FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter   November 2016

Newsletter Contents

FS-ISAC Webinars

[Case Study] Triage & Collaboration: Improving a Major's Bank Cyber Threat Security Posture | EclecticIQ | Available for download until November 22
Register Now

Critical Thinking Fundamentals | online | January 8-22
Register Now

Upcoming Events

FS-ISAC Workshop at RSA
Abu Dhabi, United Arab Emirates | November 14
Register here

Member Meeting
Melbourne, Australia | November 28
Register here

Member Meeting
London, United Kingdom | December 6
Register here

FS-ISAC Announces the Financial Systemic Analysis and Resilience Center

On October 24, the FS-ISAC announced the formation of the Financial Systemic Analysis and Resilience Center (FSARC). The FSARC's mission is to proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the US financial system from current and emerging cyber security threats through focused operations and enhanced collaboration between participating firms, industry partners, and the US Government, including the Department of Treasury, the Department of Homeland Security and the Federal Bureau of Investigation.

Earlier this year, the CEOs of eight banks – Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street and Wells Fargo – came together to proactively identify ways to enhance the resilience of the critical infrastructure underpinning much of the US financial system. The FSARC plans to invite other financial institutions that are designated by the US Government as critical infrastructure to join. The FSARC will continue to collaborate with its valued government partners and will expand its operational processes, establishing a physical location for the center and adding additional financial institutions that wish to participate in similar efforts. The FSARC is affiliated with FS-ISAC and complements the mission of FS-ISAC. Findings and adaptable mitigation strategies will be shared across the financial sector through FS-ISAC and membership.

Call for Presentations Deadline Extended

The call for presentations deadline has been extended to November 18 at 5:00 pm EST for the APAC Summit in Singapore, April 3-4. Submit your proposal today for a chance to speak before hundreds of your industry peers. Member presentations are an integral part of the Summit experience, and can be submitted as either a standalone or co-presentation. For more information and tips for selection visit fsisac-summit.com/apac-call-for-presentations.

The deadline for the Annual Summit in Orlando, April 30 – May 3, call for presentations remains November 30. For more information, tips for selection and suggested presentation topics, visit fsisac-summit.com/annual-summit-call-for-presentations.

Fall and European Summit Recap

The 2016 FS-ISAC Fall Summit in Nahsville set a new registration record with nearly 1,000 attendees, making it the most successful Fall summit in FS-ISAC history. Admiral James Stavridis delivered a thought provoking keynote on "Sailing the Cyber Sea: The New Realities of 21st Century Security." Members chose from over 70 intriguing member sessions, breakout sessions, panel discussions, workshops and sponsor showcases.

In Europe, members flocked to Barcelona for the 2016 European Summit, held November 6-9. The Summit featured keynote speaker, Sebastien de Brouwer, Executive Director, Retail, Legal, Economic and Social Policy at the European Banking Federation.

If you were unable to make it to the Summits you can read through all presentations from the Summit on the FS-ISAC portal! After logging in, head to the "Conference Materials" folder in the documents tab to review presentations from this year's event. Topics range from new social engineering trends, to the boardroom's role in cybersecurity, to third-party risk management and more!

FS-ISAC Expands Course Catalog – New Onsite and Online Sessions

FS-ISAC worked with Globalytica to create an analytical training program that provides members access to expert training courses designed to improve their critical thinking, analytic and presentation skills. The online and classroom courses address a variety of topics including fundamentals of intelligence analysis, critical thinking skills, effective writing and briefing, the use of structured analytic techniques and managing analysis.

Critical Thinking Fundamentals
8-22 January | Online
More | Register

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

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

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

To learn more about the program, view upcoming courses and register visit fsisac.com/trainings.

Update From the ISAC Analysis Team

Oracle Critical Patch Update Advisory - October 2016
Oracle released its Critical Patch Update last month offering 253 fixes for 76 products. The fixes apply to Oracle Database Server, E-Business Suite, Industry Applications, Fusion Middleware, Sun Products, Java SE and MySQL. Of those, 15 are critical with a CVSS score of 9.0 or more. The more severe bugs make it possible to compromise Oracle Web Services, Big Data Discovery, Oracle Commerce or WebLogic over HTTP.

In their release announcement, Oracle also strongly recommended that customers remain on actively-supported versions and apply Critical Patch Update fixes without delay since the company continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released fixes.

Linux Privilege Escalation Vulnerability (Dirty COW)
Phil Oester, a Linux researcher, found a race condition in the way the Linux kernel's memory subsystem handled the copy-on- write (COW) breakage of private read-only memory mappings. This allows an unprivileged local user to use this flaw to gain write access to otherwise read-only memory mappings and increase their privileges on the system. A proof-of- concept was released by the researcher who reported it and the Linux Kernel was patched two weeks ago.

Oester explained that the exploit is easy to execute and will almost certainly become more widely used. In October, he notified software vendor Red Hat of recent incidents where an attacker had deployed exploit code that leveraged Diry COW. Oester said that he uncovered the exploit for the bug, which has been around since 2007, while examining a server that appeared to have been attacked. He was able to extract the exploit and provide a Proof-of-Concept.