**FS-ISAC Securities Industry Risk Group Global Cybersecurity Brief** | **February 2019 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.

---

## Threat Predictions for 2019

The FS-ISAC Intelligence Analysis Team (IAT), in conjunction with some of FS-ISAC's security vendors, published threat predictions for 2019:

- Digital skimming is projected to increase in 2019 due to the rise of compromised credit cards by cyber criminals who are likely to exploit online payment systems.
- Artificial intelligence (AI) is projected to create new malware that could evade security controls. With malware components so widely available online, industry experts believe further development of malware to evade detection and circumvent protections will become more commonplace.
- Compromised Internet of Things (IoT) is projected to increase due to vulnerable routers and devices in homes and businesses. Use of the Mirai malware variants and attacks on smart devices are likely to continue. The high adoption of voice-controlled digital assistants are likely to be prime targets. As the intended controller of connected smart devices, this could lead to increased distributed denial of service (DDoS) and command and control (C&C) attacks.
- Spear phishing attacks targeting executives are projected to continue given how effective they are for malicious actors to gather information, gain access to company systems and dupe employees in sending false payments to these thieves. Analysts believe that there will be an increase in targeted spear phishing at the lower levels of an organization due to their lower exposure to the attack.

## US Brings Charges in EDGAR Hacking Case

On January 15, 2019, the US Securities and Exchange Commission (SEC) issued a **press release** regarding charges brought on a suspected Ukrainian hacker and several traders scheming to trade on corporate earnings news that could prematurely influence securities prices stolen from the Commission's EDGAR database. The charges against 10 defendants, including two charged criminally, relate to a suspected 2016 intrusion into EDGAR, the SEC's corporate filing system used by public companies and money managers, (***Reuters***) resulting in the heist of over $4 million USD. Two of the hackers were charged with computer fraud, wire fraud and conspiracy in a 16-count indictment filed with the federal court in Newark, New Jersey. The SEC filed related civil charges accusing six individuals and two companies in the United States, Russia and Ukraine of reaping these gains from May to October 2016.

The Department of Justice said the conspirators used a phishing attack to steal filings and install malware on SEC computers, as well as intercepted test EDGAR submissions which included real earnings information. Firms are advised to ensure all systems are up-to-date regarding malware detection software: to alert and train staff on phishing attacks and when submitting filings and reports to the EDGAR system confirm that test data does not contain actual and valid informaton.

## Don Cardinal Named Head of Financial Data Exchange (FDX)

On Dec. 13, the Financial Data Exchange (FDX) ***announced*** the appointment of Don Cardinal as Managing Director. In this new role, Cardinal will direct the daily operations of FDX and engage with the broader financial services and fintech communities to fulfill the organization's mission to develop and implement a financial industry standard for secure data sharing. Cardinal will be responsible for charting the roadmap for FDX's Durable Data API (DDA) and technical frameworks, while also expanding FDX membership among a growing list of financial institutions, aggregators, fintechs and industry groups (***DDA Information***). Cardinal brings more than 20 years of industry experience to the FDX role, having most recently served as a Senior Vice President in Global Information Security at Bank of America.

## New Ransomware Launches Phishing Attack

Researchers at MalwareHunter Team have discovered a new ransomware campaign that offers the victim more than one way to pay a ransom and obtain the decryption key. (***SC Magazine***) The different payment options now include PayPal; if the victim chooses PayPal and follows the link provided, they will end up on a phishing page where their account login credentials are then stolen. The fake PayPal page also asks for the victim to confirm details of the credit card they have associated with that account so the attackers steal this information as well.

Firms are advised to update their malware detection software, make employees aware of this attack and report back to IT staff immediately of any incident.

## FS-ISAC Cyber-Range Ransomware Exercises

Cyber-range exercises offer FS-ISAC members a more technical, hands-on keyboard experience that provides greater interaction and sharing between members in a way that helps raise capability, maturity levels and resiliency across the sector. FS-ISAC has partnered with ManTech to build a network environment and facilitate the event. Events for 2019 have been announced, please visit ***FS-ISAC*** for additional details.

### Upcoming Cyber-Range Exercises

- February 13, 2018| Zurich | **Register**
- February 28, 2018 | Online | **Register**
- March 5, 2018 | Toronto Exchange (TMX) | **Register**
- March19, 2018 | Federal Reserve Bank of Atlanta | **Register**
- April 2, 2018 | Federal Reserve Bank of Cleveland | **Register**
- July 25, 2018 | Federal Reserve Bank of Chicago | **Register**
- August 22, 2018 | Federal Reserve Bank of St. Louis, MO | **Register**

## 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. Please consider joining if you're not already a member.

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**