FS-ISAC Securities Industry Risk Group Global Cybersecurity Brief

November 2018
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.

Financial Data Exchange (FDX) Launched

FS-ISAC, in conjunction with several financial institutions, fintech firms and industry groups announced the launch of the Financial Data Exchange (***FDX***), a non-profit organization to unify the financial sector around the secure exchange of financial data. FDX will address common challenges regarding the way the industry shares consumer account information for data aggregation to enhance security, innovation and consumer controls. FDX is a subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

FDX has introduced an interoperable standard and operating framework centered on an application programming interface (API), called the Durable Data API or DDA, unveiled by FS-ISAC earlier this year (***FS-ISAC***). DDA is a product of the FS-ISAC Aggregation Work Group. DDA will benefit consumers, financial institutions and fintech companies. Consumers will have better control over their personal financial data through improved access authorization options. When permissioned by consumers, financial institutions will have a simple, consistent process for securely sharing consumer data with fintech and other companies. (***Full press release***).

Data Breach Exposes Information of 30K Employees

Early last month, Pentagon officials were alerted by their third-party providers of a data breach that affected its personnel (***Forbes***). Hackers had gained access to personal information and credit card numbers. The data was stolen from a system that maintained travel records operated by a third-party contractor. While the investigation is ongoing, the final number of employees affected could increase significantly. It is not known when the attack occurred, and the third-party vendor has not been named.

Firms should take necessary actions to review and update third party controls, ensure that vendors have proper systems and procedures in place to protect customer information.

Fileless Malware on the Rise

Fileless malware attacks are not new, but the technique is being adopted more. Researchers at Microsoft say that the move to Fileless assaults are ten times more likely to succeed compared to other methods (**SecurityWeek**) and is the next logical step to other types of attacks, especially since most antivirus solutions have become increasingly efficient at detecting malicious executables.

The Fileless malware attacks remove the need of relying on physical files and improves stealth and persistence of the attackers. For the attacker, this means the discovery of a new technique for executing the code usually abuses tools that are already available on the platform, an example being Microsoft HTML Application Host (MSHTA.exe).

Firms should utilize security and antivirus programs that not only scan for malicious executables, but also have features that include system behavior monitoring, memory scanning, and boot sector protection, to detect and terminate threat activity at runtime.

SEC Warns Firms to Strengthen Cyber Defenses

The US Securities and Exchange Commission (SEC) warned public companies they could be in violation of federal law if they do not tighten cybersecurity controls. The commission's warning came after an investigation to determine if nine companies which had been victims of cyber-related frauds had enough accounting controls in place as required by law. The reported fraud did not include any use of a sophisticated design in these attacks, but rather used technology to detect human vulnerabilities in the control system. Tactics such as business email compromise were used to attack firms, by posing as customers or senior management to trick staff into sending company funds to bank accounts controlled by the would-be criminal (***Reuters***).

The SEC did not fine the nine companies, but the Commission's report emphasized that all public companies have obligations to maintain enough internal account controls and should consider cyber threats when

fulfilling those obligations. These nine companies were not identified, but the failings on internal controls were discovered when vendors reported to authorities of nonpayment on several outstanding invoices.

Regulators and lawmakers are increasingly focused on the risks cyber criminals pose to companies and their customers. Following a series of high- profile attacks on companies the commission updated guidance on how and when companies should disclose cyber security risks and breaches. Firms should review the latest published guidance from the SEC and ensure their accounting controls are updated and thoroughly tested as well as educate staff about these risks.

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 are to be announced soon, visit fsisac.com/Exercises-CyberRange for additional details (***FS-ISAC***).

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**