FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter July 2017

Newsletter Contents

Fall and EMEA Summit Registration
EMEA Summit Session Preview
FS-ISAC Releases Tips for Ransomware
Updates from FS-ISAC Member Groups
FS-ISAC Updates STIX/TAXII Repo
Products and Services Discounts
Update from ISAC Analysis Team

Upcoming Webinars

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

FS-ISAC Expert Webinar Series: Enabling Secure Communication and Collaboration*
July 25 | Online

Preempt Webinar: Making the Case for Real-Time Insider Threat Prevention
July 25 | Affiliate Online

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

Upcoming Events

FS-ISAC Member Meeting at RSA APJ Conference*
July 26 | Singapore

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

Member Meeting*
September 4 | Barcelona

NA Cyber-Attack Against Payment Systems (CAPS) North America
September 12-13 | Online

Member Meeting*
September 13 | Utrecht, Netherlands

NA Cyber-Attack Against Payment Systems (CAPS)
September 19-20 | Online

2017 FS-ISAC Fall Summit
October 1-4 | Baltimore

*** FS-ISAC members-only**

Register Today for the Fall and EMEA Summits

Registration is now open for the **Fall Summit** (October 1-4 in Baltimore) and the **EMEA Summit** (October 30-November 1 in London)! Don't miss your chance to attend!

Fall Summit Keynote - John Brennan

This year FS-ISAC is proud to announce that John Brennan, former director of the US Central Intelligence Agency (CIA) will keynote the Fall Summit in Baltimore. Sworn into office on March 8, 2013, Brennan managed intelligence collection, analysis, covert action, counterintelligence and liaison relationships with foreign intelligence services. Before becoming director, Brennan served at the White House for four years as assistant to the President for Homeland Security and Counterterrorism following a 25-year career at the CIA.

EMEA Summit Session Preview

Here is a sneak peek at two of the amazing sessions you will want to attend:

- **Ransomware and WannaCry: Sharing Experiences of the Critical Success Factors |** Key specialists from the financial sector will discuss aspects of ransomware including potential impact, countermeasures and lessons learned from WannaCry in the financial sector. Learn about trends and anticipated developments, major challenges, the human factor, destructive wiper attacks and more.
- **Red Teaming the C-Suite: The Ultimate InfoSec Awareness Program |** Cybersecurity awareness programs can be stale, boring and ineffective. Many employees and managers grudgingly complete their mandatory trainings without truly understanding the reason. Even the C-Suite is often not fully engaged in learning from table-top exercises. This presentation will demonstrate ways of conducting red team exercises on a budget that will engage your C-Suite, make cybersecurity personal and tangible, help increase awareness, advocacy and funding for your enterprise cybersecurity program.

FS-ISAC Releases Tips to Defend Against Ransomware

In light of recent global ransomware attacks, FS-ISAC released a publicly available tip sheet on ransomware. This **paper** is in addition to the extensive information sharing and analysis by the FS-ISAC and others in response to the WannaCry ransomware attack in May and another significant event in late June targeting Ukrainian institutions and others. Tips and recommendations include:

- Isolating infected systems from your networks;
- Keeping operating systems and antivirus software up-to-date;
- Testing backups in a real-world environment; and
- Reporting any ransomware to law enforcement within 72 hours.

FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter July 2017

Updates from FS-ISAC Member Groups

The eighth quarterly meeting of the Canadian Financial Service Council (CFSC) was held on June 6, hosted by the CIBC, in Toronto. The CFSC addresses topics, challenges and opportunities specific to the Canadian domestic financial sector. Attendees discussed key issues including defining and refining metrics gathering/reporting and looking at developing best practices around utilizing cloud resources. Members also enjoyed a presentation on the various regulatory bodies in the Canadian financial services sector and how they are viewing cyberthreat issues. This session was intended to help set context for members in understanding where they should place development emphasis in their organizations. The Council's next meeting will be September 6 in Toronto and will include an educational session on the Canadian Payments system, provided by a representative from Payments Canada, followed by discussion around cyberthreat implications. For more information or to join the Council, Canadian FS-ISAC members should contact **Craigg Ballance** or **Richard Livesley**.

The Education Committee is currently developing a long-term plan to offer additional training educational resources for members. Using the **FS-ISAC Learning Academy** we post webinars, courses and other events for members to grow and develop their personal and professional skillset. If you have any training topics you would like to see in the future, please send your ideas to **trainings@fsisac.com**.

FS-ISAC Updates STIX/TAXII Repo

On June 18, FS-ISAC successfully upgraded its STIX/TAXII "repo" or Cyber-Intelligence Repository to the latest version of Soltra Edge as a part of our annual renewal. Now under the ownership of NC4, Soltra Edge is a cyberthreat communication platform for sending and receiving structured threat intelligence. The Machine Readable Threat Intelligence (MRTI) capability automatically shares intelligence between members and trusted communities using the STIX/TAXII standards.

The updated system was tested to ensure updates rolled out seamlessly to avoid impact to members. Members can expect a richer experience connecting with FS-ISAC via Soltra Edge. For more information about Soltra Edge, please visit **Soltra.com**.

Products and Services Discounts

Be sure to **visit the member discount page** on the FS-ISAC website for special offers from FS-ISAC Affiliates and Strategic Partners. Offers are updated and added frequently, please check back often for new offers.

Update from the ISAC Analysis Team

New Apache Struts2- CVE-2017-9791 / S2-048

A new security bulletin has been issued regarding Apache Struts due to the possibility to perform a remote code execution (RCE) attack with a malicious field value when using the Struts 2 Struts 1 plugin, and the value is part of a message presented to the user. The vulnerability security rating is "high" and affects Struts 2.3x with Struts 1 Plugin and Struts 1 action. The solution is to always use resource keys instead of passing a raw message to the ActionMessage class. The bulletin recommends that all Struts 2 developers are informed of the bulletin and implement the provided solution. **More.**

Android Security Bulletin—July 2017

The Android Security Bulletin contains details of security vulnerabilities affecting Android devices. Security patch levels of July 5, 2017 or later address all of these issues. The most severe of these issues is a critical security vulnerability in media framework that could enable a remote attacker using a specially crafted file to execute arbitrary code within the context of a privileged process. The severity assessment is based on the effect that exploiting the vulnerability would possibly have on an affected device, assuming the platform and service mitigations are turned off for development purposes or if successfully bypassed. There have been no reports of active customer exploitation or abuse of these newly reported issues. **More.**

Loki-Bot: Information Stealer, Keylogger and More

Loki-Bot is advertised as a Password and CryptoCoin Wallet Stealer on several hacker forums (carter, 2015) (Anonymous, 2016) (lokistov, 2015), however aside from sales pitches on the black market, not much has been published regarding the details of its characteristics and capabilities. This poses a problem to information security analysts who require such details in order to accurately prevent and/or defend against incidents involving this malware. Key characteristics of the Loki-Bot include: employment of function hashing to obfuscate libraries used; if the user is privileged, Loki-Bot sets up persistence within the registry; packets transmitted by Loki-Bot contain application data, decrypted Windows credentials, and the third packet is the malware requesting C2 commands; C2 communication includes information about the user and system; Loki-Bot encrypts both the URL and the registry key used for persistence using Triple DES encryption. **More.**