



FINANCIAL SERVICES

Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter

May 12, 2015

Newsletter Contents

FS-ISAC Webinars	1
Upcoming Events	1
FS-ISAC Announces Strategic	1
2015 BITS Emerging Payments Forum	1
New Membership Guides Available on	1
Recorded Version of Alert Filtering	1
FS-ISAC 2015 CAPP – Europe	1
FS-ISAC European Summit Call for	2
FS-ISAC Fall Summit – Registration	2
SOC Update	2

FS-ISAC Webinars

Endpoint Threats: Detecting the Undetectable (live webcast)

RSA | June 3

[Register here](#)

How to Tell Your Boss that Your Job has Changed

BAE Systems | June 10

[Register here](#)

SSL Encrypted Traffic Management Managing Risk Within Financial Institutions

Blue Coat | June 19

[Register here](#)

Upcoming Events

FS-ISAC & BITS Annual Summit

Miami Beach, FL May 17-20

[Register here](#)

FS-ISAC Cyber Threat Intelligence Training

Reston, VA June 8-12

[Register here](#)

Information Sharing Workshop

Toronto, Canada June 23

[Register here](#)

Information Sharing Workshop

Frankfurt, Germany July 14

[Register here](#)

FS-ISAC Announces Strategic Agreement with R-CISC

Through a new strategic agreement, FS-ISAC will provide key advisory services and best practices, operational support and technology capabilities to the Retail Cyber Information Sharing Center. The agreement will also enable the two information sharing centers to establish strong cross-sector sharing to better defend against cyber threats. “The R-CISC has worked diligently to establish cyber intelligence sharing in the retail sector. The new agreement with FS-ISAC will help R-CISC focus on its core mission and take information sharing to the next level.”

2015 BITS Emerging Payments Forum

FS-ISAC President and CEO Bill Nelson will be speaking at the 2015 BITS Emerging Payments Forum in Washington, D.C. on June 2nd and 3rd. This forum, which is attended by leaders from the financial services industry, technology firms, security and data providers, and government agencies will focus on threats to the payments systems, innovations and consumer interest in the payments space, critical security, fraud and resiliency controls, and emerging legislative issues and regulatory compliance challenges. A full speaker lineup and agenda can be found [here](#).”

New Membership Guides Available on the Portal

In case you missed it: A new version of the membership guide is now available on the FS-ISAC Portal. The new version incorporates an updated list of councils and working groups including the Media Response Team (MRT), Broker-Dealer Council (BDC), Card Reissuing Best Practice Working Group (CRBPWG), and Technology Service Providers Best Practice Working Group (TSP BPWG). The new membership guide can be found in the “Member Resources” document folder on the portal.

Recorded Version of Alert Filtering Webinar

Feeling overwhelmed with the amount of FS-ISAC SOC Alert Emails? Learn how to customize and manage your portal alerts to achieve the maximum benefit from your FS-ISAC membership. FS-ISAC Webinar – “Aid to Processing Shared Information” is now available in both the “Member Services” and “FS-ISAC Webinars” document folder on the portal.

FS-ISAC 2015 CAPP – Europe

FS-ISAC will offer the first ever Cyber-Attack Against Payment Processes exercise exclusively for European financial institutions on September 15-16 and September 22-23. CAPP-Europe will simulate a robust, real-world attack to challenge IR teams to practice mobilizing quickly, working under pressure, critically appraising information as it is available, and connecting the cyber dots to defend against the attack.

[Register today](#) or visit the [website](#) for more information.

FS-ISAC’s global team is looking for members to host threat calls. European Threat Calls are two Thursday’s a month at 14:00BST 15:00CEST and 9:00EDT, if any member in the European region would like to host a call, please reach out to events@fsisac.us. The APAC Threat calls are the last Wednesday of each month at 9am SGT 10am JST and 11am AEST. If any member in the Asia-Pacific region would be interested in hosting a call, please reach out to events@fsisac.us.



FS-ISAC European Summit Call for Member Presentations

Presentation proposals from FS-ISAC Members are now being accepted for the FS-ISAC European Summit, scheduled for November 30 – December 2, 2015 in London.

Member Call for Presentations

Open: 11 May
Close: 7 July, 5:00pm EDT
Notification of Acceptance: 31 July

www.fsisac-summit.com/eu-call-for-pres

Click on 'For Members:' to submit.

For members, a proposal of either a panel, standalone, or co-presentation can be submitted. There is no cost to members for speaking sessions. Member submissions that involve a sponsor will be considered sponsor sessions.

FS-ISAC European Summit – Registration is also now open!

www.fsisac-summit.com/attendee_registration_EU

FS-ISAC Fall Summit – Registration is Open!

www.fsisac-summit.com/2015-fall-summit

[Register here](#)

Member Call for Presentations

Open: April 15
Close: June 19, at 5:00pm EDT
Notification of Acceptance: July 10

www.fsisac-summit.com/fall-call-for-presentations

Click on 'For Members:' to submit.

For members, a proposal of either a panel, standalone, or co-presentation can be submitted. There is no cost to members for speaking sessions. Member submissions that involve a sponsor will be considered sponsor sessions.

From the FS-ISAC Security Operations Center

CryptoWall – a New Wave of Ransomware

Over the last few months, the FS-ISAC SOC has been tracking malicious activity associated with CryptoWall ransomware.

Like other encrypting ransomware, CryptoWall encrypts the victim's files, then prompts the victim to pay a ransom to receive the decryption key (via Bitcoin). The latest version, CryptoWall 3.0, has incorporated use of the TOR network to hide its C2 and victim payment servers, similar to the CBT-Locker (AKA Citroni) ransomware. Recent CryptoWall campaigns are being delivered using the Angler Exploit Kit, leveraging a vulnerability in Adobe Flash Player (CVE-2015-3043).

Patches for the Flash Player vulnerability were made available by Adobe in April 2015, and are described in [APSB15-06](#).

There is no reliable way to decrypt the files, short of paying the ransom. The FS-ISAC SOC 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.

Critical Vulnerability in WordPress CMS

In April, a critical cross-site scripting (XSS) vulnerability was publicly reported in WordPress Content Management System (CMS). By submitting carefully crafted content via WordPress's "comment" feature on a vulnerable WordPress site, an attacker can potentially execute arbitrary code on the server, or gain administrator control of the site.

On April 27, WordPress released version [4.2.1](#) to address this vulnerability.

WordPress, along with other CMS applications, have been popular targets of hackers, largely because they often run outside of a company's Information Security programs, resulting in a lack of regular patching and security testing. Once compromised, hackers can gain access to sensitive information stored in the system, host malicious applications, or use it as a platform to launch Distributed Denial of Service (DDoS) attacks on other organizations.

The FS-ISAC SOC encourages financial institutions to:

1. Inventory internal systems, to ensure that systems containing sensitive information are not operated outside of the company's Information Security program.
2. Ensure that all systems and applications are subject to patch management, event monitoring, and security auditing.
3. Verify that CMSs like WordPress do not run 3rd party addons that do not provide regular patch updates.