FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter
August 2016

Newsletter Contents

FS-ISAC Webinars

Webcast: How TIAA Uses Threat Intelligence to Enhance Security | Recorded Future | August 9
Register Now

Digital Transformation and the 6 Key Trends Shaping Digital Banking | Akamai | August 23
Register Now

Security Automation - STIX/TAXII Fundamentals | Cisco | August 30
Register Now

Webinar | Attivo Networks | September 15
Additional Information to Follow

Upcoming Events

Member Meeting
Sydney, Australia | August 18
Register here

Cyber Intelligence Tradecraft Training
Reston, VA | August 22 - 26
Register here

Member Meeting
London, UK | September 6
Register here

2016 CAPS Exercises for Payment Processors in North America
North America | September 7 - 8
Register here

2016 CAPS Exercises for Payment Processors in North America
North America | September 13 - 14
Register here

FS-ISAC Expands Cyber Talent in US and UK

FS-ISAC is proud to announce two new hires to the FS-ISAC staff to help further support our mission of information sharing and to meet the growing needs of our members.

• **Greg Temm** has joined as Chief Information Risk Officer. Temm, who spent the past 18 years at MasterCard, will be responsible for the global intelligence program as well as the overall risk management program for the organization.

• **Moona Ederveen** joins FS-ISAC from UBS where she served as Senior Cybersecurity Business Analyst. At FS-ISAC she will assist member services in the UK and Ireland, and will also be able to assist with FS-ISAC activities in mainland Europe as well.

LS-ISAO Membership Exceeds 100

The Legal Services Information Sharing and Analysis Organization (LS-ISAO) now has more than 100 active members, all added in less than 12 months, making it the fastest growing Information Sharing and Analysis Organization (ISAO). ISAOs are industry-specific and enable member organizations to properly and effectively submit and share real-time cyber threat intelligence and information. ISAOs also help members to understand a changing threat environment to build stronger controls to help to prevent and respond to cyber and physical risks, vulnerabilities and threats. Cindy Donaldson, Senior Vice President of Products and Services and COO, Sector Services, FS-ISAC stated, "Launched in August 2015, LS-ISAO's rapid growth and very active participation from members supports a true community defense model, which acts like a cyber neighborhood watch. FS-ISAC is proud to see the growth of information sharing in the legal community and across communities and sectors."

FS-ISAC Summit Notes

The 2016 FS-ISAC Fall Summit is just around the corner! Join us in Nashville, Tennessee from October 23-26 at the Gaylord Opryland. View the official brochure and review the session descriptions and agenda today.

The early bird registration closes on September 23, so be sure to take advantage of this great pricing option and register today. Additionally, the hotel block fills quickly so make your reservation today – you can reserve online or call (615) 889-1000 – and don't forget to mention you are with the **2016 FS-ISAC Fall Summit** to receive the group rate.

To stay up-to- date on all the latest information and details make sure to visit the Fall Summit site.

International Notes from FS-ISAC

• **EMEA:** FS-ISAC participated in the EU Financial Cybercrime Coalition (EU FCC) hosted by Europool. Discussions and presentations focused on sharing intelligence and successful case studies of collaboration between Law Enforcement and the financial services sector. Sharing fraud indicators is a hot topic with many FS-ISAC members – we have working groups in APAC, Europe and the US all looking at how to better share fraud intelligence. The top challenges for these working groups include legal questions (what can we share, especially cross border), technical (how to automate, how to express over STIX/TAXII) and organisational (fraud and cyber security often operate in separate silos).

• **APAC:** FS-ISAC has signed a memorandum of understanding with CERT Australia. As part of the agreement, CERT AU will be attending FS-ISAC member meetings in Australia. This is part of FS-ISAC's developing strategic relationship with the Australian Cyber Security Centre (ACSC), the government umbrella organization.

Upcoming Events (cont.)

Member Meeting
Phoenix, AZ | September 13
Register Now

2016 CAPS Exercises for Financial Institutions in US & Canada
North America | September 20 - 21
Register here

Member Meeting
Kuala Lumpur, Malaysia | September 22
Additional Information to Follow

2016 CAPS Exercises for Financial Institutions in US & Canada
North America | September 27 - 28
Register here

FS-ISAC Expands Exercises Program

As part of FS-ISAC's expanded exercises program, the Financial Services Sector Coordinating Council (FSSCC) and Treasury conducted a successful cybersecurity exercise at the US Treasury Department in Washington, DC. The three-hour facilitated tabletop exercise and discussion focused on a cyber-attack against a major technology service provider affecting community banks and credit unions. Participants included 65 senior leaders and experts from US Government agencies (Treasury, White House, DHS, FBI, USSS), US regulatory agencies, financial associations representing community FIs, community FIs and service providers. This is one of several sector level exercises that the FSSCC and Treasury is developing and executing, including one involving CEOs and other senior leaders which will be held in October. The exercises leverage the updated All Hazards Crisis Management Playbook. For additional details, please contact Greg Gist at greg.gist@fsscc.org.

Update From the ISAC Analysis Team

Return of Locky Ransomware

After a brief hiatus in in June, the FS-ISAC Analysis Team is receiving reports of the return of Locky Ransomware. The new variants of Locky ransomware are very similar to the previous variants, with a few notable changes:

1. Additional obfuscation of the payload employed by the downloader
2. Virtual Machine (VM) awareness

Both of these changes serve to make detection and analysis of the new variants more difficult.

Additionally, the FS-ISAC Analysis Team has received reports of a new ransomware family, dubbed "Zepto." Its functionality appears virtually identical to Locky, with the notable exception that the files it creates use a "zepto" extension. Even the ransomware's decryptor page makes reference to Locky. Due to the similarities, it appears likely to be simply a variant of Locky, rather than a new ransomware family. The FS-ISAC Analysis Team encourages financial institutions to ensure that employees' computers are backed up regularly, including off-site storage of backups, to ensure that compromised data can be recovered in the event of destructive malware infection.

Oracle Critical Patch Update for July

On July 19, Oracle released its quarterly Critical Patch Update (CPU) to address security vulnerabilities across its product lines. The advisory contains 276 new security fixes in 84 Oracle products.

Some of the more notable product families included in this advisory are:

- Oracle Database Server
- Oracle Siebel CRM
- Oracle Communications Applications
- Oracle MySQL
- Oracle JavaSE

The FS-ISAC Analysis Team is not aware of any current exploit activity leveraging these vulnerabilities. However, Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released fixes. The FS-ISAC Analysis Team encourages financial institutions to remain on actively supported versions of software, and to apply critical patches as soon as possible, in accordance with their internal patch management policies.