CYBERSECURITY WEBINAR
PRESENTED BY SIFMA AND FS-ISAC

Wednesday, August 12, 2015  |  12:00pm - 1:00pm EST
Webinar Agenda & Presenters:

*Introductions and Overview: The Legislative and Regulatory Landscape*
Karl Schimmeck – Managing Director, Financial Services Operations, SIFMA

*Global Information Sharing and Actionable Intelligence with FS-ISAC*
Bill Nelson – President & CEO, FS-ISAC

*Participating in FS-ISAC's Broker-Dealer Council*
Peter Falco – Director of Broker-Dealer Services, FS-ISAC

*Closing Remarks*
Bill Nelson – President & CEO, FS-ISAC
Introductions and Overview: The Legislative and Regulatory Landscape

Karl Schimmeck – Managing Director, Financial Services Operations, SIFMA
Global Information Sharing and Actionable Intelligence with FS-ISAC

Bill Nelson – President & CEO, FS-ISAC
Drawing some relevant correlations

“You know, you can do this just as easily online.”
Agenda Today

- Evolution of the Threat Landscape
- Anatomy of an Attack
- Role of FS-ISAC
- FS-ISAC Broker-Dealer Services
- Security Automation
- What’s Next?
- Risk Management Conclusions
Threat Trends

**Cyber Crime**
- Bad guys are mostly Eastern European although Asian groups are also active
- A complete service based economy supporting their activities
- Attacks are a mix of social engineering and technical attack.

**Hactivists**
- "Anonymous" response to WikiLeaks donation stoppage
- DDoS attacks
- Website defacement

**Nation State**
- Motivations: espionage, disruption, or destruction
- Targeting Government + private sector
Internet Crime: exploiting the www to link suppliers and users

- Online libraries and advertisements of stolen data
- Education on how to launch spamming, phishing, and key logging attacks
- Advertisements for partners for complex fraud schemes
- Recruitment
- Detailed info sharing on technical vulnerabilities of software and specific financial institutions and their service providers
Russian Hacker Toolkit and Tutorial

1. Advanced Hacking Guide with Metasploit
2. Malware Development (RATS, botnets, Rootkits)
3. Convert exe into PDF, XLS, DOC, JPG
4. Exploit development guide
5. Tech Tricks (Spoofing-SMS, email, call)
6. Download any Free Apple Apps
7. Credit Card Hacking
8. Netbanking Hacking-bypass Virtual Keyboard
9. Spreading guide to Infect 100K/Victims per day
10. Advanced Email Hacking Tricks
11. SET(Social Engineering Toolkit) module
12. Links to other Russian hacking sites
Russian Response to Cyber Crime (Outside of its Borders)

- **Russia Issues International Travel Advisory to it’s Hackers** – *Wired; Poulsen, K.* (2013, September 3). Russia’s Foreign Ministry issued a public notice advising “citizens to refrain from traveling abroad, especially to countries that have signed agreements with the U.S. on mutual extradition.”

- The notice was triggered in part by the June arrest of alleged Russian hacker Aleksander Panin, who’s charged in the U.S. with a $5 million online banking caper.

- Panin was picked up in the Dominican Republic on an Interpol Red Notice and shipped off to the U.S. in July.

- Russia said at the time the extradition was “vicious”, “inappropriate” and “unacceptable.”
Malcode Infection Techniques

• **Phishing** – Widespread email – lots of victims.

• **Spearphishing** – Targeted email aimed at a few victims.

• **Drive by Download** – the unintentional download of malicious software, typically from an infected reputable site, merely by visiting a page.

• **Fake Anti-Virus Software** – Alarming user with false infection warning, tricked into downloading malware.

• **WebInject** – functionality that can be used to modify a web page on the infected end host.

• **Malvertising** – injecting malware thru ads on legitimate webpages.
Insider Threat-- Trustwave’s List of 7 Deadly Employee Sins

1) **Pathetic Passwords**: The most common corporate password is "Password1" because it meets the minimum complexity requirements. 15% of physical security tests, written passwords were found on and around user workstations.

2) **Peeping ROM**: 71% of workers sneak a peek at a co-workers or stranger's workstation. One in three workers leaves their computers logged on when they are away from their desk.

3) **USB Stick Up**: 60% of users who find random USB sticks in a parking lot will plug them into their computers; add those sticks that includes a company logo and the number increases to 90%.

4) **Phish Biting**: 69% of phishing messages past spam filters; 27% of IT organizations have users who have fallen for malicious e-mail attacks.

5) **Reckless Abandon**: 70% of users do not password-protect their smartphones, and 89% of people who find lost cell phones rummage through the digital contents.

6) **Hooking up with Another Man's WiFi**: By 2015, the number of WiFi hotspot deployments will increase 350%, but currently, only 18% of users use a VPN tool when accessing public WiFi

7) **A Little Too Social**: 67% of young workers think corporate social media policies are outdated, and 70% regularly ignore IT policies. Just over half (52%) of enterprises have seen an increase of malware infections due to employees' use of social media
NBC.com Infected With Malware Targeting Personal Financial Information

For five hours on Thursday NBC.com distributed malware that invaded visitors' computers and targeted their banking information, says a cyber security team.

posted on February 21, 2013 at 7:34pm EST

Tessa Stuart
BuzzFeed Staff

For five hours on Thursday visitors to NBC.com were infected by a virus known to target personal financial information, according to a cyber security team based out of the Netherlands that detected the virus.
LinkedIn

REMINDERS
Invitation reminders:
• From Danny Lawrence (Key Account Director Municipalities at Lukoil)

PENDING MESSAGES
• There are a total of 23 messages awaiting your response. Visit your InBox now.

Don't want to receive email notifications? Adjust your message settings.
LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2012, LinkedIn Corporation.

*The IP (2.145.24.15) is registered to Iran, Islamic Republic Of Tehran Iran Cell Service And Communication Company (http://whois.domaintools.com/2.145.24.15)

For additional information, please contact Gary Warner, Director of Research in Computer Forensics – gar@cis.uab.edu/ 205.422.2113 or the report author, Sarah Turner (saturner@uab.edu).

© The University of Alabama at Birmingham
Spear Phishing– New Twist

From: Federal Bureau of Investigation
Sent: Monday, March 30, 2015 05:35 PM
Subject: FINAL NOTIFICATION FROM FBI

Read the attached mail and respond now or be prosecuted!!

Here’s the kicker--
Nigerian phone number with an Albanian email address!!!
Fake Anti-Virus Scam
Use of Inject Writers

Botnet Operator

Visits Criminal Marketplace

Purchases or leases banking Trojan or crimeware kit

RUSSIAN HACKERS

Visits Criminal Marketplace

Purchases code specific for targeted FI

Botnet Operator incorporates inject code with crimeware kit

Botnet Operator users delivery system for newly- customized malware

Account Hijacking

Use of Inject Writers
WebInject Example

This is the original login

Returning Users
Log On

User Id
Password
Remember my User ID
Forgot User Id/Password

Log Into Accounts

Login with the additional email field injected

Returning Users
Log On

User Id
Email
Password
Remember my User ID
Forgot User Id/Password

Log Into Accounts

Login with Secure Token entry

Enter Secure Token

Secure Token
Log Into Accounts
Malvertising

- Does not require any user action (like clicking).
- Does not exploit any vulnerabilities on the website.
- Infections delivered through Web page advertisements.
Ransomware

To release a lock your computer you should pay the fine in amount of £100. In the case of ignoring the payment, the program will remove illegal materials while keeping your personal information is not guaranteed.

You could pay the forfeit in two ways:

1) Paying through Ukash:
Use the code received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

2) Paying through Paysafecard:
Use the code (and a password if needed) received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.
Anatomy of an Attack

Financial Services Information Sharing & Analysis Center
Attacker Mindset

- An adversary will attack the network’s weakest point
  - The User
  - The Supply Chain

- Targeting has become very selective
  - Executives & staff (access to data)
  - System and network administrators (privileged credentials)
  - Third Party vendors

- Open source information gathering allows the adversary to become very familiar with target prior to attack
  - Organizational structure, technologies, research activities

- Attacker will utilize minimum complexity to be successful
  - Simple techniques allow the adversary to leverage more attacks (less training and technology required)
Common Attack Scenario
Adversary Gains Foothold

Adversary determines that it has an interest in an Organization's "protected" information
Tainted email sent to Organization's users
User clicks on link to compromised web site, remote admin tool installed
Additional tools uploaded
Using credentials gained, adversary works to establish additional footholds
Adversary frequently will perform data mining through a host (Host 2) other than the initially compromised host (Host 1).

Remote host may or may not be the same IP/Domain as initial attack.

Data mining typically occurs on file servers via share permissions.

Multiple files are typically extracted as an encrypted bundle.
DDoS Attack

Compromised PCs

Company X edge router

Your Internet ISP

Company X network and web server

Servers controlled by attackers

Your customers
Background FS-ISAC
MISSION:
Sharing Timely, Relevant, Actionable Cyber and Physical Security Information & Analysis

- A nonprofit private sector initiative formed in 1999
- Designed/developed/owned by financial services industry
- Mitigate cybercrime, hactivist, nation state activity
- Process thousands of threat indicators per month
- 2004: 68 members; 2015: 5200 members
- Sharing information globally
FS-ISAC Operations

Information Sources

- DHS
- Treasury & FS Regulators
- FBI, USSS, NYPD
- Other Intel Agencies
- iSIGHT Partners
- Info Sec
- Secunia Vulnerabilities
- Wapack Labs
- Malware Forensics
- NC4 Phy Sec Incidents
- MSA Phy Sec Analysis

GOVERNMENT SOURCES

PRIVATE SOURCES

CROSS SECTOR SOURCES

FS-ISAC 24x7 Security Operations Center

Member Communications

- Information Security
- Physical Security
- Business Continuity/Disaster Response
- Fraud Investigations
- Payments/Risk

Alerts

Member Submissions

Cross Sector (other ISACS)

Open Sources (Hundreds)
Information Sharing & Analysis Tools

Threat Data, Information Sharing
- Anonymous Submissions
- CyberIntel Listserver
- Relevant/Actionable Cyber & Physical Alerts (Portal)
- Special Interest Group Listservers (Broker Dealer Council)
- Document Repository
- Member Contact Directory
- Member Surveys
- Risk Mitigation Toolkit
- Threat Viewpoints

Ongoing Engagement
- Bi-weekly Threat Calls
- Emergency Member Calls
- Semi-Annual Member Meetings and Conferences
- Regional Outreach Program
- Bi-Weekly Educational Webinars

Readiness Exercises
- US, UK, and EU Government Sponsored Exercises
- Cyber Attack against Payment Processes (CAPP) Exercise
- Advanced Threat/DDoS Exercise
- Industry exercises-Systemic Threat, Quantum Dawn, Hamilton Series, etc.
Information Sharing: Traffic Light Protocol

- Restricted to a defined group (e.g., only those present in a meeting.) Information labeled RED should not be shared with anyone outside of the group.
- This information may be shared with FS-ISAC members.
- Information may be shared with FS-ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums.
- This information may be shared freely and is subject to standard copyright rules.
FS-ISAC Cycles of Trust

- Clearing House and Exchange Forum (CHEF)
- Payments Risk Council (PRC)
- Payments Processor Information Sharing Council (PPISC)
- Business Resilience Committee (BRC)
- Threat Intelligence Committee (TIC)
- Community Institution Council (CIC)
- Insurance Risk Council (IRC)
- Compliance and Audit Council (CAC)
- Cyber Intelligence Listserv
- Asset Manager Council (AMC)
- Broker-Dealer Council (BDC)

Member Reports Incident to Cyber Intel list, or via anonymous submission through portal

Members respond in real time with initial analysis and recommendations

SOC completes analysis, anonymizes the source, and generates alert to general membership
## Types of Information Shared

<table>
<thead>
<tr>
<th>Cyber Threats, Vulnerabilities, Incidents</th>
<th>Physical Threats, Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Malicious Sites</td>
<td>✓ Terrorism</td>
</tr>
<tr>
<td>✓ Threat Actors, Objectives</td>
<td>✓ Active Shooter</td>
</tr>
<tr>
<td>✓ Threat Indicators</td>
<td>✓ Hurricanes</td>
</tr>
<tr>
<td>✓ Tactics, Techniques, Procedures</td>
<td>✓ Earthquakes</td>
</tr>
<tr>
<td>✓ Courses of Action</td>
<td>✓ Other meteorological events</td>
</tr>
<tr>
<td>✓ Exploit Targets</td>
<td>✓ Geopolitical impacts</td>
</tr>
<tr>
<td>✓ Denial of Service Attacks</td>
<td>✓ Pandemic</td>
</tr>
<tr>
<td>✓ Malicious Emails: Phishing/Spearphishing</td>
<td>✓ Type, location, severity</td>
</tr>
<tr>
<td>✓ Software Vulnerabilities</td>
<td>✓ Impact analysis and risk mitigation</td>
</tr>
<tr>
<td>✓ Malicious Software</td>
<td>✓ Business resilience preparation and incident response</td>
</tr>
<tr>
<td>✓ Analysis and risk mitigation</td>
<td></td>
</tr>
<tr>
<td>✓ Incident response</td>
<td></td>
</tr>
</tbody>
</table>

Financial Services Information Sharing & Analysis Center
FS-ISAC Broker-Dealer Services
SIFMA’s Program to Assist Broker-Dealers with Information Sharing

- SIFMA is a contributor to funding of Soltra threat intelligence automation.
- SIFMA has funded first year FS-ISAC memberships for all small to medium size SIFMA broker-dealer members that are not already members of FS-ISAC.
  - SIFMA members need to enroll in 2015 to obtain benefits of free FS-ISAC membership.
  - There is no requirement for broker-dealers to renew after the first year; although all will be encouraged to do so.
  - FS-ISAC has created new services for broker-dealers.
FS-ISAC Broker Dealer Council

Objectives

Assist FS-ISAC members that are broker dealers in solving information security challenges by

1) Sharing with the B-D community methods to prepare, respond, and mitigate the risks associated with threats and vulnerabilities.

2) Performing analysis of threats and vulnerabilities affecting broker-dealers.
Peter Falco, Director of Broker Dealer Services for FS-ISAC

Experience
– 11 years SVP, Technical Office for municipal bond dealer
– 20 years IT and cybersecurity (Prudential, IBM)

Goals
– Generate bi-weekly threat and vulnerability summaries.
– Create, monitor and comment on Broker-Dealer email list-server.
– Facilitate monthly Broker-Dealer WebEx conference calls.
– Create and facilitate working groups.
– Develop services based upon member feedback.
Participating in FS-ISAC's Broker-Dealer Council

Peter Falco – Director of Broker-Dealer Services, FS-ISAC
Threat Intelligence- Security Automation

Will Revolutionize Information Sharing
### THE NEED FOR SPEED

**Attackers Act 150x Faster Than Victims Respond**
- Minutes vs. Weeks/ Months

<table>
<thead>
<tr>
<th></th>
<th>Seconds</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Attack to Initial Compromise (Shorter Time Worse)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10%</td>
<td>75%</td>
<td>12%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td><strong>Initial Compromise to Data Exfiltration (Shorter Time Worse)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8%</td>
<td>38%</td>
<td>14%</td>
<td>25%</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td><strong>Initial Compromise to Discovery (Longer Time Worse)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
<td>13%</td>
<td>29%</td>
<td>54%</td>
</tr>
</tbody>
</table>

- Attackers have honed their skills to come at you rapidly
- Defenders take a long time to feel the impact of an attack

---

The need for speed in cybersecurity highlights the urgency and the disparity between the quick actions of attackers and the slower reactions of victims. This table illustrates the time frames from the initial attack to various stages of compromise, showing that attackers can act much faster than defenders can respond. The data suggests that the shorter the time taken from the initial attack to compromise, the worse the impact, and vice versa for the discovery stage. This underscores the importance of rapid response and proactive measures to mitigate such threats.
Threat Intelligence Automation

• Soltra– joint venture between FS-ISAC and DTCC
  • Industry-owned utility to automate threat intelligence sharing
  • DTCC IT & scalability; FS-ISAC community & best practices
  • Funded by the industry, including SIFMA and some of its largest members
  • At-cost model; open standards (STIX, TAXII)
  • Provide platform that can be extended to all sizes of financial services firms, other ISACs and industries
  • Integrate with vendor solutions (firewalls, intrusion detection, anti-virus, threat intelligence, etc.)

• Status
  • General availability of free Soltra Edge software-- 12/3/2014
  • 1500 downloads of Soltra Edge, 40% from FS sector
  • FS-ISAC instance, January 2015
  • Membership model adopted 8/5/2015
  • Adapter and Network capabilities-- 2015
STIX Constructs

An open standard to categorize cyber threat intelligence information

Atomic

Observable

What threat activity are we seeing?

Tactical

Indicator

What threats should I look for on my networks and systems and why?

Operational

Incident

Where has this threat been seen?

Course of Action

What can I do about it?

ExploitTarget

What weaknesses does this threat exploit?

Strategic

ThreatActor

Who is responsible for this threat?

Campaign

Why do they do this?

TTP

What do they do?
Threat Intelligence Automation Solution

- Instead of 2% or less of attacks blocked, detected, or prevented, a much higher percentage of attacks are stopped in seconds.
What’s Next?

Financial Services Information Sharing & Analysis Center
Potential Emerging Threat Landscape

Mobile Platforms
Bandwidth and continuous connectivity makes it an ideal platform for launching attacks. Tools are now available on Google Play and for the iPhone.

Social Media
People instantly, globally connected 24/7. Syrian Electronic Army hacking of AP Twitter demonstrated moving markets

Supply Chain
Compromise of supply chain has occurred within financial sector. Hardware and software integrity are resource intensive challenges
Evolution from Disruptive to Destructive Attacks

Advanced DDOS – 2012, 2013
- 40+ FIs targeted, wake-up call for FS industry
- Resulted in dynamic, effective information sharing

Shamoon – 2012
- Malware executable spread using network shared drives
- Corrupts files and wipes device boot blocks at specified date
- A group named "Cutting Sword of Justice" claimed responsibility
- Attack on 30,000 Saudi Aramco workstations

South Korean Attacks – 2013
- 2 banks, media company and insurance company, patch systems targeted
- Wipers hit Windows, Linux and UNIX OS and removed file systems. Over 3,000 machines made unbootable

SONY – 2014
- SMB Worm Tool, listening implant, backdoor, proxy tool, destructive hard drive tool, destructive target cleaning tool, network propagation wiper
- Intellectual property and sensitive information released publically.
- Impact– financial system data made inaccessible, inability to disburse or collect payments, financial results delayed for many months.
12/3/2014 speech-- Sarah Raskin, Deputy Secretary of the U.S. Treasury. She provided guidance to chief executive officers, chief risk executives and boards of directors for assessing cybersecurity preparedness:

**Baseline Protections**
- Is cybersecurity part of your current risk management framework?
- Is your FI following the National Institute for Standards and Technology (NIST) Framework?
- Do you know the cyber risks of using your vendors and third-party service providers and do you know the rigor of their cybersecurity controls?
- Do you have cyber risk insurance?
- Do you engage in basic cyber hygiene (*to protect your enterprise and your customers*)?
Sarah Raskin guidance (continued)

**Information Sharing**
- Do you share information with the Financial Services Information Sharing & Analysis Center, as well as other industry groups, and if so, how often?

**Response and Recovery**
- Do you have a cyber-incident playbook, and who is the point person for managing the response and recovery?
- What roles do senior leaders and the board play in managing and overseeing the cyber incident response?
- When and how do you engage law enforcement after a breach?
- After a cyber-incident, when and how do you inform customers, investors and the general public?
Information Sharing

One Organization’s Incident becomes the Industry Response
Contact Information

Bill Nelson, President & CEO  
Peter Falco, Director Broker Dealer Council

bnelson@fsisac.us  
pfalco@fsisac.us  
908-233-3965

www.fsisac.com

Financial Services Information Sharing & Analysis Center
THANK YOU TO OUR EXCLUSIVE WEBINAR SPONSOR

[Decoded Technologies logo]