



ACH FRAUD

James Craig
Special Agent
Omaha Division
Cyber Crimes Task Force



Agenda

- FBI Overview
- Cyber Investigative Priorities and Objectives
- Case Study



FBI Priorities

1. Protect the United States from terrorist attack
2. Protect the United States against foreign intelligence operations and espionage
3. **Protect the United States against cyber-based attacks and high-technology crimes**
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational/national criminal organizations and enterprises
7. Combat major white-collar crime
8. Combat significant violent crime
9. Support federal, state, local and international partners
10. Upgrade technology to successfully perform the FBI's mission



FBI Directive

- Pursuant to the National Strategy to Secure Cyberspace signed by the President of the United States, the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) lead the national effort to investigate and prosecute cybercrime.



Cyber Investigative Priorities and Objectives



Cyber Investigative Priorities

1. Counterterrorism Intrusions

2. Counterintelligence Intrusions

3. Criminal Intrusions

4. Online Child Exploitation

5. Intellectual Property

6. Internet Fraud



Cyber Division Strategic Objectives

Objective 1

Identify and neutralize the most significant individuals or groups conducting **computer intrusions**, the dissemination of malicious code, or other computer supported operations





Cyber Division Strategic Objectives

Objective 2

Identify and Neutralize Online Predators or Groups that **Sexually Exploit and Endanger Children** for Personal or Financial Gain





Cyber Division Strategic Objectives

Objective 3

Identify and neutralize operations targeting U.S. **intellectual property**





Cyber Division Strategic Objectives

Objective 4

Identify and neutralize the most significant perpetrators of **Internet Fraud**







Omaha CCTF

- Douglas County, Nebraska, Sheriff's Office
- Omaha Police Department
- Nebraska State Patrol
- Lincoln, Nebraska Police Department
- Sarpy County, Nebraska Sheriff's Office
- LaVista, Nebraska Police Department
- Office of the Nebraska Attorney General
- Iowa Division of Criminal Investigation
- Council Bluffs, Iowa Police Department
- Bellevue, Nebraska Police Department



Computer Intrusion ACH Fraud Case Study

Operation Trident
BreACH

International Cooperation Disrupts Multi-Country Cyber Theft Ring

October 01, 2010

FBI National Press Office (202) 324-3691

The FBI and international law enforcement, working in an unprecedented partnership, have disrupted a large-scale, international organized cybercrime operation active in several countries that resulted in numerous search warrants and arrests.

Operation Trident Breach began in May 2009, when FBI agents in Omaha, Nebraska, were alerted to automated clearing house (ACH) batch payments to 46 separate bank accounts throughout the United States. Agents quickly realized the scope of the crime and partnered with local, state, and federal partners, cybercrime task forces, working groups, and foreign police agencies in the Netherlands, Ukraine, and the United Kingdom to bring those responsible to justice.

The cyber thieves targeted small- to medium-sized companies, municipalities, churches, and individuals, infecting their computers using a version of the Zeus Botnet. The malware captured passwords, account numbers, and other data used to log into online banking accounts. This scheme resulted in the attempted theft of \$220 million, with actual losses of \$70 million from victims' bank accounts.

Ukraine Arrests Five Members of Botnet Ring

The [Security Service](#) of the Ukraine (SBU), in conjunction with the U.S. Federal Bureau of Investigation said Friday that the Ukrainian agency had detained five people of interest in a worldwide cybercrime investigation tied to the "Zeus" bot.

The FBI did not announce any arrests. However, Ukraine's SBU detained five individuals who were "key subjects responsible for this overarching scheme," the FBI said. Additionally, the SBU served eight search warrants.

Metropolitan Police cracks Zeus crime ring

Police Central e-crime Unit arrests 19 in dawn raids

Phil Muncaster, v3.co.uk 29 Sep 2010

The Police Central e-crime Unit (PCeU) has arrested 19 people on suspicion of using a well known malware program to steal millions from bank accounts, according to widespread reports.

The Metropolitan Police unit arrested 15 men and four women aged 23 to 47 in dawn raids on Monday in the London area. The gang is suspected of stealing up to £6m in just three months, according to the reports.

The gang reportedly used the Zeus trojan to infect PCs and record bank log-in details and other information, making it easy to remotely access accounts and transfer funds to bogus accounts.

Detective Chief Inspector Terry Wilson said that the force expects to find more stolen funds as the investigation continues.

"We believe we have disrupted a highly organised criminal network which has used sophisticated methods to siphon large amounts of cash from many innocent people's accounts, causing immense personal anxiety and significant financial harm, which of course banks have had to repay at considerable cost to the economy," he told the [Press Association](#).

"Arrests like the ones in London don't mean the end of Zeus as it continues to be available for sale to other criminals via underground web sites, but it's still good news for everyone interested in making the internet a safer place. So hats off to the PCeU."





© Robin Bell

Scammer





© Robin Bell



© Robin Bell



Elusive Malware Distribution

Virustotal. MD5: 49e15705a2e0ec46adcd1d2937d0f8ba9 Heuristic.BehavesLike.Win32.AdSpyware.H...


File Edit View History Bookmarks Tools Help

http://www.virustotal.com/analysis/192f00ecdbe776cf0085b7

Most Visited Getting Started Latest Headlines file:///I:/DCIM/100NC... hibernate cache - Goo... HPC-2000 Portable Pa...

Genlabs, In... GenLabs, In... Detail: Gen... remove stri... :: EVA - PH... Virust... Google

Nederlands | Ελληνικά | Français | Svenska | Português | Italiano | 繁體中文 | 简体中文 | Magyar | Deutsch | Česky | Polski | Español



Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

File **tax-statement.exe** received on **2009.09.17 15:42:17 (UTC)**
Current status: **finished**
Result: **5/41 (12.20%)**

[Compact](#) [Print results](#)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.24	2009.09.17	-
AhnLab-V3	5.0.0.2	2009.09.17	-
AntiVir	7.9.1.19	2009.09.17	-
Antiy-AVL	2.0.3.7	2009.09.17	-
Authentium	5.1.2.4	2009.09.17	-
Avast	4.8.1351.0	2009.09.17	-
AVG	8.5.0.412	2009.09.17	-
BitDefender	7.2	2009.09.17	-
CAT-QuickHeal	10.00	2009.09.17	-
ClamAV	0.94.1	2009.09.17	-
Comodo	2349	2009.09.17	-
DrWeb	5.0.0.12182	2009.09.17	-
eSafe	7.0.17.0	2009.09.17	-
eTrust-Vet	31.6.6743	2009.09.17	-
F-Prot	4.5.1.85	2009.09.17	-
F-Secure	8.0.14470.0	2009.09.17	-
Fortinet	3.120.0.0	2009.09.17	-
GData	19	2009.09.17	-
Ikarus	T3.1.1.72.0	2009.09.17	-

Find: group Next Previous Highlight all Match case Reached end of page, continued from top

Done FoxyProxy: Disabled



Example of Malware Distribution

FDIC malware distribution example

Personal Insurance File - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.fdic.gov.tygeraz.eu/bankinsured/failed/personalfile/holder.php?email=85c59b1f@askgk

PERSONAL INSURANCE FILE

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

PERSONAL INSURANCE FILE

OMB Number: 0164-013
Expiration Date:

Personal Insurance File

FDIC has officially named the bank you have opened your account with a failed bank, thus, taking control of its assets.

- Download and open your personal FDIC Insurance file to check your Deposit Insurance Coverage.
- The data in each file is self-extracting: download the file into an appropriate directory, and then run it.

File Title	File Number	File size
Personal FDIC Insurance file	FDIC 5210/09E	
Adobe® PDF file		105 kb
Microsoft® Word file		105 kb

FDIC 6422/04 (10-09)
Last Updated:

[Home](#) [Contact Us](#) [Search](#) [Help](#) [SiteMap](#) [Forms](#)
[Freedom of Information Act \(FOIA\) Service Center](#) [Website Policies](#) [USA.gov](#)
[FDIC Office of Inspector General](#)



Example of Malware Distribution

NACHA example

Unauthorized ACH Transaction - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://nacha.org.corefirstid4.com/ACHNetwork/Unauthorized/report.php?transaction_id=

Services | Risk Rating | New Site Rank: - Site Report [RO] SC Infoqate Telecom SRL

Unauthorized ACH Transaction

ACH Network | Home | About Us | Conferences | Publications | ACH Network | ACH Rules | Membership | News | Resources | Site Map

- ACH News
- AAP Program
- ACH Quality
- Operations Bulletins
- Calendar
- Regional Payments Associations
- Government Relations
- Direct Deposit
- Direct Payment
- Unauthorized ACH Transactions

Unauthorized ACH Transaction Report	
Your ACH transaction was rejected by The Electronic Payments Association (NACHA). Please carefully review the transaction report.	
Transaction ID:	ACH83569202050US
Date of Rejection:	
Reason for Rejection:	See details in the report below, issued by the Electronic Payments Association.
Transaction Report:	report-ACH83569202050US.exe (self-extracting, pdf format)

The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171



GOT MULE?

GOT MULE?

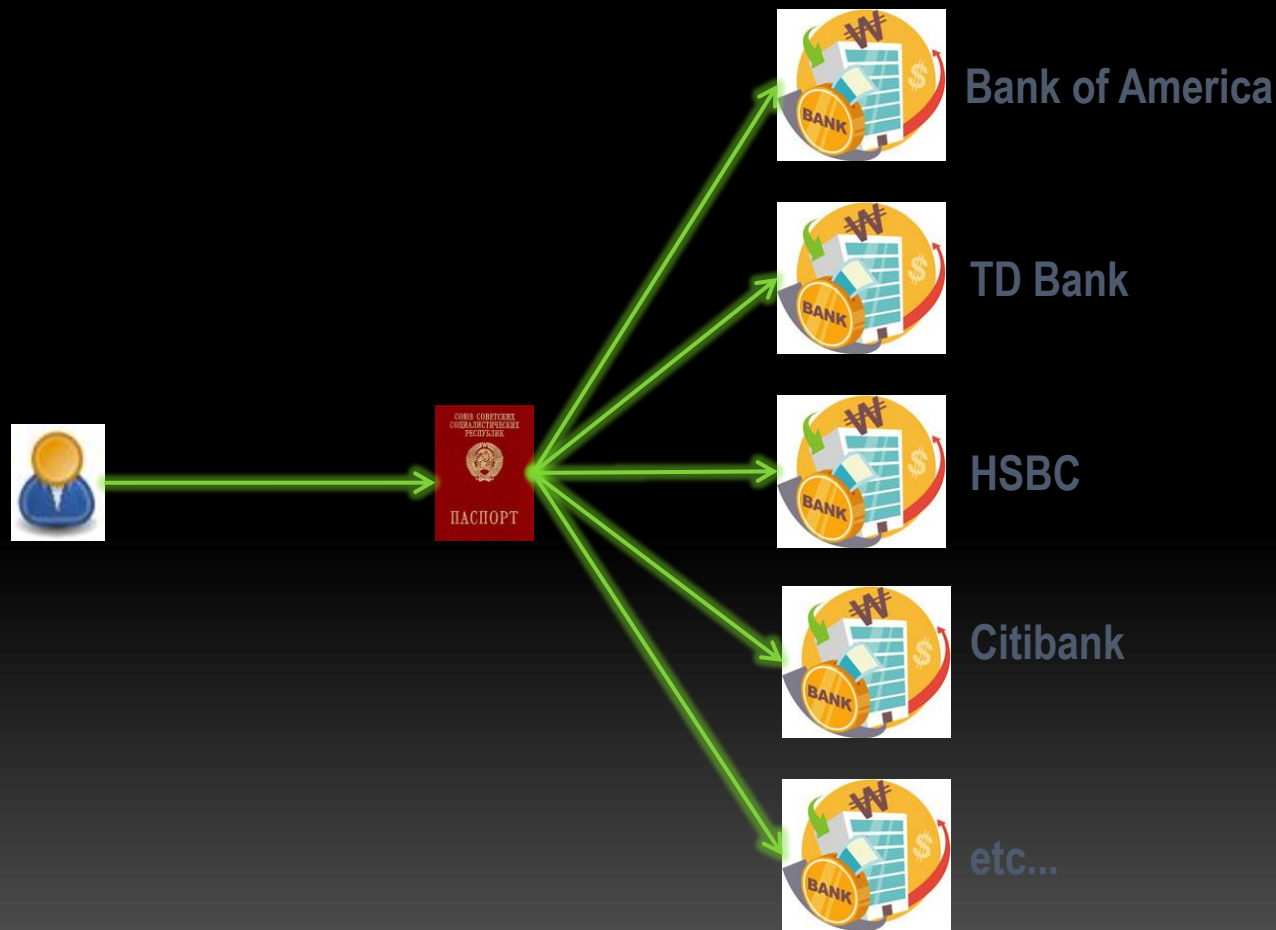


The money mule network?

- Work at Home Schemes
- Create at home business
- J1's



Simple J1 - one mule, five accts





Mule Recruitment Process

- Resume Posting sites
- Spam: “I found your resume on *blank*”
- Typically victim is recruited using forged emails sent through open form-mailers NOT from real recruitment system
- This context makes offer seem legit
- Mules directed to bogus websites to provide account details



Mule Cashout Process

- Criminals provides a list of mule accounts to 'Cashier'
- Cashier initiates ACH/Wire to mule accounts
- Typically < 10K per mule
- 2 hour cash out window
- Mule splits into three transactions at 3 different WU/MG offices
- Mule updates web site with WU/MG tracking numbers
- Funds picked up
- Next stop????



J1CO: Recruitment Process

- Word of mouth
- East European Social networking Websites



Ilya Karasev



Dmitry Saprunov



Lilian Adam



Marina Oprea



Kristina Izvekova



Sofya Dikova



Artem Tsygankov



Catalina Cortac



Ion Volosciuc



Artem Semenov



Yulia Klepikova



Maxim Panferov



Nikolai Garafulin



Dorin Codreanu



Julia Shpirko



Almira Rakhmatulina

Instant Corporations

LLC.com

from the experts at The Company Corporation

☎ 877-261-9606 Mon-Fri: 8 a.m.-9 p.m. ET Sat: 9 a.m. - 6 p.m. ET

[Order Status](#) | [Pay Invoice](#) | [Customer Service](#) | [Shopping Cart](#) Empty

HOME

LEARN ABOUT LLCs

FORM AN LLC

STARTING & GROWING MY BUSINESS

SEARCH

LLC.com helps you form your business *quickly* and *easily*.

Let us guide you through the process.



FORM AN LLC NOW

More with every formation...

- Expert customer service
- Fast filings in all 50 states
- Cheaper than an attorney

Get a Quick Quote Now

-- Select your home state --

Not sure where to form? [We can help](#)

Choose a State

We can help form your LLC in all 50 states!

[Delaware](#)

[Florida](#)

[Texas](#)

[Nevada](#)

[California](#)

[New York](#)

[New Jersey](#)

[Pennsylvania](#)

[SELECT ANOTHER STATE >](#)

Watch the new LLC 101 video

Thinking about forming an LLC?
Our new video tells you what
you need to know.

[WATCH LLC 101 NOW >](#)



Download our Free Guide to LLC formation

Our step by step guide shows
you all you need to know
about forming your LLC.

[DOWNLOAD IT NOW >](#)





Related Stats and Trends

- The FBI has over 300 active investigations on ACH fraud – majority of cases opened in last year.
- The FBI is opening 1-3 new cases per week.
- Over \$150 million in attempted losses stemming from ACH cases.
- Bank accounts associated with thousands of domestic, and J1 (student visa), money mules identified to date.



Combating the Enemy

- Foreign Relationships
- Training
- FBI Threat Focus Cells
- Cyber Crime Reporting and Cooperation Act. (S. 3155)
 - Identification of Threat Countries
 - Consultation
 - No Cooperation = Suspension, limitations and withdrawal of US Gov't provisions



"No one country, no one company, and no one agency can stop cybercrime. The only way to do that is by standing together. For ultimately, we all face the same threat. Together, the FBI and its international partners can and will find better ways to safeguard our systems, minimize these attacks, and stop those who would do us harm."

FBI Director Robert S. Mueller, III.



Partnerships

- Infragaurd
- Banking Enterprise
- CCTF

Thank You

