FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter April 2017

Newsletter Contents

Upcoming Webinars

Stop the Heist: Prevent Malware from Ruining Your Bank
Citrix | 13 April
Register here

Making Threat Intelligence Actionable with Security Automation & Orchestration
Phantom Cyber | 19 April
Register here

On-Demand Webinar 2016 Vulnerabilities – Insights from the Annual Vulnerability Review.
Flexera Software | download through 31 May
Register here

2017 Vulnerability Review
Flexera Software | download through 31 May
Register here

Threat Intelligence and Third-Party Risk Control: Protecting Your Extended Partner Network
RiskRecon | 25 May
Register here

Upcoming Events

2017 FS-ISAC Annual Summit
Lake Buena Vista, FL | 30 April-3 May
Register here

Cyber-Intelligence Tradecraft Training
London | 8-12 May
Register here

Critical Thinking Fundamentals
Online | 30 May-13 June
Register here

Annual Summit Fast Approaching

Join leading experts and peers at the FS-ISAC Annual Summit, 30 April – 3 May at the Walt Disney Swan and Dolphin. Expecting record attendance, this year's Summit features nearly 100 sessions that cover everything from information sharing to espionage, and from cyber-insurance to threat automation, and everything in between. The Summits' sessions deliver ground-breaking content making them one of the industry's "must attend" events. For more information, visit the new FS-ISAC Summit website to view the Annual Summit Brochure, session descriptions, hotel and travel information, agendas and more.

Please note: Several nights at the Swan and Dolphin are selling out quickly. If you are unable to book a room, the hotel is keeping a waitlist you can be added to by calling the hotel directly at 407-934-4000. We often see cancelations in the final weeks leading up to the Summit, so you may still be able to get a room at the Summit hotel. We recommend still booking elsewhere in the meantime to ensure you have a room in Orlando. The hotel and travel page includes recommended properties. Please email summit@fsisac.com with any questions.

FS-ISAC Execs Pen Chapter for new American Bar Association Book

Recently, FS-ISAC CEO Bill Nelson and FS-ISAC Sector Services COO Cindy Donaldson authored a chapter for a new American Bar Association book called *Law Firm Cybersecurity*. The chapter focuses on how firms defend against threats through information sharing, why legal services are a target and highlights the changing attack patterns of our adversaries. The entire book is dedicated to law firm security in the digital age; the Legal Services Information Sharing and Analysis Organization (LS-ISAO) is prominently featured, and also lauded in testimonials on the back of the book. You can find more on the American Bar Association website here.

Over the years, FS-ISAC has received a lot of inquiries from members about law firm security from a vendor management perspective. In August 2015, the Sector Services division of FS-ISAC launched the LS-ISAO and it has since grown to 116 law firm member organizations. There has been tremendous interest in the ISAO, both from firms and other industries that want the most effective security for their outside counsels. The LS-ISAO's members are actively engaged in its sharing regime, and participate in cross-sector sharing of threat intelligence with peers at FS-ISAC. We look forward to its continued growth as it helps secure the legal services industry, and boosts the security footprint of partner industries.

Your outside counsels can learn more about protecting their firms, LS-ISAO benefits and membership process by contacting rsantiago@ls-isao.com or visiting fsisac.com/ls-isao.

Call for Presentations Open for Fall and European Summits

At each Summit FS-ISAC turns to its dedicated members to produce the best conferences possible. The stimulating and creative presentations that our members deliver are one of the key reasons our Summits are regarded so highly. Now is your opportunity to submit your proposal to present at the Fall Summit in Baltimore, 1-4 October, and the European Summit in London, 30 October – 1 November! Please submit your ideas for the Fall Summit by 19 April and the European Summit before 12 May.

Member presentation proposals of either a panel, standalone or co-presentation can be submitted. There is no cost to FS-ISAC Financial Institution Members for speaking sessions. Please note: Member submissions that include a sponsor will be considered in sponsor sessions. Panels are limited to four participants and one moderator.

Upcoming Events (cont.)

Member Meeting
Melbourne | 31 May
Register here

Member Meeting
Madrid | 1 June
Register here

Member Meeting
Toronto | 7 June
Register here

Member Meeting
Brussels/La Hulpe, Belgium | 13 June
Register here

Critical Thinking from Conceptualization to Presentation
Reston, VA | 13-15 June
Register here

Stop the heist: Prevent malware from ruining your bank

13 April, 2017 | 12 p.m. ET/9 a.m. PT
Hosted by *American Banker*

Malware is the top security threat to the financial services industry. It can be used to attack point-of-sale terminals, ATMs, bank accounts, web and mobile apps, and internal systems to gain access to money transfer apps. With banks continuing to be the top target for hackers to steal highly monetize-able data, they cannot afford to rely on outdated security technologies and practices to keep them safe.

In this session, Tom Gamull, Citrix Technology Professional and Vishal Ganeriwala, Sr. Director Technical Marketing at Citrix, will explore:

1. The common malware attacks you should be aware of;
2. The guiding principles to fortify your systems; and
3. How to protect your systems with Citrix architecture and solution.

Register here.

Interested in learning more about the Brand Protection Group?

The *Brand Protection Group*, under the Products & Services Committee, invites you to attend their 2017 calls. The calls focus on addressing challenges and opportunities in protecting brands, trademarks, and copyrights in the Web, Mobile, and Social Media spaces.

The goals are to formalize and facilitate an information sharing forum between peer organizations regarding discovery, and trending in the Web, Mobile, and Social Media spaces. Also, the group will share prevention, detection, and mitigation approaches for different types of brand infringements including, but not limited to, activities involving phishing, company and employee impersonations, fraud, and related scams.

If you would like to participate on the calls in 2017, please send an email to admin@fsisac.com.

Update From the ISAC Analysis Team

Apache Struts Vulnerability - CVE-2017-5638

On March 6, 2017, Apache issued an advisory for a vulnerability in Struts 2 that is present in versions 2.3.5 to 2.3.31 and versions 2.5 to 2.510. Since then, multiple members reported malicious traffic believed to be associated with this vulnerability. In March, FS-ISAC released two Intelligence Spotlight Reports (TLP Amber and TLP Green) and convened a call with 1,500 participants to provide members background information on the vulnerability, assessment of the threat and recommended actions that firms can take to better secure impacted applications and engage service providers. The IAT created a Cyber Threat to track all observables.

Industries Targeted: Education (37%), Technology (5%), Finance (4%), Healthcare (28%), State/Local/Federal Government (<1%), Non-Profit (<1%), Manufacturing (2%), Retail (15%), Business Services (6%), Construction/Real Estate (<1%), Food/Beverage (<1%), Gaming/Entertainment (<1%)

MajikPOS - Point of Sale (POS) Malware

MajikPOS, a malware believed to target payment systems predominately in the US and Canada, has been observed since at least January of this year.

This POS malware not only collects information about the infected machine but looks to gather credentials using the tools Mimikatz, FGDump, and VNCPassview to move laterally through the network to infect other hosts. This malware also employs a memory scrapping component that searches the infected system for POS software to extract credit card data directly from memory.

As best practices, properly configured chip-and-pin credit cards with end-to-end encryption (EMVs) should be unaffected by this threat. Unfortunately, terminals that don't support them are at risk to threats like MajikPOS. While the US has adopted EMVs, many merchants still haven't implemented the PIN part of the chip-and-PIN process. To further mitigate MajikPOS, it is recommended to properly secure remote access functionalities like remote desktops and VNC, especially when these expose the host or system to the internet. Whitelisting can also be employed to reduce attack exposure by ensuring only updates associated with whitelisted applications can be installed.