FS-ISAC

CHARLES BRETZ

THE PUZZLE OF PAYMENTS SECURITY:
Fitting the Pieces Together to Protect the Retail Payments System
Information Sharing

To be forewarned is to be fore-armed
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; 2014: 5900 participants
- 2500 members bound by operating rules
- Sharing information globally
FS-ISAC Operations

Information Sources
- DHS
- Treasury & FS Regulators
- FBI, USSS, NYPD
- Other Intel Agencies

Government Sources

Private Sources
- ISIGHT Partners
- Info Sec
- Secunia Vulnerabilities
- Wapack Labs Malware Forensics
- NC4 Phy Sec Incidents
- MSA Phy Sec Analysis

Cross Sector Sources
- Cross Sector (other ISACS)
- Open Sources (Hundreds)

FS-ISAC 24x7 Security Operations Center

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

FS-ISAC, Not for publication
Information Sharing & Analysis Tools

**Threat Data, Information Sharing**
- Anonymous Submissions
- CyberIntel Listserver
- Relevant/Actionable Cyber & Physical Alerts (Portal)
- Special Interest Group Listservers (Payments Risk Council and Payment Processor Information Sharing Council)
- Document Repository
- 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 and EU Government Sponsored Exercises
- Cyber Attack against Payment Processes (CAPP) Exercise
- Advanced Threat/DDoS Exercise
- Industry exercises-Systemic Threat, Quantum Dawn Two, 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.
How FS-ISAC Works: Circles of Trust

<table>
<thead>
<tr>
<th>IRC</th>
<th>Insurance Risk Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHEF</td>
<td>Clearing House and Exchange Forum</td>
</tr>
<tr>
<td>PRC</td>
<td>Payments Risk Council</td>
</tr>
<tr>
<td>PPISC</td>
<td>Payment Processor Information Sharing Council</td>
</tr>
<tr>
<td>CIC</td>
<td>Community Institution Council</td>
</tr>
<tr>
<td>CAC</td>
<td>Compliance and Audit Council</td>
</tr>
<tr>
<td>TIC</td>
<td>Threat Intelligence Committee</td>
</tr>
</tbody>
</table>

---

**Member reports incident to Cyber Intel List**

**Members respond with initial analysis and recommendations**

**SOC completes analysis, anonymizes the source, and generates alert to general membership**
1876
First commercial telephone installation-by two bankers

1978
Electronic Funds Transfer Act

1981
First version of online banking

1993
All electronic ACH

1999
FS-ISAC established

2014
Security automation launched

Financial Services Information Sharing & Analysis Center
## The need for speed

<table>
<thead>
<tr>
<th>Time Interval</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</strong></td>
<td>10%</td>
<td>75%</td>
<td>12%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td><strong>(Shorter Time Worse)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Initial Compromise to Data Exfiltration</strong></td>
<td>8%</td>
<td>38%</td>
<td>14%</td>
<td>25%</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td><strong>(Shorter Time Worse)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Initial Compromise to Discovery</strong></td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
<td>13%</td>
<td>29%</td>
<td>54%</td>
</tr>
<tr>
<td><strong>(Longer Time Worse)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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.
SECURITY AUTOMATION STATUS

• 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
  • 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.)

• Soltra Edge
  • First available was on 12/3/2014
  • FS-ISAC instance, January 2015
  • Over 900 downloads of Soltra Edge, less than half from financial services sector
  • 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?
Instead of 2% or less of attacks blocked, detected, or prevented, a much higher percentage of attacks are stopped.

Threat Intelligence Automation Solution

- Org A
- Intelligence Repository
- Many Trusted Orgs

Financial Services Information Sharing & Analysis Center