FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | October 2017

TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

MarkMonitor Webinar: From Phishing to the Dark Web |10 October | Online

FS-ISAC Expert Webinar Series: SWIFT's Customer Security Program – Creating a Security Baseline for Financial Services* 17 October

FS-ISAC Expert Webinar Series: Patch Management Tips and Techniques for Reducing the Pain* | 24 October

Haystax Webinar: Defending Against the Wrong Enemy | Download until 31 October

Black Duck Webinar: Audits of 1000 Apps | Download until 31 October

Flashpoint Webinar: Flash Talk: EMV Circumvention | Download until 15 November

Flashpoint Webinar: Flash Talk: Russian Ban on Anonymizing Services | Download until 15 November

Citrix Webinar: Swift CSP: What You Need to Know Now | Download until 15 November

DMARC Webinar Sessions
18 October or 8 November | Online

BlackBerry Security Summit
24-25 October | London
14-15 November | New York City

2017 FS-ISAC EMEA Summit
30 October-1 November | London

FS-ISAC Gulf Regional Intel Exchange
6 November | Abu Dhabi

EMEA Summit Introduces Session Tracks

The 2017 EMEA Summit, 30 October-1 November in London is just around the corner. To help you navigate the more than 40 quality sessions, we are introducing session tracks. This year's sessions have been grouped into four tracks so you find topics and content of interest. Session tracks include:

Governance and Resiliency: Learn about and discuss upcoming legislation and regulatory mandates on the sector, including General Data Protection Regulation (GDPR), revised Payment Services Directive (PSD2) and mandatory reporting requirements. Topics related to external regulation, internal risk management and hearing a CISO case study. Meet the new EMEA Business Resiliency Council (BRC) at the Summit and hear about FS-ISAC's efforts in exercising with regional organizations.

Technology and Operations: Hear about the latest trends in using technology to deal with internal risks and external threats. Learn from FS-ISAC staff and members on how to deal with the tsunami of information overloading your teams and integrating operations with intelligence.

Testing and Security Assurance: Explore topics on testing internal applications in accordance with software development life cycle (SDLC) and open web application security project (OWASP), penetration testing and discussing the regional trend of mandatory penetration testing from the regulator like CBEST (Bank of England Cybersecurity Framework) and TIBER (Threat Intelligence Based Ethical Red Teaming). Contribute to ongoing member discussions on dealing with increased regulatory scrutiny on cybersecurity operations.

Threat Intelligence: Review the latest information on current and emerging threats hitting the financial sector. Meet the EMEA Threat Intelligence Committee (ETIC) members and hear from FS-ISAC's Global Intelligence Office (GIO) on how FS-ISAC's intelligence offering is evolving.

Learn more about *session tracks* and the EMEA Summit.

Post-Breach Tip Sheets

Data breaches that expose sensitive personally identifiable information (PII) are challenging for financial institutions who must cover fraud losses as well as consumers who must spend hours cleaning up fraudulent accounts taken out in their name. FS-ISAC along with our members have created two, TLP White tip sheets for financial institutions and their customers or members to use in the wake of data breaches. The FS-ISAC Tips for Consumers – What to do Post-Breach offers actions that the average consumer may take to protect themselves from ID Theft. The FS-ISAC Tips for Financial Institutions – What to do Post-Breach offers actions that banks and credit unions can take to protect their institution from fraud losses.

FS-ISAC CIRO Greg Temm Contributes to Computerweekly's Security Think Tank

Over the past several months, FS-ISAC's Chief Information Risk Officer (CIRO) Greg Temm has been contributing a blog to *Computerweekly's Security Think Tank*. A series featuring a variety of experts offering insights on a range of topics primarily focusing on "hackers and cybercrime prevention." These contributed blogs have covered tactics for businesses to protect from cyber-attacks, security controls to ensure a safer working environment and steps to improve cyber-resilience. Read his posts.

Responding to Hurricanes Harvey, Irma, Maria and Nate

FS-ISAC CEO Bill Nelson Pens Blog About Financial Sector's Response to Major Storms

In response to the recent, devastating hurricanes, FS-ISAC CEO Bill Nelson published a blog on LinkedIn which reiterated FS-ISAC's mission to support the resilience of the financial sector against all threats. He highlighted several ways FS-ISAC is working with government agencies and the financial industry in recovery efforts including:

- Partnering with payment technology companies to provide locations of working ATMs, stores and merchants
- Sharing cross-sector information to help financial sector employees get their firms back up and running.
- Maintaining the sectors' *All-Hazards Crisis Response Playbook* and provided the *Storm Preparedness Checklist*.
- Providing members with information about crisis-related scams to relay to their customers.

Read the full post.

Mobilizing to Share Information and Assist Members

The FS-ISAC Crisis Response Team (CRT) formed on 26 August in response to Hurricane Harvey has remained mobilized for Irma and Maria. The CRT served as a coordinator for cross-sector communications with electrical power companies and communications companies to address supply chain related concerns given the breadth and impact of these major hurricanes. As the financial sector representative, the CRT also updated the Department of Homeland Security National Incident Coordination Center (NICC), US Department of the Treasury and Federal Emergency Management Agency (FEMA) and convened the Business Resiliency Committee (BRC) daily.

Working in tandem with US government partners, the Federal Reserve System, state agencies, regional coalitions and member firms in the seven states impacted, the CRT organized, aggregated and disseminated information to the FS-ISAC members and sector through daily *Disaster Executive Briefs* (DEBs). FS-ISAC has also been using social media to share critical information on Hurricanes from handles like @FEMA and has issued public statements.

Products and Services Discounts

Did you know that as a member of FS-ISAC you can take advantage of special offers and discounts on product and services from our Affiliates and Strategic Partners? **Visit the member discount page** to see current offers. Make sure to bookmark and check back often as offers are updated and added frequently!

ISAC Analysis Team Updates

Google Chrome Extension Bypass

Google Chrome extensions have become tools for banking malware, according to open source reporting and analysis. A recent victim was contacted by phone and asked to install a seemly new bank security module that, instead, was a malicious extension hosted at the Google Chrome app store to steal victim's banking credentials. Another instance involved a targeted email phishing campaign using another Google Chrome extension prepared to steal banking credentials, credit card, CVV numbers and fraudulent "compensation tickets" to divert payments in Brazil. To increase the success rate of the phishing campaign, a previously hijacked company email account was used to send a fake layoff list to employees along with a "zip" file that contained the first part of the malware.

CVE-2017-8759 Exploiting Targets in Argentina

On September 12, Microsoft released its September 2017 Security Update that patched a zero-day exploit leveraging CVE-2017-8759. A few days later, according to open source reporting, an email spoofing an Argentinian government agency was exploiting the CVE to distribute BetaBot malware. Infection traffic included HTTP requests for SOAP code injection, JavaScript, PowerShell script and a Windows executable over TCP port 8007. Post-infection activity consisted of HTTP POST requests over TCP port 80.

Call for Presentations Open for 2018 Annual Summit

FS-ISAC hosts the only industry forum for collaboration on critical security threats facing the financial services sector. Our Summits are known for the high-quality, relevant and actionable content presented – and that cannot happen without you! The call for presentations for the 2018 Annual Summit taking place 20-23 May in Boca Raton, FL is now open.

Submit your proposal for a standalone, panel or co-presentation that provides actionable, relevant and useful information to attendees. Increase your visibility, share your knowledge and showcase your expertise - view details and submit your proposal today!

The 2018 Annual Summit is 20-23 May in Boca Raton, Fl.) Stay up-to-date, visit the Summit site.