FINANCIAL SERVICES | Information Sharing and Analysis Center

Newsletter Contents

Upcoming Webinars

Cybersecurity: Three Lines of Defense
Ernst & Young | 12 January
Register here

Strategy and Tactics for Securing Mobile Devices in Financial Organizations
Skycure | 26 January
Register here

Upcoming Events

Crack the Code with Diagnostic Techniques
Reston, VA | 17-18 January | [Optional add-on course 17-18 January — Make Your Case with Compelling Analysis]
Register here

Make Your Case with Compelling Analysis
Reston, VA | 19-20 January | [Optional add-on course 17-18 January — Crack the Code with Diagnostic Techniques]
Register here

Critical Thinking: From Conceptualization to Presentation
Reston, VA | 23-26 January
Register here

Critical Thinking Fundamentals
Online | 7-21 February
Register here

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

Registration Now 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!

FS-ISAC Summits are focused around peer-to-peer networking and building relationships or circles of trust with financial services organizations. We invite you to attend and see what new sessions and exciting innovations are developing around information sharing amongst financial institutions and threat intelligence practices.

Register for the APAC Summit | Register for the Annual Summit

New Format for Annual Summit

The 2017 FS-ISAC Annual Summit, which takes place 30 April-3 May at the Walt Disney World Swan and Dolphin in Lake Buena Vista, Florida, will feature a brand-new agenda format!

One major change you will see is the keynote has moved to Monday, 1 May at 2:30 p.m. ET. Previously the keynote was given on Tuesday morning – so please be sure to note the change so you don't miss this great presentation. Additionally, please note that the Member Technical Forum will take place on Wednesday, 3 May from 1:30 to 5 p.m.

View the early agenda and learn more about the hotel including making your online reservations.

APAC Summit Session Preview

We rely on our members to generously volunteer to help us provide the high-quality, relevant content that our Summits are famous for. We know how valuable the content is and this year's APAC Summit will feature another great collection of sessions including:

- NextGen SOCs - From Training to Cognitive | In this session learn how the next generation of SOCs are moving away from classic IT "moat and castle" approach to end-to-end incident handling, the use of cognitive computing and even military grade cybertraining. Featuring real-life scenarios, this session will share today's approach to building a SOC looking at how to handle every aspect from prevention to detection, mitigation, incident response, data sharing, media handling and more. Learn how cognitive computing is a new game changer for security teams fighting fraud and cybercrime. Finally, learn the threats being seen, specifically for the financial industry, but also issues like IoT security, the use of dark web and trends in cybercrime groups.

- Managing Integrity and Trust of Financial Institutions in the Wake of Digital Transformation and Rising Cybersecurity Challenges | Financial service institutions are embracing the cloud more than ever before and are widely regarded as having implemented the most advanced safeguards for protecting sensitive information and defending against cyber-attacks. Despite spending millions on digital security, data breaches in this sector continue to occur at an alarming rate, with the integrity and trust of the industry at stake. In this session, myths about security in the cloud will be dispelled and a clear path to protecting your organization against phishing, ransomware and other back-end cyberthreats will be shared. This session will include guest panelists from the APAC legal and regulatory communities and cloud experts to discuss overcoming perception barriers to the cloud to combat cyberthreats and ensure compliance in every organization.

For more information on these sessions, additional sessions and the event view the one-pager or visit the APAC Summit site. Also, make sure to register today!
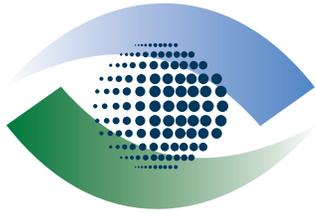
FINANCIAL SERVICES | Information Sharing and Analysis Center

Upcoming Events (cont.)

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
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

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

New Summit Website Launched

New year, new look! FS-ISAC is pleased to announce the launch of our new Summit website. The site was updated to provide easier navigation and showcases a clean, modern look - we invite you to take a look - visit now.

Training and Awareness Whitepaper & Templates Available

The *Training and Awareness Working Group* under the Products & Services Committee developed a whitepaper on best practices for establishing, managing and leading an information security awareness program. The whitepaper is now available on the FS-ISAC Portal located here Home>Workgroup Whitepapers and Deliverables>Security Awareness and Info Awareness Sharing Practices>Information Security Training and Awareness - Whitepaper & Templates. The Working Group also gathered and developed awareness related templates that can be customized to your organization, and they can be found along with the whitepaper.

Interested in learning more about the Training and Awareness Group?
The group invites you to attend their 2017 calls. The calls will focus both on end user awareness topics such as phishing/social engineering and awareness program related topics like creating champion/ambassador programs and demonstrating program value. If you would like to participate on the calls in 2017, please send an email to admin@fsisac.com.

If you have any questions about the whitepaper and template material, or if you would like to contribute templates from your organization, please contact israel.bryski@etonpark.com.

Update From the ISAC Analysis Team

Android Security Bulletin
January's Android Security Bulletin contained details of security vulnerabilities affecting Android devices. Impacts included DoS, information disclosure, elevation of privileges, and system access. The most severe of these issues is a critical security vulnerability that could enable remote code execution on an affected device through multiple methods such as email, web browsing and MMS when processing media files.

2017 Cyber Security Predictions
To bring in the new year, various companies published their predictions of cyber security issues that will be notable in 2017. Trends in predictions across reports include further development and frequency of Internet of Things (IoT) attacks, targeting of industrial systems, and increase in attacks directed at corporations. Concerning the financial services industry, Palo Alto predicts that institutions will continue to adopt public cloud computing and adopt more multi-factor authentication (MFA) in light of stolen credentials and fraudulent fund transfers seen by SWIFT member banks. The company further predicts that in 2017 attackers may target weaknesses in blockchain technology to compromise financial transactions.

Alice: A Lightweight, Compact, No-Nonsense ATM Malware
Trend Micro published a report on a new family of ATM malware called Alice. Unlike other ATM malware families, Alice cannot be controlled via the numeric pad of ATMs; neither does it have information stealing features. It is meant solely to empty the safe of ATMs. Based on PE compilation times and Virus total submission dates, Alice has been in the wild since at least October 2014. Several things stand out about Alice. It is extremely feature-lean and, unlike other ATM malware families, it only includes the basic functionality required to successfully empty the money safe of the ATM. It only connects to the CurrencyDispenser1 peripheral and it never attempts to use the machine's PIN pad. The logical conclusion is that the criminals behind Alice need to physically open the ATM and infect the machine via USB or CD-ROM, then connect a keyboard to the machine's mainboard and operate the malware through it.