FINANCIAL SERVICES | Information Sharing and Analysis Center

Monthly Newsletter | February 2019 TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

FS-ISAC Member Meetings*
12 February | Zurich
20 February | Jakarta, Indonesia
21 February | Columbus, OH
27 February | Melbourne
6 March | London

Cyber-Range Exercises
13 February | Zurich
5 March | Toronto Exchange (TMX)
19 March | Federal Reserve Bank of Atlanta

Bitglass Webinar: Banking on Cloud Security: CASBs in Finance |14 February

FS-ISAC EWS: Achieving Compliance Quickly and at Scale* | 19 February

FS-ISAC Threat Intel Roadshows
12 March | Miami
14 March | Charlotte, NC
19 March | Philadelphia
21 March | Minneapolis

FS-ISAC CAIS Exercises
19-20 March or 26-27 March | Online

Unbound Tech Webinar: Best Practices for Cryptographic Key Management and Protection | 26 February

FS-ISAC EWS: Email Anti-Impersonation for Financial Services* | 12 March

FS-ISAC EWS: Grace RAT* | 26 March

FS-ISAC EWS: Tomorrow's Security Starts Today* | 9 April

Strengthening Sectors Through New Councils

Composed of representatives from FS-ISAC membership, our special interest groups help strengthen our community by providing strategic guidance, industry context and subject matter expertise.

The CCFSE Kicks Off

The Coordinating Council for Financial Sector Europe (CCFSE) kicked off in January and serves as the European counterpart to the US Financial Services Sector Coordinating Council (FSSCC). The CCFSE is dedicated to providing guidance, requirements collection, coordination and public-private relationship management for cyber-resilience and information security in the European financial sector. This council is currently gathering requirements for European authorities to provide clear guidance on the permissible extent of fraud sharing under GDPR.

New Council Serving the Futures Industry

FS-ISAC has created the Futures Commission Merchants Council (FCMC) to better serve the futures industry. A subset of the Securities Industry Risk Group (SIRG), the FCMC will strengthen critical economic infrastructure by enabling dialog among FS-ISAC members in the alternative investment industry. Email SIRG@fsisac.com to learn more.

FS-ISAC's Kunal Sehgal Named a 2019 *One to Watch* by IDG

Kunal Sehgal, executive director of FS-ISAC Asia Pacific (AP) was named a 2019 "Ones to Watch" by IDG's CIO and the CIO Executive Council. The award, which selects rising technology leaders, recognized Kunal's role in spearheading the opening of FS-ISAC's AP Regional Analysis Centre's office and operations in Singapore. Staffed and operated entirely by FS-ISAC, the hub opened in November 2017 in association with the Monetary Authority of Singapore. Read the full announcement.

Registration Open for 2019 Annual Summit

Registration is now open for the 2019 Annual Summit taking place in Orlando, 28 April-1 May. Visit our website to learn more and register!

2019 AP Summit – CFP Closes 23 February

Time is running out to submit your Call for Presentations (CFP) for the AP Summit (10-11 July | Singapore). We truly could not make these Summits happen without the impactful presentations from our members and the value they bring to our community. The CFP closes 23 February, submit a proposal today.

ISAC Analysis Team Updates

"Cobalt" Using Google in Recent Attacks

Cobalt has a history of targeting banks all over the world. In the current campaign, hackers are using URL redirection in PDF documents to get victims at banks and government agencies to download malicious payloads. FS-ISAC's members have observed this activity and IOCs have been shared. More information here (OSINT).

Emerging Threat – Ryuk Ransomware

One of the latest emerging threats to the financial sector is *Ryuk Ransomware*. Recently, attribution for the malware has changed from North Korea (Lazarus Group) to financially motivated Russian criminals (Grim Spider). The threat actors have collected between three and four million dollars in Bitcoin since August of 2018 with their targeted attacks called *Big Game Hunting*. FS-ISAC's GIO has provided information on the ransomware and it justified the current elevated threat levels. Based on OSINT research and reports, its activity is increasing and evolving. Learn more.

TA505: ServHelper and FlawedGrace Malware Campaigns

During most of 2018, security company Proofpoint noted that some threat actors were abandoning ransomware as their primary payload and shifting to distribution of downloaders, information stealers and remote access Trojans (RATs). At the end of last year, well-known threat actor TA505 began targeting banks and retail businesses as it distributed a new back-door called *ServHelper* and the previously observed RAT *FlawedGrace* in order to invest in long-term criminal activity. The group carried out many campaigns using weaponized Office and PDF documents to deliver malware such as Dridex, FlawedAmmy, Locky ransomware and GlobeImposter. This actor has not historically targeted a particular region of the world but has rather focused on retail organizations and the financial services sector.

The malware ServHelper was first spotted in a small TA505 malspam campaign on 9 November 2018. New commands and functionality have been added to almost every new campaign observed since. A "Tunnel" remote desktop variant sets up reverse SSH tunnels to allow the threat actor to access the infected host via Remote Desktop Protocol (RDP). In this version, the malware contains functionality to hijack user accounts or their browser profiles. A second variant is a basic downloader. In some campaigns, this variant downloads FlawedGrace.

FlawedGrace RAT was last seen in late 2017, when it was distributed via an email campaign. The coding style and techniques, however, suggest that FlawedGrace was not written by the same developer as ServHelper according to Proofpoint. This RAT is a large program written in C++. It has been built using object-oriented and multi-threaded programming techniques designed to make reverse-engineering and analyzing the malware harder.

The infrastructure used to launch the observed campaigns remains unknown for the time being, but it does not show the hallmarks specific to Necurs botnet, which TA505 has relied on for massive campaigns in the past. Seeing how these campaigns are targeting financial institutions and retailers, it is likely that the threat actor is looking to steal banking credentials or attempt to use corporate credentials to gain access to sensitive information that could be traded in for profit. The malware variants observed through the various campaigns show TA505's attempts to avoid detection and ensure maximum, durable returns. Learn more.

Sponsor a 2019 FS-ISAC Building Cybersecurity Diversity Scholarship

FS-ISAC is now accepting new mentoring sponsors to support its Building Cybersecurity Diversity Scholarship (BCD). The deadline to sponsor a 2019 scholarship is 15 March! As a mentoring sponsor, your organization will provide financial support and mentorship to a female student or students pursuing degrees, training and/or program certifications in cybersecurity. Any FS-ISAC member or affiliate may sponsor. Step up to encourage and mentor new talent coming into the industry. Learn more about sponsoring.

Delivering Threat Intel – FS-ISAC 2019 Spring Roadshows

The FS-ISAC Threat Intel Roadshow is gearing up for our 2019 Spring series with stops in Miami (12 March), Charlotte, NC (14 March), Philadelphia (19 March) and Minneapolis (21 March). Join us for a free, members-only day of interactive and engaging discussions focusing on the threats that member companies stare down daily.

The highly curated sessions feature intel trend experts, executive leaders, front line analysts. Join FS-ISAC and local members for a day of closed-door, collaborative deep-dives into the threats keeping cyber professionals awake at night. Learn more and save your seat today.

FDX to Talk About Data Privacy at the Retail Banking Conference

American consumers are highly concerned about data privacy and data sharing when using financial applications. Join Financial Data Exchange at the Retail Banking Conference 26-28 March in Austin, TX for a panel discussion on giving consumers control of their data can improve customer engagement. Register today and use code SHARING to save $200.