FINANCIAL SERVICES Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | September 2017

TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

FS-ISAC Expert Webinar Series: Imbalancing Act - Addressing the Information to Action Challenge* | 12 September | Online

NA Cyber-Attack Against Payment Systems (CAPS) North America
12-13 September or 19-20 September

Demystifying .BANK: Implementing Security Requirements and Educating Customers [fTLD Webinar] | 18 September | Online

FS-ISAC Dublin Reception
19 September | Dublin

DMARC Webinar Sessions
20 September | Online
18 October | Online

FS-ISAC Expert Webinar Series: Attack and Recovery* | 26 September | Online

Affiliate Webinar: BeyondTrust - Unix/Linux Privilege Management: What a Financial Services CISO Cares About
27 September | Online

2017 FS-ISAC Fall Summit
1-4 October | Baltimore

APAC Cyber-Attack Against Payment Systems (CAPS) Online
10-11 October or 17-18 October

EMEA Cyber-Attack Against Payments Systems (CAPS) Online
10-11 October or 17-18 October

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

Plan Your Content Experience in Baltimore

The Fall Summit online brochure provides you with the sessions, agenda, keynote and other details related to Summit attendance. Take a few minutes to view the brochure and then use our 'session track' designations to identify sessions related to the topics you want most and plan out your content agenda. Session for the Fall Summit have been broken down into the following tracks:

- **Governance:** Learn about and discuss topics on governance-related areas, including regulatory compliance, public and private collaboration, human factors, internal risk management and prevention and mitigation.
- **Resiliency:** Informative sessions discussing the latest on industry exercises and developments such as information gathered from exercises (CAPS, Hamilton Series), Sheltered Harbor and FSARC, as well as sessions for sharing incident response and crisis communication techniques.
- **Technology and Operations:** Information sharing sessions designed to help address internal technology and operational functions. Topics are holistic and cover many areas across operations such as identity management, insider threats, security information and event management (SIEM) tools, payments, perimeter and proxies.
- **Testing and Security Assurance:** Dedicated session on all things testing, from testing internal applications in accordance with software development life cycle (SDLC) and open web application security project (OWASP) to penetration testing and cyber-ranges.
- **Threat Intelligence:** Sessions dedicated to sharing the latest information on current and emerging threats hitting the finance sector. Topics focus on the latest threats, threat automation, threat analysis and how financial organizations are addressing them.

View details on tracks and sessions.

continued page 2

Special FS-SIAC Communities Report Session at Fall Summit

Join the **FS-ISAC Communities Report,** a special session at the 2017 FS-ISAC Fall Summit in Baltimore taking place on Monday 2 October from 10-10:45 a.m. This session will include updates from FS-ISAC working group and committee members on what these communities are currently working on and how you can get involved.

Did you know FS-ISAC recently updated our Twitter handle?
Make sure to follow us **@FSISAC**

Amazing Keynote and More Than 40 Sessions at the EMEA Summit

The 2017 FS-SIAC EMEA Summit (30 October-1 November, London) keynote, *The Future of Cybersecurity – a Hacker's Perspective*, will be delivered by internationally recognized researcher, author and speaker Keren Elazari! Join Elazari on Monday 30 October as she discusses all matters related to cybersecurity and hacker culture.

You don't want to miss this keynote or the great content we have lined up, such as these high-quality, financial sector-relevant sessions:

Cybersecurity and the 323-Year-Old Bank: Using Threat Intelligence to Tell Your Story and Inspire Your People

Cybersecurity is a people challenge every bit as much as is it a technical challenge. Unlike technology, people need motivating, educating and inspiring and when you get this right, your people become your first line of defence. This presentation will show how threat intelligence was used to tell the story of why cybersecurity matters in a 323-year-old organization and how threat intelligence drives risk, policy, education and investment as well as threat detection.

Positive Regulatory Engagement Over Regulation: The Changing Nature of the Relationship

Cyber-resilience is a sector top priority and regulators want to be part of the solution not the problem. Rather than dictating compliance regulators are looking to collaborating on security. This session explores how coordination of cybergroups are proving to be a vehicle for open and productive collaboration. Learn about how CBEST (Bank of England Cybersecurity Framework) helped modify the intrusive nature of the testing and has changed the relationship that firms' cybersecurity teams have with their regulators, reinforcing the desire for a collaborative over a compliance based approach to securing the sector.

View the full brochure. Learn more and register today.

Fall Summit, continued

Plan to join us for one of the three trainings debuting at the Fall Summit. *Sunday trainings require an additional fee and registration that are separate from your Summit registration.*

Sunday (1 October) | 11 a.m.-4 p.m.

- Oasis - STIX 2.0 Workshop
- Treadstone 71 – Intelligence for C-Suite and Stakeholders

Monday (2 October) | 8-11 a.m.

NCSA - The NIST Cyber Security Framework - Small and Medium Business Cybersecurity Workshop

This Fall Summit is going to be amazing. Registration is still open and there is still time to book your hotel and travel (the Baltimore Waterfront Marriott is amazing). To stay up-to-date on the latest Summit details, visit the Fall Summit site.

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

New Locky Ransomware Variants: Diablo and Lukitus

Vendor reporting of these new variants began on 17 August when cybersecurity vendor Comodo described a new worldwide ransomware campaign. Comodo first detected a campaign on 9 August identifying at least 62,000 related phishing emails that lead to the new Diablo variant of Locky. The Lukitus variant was detected last week, targeting Austria, the US and Great Britain according to Fortinet. Locky had fallen off the radar for a bit, but the resurgence with two new variants suggests to researchers a growing sophistication, organization, and size of ransomware attacks A particular concern with these new variants is that the emails which deliver them can be designated as containing an "unknown" file type and may make it past endpoint solutions that detect previous versions of Locky. It is recommended by Comodo to adopt a "default deny" policy which entails blocking all unknown files from an IT infrastructure until they're verified as safe.

HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides technical details on the tools and infrastructure used by cyber actors of the North Korean government to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally. Working with US government partners, DHS and FBI identified internet protocol (IP) addresses associated with a malware variant, known as DeltaCharlie, used to manage North Korea's distributed denial-of-service (DDoS) botnet infrastructure. This alert contains indicators of compromise (IOCs), malware descriptions, network signatures and host-based rules to help network defenders detect activity conducted by the North Korean government. The US government refers to the malicious cyber-activity by the North Korean government as HIDDEN COBRA. More information related to HIDDEN COBRA activity. https://www.us-cert.gov/hiddencobra

Save the Date

The 2018 Annual Summit (20-23 May, Boca Raton, Fl.) will open the Call for Presentations on 20 September! Stay up-to-date, visit the Summit site.

Follow us on Twitter @FSISAC or **join the discussion on LinkedIn**.