FINANCIAL SERVICES | Information Sharing and Analysis Center

Monthly Newsletter | May 2019 TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

FS-ISAC Member Meetings*
20 May | Taiwan
21 May | Dublin
29 May | Bangkok
12 June | Toronto
19 June | Sydney
25 June | London
25 June | Madrid
5 September | South Africa
5 September | Amsterdam
10 September | Oslo

Cyber-Range Exercises
10 July | Federal Reserve Bank of New York
25 July | Chicago
22 August | St. Louis, MO
16 October | Kansas City, MO

Affiliate Event: Lookingglass Cybersecurity Roadshows | Multiple US Cities

Affiliate Webinar: TruSTAR – Five Must- Do Security Strategies to Combat Account Takeover Fraud | 15 May | Online

FS-ISAC EWS: Financial Services and Systemic Cyber-Attacks* | 21 May | Online

Affiliate Webinar: Sixgill – Compromised Credentials: The Cyber Underbelly of Global Corporations| 21 May | Online

Affiliate Webinar: Forcepoint – Understanding the Importance of Trust | 22 May | Online

FS-ISAC EWS: Attacks on ATMs* | 4 June | Online

Unique Events, Trainings and AP Summit

The Asia Pacific Summit is just around the corner. Get the most out of your time in Singapore.

FS-ISAC AP SUMMIT

Threat Hunting Training | 9 July

This hands-on training is designed to introduce you to new methods and threat datasets to quickly and thoroughly investigate attacks. Register here.

APAC Regional Intelligence Exchange | 12 July

A closed-door, TLP Red session where intelligence can be shared freely among participants. Register here.

Register for the AP Summit, 10-11 July.

Solutions Showcase: Secure Browsing and AI Automation

Join FS-ISAC, Garrison, Bandura Cyber, Shape Security and Blue Hexagon on 29 May for a Solutions Showcase on how to protect users and networks via secure browsing, AI automation and enhancing your SIEM capabilities through the introduction of deep-learning. Learn more.

Early Bird Registration for 2019 EMEA Summit Now Open

Join FS-ISAC, industry thought leaders and peers for the 2019 EMEA Summit, 28-30 October in Berlin! Early bird registration is open, register here.

ISAC Analysis Team Updates FIN6 Changing Tactics

Fin6 has been seen changing tactics in the wild as recently reported by FireEye. They have gone from compromising Point of Sale systems to distributing LockerGoga and Ryuk ransomware. One of FIN6's tactics is to compromise an internet facing system to then steal credentials to move laterally within the target environment using the Windows' Remote Desktop Protocol (RDP). Compromised servers are used as malware "distribution" servers. These are also used to stage LockerGoga and Ryuk ransomware, additional utilities and deployment scripts to automate installation of the ransomware. Members will need to be aware of the change in tactics. Please visit the FS-ISAC Portal for details.

Facebook Groups Serving as New Black Market

Recent reports from researchers at Cisco Talos have discovered a total of 74 Facebook groups with more than 380,000 members who have been acting as marketplaces for illegal activities. In 2018 security researcher Brian Krebs reported findings of 120 private Facebook groups with a total of approximately 300,000 members promoting various kinds of cyberfraud. Many of these groups have been around for eight to nine years.

By just logging into Facebook and searching for "spam" or "CVV", users can find groups that sell and trade stolen bank/credit card information, credentials and spamming tools. Talos worked with Facebook security and all the groups they identified as malicious have been taken down. Members may want their security teams taking a closer look at what is on Facebook regarding their institutions.

Botnet Deploys Malware Families Through US-Based Servers

Researchers at Bromium, (a security firm) have been tracking a phishing and malware campaign that is using servers based in US data centers to spread malware such as GandCrab ransomware and Dridex and Trickbot banking trojans. They indicate there may be a connection to the Necurs botnet.

Emails and documents examined were in English and lures used in this campaign were only relevant to a US audience. Research indicates servers used in these campaigns are still active. FS-ISAC trusted partners and members have reported observing IOCs from the Bromium report. Visit the FS-ISAC Portal for more.

Apply for a *Building Cybersecurity Diversity* Scholarship

The *Building Cybersecurity Diversity* Scholarship is still accepting applications in the US, Europe and Asia Pacific regions until 15 June. Apply here.