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 Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

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.

Presentations Announced for FS-ISAC Americas Fall Summit

Join us this fall for another great lineup of presentations at the FS-ISAC Americas Fall Summit this 17-20 November in Washington, DC. The three-day summit will bring together around 800 thought leaders, executives and members building stronger relationships through thought provoking sessions on topics including security and technology operations, threat intelligence, emerging technologies, fraud, outsourcing, resiliency, and more.

Attendees are encouraged to attend these interactive sessions. A few sessions of interest for attendees include:

- *Opening Keynote Investigative reporter Brian Krebs who writes about cybercrime at the award-winning Web site KrebsOnSecurity.com*
- *Fighting BEC Cybercrime at Scale*
- *Compliance in Cloud: Paced Migration is Key*
- *Protecting your Riskiest Asset in the Cloud: Office 365*
- *S&P's Journey to Build a Security-First Culture*
- *Traveling is Risky Business: Developing a High-Risk Travel Program*
- *Silver Showcase: Destructive Malware – Lessons from the Trenches*
- *Building the Bridge between Security and the Business*
- *Use-Case for Simplifying Cybersecurity Regulatory Compliance*
- *Making Cloud the Most Secure Environment for Financial Services*
- *Mobile Risk and Compliance in a Post-Perimeter Era*
- *The Potential Impact of Deepfakes on Market Manipulation*

Registration is now open for FS-ISAC's 2019 Americas Fall Summit, 17-20 November in Washington, DC. The Summit agenda includes numerous concurrent track discussions and plenty of networking opportunities. Register today.

Hackers Attack SSL VPNs

Hackers have been hunting for vulnerable SSL VPNs specifically manufactured by Pulse and Fortinet in response to discovered security flaws. (BankInfoSecurity). Security experts have noticed a surge in scanning attempts by attackers trying to locate and automatically hack these devices, exploiting known flaws that allow them to steal passwords and other sensitive data. If a hacker obtains a password from these devices, he can gain access to an organization's networks and resources.

Manufacturers recommended that owners of these devices install these updates as quickly as possible. There are about 42,000 Pulse Secure SSL VPN endpoints seen online and more that 14,000 of them are in the United State and are not updated with the security fix.

Pension Fund Reports $4.2 Million Theft

Reports from The Oklahoman, a Oklahoma City based daily newspaper, state that the Federal Bureau of Investigation (FBI) is conducting an investigation of a cyber theft of $4.2 million in funds from the pension system for retired Oklahoma Highway patrol troopers. A noticed posted on the Oklahoma Law Enforcement Retirement System website said it has notified the FBI, although couldn't comment on details of the breach. The article reported that the stolen pension funds will be recovered and no pension benefits to members or beneficiaries were impacted or are at risk. The attack took place on 26 August, when an employee's email account was hacked.

A similar attack occurred regarding pension funds in Pennsylvania where hackers stole about $100,000, as well as a separate cyberattack in Iowa. State pension and payroll systems are tempting targets for hackers, as they contain large sums of money (as well as outdated technology), which contributes to the biggest vulnerability to any of these organization - its employees. Firms should advise and educate employees on tricks and schemes hackers utilize to attempt access into systems or transfer funds to other accounts, such as phishing schemes and business email compromise.

Bulgarian Man Sentenced in Phishing Campaign

A Bulgarian man has been sentenced to nine years in prison after pleading guilty in connection with his role in running a large scale phishing campaign that scammed victims out of $51 million USD over several years (BankInfoSecurity). Svetoslav Donchev was arrested by Bulgarian and Metropolitan police at his home in Pleven, Bulgaria where he lived with his parents. Investigators also confiscated a computer that contained details of the phishing scheme. Donchev was extradited to the UK and he pleaded guilty to five charges. Donchev and the unnamed cybercriminal gang targeted over 50 UK companies, stealing personal and financial data on as many as 500,000 individuals.

The criminal activity facilitated the compromise of hundreds of thousands of victims' personal details, including banking credentials and other financial information. Investigators are not clear when this scheme started, but investigators believed that Donchev helped create website scripts that were designed to look like legitimate webpages but were connected to servers controlled by the criminal gang. Victims were sent phishing emails that claimed their accounts needed verification to allow for a cash refund from the company that had its websites spoofed. Those emails contained links back to phony websites. The credential information was then sold on the dark net sites. Donchev also created software to help the phishing email bypass security features in various web browsers.

Zero Day Vulnerability Found in Internet Explorer

Last week Microsoft release an emergency security update to patch a vulnerability in Internet Explorer web browser. The flaw was reported to Microsoft by a Google security engineer (Computerworld). The security bulletin that accompanied the release of the patch explained the vulnerability was a remote code vulnerability, where a hacker could introduce malicious code into the browser (Microsoft). Remote code vulnerabilities, also called remote code execution, or RCE, which are very serious. Microsoft explains a scenario where an attacker could host a specifically crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website by sending an email.

While the browser was demoted with the release of the Window 10, the software company to continue to support the browser, particularly version 11 which remains necessary in many enterprises and organizations for running older web applications and intranet sites. Firms that continue to use Internet Explorer should apply the patch provided by Microsoft.

About FS-ISAC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is an industry consortium dedicated to reducing cyber-risk in the global financial system. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to - peer network of experts to anticipate, mitigate and respond to cyberthreats. FS-ISAC has nearly 7,000-member firms with users in more than 70 countries. Headquartered in USA, the organization has offices in the UK and Singapore. To learn more, visit www.fsisac.com. This newsletter is not intended to replace the benefits of joining FS-ISAC's member-based organization. Please consider joining if you're not already a member.

Thank you,

FS-ISAC SIRG Team

If you have any questions about this week's report, please contact the FS-ISAC SIRG.

This newsletter contains content developed by FS-ISAC as well as links to content developed by third-parties.

FS-ISAC makes no claims or warranties as to the accuracy of information provided by third-parties. All copyrights remain with their respective owners.

Financial Services Information Sharing and Analysis Center

fsisac.com