FS-ISAC Securities Industry Risk Group **May 2018**
Global Cybersecurity Brief **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**).

More Than 10% of Employees Fail Social Engineering Attacks

Security firm Positive Technologies (**PT Report**) reports that social engineering attacks are successful in cyber attacks (**Computer Weekly**). The report is based on 3,000 emails containing links to websites, password entry forms and other malicious attachments. Surprisingly, 17% of the recipients were tricked into taking actions that could have resulted in compromised computers and networks. The study also found that when users could not open the attachment or the access the link supplied in the email, they would contact or forward the malicious note to their IT department, for assistance.

Firms should educate users on protocol for when they receive suspicious emails and how to properly react to them. They should take a 'think before your click' approach, especially if users are not sure the message they receive is legitimate. If they feel it's not, a reach out to the sender via phone should be the user's next action.

Verizon 2018 Data Breach Investigations Report: Executive Summary

On April 10, Verizon released its 11th annual Data Breach Investigations (DBIR) (**Report)**. The 2018 report is based on data from 67 organizations in 65 countries and includes analysis on 53,308 security incidents and 2,216 breaches. Key findings:

- Financially-motivated attacks remain the most common and account for 76 percent of breaches.
- Ransomware is the most prevalent type of malicious software and was found in 39 percent of malware-related incidents.
- The human factor remains a key weakness due to employees falling for social attacks.
- Financial pretexting has doubled in the last year and is targeting HR departments.
- Phishing attacks pose a major threat to businesses.
- DDoS attacks are prevalent and security standards need to be addressed by organizations.
- About 73 percent of cyberattacks were perpetuated by outsiders, with organized crime groups accounting for 50 percent of attacks, and nation-state or state-affiliated involved in 12 percent.
- Internal actors account for about 28 percent of attacks.
- 68 percent of breaches took several months to discover
- 87 percent of the breaches had data compromised within minutes.
- In the financial and insurance industry Trojan botnets and DDoS attacks are the major risks, with ATM skimmers and jackpotting being the main threats from organized criminals.

Biggest Risks for the Financial and Insurance Industry

- **Frequency** 598 incidents, 146 with confirmed data disclosure
- **Top patterns** Denial of Service, Crimeware, Payment Card Skimmers, and other threats represent 82% of all security incidents
- **Threat actors** 92% External, 7% Internal, 1% Partner
- **Actor motives** 93% Financial, 5% Espionage
- **Data compromised** 36% Personal, 34% Payment, 13% Bank (chart on pg. 31 of DBIR)

Trojan Botnets and DDoS attacks: The report shows that trojan botnets and DDoS are the most prevalent attacks facing the financial industry. There were over 40,000 Trojan botnets incidents and this is a major concern. DDos attacks have been on the rise and pose a threat to businesses by disrupting operations. Organizations need to be prepared if an attack were to occur.

ATM skimmers and jackpotting: Payment card skimmers are being installed on ATMs and is big business for organized crime groups. ATM jackpotting is another concern where criminals can spit out money from ATMs.

Additional Details

Ransomware is top cyberthreat: Ransomware is the most common type of malicious software and remains a key threat for global organizations. Ransomware attacks have doubled since 2017 and were found in 39 percent of malware-related data breaches. For cybercriminals it is easy to deploy, there's little risk or cost involved, and only takes a few minutes to conduct. Business critical systems are now being targeted by ransomware attacks and cybercriminals are demanding higher ransoms. Despite the mounting threat, many businesses are not taking appropriate action steps in setting up security defenses to combat ransomware attacks, and this is highly problematic.

Human factor remains key weakness: Employees are continuing to fall prey to social attacks. Phishing and pretexting represented 98 percent of social incidents and 93 percent of all breaches, with email continuing to be the most common entry point with 96 percent. The high rate of social attacks highlights the need for employees to be educated and trained on cybersecurity.

Financial pretexting targets HR departments: Financial pretexting has doubled in the past year from 61 incidents to 170 incidents. Eighty eight of the incidents targeted HR employees to obtain personal data for filing fraudulent tax returns.

Phishing attacks should not be overlooked: Although 78 percent of people did not click on a phishing campaign last year, 4 percent of people did click on it, and it only takes one victim for cybercriminals to gain access into an entire organization.

DDoS attacks are prevalent: The report shows that DDoS are commonplace and can impact an organization by acting as a distraction for cybercriminals to perform other malicious activities. Although DDoS attacks have the power to disrupt an entire organization, they can be prevented if proper security measures are in place.

Outsiders pose most serious threat: About 73 percent of cyberattacks were perpetuated from outsiders, with organized crime groups accounting for 50 percent of attacks, and nation-state or state-affiliated involved in 12 percent. While Internal actors accounted for about 28 percent of attacks.

GAO Highlights Better Steps Needed by Regulators

The United States Government Accountability Office (U.S. GAO) published a paper that provides information on various aspects of fintech activities (**GAO**). The report addressed fintech payments, lending, and wealth management products. The GOA assessed the following in regard to these topics:

- Benefits, risks, and protections of these products for end users.
- Regulatory oversight of fintech firms.
- Regulatory challenges for fintech firms.
- Steps taken by domestic and other countries' regulators to encourage financial innovation within their countries.

The GAO reviewed all available data, literature and agency documents and analyzed relevant laws and regulations. Interviews were conducted with more than 100 federal and state regulators in the US, four regulatory agencies in other countries, and market participants.

The report makes several recommendations related to improving interagency coordination and addressing competing concerns on financial account aggregation. And whether it would be feasible to adopt regulatory approaches like regulatory agencies outside the United States.

Sheltered Harbor Names Don Callahan as Co-Chairman of the Board

Sheltered Harbor, a subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC), today announced that its board of directors appointed Don Callahan, head of Operations & Technology at Citi, as co-chairman of Sheltered Harbor's board of directors (**Markets Insider**). Callahan replaces outgoing co-chairman Jim Rosenthal.

For more about Sheltered Harbor, please visit their site (**Join SH**) or contact them at: **info@shelteredharbor.org**.

New Ransomware Uninstalls AV Software

Researchers at MalwareHunter Team had found a new ransomware variant dubbed 'AVCrypt' that when installed will attempt to remove any antivirus and other security software before it attacks (**MalwareHunter Team**). The ransomware also attempts to remove numerous services including Windows Update and provides no contact information (**Bleeping Computer**). Analyst are not sure if this ransomware is still in development or may be a wiper malware, where it's ultimate intention is to delete all files and data from a PC.

Firms should ensure that all antivirus and security software are updated, and user account access is set properly on PC, and update and review all mitigation plans.

EMEAS Summit Call for Presentations Closes 11 May

FS-ISAC Summits are known for the high-quality, relevant and actionable content presented – and that cannot happen without you! The call for presentations for the 2018 EMEA Summit (1-3 October, Amsterdam) is open! Increase your visibility, share your knowledge and showcase your expertise – **submit your proposal** for the EMEA Summit today.

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**.

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 Analysis Center **www.fsisac.com**