FINANCIAL SERVICES Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter **December 7, 2015**

Newsletter Contents

FS-ISAC Webinars 1
Upcoming Events 1
FS-ISAC Releases Destructive Malware Best Practices Paper 1
European Summit a Major Success 1
Top Threats for 2016 1
Save the Date: FS-ISAC APAC Summit Coming in 2016 2
Update from the Broker-Dealer Council 2
FS-ISAC Outreach.....2
From the ISAC Analysis Team.....2

FS-ISAC Webinars

Predictive Intelligence: Maximizing Adversary Operational Insights
Brighttalk; Symantec | December 17
Register here

Securing the Complex Digital Attack Surface - How Viewpost Does It
BrandProtect | January 20
Register here

Upcoming Events

Information Sharing Workshop
Paris, France | February 2
Register here

Member Meeting
Australia | February 9
Registration Coming Soon

UK Member Meeting
London | February 16
Registration Coming Soon

Member Meeting
Singapore | March 9
Registration Coming Soon

2016 FS-ISAC Annual Summit
Miami Beach, FL | May 1 - 4
Register here

FS-ISAC Releases Destructive Malware Best Practices Paper

The FS-ISAC released a best practices paper on destructive malware and data integrity for US financial Institutions based on input from 85 experts from 36 companies and associations and 7 government agencies (including National Institute of Standards and Technology, Treasury Department, Department of Homeland Security and National Security Agency), who participated in the Destructive Malware Data Integrity Task Force (DMDITF). Destructive cyberattacks, while rare, are potentially catastrophic, and can present a significant threat to an organization's daily operations and business continuity. Recent cyberattacks against the Las Vegas Sands and SONY Entertainment illustrate how destructive malware attacks can both disrupt operations and harm brand reputation. The FS-ISAC launched the task force in May in response to learnings from a series of cybersecurity exercises sponsored by several government agencies and financial sector associations. An executive summary is publicly available, but a more detailed paper and resource guide is available on secure portion of the FS-ISAC Portal or upon request.

European Summit a Major Success

The second annual European Summit was held from November 30 – December 2 this year in London, England. Featuring keynote speaker, Dr. Ian Levy, Technical Director, Communications-Electronics Security Group (CESG), the Summit was attended by over 385 individuals (up from 282 last year). This year's Summit also saw Tracy Watts from Lloyds Banking Group receive the FS-ISAC Excellence in Information Sharing Award. For those who were unable to attend the Summit, presentations have been made available on the Portal in the "Conference Materieals" folder of the Documents.

Top Threats for 2016

The FS-ISAC's top analyst anticipates four top trends for 2016 based discussions with FS-ISAC members and projections from private intelligence services:

1. Email will continue to be a primary vehicle for injecting malware and conducting reconnaissance, including targeted attacks to senior executives. As security teams improve email filtering and examination capabilities and users become more aware of email tactics, the delivery of malware may migrate to delivering malware through web pages or online advertising (often referred to "malvertizing").
2. Adversaries will continue to abuse the trust individuals have with other and each with trusted assets by impersonating a trusted individual or entity in order to deceive, destroy, disrupt, or steal.
3. Adversaries will continue to target the financial services industry for foreign espionage operations, steal funds, obtain sensitive information, disrupt operations, destroy data/equipment, or harm the reputation of financial institutions. Security practitioners will be challenged in distinguishing hostile expressions from real cyber threats by adversaries.
4. News media coverage of cyber threats will rise leading to greater "Fear, Uncertainty and Doubt" (FUD), which will draw security teams away from real threats to respond to specious media reports. While debate among U.S. presidential campaigns has yet to focus on cyber threats, the policy debate will include cyber threats and mitigation strategies.

continued on next page

Save the Date: FS-ISAC APAC Summit Coming in 2016

Join the FS-ISAC for the 1st Annual APAC Summit in Singapore, 20-23 June, 2016. For more information, please visit: www.fsisac-summit.com/2016-fs-isac-apac-summit. **FS-ISAC Member Presentation Proposals will open next week.** Don't miss out on this opportunity to submit either a panel, standalone, or co-presentation. There is no cost to members for speaking sessions. Member submissions that involve a sponsor will be considered sponsor sessions.

Call for Presentation Opens, Tuesday 15 December, 2015 and closes on Wednesday, 20 January, 2016

Update from the Broker-Dealer Council

Over the past 2-3 months there has been an increase in participation within the Broker Dealer council. The council recently had a presentation and a Q & A from the SEC's OCIE office regarding an alert to firms regarding exams and cybersecurity which was very helpful for members. As membership continues to grow within the BDC, members continue to share information and experience on a range of topics from cyber threats to regulatory audits. Current BDC members have been working on several projects including a questionnaire for the BDC to help better categorize the types of members and firms currently participating in the council. The BDC looks forward to the new year and continued growth and support.

FS-ISAC Outreach

FS-ISAC has been involved of a number of outreach and speaking events on behalf of its membership and information sharing initiatives. Last month our executive team delivered a variety of keynotes, panel discussions, and moderations. Outreach opportunities included events with US regulatory agencies such as the Office of the Comptroller of the Currency (OCC) and the Federal Financial Institutions Examination Council (FFIEC), as well as a number of state bank conferences such as the Executive Leadership of Cybersecurity (ELOC) series.

From the FS-ISAC Analysis Team

Oracle Security Updates

Oracle released Security Alert CVE-2015-4852 on November 10, 2015 to address the publicly-reported deserialization vulnerability involving Oracle WebLogic Server and the Apache Commons library. This vulnerability is present in the "common-collections" library in Java. The exploits demonstrated have to be initiated from the local network, but in poorly configured environments this may lead to truly remote attacks being successful. The products affected have updates available.

Armada Collective Blackmails Swiss Hosting Providers

Several independent reports from hosting providers in Switzerland claimed that they were blackmailed by hacker group Armada Collective. A recent incident occurred in Greece where the hackers threaten to bring down lenders electronic systems. The modus operandi observed was the same as DD4BC, which they demanded a ransom in BTC (Bitcoins) and at the same time the hackers launch a Distributed Denial of Service Attack (DDoS) against the victim's web site to prove their influence. The attackers threaten their victim about the consequences of not paying which will end in a more severe DDoS attack to bring the victims website down.

eDellRoot and DSDTestProvider certificates Vulnerability

A root certificate found on PCs with Dell Foundation Services application from factory installs on Dell computers are vulnerable to man-in-the-middle attacks and allow attackers to sign code. The private key associated with eDellRoot that is used across a number of Dell computers have been exposed. Dell revealed that the DSDTestProvider holds similar characteristics to eDellRoot and that both certificates intended for use by dell support. Updates are available to check and remove the eDellRoot certificate and Dell has provided an article with instructions on the removal of the eDellRoot and DSDTestProvider certificates.