FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | December 2018

TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

Account Takeover and Payment Fraud Webinar Training | 18 December | Online

Cyber-Range Exercise
30 January | Federal Reserve Bank of Boston

Cyber-Range Exercise
13 February | Zurich

FS-ISAC Member Meeting*
12 February | Zurich

Cyber-Range Red Team/Blue Team Exercise
28 February | Online

Cyber-Range Exercise
5 March | Toronto Exchange (TMX)

FS-ISAC Member Meeting*
6 March | London

Cyber-Range Exercise
19 March | Federal Reserve Bank of Atlanta

Cyber-Attack Against Insurance Systems (CAIS) Exercise | 19-20 March or 26-27 March 2019 | Online

Cyber-Range Exercise
2 April | Federal Reserve Bank of Cleveland

FS-ISAC 2019 Annual Summit
28 April-1 May | Orlando

Cyber-Range Exercise
25 July | Federal Reserve Bank of Chicago

Cyber-Range Exercise
22 August | Federal Reserve Bank of
St. Louis, MO

Diversity Matters: FS-ISAC Awards Scholarships to Build Talent Pipeline in the US and Globally

To meet the evolving needs of the cybersecurity threat landscape and to create a more diverse workforce FS-ISAC recognized **14** women with its Building Cybersecurity Diversity (BCD) scholarship in the US, The recipients were recognized at FS-ISAC's Fall Summit in Chicago.

FS-ISAC awarded a total of **24** scholarships globally in 2018. The US, Singapore and European recipients are sponsored and mentored by leading banks and technology companies. A 2018 Cybersecurity Workforce Study found that cybersecurity professionals are focusing on developing new skills as the workforce gap widens. According to the report, that gap now stands at more than 2.9 million workers globally, with 2.14 million cybersecurity staff required in the Asia-Pacific region and almost half a million required in North America.

BCD Scholarship recipients pictured from left to right: Sun Meng, Gayathri Sugumar, Tan Zhi Xuan Francine, Yvonne Soh and Tan Lixin.

BCD Scholarship recipients pictured from left to right: Freya Hardwick, Catalina Sagan, Courtney Lun, Zoe Mackenzie and Selina Cho.

BCD Scholarship recipients pictured (left to right, top to bottom) Rachel Adams, Jessa Gramenz, Jonielle Sablan, Deepika Chickmagalur Ramesh, Camelia Simoiu, Kim Hertz, Sarah Tucker, Leaticia Osuagwu, Sarah Cooney, Megan Culler, Sherry Peng, Natalie Larsen and Victoria Sykora-Lovaas. (Not pictured: Balkis Nasery).

At the Fall Summit in Chicago, 14 US scholarship recipients were the latest addition to a prestigious list of rising cybersecurity professionals preparing to address cyber-attacks and finding solutions to stay ahead of cybercrime. The scholarship offers $5,000 and a trip to attend one of FS-ISAC's four Summits to be mentored by and network with influential industry leaders. Read the full release.

FS-ISAC Cyber-Exercises and Sheltered Harbor Included in FFIEC Cybersecurity Resource Guide

The Federal Financial Institutions Examination Council (FFIEC) released an extensive list of cybersecurity awareness resources and statements for financial institutions on their website called the Cybersecurity Resource

continued, page 2

Products and Services Discounts

Did you know that as a member of FS-ISAC you can take advantage of special offers and discounts on product and services from our Affiliates and Strategic Partners? **Visit the members discount page** to see current offers. Make sure to bookmark and check back often as offers are updated and added frequently!

ISAC Analysis Team Updates

FASTCash Attacks and HIDDEN COBRA

The US Computer Emergency Readiness Team (CERT), the Department of Homeland Security (DHS), the Department of the Treasury and the Federal Bureau of Investigation (FBI) issued an alert on "FASTCash" attacks. The attacks have been attributed to malicious cyberactivity by the North Korean government. The US government refers to this malicious activity as HIDDEN COBRA. HIDDEN COBRA has been stealing money from Automated Teller Machines (ATMs) from banks since at least 2016. In all reported FASTCash attacks, the attackers have compromised banking application servers running unsupported versions of the IBM Advanced Interactive eXecutive (AIX) operating system beyond the end of their service pack support dates.

Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims. Some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Commercial reporting has referred to this activity as Lazarus Group and Guardians of Peace. DHS and FBI assess that HIDDEN COBRA actors will continue to use cyber to advance their government's military and strategic objectives. Analysts are encouraged to review the information provided in this alert to detect signs of malicious network activity. In one incident in 2017, HIDDEN COBRA actors enabled cash to be simultaneously withdrawn from ATMs located in more than 30 different countries. In another incident in 2018, HIDDEN COBRA actors enabled cash to be simultaneously withdrawn from ATMs in 23 different countries.

Metamorfo Credential Harvesting Campaign

A new malware string developed in Delphi, called Metamorfo, has been observed targeting financial institutions in Brazil. Information on the compromised system is exfiltrated and then sent to a C2 server. This trojan is deployed through two different infection processes which have been seen between late October into November. The first campaign was identified utilizing a file archive which is hosted on a free web-hosting platform containing a Windows LNK file. Its function is to download and then execute a PowerShell script from a malicious server. The script then downloads a file archive which is hosted on Amazon Web Services (AWS) which contains both a compressed payload (.PRX) file and a dynamic-link library (.DLL). The library extracts the payload and executes library injection of Metamorfo.

The second campaign functions with more complexity by utilizing malicious Portable Executable 32-bit executables, delivered via file archives, to perform the initial stage of infection by creating a batch file in a subdirectory of %TEMP%. Windows Command Processor is then used to execute the batch file which runs instructions via PowerShell to download content from the C2 server and then pass it through the Invoke-Expression (IEX) tool which converts the strings received into PowerShell script. This script then goes into sleep mode for 10 seconds after which it extracts the file archive and saves the DLL to a subdirectory of %APPDATA% on the system. Finally, RunDLL32 is used to execute the malware. Indicators related to this malware are available within the FS-ISAC repository.

FS-ISAC Publishes Paper on Threat Information Sharing and General Data Protection Regulation (GDPR)

FS-ISAC's latest paper, "Threat Information Sharing and GDPR: A Lawful Activity that Protects Personal Data," introduces threat information sharing under GDPR, the types of personal data and non-personal data comprised in threat information and traffic light protocol. It concludes that threat information sharing and the processing of personal data by FS-ISAC and its members advances the fundamental tenets of GDPR - to protect the fundamental rights and freedoms of individuals in respect of their personal data - and is considered lawful. View this TLP Green paper by logging into the FS-ISAC Portal.

FFIEC, continued

Guide for Financial Institutions. The guide provides snapshot information on security resources available to financial institutions in the US as well as the type of information the organization provides. FFIEC included information on FS-ISAC, Sheltered Harbor and FS-ISAC's Cyber-Attack Against Payment Systems (CAPS) exercises. The CAPS exercises are free to any financial institution. Financial institutions can participate via a virtual, confidential two-day, tabletop exercise that simulates an attack on payment systems and processes. In 2018, a record 2,081 total financial institutions participated in the North America, Asia-Pacific and Europe, Middle East and Africa exercises.