FS-ISAC Executive Brief

TLP GREEN
November 2017

About FS-ISAC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) helps assure the resilience and continuity of the global financial services infrastructure through sharing threat and vulnerability information, conducting coordinated contingency planning exercises, managing rapid response communications, conducting education and training programs, and fostering collaborations with and among other key sectors and government agencies.

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

On November 13, the FS-ISAC and Johns Hopkins University Applied Physics Laboratory (JHU APL) 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.

FS-ISAC Supports Cyber Exercises to Enhance Sector Resilience and Preparedness

FS-ISAC contributed to two significant cyber exercises that help the financial sector and other sectors be better prepared. On November 7-8, the FS-ISAC participated in the Securities Industry and Financial Markets Association's (SIFMA) Quantum Dawn IV exercise, which simulated a large-scale cyber-attack against numerous financial institutions with rolling impacts for the sector, markets and customers. The goal of this exercise is to practice and improve coordination among financial institutions and with partners in other sectors in preparation for a major incident. FS-ISAC engaged members from the Threat Intelligence Committee, Sheltered Harbor, Media Response Team and Business Resilience Committee. On October 30, the FS-ISAC developed and participated in the "Tri-Sector Exercise", which simulated an attack on an electrical power facility, data center and technology service provider resulting in power outages and service disruptions to financial services firms. Approximately 45 experts and officials from three sectors (financial services, energy and telecommunications) and numerous US Government agencies (e.g., Treasury, DHS, FDIC, Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC), US Commodity Futures Trading Commission (CFTC), law enforcement) participated in the exercise.

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 November 14. 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. The Centre has already assisted members in responding to incidents. 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.

Threat Landscape DDoS Attacks Leveraged Against UK Banks

Unknown threat actors have turned again to distributed denial of service (DDoS) attacks to cause disruption to business networks. Members in the United Kingdom 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. Corero estimates that businesses see eight attempted DDoS attacks daily. DDoS using botnets of internet of things (IoT) devices may be partially responsible for increase. One such botnet that recently gained notoriety for its potential threat is the IoTrooper, also known as the Reaper botnet. It leveraged vulnerable internet-connected webcams, security cameras, and digital video recorders (DVRs) to grow in size, however, initial estimates of its power by security researchers at Check Point were found to be overstated. 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.

Trojan Attacks Steal Data and Disrupt Service to Financial Institutions Globally

Throughout November, FS-ISAC has released alerts and reports about several trojan attacks targeting or impacting the financial industry. The names of these trojan attacks include FALLCHILL, Volgmer, IcedID and Silence and are designed to steel data or disrupt service. For example, FALLCHILL, Volgmer, IcedID and Silence have been discovered on systems throughout the world targeting financial institutions for the purpose of data theft or service disruption. FALLCHILL and Volgmer are remote access trojans (RAT) likely used by the North Korean hacking group Hidden Cobra. The US Department of Homeland Security and Federal Bureau of Investigation released threat detection and risk mitigation guidelines for these trojans in their joint Technical Alert earlier this month. The IcedID and Silence trojans both infiltrate systems using spear phishing campaigns and can be mitigated with employee training to avoid malicious emails, enabling protected view for email attachments and ensuring anti-virus programs are fully updated on all systems. FS-ISAC released Technical Analysis Reports (TAR) for both IcedID and Silence which can be found through the portal.