Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – January 2020

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.

GDPR Breaches Relate to Millions in Fines

After a year and a half since the General Data Protection Regulation (GDPR) came into existence, companies have been **fined millions of dollars** for various data breaches. According to analysis, the top 10 biggest GDPR fines combined amount to over $400 million USD. The top three biggest breaches make up almost 90% of the combined sum, with no financial services firms being named in the top three.

The biggest fines were against an airline company for $225 million whose data breaches revealed financial details and sensitive personal information of its customers. The second largest fine was against a major hotel, where personal data of 339 million customers was stolen. It was later determined that the breach was made possible after the acquisition of another company. The third fine was for $55 million against a popular search engine. The fine was levied after concluding that the search engine wasn't clear about its data consent policy and did not give its users enough control over their data.

GDPR was created to make sure organizations gather, store, protect and share information that they have on EU citizens in a lawful, ethical way.

Hacktivist Offers Bounty on Banking Data

Hacktivist Phineas Fisher, previously known for targeting surveillance companies as well as law enforcement and political entities, has reportedly compromised a bank to steal money, documents, and emails. The stolen documents and emails were given to a leaking website called Distributed Denial of Secrets. Further, the actor is offering $100,000 to other hackers who carry out politically motivated hacking activity. This aligns with their most recent manifesto, released on 15 November, stating that hacking is a tool used to fight economic inequality and establishing a Hacktivist Bug Hunting Program which essentially pays hackers to carry out politically motivated hacks against companies that lead to leaking of documents that are deemed to be in the public's interest. One bank confirmed a breach carried out by a criminal hacking group but did not explicitly name Phineas Fisher, though media reporting from security researchers has indicated a connection. Separately, a trove of consumer data—nearly 1.2 billion records in all has been publicly exposed via an unsecured server. The data appears to be profile information, including phone numbers and email addresses as well as work history, linked to social media accounts. Such data could be used to impersonate individuals or hijack accounts. The server has been taken offline, but it is unknown if the data was accessed prior to that.

APT33 utilizes small, elusive botnets on US and global targets

Reputed Iranian threat actor APT33 has been employing more than a dozen secret botnets to infiltrate and spy on the networks of various Middle Eastern, US and Asian organizations, and are even setting up their own VPN networks to conceal their operations, according to TrendMicro. APT33, aka Refined Kitten, is particularly known to target the oil and aviation industries and is commonly associated with the Shamoon and StoneDrill disk wiper malware programs. The botnets are small and elusive, noting that each is made up of a dozen or fewer infected computers used to maintain persistence in highly targeted, compromised networks. The malware running individual bots is mostly limited to downloading and running additional malicious code.

FS-ISAC Cyber-Range Ransomware, Business Email Compromise and *new* Cloud Leak 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. These popular exercises sell out quickly, so register early! For additional information, visit us **online**.

Upcoming Cyber-Range Exercise scenarios focus on Ransomware, Business Email Compromise (BEC) or Cloud Leak (NEW) attacks:

- 3 March | FS-ISAC Cloud Leak Exercise | Atlanta, GA | Register
- 22 April | FS-ISAC Ransomware Exercise | Dallas, TX | Register
- 16 June | FS-ISAC Business Email Compromise Exercise | Toronto, CA | Register
- 22 July | FS-ISAC Business Email Compromise Exercise | Minneapolis, MN | Register
- 18 August | FS-ISAC Cloud Leak Exercise | St. Louis, MO | Register

Additional dates and locations (Boston, New York, Chicago, Kansas City and San Francisco) will be added soon!

Please check the FS-ISAC events page where you can filter by Exercises for more dates or send questions about these cyber-range exercise events or other FS-ISAC exercises to Exercises@fsisac.com.

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

Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – January 2020

fsisac.com