

FINANCIAL SERVICES

Information
Sharing and
Analysis Center

FS-ISAC Monthly Newsletter

November 6, 2014

Newsletter Contents

New On-Site Cyber Threat Intelligence Training Course 15-19 December, 2014	1
Soltra Edge Launches	1
Partner Webinars.....	1
Upcoming Events	1
European Summit In Review	2
FS-ISAC SOC Threat Updates.....	2

Partner Webinars

Home Depot, SEC, and Increasing Board Oversight: Why Metrics Matter More and More

BitSight | November 12

[Register here](#)

Account Takeover Fraud Prevention

PhishLabs | November 18

[Register here](#)

Fill The Security Gaps In Your Firm's Mobile Deployment

Lacon | December 10

[Register here](#)

Upcoming Events

Workshop and Threat Exercise

Brazil | December 4

Registration link coming soon

Cyber Threat Intelligence Training

Reston, VA | December 15 - 19

[Register here](#)

New On-Site Cyber Threat Intelligence Training Course 15-19 December, 2014

In an effort to provide new resources to our members, FS-ISAC is now offering a week-long, hands-on training course on Cyber Threat Intelligence. Conducted by cyber expert Jeff Bardin, the program is held at the FS-ISAC Security Operations Center (SOC). Topics covered include:

- Cyber Intelligence lifecycle from Collections to Dissemination
- Critical Thinking, Cognitive Bias, Structured Analytic Techniques, Types of Analysis, Analytic Writing
- Credibility and reliability of sources, denial and deception detection, analysis of competing hypothesis
- Methods of research, open source tools, cyber personas, and methods of anonymity
- Hands on use of open source tools applying classroom lecture with a 4-5 day apprenticeship, plus a live research exercise that spans 3 days
- Discussions of past and live use cases targeting adversaries, corporate attack surface identification and methods of creating your own cyber intelligence capability integrated with FS-ISAC

Additional classes will be held in 2015. Just for FS-ISAC members, the registration fee represents a 33% savings off the normal fee.

[Register today](#)

Soltra Edge Launches

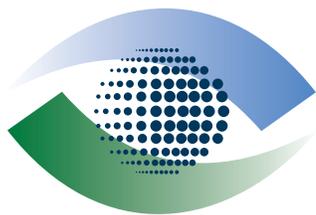
This week, Soltra, the new joint venture between FS-ISAC and DTCC announced the launch of its first product, Soltra Edge. Soltra Edge is a software solution designed to collect massive amounts of cyber threat intelligence from a variety of sources, convert it into standardized language and enable users to take immediate action. Soltra Edge collects, standardizes and routes the flow of cyber threat intelligence between people, communities and devices.

The basic version of Soltra Edge, which contains the features most needed by many organizations, will be available at no cost. Additional versions that support the requirements of larger entities will also be released. Soltra Edge will be available on or around December 2, 2014.

For more information:

Joint Venture website: www.soltra.com

Press release: www.fsisac.com/news



FINANCIAL SERVICES

Information
Sharing and
Analysis Center

FS-ISAC Monthly Newsletter

November 6, 2014

European Summit In Review

This week, FS-ISAC held its first European Summit in London, UK. Over 300 attendees, including members, prospective speakers and sponsors joined together to share information, get updates on the latest cyber security trends, network and help influence the direction of information sharing in Europe. Topics covered ranged from automated threat intelligence sharing to preventing account takeovers and from regional information sharing trends to cyber threat simulation exercises. Each day also featured CISO-led panel discussion.

Presentations from the event will be available shortly to members on the FS-ISAC member portal path:

Conference Materials/Fall 2014
European Summit/

FS-ISAC SOC Threat Updates

Dyre – A New Banking Trojan

Since mid-October, the FS-ISAC SOC has been tracking a new banking Trojan called Dyre or Dyreza. The Dyre Trojan is typically delivered via a phishing email with a malicious PDF attachment. If successful, Dyre monitors the infected machine's browser for connections to online banking websites and steals the user's login credentials.

The FS-ISAC SOC encourages financial institutions to ensure that their computers are patched with the latest Adobe Reader updates, and to encourage employees to follow safe internet browsing and email habits, including never opening links or attachments in unsolicited emails. Financial institutions are also encouraged to monitor for suspicious online banking activity.

POODLE – A New Vulnerability in SSLv3

For the past few weeks, the FS-ISAC SOC has been following a new vulnerability in Secure Socket Layer (SSL) version 3.0. Since 1996, SSLv3 has been in use for encrypting secure internet browser communications. Although SSL has been succeeded by Transport Layer Security (TLS), it is still supported as an option in most web browsers and web servers. The vulnerability, known as POODLE, potentially allows an attacker to decrypt secure communications that still support SSLv3 as an option.

The FS-ISAC SOC is not aware of any exploit activity using the POODLE vulnerability. Nonetheless, FS-ISAC is urging financial institutions to disable support for SSLv3 on all web servers as soon as possible.

Cyber Criminals Are Gearing Up for the Holiday Season – Are your Point of Sale Systems Ready?

The past couple years have seen a sharp increase in Point of Sale (PoS) system attacks. FS-ISAC is expecting this holiday shopping season to be an busy one for cyber criminals looking to steal customer credit card data from PoS systems.

In response, FS-ISAC, in cooperation with the US Secret Service and the Retail Cyber Intelligence Sharing Center (R-CISC), is preparing to release an advisory for retailers and merchants to defend their PoS systems against cyber attacks. The advisory will provide specific recommendations and risk mitigation techniques, based on lessons learned from recent PoS compromises.