Organized Cyber Crime and Bank Account Takeovers

Fred Bailard, Executive Vice President, Presidio Bank

Brian Busony, Assistant to the Special Agent in Charge, US Secret Service

Gene Lilienthal, Senior Examiner, Federal Reserve Bank Of San Francisco

March 14, 2013
Topics For Today

- Why Should Banks Be Concerned About Cyber Crime
  - What Tactics Are Used
  - What Is The Cost
  - Mobile Device Threat

- Who Are We Fighting & What Is Their Motivation

- What Can We Do To Fight This Threat
Why Should Banks Be Concerned About Cyber Crime

• In 2012, terms like “fiscal cliff” and “regulatory burden” became part of the bank lexicon. With the increasing threat of cyber attacks 2013 may see terms like “Project Blitzkrieg,” “Mobile Attacks”, “Blackhole” and “Shamoom” added to the vernacular—and to the list of top priorities.

• Fraudsters, hackers and cybercriminals are improving their methods for account takeover and compromised identities that target a Banks’ customers and employees.

• Unique strains of malware topped 100 million in 2012, and the growth continues at an accelerated pace. Financial institutions must protect themselves and their customers with a layered approach to online fraud mitigation, without degrading the online experience for the customer.

• Symantec placed the cost of IP theft to U. S. companies at $250 billion a year, global cybercrime at $114 billion annually ($388 billion when you factor in downtime), and McAfee estimates that $1 trillion was spent globally under remediation.

• Protection from financial loss to both our clients and the bank, the cost of reputational harm, risk from social media and legal actions against the bank.
  • 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.

• There is a heighten value in knowing the emerging threats to watch for that may help all of us prepare our cybercrime prevention strategies and tactics and at a minimum adhere to FFIEC authentication guidance.
The Threat

ACCOUNT TAKEOVERS GROWING >150% PER YEAR

MOBILE BANKING USERS

ONLINE BANKING USERS

MALWARE

2006 2007 2008 2009 2010 2011 2012
Let’s Look At The Tactics Used

While there are many types of attacks for the purposes of this presentation we will focus on the most common types of threats for 2013.

**Mobile fraud**
Because clients can now carry out financial transactions on many mobiles, their phone/tablet is vulnerable to the same types of scams as their computer.

**Phishing scams**
Phishing scams use emails, pop-ups or messages that look as if they come from trustworthy organizations to trick our clients out of information such as passwords and credit card details.

**Malware**
Malware is malicious software and is a common name for all kinds of unwanted software such as viruses, worms and Trojans that could harm one’s files and programs.

**Distributed denial of service**
This is a denial of service attack in which the perpetrators are more than one in number and geographically displaced. It is very difficult to control such attacks.

**Money mule scams**
Money mule scams use clever ways to trick individuals into letting the scammers use your accounts for illegal money transactions. The scammers usually have a reason why they can’t pay their own money – gained using illegal methods – into their accounts and ask to pay it into the individual’s instead. The individual then withdraws it and sends it overseas using a wire service for a commission. Then if they get caught, it is the individual who becomes traceable and accountable, not the real criminal.

**Social networking risks**
Social networking sites can be a target for criminals on the lookout for people’s personal details, which they can then use to commit fraud.

**Identity theft**
Identity theft happens when someone uses your personal information to pretend to be you.
Primary goals of targeted cyber attacks on companies in 2012, by country (in U.S. dollars)

This statistic provides information on the main objectives of cyber criminals who target companies through cyber attacks, as perceived by global respondents (business leaders and IT security practitioners). In 2012, 70 percent of survey respondents in the United States considered financial fraud to be the primary goal of cyber criminals targeting their businesses.

Source: Ponemon Institute
Source: Hackmageddon.com
What Is The Cost
Financial damage caused by cyber attacks in the U.S. in 2012

Worldwide

Average cost of a successful cyber attack for a U.S. company in 2012, by amount of damage (in U.S. dollars)

<table>
<thead>
<tr>
<th>Damage Category</th>
<th>Share of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 10,000</td>
<td>2.00</td>
</tr>
<tr>
<td>10,000 to 50,000</td>
<td>9.00</td>
</tr>
<tr>
<td>50,001 to 100,000</td>
<td>10.00</td>
</tr>
<tr>
<td>100,001 to 200,000</td>
<td>13.00</td>
</tr>
<tr>
<td>200,001 to 300,000</td>
<td>30.00</td>
</tr>
<tr>
<td>300,001 to 400,000</td>
<td>22.00</td>
</tr>
<tr>
<td>400,001 to 500,000</td>
<td>7.00</td>
</tr>
<tr>
<td>500,001 to 1 million</td>
<td>4.00</td>
</tr>
<tr>
<td>More than 1 million</td>
<td>3.00</td>
</tr>
</tbody>
</table>

This statistic shows the estimated damage a successful cyber attack will cost a U.S. business. In 2012, only 2 percent of respondents believed a single successful cyber attack would cost their company less than 10,000 U.S. dollars whereas 30 percent thought their losses to be about 200,001 to 300,000 U.S. dollars.

Source: Ponemon Institute
This statistic gives information on the percentage of annualized cybercrime cost of U.S. companies in 2012, by type of attack. During that year, 26 percent of costs caused by cybercrime were due to malicious code.
Mobile Threat

With online technology rapidly moving from computers to the palms of our hands, cybercriminals and hackers are evolving their methods to fit the times. Whether it's the new Windows 8 OS or the trendy HTML5 browser language, cybercriminals will be stepping up their game in 2013 to capitalize on the newest technology.

Mobile banking and m-commerce have gained massive global traction over the past three years, with almost 600M people expected to use mobile banking services in 2013, up from 185M in 2011. With so many devices from smartphones to tablets to PCs, so many transactions and growing consumer demand for mobile banking, it's easy to understand why this is a major focus for banks.
The Global Tablet Market Grows 78% in 2012

Global shipments of smart connected devices in 2011 and 2012 (in million units)

- **Smartphone**: 494.5 million in 2011, 722.4 million in 2012 (+48%)
- **Tablet**: 72.0 million in 2011, 128.3 million in 2012 (+78%)
- **Portable PC**: 209.1 million in 2011, 202.0 million in 2012 (-3%)
- **Desktop PC**: 154.8 million in 2011, 148.4 million in 2012 (-4%)

Source: IDC
User Behavior

RISKY BEHAVIOR ON POTENTIALLY UNSECURE WI-FI

- 67% ACCESS PERSONAL E-MAIL
- 63% ACCESS THEIR SOCIAL NETWORK ACCOUNT
- 31% SHOP ONLINE
- 24% ACCESS THEIR BANK ACCOUNT
## Mobile Device Phishing Risk Evaluation

<table>
<thead>
<tr>
<th>Legitimate Behavior</th>
<th>Prevalence</th>
<th>Attack Technique</th>
<th>Accuracy</th>
</tr>
</thead>
</table>
| **Mobile Sender > Mobile Target**  
Social sharing, upgrades, game credits  
Social sharing, upgrades, game credits  
Social sharing, upgrades, game credits | Very Common  
Very Common  
Very Common | Fake mobile login screen  
Task interception  
Scheme squatting | Perfect  
Perfect  
Low |
| **Mobile Sender > Web Target**  
Embedded login pages  
Opening a target in the browser  
Opening a target in the browser  
Opening a target in the browser  
Embedded HTTP page links to HTTPS login  
App sends user to HTTP page in browser that links to HTTPS login | Common  
Very Uncommon  
Very Uncommon  
Very Uncommon  
Very Uncommon  
Uncommon | Keylogging  
URL bar hiding  
URL bar Spoofing  
Fake browser  
Active network attack  
Active network attack | Perfect  
High  
High  
Perfect  
High |
| **Web Sender > Mobile Target**  
Link to mobile e-mail or Twitter Web site  
Link to mobile e-mail or Twitter  
Link to mobile e-mail or Twitter | Common  
Common  
Common | Spoofs mobile app  
Task interception  
Scheme squatting | High  
Perfect  
Low |
| **Web Sender > Web Target**  
Payment via PayPal or Google Checkout  
Payment via PayPal or Google Checkout  
User follows link from HTTP to HTTPS | Common  
Common  
Very Common | Hide the URL bar  
Spoof the URL bar  
Active network attack + URL bar spoofing | High  
High  
High |

We match each attack technique with the legitimate behavior that it subverts, along with how common the legitimate behavior is. The most effective attacks mimic common behavior with perfect accuracy. “Perfect” accuracy means the user cannot distinguish the attack from the original, and “high” accuracy means the user can only identify the attack by doing something unusual.

Source: Adrienne Porter Felt and David Wagner from the University of California, Berkeley
Sample Scenario

Capturing your messages and your bank account

We have begun to see Android malware that eavesdrops on incoming SMS messages and forwards them to another SMS number or server. This sort of data leakage represents a significant risk, both to individuals and to organizations.

The potential exists for attacks like these to target Internet banking services that send mobile transaction authentication numbers via SMS. Many banks send authentication codes to your phone via SMS each time you do an online transaction. This means that just stealing a login password is no longer enough for criminals to raid your account. But malware on your phone, such as the Zeus-based Andr/Zitmo (and similar versions targeting BlackBerry) are capable of intercepting those SMS messages.

Consider the following hypothetical scenario. Through a conventional phishing attack, a victim gives criminals sufficient information to allow them to sign in to your mobile banking account and also port your phone number (this has happened). They can now log in to your online bank account while also receiving an SMS containing the second-factor authentication token needed to complete a transaction.

Through the use of a malicious Android app that harvests SMS messages in real time and in concert with a social engineering attack, attackers open a brief window of opportunity to steal this token and use it before you can stop them.
Who Are We Fighting & What Is Their Motivation

These criminals are building businesses based on the development, management, and sale of malicious services.

These criminal groups:

• Have programmers who write the malicious software

• Salespeople who sell the code or lease out their services and,

• In some instances provide dedicated support personnel.
Examples – Internet Black Market Pricing Guide

• **Exploit code for known flaw** - $100-$500 if no exploit code exists
  – Price drops to $0 after exploit code is “public”

• **Exploit code for unknown flaw** - $1000-$5000
  – Buyers include iDefense, Russian Mafia, and some Governments, etc.

• **List of 5,000 IP addresses of computers infected with spyware/trojans for remote control** - $300-$1,000

• **List of 1,000 working credit card numbers** - $1,000-$10,000

• **Annual salary of a top-end skilled black hat hacker working for spammers** - $200K-$400K
Sample Cyber Crime AD Site

<table>
<thead>
<tr>
<th>Type</th>
<th>Europe</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe Visa Classic</td>
<td>$90</td>
<td>$30</td>
</tr>
<tr>
<td>Europe Master Card</td>
<td>$90</td>
<td>$30</td>
</tr>
<tr>
<td>Europe Visa Gold</td>
<td>$125</td>
<td></td>
</tr>
<tr>
<td>Europe Visa Business/Corporate/Purchasing</td>
<td>$185</td>
<td></td>
</tr>
<tr>
<td>Europe Visa Platinum</td>
<td>$190</td>
<td></td>
</tr>
<tr>
<td>Europe Visa Classics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switzerland, France, Turkey</td>
<td>$100</td>
<td></td>
</tr>
<tr>
<td>Europe Visa Gold, Switzerland, France, Turkey</td>
<td>$195</td>
<td></td>
</tr>
<tr>
<td>USA Visa Classic</td>
<td>$38</td>
<td></td>
</tr>
<tr>
<td>USA Master Card</td>
<td>$38</td>
<td></td>
</tr>
<tr>
<td>USA Visa Gold, Platinum</td>
<td>$46</td>
<td></td>
</tr>
<tr>
<td>USA Visa Business, Corporate, Purchasing</td>
<td>$49</td>
<td></td>
</tr>
<tr>
<td>AmEx</td>
<td>$38</td>
<td></td>
</tr>
<tr>
<td>Discover</td>
<td>$42</td>
<td></td>
</tr>
<tr>
<td>Diners, JCB</td>
<td>$50</td>
<td></td>
</tr>
</tbody>
</table>

In stock dumps from EU and USA.

All types of dumps, also all countries from all world. When you do order you can get fast consultation about best working bins in your region.
Payment via Webmoney, e-gold, WU.
Min order for WM and e-gold is $200
Min order for WU is $200

Quality and size of "exhaust" dumps, at an optimum choice of the country dumps, concerning the country of use on grows many.
Sample Cyber Crime AD Site
Sample Cyber Crime AD Site
What Can We Do To Fight This Threat
Key Considerations

Security is evolving from a device-centric to a user-centric view, and the security requirements are many. A modern security strategy must focus on all the key components — enforcement of use policies, data encryption, secure access to corporate networks, productivity and content filtering, vulnerability and patch management, and of course threat and malware protection.

An Effective and Sustainable Online Banking Fraud Prevention Strategy Should Include:

1. Development of a sound strategy that addresses online and mobile risks

2. A layered security approach using some or all of these elements

   • Multi-Factor out of Band
   • Behavioral Analytics and Transactional Anomaly Detection
   • Data Encryption
   • VPN Tunneling
   • Keyboard Encryption
   • Harden Shell Browser and Operating System
   • Anti-Virus Software
   • Strong Password Configuration

3. Minimize User Impact

4. Communication and Education

   • Customers
   • Employees

5. Proven Security Partner(s)
Sample Security Client Bulletin

Our bank has sent out the email below regarding the recent serious Java problem. I am forwarding to the whole team in the hope it is helpful in ensuring you minimize the risk to your computer…..hope it is helpful.

From: Presidio Bank - Client Service <PresidioBankClientService@presidiobank.com>
Subject: IMPORTANT: Java Update
Date: January 14, 2013 12:41:51 PM PST

*******************************PLEASE DO NOT REPLY TO THIS EMAIL*******************************

Dear eBanking and RCD Clients:

Security Information Bulletin

Oracle has released an emergency software update to fix a security vulnerability recently discovered in Java 7. The security bulletin which describes the vulnerability can be found at: http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html

We recommend that our clients upgrade to the latest version of Java (Java 7u11), which incorporates the fix for the vulnerability. The release notes for Oracle’s Java 7u11 release can be found at: http://www.oracle.com/technetwork/java/javase/7u11-relnotes-1896856.html

The easiest way to update Java is to visit www.java.com and
1. Click the “Do I have Java?” link.
2. Click the “Verify Java version” button.
3. If you don’t have the latest version the site will inform you that a newer version of Java is available, and you should click the “Download Java Now” button to begin the installation of the latest version.

If this information impacts anyone else in your company or at home, please forward a copy of this email to them.

Sincerely,

Presidio Bank
Cash Management Department
Employee activities that pose the greatest risk for cyber attacks

United States

This statistic provides information on the seven employee activities that were said to pose the greatest risk for facilitating cyber attacks on U.S. companies. The amount of risk was measured on a scale from one to seven, with seven representing the highest risk. On average, the use of mobile devices was seen as the riskiest employee activity with U.S. respondents giving this a 6.3 rating on the index scale.
Resources

Mcafee Threat Predictions – 2013

Norton Cyber Crime Report - 2012

Sophos Security Threat Report

Global Knowledge – Top Ten Cybersecurity Risks

Infosecurity: RSA 2013: Security is not keeping pace with threats

F-Secure – Threat Report

IronKey – When ‘Secure Enough’ Isn’t Enough

Ponemon Institute – 2012 Cost of Cyber Crime in the United States

Measuring the cost of cybercrime
Questions?

Fred Bailard
EVP
Presidio Bank
415-229-8402
fbailard@presidiobank.com
Secret Service Dual Mission

Protection
- President
- Vice-President
- Former Presidents
- Candidates for POTUS
- Foreign Heads of State
- Others by appointment

Investigations
- Cyber Crimes
  - Hacking
  - Computer / Internet Fraud
  - Data Breaches
- Counterfeit
  - Currency
  - Treasury Obligations
- Financial Crimes
  - Identity Crime
  - Check Fraud
  - Access Device Fraud
  - Bank Fraud
  - Mortgage Fraud
Secret Service Resources

- 142 Domestic Offices
- 24 Foreign Offices
- 3,500 Special Agents
- 1,400 Uniformed Division Officers
- 2,000 technical, professional and support personnel
Secret Service Resources to Investigate Cyber / Financial Crimes

- Electronic Crimes Special Agent Program (ECSAP)
- Electronic Crimes Task Forces (ECTF) - 31
- Financial Crimes Task Forces (FCTF) - 38
- Cell Phone Forensic Facility – Tulsa, OK
- National Computer Forensic Institute (NCFI) – Hoover, AL
- Computer Emergency Response Team (CERT)
- DOJ/CCIPS(Computer Crimes and Intellectual Property Section)
Secret Service

Tulsa Initiative

- Partnership with the University of Tulsa, Digital Forensic Center of Information Security
- Expands the forensic capabilities of law enforcement regarding cellular telephones, smart phones and other mobile computing devices
- Tulsa supplies interns who specialize in information technology / digital forensics
The mission of the National Computer Forensic Institute (NCFI) is to provide state and local law enforcement, prosecutors and judicial officials a national standard of training in electronic crimes investigations, network intrusion response, computer forensics and high tech crime prosecution.
Advanced forensic facility in Pittsburgh, PA
- Carnegie Mellon University (Collaborative Innovation Center)
- Provide investigative support to field offices
- Conduct basic and applied research
- Coordinate training opportunities between CERT and the Secret Service
- Access to over 150 scientists, researchers, and technical experts in the field of computer security
Electronic Crimes Task Forces

Not listed: London, England
Rome, Italy
Electronic Crimes Task Force Initiative

A Different Law Enforcement Model for the Information Age
The Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.
Goals of an Electronic Crimes Task Force

- Establish a strategic alliance of federal, state and local law enforcement agencies, private sector technical experts, prosecutors, academic institutions and private industry.

- To confront and suppress technology-based criminal activity that endangers the integrity of our nation’s financial payments systems and poses threats against our nation’s critical infrastructure.
Electronic Crimes Task Force

Three principles of a successful Electronic Crime Task Force:

- Prevention/Response/Resiliency
- Trusted Partnerships
- Criminal Investigations
Prevention

- The guiding principle of the Electronic Crime Task Force’s approach to both our protective and investigative missions is our “focus on prevention”.
- “Harden the target” through preparation, education, training and information sharing.
- Proper development of business policies and procedures before the incident.
Response & Resiliency

- Strong documentation and reporting practices starting at the beginning of the incident.
- Internal computer forensics and log analysis.
- Technical briefings for law enforcement during the entire course of the investigation.
- Contingency planning to bring operations back online.
Trusted Partnerships

- Ongoing Task Force liaison with the business community.
- Business community provides technical expertise and assistance to law enforcement in the rapidly changing technology world.
- Development of business continuity plan, risk management assessment and return on investment.
- Task Force provides “real time” information on issues whenever possible.
- Table Top exercises with private industry and government.
Criminal Investigations

- Liaison and instructions to victims
- Early law enforcement involvement is critical
- “Solve the problem”
- Follow up and ongoing dialogue with the victim
“Cyber Intelligence Section”
United States Secret Service (CIS)

- Analysis & Exploitation Unit
- Cyber Threat Unit
- Investigations Group
  - Belgium
  - Latvia
- Transnational Groups
  - Ukraine
- Operations Group
  - Netherlands
  - Lithuania
  - UK
Cyber Threat Unit

Investigative Group – responsible for investigating large scale data breaches or other major cyber related cases.

Operations Group – responsible for conducting proactive undercover investigations against major cyber criminals and organized groups.

Transnational Group – Temporary Duty Assignments around the world to liaison and actively work with foreign law enforcement entities.
Cyber Intelligence Section

- Databases of over 15 years worth of cyber evidence:
  - Seized media
  - E-mail search warrants
  - Images of criminal forums/sites
  - Data from when experienced criminals were new

- Combination of agents and analysts.

- Liaison with cyber components of domestic and foreign agencies:
  - US law enforcement and intelligence
  - Foreign law enforcement
  - Private sector research
Questions?
Brian Busony
Assistant to the Special Agent in Charge
San Francisco Field Office
Electronic Crimes Task Force
415/273-8504
Brian.Busony@ussd.dhs.gov
Takeaways

• Build relationships for threat awareness with staff, executives, service providers, your board of directors, customers, peers, professional organizations, law enforcement and regulators
• Follow regulatory guidance
• Perform ongoing risk assessments including service providers for account takeover, DDoS and other threats
• Use layered controls for anomaly detection and monitoring
• Test capabilities and report to senior management and board
• All institutions can be threatened by distributed denial of service attacks
• Law enforcement has great capabilities at their disposal
Resources

• Some resources:
Some Account Takeover Resources

- More Resources on account takeover:
  - FFIEC Guidance (and Supplement) Authentication in an Internet Banking Environment
  - FFIEC Information Security Booklet
  - FFIEC Guidance on GLBA 501(b) and Incident Response
  - FFIEC Outsourcing Technology Services Booklet
  - Texas Bankers Electronic Crimes Task Force: Best Practices Reducing the Risk of Corporate Account Takeover
  - Verizon Data Breach Investigations Report
Some DDoS Resources

- Resources on distributed denial of service:
  - FFIEC Guidance BCP Booklet
  - FFIEC Outsourcing Technology Services Booklet
  - Gartner - Arming Financial and E-Commerce Services Against Top 2013 Cyberthreats
  - Bankinfosec.com list of denial of service resources
    http://www.bankinfosecurity.com/search.php?search_keyword=denial+of+service