



Cyber Security Threat Landscape

28th Annual FIRMA National Risk Management Training Conference

April 30, 2014

Errol Weiss, Director, Citi Cyber Intelligence Center

Financial Services
Information Sharing & Analysis Center

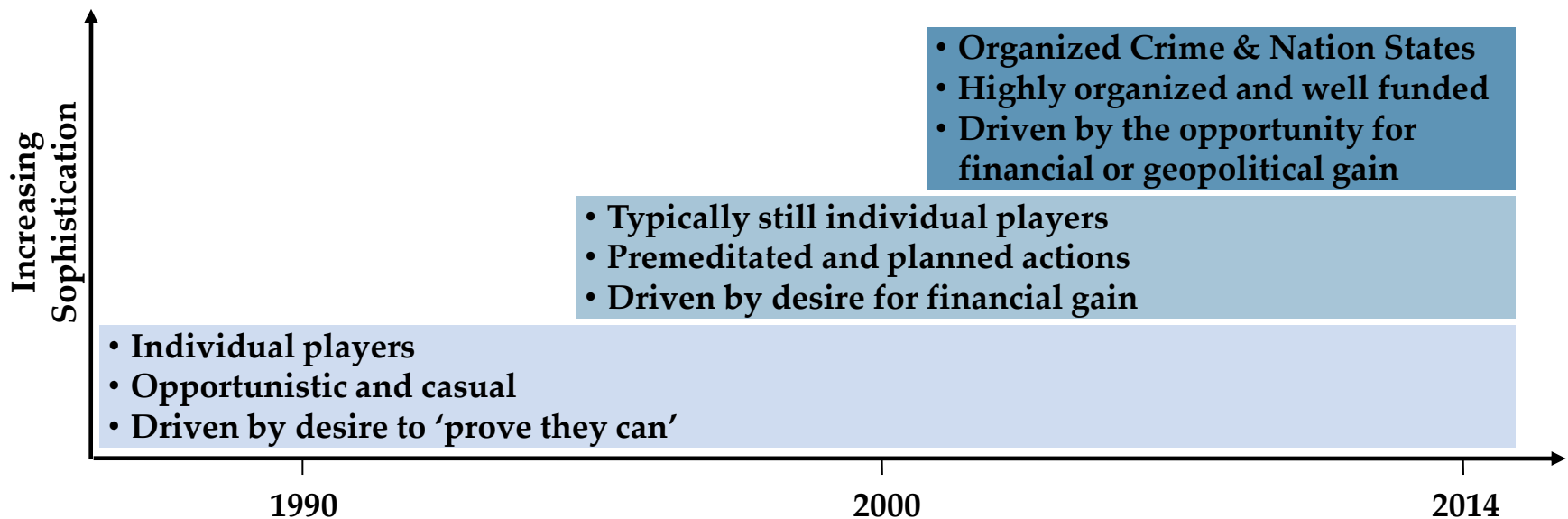
Agenda

- Threat Trends
 - Who is behind the attacks & why?
 - What are the bad guys doing?
- Mitigation Techniques
- What's Next?

Introduction

Citi's Cyber Intelligence Center (CIC)

- Established to address the evolving and maturing threat landscape, including well organized and sophisticated attackers.
- **Mission:** as part of an “intelligence led” strategy, enhance the safety and soundness of the global Citi franchise by sharing timely and actionable intelligence to Citi stakeholders who are empowered to take action and providing situational awareness to internal decision-makers.



Cyber Threat Actors

Cyber Criminals

Motivation: Make Money

Methods: Very mature underground economy supporting every facet of cyber criminal activity



Cyber Terrorism

Motivation: Instill fear to have targets comply with demands or ideology

Methods: Currently using Cyber to “Enable” their programs (Recruit, Incite, Train, Plan & Finance). But there is growing concern they can easily acquire “Disruptive” and possibly “Destructive” capabilities.



Hactivists

Motivation: Seek Publicity to their Geopolitical agenda

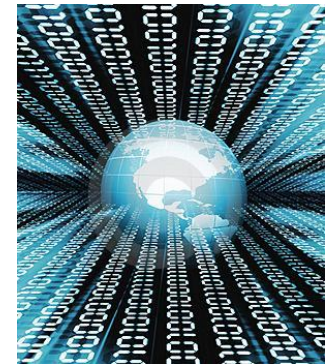
Methods: Disruption and Defacement



Nation State

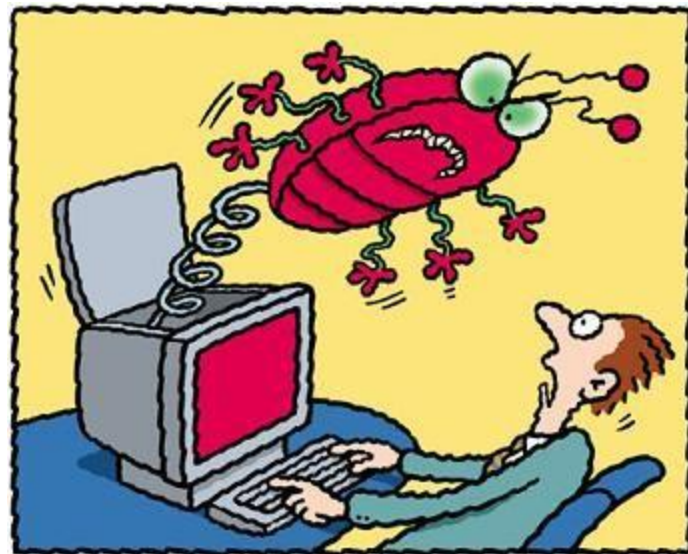
Motivation: Political advantage to improve self interests

Methods: Advanced operations to target specific individuals to gain a foothold into target's infrastructure. Once a foothold is established, adversary is very patient to perform reconnaissance and methodically plan their attack. Often leaving back doors to re-establish access to the target in case their primary means is identified and mitigated.

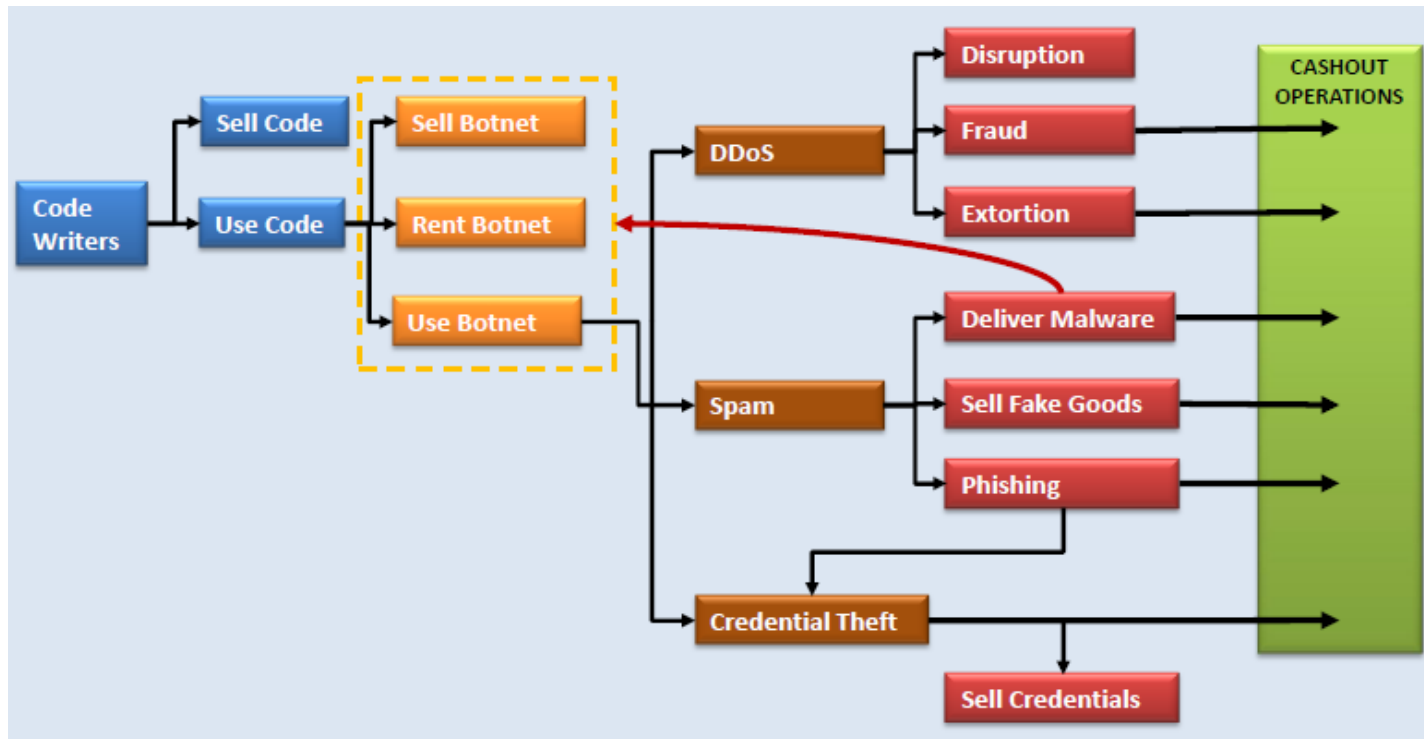


What is Malware?

- Malicious Software
- Types
 - Virus
 - Worm
 - Trojan Horse
 - Adware (aka Malvertising)
 - Crimeware
 - Spyware
 - Scareware
 - Rootkits



Cybercrime Operations



Source: iSight Partners



Adversaries are highly motivated, sophisticated, extremely well organized, and collaborative.

Internet Crime: exploiting the web 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

Russian Hacker Toolkit and Tutorial

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

Russia Hackers :: >>>> Top Secret <http://russiahackers.ru/>

 Search for...

All break Info/Russia Hackers is pleased to announce RH2.5 Kit ver 2011 that users can use to Hack & secure computer systems by knowing exactly how a hacker would



 **Hacking Tools**
We sell latest zero day exploits (doc, xls, pdf, PSD), Java driveby, browser patches, remote pen testing tools, VPN, VPS, Bots, etc...
Contact us for Latest tools.
root@russiahackers.ru or russiahackers@gmail.ru

 **Hacking Marketplace**
Submit your requirement related to Ethical hacking, exploits, crypters, botnets, anything!
Email at: root@russiahackers.ru or russiahackers@gmail.ru

 **Hire a Hacker**
Hire a Hacker for Offensive and Defensive services. Internal on-site penetration testing gives the business the assurance it needs to conduct safely on the internet and with business partners.
Email at: root@russiahackers.ru or russiahackers@gmail.ru

Russia Hackers
Russian Hacking marketplace ::
Russia Hackers is pleased to announce RH2.5 Kit ver 2011 that users can use to Hack & secure computer systems by knowing exactly how a hacker would break into it.
Collection of Advanced Hacking Guide & Tools.
PDF Guide:
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 Apple Apps free of cost
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 for other Russian hacking sites

Buy Now PDF guide: Cost: 300-USD
Other cost: 100 USD
Pay With Liberty Reserve

Tools/Services:
(Value more than 1500 USD)
1. Polymorphic Crypter's (to make files undetectable-bypass all AV Scandime, runtime)
2. Java Driveby FUD (display your site by URL on target)
3. Immunity Canvas (hack remote pc with IP address)
4. Paid Botnets (Spreye, etc)
5. IRC Bots(Ganga, niger, etc)

News & Events
Liberty Reserve Payment gateway added to receive Payments.
10/Jan/2010
06/1/2011
New version Launched.
15/Aug/2009

New Features
100% working latest exploits
Google Translate: Change Language
Select Language
Powered by Google Translate

1 of 2 01/13/2011 07:26 AM

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.

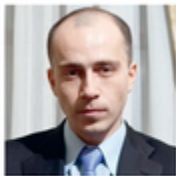
Chronopay direct participant on several major cyber-crime operations including music piracy, DNS changers, scareware, and fake pharmacy distribution networks. Igor Gusev, a former partner of Vrublevsky, claimed that Vrublevsky was also behind RedEye, a notorious organizer of spam, fake anti-viruses, and porno distribution networks.



Chronopay founder arrested for cyber attack on competitor Assist

By [East-West Digital News](#) / Jun 27, 2011

Pavel Vrublevsky, the founder and main owner of electronic payment company [ChronoPay](#), was arrested last Thursday, being suspected of having organized a cyber attack on the website of [Assist](#), a competitor [ChronoPay](#), in an attempt to block payment transactions with the Aeroflot website.



ChronoPay owner Vrublevsky pleads guilty in cyber attack case, court extends detention







By [East-West Digital News](#) / Nov 02, 2011 / [3 Comments](#)

Moscow city court confirmed almost two months of extended detention for prominent Russian Internet businessman Pavel Vrublevsky, who is expected to be held until December 23. The court has rejected an appeal filed by Vrublevsky's attorneys to release the entrepreneur on bail for 30 million rubles, a sum of almost \$1 million.

Malware Infection Techniques

- **Phishing** – Widespread email – lots of victims
- **Spear-Phishing** – 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

Drive by download

1. [ICC Cricket World Cup 2011 Wallpaper](http://www.thecricfanclub.com/wallpapers/icc-cricket-world-cup-2011) 
www.thecricfanclub.com/wallpapers/icc-cricket-world-cup-2011 [Cached](#)
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 Wallpaper Site ...](http://www.worldcupwallpaper.com/) 
www.worldcupwallpaper.com/ [Cached](#) - [Similar](#)
You +1'd this publicly. Undo
World Cup Wallpaper | unOfficial FIFA WorldCup Wallpapers Site - worldcupwallpaper.com.
3. [World Cup Wallpapers](http://www.worldcupwallpapers.com/) 
www.worldcupwallpapers.com/ [Cached](#)
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 \(for Minimalism Lovers ...\)](http://www.smashingmagazine.com/.../fifa-football-world-cup-2010-wallpapers) 
www.smashingmagazine.com/.../fifa-football-world-cup-2010-wallpapers [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](http://www.soccer-desktop.com/) 
www.soccer-desktop.com/ [Cached](#) - [Similar](#)
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](http://www.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

 Follow



55



605



76



3



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.



Drive-by Email -> Open email or view email preview screen

The screenshot displays the Microsoft Outlook interface with the following components:

- Top Ribbon:** Includes tabs for File, Home, Send / Receive, Folder, View, Add-Ins, and Norton. The Home tab is active, showing various email actions like New E-mail, New Items, Ignore, Clean Up, Delete, Reply, Forward, and Meeting.
- Left Sidebar:** Shows the 'Favorites' section with 'Inbox (24)' selected. A red arrow points to the 'Inbox' folder.
- Mail List:** Displays a list of emails. The top email, 'American Banker 1:33 PM Washington/Regulatory Update', is highlighted with a red circle and a red arrow pointing to it.
- Email Preview:** The selected email is displayed in the main pane. The subject is 'Washington/Regulatory Update' and the sender is 'American Banker <americanban...>'. The preview text includes: 'If there are problems with how this message is displayed, click here to view it in a web browser. Click here to download pictures. To help'. The email is dated 'Mon 2/13/2012 1:30 PM' and from 'bnelson@fsisac.us'. Below the preview, there is a section titled 'Today's Regulatory Ref' with a link 'Industry Warns Market-Risk Pla...'. A red circle highlights the entire email preview area.
- Right Sidebar:** Shows a calendar for February 2012. The date '13' is highlighted with a red circle and a red arrow pointing to it. Below the calendar, there is a section titled 'Planning and Updates Call' with the time '1:30 PM - 2:30 PM' and location '6th Floor: Hutchinson Room (Roundtable)'. Below that, it says 'Tomorrow Valentine's Day: United States'.
- Bottom Status Bar:** Shows 'Items: 363' and 'Unread: 296'.

Fake Anti-Virus Scam

The image shows a Windows XP desktop environment. In the background, a 'My computer' window is open. Overlaid on this is a 'Windows Security Alert' dialog box. The alert box has a blue header and a shield icon. It contains the text: 'To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.' Below this, there is a table listing detected spyware and adware. The table has two columns: 'Detected spyware and adware on your computer:' and 'Filename:'. The entries are: W32.Pykspa.F (FontData.fdb), Trojan.Spyeye (ntio412.sys), W32.Daprosy (corelp.lrs), Trojan.Bankpatch.D (desktop.ini), and Trojan.Vundoigen5 (d3d8.dll). At the bottom of the alert box are 'Remove all' and 'Cancel' buttons. Below the alert box, there is a 'WARNING' banner with a yellow exclamation mark icon. Below the banner is a table showing the results of a virus scan. The table has three columns: 'Name', 'Type', and 'Threat level'. The entries are: W32.Pykspa.F (Virus, High), Trojan.Spyeye (Virus, Medium), W32.Daprosy (Virus, Critical), Trojan.Bankpatch.D (Virus, Medium), and Trojan.Vundoigen5 (Virus, Critical). At the bottom of the scan results window is a 'Recommend: Click "Start Protection" button to erase all threats' and a 'Start Protection' button. In the bottom left corner of the desktop, there is a '100% SECURE SITE' badge with a padlock icon.

Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
W32.Pykspa.F	FontData.fdb
Trojan.Spyeye	ntio412.sys
W32.Daprosy	corelp.lrs
Trojan.Bankpatch.D	desktop.ini
Trojan.Vundoigen5	d3d8.dll

Remove all **Cancel**

WARNING

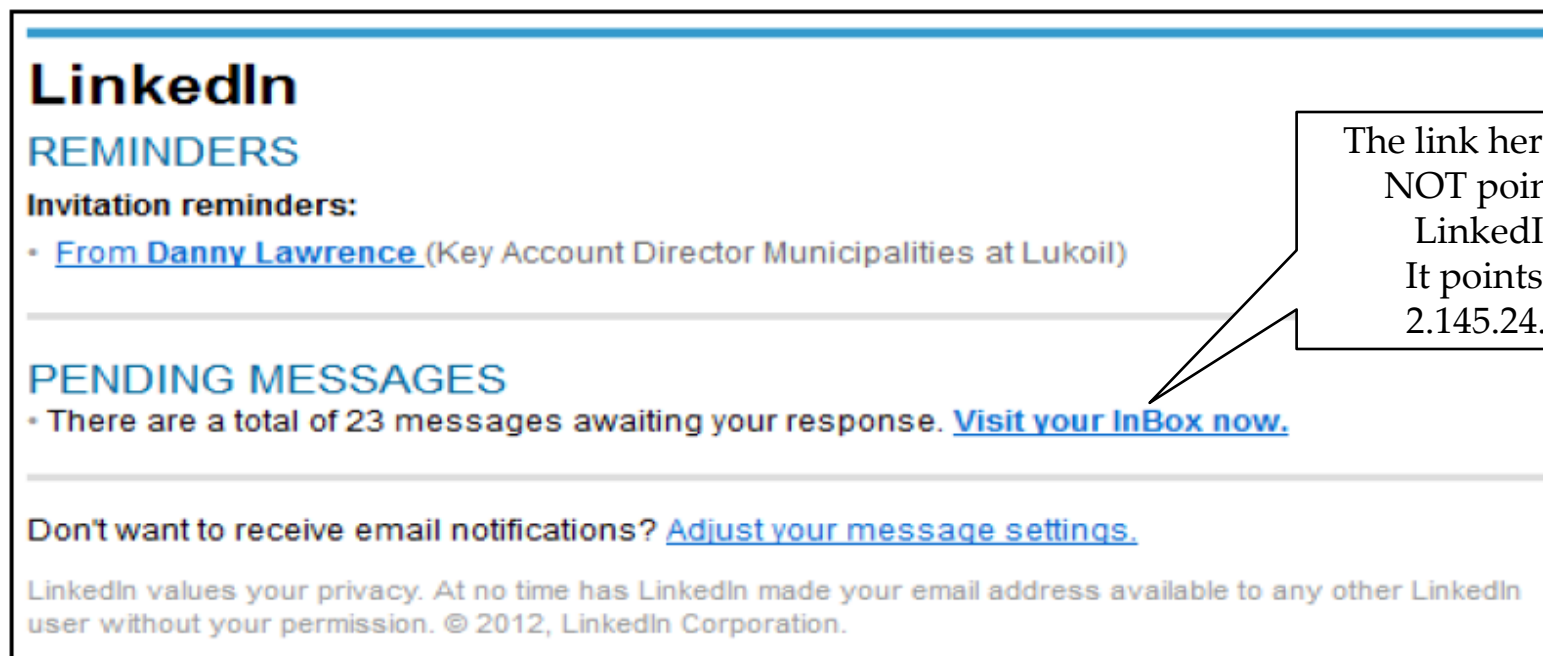
Name	Type	Threat level
W32.Pykspa.F	Virus	High
Trojan.Spyeye	Virus	Medium
W32.Daprosy	Virus	Critical
Trojan.Bankpatch.D	Virus	Medium
Trojan.Vundoigen5	Virus	Critical

Recommend: Click "Start Protection" button to erase all threats

Start Protection

100% SECURE SITE

LinkedIn Spear Phishing



*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).

FedEx Spear Phishing

FedEx.**FedEx Billing Online - Ready for Payment**

fedex.com

Hello [REDACTED]
You have a new not paid invoice(s) from FedEx that is ready for payment.

The following invoice(s) are ready for your review :

Invoice Number
5210-78941

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).

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

- Targeted email campaigns to avoid detection and maximize delivery
- Malicious attachment or link to malicious site

Dun & Bradstreet
CREDIBILITY CORP



INQUIRY ALERT

New Complaint : 8585372

Dun & Bradstreet has received the above-referenced complaint from one of your customers regarding their dealings with you. The details of the consumer's concern are included on the reverse. Please review this matter and advise us of your position.

In the interest of time and good customer relations, please provide the DnB with written verification of your position in this matter **by Oct 25, 2013**. Your prompt response will allow DnB to be of service to you and your customer in reaching a mutually agreeable resolution. Please inform us if you have contacted your customer directly and already resolved this matter.

The Dun & Bradstreet develops and maintains Reliability Reports on companies across the United States and Canada . This information is available to the public and is frequently used by potential customers. Your cooperation in responding to this complaint becomes a permanent part of your file with the Dun and BradStreet. **Failure to promptly give attention to this matter may be reflected in the report we give to consumers about your company.**

We encourage you to print this complaint (attached file), answer the questions and respond to us.

We look forward to your prompt attention to this matter.

To ensure delivery of Dun & Bradstreet Credibility Corp. emails to your inbox and to enable images to load in future mailings, please add alerts@dandb.com to your email address book or safe senders list.

Privacy and Unsubscribe Notice:

To unsubscribe or modify your email alert settings, please login to your account, click "alerts", select "alert settings", and choose the email settings you wish to disable then click "save" to make the desired changes. Your privacy is important to us, please see our privacy policy. To view our terms of service, please click [here](#) If you have any questions, email us at customerservice@DandB.com. Please do not reply to this email.

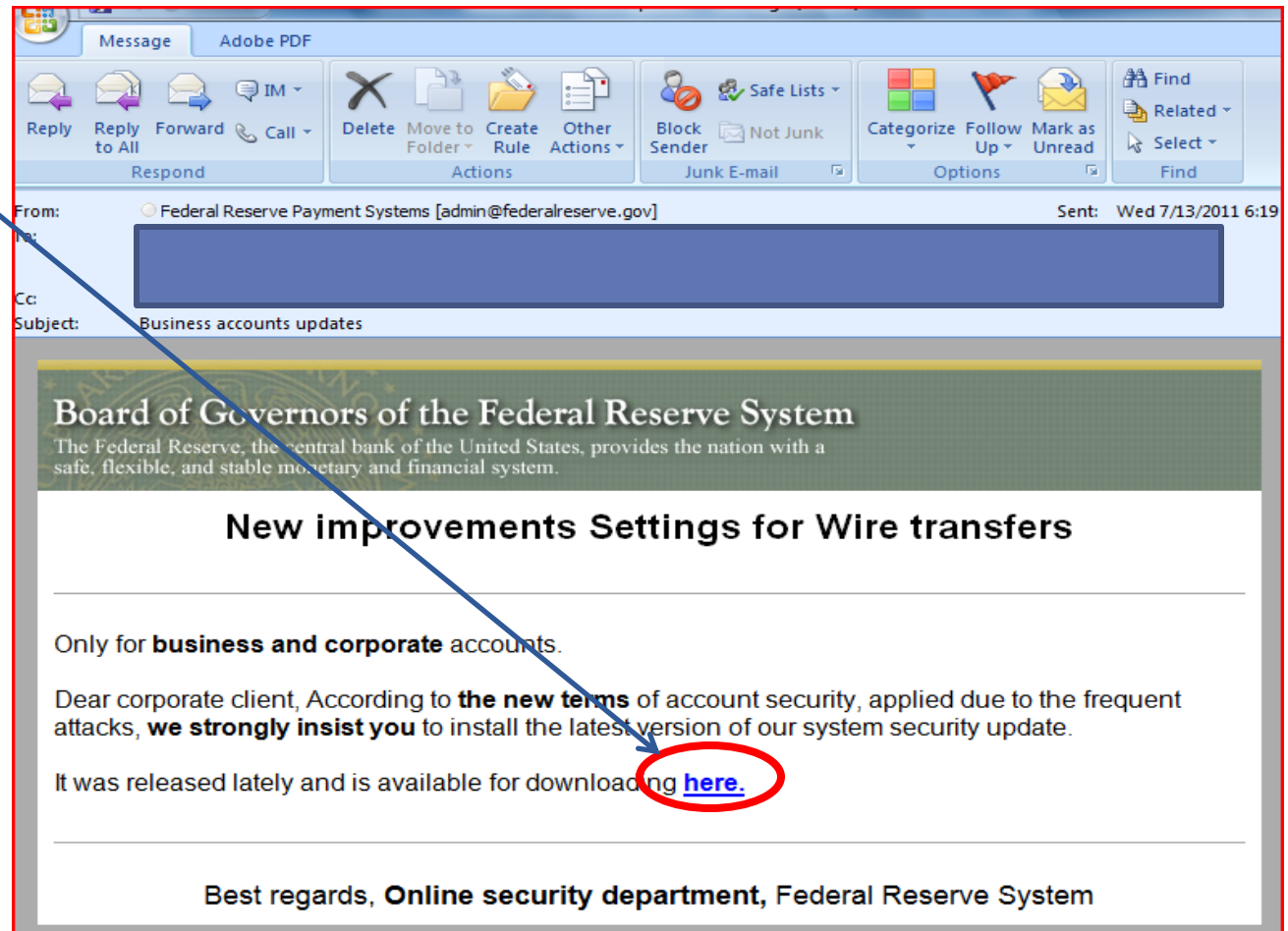
) 2013 Dun & Bradstreet Credibility Corp.

Dun & Bradstreet Credibility Corp., 103 JFK Parkway, Short Hills, NJ 07078

Source: UAB 10/17/2013

Spear Phishing

- What does it look like?
 - The link here will lead the victim to download malware.



Spear Phishing

From: Arbitration Commission at ICC [arbitration@iccwbo.org] Sent: Mon 8/22/2011 10:53 AM
To:
Cc:
Subject: Complaint No 87710 filled against you.

This email is intended to make you aware of the complaint number No 87710 filled with the International Chamber of Commerce by Hughes Trading LTD on 13.08.2011. The ICC is an arbitrary organization and this through this message we make an appeal to your common sense trying to reach a common ground and debate the complaint filled by our member before moving forward to legislative solution. A copy of the complaint as well as more information regarding the complaint filled against your company is available at :

<http://www.iccwbo.org/>

The Commission on Arbitration aims to create a forum for experts to pool ideas and impact new policy on practical issues relating to international arbitration, the settlement of international business disputes and the legal and procedural aspects of arbitration. The Commission also aims to examine ICC dispute settlement services in view of current developments, including new technologies.

Citi received 705 of these fake phishing emails.

From: u130426@server55.neubox.net on behalf of Mark Wahlberg - WM LLP law [mark.wahlberg@wmllp.com] Sent: Tue 8/16/2011 8:21 AM
To:
Cc:
Subject: Cease and desist!

We hereby inform you that you are infringing on copyrighted material, I represent Phoenix Meresix/MB5 LP. It has come to my attention that you have used and/or published on your website (commencing on or about May 18, 2011, pursuant to our information and good faith belief) and continue to publish without permission a number of pieces owned by Phoenix Meresix (webpages, text, images, animated clips, source code, etc.) at your site including, but not limited to, the following url references cited below.

INDEX OF YOUR INFRINGING WEBPAGES:
<http://www.abmps.com/complaint.html>

Mark Wahlberg,
Bretz & Coven, LLP

Citi received 563 of these fake phishing emails.

From: Amazon.co.uk [mailto:auto-shipping@amazon.co.uk]
Sent: Wednesday, August 24, 2011 1:26 PM
To:
Subject: Your Amazon.co.uk order has been shipped (#026-0192826-2172312)

Dear Michael

Greetings from [Amazon.co.uk](http://www.amazon.co.uk)

We are writing to let you know the item(s) pertaining to your order (Order #026-0192826-2172312)

For more information about your order and delivery estimates, please visit:
<http://www.amazon.co.uk/account/tracking/Order=#026-0192826-2172312>

Your order #026-0192826-2172312

Qty	Item	Price	Delivery	Subtotal
1	Nikon D3000 Digital SLR Camera	£309.99	1	£309.99

Amazon.co.uk items:

1 Nikon D3000 Digital SLR Camera... £309.99 1 £309.99

Dispatched via DHL Express

Your payment card has been charged a total of £309.99 and this will appear on your statement as 'Amazon.co.uk'

Should you have any questions, feel free to visit our online Help Desk at:
<http://www.amazon.co.uk/help>

If you've explored the above links but still need to get in touch with us, you will find more contact details at the online Help Desk.

Note: this e-mail was sent from a notification-only e-mail address that cannot accept incoming e-mail. Please do not reply to this message

Thank you for shopping at Amazon.co.uk

Expecting something from Amazon?

The phishers hope you are!

We received 9 of these fake phishing emails, some to very senior executives at Citi.

UAB Report of Spear Phishing Emails

<u>DATE</u>	<u>SPOOFED BRAND</u>	<u>ATTACK TYPE</u>	<u>INITIAL VT DETECTION RATE</u>
6/20/2012	Verizon Wireless	BlackHole Exploit Kit > Generic Bad thing	3 out of 42
6/20/2012	UPS + DHL	Zipped .EXE > Generic Bad Thing	4 out of 42
6/19/2012	USPS	Zipped .EXE > SpyEye/Cridex/Bredolab	5 out of 42
6/18/2012	Verizon Wireless	BlackHole Exploit Kit > Ransom/Birele/ZeuS	0 out of 42
6/15/2012	Verizon Wireless	BlackHole Exploit Kit > ZeuS/Cridex	4 out of 42
6/15/2012	Habbo.com	BlackHole Exploit Kit > ZeuS/Cridex	20 out of 35
6/14/2012	Tax Payment Failed/IRS	BlackHole Exploit Kit > Zeus	4 out of 35
6/14/2012	DHL	Zipped .EXE > Andromeda	27 out of 42
6/12/2012	Twitter.com	BlackHole Exploit Kit > ZeuS	14 out of 42
6/12/2012	LinkedIn.com	BlackHole Exploit Kit > ZeuS	12 out of 42
6/12/2012	Amazon.com	BlackHole Exploit Kit > Cridex/Carberp/Dapato	5 out of 42
6/11/2012	Paypal.com/eBay.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	5 out of 42
6/11/2012	Amazon.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	4 out of 42
6/11/2012	Myspace.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	4 out of 42
6/8/2012	Xanga.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	5 out of 38
6/6/2012	Craigslist.com	BlackHole Exploit Kit > Cridex/ZeuS	5 out of 42

Scareware / Extortion

 CryptoLocker

Σ3



Private key will be destroyed on
**9/8/2013
5:52 PM**

Time left
56 : 16 : 12

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key [RSA-2048](#) generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR / similar amount** in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>

Scareware / Extortion



THE **FBI**
FEDERAL BUREAU OF INVESTIGATION

All activity of this computer has been recorded
If you use a webcam, videos and pictures were saved for identification



Video-recording: ON



You can be clearly identified by resolving your IP address and the associated hostname

Your IP Address:

Your Hostname:

Location:

Your Computer has been locked!

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Described below are possible violations, you have made:

Article 274 – Copyright

A fine or imprisonment for the term of up to 4 years
(The use or sharing of copyrighted files – movies, software)

Article 183 – Pornography

A fine or imprisonment for the term of up to 2 years
(The use or distribution of pornographic files)

Article 184 – Pornography involving children (under 18 years)

Imprisonment for the term of up to 15 years
(The use or distribution of pornographic files)

Article 184 – Promoting terrorism

Imprisonment for the term of up to 15 years
(You have visited websites of terrorist organizations)

Article 297 – Neglect computer use, entailing serious consequences

A fine or imprisonment for the term of up to 2 years
(Your computer has been infected with a virus, which, in turn, infected other computers)

Article 188 – Gambling

A fine or imprisonment for the term of up to 2 years
(You have been gambling, but according to the law residents of the your country are not allowed gambling in any format)

In connection with the decision of the Government as of August 22, all of the violations described above could be considered as conditional in case of payment of a fine.

Amount of the fine is \$200. Payment must be made within 48 hours after the discovery of the violation.

If the fine has not been paid, you will become the subject of criminal prosecution.

After paying the fine your computer will be unlocked

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of \$200.



Exchange your cash for a MoneyPak voucher and
use your voucher code in form below.

Code:

1 2 3 4 5 6 7 8 9 0

Submit

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

In this case a criminal case against you will be initiated automatically.

FRAUD ALERT: Use your MoneyPak number only with businesses listed at MoneyPak and United States Federal Bureau of Investigation. If anyone else asks for your MoneyPak number? It's probably a scam. If a criminal gets your money, Green Dot is not responsible to pay you back.



Where can I buy
MoneyPak



CVS/pharmacy

Walgreens

Walmart



100%
Secure Payments

Mobile Malware



The Kaspersky Lab Security News Service

- 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.

Mobile Application Threats



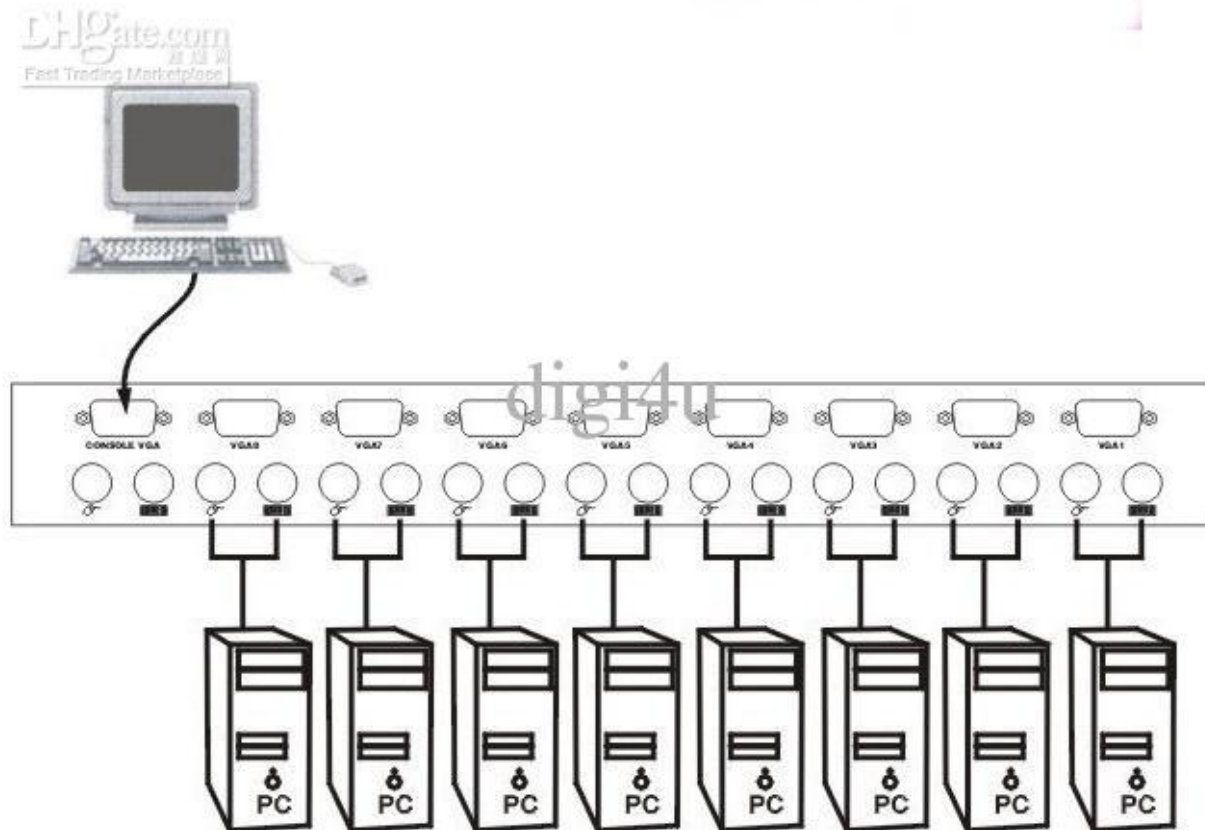
Mobile Application Threats



Identity Theft on your smartphone???

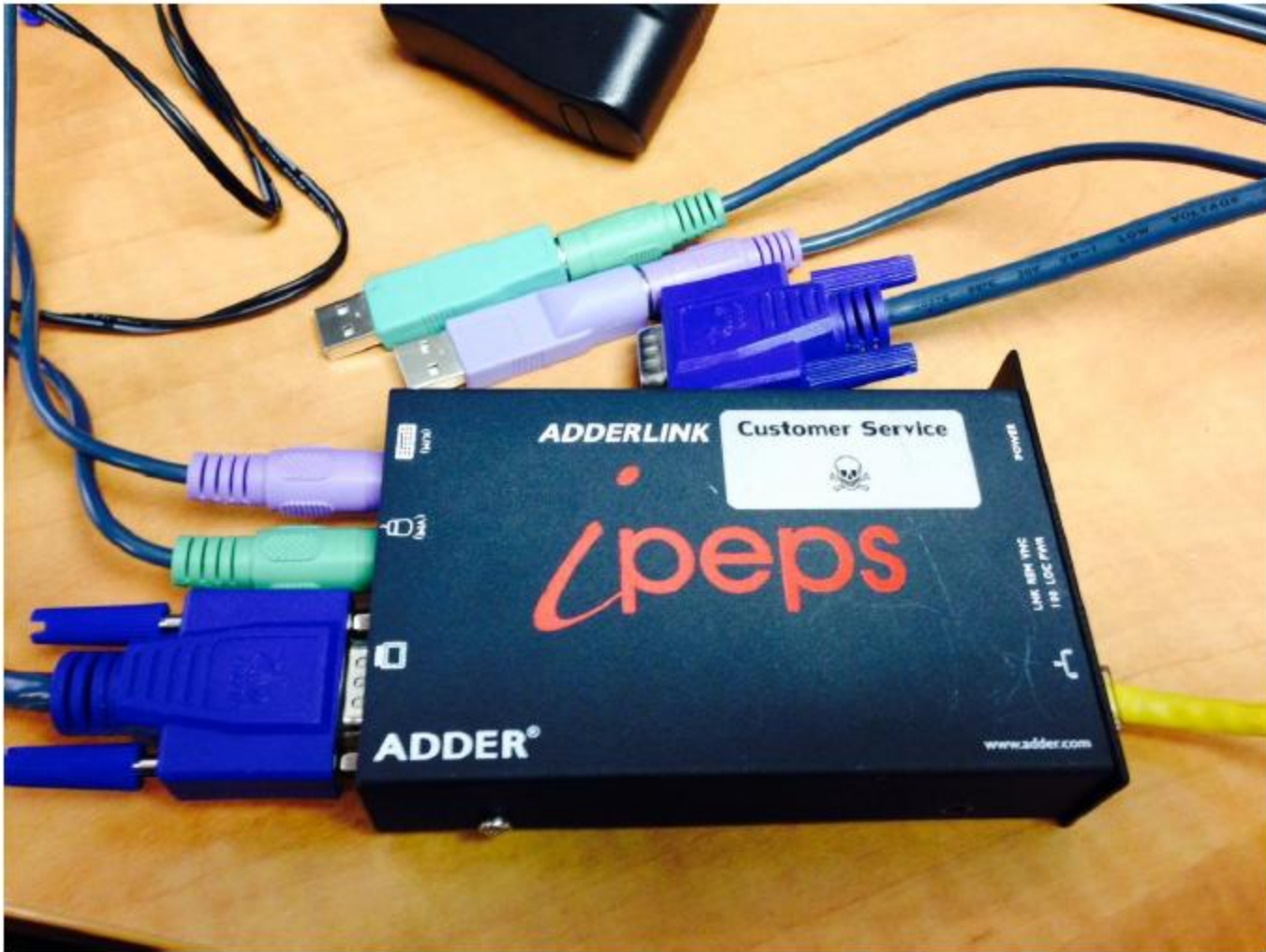
- Pop-up a system alert prompting them to contact Citibank Support
- Provides a phone number to the dialer
- The app has permissions to
 - report user's location
 - record the audio of the call
 - deliver intercepted information back app author

What is a KVM Switch?



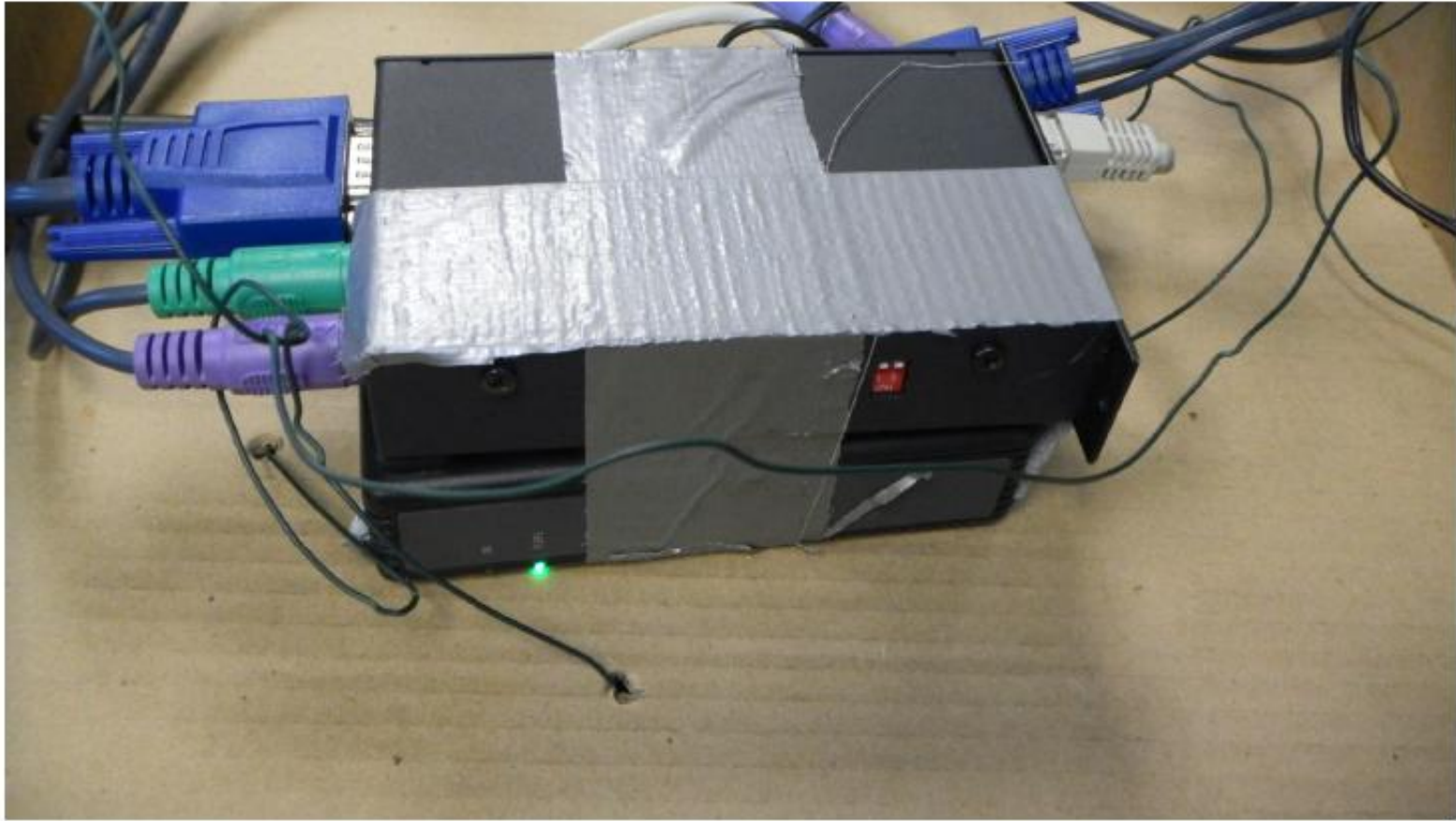
KVM = Keyboard + Video + Mouse

KVM up close



KVM devices found in UK Banks

KVM Device with Leads, Taped to 3G Router



Some not so obvious



Skimming devices found on six registers at a Nordstrom department store in Florida last week.

Source: [Krebsonsecurity](https://krebsonsecurity.com)

Recent Data Aggregator Breaches

- September 25, 2013, Security Researcher, Brian Krebs, published a report on underground Identity Theft Service, ssndob.ms
- Criminals ran a small botnet that stole data from computers at LexisNexis, Dun & Bradstreet and Kroll Background America
- The report suggests compromised data aggregators were the source for the ssndob ID Theft Service
- Marketed as a reliable and affordable service to look up SSNs, birthdays and other personal data on any U.S. resident
- Existence for at least two years
- Prices range from 50 cents to \$2.50 per ssndob record, and \$5 to \$15 for credit and background checks



User: ssndob@ssa.gov. Balance: \$316. Searches queue (ALL/VIP): 0/0

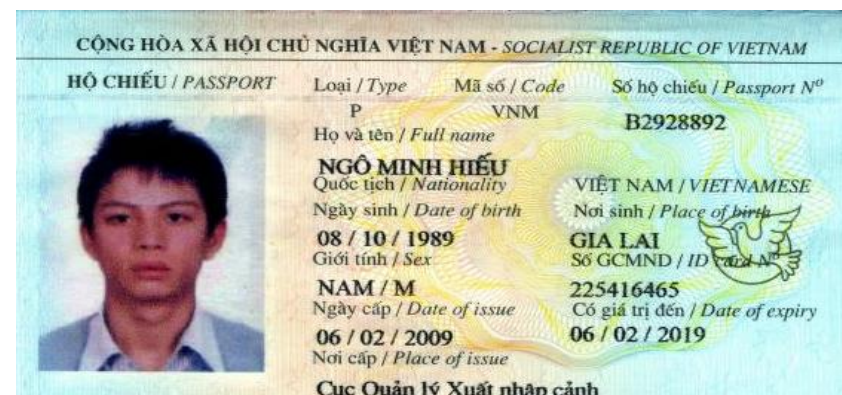


Logged In Successfully

Recent Data Aggregator Breaches

- Follow on report on October 20th revealed that another ID Theft Service, superget.info, sourced sensitive personal information from Experian
- Criminal obtained access to Experian data by posing as a U.S.-based private investigator
- Paid Experian with wires from a Singapore bank account
- Indictment unsealed revealed the true identity is Hieu Minh Ngo, a 24 year old Vietnamese native

Homepage Search SSN, DOB USA History My Account Contact Admin There's 4 online user(s) in total of 1007		
History Filter : <input type="text" value="All"/>		
ID	Input Param	Search Result
1	First Name : MICHAEL Last Name : Middle Name : City : State : NY	firstname:MICHAEL middlename:A lastname: dateofbirth:N/A age:N/A housenumber:43 predirection:N/A streetname: streetsuffix:RD postdirection:N/A unidesignator:N/A city:ROCKY POINT state:NY zipcode:11778 datereported:08-01-2000 phonenummer: sourceid:TH datecreated:08-01-2000 dateupdated:08-01-2000 ssn:Click to show
2	First Name : MICHAEL Last Name : Middle Name : City : State : NY	firstname:MICHAEL middlename:A lastname: dateofbirth:N/A age:N/A housenumber:43 predirection:N/A streetname: streetsuffix:RD postdirection:N/A unidesignator:N/A city:ROCKY POINT state:NY zipcode:11778 datereported:08-01-2000 phonenummer: sourceid:TH datecreated:08-01-2000 dateupdated:08-01-2000 ssn:Click to show



Threat Remediation

- Reassess the effectiveness of using PII in stepped up authentication strategies.
- Provide support / call center staff with guidance on how to handle phone calls from customers if their accounts or identity are at risk due to the recent data aggregator breaches.



Merchant Point of Sale Breaches

Financial Services Information Sharing & Analysis Center



18 Sources: Target Investigating Data Breach

DEC 13

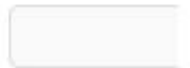


Nationwide retail giant **Target** is investigating a data breach potentially involving millions of customer credit and debit card records, multiple reliable sources tell KrebsOnSecurity. The sources said the breach appears to have begun on or around Black Friday 2013 — by far the busiest shopping day the year.

Update, Dec. 19: 8:20 a.m. ET: Target released a **statement** this morning confirming a breach, saying that 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013.

Original story;

According to sources at two different top 10 credit card



Target Breach



- December 19, 2013 Target issues press release regarding a security breach.
- Press Release provided compromise time window Nov 27th to Dec 15th, 2013
- Breach is contained as of Dec 15th
- Estimated 40 Million cards (track data) exfiltrated in the data breach (Name, Account #, Expiration Date, CVV1).
 - CVV1 (or CVC1) is encoded into the magnetic stripe (track 2) and is used to validate the card in “card present” transactions.
 - CVV2 (or CVC 2) is a 3 digit code on the signature line of the card, used to verify the card for Mail Order / Telephone Order (MOTO) and Internet transactions.
- Breached data is used to encode track data onto cards to facilitate counterfeit card fraud.
- 1.7MM Cards tied to the breach are available for sale in the underground.
 - MC BINS - \$44
 - Visa BINS - \$21



A graphic advertisement for stolen cards sold under the "Tortuga" base.

Malware Used in the Target Breach

The Malware – Kaptoxa ("Kar-toe-sha") also known as Trojan.POSRAM

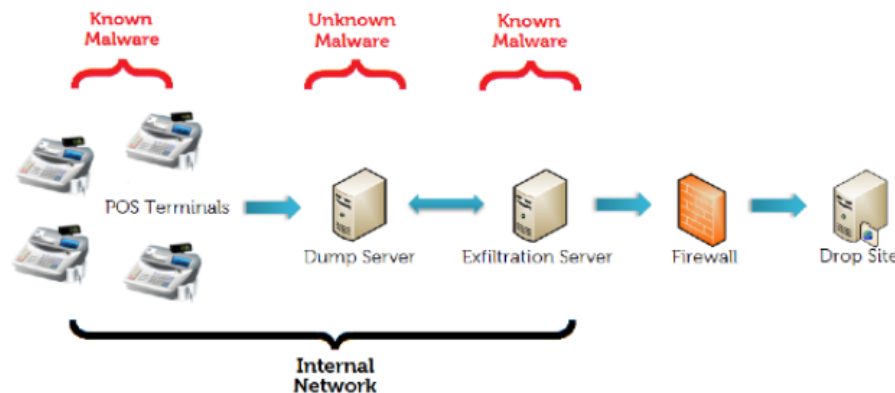
- Monitors the memory address space on the Point-of-Sale device and extracts credit card data from memory
- The code is based on BlackPOS, allegedly developed in 2013 by a Ukrainian teen who uses the nickname Rescator



The Attack Chain - The attacker used a variety of tools to penetrate the environment, maintain persistence and extract data

- INFECTION via third party HVAC vendor who was compromised via an email phishing attack and moved across a b2b connection
- EXFILTRATION – The malware ran undetected for days on each PoS and data was then moved via a temporary NetBIOS share to an infected host inside Target's network and exfiltrated out through an FTP connection to an external host.

Figure 2 - Diagram of Data Exfiltration



Source: Dell SecureWorks

Target Breach

Target's Response – A **public apology** and a promise to improve security, in part by accelerating a shift to more secure payment cards

SUMMARY – This was a sophisticated attack in the way the attacker put everything together and was able to orchestrate the overall attack, and to a lesser extent the individual components



Threat Remediation

- Examine third party connections, implementation standards and practices
- Evaluate internal software distribution, patch update and management systems
- Need better collaboration and information sharing between merchant / retailers

A “Kill Chain” Analysis of the
2013 Target Data Breach

Majority Staff Report For Chairman Rockefeller
March 26, 2014



COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION

Sources:

http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=192fc371-576b-4361-a983-ac70489f9627

http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883



Risk Mitigation Recommendations

Financial Services Information Sharing & Analysis Center

Account Takeover Fraud Advisory

- Co-Branded with US Secret Service, FBI, Internet Crime Complaint Center (IC3) and FS-ISAC
- Problem
- How it's Done
- How to Protect, Detect, and Respond

N.Y. Firm Faces Bankruptcy from \$164,000 E-Banking Loss

European Cyber-Gangs Target Small U.S. Firms, Group Says

e-Banking Bandits Stole \$465,000 From Calif. Escrow Firm

La. firm sues [bank] after losing thousands in online bank fraud

Cyber attackers empty business accounts in minutes



- **Protect**

- Education
- Enhance security of computer and networks
- Enhance security of corporate banking processes and protocols
- Understand responsibilities and data breach notification requirements and liabilities

- **Detect**

- Monitor and reconcile accounts at least once a day
- Discuss options offered by your financial institution to help detect or prevent out-of-pattern activity (including both routine and red flag reporting for transaction activity)
- Note any changes in the performance of your computer
- Pay attention to warnings
- Be on the alert for rogue emails
- Run regular virus and malware scans

- **Respond**

- If you detect suspicious activity, immediately cease online activity and remove computer system from the network
- Ensure employees know how and who to report suspicious activity to within your company and at your financial institution
- Immediately contact your financial institution so that the following actions may be taken
- Maintain written chronology events, losses, and steps taken to report incident
- File a police report and provide the facts and circumstances surrounding the loss
- Have a contingency plan to recover systems suspected of compromise
- Consider whether other company or personal data may have been compromised
- Report exposures to PCI DSS



INTERNET CRIME COMPLAINT CENTER



Fraud Advisory for Businesses: Corporate Account Take Over

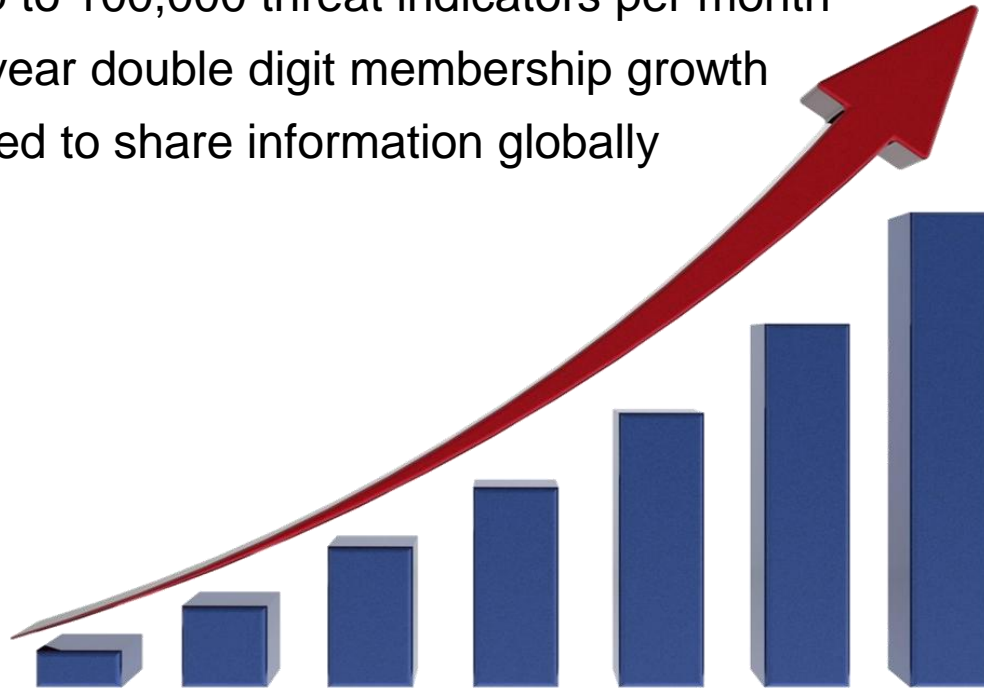
Available here:

<http://www.ic3.gov/media/2010/corporateaccounttakeover.pdf>



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
- ⊙ Process up to 100,000 threat indicators per month
- ⊙ Year over year double digit membership growth
- ⊙ Now enabled to share information globally

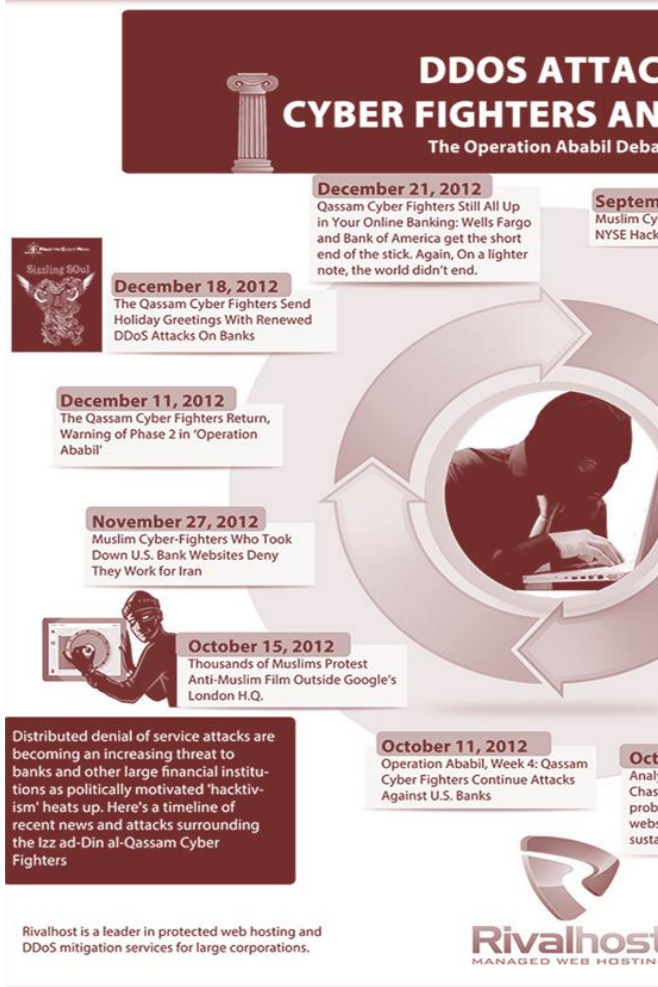


FS-ISAC Intelligence in Action

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 Subject Matter Experts at peer financial institutions
- ✓ No attribution
- ✓ A sense of community and not having to go it alone

FS-ISAC Intelligence in Action



- ⊙ Al-Qassam Cyber Fighters – Coordinated attacks against FIs beginning September 2012
- ⊙ 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 firm**

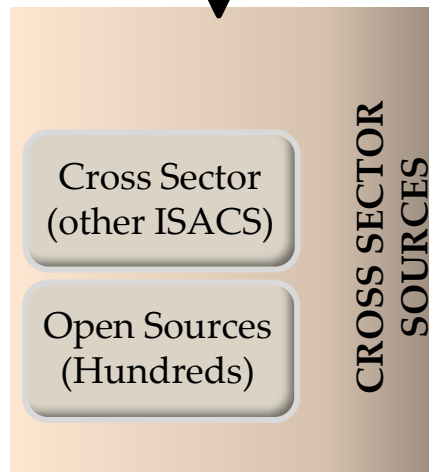
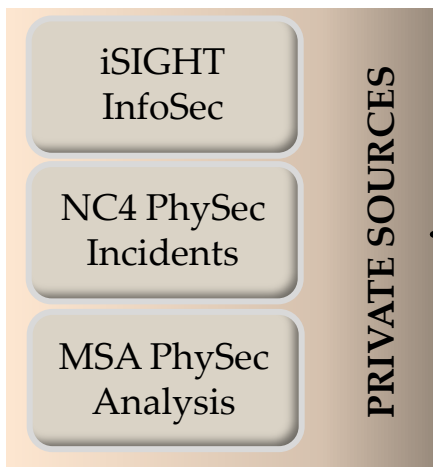
Mission

FS-ISAC's mission: share timely, relevant and actionable information and analysis of physical and cyber security information pertaining to threats, vulnerabilities and incidents.

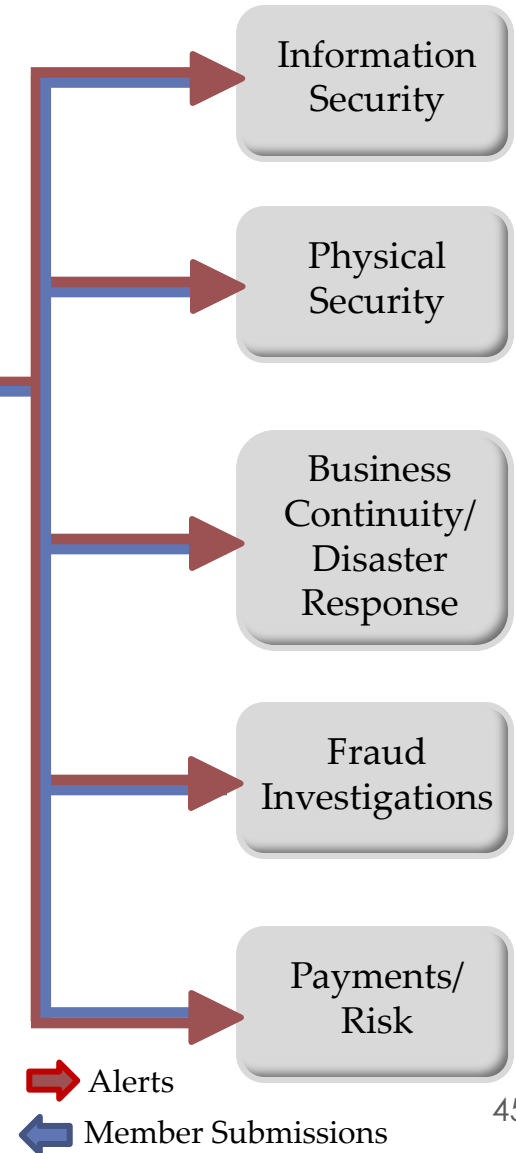
Facilitate sharing between government and member financial institutions, between members, and with other sectors in order to help protect the global financial services critical infrastructure.

FS-ISAC 24/7 Security Operations Center

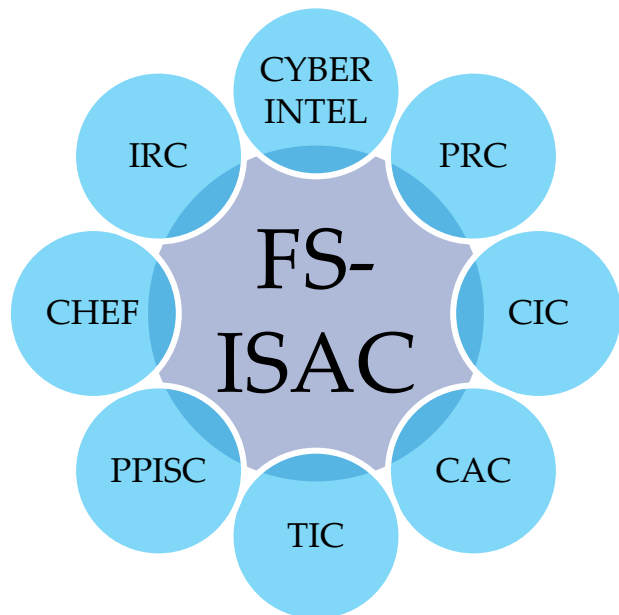
Information Sources



Member Communications



How FS-ISAC Works: Circles of Trust



- Clearing House and Exchange Forum (CHEF)
- **Payments Risk Council (PRC)**
- Payments Processor Information Sharing Council (PPISC)
- Business Resilience Committee (BRC)
- Threat Intelligence Committee (TIC)
- Community Institution Council (CIC)
- Insurance Risk Council (IRC)
- Compliance and Audit Council (CAC)
- **Cyber Intelligence Listserv**
- Education Committee
- Product and Services Review Committee
- Survey Review Committee
- Security Automation Working Group (SAWG)

Member Reports
Incident to Cyber
Intel list



Members respond with
initial analysis and
recommendations



SOC completes analysis,
anonymizes the source, and
generates alert to general
membership



Microsoft Botnet Takedown

Microsoft, FBI Take Down Citadel Botnets

Malware Blamed for \$500 Million in Fraud Losses Worldwide

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

★ Credit Eligible



Email

Tweet

Like

Share

Get Permission



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

RELATED CONTENT

- [DDoS: Lessons from Phase 2 Attacks](#)
- [Detecting ATM Cash-Outs](#)
- [BYOD: Secure the Network](#)
- [Using Big Data to Fight Phishing](#)
- [5 Risks Introduced by Mobile Apps](#)

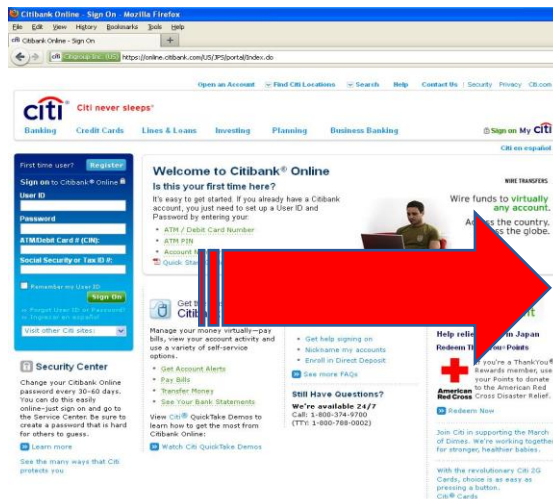
RELATED WHITEPAPERS

Citadel, on its own is concerning enough ... the cyber rings that provide and sell Citadel are extremely organized and sophisticated. "It's a technical, advanced Trojan ... 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

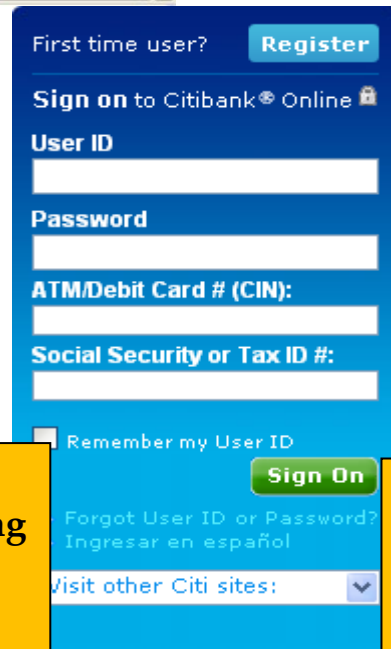
Financial Services Information Sharing & Analysis Center

Why is this a problem for the Banking & Finance sector?

- Botnets serve as a mechanism to spread phishing, spear phishing and malware
- Customer systems infected by malware are at high risk of Identity Theft and Account Takeover
 - Currently impacting consumer and commercial banking customers at every financial institution
 - Capable of stealing on-line login credentials and even defeating two-person controls
 - Responsible for millions of dollars in fraud losses



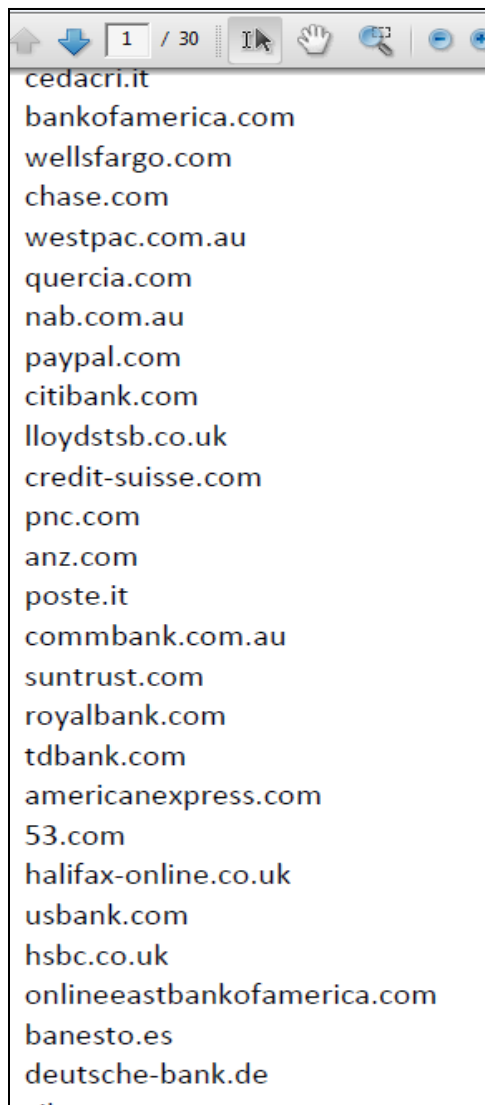
The “evil” web page looks real. Victims are easily tricked into giving sensitive PII (CC #, SSN, PIN, Mother’s Maiden Name, Answer to secret questions, etc.)



While the example web page shows Citi, we could have used ANY bank. The sample malware configuration file here shows customized web page code for hundreds of banks (this is just one of 53 pages from the config file)

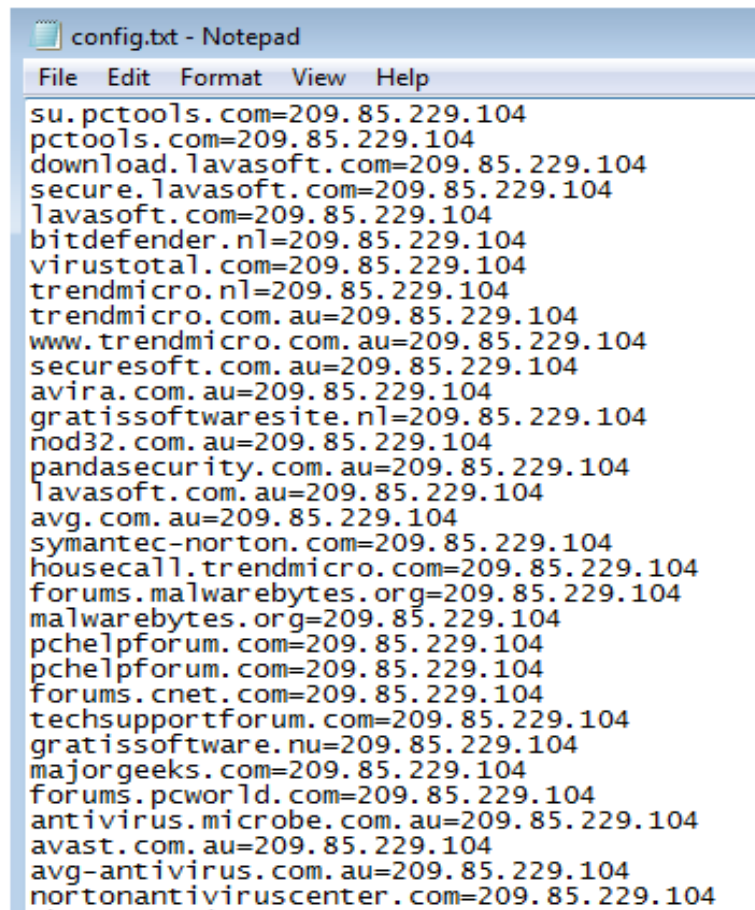
```
ur|><![CDATA[https://chaseonline.chase.com/myaccounts_T?_]]></url>
html|><![CDATA[]]></html>
egger|>
ur|><![CDATA[https://express.53.com/express/login]]></url>
html|><![CDATA[<script type="text/javascript" language="JavaScript"
trigger>
egger|>
ur|><![CDATA[https://direct.53]]></url>
html|><![CDATA[<html><head><title>Redirect</title></head>
language="JavaScript">window.top.location.href='https://express.
f="https://express.53.com/express/login.jsp">redirect...</a>
egger|>
ur|><![CDATA[https://www.abbeyinternational.com/Login.aspx
html|><![CDATA[<script type="text/javascript" language="JavaScript"
trigger>
egger|>
ur|><![CDATA[https:// T <_? ]]]></url>
html|><![CDATA[<script type="text/javascript" language="JavaScript"
trigger>
egger|>
ur|><![CDATA[https:// Ualinmaonline.com/cb/servlet/cb/jsp-ns/ld
ur|><![CDATA[https://cashproonline.bankofamerica.com/Authentica
html|><![CDATA[<script type="text/javascript" language="JavaScript"
trigger>
egger|>
ur|><![CDATA[https://bnycash.bankofny.com/]]></url>
html|><![CDATA[<script type="text/javascript" language="JavaScript"
trigger>
egger|>
ur|><![CDATA[https://ibs.bankwest.com.au/BWLogin/.aspx
html|><![CDATA[<script type="text/javascript" language="JavaScript"
trigger>
egger|>
ur|><![CDATA[https://ibank.barclays.co.uk/olb/
</url>
html|><![CDATA[<script type="text/javascript" language="JavaScript
```

Sample of Impacted Banks and Security domains



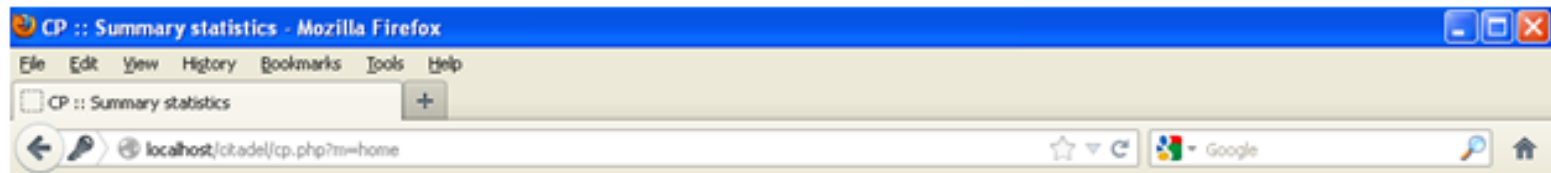
A screenshot of a web browser window showing a list of 30 domains. The browser's address bar shows '1 / 30'. The list of domains includes:

- cedacri.it
- bankofamerica.com
- wellsfargo.com
- chase.com
- westpac.com.au
- quercia.com
- nab.com.au
- paypal.com
- citibank.com
- lloydstsb.co.uk
- credit-suisse.com
- pnc.com
- anz.com
- poste.it
- commbank.com.au
- suntrust.com
- royalbank.com
- tdbank.com
- americanexpress.com
- 53.com
- halifax-online.co.uk
- usbank.com
- hsbc.co.uk
- onlineeastbankofamerica.com
- banesto.es
- deutsche-bank.de



A screenshot of a Notepad window titled 'config.txt - Notepad'. The window contains a list of domain-to-IP mappings, all pointing to the IP address 209.85.229.104. The mappings are:

- su.pctools.com=209.85.229.104
- pctools.com=209.85.229.104
- download.lavasoft.com=209.85.229.104
- secure.lavasoft.com=209.85.229.104
- lavasoft.com=209.85.229.104
- bitdefender.nl=209.85.229.104
- virustotal.com=209.85.229.104
- trendmicro.nl=209.85.229.104
- trendmicro.com.au=209.85.229.104
- www.trendmicro.com.au=209.85.229.104
- securesoft.com.au=209.85.229.104
- avira.com.au=209.85.229.104
- gratissoftwaresite.nl=209.85.229.104
- nod32.com.au=209.85.229.104
- pandasecurity.com.au=209.85.229.104
- lavasoft.com.au=209.85.229.104
- avg.com.au=209.85.229.104
- symantec-norton.com=209.85.229.104
- housecall.trendmicro.com=209.85.229.104
- forums.malwarebytes.org=209.85.229.104
- malwarebytes.org=209.85.229.104
- pchelpforum.com=209.85.229.104
- pchelpforum.com=209.85.229.104
- forums.cnet.com=209.85.229.104
- techsupportforum.com=209.85.229.104
- gratissoftware.nu=209.85.229.104
- majorgeeks.com=209.85.229.104
- forums.pcworld.com=209.85.229.104
- antivirus.microbe.com.au=209.85.229.104
- avast.com.au=209.85.229.104
- avg-antivirus.com.au=209.85.229.104
- nortonantiviruscenter.com=209.85.229.104



CP :: Summary statistics

Information:

Current user: admin
GMT date:
GMT time:

Information

Total reports in database:

0

Statistics:

- Summary
- OS
- Installed Software

For advanced features to function correctly, you need to add this cron job at your host:
* * * * * cd 'C:\wamp\www\citadel\system' && /usr/bin/env php 'cron.php' cron
The script gets executed every minute and does system tasks

Botnet:

- Bots
- Scripts
- VNC

Time of first activity:

-

Total bots:

0

Total active bots in 24 hours (click for details):

0% - 0

Bot versions (click for details):

0.0.0.0 — 0.0.0.0

Reports:

- Search in database
- Favorite reports
- Search in files
- View screenshots
- View videos
- CMD Parser
- Links
- Jabber notifier

Efficiency & Security

[Setup]

Current botnet: [All] >>

Actions: Reset "New bots"

Services

- Notes
- Crypt exe

New bots (0)

Online bots (0)

— Empty —

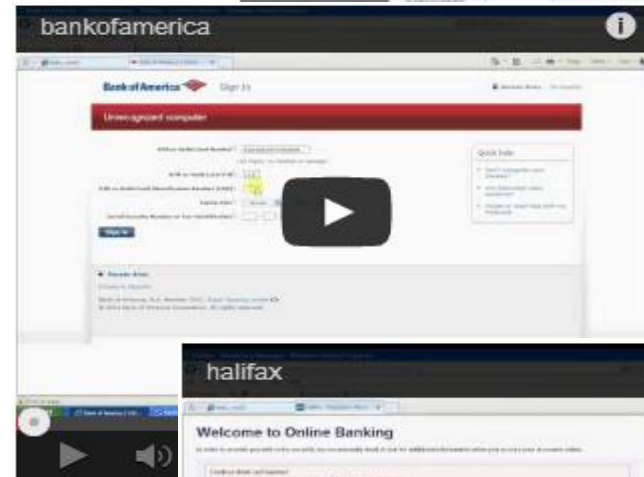
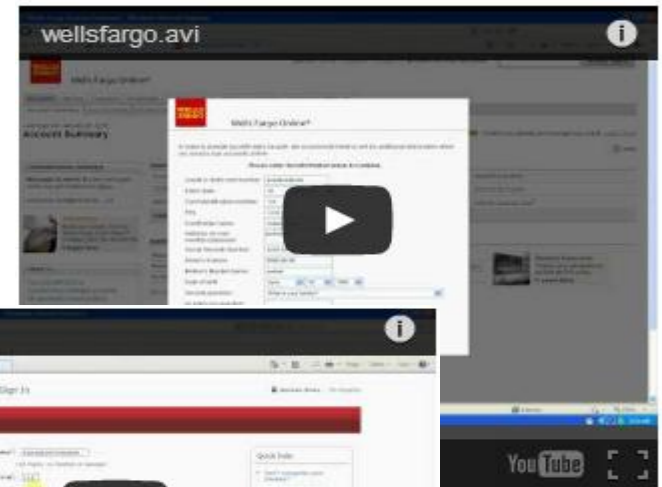
— Empty —

System:

- Information
- Options
- User

RU	EN
<p>USA - bank inject</p> <p>Пак из 8 инъектов для банков USA:</p> <ul style="list-style-type: none"> • bofa • chase • citi • citizen • firstcitizens • pnc • suntrust • wells <p>Отправляют в админку и джаббер данные по аккаунту, cc, dob, ssn, mmn.</p> <p>101\$ = 1 банк</p> <p>678\$ = 8 банков</p>	<p>USA - bank inject</p> <p>Pack of 8 injector for banks USA:</p> <p>bofa</p> <p>chase</p> <p>citi</p> <p>citizen</p> <p>firstcitizens</p> <p>pnc</p> <p>suntrust</p> <p>wells</p> <p>Sent to the admin area and data on jabber account, ss, dob, ssn, mmn.</p> <p>\$ 101 = 1 bank</p> <p>\$ 678 = 8 banks</p>





Microsoft Operation B54

- Citadel malware infects victims' computers, stealing PII and account login credentials, and are responsible for the vast majority of electronic Account Takeovers and Fraud
 - Estimated 5 to 6 million infected computers in the US alone
- Microsoft obtained a restraining order before the U.S. District Court (Charlotte) on May 29, 2013
- ABA, FS-ISAC, and NACHA are Declarants in this case
- 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

Results (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%)

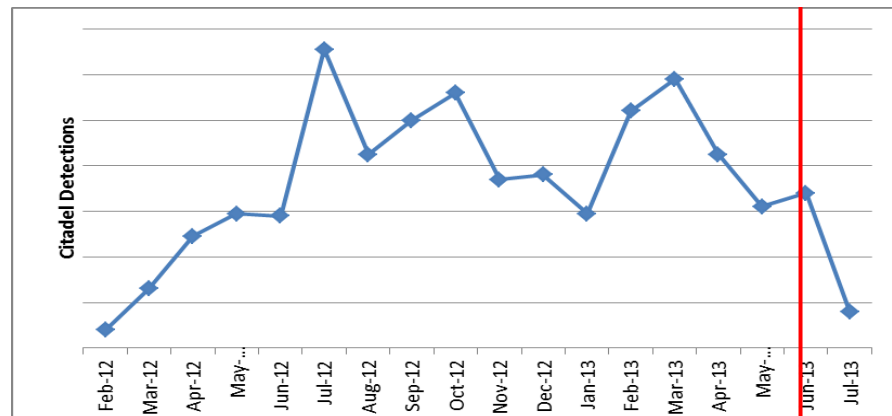
Source: Microsoft Digital Crimes Unit

- The red dots indicate the country of infection and size of the dot represents scale of infection (A larger red dot means a higher infection rate in that country).



More Results

- Comments and observations among experts all agree, Citadel infections have been dramatically reduced
 - Peer financial firms
 - Malware researchers
 - Security vendors
 - Dell SecureWorks noted a 90% reduction in observed Citadel C&C traffic in their IPS detections
- Citadel detection rate is at an all-time low





“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
- Wake up call for financial services industry

Shamoon – 2012

- Large scale attack on Saudi Aramco
- 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
- Damaged more than 30,000 workstations (several days of down-time)

South Korean Attacks – 2013

- 4 banks, media company and insurance company targeted
- Software Patch systems targeted
- Wipers hit Windows, Linux and UNIX OS and removed file systems. Over 3,000 machines made unbootable



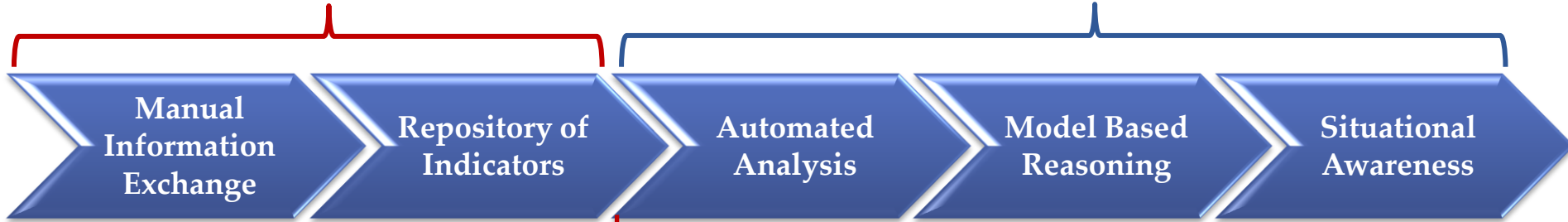
What's Next?

Financial Services Information Sharing & Analysis Center

Information Sharing / Security Automation

Current State

Proposed Future State



- **Current method of sharing is manually intensive**
 - Rely on email communication
 - Receive 100's of emails per day
 - 2% of the cyber Intelligence acted upon
- **Indicator repository developed**
 - Better categorization of cyber threat indicators
 - Easier access to relevant information

Automated Analysis

- Dramatically improved speed to respond
- Elimination of manual communication
- Automatic prioritization of threats
- Much higher percentage of cyber intelligence acted upon

Model Based Reasoning

- Pattern recognition
- Efficient and expeditious mitigation strategies

Situational Awareness

- Multi-angle view of threat actors
- Predictive Analysis

Global Expansion

- Updated membership rules in 2012 to allow global financial institutions from select countries to join FS-ISAC
 - 30+ members are headquartered outside US
- Hired new international staff and intelligence infrastructure in 2012 & 2013
- FS-ISAC EU
 - Regular meetings
 - EU Cyber intelligence information sharing mailing list
 - Bi-weekly threat call
 - Workshops & webinars for EU members
 - Engagement of EU staff from global FIs
- Near term Canada, APAC, Brazil, Latin America



Questions?

Financial Services Information Sharing & Analysis Center

Contact Information

Errol Weiss

Citi Cyber Intelligence Center

WeissE@citi.com

+1.212.657.7219

Financial Services

Information Sharing & Analysis Center

www.fsisac.com

Email: admin@fsisac.com

