FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | May 2018

TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

Virtru Webinar: Reassessing Email Protection for the Cloud Era | 8 May | Online

Symantec & Royal Bank of Canada Webinar: Solving Mobile Security - Peer-Tested Strategies That Work | 22 May | Online

Member Meetings*
30 May | Brussels
6 June | Melbourne
13 June | Stockholm
14 June | London
26 June | Toronto
13 November | Frankfurt

FS-ISAC Chapter Meetings*
3 July | Dublin
6 November | Edinburgh

Threat Intelligence - an Active Cyberdefense Posture Training
17-21 September | Reston, VA

2018 FS-ISAC Annual Summit
20-23 May | Boca Raton, FL

2018 FS-ISAC AP Summit
18-19 July | Singapore

2018 FS-ISAC EMEA Summit
1-3 October | Amsterdam

2018 FS-ISAC Fall Summit
11-14 November | Chicago

FS-ISAC and SPARK Institute Form the Retirement Industry Council (RIC)

FS-ISAC, in partnership with the SPARK Institute, launched the Retirement Industry Council (RIC) to expand voluntary information sharing and threat intelligence to members within the retirement industry like 401(k) firms; mutual and pension funds; and others in the $25 trillion retirement investment community. The RIC will share information about solving security challenges and will focus on the combination of physical and cybersecurity threats faced by the retirement industry. To participate, you need to be a member of FS-ISAC or the SPARK Institute's Data Security Oversight Board (DSOB). More.

FS-ISAC and Sheltered Harbor Will Receive 2018 CIO 100 Awards

IDG's CIO today announced that FS-ISAC and Sheltered Harbor are each individual recipients of the 2018 CIO 100 Awards. The 31st annual award program recognizes organizations around the world that exemplify the highest level of operational and strategic excellence in information technology. FS-ISAC's crucial innovation is to have created the our first-ever centralized platform for cyberprofessionals to aid in combatting ever-increasing cyberthreats. Sheltered Harbor, a subsidiary of FS-ISAC, is recognized for creating a safety net for consumers in a worst-case security scenario. Sheltered Harbor's mission is to safeguard consumers and the financial sector from cyber and physical attacks. FS-ISAC and Sheltered Harbor will be recognized at The CIO 100 Symposium & Awards Ceremony. More.

CIO 100 HONOREE 2018

FS-ISAC AP Summit Registration Open

FS-ISAC Summits are focused around peer-to-peer networking and building relationships or *circles of trust* with financial services organizations. Registration for the FS-ISAC AP Summit (18-19 July, Singapore) is now open. Learn more and register today.

ISAC Analysis Team Update

Nation-States Threat Landscape

Nation-states may be exploiting a vulnerability identified by Cisco to target critical national infrastructure. For example, Russian cyber-actors leveraged a number of legacy or weak protocols and service ports associated with network administration activities. This month, Cisco published a Talos blog stating that it was aware of specific advanced actors targeting their switches by leveraging a protocol misuse

continued, page 2

ISAC Analysis Team Update, continued

issue in the Smart Install Client. Using Shodan, Cisco found that 168,000 systems were potentially exposed via the Cisco Smart Install Client. The blog found that Cisco observed related scanning activity for the Smart Install client since February 2017, a time frame consistent with information provided in an April 2018 Technical Alert (TA) detailing ongoing malicious cyber-activity carried out by the Russian government.

The FBI and the UK's National Cyber Security Centre (NCSC) have high confidence that Russian state-sponsored cyber-actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks and potentially lay a foundation for future offensive operations. Targets of this malicious activity are primarily government and private sector organizations, critical infrastructure owners and operators, and the Internet Service Providers (ISPs) supporting these sectors.

Based on information available, it is not clear if the financial services sector is a direct target of these ongoing campaigns. Threats to other critical sectors and those targeting the digital supply chain remain a concern for members as they assess risk to third-party suppliers and the infrastructure they depend on.

Critical Drupal Patches

On 25 April 2018 there was a security release for **Drupal 7.x, 8.4.x, and 8.5.x**. This security release is outside of the regular schedule of security releases. For all security updates, the Drupal Security Team urges customers to reserve time for core updates at that time because there is some risk that exploits might be developed within hours or days. This security release is a follow-up to the one released as SA-CORE-2018-002 on 28 March. If your site is on a Drupal 8 release older than 8.4.x, it no longer receives security coverage and will not receive a security update. Upgrading is strongly recommended as older Drupal versions contain other disclosed security vulnerabilities. The CVE for this issue is CVE-2018-7602. The Drupal-specific identifier for the issue will be SA-CORE-2018-004.

Operation GhostSecret

According to ThaiCERT law enforcement officials in Thailand worked with McAfee to investigate and seize servers belonging to "Operation GhostSecret". The joint actions have revealed that the operation is linked to the Hidden Cobra group, which has possible ties to North Korea. This group is also known Lazarus Group, Reaper or Group 123. McAfee made the links between Operation GhostSecret and Hidden Cobra via the usage of Trojan Manuscript (Bankshot), Destover malware, and a reused SSL certificate. The initial investigation pointed to Operation GhostSecret targets that belonged to the Financial Sector. However, evidence also exists for targets in the critical infrastructure and healthcare sectors across seventeen countries.

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!

FS-ISAC 2018 CAPS Exercises

The 2018 FS-ISAC Cyber-Attack Against Payment Systems (CAPS) exercises are gearing up. These regional, two-day, tabletop simulation exercises for payment professionals present a robust, real-world cyber-attack scenario to challenge incident response teams and test incident response preparedness. See below for the 2018 North America, Europe, Middle East and Africa (EMEA) and Asia-Pacific (AP) exercise dates.

- **AP Sessions |** 11-12 September or 18-19 September
- **EMEA Sessions |** 11-12 September or 18-19 September
- **North America Sessions |** 9-10 October or 16-17 October

Learn more and view the FAQs.

Last Chance to Submit Your Proposal for the FS-ISAC EMEA Summit

The FS-ISAC 2018 EMEA Summit (1-3 October, Amsterdam) is one of the most respected and fasted growing financial services security events in the EMEA region. Developed by practitioners and solution providers the relevancy of the content is actionable and topical. Join this distinguished line-up of subject matter experts teaching and sharing on cybersecurity topics that keep security professionals up at night. We are currently accepting proposals until 11 May for presentations that focus on:

- Cloud-based solutions and security
- Big data and analytics to reduce risk
- Artificial intelligence as a defense
- Cybercrime and disruption approaches
- Workflow automation and orchestration
- Threat hunting tactics
- Data privacy and protection
- Digital objects and identities
- Governance and reporting
- Legal and regulatory issues

If you have content driven session idea that provides actionable, relevant and useful information to attendees we encourage you to increase your visibility, share your knowledge and showcase your expertise - **submit your proposal today**!