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**).

U.S. Regulators Give Guidance to Advisory Firms on Cybersecurity

The US Securities and Exchange Commission encourages advisory firms to protect their information systems from hackers. According to results from a new round of cybersecurity examinations by the Securities and Exchange Commission (SEC) advisors need to do a better job abiding by their stated cybersecurity policies and correct all vulnerabilities that are revealed in tests performed by firms (**InvestmentNews**).

The commission's report also advised that firms need to do a better job of keeping patches up-to-date on their systems (**SEC Exam Risk Alert**). During the period of September 2015 through June 2016, the commission examined advisory firms and broker dealers (75 in total) and shared their results in the alert. The SEC staff found that few firms had applied system patches that included critical security flaws to their systems. The report also mentioned that advisors were doing a better job than broker dealers with formal procedures for verifying customers' identities when their clients request an electronic transfer.

Recently SEC chairman Jay Clayton says that public traded U.S. businesses must better describe to investors the cybersecurity risks their firms face (**BankInfo Security**). At a panel discussion in Washington, Mr. Clayton said he will continue the commission's focus on cybersecurity as a a top enforcement priority.

Firms should review and update all their cybersecurity related procedures and ensure systems are update to date with the latest patches and security fixes.

TrickBot Malware Targets France and the UK

The FS-ISAC has received new reports of the TrickBot malware related activity. Analysts at FS-ISAC have been tracking TrickBot phishing emails that are claiming to be from financial institutions. There has been a recent new TrickBot campaign, reportedly targeting the French, UK and US finance sector (**SecurityZap**). At one point 75,000 phishing emails were sent in 25 minutes, demonstrating the scale of the problem and the intent of the attackers. Members are encouraged to log into the portal for the latest indicators of compromise (IOCs) and mitigation advice (**FS-ISAC Portal**) to prevent this malware from attacking their systems.

FS-ISAC Releases Tips to Defend Against Ransomware

In light of recent global ransomware attacks, FS-ISAC released a publicly available tip sheet on ransomware (**FS-ISAC**). This paper is in addition to the extensive information sharing and analysis by the FS-ISAC and others in response to the WannaCry ransomware attack in May, and another significant event in late June targeting Ukrainian institutions and other institutions.

Tips and recommendations include:

- Isolating infected systems from your networks;
- Keeping operating systems and antivirus software up-to-date;
- Testing backups in a real-world environment; and
- Reporting any ransomware to law enforcement within 72 hours.

Patches Released for New Outlook Vulnerabilities

Microsoft has release patches for several important vulnerabilities affecting it email and calendar application Outlook (**Security Week**). While none of the flaws have been disclosed or have been exploited attacks, the security holes are related to the Click-to-Run(C2R) technology used to install Office Products. One vulnerability is a memory corruption that can be leveraged for remote code execution (**CVE-2017-8663**). This weakness can be exploited by getting an Outlook user to open a specially crafted file that is sent via email. An attacker who successfully exploits this vulnerability can take control of the affected system and can install programs, view, edit or delete data, as per the Microsoft advisory.

Another vulnerability (**CVE-2017-8571**) can lead to arbitrary code execution. This vulnerability can bypass the controls that exists, due to the way Outlook handles input. An attacker can exploit the flaw by fooling the user into opening or interacting with a specially crafted document.

A third security hole is an information disclosure bug that exists because the application improperly discloses memory content (**CVE-2017-8572**). If the attacker knows the memory address of a targeted object, they can trick the target into opening a special file to obtain information that be useful for accessing the victim's computer and data. Microsoft has said that the patches also address several know issues in their June 2017 security updates. It is advised for firms to install these recommend patches to correct these vulnerabilities. Firms should ensure that once that patches are installed the Outlook application runs with no issue.

Vulnerability Found in Hong Kong Trading Apps

The Mobile Security Research Lab of Hong Kong released the results of a study of 140 Android Stock Trading Mobile Applications (**MSR Labs**). MSR found that over a third of apps are insecure (**MSR Results**). Applications evaluated were provided by "participants of the Hong Kong Exchanges and Clearing Limited (HKEX)". The lab followed the OWASP Mobile Top 10 of 2016 criteria for evaluation (**OWASP**).

The study found that most of the apps had no Multi-Factor Authentication (MFA), over a third did not use proper encryption for credential or transaction data, and over 86% of the apps did not meet the Top 5 severity evaluation criteria. The study opined that the vulnerabilities found contributed to the $100 million in unauthorized trades reported by the Securities and Futures Commission (SFC) in Hong Kong over the course of 18 months. The FS-ISAC cannot confirm this finding, due to incomplete data on the 27 "cybersecurity incidents" reportedly responsible for the losses.

Separately, Android's latest security bulletin (**Android.com**) included critical vulnerabilities in media framework that could allow remote execution of arbitrary code within the context of a privileged process (**CVE-2017-0714/0723**). Integrating security into the mobile application development process early on will help members establish secure mobile apps, and FS-ISAC encourages best practice sharing between members

EMEA Summit – Keynote Announced and Session Previews on the Hidden Face of Cybercrime and Money Muling

The 2017 FS-SIAC EMEA Summit (30 October-1 November | London) keynote, *The Future of Cybersecurity – a Hacker's Perspective*, will be delivered by internationally recognized researcher, author and speaker Keren Elazari! Join Elazari on Monday 30 October as she discusses all matters related to cybersecurity and hacker culture. You don't want to miss this keynote or the great sessions we have lined up, such as these high-quality, financial sector-relevant sessions:

Money Muling | The session will review a real case study of a criminal business – with very little technical expertise – monetizing stolen credit card data. The presenter, a former law enforcement officer, will talk to how the case was investigated, how they identified the money mule network behind the thefts, and eventually how LE arrested the perpetrators. The speaker will also take the audience through a global law enforcement exercise that examined the "cradle to grave" use of the dark web to buy stolen login credentials and monetize them**.**

Offline and Local: The Hidden Face of Cybercrime | The conventional wisdom is that cybercrime is a largely anonymous activity that exists essentially in cyberspace. The supposed anonymity of attackers feeds into a narrative that cybercrime is strange, new, ubiquitous and ultimately very difficult to counteract. The central purpose of this presentation is to dispute this view. When one looks for it, there is actually a strong offline and local element within cybercrime, alongside the online dimension. In order to investigate this claim and its implications for policing, the core of this presentation is dedicated to a case study from Romania.

Registration is open - **register today**, **make your travel arrangements** and **learn more**.

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**