FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | November 2017 TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

FS-ISAC Expert Webinar Series: Securing the Human Layer* | 14 November | Online

NowSecure Webinar: Danger in the App Store | 14 November | Online

BlackBerry Security Summit
14-15 November | New York City

Citrix Webinar: Swift CSP: What You Need to Know Now | Download until 15 November

Flashpoint Webinars: Flash Talk -
- **EMV Circumvention**
- **Russian Ban on Anonymizing Services**

Download until 15 November

Illusive Networks Webinar: Deception at the Scale and Speed of Large Enterprises
29 November | Online

Sydney Member Meeting* | 29 November

Akamai Webinar: State of the Internet/ Security Report – Q2 2017 Findings
Download until 30 November

Black Duck Webinar: Audits of 1000 Apps
30 November | Online

Haystax Webinar: Defending Against the Wrong Enemy | 30 November | Online

EclecticIQ Webinar: How to Overcome the Threat Intelligence Cycle Paralysis?
30 November | Online

MarkMonitor Webinar: From Phishing to the Dark Web - The Life Cycle of a Cyber-Attack
Download until 30 November

FS-ISAC Member Surveys Recent Results

FS-ISAC members (basic to platinum levels) have the ability to survey the membership. Some recent survey results posted to the Portal include:

Mitigating ATM Connection Risk

The goal of this survey was to determine what steps other institutions have implemented to mitigate the risk of connecting ATM's to the bank's internal network.

Third-Party Incident Response Vendor Usage

The intent of this survey was to determine what vendors are leveraged for incident response (IR) activities, the specifics around when a vendor is engaged and for what purposes.

Patch Management 2017

The purpose of this survey was to determine best practices and controls around security patching of servers and workstations with the objective of reducing the risk of exploitation of vulnerabilities.

Survey results are TLP Amber. To view the survey results login to the FS-ISAC Portal, navigate to Documents, Surveys folder, 2017 Member Survey Results folder. All member surveys conducted from 2014 to present are also available in the Surveys folder under the title: Directory of FS-ISAC Member survey results, which lists the title, goal and release date.

FS-ISAC Members (Basic, Core, Standard, Premier, Gold and Platinum) have the ability to survey the membership by completing the *FS-ISAC Survey Request Form*, located on the Portal in the Surveys folder under Documents. For more information about member surveys, please review the *FS-ISAC Member Survey Request Process* document also located in the Surveys folder or contact Jill Bost.

Automation Initiatives Updates

To keep you, our members, up to date FS-ISAC recently published the ***FS-ISAC Automation Initiatives (October 2017)***. This document provides a brief overview of several important open standards that FS-ISAC supports to help members automate sharing information and analysis. FS-ISAC is committed to continuing to support the development and adoption of these initiatives by working with the appropriate standards bodies to develop supporting open standards; encouraging adoption by third-party vendors, service providers and peers; and assisting members with integration with their existing security tools. To view this member-only resource, please login to the FS-ISAC Portal and navigate to the Documents folder.

PwC Global State of Information Security Survey 2018 Report

PwC published key findings from the Global State of Information Security Survey 2018 (GSISS) in a report titled *Strengthening Digital Society Against Cyber Shocks.* FS-ISAC CEO Bill Nelson provided commentary for the report about next steps global business leaders should take in response to cyber-attacks. He specifically mentions the importance of information sharing, the value of simulated cyber-exercises and the roles of the Financial Systemic Analysis & Resilience Center (FSARC) and Sheltered Harbor to enhance financial sector resilience. Nelson also noted that Global Resilience Federation (GRF) can help other sectors and communities establish information sharing capabilities.

PYMNTS Feature

FS-ISAC was featured in the monthly *Faster Payments Tracker by PYMNTS*. In the article, *Putting FIs Through Cybersecurity Drills To Prepare For The Next Big One*, CEO Bill Nelson discusses FS-ISAC's efforts to help members prepare for incidents through cyber-exercises like the Cyber-Attack Against Payment Systems (CAPS) program. In 2017, more than 2,000 members have participated in CAPS exercises around the world. These simulated exercises are invaluable for testing and fine-tuning incident response and defense capabilities. As Bill Nelson put it, "it's practicing and getting the muscle memory of what happens — if this does happen — to you as a company. The exercises are key to making sure people know what to do when it happens."

FS-ISAC Launching New Cloud Security Working Group

In response to member requests following the Expert Webinar Series session Cloud Security for the Financial Services Sector: Standards and Best Practices, FS-ISAC is developing a new Cloud Security Working Group. The working group, which currently has 108 members, will share insights related to cloud security and work to develop a guide for decisions around cloud security. If you would like to participate in the group or have questions, please contact Dennis Gross.

Fall and EMEA Summit Recaps

FS-ISAC hosted two of our four Summits for our members to come together and share insights about new threats and best practices for the financial sector in October. From 1-4 October, FS-ISAC held its Fall Summit in Baltimore for nearly 1,000 attendees. Highlights included a CISO Panel on Innovation, Capture the Flag and tracks on governance, resiliency, technology and operations, testing and security assurance, threat intelligence and more. FS-ISAC's EMEA Summit was held in London from 30 October- 1 November. Close to 400 attendees joined Keren Elazari, *The Future of Cybersecurity – a Hacker's Perspective*, more than 40 amazing sessions, an innovation challenge and more.

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 member discount page** to see current offers. Make sure to bookmark and check back often as offers are updated and added frequently!

ISAC Analysis Team Update

FS-ISAC Portal Quick Reference Guide

The ISAC Analysis Team recently published a quick reference guide for the FS-ISAC Portal and products based on frequently asked questions from members. This document provides an overview of the portal alert types, a mission center user guide and guides for other resources available through the Portal. The ***FS-ISAC Portal – Quick Reference Guide*** can be found on the FS-ISAC Portal homepage or by navigating to the Documents tab then Member Resources folder.

Far East International Bank (FEIB) Compromise

On October 6, 2017, Taiwan media reported that the systems of the Far Eastern International Bank (FEIB) were compromised which resulted in fraudulent wire transfers to overseas accounts. Fraudulent transfers were detected by FEIB on October 3 and reported to the Financial Supervisory Commission (FSC) Banking Bureau on October 5 after FEIB had conducted initial investigations.

The Hong Kong Monetary Authority (HKMA) reported that the attack commenced with email scams with a malicious program hidden in an attachment and that the malware was not detected by the FEIB's AV software (unconfirmed reports point it to be Trend Micro). A local forensics company was assisting FEIB in the investigations.

There were also unconfirmed reports that the systems were unable to boot up. All these seem to suggest that there could be some effort by the malicious actors to distract the bank from noticing the fraudulent transfers, however it is still too early to know the specific technique used. What seems to have led the FEIB to detect the incident was the MT202COV messages without the corresponding MT103 message or missing the field 53 in subsequent order. Efforts to trace and recover the lost funds is ongoing and current loss estimate is less than $500,000 USD.

In our FS-ISAC Advisory Report on October 24, various malware samples have been uploaded to malware repositories which appear to originate from the intrusion. These include both known Lazarus group tools, as well as a rare ransomware variant called 'Hermes' which may have been used as the distraction or cover-up for the security team while the heist was occurring.

Follow us on Twitter @FSISAC or **join the discussion on LinkedIn**.