FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | August 2018

TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

FS-ISAC Solutions Showcase: From Identification to Detection* |15 August

FS-ISAC Expert Webinar Series*
- **Best Practices in Defense of DDoS Attacks Targeting FIs |** 11 September
- **Account Takeover - An Identity Deception Threat |** 25 September
- **Best Practices for Building an Insider Threat Program |** 9 October

FS-ISAC Threat Intel Roadshow*
11 September | Boston
13 September | Atlanta
18 September | Phoenix
20 September | Dallas

FS-ISAC Member Meetings*
29 August | Hanoi, Vietnam
26 September | Dubai
13 November | Frankfurt

FS-ISAC Chapter Meetings*
6 November | Edinburgh

Cyber-Range Ransomware Exercise
29 August | St. Louis
17 September | Chicago
10 October | San Francisco
24 October | Kansas City, MO

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

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

FS-ISAC Roadshows Bring Threat Intel Content and Experts to You

The FS-ISAC Threat Intel Roadshow is delivering an interactive and engaging forum focused on the threats that member companies stare down daily. The highly curated sessions feature intel trend experts, executive leaders, front line analysts that know this business of stopping bad actors. Topics include insourcing versus outsourcing threat intel; how to use threat intel findings; nation-state capabilities and destructive attacks; threat intel management and operations; and emerging trends and TTPs. Plan to join your local FS-ISAC members in Atlanta, Boston, Dallas and Phoenix in September for this free member day of closed-door, collaborative deep-dives into the threats keeping you awake at night. Learn more and register today.

Insider Threat Framework Whitepaper

The Insider Threat Working Group (North America branch) published a whitepaper in June on *the Insider Threat Framework*. Using the NIST Framework Core five concurrent and continuous function of Identify, Protect, Detect, Respond and Recover, the whitepaper outlines the main functions related to an insider threat program. This whitepaper and provided matrix are TLP GREEN and available to FS-ISAC members on the Portal.

Extortion Phishing Email Campaigns on the Rise

FS-ISAC has seen an up-tick in extortion phishing emails being shared. One commonly used campaign involves being threat actors sending an email stating that they know the recipient's password, have installed malware on the computer, created videos of the recipient using adult websites through their webcam and have stolen the recipient's contacts. Unfortunately, the threat actors may know a recipient's password from data breaches but no one has caught a recipient doing anything and members should know that this is just a scam.

Threat actors are finding leaked account credentials from data breaches and are using those leaked passwords when contacting victims. FS-ISAC members have reported passwords they are observing from these extortion emails may be from old LinkedIn accounts. If the passwords sent in the email is one that you are currently using, change it immediately. In addition to changing your passwords it is also important to verify the accuracy of the claim and determine if it is a hoax. To verify the accuracy of the claim:

- Confirm that malware was not placed on the system by running an antivirus scan.
- Ensure that the antivirus program uses updated signatures.
- Reimage the machine and reset passwords if malware is discovered.
- Speak with the employee to determine any relevant information they may have.
- Provide social engineering training to employees and direct them to immediately report potential hoaxes.
- Implement spam filtering at the email gateway to filter out emails with known phishing indicators, such as known malicious subject lines.

continued, page 2

ISAC Analysis Team Updates

PowerGhost – cryptoMiner Leveraging EternalBlue

FS-ISAC members should be aware of a new cryptoMiner called PowerGhost. Discovered by Kaspersky, PowerGhost leverages the National Security Agency (NSA)-linked EternalBlue exploit to spread. The malware uses multiple fileless techniques to discreetly gain a foothold in corporate networks. This means that data is not stored to its body directly onto a disk increasing the complexity of its detection and remediation. This type of malware can also attack less powerful computerized systems without being noticed, including queue management systems and point of sale terminals which increases the attack surface for campaigns using PowerGhost.

ZombieBoy – cryptoMiner Exploiting Multiple CVEs

Another cryptoMiner exploiting multiple CVEs is ZombieBoy. This new addition to cryptomining has clocked in at $1,000 USD per month in returns. ZombieBoy is an extremely infectious worm utilizing WinEggDrop in the identification of new hosts. ZombieBoy compromises the networks it infects by exploiting numerous vulnerabilities including CVE-2017-9073 which is essentially a remote desktop protocol or RDP vulnerability on Windows XP and on Windows Server 2003 and Server Message Block (SMB) exploits CVE-2017-0146 and CVE-2017-0143. EternalBlue and DoublePulsar are used by the malware in the creation of numerous backdoors which increases the cryptominers chances of compromising a network while making it more difficult to identify and eradicate.

FS-ISAC Awards Cybersecurity Scholarships in Singapore

FS-ISAC announced the recipients of the Building Cybersecurity Diversity (BCD) scholarship in Singapore. The announcement was made at the FS-ISAC AP Summit in Singapore. The scholarship was started by FS-ISAC in 2016 to bridge the diversity gap by helping women interested in cybersecurity kickstart their careers. This is the first year the BCD scholarship is being offered in Asia-Pacific. To date, FS-ISAC has awarded seven scholarships, with additional scholarships to be awarded in Europe and the US later this year. The scholarship offers $5,000 and a trip to the regional summit for a chance to learn and network with influential industry leaders. Scholarship recipients are also paired with industry mentors.

Registration is Open for EMEA and Fall Summits

FS-ISAC Summits are focused around peer-to-peer networking and building relationships or *circles of trust* with financial services organizations. Registration is open for the FS-ISAC EMEA Summit (1-3 October, Amsterdam) and the FS-ISAC Fall Summit (11-14 November, Chicago).

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!

Phishing, continued

- Implement Domain-Based Message Authentication, Reporting and Conformance (DMARC), a validation system that minimizes spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures.
- Adhere to best practices, such as those described in CIS, NIST and other similar frameworks.

To check if it is a hoax:

- Determine if the email contains any specific knowledge about operations or if the language is generic and appears to be part of a mass mailing campaign.
- Conduct searches on keywords, the cryptocurrency wallet ID and sender's email address, as this may yield multiple examples of others affected by the same hoax.
- Check the cryptocurrency wallet ID for transactions to the wallet, which may provide insight into the threat actor's operations.
- Contact FS-ISAC and other information sharing resources to determine if other members report receiving similar emails.

Finally, FS-ISAC has observed activity suggesting people are paying the ransom for some of these emails. Tracking 42 bitcoin wallets cited in the extortion campaign, 30 victims had paid the blackmail demand – for a total of more than $50,000 USD in a one-week period. One wallet alone received 2.54 bitcoins which equates to over $18,000 USD. There has been no suggestion that paying the ransom guarantees any compliance from the threat actors to cease.

FS-ISAC and Cyber Security Agency of Singapore (CSA) Announce Collaboration

FS-ISAC and CSA signed a Memorandum of Understanding (MoU) to advance security threat intelligence sharing and to conduct joint exercises to protect the financial services sector in Singapore. The MoU was signed at FS-ISAC's AP Summit in Singapore. Asia-Pacific is increasingly a top target for cybercriminals and the region is seeing a growing need to bolster cyber-intelligence cooperation to enable cyber-readiness. The collaboration between the two entities will enhance security threat intelligence sharing, helping Singapore to combat cybercrime. Established under the Prime Minister's office, CSA is a law-making body serving 11 critical sectors in Singapore including the financial services sector. Read the full release.