Cyber Fraud, Account Take-over, Man-in-the-Middle, Cross-channel fraud – How Can You Keep Ahead of the Criminals?

George Tubin  
Security Strategist  
Trueteer

Jason Berryhill  
Special Agent  
Secret Service

Jim Maimone, CTP  
SVP Payables & Receivables  
Santander Bank, NA
Today’s Agenda

Tools of the Cyber Criminals
George Tubin
Security Strategist, Trusteer

Trends in Financial Crime
Jason Berryhill
Special Agent, Secret Service

Best Practices for Your Company
Jim Maimone, CTP
SVP Payables & Receivables
Santander Bank, NA

Q&A
Malware & Phishing
Definition of Key Terms

- **Phishing**
  - Email that uses social engineering to trick recipient into taking some type of harmful action

- **Malware**
  - A variety of malicious software designed to gain access to computers, steal data, and evade detection

- **Man-in-the-Browser (MitB)**
  - A form of malware that essentially takes control of the web browser

- **Man-in-the-Middle (MitM)**
  - A form of cyber-attack where an intermediary can intercept and alter all web communication

- **Malvertising**
  - The use of online advertising to spread malware when inserted into high-profile reputable websites can "push" exploits to web users
Three Lost Battles:
Why we can’t eliminate fraud once and for all

- System vulnerabilities continue to emerge
- Malware bypasses security controls
- Humans will make mistakes


SHA256: 869579dd3b038f9f2ca6b04e250698d6a0d31716e49c1fed0b149ee250c56e
File name: file-2344493_sawt
Detection ratio: 2 / 42
Analysis date: 2011-06-01 23:02:18 UTC (1 year, 2 months ago)
Cyber-Fraud in Financial Services

Fraud from Customer Device

Criminal

Cross Channel Fraud

Fraud from Criminal Device

ATO

TRX

Online Banking

Customer

WWW

Credentials, Data

Attack
The Root Cause of Most Fraud: 
Man-In-The-Browser Malware and Phishing

MitB is the biggest risk...

... which is why regulators are focused on the problem

"Controls implemented in conformance with the Guidance several years ago have become less effective."

"Malware can compromise some of the most robust online authentication techniques"

"banks need to take precautions assuming all PCs are infected with Zeus"

Source: McKinsey & Company

AFP® Annual Conference
Anatomy of Malware Attack

User Target → Social Engineering

System Exploit → Web / OS Vulnerability

Malware Infection → Code Install

Fraud Scheme Execution → Web Injection, Capture Credentials

Money Loss → Mule Transfers, Real-time Fraud
MitB Malware: Anything Goes

PII Theft

Credentials Theft

Social Engineering

AFP Annual Conference
How Effective Are Anti-Virus Applications?

65% of machines infected with Zeus have an installed anti-virus product

- 55% infected with AntiVirus Up-to-date
- 10% infected with AntiVirus outdated
- 35% No Antivirus Found
- 10% Antivirus Found but not Up-to-Date
How Trusteer Rapport Detects Financial Malware

Trusteer: What it does?
Crime Logic (100s)

- Exploit
- Infect
- Hook
- Inject
- Access
- Theft

Legacy: What it is?
Files and Signatures (1000000s)
Real Life Malware Examples
Cybercriminals: The Perfect Storm

- **Nation-State Cyberwarfare**
  - Intensive training programs
  - Meager pensions

- **Organized Crime**
  - Highly advanced underground economy
  - Programmers “forced” to collaborate
Vulnerabilities Are NOT Going Away

- **2013 0-days (critical)**
  - Java – Jan 10, Jan 16
  - Adobe Flash, two – Feb 7
  - Microsoft “Megapatch” – Feb 12
  - Google Chrome – March 11
  - Chrome OS – April 13
  - IE 8 – May 6

- **And, Breaches on the Rise**
  - Operation Red October
  - NYT, WSJ, Washington Post
  - Federal Reserve
  - Twitter, Facebook, Microsoft
  - Bit9!
Malvertising: Surf the Web, Get Infected

- From “Malicious Advertising”: the use of online advertising to spread malware.
  - Inserted into high-profile reputable websites
  - Can "push" exploits to web users

- Recent Campaign
  - Several ad networks hosting campaigns, including: Clicksor, linkbucks.com, Hooqy Media Advertiser, and traff.co
  - Blackhole Exploit Kit targeting Java 0-day vulnerability
You Can’t Even Trust Twitter!

Twitter Malware: Spreading More Than Just Tweets

```javascript
function _PostTweet()
{
    var a = $('input[name="authenticity_token"]').val();
    a.length > 0 && $.post("/i/tweet/create", {
        authenticity_token: a,
        place_id: "",
        status: _GetRndMsg()
    }).always(function () {
        ar[0].msgsent = 1, SetO(), window.location.href = window.location.href
    });
}
```

The Associated Press

"Breaking: Two Explosions in the White House and Barack Obama is injured"

12:07 PM - 23 Apr 13

AFP® Annual Conference
Cross-Channel Check Fraud

- Malware captures check images in a compromised account
- Counterfeit checks are created using specialized paper and ink
- Counterfeit checks are typically presented in retail stores

I can do $5 dollar per cheque if you provide your own account numbers. If you need bank accounts it will be $50 per working /tested /verified accounts

Login correct into BK account and act as it will be your own account always verify the transfer history if it is available. Try to keep the transfer in balance with the owner history

AFP® Annual Conference
TRENDS IN FINANCIAL CRIME

Presented by

Special Agent
Jason Berryhill
THE U.S. SECRET SERVICE

The mission of the United States Secret Service is to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and to protect national leaders, visiting heads of state, and government designated sites to include National Special Security Events.
THE U.S. SECRET SERVICE

• What we investigate:
  – Financial Crimes / Electronic Crimes
    – Access Device Fraud, Financial Institution Fraud, Identity Theft, Computer Fraud, Bank Fraud
  – Computer Based Attacks
    – Nation’s Financial Banking and Telecommunications infrastructure
  – Counterfeiting of Obligations
    – Securities (i.e. currency) of the United States
THE U.S. SECRET SERVICE
The Future of Financial Crimes

Cyber Crime
(Investigative Mission)

PIN Pads Hacked at Michaels Stores Nationwide

Hackers attack PBS, post fake 'Tupac still alive' story

Malaysian hacker Lin Mun Poo nabbed in Brooklyn after cracking into Fed Reserve network
THE U.S. SECRET SERVICE
The Future of Financial Crimes

Cyber Crime
(Protective Mission)

Palin webmail hacker conviction upheld
More than a prank
By John Leyden • Get more from this author
Posted in Crime, 28th September 2010 11:38 GMT
Free whitepaper – The Register Guide to Enterprise Virtualization
CYBERCRIME
What exactly is it?

Any crime that involves a computer and/or a network.

The computer may have been used in the commission of a crime, serve as an electronic storage container or

It may be the target.
ACCESS DEVICE FRAUD
Emerging Techniques - Keylogger

Keylogger

MasterCard
VISA
AMERICAN EXPRESS

Internet

BANK

AFP® Annual Conference
ACCESS DEVICE FRAUD
Emerging Techniques – Memory Dump

Memory Dump

Internet

AFP® Annual Conference
ACCESS DEVICE FRAUD
Emerging Techniques – Network Sniffers
ACCESS DEVICE FRAUD

Typical Skimmers
Gas Pump Skimming
ACCESS DEVICE FRAUD
Emerging Techniques – The Prize
<table>
<thead>
<tr>
<th>Account Number</th>
<th>Credit Union</th>
<th>Approved Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>E6080353531649482</td>
<td>Los Angeles Firemen's Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>E6080353531649482</td>
<td>Los Angeles Firemen's Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>B4313020463012866</td>
<td>MSNA America Bank, N.A. Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>B4313022254012300</td>
<td>MSNA America Bank, N.A. Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>41689200000259688</td>
<td>Members Choice Credit Union Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>B4608273970417600</td>
<td>Merchants &amp; Farmers Bank Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>B4120613049223616</td>
<td>Merrick Bank Corporation Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>B4120613049900316</td>
<td>Merrick Bank Corporation Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>B4120613049343300</td>
<td>Merrick Bank Corporation Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>B4443041102869360</td>
<td>Merrill Lynch Bank and Trust Company Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>B4489031037024707</td>
<td>National City Bank Classic Union</td>
<td>Approved</td>
</tr>
<tr>
<td>B44896838056202813</td>
<td>National City Bank Classic Union</td>
<td>Approved</td>
</tr>
</tbody>
</table>
ACCESS DEVICE FRAUD
Emerging Techniques – Carding Forums
Stolen Account Numbers, What Happens Next......

- The Data is Copied/Re-encoded onto:
  - White Plastic
  - Lost/Stolen Cards
  - True Counterfeit
  - Account Numbers Utilized Through Phone or Internet transactions
Card Counterfeiting: Start to finish
ACCESS DEVICE FRAUD
Emerging Techniques – Creating Duplicate Cards
Emerging Techniques – Phishing

- PayPal: 32.06%
- eBay: 16.85%
- PayPal: 11.19%
- Chase: 10.83%
- Bank of America: 9.54%
- Ally Bank: 4.90%
- IRS: 3.99%
- HSBC: 3.69%
- NatWest: 3.69%
- Abbey: 1.63%
- Other: 1.63%
Emerging Techniques – Phishing

Key ways to Detect Phishing

1. Questionable Sender's Address
2. Sense of Urgency
3. Non-US Dating Format
4. Threat!
5. Link & URL in Status Bar Doesn't Match

AFP® Annual Conference
Emerging Techniques – Phishing With Malware
Quick Response (QR) code is a type of matrix barcode (or two-dimensional code) first designed for the automotive industry. Since its inception it has become a major marketing/advertising tool. On a smartphone, QR codes can perform changes. Risks include linking to dangerous websites with browser exploits, enabling
• Microphone
• Camera
• GPS
• Browsing Activity
• Exfiltrating sensitive data (passwords, files, contacts, transactions)
And then streaming those feeds to a remote server for data collection.
IDENTITY THEFT

Emerging Techniques – QR Codes
Unauthorized Access
Loss of Proprietary Information
Corporate Disruption
CASE STUDIES
Operation Retail Resale – Sentenced - GUILTY

Ex-staffer sentenced to 2-6 years for hacking into Gucci's system

A disgruntled ex-computer tech at Gucci’s US Headquarters in Manhattan was sentenced to anywhere from two to six years prison today for hacking into his old system two years ago and shutting down the whole operation's computers for a full day.

The high-tech hijinks of touchy techie Sam Chihlung Yin, 35, crashed the computers of the luxury goods retailer for nearly 24 hours. Yin, of Jersey City, completely wiped the email server, deleting everything in the company’s e-mail mailboxes -- in many cases permanently.

But it didn’t matter whether Yin used a keyboard instead of a weapon of violence, said his sentencing judge, Manhattan Supreme Court Justice Michael Sonberg.

"I do think that people who commit white collar crimes should be punished," the judge said.

“A white collar criminal does as much damage to society as a robber, a burglar or an assailant,” the judge said.
CASE STUDIES
Operation Retail Resale

• Network Administrator was fired from company
  – While employed created a fictitious employee
    ➢ Email account
    ➢ VPN Token (use to remote login)

• Unauthorized accessed of company network for a two (2) hour period resulted in:
  – Deletion of virtual servers
  – Shut Down a Storage Area Network
  – Deleted a disk containing corporate mailboxes from email server
  – Not only disrupted corporate email but all store managers across the U.S and
    the e-commerce sale team (resulted in $1000’s of lost sales)
OPERATION FEDERAL RESERVE

U.S. Secret Service Sting Nabs Man who Hacked into Federal Reserve Computers

By JACK CLOHERTY, PERRE THOMAS (@PerreTABC), and JASON RYAN
WASHINGTON Nov. 19, 2010

A U.S. Secret Service undercover sting has apparently netted a big fish from the ocean of computer crime.

Lin Mun Poo allegedly hacked into U.S. financial institutions and stole more than 400,000 credit and debit card numbers.

He is charged with hacking into the supposedly secure computer system at the Federal Reserve Bank of Cleveland, and penetrating servers used by defense contractors and major corporations, potentially giving him access to sensitive national security information.

All of this, while sitting at home in Malaysia. Secret Service sources describe Poo as a "big fish," an "extremely sophisticated and dangerous computer hacker."

The 32 year-old Malaysian native was arrested on October 21 in New York by the Secret Service, and is being held without bail. Authorities are still investigating the extent of the damage Poo allegedly caused.

Poo's arrest was the result of a Secret Service undercover sting, according to the criminal complaint filed in the case.
Jun 25 11:06:35 <Cl>   u hacked federal reserve
Jun 25 11:06:35 <Cl>   ?
Jun 25 11:06:44 <immunity> yeah
Jun 25 11:06:46 <immunity> windows box
Jun 25 11:06:47 <immunity> brb
Jun 25 11:06:53 <immunity> I need to boot into windows

May 04 19:26:05 <f1ex>  wow dude
May 04 19:26:10 <f1ex>  the fssecurecard is big
May 04 19:26:17 <f1ex>  department of homeland security servers
May 04 19:26:19 <f1ex>  also under them
May 04 19:26:20 <f1ex>  wtf
May 04 19:30:52 <f1ex>  http://209.235.104.117/ <-- fsv's network
May 04 19:33:04 <f1ex>  DUDE!
May 04 19:44:35 <Cl>   yeah
May 04 19:44:36 <Cl>   1 sec
May 04 19:44:38 <Cl>   checking
May 04 19:44:44 <f1ex>  dude
May 04 19:44:47 <f1ex>  they freaking
May 04 19:44:51 <f1ex>  install the shell
May 04 19:44:54 <f1ex>  for their own system
May 04 19:45:12 <f1ex>  I am going thru the logs
May 04 19:45:15 <f1ex>  of some of the servers
May 04 19:45:24 <f1ex>  this is under fssecure the network I scan
May 04 19:45:51 <Cl>   u sure?
May 04 19:46:02 <f1ex>  look at that shit dude

Jun 25 11:53:49 <immunity> have sql server running to
Jun 25 11:55:15 <immunity> federal reserve = usa gov bank right?
Jun 25 11:56:17 <Cl>   its main
Jun 25 11:56:18 <Cl>   bank
Jun 25 11:56:31 <Cl>   it might be the perfect place
CASE STUDIES
Operation Federal Reserve

Lin Mun Poo
(considered one of the top hackers of present day)

- Hacked the Federal Reserve Bank of Cleveland
- Penetrated Servers of defense contractors and other major corporations
- Penetrated Servers of FedComp, a data processor of Federal Credit Unions as well as other financial institutions and Point of Sale companies
  - Had over 400,000 Credit/Debit card numbers on his encrypted laptop
CASE STUDIES
Operation Federal Reserve

- USSS Surveillance operation observed Poo selling 30 Credit Card numbers for $1,000 upon arrival in NYC

- Poo believed he was traveling to NYC to meet up with a Credit Card Fraud Cashing ring who could withdraw cash from ATM machines
  - Example of Hackers increasing ties with organized crime rings

- During interrogation Poo admitted to “Port Scanning the Internet” looking for corporations using a particular server in order to exploit its vulnerabilities.
  - He would scan batches of IP addresses each day

- Additional evidence of other compromised corporations / servers were on his heavily encrypted laptop computer that was seized at the time of his arrest

- Sentenced to 10 years in prison by NY U.S. District Judge.
WHAT CAN WE DO FOR YOU?

- Incident Response
  - Respond to the scene to interview the victim and image the computers.

- Analysis
  - Identify how the attacker gained access and how the information was stolen.
  - Work with the US Attorney’s office for effective prosecution.
  - Pursue the arrest of the attacker(s) and seizure of assets.
Best Practices for Your Company

Case Studies

Jim Maimone
Santander
Check Fraud Knows No Boundaries

Just because you are a US-based company doesn’t mean you’re not susceptible to International Check Fraud Scams.
First assignment, you will be evaluating any Money Gram location in your area as a way of rating their competency and good customer service by doing a money transfer to the Agent assigned to you. Please follow these steps:

1. At the Money Gram fill up the Blue or Red Color Money Transfer Form which will say SEND on it, for $2,357.00 Cent plus $178 send fees for Money in 10 Minutes option.
2. Receiver’s name is: [redacted] at our branch in [redacted] State is [redacted] and country USA.
3. Upon completion of this transaction, call your account manager immediately with your receipt to confirm the transaction.
4. Complete the evaluation form at home with your honest opinion and fax it to Fax: 1-877-689-1866

Second assignment, you will take out the sum of $100.00 for shopping at one of the retail stores listed; WAL-MART, COSTCO, BESTBUY, HOME DEPOT. Etc. Items you buy are yours to keep as a bonus. Please inform us if employees are helpful to customers. Failure to complete these two assignments respectively will lead to employment termination.

Please note that it is mandatory for you to call-in upon completion of each assignment and report to your account manager and fax your evaluation and all receipts for verifications purposes. Any jobs done but not reported will be considered “NOT DONE” and you will not be sent any other assignment until further notice. Call your Account Manager to activate the enclosed payroll check before depositing in your bank account. We appreciate your confidentiality and integrity as our “Secret Shopper” representative. Complete the evaluation form at home with your honest opinion and fax it to Fax: 1-877-689-1866

Below is the breakdown on how to spend the enclosed check:

1. Your Salary.......................................................... $ 340.00
2. Survey funds to be transferred $2,357.00 + $178 send fees .......... $2,535.00
3. Fund needed for shopping...........................................$100.00
Total.................................................................................$ 2,975.00

Stores and organizations such as The Gap, Wal-Mart, Pizza Hut, and Western Union amongst many others pay our Secret Shoppers to shop in their establishments and report their experiences. On top of being paid for shopping you are also allowed to keep purchases for free. WE NEVER charge fees to the shopper. Helping to drive exceptional bottom-line performance, nearly 800,000 shoppers have registered at our website, performing millions of mystery shopping task throughout Europe and North America. With our continual investment in the latest internet and communication technologies, you can be rest assured that working with US is a satisfying and rewarding experience. It’s fun and rewarding, you are not obliged to accept this offer. There is no charge to become a shopper and you do not need previous experience. This program is run on a weekly basis.

AFP® Annual Conference
Positive Pay
International Check Fraud Scheme

Suspicious Activity
• Discovered an abnormal amount of check suspects

Called Local Authorities
• Good instincts knew it was just not right

Authorities Discovered they were a victim of an International Check Fraud Ring

Fortunately, by effectively using Positive Pay, the company experienced no loss
Control Access to All Information

The man-in-the-middle may be able to take advantage of you in your payments module

However, your account information may be just as valuable
Effective use of Dual Approval for Payments

Dual Approval Set Up for Wire Transfer
• Reviewed Wire Activity Completely

You can’t just look at the summary information
• A good practice is to review all the payment detail

Company Discovered a Wire Fraud
• Discovered that the only the Beneficiary Bank was changed

Fortunately, the approver detected the change & the company experienced no loss
How a little information can create a cross-channel nightmare

Account information was not thoroughly protected

Fraudster was able to obtain account information

Through some social engineering the fraudster was able to obtain information to originate wire transfers through a call center

Unfortunately, the company could have done a better job of securing access to critical account information to prevent the fraud
An Ounce of Prevention – ACH Debit Blocks

A Creative Employee
• Discovered they could use their payroll check’s ABA & account number to purchase goods on the Internet

Company Monitored Accounts Regularly
• Company was able to return some of the debits in time

The use of ACH Debit Protection on their Payroll Account would have been an effective tool

Unfortunately, the losses could have been prevented
Key Takeaways

• Despite the industry’s best efforts
  – Software vulnerabilities will continue
  – Malware will continue to evolve

• Advanced malware will remain difficult to prevent and detect
  – This sophisticated technology threat cannot be beaten without equally sophisticated prevention technology
  – Silver bullets do not exist

• Fraud prevention is a shared responsibility
  – Financial institutions must provide education, tools, support
  – Bank clients must know their responsibilities and take advantage of bank-provided tools
Questions?
Appendix
Speaker

Jason Berryhill
Special Agent, Secret Service
CISSP, EnCE

- Jason is a specialist in digital forensic analysis and network intrusion.

- He has been involved in electronic cases dealing with intrusions into networks, phishing attacks, malware, intellectual property theft, and more.

United States Secret Service
Electronic Crimes Task Force
(702) 868-3000
j.berryhill@usss.dhs.gov
www.secretservice.gov/ectf.shtml
George Tubin  
Senior Security Strategist, Trusteer  

- Over 18 years in the financial services industry.  
- Primarily focused on fraud and risk management strategies.  
- Trusteer is the leading provider of endpoint cybercrime prevention solutions to protect organizations against financial fraud and data breaches.
### About Trusteer

| Company | Founded in 2006  
| --- | ---  
|  | Endpoint Cybercrime Prevention  
|  | 100,000,000 Endpoints  
| Solutions | Protecting applications on any device against advanced threats and data loss  

| Application protection at a large scale | Top US Banks | Top UK Banks  
| --- | --- | ---  
| 10/20 | 9/10  
| 3/5 | 2/4  
| Top Canadian Banks | Top Australian Banks  

**AFP® Annual Conference**
Jim Maimone, CTP
SVP Payables & Receivables
Sovereign Bank, N.A.

- Over 20 years in Transactional Banking
- Responsible for product management and product development
Who is Santander?

With a high market share in 10 major markets

- **USA**
  - Mkt. Share: 10%
  - Branches: 722
  - Customers: 1.7 mill.

- **Mexico**
  - Mkt. Share: 16%
  - Branches: 1,123
  - Customers: 9.6 mill.

- **UK**
  - Mkt. Share: 12%
  - Branches: 1,266
  - Customers: 26.3 mill.

- **Poland**
  - Mkt. Share: 9%
  - Branches: 1,177
  - Customers: 5.3 mill.

- **Brazil**
  - Mkt. Share: 13%
  - Branches: 3,782
  - Customers: 26.8 mill.

- **Spain**
  - Mkt. Share: 10%
  - Branches: 4,752
  - Customers: 14.7 mill.

- **Chile**
  - Mkt. Share: 20%
  - Branches: 496
  - Customers: 3.4 mill.

- **Argentina**
  - Mkt. Share: 9%
  - Branches: 372
  - Customers: 2.5 mill.

- **Portugal**
  - Mkt. Share: 10%
  - Branches: 677
  - Customers: 2.3 mill.

- **Germany**
  - Mkt. Share: 14%
  - Branches: 304
  - Customers: 7.0 mill.

---

(1) Loans
(2) Total business, including operating announced on February 2012 regarding the merger of BZ WBK with Kredyt Bank
(3) Instalment consumer loans
(4) Including SCF business
(5) Total loans (mortgages, UPLs, and SMEs)
Disclaimer

This document was prepared by Banco Santander, S.A. ("Santander") as well as its’ subsidiaries and affiliates and is solely for informative purposes and may only be used as a working document for discussion. Santander takes no responsibility whatsoever for any consequences that could derive from its distribution or use for purposes or objectives other than for information purposes.

Our opinion expressed herein are provided solely and exclusively for the benefit of the Company, its subsidiaries and shareholders, and not for any other individual or legal entity. Consequently, this document may not be used, broadcast, quoted or used in any way with any other purpose nor may it be published or included in any document whatsoever without our prior written consent.

Santander accepts no responsibility whatsoever in relation to a possible independent verification of all or part of the information provided, which has been assumed to be correct and accurate. Consequently, no type of manifestation or guarantee, either explicit or tacit, is formulated in respect of the veracity, accuracy, comprehensiveness, sufficiency or correctness of the information provided for the opinion contained in this document and, thus, neither Santander nor any of its subsidiaries or associates, administrators, members, managers or employees assume any responsibility whatsoever for any loss or claim that might derive from any use of this document or its contents or arise in relation to this document in any other manner.
Thank you!