FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | July 2018

TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

FS-ISAC Member Meetings*
19 September | Dubai
13 November | Frankfurt

FS-ISAC Chapter Meetings*
3 July | Dublin
6 November | Edinburgh

Cyber-Range Ransomware Exercise
25 July | Amsterdam
29 August | St. Louis
17 September | Chicago
10 October | San Francisco
24 October | Kansas City, MO

Threat Intelligence: Protect Your Company's Critical Data and Assets
17-21 September | Reston, VA
18-22 February 2019 | Reston, VA

Counterintelligence: Counterintelligence in a Digital World
15-18 October | Reston, VA
13-17 May 2019 | Reston, VA

2018 FS-ISAC AP Summit
18-19 July | Singapore

2018 FS-ISAC EMEA Summit
1-3 October | Amsterdam

2018 FS-ISAC Fall Summit
11-14 November | Chicago

Registration is Open for EMEA and Fall Summits

FS-ISAC Summits are focused around peer-to-peer networking and building relationships or *circles of trust* with financial services organizations.

Registration for this year's **FS-ISAC EMEA Summit** is open. This Summit features more than 30 sessions divided into six tracks including hot topics such as:

- Threat hunting: What are your peers doing? New tools and techniques!
- Regulatory harmonization and GDPR update
- Merging cyber-risk into business and risk modelling
- Intelligence automation
- Making security more agile

Join us in Amsterdam 1-3 October 2018. Learn more, view the agenda and make sure you register today.

Early bird registration for the **FS-ISAC Fall Summit**, taking place 11-14 November in Chicago is open. In honor of Veteran's Day, FS-ISAC will donate $10 USD to a local Chicago Veterans charity for every person who registers before 30 September. What are you waiting for? Learn more, book your hotel and travel and register now!

Learn more about FS-ISAC Summits.

FS-ISAC Cyber-Range Ransomware Exercises

Cyber-range exercises offer FS-ISAC members with a more technical, hands-on-keyboard experience that provides greater interaction and sharing between members in a way that helps raise capability maturity levels and resiliency across the sector. FS-ISAC has partnered with ManTech to build a network environment and facilitate the event. Learn more and register for one of these upcoming sessions:

- 25 July | Amsterdam
- 29 August | Federal Reserve Bank of St. Louis
- 17 September | Federal Reserve Bank of Chicago
- 10 October | Federal Reserve Bank of San Francisco
- 24 October | Federal Reserve Bank of Kansas City, MO

FS-ISAC and BlackHorse Trainings: Committed to Your Security

FS-ISAC is committed to helping keep your organization safe from malware and security threats. That is why we offer training courses that are developed alongside industry and educational experts to bring you quality, reliable and actionable content. In coordination with BlackHorse, we have two exciting new courses open for registration.

continued, page 2

ISAC Analysis Team Updates

June Trickbot Activity

Changes were noted by open source researchers, myonlinesecurity.co.uk, malware-traffic-analysis.net and hybrid analysis in late June regarding Trickbot's delivery system. Microsoft Equation Editor Exploit CVE-2017-11882 in Word docs to deliver the payload had been the most recent methodology used until early June when they reverted to the more standard "auto-open" macro in word. CVE-2018-8174 was utilized for a short period around 25 June but the infection vector was greatly reduced due to it being an internet explorer exploit. Two days later researchers noted that Trickbot had resumed using word documents embedded with malicious macros. What was new was the usage of the InkPicture active x control within a visual basic script which activates a PowerShell script to obtain malware. This time saw Trickbot subjects which included bank invoices, payment documentation, and tax documentation. During this month some of the financial lures used were targeted at major financial institutions as well as US and UK government tax authorities.

Joomla! Released Version 3.8.9

On 26 June Joomla! released version 3.8.9 which contained two security fixes and fifty-two bug fixes. CVE-2018-12712 affects Joomla! 2.5.0 through 3.8.8 before 3.8.9. The autoload code checks classnames to be valid, using the "class_exists" function in PHP. In PHP 5.3, this function validates invalid names as valid, which can result in a Local File Inclusion. CVE-2018-12711 affects Joomla! 1.6.0 through 3.8.8 before 3.8.9. In some cases, the link of the current language might contain unescaped HTML special characters. This may lead to reflective XSS via injection of arbitrary parameters and/or values on the current page URL. Although Joomla! classified both vulnerabilities as low priority, we encourage members to address any content management systems (CMS) vulnerabilities in a timely manner. As of June 2018 Joomla! accounts for more than two million websites as the third most utilized CMS, after WordPress and Adobe Dreamweaver. This makes it an attractive target for threat actors.

BlackHorse trainings, continued

Threat Intelligence: Protect Your Company's Critical Data and Assets
17-21 September 2018 or 18-22 February 2019 | Reston, VA

An advanced one-week cybertraining program that equips you with the necessary skills and tools to stay a step ahead of your adversaries.

Counterintelligence: Counterintelligence in a Digital World
15-19 October 2018 or 13-17 May 2019 | Reston, VA

An advanced one-week cybertraining program that equips your organization with the necessary skills and tools to stay a step ahead of adversaries and protect against threats to your corporation, its holdings, physical assets, employees and customers.

Learn more and register today.

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!

FS-ISAC Launches Separate Info Sharing Group for Central Banks, Regulators and Supervisors

Inaugural global community will bring together financial regulators, central banks and supervisors to combat cyber and physical crime, enhancing financial sector resiliency.

CERES FORUM

The CERES Forum will provide a trusted means for peer **CE**ntral banks, **RE**gulators and **S**upervisors to:

- Share best practices concerning regulatory and compliance controls
- Hear from industry which controls are most effective
- Distribute rapidly information on cyber threats, vulnerabilities, incidents and other threat intelligence that could impact financial services, including those attacks that target central banks, regulators and supervisors

The CERES Forum, which officially launched on 1 July, is the first such global platform, bringing together these agencies to guard against ever-growing cyber and physical threats. Read the full release.

FS-ISAC 2018 CAPS Exercises

FINANCIAL SERVICES CAPS 2018 CYBER-ATTACK AGAINST PAYMENT SYSTEMS EXERCISE

The 2018 FS-ISAC Cyber-Attack Against Payment Systems (CAPS) exercises are gearing up. These regional, two-day, tabletop simulation exercises for payment professionals present a robust, real-world cyber-attack scenario to challenge incident response teams and test incident response preparedness. See below for the 2018 North America, Europe, Middle East and Africa (EMEA) and Asia-Pacific (AP) exercise dates. Learn more and view the FAQs.

- **AP Sessions |** 11-12 September or 18-19 September
- **EMEA Sessions |** 11-12 September or 18-19 September
- **North America Sessions |** 9-10 October or 16-17 October

© 2018 FS-ISAC, Inc. | All rights reserved. | fsisac.com | TLP **WHITE**

FINANCIAL SERVICES Information Sharing and Analysis Center