FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | December 2017 — TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

FS-ISAC Solutions Showcase*
13 December

DMARC Webinar Session
20 December

DomainTools Webinar: Best Practices for Building a Security Technology Strategy
Available for download until 31 December

Akamai Webinar: State of the Internet/ Security Report – Q2 2017 Findings
Available for download until 31 December

Bochum, Germany Member Meeting*
30 January

London Member Meeting*
1 March

Zurich Member Meeting*
7 March

London Insurance Member Meeting*
12 April

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

London Member Meeting*
14 June

2018 FS-ISAC AP Summit
17-18 July | Singapore

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

FS-ISAC Launches First Virtual Solutions Showcase

Based on the popular Silver Solutions Showcase at FS-ISAC Summits, FS-ISAC is launching a member-only, virtual Solutions Showcase initiative to help members research security tools and provide demonstrations in a low-pressure sales environment throughout the year. This one-stop, virtual day connects members with trusted affiliate partner providers to find the right solutions for various security needs.

The inaugural virtual Solutions Showcase provides live discussions from multiple solution providers on various topics followed by facilitated Q&A. Future sessions will be targeted to specific, emerging security challenges and audiences. Sessions will be recorded and available on the member Portal for 12-months of on-demand viewing.

The first Solutions Showcase will take place on 13 December 2017. The day will kick off at 10 a.m. EST with a demonstration from BrandProtect; 11:15 a.m. with Perch Security; 12:30 p.m. with AlienVault; 1:45 p.m. with NSS Labs; and 3 p.m. with Blackberry. A detailed list of presentations can be found here. Members register here.

FS-ISAC and JHU APL Partner to Advance Cybersecurity Automation in Financial Sector

FS-ISAC and Johns Hopkins University Applied Physics Laboratory (JHU APL) recently announced an effort to operationalize the Integrated Adaptive Cyber Defense (IACD) framework. The IACD framework guides implementation of commercially available automation technology to improve cybersecurity orchestration and information sharing. Tests of the IACD have shown a reduction in investigation and response time from 11 hours to 10 minutes. The IACD also enables an operations team handling 65 events per day to automatically process up to 95 events at the same time. Through this partnership, FS-ISAC will support greater adoption of the framework within the financial sector and JHU APL will provide technical assistance to FS-ISAC and member organizations that adopt the IACD. The US Department of Homeland Security is providing funding to JHU APL for this initiative. Read the full release.

New Asia-Pacific Regional Analysis Centre Allows for 24/7 Threat Intelligence Sharing

FS-ISAC's first full-time office outside of the US officially opened on 14 November. The Regional Analysis Centre in Singapore supports 24/7 local and global coverage with threat information sharing, actionable intelligence and steps to help mitigate the fallout from an incident. Additionally, the Analysis Centre increases FS-ISAC's ability to understand threats in Asia-Pacific and the potential global impacts. In October, the Centre released recommendations and reports about account takeover attacks leveraging SWIFT on the Taiwanese Far Eastern International Bank (FEIB), alerting members to the attack within a day of its discovery. Read the full release.

ISAC Analysis Team Update

Paradise Papers

"Paradise Papers" are a global investigation from the International Consortium of Investigative (ICIJ) Journalists and 95 media partners. The initial leak was provided to the ICIJ by a German newspaper, Süddeutsche Zeitung, however, the identity of the original source is unknown. The reported 13.4 million leaked files are from a combination of offshore service providers (including Appleby and Asiaciti) and company registries. The leaked data contained nearly seven million loan agreements, financial statements, emails, trust deeds and other paperwork. Records in the leak range from complex, 100-page corporate transaction sheets and dollar-by-dollar payment ledgers to simple corporate registries of countries.

Key findings of the investigation include:

- Reveals offshore interests and activities of more than 120 politicians
- Exposes the tax engineering of more than 100 multinational corporations
- Details of how owners of luxury items use tax avoidance structures

For more information please visit the ICIJ investigation page.

November Microsoft/Adobe updates

On November 14, 2017, Microsoft released their monthly updates/patches, including 53 vulnerabilities, 19 of which are critical. The November security release consists of security updates for the following software: Internet Explorer, Microsoft Edge, Microsoft Windows, Microsoft Office and Microsoft Office Services and Web Apps, ASP.NET Core and .NET Core, & Chakra Core. Notable are four vulnerabilities with public exploits identified by Microsoft as CVE-2017-11848, CVE-2017-11827, CVE-2017-11883 and CVE-2017-8700.

Adobe released nine security bulletins in November covering the following: Adobe Experience Manager, Adobe Shockwave Player, Adobe Digital Editions, Adobe InDesign, Adobe DNG Converter, Adobe Acrobat and Reader, Adobe Connect, Adobe Photoshop CC and Adobe Flash Player. According to Adobe, "None of the vulnerabilities patched today (November 14, 2017) are under active attack". The Acrobat and Reader update included patches for 56 vulnerabilities, most of which are critical remote code execution vulnerabilities. Acrobat and Reader DC 2017.012.20098 and earlier are affected as are Acrobat and Reader 2017 2017.011.30066 and earlier, Acrobat and Reader DC 2015.006.30355 and earlier and Acrobat and Reader XI 11.0.22 and earlier.

UK Banks Weather DDoS Attacks

Unknown threat actors have turned again to distributed denial of service (DDoS) attacks to cause disruption to business networks. Members in the United Kingdom (UK) report recurring DDoS attacks in the months of October and November. While these attacks have had relatively low impact to business operations and website availability, it has caused an increased operational tempo by security teams needing to adapt to the changing attacks. Other European members also report sporadic attacks; however, it is not currently known if any of these attacks are related to the persistent campaign in the UK. This is not believed to be linked to the DDoS extortion gang --the Armada Collective-- demonstrating attacks against finance-related firms in Europe as none of the other attacks were associated with a ransom demand. FS-ISAC is coordinating cross-border public-private partnerships to determine if there are any links.

Security researchers at Corero Network Security revealed new data suggesting that, as a whole, businesses are seeing a significant increase in DDoS attacks in the third quarter of 2017, estimating that businesses see eight attempted DDoS attacks daily. Members should consult their DDoS mitigation providers and work with their internal response teams to ensure that they are implementing best practices. FS-ISAC does have DDoS mitigation documentation available on the portal. Some members have also reported DDoS extortion attacks but FS-ISAC largely considers these to be low threat and lacking credibility, as threat actors seldom follow through with their posed threats.

Cobalt Gang synchronized ATM heists across Europe, Russia and Malaysia

The Cobalt Gang conducted a massive simultaneous ATM heist within a few hours. Spear-phishing emails were sent to bank employees, impersonating the European Central bank, the ATM maker Wincor Nixdork, among other institutions. These emails delivered attachments containing an exploit for the MS Office vulnerability CVE-2015-1641, which is a remote memory-corruption vulnerability. An attacker can leverage this issue to execute arbitrary code in the context of the currently logged-in user. Failed exploit attempts will likely result in denial-of-service conditions.

If the exploit was successful, a malicious payload was injected. Additional methods and exploits were used to assure persistence and gain additional privileges. Ultimately, attackers gained control over several computers inside bank networks. Once compromised, the attackers used legitimate channels to remotely access the bank. Finally, the attackers found workstations that controlled ATMs and would load the ATMs with software to allow them to control cash dispensers. The final strikes took place within a few hours, in which money mules would collect the physical cash from the compromised ATMs.

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!