FINANCIAL SERVICES Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter **April 12, 2016**

Newsletter Contents

FS-ISAC Webinars

AFFILIATE WEBINARS

Cast Your Nets to Catch Next Generation Phishers | BrandProtect | April 13
Register here

Report: Research: Vulnerability Review 2016 | Flexera Software (formally Secunia) | available for download until May 9
Download Here

WEBINARS

Cloud Security You Can Bank On: A Western Union Case Study | Skyhigh | April 26
Register here

It's About Time Vulnerability Management Evolves | Digital Defense | available for download until May 25
Download Here

Upcoming Events

Information Sharing Workshop
Amsterdam, Netherlands | April 13
Register here

Information Sharing Workshop
Kuala Lumpur, Malaysia | April 21
Register here

CFSC Meeting
Toronto, Ontario | April 22
Register here

Member Meeting
Singapore, Asia | April 27
Registration will be available soon

Registration Open for All Summits

Registration for all of FS-ISAC's Summit events are now open – Annual Summit registration is hitting record levels! Each Summit features a stellar line-up of the leading experts in data and information security. Join them as they discuss the latest trends, challenges, and solutions in today's threat environment.

- Register for the **Annual Summit** in Miami Beach (May 1-4) here.
- Register for the **APAC Summit** in Singapore (June 20-22) here, Early Bird Registration ends May 20.
- Register for the **Fall Summit** in Nashville, TN (October 23-26) here, Early Bird Registration ends September 23.
- Register for the **European Summit** in Barcelona (November 6-9) here, Early Bird Registration ends September 23.

For more information on all of FS-ISAC's Summits visit www.fsisac-summit.com.

Call for Presentations – Fall and European Summits

Providing world-class content at our Summit events starts with you! Presenting at the Summits builds credibility, generates awareness and shows your commitment to strength in sharing. FS-ISAC will begin accepting member panel, stand-alone or co-presentation proposals for the Fall Summit on April 15 and for the European Summit on April 29!

To learn more about the call for presentations, hot topics and content, tips for selection or to submit your proposal visit www.fsisac-summit.com.

US Government & Financial Sector Releases Sector-Specific Plan

The US Treasury and Homeland Security Departments, in partnership with the Financial Services Sector Coordinating Council (FSSCC), released the Financial Services Sector-Specific Plan (SSP) this month. The plan provides an overview of the sector, the cyber and physical risks it faces, and outlines the following key goals: increased sharing of actionable intelligence, collaboration with security and intelligence agencies, and discussion of policy and regulatory initiatives that advance infrastructure security and resilience.

CISA Implications for ISACs and Financial Institutions

The US Department of Homeland Security (DHS) has begun implementing the Cybersecurity Information Sharing Act (CISA) by opening the Automated Indicator Sharing (AIS) process for business. AIS provides a vehicle for private sector entities to share cyber threat indicators and defensive measures directly with DHS while receiving liability protections covered under CISA. Private sector entities may also receive these protections by sharing directly with another entity or with an ISAC. Any member firm wishing to remain anonymous may do so by sharing through the ISAC. Information shared with DHS cannot be anonymous, however information shared by a member with an ISAC will, if the ISAC shares it with DHS, be seen as coming only from the ISAC, not the member.

Upcoming Events (cont.)

2016 FS-ISAC Annual Summit: "Strength in Sharing: Expanding the Trust"
Miami Beach, FL | May 1 - 4
Register here

Member Meeting
Melbourne, Australia | May 19
Register here

Member Meeting
Dublin, Ireland | June 8
Register here

Fundamentals of Intelligence Training
Reston, VA | June 13 - 16
Register here

Information Sharing Workshop
Toronto, Ontario | June 13
Register here

Information Sharing Workshop
New York, NY | June 15
Register here

2016 FS-ISAC APAC Summit: "Strength in Sharing: Expanding the Trust"
Singapore | June 20-22
Register here

FS-ISAC Members Create New Regional Information Exchange

FS-ISAC is excited to announce our first Asia-Pacific Regional Information Exchange (RIE) in Singapore – to be held Monday, June 20, 2016 before the inaugural APAC Summit. Like the global Advanced Threat Technical Exchange (ATTE), the RIE is a member-only meeting for in-depth information sharing about trends and mitigation strategies affecting a specific region. This meeting is by members, for members, and includes sensitive information best suited for face-to-face meetings. Be sure to check the FS-ISAC Events page for registration information.

OASIS – STIX Training

Going to the Annual Summit this Spring? Stick around for a special STIX Training, hosted by OASIS May 5. Space is limited, register today!

From the FS-ISAC Analysis Team

US Department of Justice Indicts Cyber Actors Accused of Involvement in 2012-2013 DDoS Attacks against Financial Services Firms

On Thursday, March 24 the US Department of Justice (DoJ) released indictments against a number of suspected cyber actors. These individuals are accused of being involved in the 2012-2013 DDoS attacks against Financial Services firms.

While FS-ISAC does not expect there to be any retaliatory actions, we encourage members maintain vigilance, paying particular attention for possible cyber activity targeting the financial services sector. This could include spear phishing campaigns, increased probing, or DDoS activity.

Members are encouraged to report any suspicious activity via member communication methods. Members can also contact the FS-ISAC IAT with specific questions.

The key points for members to keep in mind are:

1. This is not a new attack. This is a legal action relating to attacks from over three years ago.
2. Those attacks did not result in any breaches or loss of customer data within the financial sector.
3. That experience did intensify the cyber threat intelligence sharing and enhanced cyber readiness across the sector.

HID VertX / Edge 'discoveryd' Command Injection Remote Code Execution Vulnerability

Certain models of HID Global brand door controllers contain a software vulnerability allowing malicious actors to remotely control the lock and unlock mechanism. This pertains to HID's VertX and Edge card reader product lines.

HID controllers are prevalent across most sectors making this exploit a likely attack vector for malicious actors attempting to gain physical access to facilities.

HID stated that these controllers are sold through a "closed" channel of development partners, so the documentation, as well as the firmware fix, is available to those partners through their password protected developers site. The partners were notified via newsletter, as well as an email to registered users of the developers site.

The vulnerability was identified in an improperly sanitized input that allows Linux commands to be executed by the HID door controller as the root user. Sending malicious commands to the HID device does not require any specialized tools other than a PC utilizing a Linux Operating System. The actor also needs access to the network in which the HID system resides. If the controllers are on a segmented network, exploiting this vulnerability would be more difficult than on a network facing the Internet.

As this vulnerability potentially facilitates compromises to physical security, it could result in an increased opportunity for the commission of additional crimes. As such, it is recommended to:

- Verify and apply vendor issued patches.
- Segment HID door controllers to make them inaccessible from the Internet.
- Apply networking best practices such as (but not limited to): network segmentation and IP whitelisting.