FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | March 2018

TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

Rescheduled: Enabling Real, Multi-Layer Mobile Security: EFT, DRM and Third-Party AppSec Vetting* | 13 March

FS-ISAC Expert Webinar Series: How Intelligent Assistants Augment the SOC Team* | 20 March

Threat Intelligence - an Active Cyberdefense Posture Training
23-27 April | Reston, VA
7-10 May | Singapore

Member Meetings*
16 May | Cape Town, South Africa
13 June | Stockholm
14 June | London

Member Receptions*
3 July | Dublin
6 November | Edinburgh

2018 FS-ISAC Summits

2018 FS-ISAC Annual Summit
20-23 May | Boca Raton, FL

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

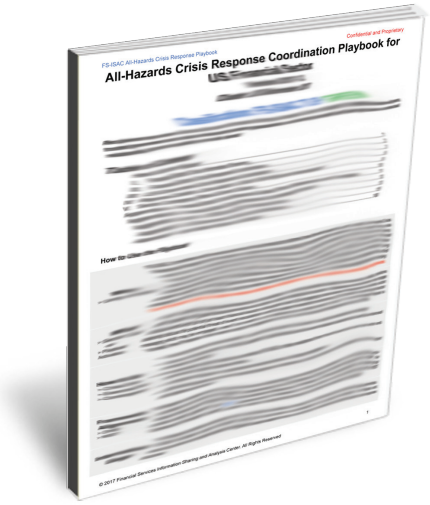
2018 FS-ISAC EMEA Summit
1-3 October | Amsterdam

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

All-Hazards Crisis Response Playbook Gets an Update

A critical role of FS-ISAC is to evaluate, communicate, coordinate, escalate and respond to major cyber and physical events. This helps the financial sector to be more resilient. FS-ISAC's recently updated the *2016 All-Hazards Crisis Response Coordination Playbook* to:

- Clarify how various sector stakeholder's Playbooks align with the All-Hazards Process
- Incorporate the Financial Systemic Analysis & Resilience Center (FSARC) and Sheltered Harbor activities
- Expand the listing of Media Response Team (MRT) activities
- Include new government crisis response standards: Presidential Policy Directive 41, National Cyber Incident Response Plan (NCIRP) and the Cybersecurity Enhanced Coordination Procedures (CECP)
- Add instructional crisis team appendices
- Simplify playbook activation
- Add the roles of FDIC and Federal Reserve, observed during Hurricane Maria



To see the latest playbook, visit the FS-ISAC member portal.

FS-ISAC Enables Safer Financial Data Sharing Among Financial Institutions and Aggregation Companies

In an effort to keep consumer financial information and businesses safer from cyberattacks, the FS-ISAC announced the publication of an updated application programing interface (API) for secure, tokenized data transfer. The *free* API and its associated Control Considerations White Paper, is the culmination of more than one year of activities of the FS-ISAC Data Aggregation Work Group, comprising more than 25 financial services firms and contributions from multiple financial technology firms that provide data aggregation tools and services. Creating a standard API for secure data sharing benefits everyone in the data aggregation ecosystem. Members may access the FS-ISAC Portal to for the API and whitepaper.

ISAC Analysis Team Update

Adobe Security Updates Address Vulnerability on Remote Code Execution

Adobe has released security updates for Adobe Flash Player for Windows, Macintosh, Linux and Chrome OS. These updates address critical vulnerabilities that could lead to remote code execution in Adobe Flash Player 28.0.0.137 and earlier versions. Successful exploitation could potentially allow an attacker to take control of the affected system. Adobe is aware of a report that an exploit for CVE-2018-4878 exists in the wild, and is being used in limited, targeted attacks against Windows users. These attacks leverage Office documents with embedded malicious Flash content distributed via email. Cisco's Talos identified that an attacker exploited this vulnerability with a Flash object embedded in a Microsoft Excel document. By opening the document, the exploit was executed to download an additional payload from a compromised website. They identified that the downloaded payload is the well-known Remote Administration Tool named ROKRAT. Group123 was identified in Cisco's report, in which they noted that they now confidentially assess Group 123 has a highly skilled, motivated, and sophisticated group. FireEye believes the threat actor is North Korean and is tracking them as TEMP.Reaper. FireEye observed operators directly interacting with their command and control infrastructure from IP addresses assigned to the STAR-KP network in Pyongyang. At this time, the FS-ISAC is not aware of any US targeting by Group123. Members are now highly encouraged to apply the new Adobe Flash Player update at their earliest convenience, pending internal policies and reviews.

Two New SWIFT Related Incident Reported

Last week, news media reported two (2) SWIFT related incidents. One involved a Russian bank where threat actors reportedly stole $6 million USD by compromising a computer within the bank's network. The computer presumably had access to the bank's SWIFT system which likely resulted in the actors issuing SWIFT instructions to transfer money to their own bank accounts. Another incident involved an Indian bank which reportedly lost nearly $2 million USD to threat actors who had compromised the bank's systems and issued three unauthorized remittances via the bank's SWIFT system to lenders overseas. So far, we do not have any other information about the attack vectors or malware used for these incidents. FS-ISAC members with any information are encouraged to share on the member Portal.

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!

New FS-ISAC Training: Threat Intelligence - an Active Cyberdefense Posture

Identify threats with hands-on experience in a safe, digital environment.

Join FS-ISAC and training partner BlackHorse for a five-day, fully immersive and bespoken digital training program that equips attendees with the skills to safely and effectively research open source and publicly available information on the internet for a myriad of threat identification, resource allocation and security objectives. Experience a complete digital immersion in commercial best practices and techniques to safely and securely gain advanced techniques and methods to identify threats originating from easily accessible data domains such as publicly available information, social media and many more. Upcoming sessions in Reston, VA and Singapore. Learn more and register today.

Building Cybersecurity Diversity (BCD) Scholarship – AP and US Taking Applications

The women's scholarship program is going global. FS-ISAC is now offering scholarships to women in Singapore, the United Kingdom and the United States. If you know someone a female student in cybersecurity please make sure to alert them on this outstanding opportunity. Applications are currently open for AP (Singapore) and US. The UK (London) application will open on 15 March. If you have questions or need more information, please visit us online or email us today.