FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | October 2018

TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

FS-ISAC Cyber-Attack Against Payment Systems (CAPS) Exercise - North America
16-17 October

CUNA, FS-ISAC and FSSCC Webinar: Easy and Effective Cyber-Exercises for Credit Unions | 17 October

LookingGlass Webinar: Through the LookingGlass - Top Trends to Keep Your Organization Cyber-Aware | 24 October

Cyber-Range Ransomware Exercise*
24 October | Kansas City, MO

Crowdstrike Webinar: Going Far Beyond Antivirus - Capabilities for Effective Endpoint Protection | 26 October

Cyber-Intelligence Analyst Course (Level One) | 29 October-2 November | Singapore

FS-ISAC Expert Webinar Series*
- The Rise of State-Sponsored Attacks on the Financial Services Industry | 23 October
- The Future of Digital Payments | 27 November
- Using the Power of Threat Intelligence to Disable Banking Trojans | 11 December

FS-ISAC Solutions Showcase - From Detection to Disclosure* | 30 October

Infoblox Webinar: Five Security Experts Say "Hack, No!" to DNS Threats | 31 October

FS-ISAC Member and Chapter Meetings*
31 October | Kuala Lumpur, Malaysia
6 November | Edinburgh (Chapter Meeting)
13 November | Frankfurt
14 November | Israel

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

FS-ISAC 2019 Annual Summit
28 April-1 May | Orlando

FS-ISAC Expands Exercises in EMEA

During the recent EMEA Summit in Amsterdam, FS-ISAC announced the expansion of the exercises into the EMEA region. The exercises organized by FS-ISAC and hosted by the largest Dutch bank ING, mimicked an online attack on a real-world bank network environment. From a range of prominent financial institutions, including the Dutch Payments Association and the Association of Financial Markets in Europe (AFME), the exercise tested how network defenders organized and communicated among themselves to varying degrees of success. The cyber-assault mirrored the infamous WannaCry ransomware attack of 2017 that is estimated to have affected more than 200,000 computers across 150 countries and caused damage estimated in the billions of dollars.

continued, page 2

A Rocking Cybersecurity Keynote, Return of the Titans and Sessions Galore All at the Fall Summit

FS-ISAC is excited to announce that Jeffrey Baxter, National Security Expert and founding member of Steely Dan will keynote the 2018 FS-ISAC Fall Summit taking place 11-14 November in Chicago. The keynote takes place on Monday 12 November.

Then, back by popular demand, you won't want to miss this year's *Tempt the Titans*! Make sure you plan to attend this member favorite. Attendees will 'vote' for their favorite early stage firm and then the top three companies will pitch to the Titans on Wednesday 14 November.

You will want to start planning your agenda today from our more than 120 sessions and eight tracks. Learn more and register today!

FS-ISAC Solutions Showcase - From Detection to Disclosure

FS-ISAC Solutions Showcases are an all-day, virtual, members-only event designed to help you evaluate security product demonstrations presented by technical experts in a secure low-pressure environment. Join us on 30 October for our next ***Solutions Showcase – From Detection to Disclosure*** featuring five solution providers that mitigate kill-chain progression at each level.

Join our cybersecurity vendors as they demo what helps the financial sector to detect network traffic, validate tools, identify threats and all the way to disclosing the vulnerability. Presentations start at the top of the hour. View the agenda, learn more and register today. Did you miss a showcase or want to view a session again? View past showcases again on-demand!

ISAC Analysis Team Updates

Account Takeover Attacks Heating Up

Account takeover attacks (ATO) have been a concern for many years. In recent months, the FS-ISAC has observed an uptick in references and concern with ATO attacks on the cyber-intel list. In addition, several reports by external researchers have come out indicating that credential stuffing is on the rise. These attacks are often utilized by botnets. According to recent Agari research there has been a 126% increase of targeted email attacks that exploit ATO. Research found that 44% of organizations were victims of targeted email attacks launched via a compromised account in the past 12 months. FS-ISAC members need to evaluate whether their existing email security controls can analyze, detect and block ATO-based email attacks.

Increase in Ramnit and Ngioweb Malwares

FS-ISAC trusted partners have reported that several members have been affected recently by Ramnit malware. Ramnit consists of bot building worms and trojans capable of stealing credentials and delivering additional malware. Efforts to mitigate these botnets in the past have been unsuccessful, with new campaigns surfacing shortly after the previous threats were shut down. Recently, cybersecurity researchers have been observing a Ramnit botnet variant known as the "Black" botnet dropping Ngioweb malware on to victim machines. Between May and July of 2018, Checkpoint observed more than 100,000 new 'Black' botnet infections. Ramnit spreads through malicious emails and links sent through eCommerce and social media sites and then communicates via port 447. Ramnit also acts as a delivery mechanism for Ngioweb malware which represents a multifunctional proxy server that uses its own binary protocol with 2 layers of encryption. The proxy malware supports back-connect mode, relay mode, IPv4, IPv6 protocols, TCP and UDP transports with first samples seen in the second half of 2017. The name for the malware has been chosen as a domain name hardcoded in the malware configuration "ngioweb[.]su".

Virobot Malware

The FS-ISAC researched new malware this week called Virobot. This specific type of Ransomware happens to be a botnet and a keylogger all in one, with a French connection that seems to come from PyLocky ransomware. So far, Virobot has been primarily focusing on victims in the US. It is spread by spam emails and is unique in the sense that it doesn't belong to any previous Ransomware family. After Virobot infects a machine, it becomes part of a spam botnet that pushes the ransomware to more victims. While writing on this topic, no observables were matched against our FS-ISAC repository, but members should still be on the lookout for indicators of compromise.

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 discounts page** to see current offers. Make sure to bookmark and check back often as offers are updated and added frequently!

Scholarships for EMEA Summit

The financial industry is on the front lines of addressing new and emerging cybersecurity threats that have a global impact. FS-ISAC and its members have long recognized that to meet these growing and changing cybersecurity threats, we need to build a diverse workforce. To confront this gap at an industry level, FS-ISAC launched the Building Cybersecurity Diversity (BCD) Scholarship program in 2016 to introduce women interested in careers in cybersecurity to the financial community. Through the generosity of our members and solution providers, the BCD Scholarship provides financial support and introduces top students to opportunities in the financial industry. To learn more or for questions visit us online or email. Please note the application process for 2018 is closed.

EMEA Exercises, continued

FS-ISAC Exercises enable members to develop best practices for their respective institutions and help with crisis response coordination within the sector, cross-sector, with law enforcement and other governing bodies. FS-ISAC is building a range of customized exercises for the financial services sector including:

- **Cyber-Attack Against Payment Systems (CAPS) -** This annual virtual exercise is aimed at payment companies, free to all regulated financial institutions in EMEA, Asia-Pacific and the Americas. Participating members benefit from testing their organization's readiness in case of an attack and free benchmarking against peers.
- **Cyber-Attack Against Insurance System (CAIS) -** This virtual exercise simulates an attack on insurance companies to help gauge their readiness in the event of an incident. The exercise is available to all insurers via remote participation.
- **Cyber-Range Exercises -** Members participate in a technical, hands-on-keyboard experience that provides greater interaction and sharing, helping to increase capability maturity levels and resiliency across the financial services sector.

View the full release and visit us to learn more about FS-ISAC Exercises.