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

FS-ISAC Launches CERES Forum

The FS-ISAC announced the launch of the CERES (**CE**ntral banks, **RE**gulators and **S**upervisor) Forum effective July 1, 2018. The CERES Forum is a new information sharing group for central banks, regulators and supervisors to share information impacting global security and resiliency. The Forum is the premier global platform bringing together these entities to guard against ever-growing cyber and physical threats and to meet their unique needs.

The impact of cyber-attacks, including the 2017 WannaCry, data breaches and account takeover attacks leveraging global payments systems against central banks and regulators demonstrate that security is a global concern. The CERES Forum will help these entities become more effective in defending against attacks that could potentially impact the global financial services sector as well as the world's economies.

The new forum is separate from the FS-ISAC community of banks, credit unions, insurance companies, investment companies and other financial institutions, which provides a trusted space for private financial institutions to share information.

A new standalone secure portal and processes will ensure FS-ISAC member confidentiality.

The mission of the CERES Forum is to provide a trusted means for central banks, regulators and supervisors to:

- Share best practices related to regulatory and compliance controls
- Gather useful feedback from industry experts about which controls are most effective
- Rapidly Distribute information on cyberthreats, vulnerabilities, incidents and other threat intelligence that could impact financial services, including attacks that target central banks, regulators and supervisors themselves

Although employees working in operations from over three dozen central banks, regulators and supervisory entities are already members of FS-ISAC, this is the first time a community is being created to focus on the needs of supervisory and regulatory employees. The Monetary Authority of Singapore (**MAS**), which collaborated with FS-ISAC to establish an Asia Pacific Regional Intelligence and Analysis Centre in 2017 to encourage sharing and analysis of cybersecurity information between financial institutions in the region, also played a key role in conceptualizing the CERES Forum. For more information on the CERES Forum and how to join the community, please visit the CERES Forum website for more information (**CERES Forum**).

Flaws in PGP and S/MIME Can Reveal Past Encrypted Emails

Existing flaws in popular email programs like macOS mail and Outlook make it possible for attackers to access the plaintext of messages encrypted using Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) standards (***Electronic Frontier Foundation***). Dubbed 'EFAIL', the flaws have been present for more than a decade. To exploit them, an attacker would require some type of access to an encrypted message. At this point in time there are no fixes for the issues. Researchers who disclosed the flaws recommend temporarily disabling PGP and S/MIME in email applications

---

Fake GDPR Alerts are Latest Phishing Attack

In its latest quarterly fraud report, RSA shows 'newsjacking' becoming an increasingly powerful method for phishing attacks (***RSA***). Recent news items are being leveraged to fuel new phishing campaigns as analysts believe attacks will send fake alerts about the EUs General Date Protection Regulation now that enforcement has begun (***BankInfoSecurity***).

The RSA report contains global and consumer fraud attack data plus analysis from the company's fraud and risk intelligence team for the Q1 2018. Firms should download and review the information published in this report as the information provided will help firms share information and provide awareness with all employees.

Six Month Campaign Leads to 74 Arrests in BEC Scam

The FBI, Department of Homeland Security, the Treasury Department and other US and global law enforcement agencies arrested 74 individuals for perpetrating business email compromise schemes (BEC). The coordinated global law enforcement effort called "Operation Wire Wire" lasted six months and led to the arrests of 42 suspects in the States, 29 in Nigeria and the remaining three in Canada, and included a seizure of $2.4 million. It also led to the 'disruption and recovery' of about $14 million in fraudulent wire transfers (**BankInfoSecurity**).

BEC scams typically involve messages that impersonate a company official requesting urgent payment of funds, resulting in fraudulent wire transfers or checks. Firms should ensure spam filters are updated on email servers, educate employees to confirm and verify if strange or abnormal transfer request come in via email.

MnuBot: A New Banking Trojan

On May 29, 2018 researchers at IBM released a technical report highlighting they have spotted a new banking trojan named MnuBot, which uses some typical tricks to avoid easy detection on compromised hosts (***Security intelligence***). As per the researchers, MnuBot has the same capabilities as most Remote Access Trojans (RATs), allowing an attacker to gain remote access as well as display fake windows of various banks on infected machines. As per the report, this new banking Trojan is composed of two main components that are tasked for two stages. In the first stage, the malware searches for a file called ***Desk.txt*** within the ***%AppData%Roaming*** folder and continually checks the foreground window name in the new desktop searching for bank names in its configuration. The second stage will query the command and control server, which is executable according to the specific bank name that was found. The trojan uses a remote Microsoft SQL database as their C2 server to evade detection of malicious activities on the endpoint security devices. As per the researchers, MnuBot is more actively targeting internet users in Brazil and Latin America to perform illegal transactions on victim's open banking sessions. FS-ISAC members with more information about the malware or indicators are encouraged to share via portal or email distribution lists.

Software Patch Addresses Code Execution Vulnerability

Last week, software maker Microsoft released a software patch to address a remote code execution affecting the 'wimgapi' library, which is used to perform operations on Windows Imaging Format (WIM) file format (**SecurityWeek**). An attacker can exploit the flaw using a specially-crafted WIM image to achieve direct code execution. The attacker could execute malicious code with the same access rights (**CVE-2018-8210**). They could also crash the system with a denial of service attack, because WIM files do not have a registered file type handler (Open With) by default. On a side note, the issue cannot be triggered if the user double clicks on a WIM file, unless the file handler is registered first.

To address this issue, the software maker released an update that corrects the vulnerability. There are no mitigation plans or workarounds and only installing the patch will resolve the issue. Firms should read the CVE mentioned above and develop a plan to implement this patch to any Windows machines within their firm.

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**