FINANCIAL SERVICES Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter **June 14, 2017**

Newsletter Contents

Upcoming Webinars

Securing the Cloud for Financial Services
Bitglass | June 21
Register here

Cyberthreat Mitigation [NEACH Series 2]
Online (Paid Webinar) | June 22
Register here

Transforming Cybersecurity in Financial Services
McAfee | June 22
Register here

Cyberthreat Compliance [NEACH Series 3]
Online (Paid Webinar) | July 20
Register here

Future Cyberthreat Trends [NEACH Series 4]
Online (Paid Webinar) | August 24
Register here

Upcoming Events

Cyber-Intelligence Tradecraft Training
Singapore | June 19-23
Register here

Member Meeting
London | June 22
Register here

Cyber-Intelligence Tradecraft Training
Melbourne | June 26-30
Register here

FS-ISAC Expert Webinar Series: Threat of IoTs
Online | June 27
Register here

Cybersecurity and Crab Cakes in Charm City

Where can you connect with peers over crab cakes, learn the latest in cybersecurity and resiliency, and enjoy the convenience of Charm City? It's easy…just plan on attending the 2017 FS-ISAC Fall Summit on October 1-4 in Baltimore.

The 2017 FS-ISAC Fall Summit in Baltimore is gearing up to be one of the best Summits yet, and is set to deliver superb content including more member sessions than ever before. Connect with your peers at a great location set perfectly between the financial hubs of the Northeast and the nation's capital. While you're here, explore Baltimore's beautiful Inner Harbor, enjoy some famous blue crab and take in the historic sights and sounds of the Mid-Atlantic.

Registration opens soon. Learn more about the Summit and book your hotel and travel now!

How to Make the Most of Your FS-ISAC Membership

This month, the FS-ISAC Business Relationship Management (BRM) team and APAC Regional Directors held an hour-long briefing entitled "How to Make the Most of your FS-ISAC Membership – Asia-Pacific Services Update." The team addressed and updated members on how to share and receive information, how to manage FS-ISAC's intelligence, region specific committees and working groups, new intelligence products, upcoming events and whom to contact to get involved.

FS-ISAC plans to make similar briefings each quarter for all regions, so keep an eye out for registration details coming soon!

FFIEC Cybersecurity Self-Assessment Tool Updated

The Federal Financial Institutions Examination Council (FFIEC) released an updated version of the Cybersecurity Assessment Tool, commonly referred to as the CAT, during the week of May 30. The FFIEC provided an updated tool and appendices to help financial institutions to "identify their risks and determine their cybersecurity preparedness."

FS-ISAC and the FSSCC developed an automated tool for member institutions to use to complete the 2015 version of the CAT. FS-ISAC has received the updated, 2017 version of the FFIEC CAT and is evaluating the changes in the new version and working with members to make an updated version of the automated CAT tool available for download soon.

Aggregation Working Group Update

The FS-ISAC co-hosted the first joint workshop on next generation aggregation standards on May 18-19. Many FI's and aggregators participated in the bi-coastal, two-day event.

Participants agreed that the Aggregation Working Group's work is important and must continue to keep specifications current and increase adoption. Topics addressed included: standardizing terminology between parties, expansion of the Durable Data API data set, additional authentication proposals for best practices, general security and operability expectations and common testing and certification for participants to minimize overhead and increase adoption.

The Aggregation Working Group would like to recognize Anil Mahalaha (Fidelity), Don Cardinal (Bank of America) and Eric Guerrino (FS-ISAC) for their exceptional efforts to making this a reality. For more information, please contact admin@fsisac.us.

Upcoming Events cont.

Critical Thinking Fundamentals
Online | July 17-31
Register here

Cyber-Intelligence Tradecraft Training
Reston, VA | August 21-25
Register here

Attend Joint OASIS-ISAC STIX 2.0 Workshop at Borderless Cyber

Join FS-ISAC, OASIS and NH-ISAC at the STIX 2.0 Workshop for ISAC members, June 20 in New York City. This half-day workshop is specifically designed to provide ISAC members with need-to-know information on the next generation of automated threat intelligence sharing standards. Learn more

Update From the ISAC Analysis Team

Jaff Ransomware
This May, a major ransomware campaign took place, although this one did not grab headlines like WannaCry did. Jaff ransomware, which has been mistaken for Dridex, Locky and Wannacry, was launched by the Necurs botnet which sends phishing emails with a malicious .pdf attachment. Although there is no evidence that the campaigns are related, Jaff presents many similarities to all three of the other ransomwares.

The .pdf attachment contains an embedded DOCM file, which, when opened, requests additional permissions to enable macros. If approved, the macro script generates a URL that delivers and executes the payload. Once Jaff executes, it encrypts the victim's files and displays a ransom note that directs them to install Tor and visit a tor site which provides instructions for payment. In addition, initial reports indicate that when it encrypts files, Jaff appends all file extensions to ".jaff". However, SANS Internet Storm Center noted on May 23 that a Jaff sample changed the file extensions to ".wlu". SANS asserts that this change is evidence of a Jaff 2.0 campaign that may be unrelated to the initial outbreak.

DocuSign Breach and Phishing Campaigns
On May 9, DocuSign issued an alert warning of an increased number of phishing emails leading to malicious Word documents. The emails used DocuSign branding in the headers and body of the email and the sender email addresses mimicked the DocuSign domain. The company followed up on May 15 with another alert citing the same type of phishing emails sent from DocuSign-related domains and complete with DocuSign branding. The company added confirmation that "a malicious third party had gained temporary access to a separate, non-core communication system used for service-related announcements." According to the statement, only email addresses were accessed. Frequently asked questions and recommendations are available on DocuSign's blog.

The FS-ISAC Analysis Team infers that the increase in quantity of phishing emails could be due to the unauthorized third-party accessing email addresses of customers who would expect to receive emails from DocuSign. The date of the unauthorized access has not been provided by the company. The initial alert for the malicious email campaign was issued on May 9 and confirmation of the access on May 15. It is possible that the breach happened days or weeks prior to the announcement and is related to the May 9 alert. It is also possible that an initial campaign began on May 9 then expanded the following week after the actors gained access to additional target emails.

HP Laptop Vulnerability
In late April, Swiss security firm Modzero discovered that a Conexant brand audio driver located in the Windows system folder was recording keystrokes on Hewlett-Packard laptops. According to the firm, Conexant's MicTray64 program is installed with the Conexant audio driver package and registered as a Microsoft Scheduled Task to run after each user login. The program monitors all keystrokes made by the user to capture and react to functions such as microphone mute/unmute keys/hotkeys. In addition to the handling of hotkey/function key strokes, all key-scan code information is written into a logfile - path (C:\Users\Public\MicTray.log) that is stored in the user's home directory. The business impact for this vulnerability is leaking of sensitive information or user input by anyone able to read files in the MicTray log (C:\Users\Public\MicTray.log) or call the function MapViewOfFile(). In addition, Modzero notes that this allows malicious actors to capture keystrokes without being caught by Anti-virus heuristics looking for malicious tasks. Any entity (person or malware) with access to the user's files on one of the models, can see passwords, visited web pages, private messages and more.

In response, HP published a corresponding security bulletin (HPSBGN03558) and released a new driver package without keylogging functions for affected product models, which include HP EliteBook, ProBook, and ZBook. The vulnerability was assigned the CVE-ID 2017-8360. Proof of concept details are available in the advisory.