Agenda

• Threat Trends
• Fraudster/Attacker Techniques
• Account Takeover Attacks
• Criminal DDoS
• Mitigation Techniques
• FS-ISAC Overview and Hive Intelligence
• 2013 Microsoft FS Industry Civil Action
• What’s Next?
Evolution of Threat Landscape

Financial Services Information Sharing & Analysis Center
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
- WikiLeaks
- Anonymous, Lulzsec
- DDoS attacks
- Data loss—combination of hacking and insiders

Nation State
- Motivations: espionage (APT), disruption (AQCF)
- 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
Corruption

Corruption exists at some level in all countries; however, the interaction between government officials and TOC (Transnational Organized Crime) networks is particularly pernicious in some countries. Among numerous examples, ... in Russia, the nexus among organized crime, some state officials, the intelligence services, and business blurs the distinction between state policy and private gain.
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
The basketball league is headed by Sergei Ivanov, a former KGB officer who was tapped by Russian President Vladimir Putin as deputy prime minister of Russia.

Russian Vice Premier Sergei Ivanov (left) and ChronoPay co-founder Pavel Vrublevsky at a Russian Basketball League game, April 2011.
Chronopay was mentioned multiple times in research papers and investigations of several major cybercrimes, including music piracy, DNS changers, scareware, and fake pharmacy distribution networks. Igor Gusev, a former partner of Vrublevsky, claimed that Vrublevksy was also behind RedEye, a notorious organizer of spam, fake anti-viruses, and porno distribution networks.
Russian Response to Cyber Crime (Outside of its Borders)

• Russia Issues International Travel Advisory to its 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** – Tricking search engines (Google, Bing, Yahoo, etc.) to display links to malicious content
- **Fake Anti-Virus Software** – Alarming user with false infection warning, tricked into downloading malware
- **Pharming/DNS Redirection** – Modifying user PC or DNS provider to send traffic to malicious servers
- **Drive by Email** – Opening email or preview panel
1. **ICC Cricket World Cup 2011 Wallpaper**
You +1’d this publicly. Undo
4 hours ago – Download Wallpapers of ICC Cricket World Cup 2011. Cricket Leading Portal, The Cric Fan Club Offers World Cup Cricket Wallpapers in ...

2. **World Cup Wallpaper | unOfficial FIFA WorldCup Wallpapers**
www.worldcupwallpaper.com
You +1’d this publicly. Undo
World Cup Wallpaper | unOfficial FIFA WorldCup Wallpapers Site - worldcupwallpaper.com.

3. **World Cup Wallpapers**
www.worldcupwallpapers.com
You +1’d this publicly. Undo
Cool World Cup Wallpapers. ... 1682 views World Cup Wallpapers Germany team2. 2.38/5. World Cup Wallpapers Mario... 963 views World Cup Wallpapers ...

4. **FIFA Football World Cup 2010 Wallpapers (for Minimalism Lovers ...**
www.smashingmagazine.com/.../fifa-football-world-cup-2010-wallp... Cached - Similar
You +1’d this publicly. Undo
Jun 6, 2010 – The 2010 Football World Cup is coming up in a couple of days and we decided to celebrate this event with an exclusive set of very simple ...

5. **Soccer Desktop**
www.soccer-desktop.com
You +1’d this publicly. Undo
Free soccer desktop wallpapers, screensavers, cursors and icons. ... Steven Gerrard Wallpapers. Posted by admin ... Some WorldCup and Sexy Screensavers ...

6. **ICC World Cup 2011 Wallpapers - Santabanta.com**
www.santabanta.com › CricketCached
You +1’d this publicly. Undo
Wallpaper # 1-10 of 25 ICC World Cup 2011 wallpapers at 1024x768, 1280x1024 and 1280x800 resolution with ICC World Cup 2011 desktop pictures, photos ...
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.
Fake Anti-Virus Scam
Pharming/DNS Redirection
Drive-by Email -> Open email or view email preview screen
LinkedIn Spear Phishing

“linkedin.com” Malware—September 4, 2012

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
Fed Ex Spear Phishing
“fedex.com” Malware– September 6, 2012

FedEx Billing Online - Ready for Payment

fedex.com

Hello
You have a new not paid invoice(s) from FedEx that is ready for payment.
The following invoice(s) are ready for your review:

<table>
<thead>
<tr>
<th>Invoice Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>5210-78941</td>
</tr>
</tbody>
</table>

To pay or review these invoices, please sign in to your FedEx Billing Online account by clicking on this link: http://www.fedex.com/us/account/fbo

Note: Please do not use this email to submit payment. This email may not be used as a remittance notice. To pay your invoices, please visit FedEx Billing Online, http://www.fedex.com/us/account/fbo

Thank you,
Revenue Services
FedEx

This message has been sent by an auto responder system. Please do not reply to this message.

*The IP (109.162.10.160) is registered to Ukraine Kiev Kyivstar Gsm (http://whois.domaintools.com/109.162.10.160)

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).
Email address: noreply@direct.nacha.org <farmyardrd660@freefallradio.com>

Subject line: Direct Deposit payment was rejected

We would like to notify you, that your latest Direct Deposit transaction (ID719346582090) was declined, because your business software package was out of date. The detailed information about this matter is available in the secure section of our web site:

Details

Please contact your financial institution to acquire your updated version of the software needed.

Yours faithfully,

ACH Network Rules Department
NACHA | The Electronic Payments Association

17589 Sunrise Valley Drive, Suite 279
Herndon, VA 27029
Phone: 703-xxx-xxxx Fax: 703-xxx-xxxx
IRS Phish

Your Tax Payment (ID: 44185255023500), recently from your checking account was returned by your bank.

Canceled Tax Transfer

Reason for rejection, see details in the report below: http://simurl.com/zehfem

After you get your Electronic Filing PIN, enter it in the Electronic Filing PIN field when filing your return. The Electronic Filing PIN is a temporary PIN used by the IRS to verify your identity when you e-file. Keep a copy of your signed tax return for your records.

Internal Revenue Service, Metro Plex 1, 8401 Corporate Drive, Suite 300, Landover, MD 20785
Spear Phishing– New Twist

From: OFFICIAL MAIL
Sent: Wednesday, March 30, 2011 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!!!
<table>
<thead>
<tr>
<th>DATE</th>
<th>SPOOFED BRAND</th>
<th>ATTACK TYPE</th>
<th>INITIAL VT DETECTION RATE</th>
<th>LATEST VT RATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/20/2012</td>
<td>Verizon Wireless</td>
<td>BlackHole Exploit Kit &gt; Generic Bad thing</td>
<td>3 out of 42</td>
<td>4 out of 40</td>
</tr>
<tr>
<td>6/20/2012</td>
<td>UPS + DHL</td>
<td>Zipped .EXE &gt; Generic Bad Thing</td>
<td>4 out of 42</td>
<td>6 out of 42</td>
</tr>
<tr>
<td>6/19/2012</td>
<td>USPS</td>
<td>Zipped .EXE &gt; SpyEye/Cridex/Bredolab</td>
<td>5 out of 42</td>
<td>10 out of 42</td>
</tr>
<tr>
<td>6/18/2012</td>
<td>Verizon Wireless</td>
<td>BlackHole Exploit Kit &gt; Ransom/Birele/ZeuS</td>
<td>0 out of 42</td>
<td>20 out of 42</td>
</tr>
<tr>
<td>6/15/2012</td>
<td>Verizon Wireless</td>
<td>BlackHole Exploit Kit &gt; ZeuS/Cridex</td>
<td>4 out of 42</td>
<td>28 out of 42</td>
</tr>
<tr>
<td>6/15/2012</td>
<td>Habbo.com</td>
<td>BlackHole Exploit Kit &gt; ZeuS/Cridex</td>
<td>20 out of 35</td>
<td>29 out of 42</td>
</tr>
<tr>
<td>6/14/2012</td>
<td>Tax Payment Failed/IRS</td>
<td>BlackHole Exploit Kit &gt; Zeus</td>
<td>4 out of 35</td>
<td>29 out of 42</td>
</tr>
<tr>
<td>6/12/2012</td>
<td>DHL</td>
<td>Zipped .EXE &gt; Andromeda</td>
<td>27 out of 42</td>
<td>35 out of 42</td>
</tr>
<tr>
<td>6/12/2012</td>
<td>Twitter.com</td>
<td>BlackHole Exploit Kit &gt; ZeuS</td>
<td>14 out of 42</td>
<td>29 out of 42</td>
</tr>
<tr>
<td>6/12/2012</td>
<td>LinkedIn.com</td>
<td>BlackHole Exploit Kit &gt; ZeuS</td>
<td>12 out of 42</td>
<td>29 out of 42</td>
</tr>
<tr>
<td>6/12/2012</td>
<td>Amazon.com</td>
<td>BlackHole Exploit Kit &gt; Cridex/Carberp/Dapato</td>
<td>5 out of 42</td>
<td>24 out of 41</td>
</tr>
<tr>
<td>6/11/2012</td>
<td>Amazon.com</td>
<td>BlackHole Exploit Kit &gt; Cridex/ZeuS/Dapato</td>
<td>4 out of 42</td>
<td>24 out of 41</td>
</tr>
<tr>
<td>6/11/2012</td>
<td>Myspace.com</td>
<td>BlackHole Exploit Kit &gt; Cridex/ZeuS/Dapato</td>
<td>4 out of 42</td>
<td>27 out of 41</td>
</tr>
<tr>
<td>6/8/2012</td>
<td>Xanga.com</td>
<td>BlackHole Exploit Kit &gt; Cridex/ZeuS/Dapato</td>
<td>5 out of 38</td>
<td>30 out of 42</td>
</tr>
<tr>
<td>6/6/2012</td>
<td>Craigslist.com</td>
<td>BlackHole Exploit Kit &gt; Cridex/ZeuS</td>
<td>5 out of 42</td>
<td>32 out of 42</td>
</tr>
</tbody>
</table>
Account Takeover Attacks

Financial Services Information Sharing & Analysis Center
Drawing some relevant correlations

"You know, you can do this just as easily online."
30 Wash. Hospital Hit By $1.03 Million Cyberheist

Organized hackers in Ukraine and Russia stole more than $1 million from a public hospital in Washington state earlier this month. The costly cyberheist was carried out with the help of nearly 100 different accomplices in the United States who were hired through work-at-home job scams run by a crime gang that has been fleecing businesses for the past five years.

Last Friday, The Wenatchee World broke the news of the heist, which struck Chelan County Public Hospital No. 1, one of several hospitals managed by the Cascade Medical Center in Leavenworth, Wash. The publication said the attack occurred on Apr. 19, and moved an estimated $1.03 million out of the hospital’s payroll account into 96 different bank accounts, mostly at banks in the U.S.
Account Takeover

Password-stealing Trojan sent as e-mail attachment

Online banking credentials sent to criminal

Criminal logs into victim company’s bank account

Criminal Sends Sub-$10,000 Payments to Money Mules

Mules withdraw cash and forward to criminals overseas
Evolution of Attacks and Response: August 2009 Business Account Takeover

The Attack:

- Spear Phishing email requests clicking on embedded link
- Link downloads malware onto their individual computers.
- Malware contains keylogger which harvests online banking credentials.
- **If Two Factor Authentication not used**, username and password credentials used to login manually to account and initiate funds transfer.
- **If Two Factor Authentication is used**, Trojan will IM criminal when user is online and will support session hijacking.
**Fake Maintenance Page, Allows Criminals Time to Make a Transaction**

<table>
<thead>
<tr>
<th>Your FI NAME</th>
<th>MAINTENANCE PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thank you for your submission</td>
<td></td>
</tr>
<tr>
<td>Please allow 15 to 30 minutes for your request to be synchronized with our server.</td>
<td></td>
</tr>
<tr>
<td>You will be able to login after the request is synchronized.</td>
<td></td>
</tr>
<tr>
<td>Multifactor authentication will only be required for the pre-selected functions.</td>
<td></td>
</tr>
</tbody>
</table>
Deep Dive: DDoS Associated with Cybercrime

Financial Services Information Sharing & Analysis Center
DDOS Attack Against FIs to Hide Account Takeovers

- Criminals use malware to originate unauthorized wire transfers and ACH.
- Business customers have a pattern of checking balances and making many online transactions everyday.
- The criminals launched denial of service attacks against the banks’ online banking system to obscure the unauthorized activity.
- Hundreds of Dirt Jumper DDoS attacks reported in 2012.
- Dirt Jumper and related DDoS malware attacks have proliferated worldwide in 2013.
DDoS Attack on Bank Hid $900,000 Cyberheist

A Christmas Eve cyberattack against the Web site of a regional California financial institution helped to distract bank officials from an online account takeover against one of its clients, netting thieves more than $900,000.

At approximately midday on December 24, 2012, organized cyber crooks began moving money out of corporate accounts belonging to Ascent Builders, a construction firm based in Sacramento, Calif. In short order, the company’s financial institution – San Francisco-based Bank of the West – came under a large distributed denial of service (DDoS) attack, a digital assault which
DDoS attack used in conjunction with Account Takeover

Distributed Denial Of Service Attacks (DDoS) - Architecture Diagram
DDoS Attack

Compromised PCs

Company X edge router

Your Internet ISP

Company X network and web server

Your customers

Servers controlled by attackers
Growing Botnet

- Started small with only a few hundred compromised servers and PCs
- Currently includes tens of thousands of compromised servers and PCs
- Attackers continue adding bots to stay ahead of blacklists
Risk Mitigation
Recommendations

Financial Services Information Sharing & Analysis Center
Layered Security Techniques

- Customer education.
- Information Sharing. Examples include FS-ISAC member submissions, alerts, Payments Risk Council, Community Institution Council.
- Customer updates about current threats.
- Up-to-date anti-malware software on customer computers.
- Desktop machines and web servers updated with security patches and anti-virus software.
- Phishing email monitoring and take down services.
Layered Security continued...

- Multifactor authentication systems.
- Encryption.
- IP/URL filtering.
- Bank-hosted security software to protect online sessions/browser security.
- Systems to detect when a customer’s computer maybe compromised.
- Software to clean a customers machine of malware.
- Stand alone PCs for customers where email and web browsing functions are disabled.
- Unique hardware and browser for financial transactions.
Layered Security continued...

- Hardware tokens for PC initiated payments.
- Tokens on smart phones.
- One time PINs via SMS.
- Anomaly detection at log in.
- Anomaly detection at transaction level.
- Calling customer’s back to verify wires and ACH originated online.
- SMS and/or email alerts on all wires and ACH transactions, with or without SMS back to block.
- ACH debit block and/or positive pay type of systems for ACH.
- Wire and ACH white list systems.
Even more... layered security techniques.

• Dual control.
• Turning off unused payment services.
• Transaction limits.
• Reissue of account numbers and/or credentials.
• Systems to protect mobile applications.
• Systems to detect when mobile devices are compromised.
• Malware infections of mobile smartphones increased more than 780% from 2011 to the end of 2012
• 99% of the mobile malware available specifically targeted Android devices.
• Over 6,000 new pieces of Android malware per month in the latter half of 2012.
• The largest category of mobile malware in 2012 was SMS Trojans masquerading as legitimate apps. All were designed to target bank accounts.
Hive Intelligence: A Business Case for Information Sharing

Financial Services Information Sharing & Analysis Center
What is Hive Intelligence?

• In nature, individuals act for the good of the group
• Hive intelligence sharing is the notion of bringing together a community of shared interests (the hive), to test, perfect, replicate and transfer knowledge
• Cohesion and complex cooperation requires tight communications, a command and control system and a common objective
What is Hive Intelligence?

• It is the result of the synergies among data-information-knowledge; software-hardware; and experts (those with new insights as well as recognized authorities) that continually learns from feedback to produce just-in-time knowledge for better decisions than these three elements acting alone.

• The threat continues to grow and expand. Sharing of intel between attacking groups is common.

• Budgets of defenders are tight; especially personnel budgets.
Hive Intelligence in Action

- **AI-Qassam Cyber Fighters** – Coordinated attacks against FIs beginning 09/12 and continuing to this day.
- Characterized by highly sophisticated attacks; multiple targets, and adaptability to defensive measures.
- Collective Intelligence supplied by FS-ISAC members single most effective tool in FIs’ defensive arsenal.
- **ROI:** Intelligence capability expanded 20 fold for each FI, at ZERO cost.
Hive Intelligence in Action

Intelligence sharing included:

✓ Early Warning
✓ Technical insights into types of attacks and success/failure of attacks based on defensive measures used by others
✓ Collective expertise of vendors, government as well as FI SMEs
✓ No attribution
✓ A sense of community and not having to go it alone
About FS-ISAC

- A nonprofit private sector initiative formed in 1999
- Designed/developed/owned by financial services industry
- Mitigating some of largest recent cyber threats & fraud activity
- 240,000 threat indicators shared, adding thousands each month
- Year over year double digit membership growth
- Now enabled to share information globally
FS-ISAC 24/7 Security Operations Center

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

Government Sources
- iSIGHT InfoSec
- NC4 PhySec Incidents
- MSA PhySec Analysis

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

Private Sources

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

Alerts

Member Submissions
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.
Going beyond Layered Defense

Defense in Depth vs. Active Defense
Changing the Economics, Cyber Defense Symmetry

Advantage: Attackers

Cost to Attack

Advantage: Defenders

Cost to Defend

Current State of Cyber-Symmetry
(Rogues can play)

Future State of Cyber-Symmetry
(Only nation-states can play)

Policy Effectiveness

Cyber Warfare Symmetry
Microsoft Botnet Takedown

Financial Services Information Sharing & Analysis Center
Citadel, on its own is concerning enough. Maor says the cyber rings that provide and sell Citadel are extremely organized and sophisticated. "It's a technical, advanced Trojan," he says. "You have a Citadel group or community that offers technical support for the fraudsters and information about new versions of the Trojan. ... They offer a knowledge database, where you can ask questions."  Etay Maor, RSA Security
Microsoft, FBI Take Down Citadel Botnets

Malware Blamed for $500 Million in Fraud Losses Worldwide

By Tracy Kitten, June 6, 2013. Follow Tracy @FraudBlogger

Federal authorities, along with the Microsoft Digital Crimes Unit, the Financial Services Information Sharing and Analysis Center and other private-sector partners, say they have shut down more than 1,400 botnets responsible for spreading the Citadel malware that compromises online credentials and identities.

According to a June 5 blog posted by Microsoft, this takedown known as Operation b54 was the most aggressive botnet operation to date, and also involved assistance from the American Bankers Association, NACHA - The Electronic Payments Association, Agari, A10 Networks and Nominum.

"With a court ordered civil seizure warrant from the U.S. District Court for the Western District of North Carolina, Microsoft executed a simultaneous operation to disrupt more than 1,400 Citadel botnets which are responsible for over..."
Microsoft’s Citadel Takedown

- Citadel is a crime kit, filling the void after the Zeus botnet was weakened by prior actions.
- Microsoft is worked to take control of many of the C2 servers.
- Machines with Citadel malware received software to remove a file that blocks access to AV services.
- Machines without AV services…MS pushed an interstitial page to compromised computers urging the owner to go to a MS security patch site.
Microsoft Operation B54

• Microsoft obtained a restraining order before the U.S. District Court (Charlotte) on May 29, 2013

• Seizures were executed on June 6
  – Domain seizures - sever command and control structures of the Citadel malware by cutting off communications to nearly 1,500 Citadel botnets
  – Server seizures – servers obtained by Federal Law Enforcement in NJ and PA

• Microsoft working closely with FBI on Operation B54 to coordinate the civil and criminal actions

• ABA, FS-ISAC, and NACHA are Declarants in this case
Results (as of July 23, 2013)

• Approximately 3,500 domains were being used by Citadel for Command & Control of victim computers

• As a result of the court order, 82% of the Citadel botnet has been disrupted
  ✓ 2,340 domains are now redirected to the Microsoft owned sinkhole (67% of domains)
    ▪ 40% of these systems have been cleaned by MSRT (Microsoft’s Malicious Software Removal Tool)
  ✓ 138 domains sinkholed by CERT (3.97%)
  ✓ 393 domains disabled by Country Registries (11.25%)
  ✓ 621 domains NOT under control (17.78%)

• Dell SecureWorks noted a 90% reduction in observed Citadel C&C traffic
What’s Next?

Financial Services Information Sharing & Analysis Center
“Disruption is the Pathway to Destruction”

Art Coviello, Executive Chairman, RSA

Financial Services Information Sharing & Analysis Center
Evolution from Disruptive to Destructive Attacks

Advanced DDOS – 2012, 2013
• 40+ FIs targeted
• Resulted in dynamic, effective information sharing
• Wake up call for financial services industry

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 targeted
• Patch systems targeted
• Wipers hit Windows, Linux and UNIX OS and removed file systems. Over 3,000 machines made unbootable
Contact Information:

Bill Nelson, President & CEO  
bnelson@fsisac.us
Eric Guerrino, EVP Operations  
eguerrino@fsisac.us
Denise Anderson, VP Gov’t and C/S Programs  
danderson@fsisac.us
Robin Fantin, VP Marketing  
rfantin@fsisac.us
Rick Lacafta, Director of Insurance Services  
rlacafta@fsisac.us
Charles Bretz, Payments Risk Director  
cbretz@fsisac.us
Beth Hubbard, Director of Member Services  
bhubbard@fsisac.us
Alan Stockey, Director EU  
astockey@fsisac.eu
Craigg Ballance, Director Canada  
cballance@fsisac.ca

www.fsisac.com