

AFP®



Annual Conference

OCTOBER 27-30, 2013 | LAS VEGAS

ORIGINAL → ESSENTIAL → UNBIASED → INFORMATION

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

George Tubin

Security Strategist

Trusteer

Trusteer

Jason Berryhill

Special Agent

Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Jim Maimone, CTP

SVP Payables &
Receivables

Santander Bank, NA

 **Santander**

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

Trusteer

Definition of Key Terms

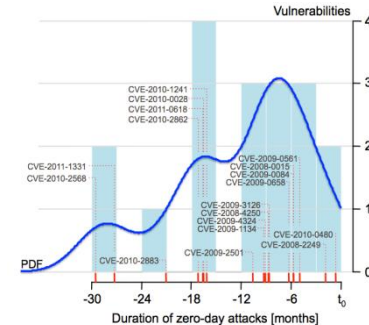
- **Phishing**
 - Email that uses social engineering to trick recipient into taking some type of harmful action
- **Malware**
 - A variety of malicious software designed to gain access to computers, steal data, and evade detection
- **Man-in-the-Browser (MitB)**
 - A form of malware that essentially 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



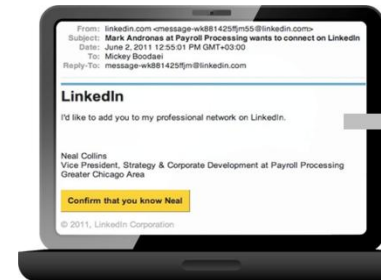
Malware bypasses security controls



SHA256: 869579adb68399f2cad684e49dfed0b149ee250c58e
File name: file-2324493_swat
Detection ratio: 2 / 42
Analysis date: 2011-06-01 23:02:18 UTC (1 year, 2 months ago)



Humans will make mistakes



Blackhole

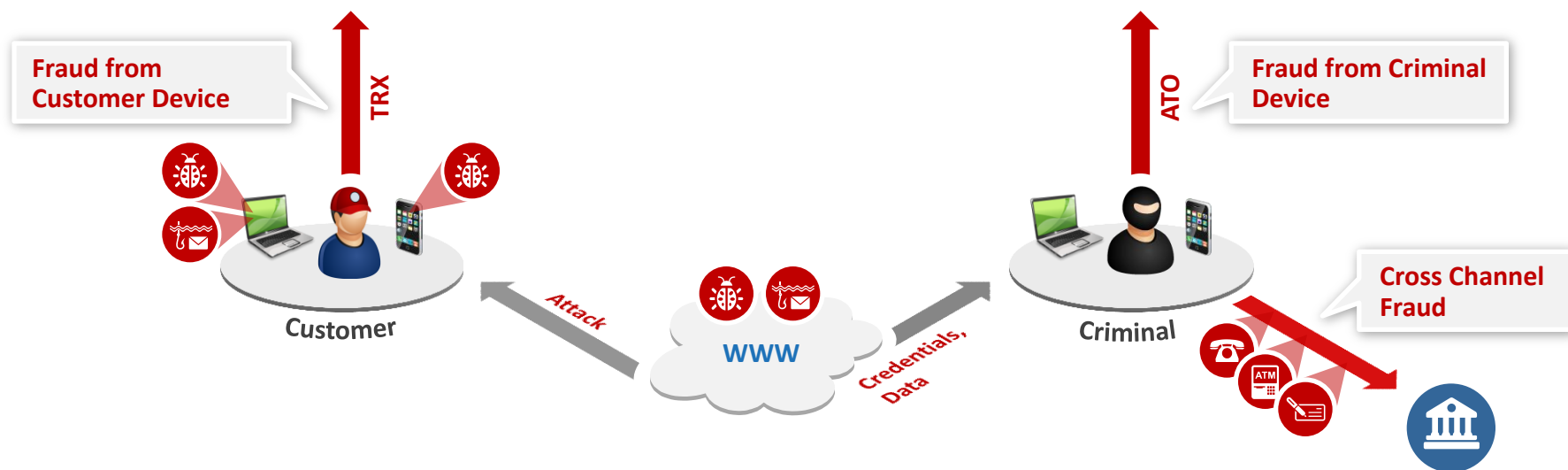


Zeus

Cyber-Fraud in Financial Services

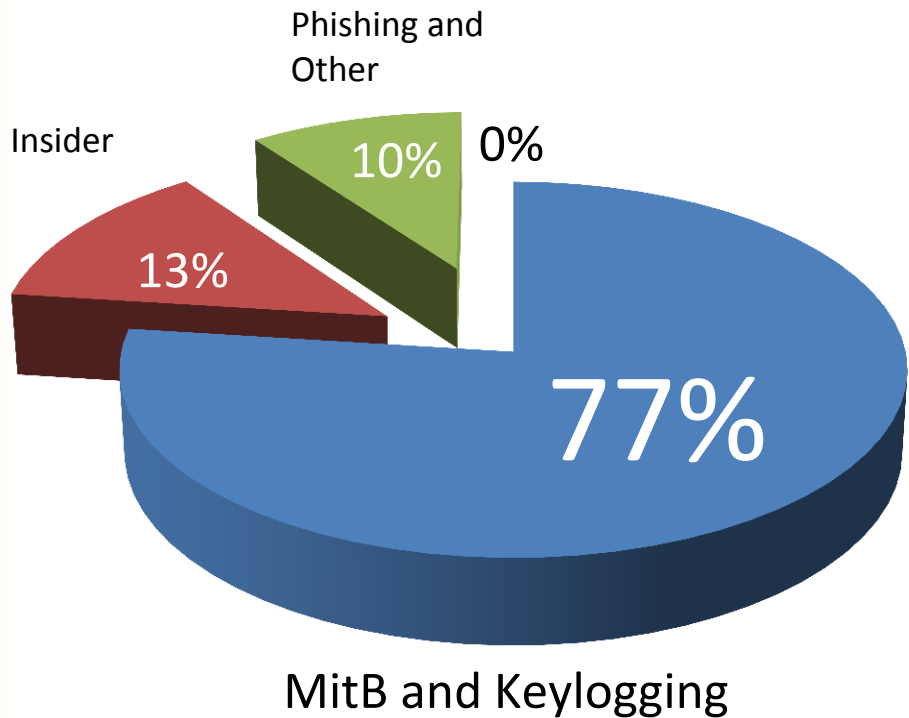


Online Banking



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

MitB is the biggest risk...



Source: McKinsey&Company

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

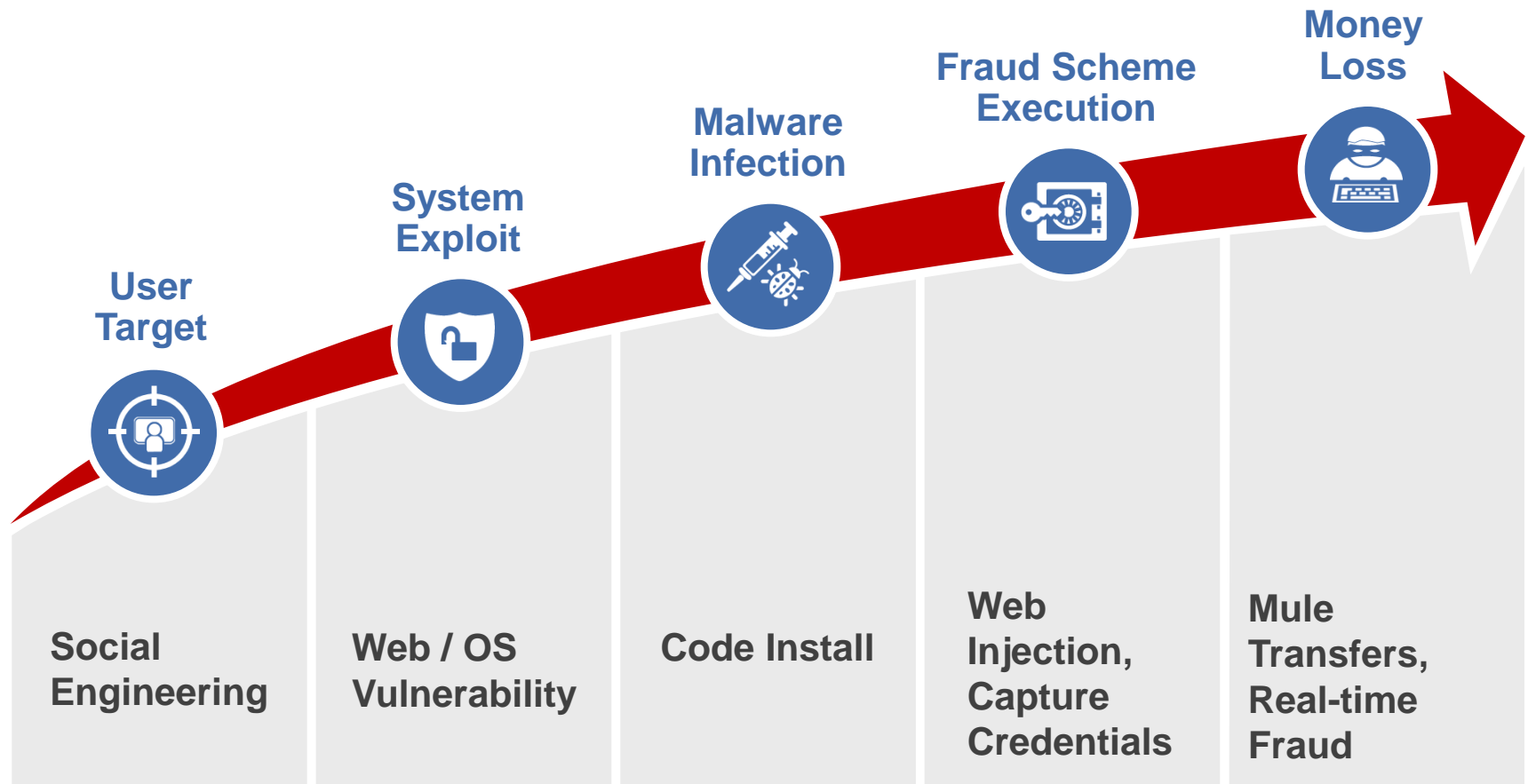


“Controls implemented in conformance with the Guidance several years ago have become less effective..”

“Malware can compromise some of the most robust online authentication techniques”

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

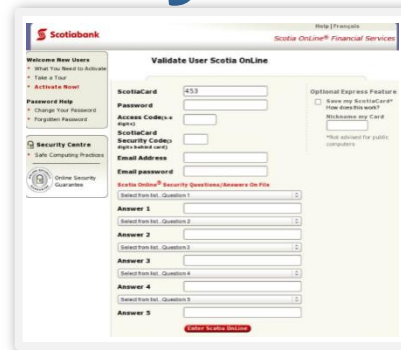
Anatomy of Malware Attack



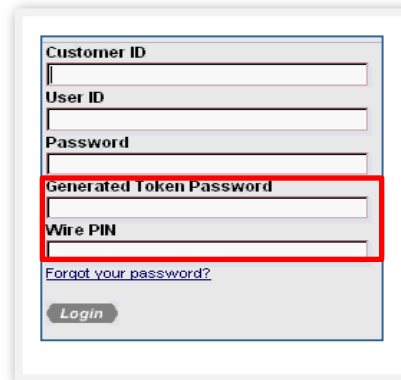
MitB Malware: Anything Goes



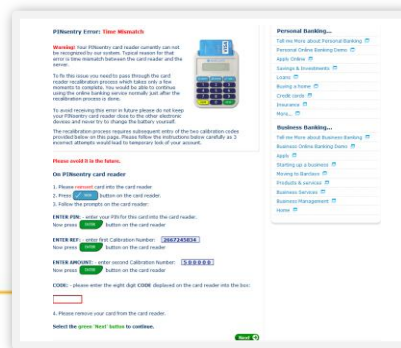
PII Theft



Credentials Theft



Social Engineering



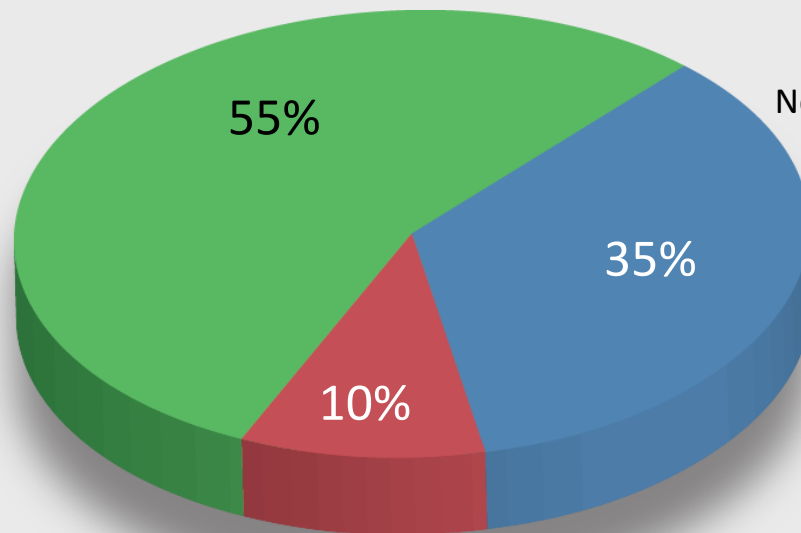
How Effective Are Anti-Virus Applications?

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

55% infected with AntiVirus Up-to-date

10% infected with AntiVirus outdated

Antivirus is Up-to-Date



No Antivirus Found

Antivirus Found but not Up-to-Date

How Trusteer Rapport Detects Financial Malware

Trusteer

Trusteer: What it does?

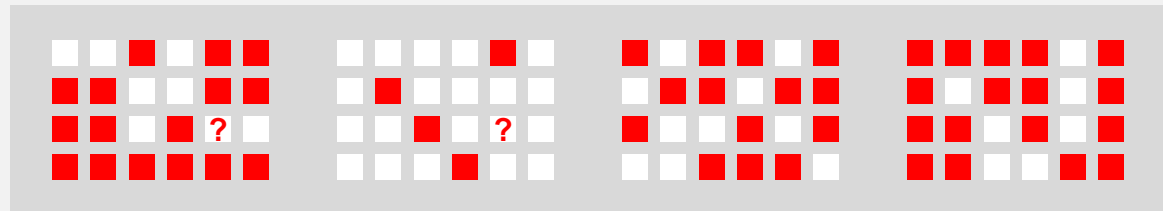
Crime Logic (100s)



Anti-Virus

Legacy: What it is?

Files and Signatures (1000000s)



The Trusteer logo consists of the word "Trusteer" in a sans-serif font. The "Trustee" part is in blue and the "er" part is in green.A large graphic composed of several overlapping circles in various shades of green and blue. The central circle is the darkest green and contains the text "Real Life Malware Examples". The other circles are lighter shades of green and blue, creating a layered effect. The circles are arranged in a way that they appear to be connected or flowing together.

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



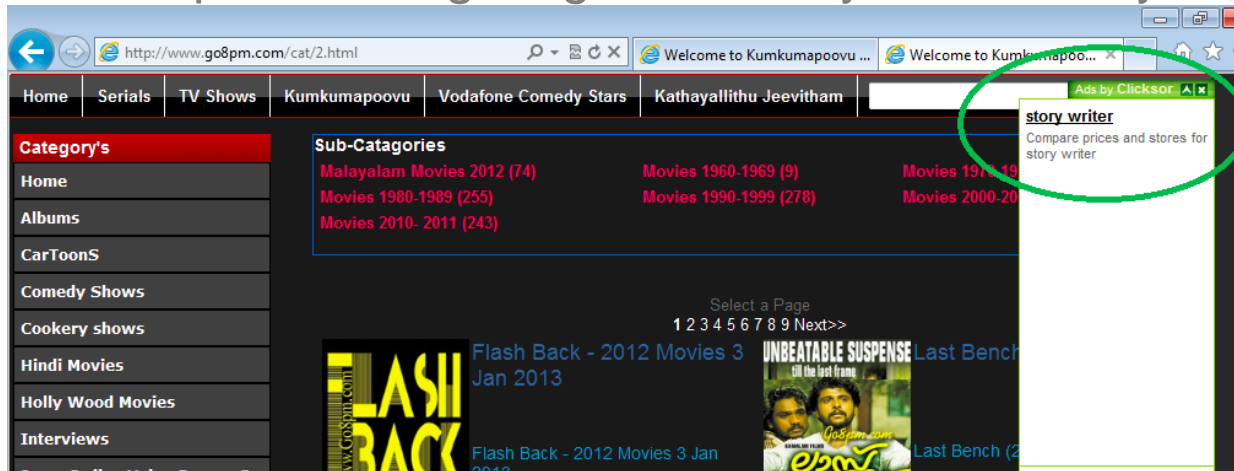
- **And, Breaches on the Rise**

- 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

```
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  
    })  
}
```



AP The Associated Press  

@AP

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

 Reply  Retweet  Favorite  Buffer  More

3,242 RETWEETS 153 FAVORITES

12:07 PM - 23 Apr 13

Cross-Channel Check Fraud



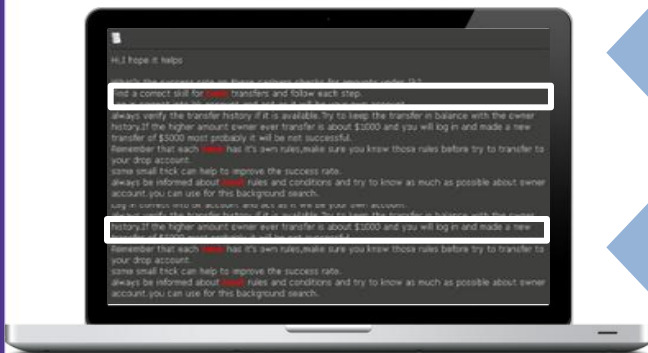
Malware captures check images in a compromised account



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

TRENDS IN FINANCIAL CRIME

Presented by

Special Agent
Jason Berryhill



*U.S. Department of
Homeland Security*

United States
Secret Service

AFP® Annual Conference



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



**HACKER
DETECTED!!**



THE U.S. SECRET SERVICE

Past, Present, Future of Financial Crimes

**Counterfeit
Currency**



THE U.S. SECRET SERVICE

The Future of Financial Crimes

Cyber Crime
(Investigative Mission)



securitynews
DAILY

Alerts! Cybercrime Home & Auto Identity Theft Internet Scams Malware

PIN Pads Hacked at Michaels Stores Nationwide

May 10, 2011 | 5:21 PM ET | By Paul Wagenseil, SecurityNewsDaily Managing Editor



cnet News

Home > News > Privacy & data protection

January 18, 2007 4:32 AM PST

XYZ hack exposes consumer data

By Jon... NYDailyNews.com
Staff V...
Last m...

DAILY NEWS | Crime

News Sports Gossip Entertainment Events Local

National World Politics Crime Headlines / Archives Photos

True Crime Stories The Mob

Article Comments (8)

Malaysian hacker Lin Mun Poo nabbed in Brooklyn after cracking into Fed Reserve network

BY JOHN MARZULLI
DAILY NEWS STAFF WRITER

Friday, November 19th 2010, 4:00 AM



Security on **msnbc.com**

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

'Lulz Boat' group claims attack was in response to a documentary on WikiLeaks

THE U.S. SECRET SERVICE

The Future of Financial Crimes

Cyber Crime (Protective Mission)



Hardware Software Music & Media Networks Security Public Sector

Crime Malware Enterprise Security Spam ID

Print Post comment Retweet Facebook

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](#)

Tweets Favorites Following Followers Lists


 **foxnewspolitics** foxnewspolitics
We wish @joebiden the best of luck as our new President of the United States. In such a time of madness, there's light at the end of tunnel
6 hours ago

 **foxnewspolitics** foxnewspolitics
BREAKING NEWS: President @BarackObama assassinated, 2 gunshot wounds have proved too much. It's a sad 4th for #america. #obamadead RIP
6 hours ago

 **foxnewspolitics** foxnewspolitics
#ObamaDead, it's a sad 4th of July. RT to support the late president's family, and RIP. The shooter will be found
6 hours ago

 **foxnewspolitics** foxnewspolitics
@BarackObama shot twice at a Ross' restaurant in Iowa while campaigning. RIP Obama, best regards to the Obama family.
6 hours ago

 **foxnewspolitics** foxnewspolitics
@BarackObama has just passed. Nearly 45 minutes ago, he was shot twice in the lower pelvic area and in the neck; shooter unknown. Bled out
6 hours ago

 **foxnewspolitics** foxnewspolitics
@BarackObama has just passed. The President is dead. A sad 4th of July, indeed. President Barack Obama is dead
6 hours ago

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



ACCESS DEVICE FRAUD

Emerging Techniques – Memory Dump

Memory Dump



Memory Dump

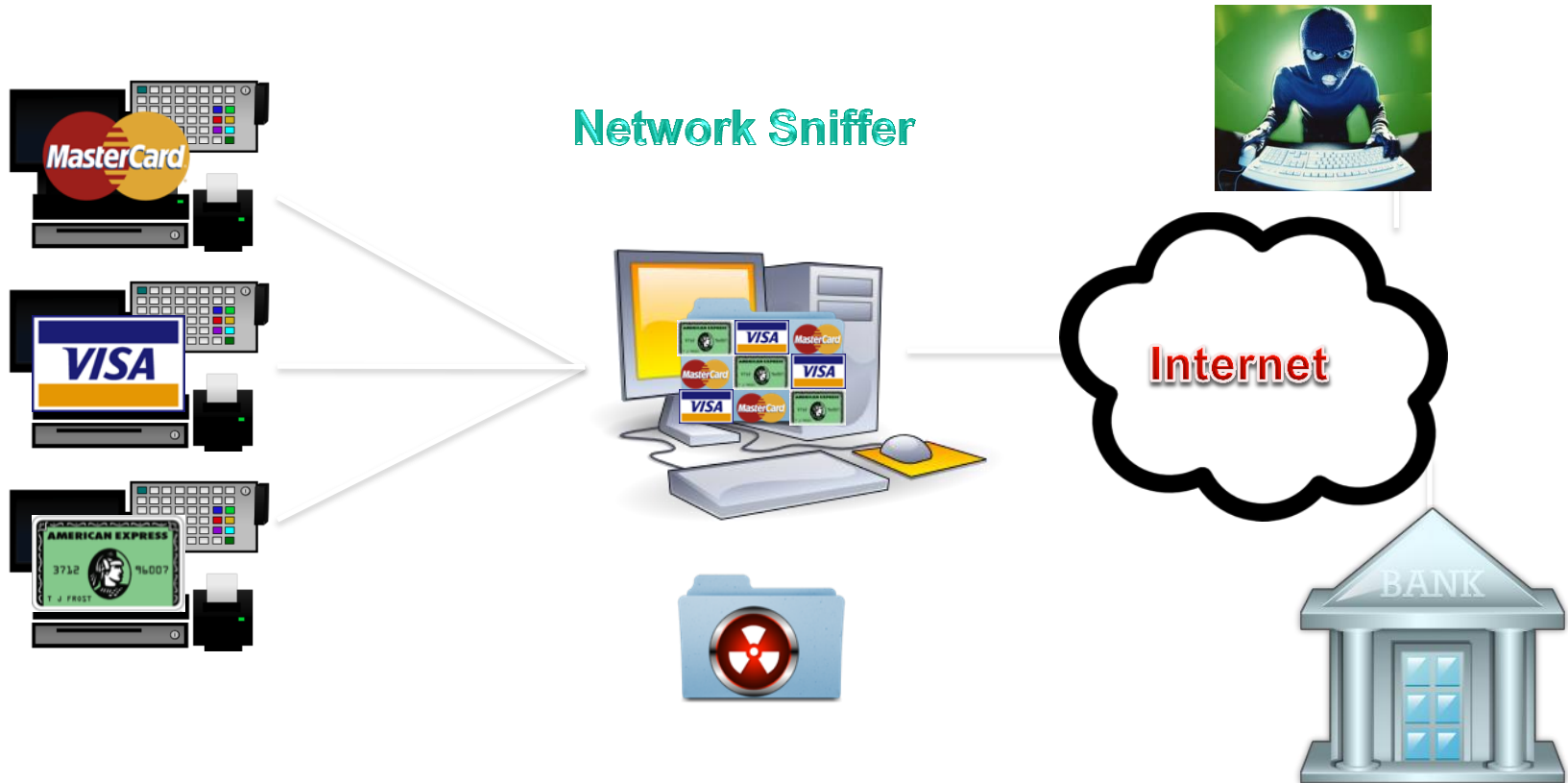


Internet



ACCESS DEVICE FRAUD

Emerging Techniques – Network Sniffers

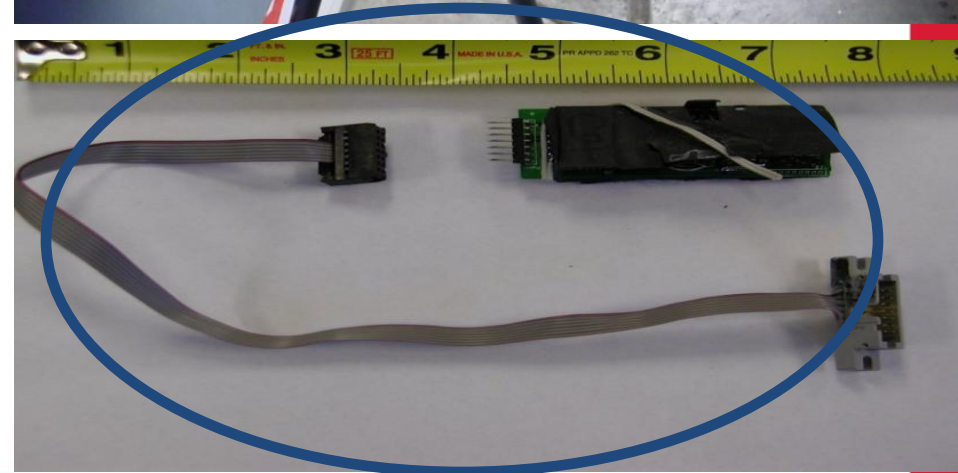
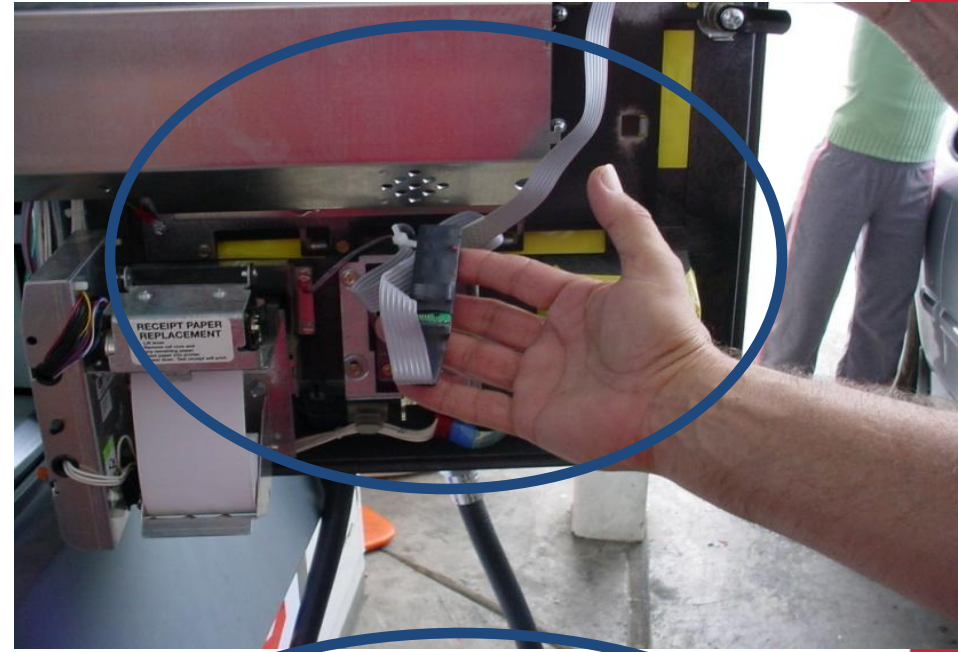


ACCESS DEVICE FRAUD

Typical Skimmers



Gas Pump Skimming



ACCESS DEVICE FRAUD

Emerging Techniques – The Prize



U.S. Department of
Homeland Security

United States
Secret Service

AFP® Annual Confer

C:\Users\William Smith\Desktop\bpk - Log Viewer

January, 2012						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Today: 1/12/2012

Select a date or date range in the calendar to view log records. Drag the mouse to select a range of dates.

PERFECT
KEYLOGGER

Open log... Find...
Save log as... Delete these records...
Close Show entire log

Show: Keystrokes Chats Screenshots Websites [Click here to print the log](#)

8:18 AM
1/12/2012

MSN Hotmail - Message

http://by107fd.bay107.hotmail.msn.com/cgi-bin/getmsg?msg=2E98B7A6-40C3-4EBC-A326-EC87DD58CCDB&start=0&len=616

Fantasy Football MySpace CCpowerForums HotMail Safe-Mail The Grifters Paysec.ru DarkMarket Cardersmarket Gmail Google Yahoo! Mail WhatisMyIP.com IP Chicken DNS Stuff!

B4608053516494892^Your/Name^06021010000000000013300000
 4608053516494892=06021010000013300000 Los Angeles Firemen's
 Credit Union CLASSIC Approved

B4608053516494413^Your/Name^060210100000000000441000000
 4608053516494413=06021010000044100000 Los Angeles Firemen's
 Credit Union CLASSIC Approved

B4313020463012866^Your/Name^060210100000000000377000000
 4313020463012866=06021010000037700000 MBNA America Bank, N.A.
 CLASSIC Approved

B4313032254001230^Your/Name^060210100000000000073000000
 4313032254001230=06021010000007300000 MBNA America Bank, N.A.
 CLASSIC Approved

B4168920000259688^Your/Name^0602101000000000000876000000
 4168920000259688=06021010000087600000 Members Choice Credit Union
 CLASSIC Approved

B4608273970047610^Your/Name^060210104671000000677000000
 4608273970047610=06021010467167700000 Merchants & Farmers Bank
 CLASSIC Approved

B4120613049252361^Your/Name^0602101100000000000895000000
 4120613049252361=06021011000089500000 Merrick Bank Corporation
 CLASSIC Approved

B4120613049900316^Your/Name^0602101100000000000803000000
 4120613049900316=06021011000080300000 Merrick Bank Corporation
 CLASSIC Approved

B4120613049334300^Your/Name^0602101100000000000823000000
 4120613049334300=06021011000082300000 Merrick Bank Corporation
 CLASSIC Approved

B4443041102869360^Your/Name^0602101000000000000881000000
 4443041102869360=06021010000088100000 Merrill Lynch Bank and
 Trust Company CLASSIC Approved

B4489031037024707^Your/Name^0602101100000000000505000001
 4489031037024707=060210110000050500001 National City Bank
 CLASSIC Approved

B4489683806202813^Your/Name^0602101189690000000524000001
 4489683806202813=06021011896952400001 National City Bank of

FREE Shipping



Click here

ACCESS DEVICE FRAUD

Emerging Techniques – Carding Forums

Вход - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.carder.info/

Carder.info

Carder.info - Информационный ресурс кардеров

Здравствуйте Гость ([Вход](#) | [Регистрация](#))

[Carder.info -> Вход](#)

Обнаружены следующие ошибки:

Администратор форума, требует авторизации всех

Перед авторизацией, Вы должны зарегистрироваться
Если Вы не зарегистрированы, Вы можете сделать это

Я забыл свой пароль! [Нажмите сюда!](#)

[Вход](#)

Введите Ваши данные для авторизации, ниже

CardingWorld

Сервис который Вы так долго ждали!

Brotherhood of Carders

Помощь Поиск Участники Календарь

[Регистрация](#)

www.CardingWorld.net

Тогда
lq: 73

Mazafaka.CC - Network Terrorism Forums - Mozilla Firefox

http://forum.mazafaka.cc/

Enlarge your dollar with Mazafaka.CC

NAME | MAZAFKA.CC | REGISTERED | SEARCH | REGISTER | FBI | SEARCH

User Name User Name Remember Me?

Password

Welcome to the Mazafaka.CC - Network Terrorism Forums.

If this is your first visit, be sure to check out the [FAQ](#) by clicking the link above. You may have to [register](#) before you can post; click the register link above to proceed. To start viewing messages, select the forum that you want to visit from the selection below.

Russian speaking carders

Forum	Last Post	Threads	Posts	Moderator
Правила форума Условия и правила форума	Правила размещения рекламы на... by carder 8th January 2005 17:20 *	3	3	carder
Новости форума, объявления, отзывы и пожелания (1 Viewing) Последние новости от mazafaka.ru, различные предложения, отзывы и вопросы к администрации.	Плюшки с кодировкой by zzzz Today 15:23 *	50	399	
Новости в мире Кардинга Самые свежие новости из жизни кардинга	Обращение к управлению К by Muz77Kur70 Today 18:03 *	70	441	

Кардинг
Все темы,
Модератор

Новости
Новости, и
источники
Модератор

Безопасн
Все о без
себя.
Модератор

Обналич
Обналич
и т.д.
Модератор

Реальны
Продажа/т
т.д.
Модератор

Продажа
Покупка/п

ACCESS DEVICE FRAUD

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

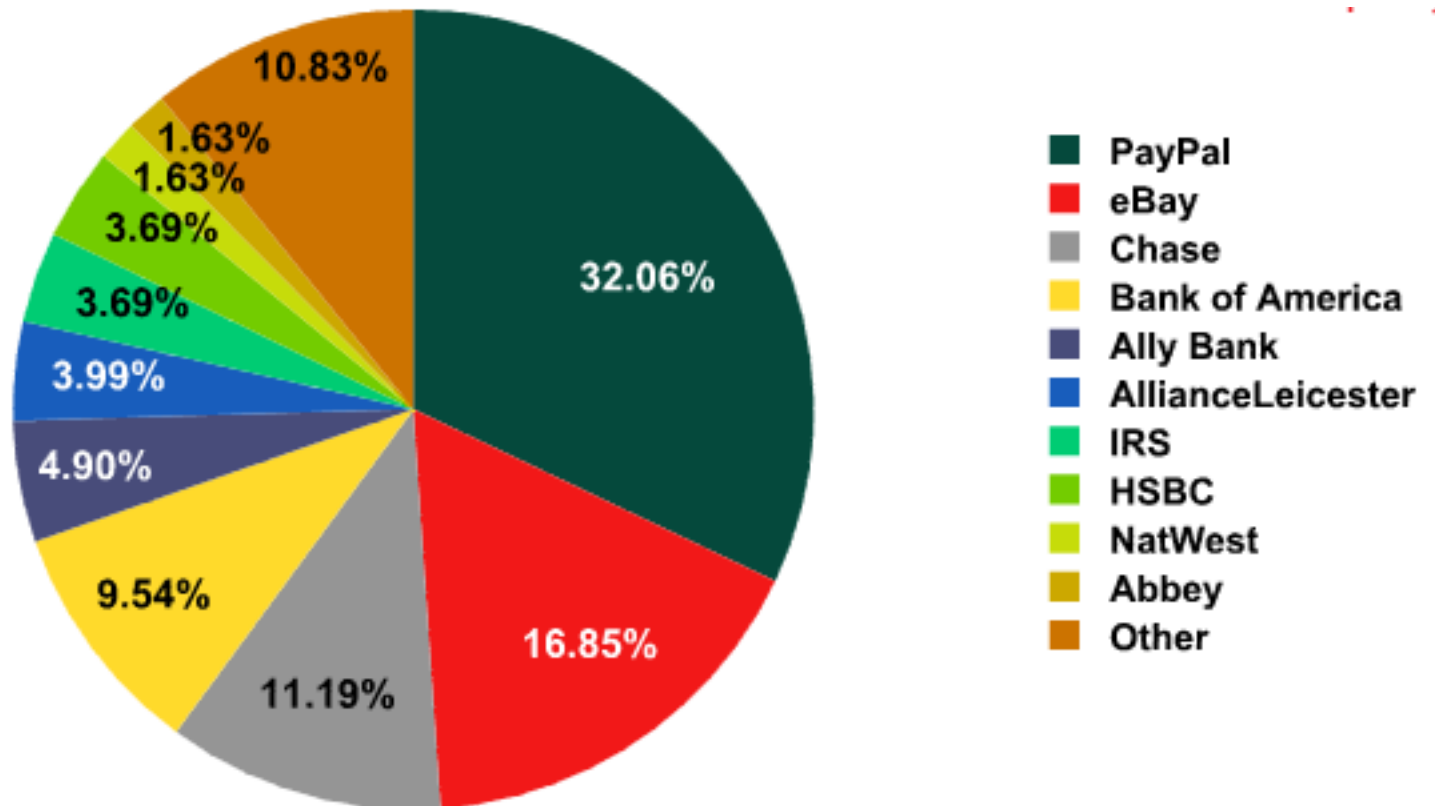


ACCESS DEVICE FRAUD

Emerging Techniques – Creating Duplicate Cards



Emerging Techniques – Phishing



Emerging Techniques – Phishing

Key ways to Detect Phishing

From: admin@reply8647.user.ebaybid.com
Date: Wednesday, October 11, 2006 7:50 AM
To: @hotmail.com
Subject: RE: Alert Message 99820565515184

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

Dear @hotmail.com,

We are contacting you to remind you that on 10 OCT 2006 we identified some unusual activity in your account coming from a foreign IP address: 201.8.43.167 (IP address located in China). We have been notified that a card associated with your account has been reported as lost or stolen and involved in fraudulent transactions, or that there were additional problems with your card.

According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be marked as fraudulent , and will remain open for investigation. You will pay for the fees wich will result from the financial transactions between eBay and FIT (Fraud Investigations Team).

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&co_partnerId=2&pUserId=&siteid=0&pageType=&pa1=&i1=&bshowgif=&UsingSSL=yes

eBay's Privacy Policy and Law Enforcement Disclosure: We care deeply about the privacy of the eBay community and will protect the privacy of our members even while working closely with law enforcement to prevent criminal activity. If you have any questions, please visit eBay's Privacy Central for more information.

http://user47id.com/.../

Emerging Techniques – Phishing With Malware

The screenshot displays a Windows XP desktop environment. In the foreground, a 'Windows Security Alert' dialog box is open, reporting the detection of spyware and adware. The detected items are:

- Adress.Trojan** (Filename: tcp-service.exe)
- zserv.Transponder.Trojan** (Filename: zserv.dll)
- Wstart.TrojanDownloader** (Filename: wstart.dll)

The alert includes a description: 'This program is potentially dangerous for your system. Trojan\Malware\Downloader stealing passwords, credit cards and other personal information from your computer.' and advice: 'You need to remove this threat as soon as possible!'.

In the background, the 'Live PC Care' application is running, showing 'Scan results: 20 potential threats found.' The results are as follows:

Name	Alert level	Action	Status
SpanTool.Win32.Delf.h	Critical	Remove	Not cleaned
Trojan-Spy.HTML.Bayfraud.hn	Critical	Remove	Not cleaned
Trojan-Spy.HTML.GMfraud	Critical	Remove	Not cleaned
Trojan-PSW.Win32.Antigen.a	Medium	Remove	Not cleaned
Trojan-PSW.VBS.Half	Critical	Remove	Not cleaned
Trojan-IM.Win32.Faker.a	Low	Remove	Not cleaned
Trojan-Spy.HTML.Paypal.hn	Critical	Remove	Not cleaned
Trojan-Spy.HTML.Bankfraud.tx	Critical	Remove	Not cleaned
Trojan-Spy.HTML.Sunfraud.a	Critical	Fix	Infected
BAT.Looper	Critical	Fix	Infected

The 'Trojan-Spy.HTML.Paypal.hn' entry is highlighted, with details: Virus name: Trojan-Spy.HTML.Paypal.hn; Security Risk: [5 red bars]; Infected file: C:\Documents and Settings\Administrator\Recent\pal.tmp; Description: This Trojan takes the form of a counterfeit HTML page and uses spoofing technology. It is designed to steal confidential information from users of the PayPal payment system.

A 'Recommended' message at the bottom of the scan results window states: 'Please click "Remove all" button to erase all infected files and protect your PC.'

IDENTITY THEFT

Emerging Techniques – QR Codes



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



QR Code Generator: QR Stuff x

www.qrstuff.com

Are you using Tor? Google Maps centralops yahoo mail Fone Finder query fo NumberInvestigator

QRStuff.com
Get your QR codes out there!

Register Forgot Password? LOG IN

HOME ABOUT THIS SITE QR CODES PHONE SOFTWARE EXAMPLES FAQs AFFILIATES

SHARE

Editable short URL's
 High resolution artwork files
 Account history
 Batch process up to 500 QR codes at a time
 Scan analytics

SUBSCRIBE NOW FROM \$3.95

twitter QRStuff Blog

ENTER DATA TO ENCODE

1 DATA TYPE

- Website URL
- YouTube Video
- Google Maps Location
- Social Media
- iTunes Link
- Plain Text
- Telephone Number
- SMS Message
- Email Address
- Email Message
- Contact Details (VCARD)
- Event (VCALENDAR)
- Wifi Login (Android Only)
- Paypal Buy Now Link

2 CONTENT

Website URL

Embed URL into code as-is
 Use our qrs.ly URL shortener

Subscribers get analytics and dynamic destination editing for shortened URL's.

3 FOREGROUND COLOUR

QR CODE PREVIEW

CASE STUDIES

OPERATION RETAIL RESALE

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

Unauthorized Access
Access Device Fraud

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



By JACK CLOHERTY, PIERRE THOMAS (@PierreTABC), 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.

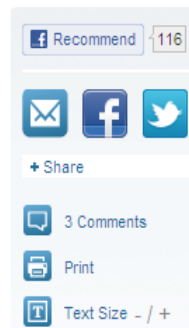
Lin Mun Poo allegedly hacked into U.S. financial institutions and stole more than 400,000 credit and debit card numbers.

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 <CI> *u hacked federal reserve*
 Jun 25 11:06:35 <CI> ?
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 fsvsecurecard 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 <CI> yeah
 May 04 19:44:36 <CI> 1 sec
 May 04 19:44:38 <CI> 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 fsvsecure the network I scan
 May 04 19:45:51 <CI> u sure?
 May 04 19:45:59 <f1ex> http://209.235.105.195:8080/cmd/cmd.jsp?cmd=id
 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 <CI> its main
 Jun 25 11:56:18 <CI> bank
 Jun 25 11:56:31 <CI> 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.



```
Host: 127.0.0.1
Ports to scan: 65566
Now Scanning Ports...
Port 135 is open!
Port 443 is open!
Port 445 is open!
Scanning port 574
Port Scanner
```


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.

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

Speaker



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



Global

Boston, Charlotte, San Francisco, New York, London, Paris, Tel Aviv, Sydney, Santiago, Toronto, Vienna

Application protection at a large scale

10/20

Top US Banks



3/5

Top Canadian Banks



9/10

Top UK Banks



2/4

Top Australian Banks



Speaker

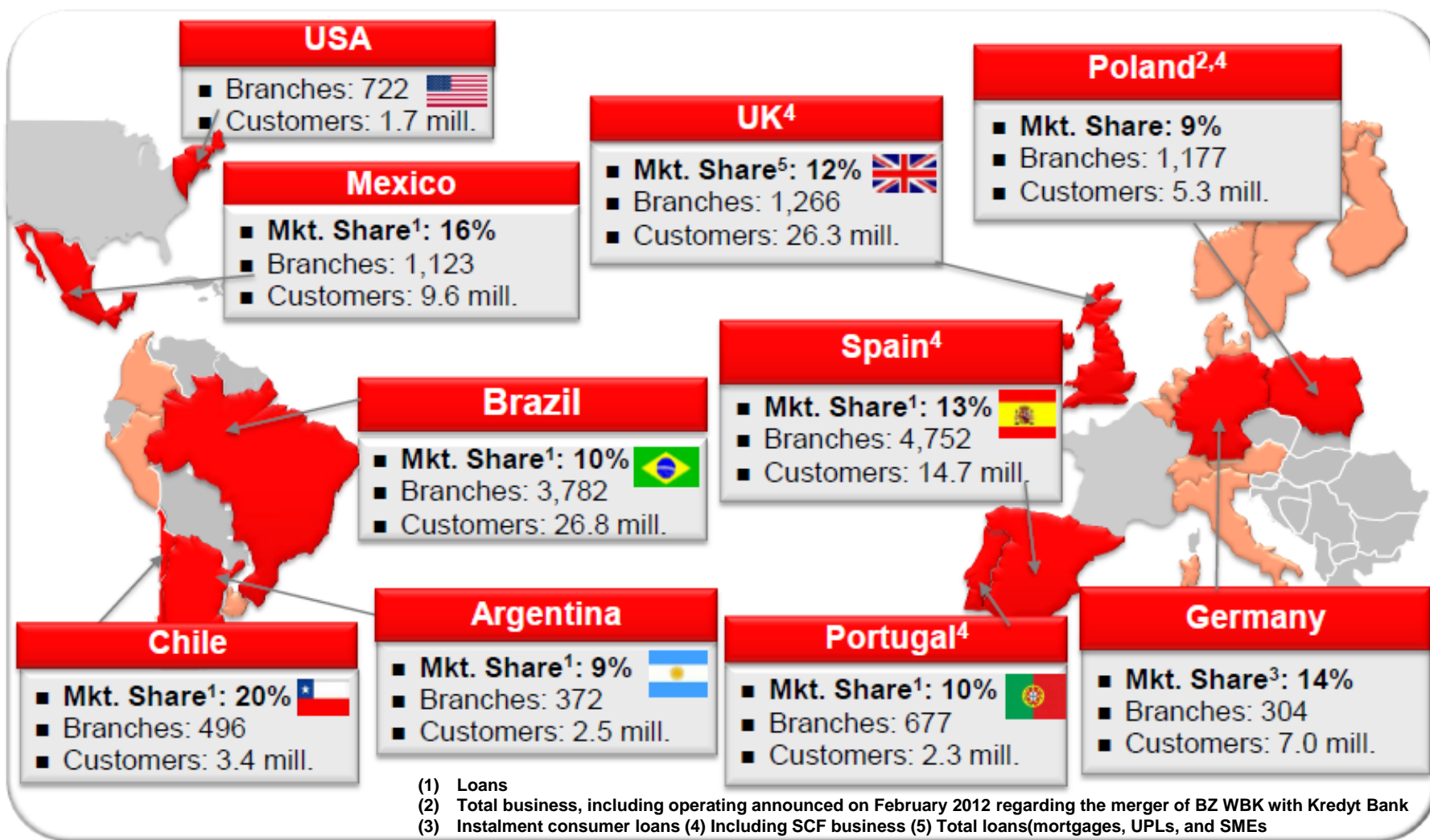


Jim Maimone, CTP
SVP Payables & Receivables
Sovereign Bank, N.A.

- 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



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!