



Newsletter Contents

FS-ISAC Publishes 2017 – Mid 2018 Annual Report

Call for Presentations for 2019 Annual Summit Now Open

FS-ISAC Launches Banking and Fintech Collaboration to Enhance Security and Consumer Control

ISAC Analysis Team Updates

Upcoming Events and Webinars

* FS-ISAC members-only

Cyber-Range Ransomware Exercise

30 January | Federal Reserve Bank of Boston

13 February | Zurich

19 March | Federal Reserve Bank of Atlanta

Expert Webinar Series*

Overcoming the Top Ten Challenges to Omnichannel Fraud Management

27 November

Expert Webinar Series*

Using the Power of Threat Intelligence to Disable Banking Trojans

11 December

Security Innovation Webinar: Your Bank's Digital Side Door | 27 November

Member and Chapter Meetings*

6 November | Edinburgh (Chapter Meeting)

13 November | Frankfurt

13 November | Tokyo

13 November | Sao Paulo

14 November | Israel

19 November | Mumbai

21 November | Sydney

27 November | Vienna

5 December | London (Chapter Meeting)

12 February 2019 | Zurich

6 March 2019 | London

FS-ISAC 2018 Fall Summit

11-14 November | Chicago

Cyber-Attack Against Insurance Systems (CAIS) Exercise

19-20 March or 26-27 March 2019 | Online

FS-ISAC 2019 Annual Summit

28 April-1 May | Orlando

Call for Presentations 31 Oct-5 Dec

FS-ISAC Publishes 2017 – Mid 2018 Annual Report

FS-ISAC recently unveiled the [2017–Mid 2018 Annual Report](#). Some of the highlights include:

- Expanded globally to 7,000 members with headquarters in 45 countries;
- Responded to major threats and incidences including global ransomware attacks, response to the breach of a major consumer reporting bureau, account takeover attempts, major software vulnerabilities, compliance with Europe's General Data Protection Regulation (GDPR) and numerous hurricanes;
- Grew member engagement in our [Expert Webinar Series](#) and [Solutions Showcases](#);
- Opened Asia Pacific Regional Intelligence and Analysis Centre in Singapore to supplement our operations in London and our primary operations center in Reston, VA;
- Matured analysis via the Global Intelligence Office and the publication of *Technical Analysis Reports*, *Weekly Watch Reports*, *Spotlight Reports* and *Flash Reports*;
- Launched new cyber-range exercises; achieved record attendance for [CAPS exercises](#); collaborated with US Treasury and FSSCC on additional "Hamilton Series" exercises;
- Introduced new program to brief member CEOs and board of directors on cyber-risk;
- Broke attendance records at our four Summits; and
- Supported Sheltered Harbor and Financial Systemic Analysis & Resilience Center (FSARC).



Read the [2017–Mid 2018 Annual Report](#).

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 discounts page** to see current offers. Make sure to bookmark and check back often as offers are updated and added frequently!

ISAC Analysis Team Updates

Application Vulnerability Related to jQuery File Upload

A widely used plugin for jQuery, called *jQuery File Upload*, is affected by an 8-year-old vulnerability (CVE-2018-9206) that potentially places nearly 8,000 different software applications at risk for remote code-execution (RCE). jQuery File Upload is an open-source package for developers that can be described as a file upload Widget for jQuery with multiple features. The PHP upload handler in versions before v9.24.1 allowed uploading of all file types in the web server's root path by default. After writing up a quick test, the discoverer, Cashdollar, was able to confirm that he could upload a web shell and run commands on the server with the privileges of the web server. Cashdollar noted that the attacker does not need any form of authentication to upload files onto the server. This could open a window to a whole set of attacks.

The flaw was introduced when Apache webserver disabled a default security control, and Adversaries have already posted proof-of-concept videos online showing how to exploit the problem. jQuery File Upload creator, Blueimp, has corrected the problem in the latest version of its software, by only allowing image-file uploads by default. However, applications that use the base code will have to issue their own fix. Members who use jQuery File Upload code are highly encouraged to update to the latest fixed version if possible.

GandCrab Decryption Tool Released for Multiple Ransomware Versions

The *No More Ransom* project released an updated decryption tool for the GandCrab ransomware. The tool was developed by the Romanian Police, Europol and Bitdefender, with support from the FBI and other law enforcement agencies. It can recover files locked by GandCrab v1, v4 and the latest v5. Bitdefender also said they're still working on creating a decrypter for v2 and v3. The Romanian antivirus maker was able to create the latest decrypter after the GandCrab developer released legitimate decryption keys for victims located inside Syria, out of compassion. With its ransomware-as-a-

service model, GandCrab has been the most active and widespread ransomware strain this year, taking the place of Locky and Cerber, which were the leading ransomware strains of 2016 and 2017.

A week after Bitdefender released the first version of the decryption tool (March 2018), the malware developer released GandCrab v2. In August 2018 after antivirus company AhnLab released a vaccine to prevent victims from being infected with a particular GandCrab version, the author included a zero-day vulnerability for the antivirus inside the malware's code. The GandCrab author never took any retaliatory action against Bitdefender or any law enforcement agencies involved in the making of the decryption tool after its first release. The ISAC Analysis Team will continue monitoring these events and provide updates and details as needed.

FS-ISAC Launches Banking and Fintech Collaboration to Enhance Security and Consumer Control

FS-ISAC, together with top banks, financial technology firms (fintechs) and other industry groups, announced the creation of the Financial Data Exchange (FDX) in mid-October. FDX creates an interoperable standard enabling secure data sharing, providing consumers with greater control and fostering innovation.



In the past, the sharing of data from a financial institution (FIs) with an aggregator was accomplished through "screen-scrapping". Now, a single standard for the sharing of consumer data will eliminate the need for the archaic "screen-scrapping" technique. In addition to making data sharing easier between FIs and fintechs, the FDX platform will give consumers more control over their data. [More](#).

Call for Presentations for 2019 Annual Summit

The Call for Presentations (CFP) for the 2019 Annual Summit, 28 April-1 May in Orlando, is now open!

Increase your visibility, share your knowledge and showcase your expertise – [submit your proposal](#) for the Annual Summit. The deadline for submissions is **5 December 2018**. Visit the [Summit site](#) to learn more about FS-ISAC Summits.

Follow us on Twitter @FSISAC or join the discussion on LinkedIn.

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

