FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter February 2017

Newsletter Contents

Upcoming Webinars

The SANS 2016 Survey on Security and Risk in the Financial Sector
ForeScout Technologies | Available for viewing until 31 March
Register here

Application Security Essentials Toolkit
Whitehat Security | Available for download until 31 March
Register here

Upcoming Events

Make Your Case with Compelling Analysis
Reston, VA | 13-14 February | [Optional add-on course 15-16 February — Break the Mold with Innovative Techniques]
Register here

Break the Mold with Innovative Techniques
Reston, VA | 15-16 February | [Optional add-on course 13-14 February — Make Your Case with Compelling Analysis]
Register here

Member Meeting
Sydney, Australia | 22 February
Register here

Member Meeting
Irving, TX | 27 February
Register here

Strategic Foresight Analysis
Reston, VA | 7-9 March | [Optional add-on course 8-9 March — Managing Analysis]
Register here

Registration Open for the APAC and Annual Summits

Registration is now open for both the APAC Summit (3-4 April, 2017 in Singapore) and Annual Summit (30 April-3 May, 2017 in Lake Buena Vista, FL). Don't miss your chance to attend these unique events! Early Bird Registration will remain open until 17 March for the APAC Summit and 1 April for the Annual Summit. Sign up today!

FS-ISAC Summits highlight the world's leaders in information and physical security. From information sharing to the internet of things, and from ransomware to threat automation, the Summits' sessions deliver ground-breaking content and are one of the industry's "must attend" events. For more information, visit the new FS-ISAC Summit website and view the APAC Summit and Annual Summit (coming soon!) Brochures, hotel and travel information, and agendas.

Register for the APAC Summit | Register for the Annual Summit

Disruption to Digital Crown Jewels: Compelling APAC Summit Sessions

Be sure to catch-up on some of the unique and exciting presentations at this year's APAC Summit. Presentations at FS-ISAC Summits are all vetted by FS-ISAC members and these highly relevant and timely sessions are presented by members, partners and affiliates. Recently added sessions include:

Digital Disruption: Reducing Risks in a Digital Age | Common use cases from a dozen Financial firms have been compiled and analyzed over the past 12 months to showcase how new architectures and threat intelligence can tackle the entire range of external threats from traditional phishing to the latest social media attacks.

Crown Jewels and Data Assets | Data in the digital age is a crown jewel asset, yet many financial institutions are challenged to understand the entire spread of where their data assets are and where they go, let alone the controls required to secure their data at rest, in transit and in use. Learn how an outcome-focused approach to data security through a business enabled process re-engineering lens will help build and drive an information loss prevention program.

Global Services Update

In February, FS-ISAC is launching a new regional governance structure in further support of our existing mission. This new model creates Regional Threat Intelligence Committees (RTICs) and Regional Strategy Committees (RSCs) in the EMEA and APAC regions. These new groups enable FS-ISAC and its membership to provide increased regional focus of threat intelligence, address region-specific challenges and enhance relevant services to our members around the globe. The members of these committees have been selected via peer nominations. Many of these groups will start work in February 2017.

Join the Discussion!
Fraud and cybercrime mailing lists for EMEA and APAC members bring fraud investigators, analysts and eCrime intelligence specialists together to discuss trends and policy issues. The new ATM Security list unites global ATM Security managers, engineers, investigators and ATM brands together to discuss best practices and the threat landscape. Also, we invite members to participate in a number of working groups catered to specific topics like Legal & Regulatory (Europe), Insider Threat (all regions) and Security Testing (Europe). If you are interested in getting involved in any of these lists or groups, please contact admin@fsisac.com with "ATM Security list inquiry" in the subject line.

Upcoming Events (cont.)

Managing Analysis
Reston, VA | 8-9 March | [Optional add-on course 6-7 March — Strategic Foresight Analysis]
Register here

Research Design for Analysis
Online | 14-28 March
Register here

Member Meeting
Edinburgh, United Kingdom | 29 March
Register here

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

Sheltered Harbor Membership Expanding

Sheltered Harbor is a financial industry resiliency initiative that will enable restoration of customer account data in the event of the loss of an institution's operational capability. This initiative, announced in November 2016, is now expanding membership to the broader banking and brokerage community. FS-ISAC is heavily involved and we are now working with the Sheltered Harbor team to promote the initiative and encourage increased participation. If you would like further information on how to join, please contact Info@shelteredharbor.org

Help Develop the FS-ISAC Security Kit

FS-ISAC has developed a Security Kit to provide smaller member institutions with a set of security practices to help them strengthen their information security program in light of the increasing security threats in the financial services sector. The product continues to evolve and offers value to small, medium and large institutions.

Progress on this effort can be tracked here: (portal.fsisac.com/group/fs-isac-organization/wiki). Also, there are many more topics that we can include in our Security Kit and we are looking for members to contribute content of their interest. Send an abstract on your topic and we'll assist you in finalizing the material for the Security Kit! All submissions can be sent to John South (jsouth@fsisac.com).

Update From the ISAC Analysis Team

Oracle Critical Patch Update - January 2017
As part of its quarterly Critical Patch Update (CPU), Oracle patched 270 vulnerabilities in January 2017 across 45 different products. This included E-Business Suite and MySQL database. Around 40 percent of the issues fixed were remotely exploitable without authentication. In 2015, the average number of vulnerabilities Oracle patched was 153 per quarterly patch. Last year that figure shot up to 227. Oracle strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update fixes without delay.

Zeus Sphinx Trojan infection campaign leveraging Sundown EK
With the disappearance of the Angler and Nuclear exploit kits, a gap was left in the market that has been quickly filled by more prominent kits such as RIG EK and its variants. Smaller players like Sundown, however, have also stepped up to claim their place in the market.

According to Trend Micro, the newly updated Sundown EK was used by multiple malvertising campaigns to distribute malware. The most affected countries were Japan, Canada, and France, with Japanese users accounting for more than 30% of the total targets. IBM Trusteer reported on new Zeus Sphinx Trojan infection campaigns, with configurations targeting banks in Canada. In other previous campaigns, Sphinx variants targeted UK banks in 2015, or Brazilian banks just last summer coinciding with the summer Olympics. In this case, Sphinx's operators focused the target list on Australian banks and Canadian credit unions (likely seeing them as the lower hanging fruit in Canada's financial sector). These operators have been using two distribution methods in their recent campaigns, including malvertising that leads to the Sundown exploit kit.

The ISAC Analysis Team will continue monitoring Zeus Sphinx Trojan infection campaigns and Sundown EK updates for any activity that may affect financial institutions.