FINANCIAL SERVICES Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter **March 2017**

Newsletter Contents

Upcoming Webinars

All about the thousands of 2016 vulnerabilities. From Secunia Research.
Secunia | 15 March
Register here

Making Threat Intelligence Actionable with Security Automation & Orchestration
Phantom Cyber | 19 April
Register here

Upcoming Events

Member Meeting
Edinburgh, United Kingdom | 29 March
Register here

2017 FS-ISAC APAC Summit
Singapore | 2-5 April
Register here

Cyber-Intelligence Tradecraft Training
Reston, VA | 3-7 April
Register here

RIE in Singapore
Singapore | 5 April
Register here

2017 FS-ISAC Annual Summit
Lake Buena Vista, FL | 30 April-3 May
Register here

Cyber-Intelligence Tradecraft Training
London | 8-12 May
Register here

Member Meeting
Canada | 7 June
Registration will be available soon

Monetary Authority of Singapore and INTERPOL to Keynote APAC Summit

The agenda for the FS-ISAC 2017 APAC Summit taking place 3-4 April in Singapore is getting the final touches and we are excited to announce the keynote speakers for the event. Plan to join Ken Chua, Deputy Director, FinTech and Innovation Group, Monetary Authority of Singapore (MAS) on 3 April, for a presentation on Fintech and the Sandbox. Then on 4 April, hear from Paul Ward, Assistant Director of the INTERPOL Global Complex for Innovation (IGCI) Cyber Fusion.

For more information on these keynotes, additional sessions and the event view the official APAC Summit brochure, the one-pager or visit the APAC Summit site. Also, make sure to register today!

APAC Summit Brochure | One-pager | APAC Summit site | Register

Networking in the Magic of Epcot at the Annual Summit

Make sure to register for the FS-ISAC Annual Summit in Orlando today! Early bird registration will remain open until 1 April, so head on over to the Summit Website to register and check out all the exciting evets we have in store for you this year at the Summit.

While at the Summit, come and enjoy exclusive access to a little Disney Magic at Epcot and network with your peers! We will kick off the evening at the World ShowPlace, an exclusive event venue located inside of the Epcot World Showcase. You will step into a space featuring dinner, drinks and entertainment that includes the world-famous Illuminations: Reflections of Earth! Laser and Firework show and access to Soarin', the most popular ride in the park.

FS-ISAC Announces Mortgage Risk Council

FS-ISAC launched the Mortgage Risk Council (MRC) to provide an information sharing community for FS-ISAC members in the mortgage industry. Goals of the Council include: understanding cyber security risks as they relate to the mortgage industry; sharing experiences and best practices in cyber security for the mortgage industry; conducting benchmarking activities; interpreting and influencing legislature as it pertains to the mortgage industry. Membership to the council is specific for employees of FS-ISAC member firms in the mortgage industry whose responsibilities include: regulatory compliance, information and network security, threat detection, threat intelligence and/or incident response. If you wish to join the MRC, please email admin@fsisac.com.

Upcoming Events (cont.)

Cyber-Intelligence Tradecraft Training
Singapore | 19-23 June
Registration will be available soon

Member Meeting
London | 22 June
Register here

Affiliate Webinar - Phantom in Focus: Making Threat Intelligence Actionable with Security Automation & Orchestration

With no shortage of threat intelligence available to analysts, the bigger challenge nowadays is extracting value from shared intelligence without being overwhelmed by it at the same time. In this quarterly session hosted by Phantom CEO, Oliver Friedrichs, learn about automated indicator hunting, one of the many use cases for Security Automation & Orchestration platforms. Oliver will also share details about the newly announced Phantom 2.1 platform, as well as highlight the latest Phantom Apps which integrate security technologies, providing a layer of connective tissue between them.

Event Registration: https://tinyurl.com/jehqlvn

Sheltered Harbor Website Live

The Sheltered Harbor initiative — an industry effort to improve sector-wide resilience in the face of a cyberattack — recently launched its website, ShelteredHarbor.org. The site provides detailed information about the initiative, including frequently asked questions, and a form for those interested in joining. More information can be had by contacting info@shelteredharbor.org.

Call for Presentations: Fall Summit, European Summit

For every FS-ISAC Summit, our members are looked upon to propose topics and speakers to produce conferences tailored to the themes and topics you want to hear. Now is your opportunity to provide input for the Fall Summit in Baltimore, October 1-4, and the European Summit in London, October 30-November 1. Now is your opportunity to submit your proposal to present at one of these first-class summits.

Call for Presentations for the 2017 Fall Summit will open March 15, while European Summit presentation submissions will be accepted beginning March 30 – so start getting your proposal together and thinking about your submission! As always, visit the Summit site for more information.

Update From the ISAC Analysis Team

Dridex's Cold War: Enter AtomBombing
IBM X-Force discovered that Dridex, one of the most nefarious banking Trojans active in the financial cybercrime arena, recently underwent a major version upgrade that is already active in online banking attacks in Europe. IBM cybercrime labs detected Dridex v4, featuring updated code with a new and innovative injection method based on a technique dubbed AtomBombing, which was first disclosed in October 2016 by security firm enSilo. Dridex is the only banking Trojan encountered to use AtomBombing. This change is especially significant when it involves Trojans believed to be operated by an organized cybercrime gang because it's likely to result in other codes adopting the same method in the future.

Dridex's developers also worked on a major upgrade to the malware's configuration encryption. This upgrade includes implementing a modified naming algorithm, a robust but easy-to- spot persistence mechanism and a few additional enhancements. According to IBM Security detection, Dridex v4 is already out and active in campaigns that mostly target UK banks. Dridex attacks on online banking users in the UK are based on its hVNC RAT capabilities and redirection attack scheme, which appears to have replaced the webinjects method as Dridex's top M.O.

Adobe Security Bulletins
On February 14, 2017 Adobe released security updates for Adobe Flash Player and Adobe Campaign. The Adobe Campaign update resolves a moderate security bypass vulnerability affecting the Adobe Campaign client console. An authenticated user with access to the client console could upload and execute a malicious file, potentially resulting in read and write access to the system. This update also resolves a moderate input validation issue that could be used in cross-site scripting attacks.

The Adobe Flash Player updates address vulnerabilities rated as Priority 1, meaning that the update resolves vulnerabilities being targeted, or which have a higher risk of being targeted by exploits in the wild. The Flash vulnerabilities could result in remote code execution and allow an attacker to take control of the affected system. Vulnerability types include type confusion, integer overflow, use-after- free, heap buffer overflow, and memory corruption. At this time, the IAT has not detected any reports of these Priority 1 vulnerabilities being exploited in the wild.