, turning off the firewall and shutting down other security programs (**SC Magazine**). The ransomware also tries to spread itself via USB drives and overwrites a computer's master boot record with a boot loader.

2018 FS-ISAC Annual Summit

The 2018 FS-ISAC Annual Summit will be held at the Boca Raton Resort & Club, in Boca Raton, FL from May 20 - 23, 2018. FS-ISAC has reserved a block of rooms at a group rate (**More Details**). FS-ISAC Summits are a source of nutritional brain food and give you the energy to tackle your compliance, security and technical challenges. The complete brochure for the session is available online to view sessions. (**Summit Brochure**)

Members may be interested in the following sessions:

Day	Time	Session Name
May 21	8:30AM	FS-ISAC 101 and Meeting BRM
May 21	8:30AM	Securing a City's Digital Future: NYC Cyber Command
May 21	9:30AM	Strength in Numbers: Sharing Information Across Intel Silos
May 21	2:45PM	Data Loss Prevention in Day to Day Business
May 21	2:45PM	The TICS are Talking
May 22	8:45AM	5 Steps to Protect Financial Services Data on Mobile Devices
May 22	9:30AM	Making a Difference in the Financial Sector-Automating Information Exchange and Defense
May 22	10:45AM	Drowned in Intel? How Small and Midsize Financial Institutions are Getting Their Inbox Back
May 22	10:45AM	Auditing Cyber Security
May 22	11:30AM	Incident Response: War Stories and Pragmatic Guidance
May 22	2:15PM	Account Takeover Analysis and Mitigation
May 22	2:15PM	Cyber-risk, Market Failures, and Financial Stability
May 22	3:30PM	Building a Robust Security Awareness Program
May 23	8:15AM	The Buck Stops Here: Role of CEOs and Boards in Addressing Cyber Threats
May 23	1:30AM	TLS 1.3: The Short and Long-Term Impacts on Security Operations
May 23	3:45PM	The Evolution of Your Third-Party Risk Program

Please make your reservations now, as the main hotel and the back-up hotel are full, although waiting lists are available. A third hotel has been secured and is accepting reservations. For all details, please visit the Summit website. Reservation requests for the FS-ISAC Annual Summit will be accepted through Friday April 27, 2018. Reservations requests received after this date are on space and price availability. 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**