FBI CHALLENGES IN A CYBER-BASED WORLD

Federal Bureau of Investigation

Assistant General Counsel
Robert Bergida

202-651-3209

Overview

- Cyber Threats
- FBI Mission
- FBI Response

“Terrorism remains the FBI’s top priority. But in the not too distant future, we anticipate that the cyber threat will pose the number one threat to our country.”

Cyber Threat

- Verizon 2012 Data Breach Investigations Report

  - Exploitable weakness v. targeted attack

Key questions compliance officers should ask about cyber security practices in their organizations:

1. How do we track the information leaving our company and its destination?
2. How do we know who is really logging into our networks and from where?
3. How do we control the software running on our various devices?
4. How can we limit information that is voluntarily made available to a cyber adversary?

Cyber Threat

SEC Guidance10/13/11

- Costs of successful cyber attacks:
    - Remediation Costs
    - Increased cyber security protection costs
    - Lost revenues
    - Litigation
    - Reputational damage

- Potential duty to disclose cyber security risks and cyber incidents
    - Evaluate cyber security risks
    - account for prior cyber incidents – severity/frequency

State Data Breach Laws

FBI Core Values

Rigorous Obedience to the Constitution

Respect

Compassion

Fairness

Integrity

Accountability

Leadership

Cyber Division

Cyber Division Strategy

Identify and disrupt the most significant individuals, groups and foreign powers conducting computer intrusions, the dissemination of malicious code, or other nefarious computer supported network operations.

Identify and disrupt online predators or groups that sexually exploit and endanger children for personal or financial gain.

Identify and disrupt operations targeting U.S. intellectual property.

Identify and disrupt the most significant perpetrators of Internet fraud. .

Cyber Division

Cyber National Security

Cyber Crime/Computer Intrusion Investigations

Strategic Outreach & Initiatives

Cyber Intelligence Analysis

Cyber Partnerships and Alliances

Cyber Division

Cyber Partnerships and Alliances

NCIJTF

Cyber Crime Task Forces

InfraGard

Internet Crime Complaint Center (IC3)

Cyber Initiative and Resource Fusion Unit (CIRFU)

Cyber Division

InfraGard

Member represent businesses, academic institutions, state and local law enforcement agencies.

Managed locally by volunteer members across 86 national chapters who meet regularly with members – promote dialogue with the FBI

Member chapters are geographically linked to local FBI Field Offices and are supported directly by FBI SA InfraGard Coordinators, as well as nationally by FBI HQ Public Private Alliance Unit and the InfraGard National Members Alliance.

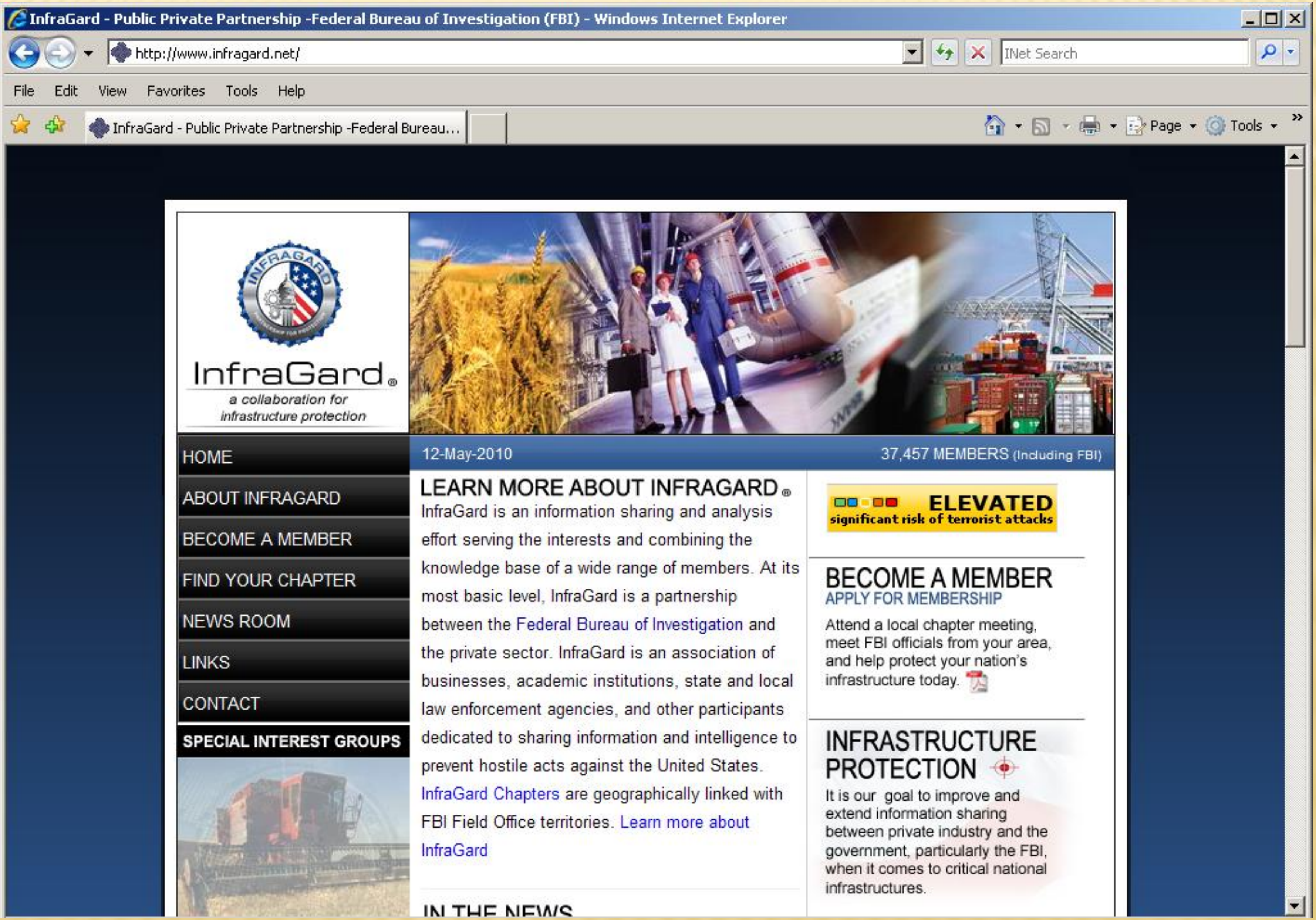
Better understand emerging trends

Open to US citizens and legal resident aliens 18 years and older from the private sector. All applications undergo an FBI vetting process.

50,000+ members – individual are members, not the organization to which they belong.

Web portal: www.infragard.org

InfraGard.net


InfraGard - Public Private Partnership -Federal Bureau of Investigation (FBI) - Windows Internet Explorer
http://www.infragard.net/
INet Search
File
Edit
View
Favorites
Tools
Help
InfraGard - Public Private Partnership -Federal Bureau...
Page
Tools
InfraGard®
a collaboration for infrastructure protection
HOME
ABOUT INFRAGARD
BECOME A MEMBER
FIND YOUR CHAPTER
NEWS ROOM
LINKS
CONTACT
SPECIAL INTEREST GROUPS

12-May-2010

37,457 MEMBERS (Including FBI)

LEARN MORE ABOUT INFRAGARD®

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Learn more about InfraGard

IN THE NEWS

ELEVATED
significant risk of terrorist attacks

BECOME A MEMBER

APPLY FOR MEMBERSHIP

Attend a local chapter meeting, meet FBI officials from your area, and help protect your nation's infrastructure today.

INFRASTRUCTURE PROTECTION

It is our goal to improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures.

Criminal Threats to Internet Users

- Cyber Extortion
  - Individuals threaten to use “Social Networking” power
  - Extortion-based DDoS attacks
  - Scareware/Fraudulent Antivirus Software
- Phishing
  - Ongoing case with major bank, 350 subjects identified, over 50 in a cooperating foreign country
  - 2000 phishing transactions totaling $4 million
- Botnets
  - Enable other criminal activity, Spam, distribution of additional Malware (Keyloggers, DNSChanger etc.)

One type of Cyber Extortion

a. *These things, unless you honor the below claim, WILL HAPPEN on March 8, 2010.*

b. *As you have denied my claim I can only respond in this way. You no longer have a choice in the matter, unless of course you want me to continue with this outlined plan. I have nothing to lose, you have everything to lose.*

c. *My demand is now for $198,303.88. This amount is NOT negotiable, you had your chance to make me an offer, now I call the shots.*

d. *I have 6 MILLION e-mails going out to couples with children age 25-40, this e-mail campaign is ordered and paid for. 2 million go out on the 8th and every two days 2 million more for three weeks rotating the list. Of course it is spam, I hired a spam service, I could care less, The damage [sic] will be done.*

e. *I am a huge social networker, and I am highly experienced. 200,000 people will be directly contacted by me through social networks, slamming your integrity and directing them to this website within days.*

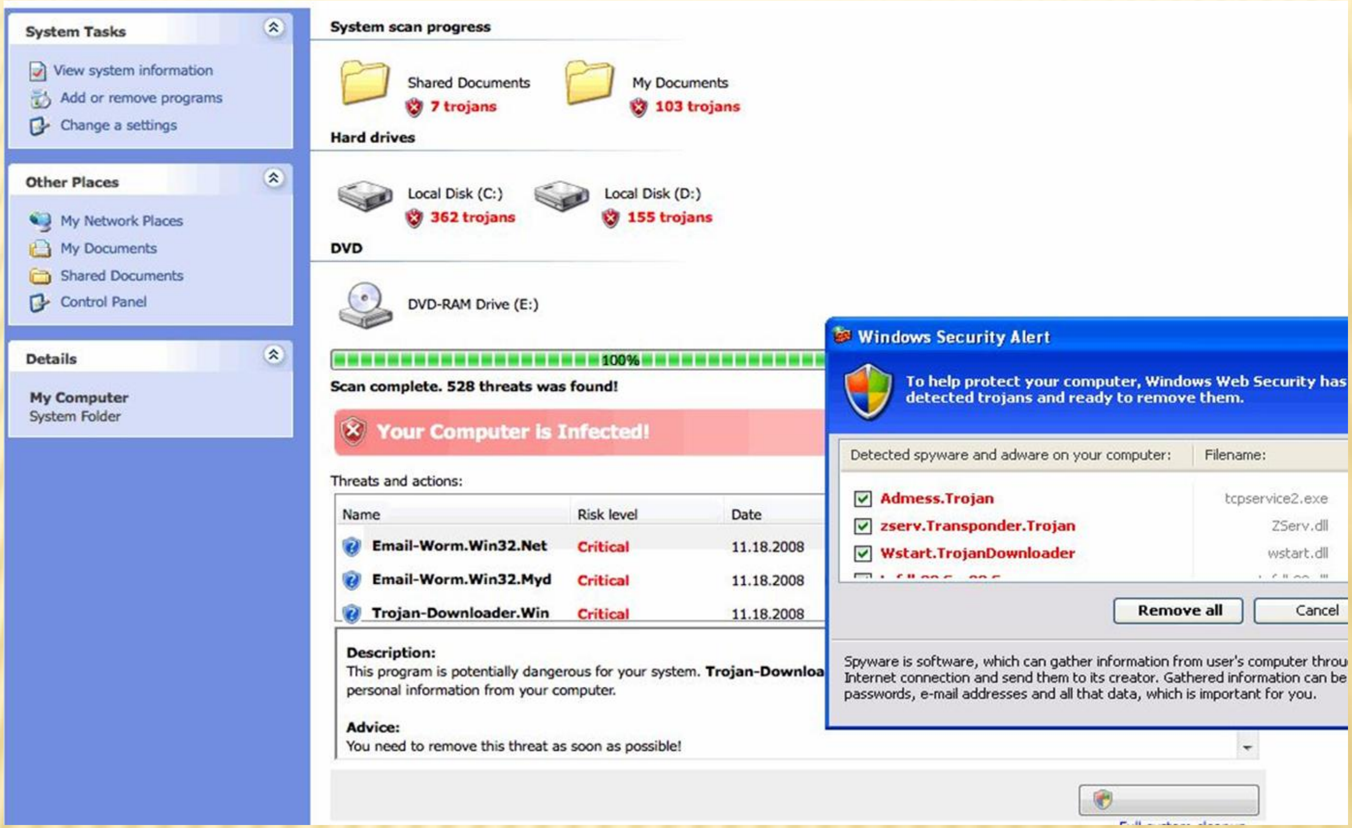
f. *I think you get the idea, I am going to drag your company name and reputation, through the muddiest waters imaginable. This will cost you millions in lost revenues, trust and credibility not to mention the advertising you will be buying to counter mine. Sad thing is it's almost free for me!*

g. *The process is in motion and will be released on March 8th, 2010. If you delay and the site goes live, The price will then be $3,000,000.00.*

DDoS Extortions

- Recent trend targeting online product retailers
  - Company receives an extortion threat via email, online chat or their 1-800 telephone number
  - Demand to “pay $,$$$ within five minutes or your website will be shut down…”
  - Many go unreported
  - Victims appear to be targets of opportunity
  - These tend to roll into Botnet investigations

Scareware – also a form of Cyber Extortion



System scan progress

Shared Documents
7 trojans

My Documents
103 trojans

Hard drives

Local Disk (C:)
362 trojans

Local Disk (D:)
155 trojans

DVD

DVD-RAM Drive (E:)

100%

Scan complete. 528 threats was found!

Your Computer is Infected!

Threats and actions:

Name	Risk level	Date
Email-Worm.Win32.Net	Critical	11.18.2008
Email-Worm.Win32.Myd	Critical	11.18.2008
Trojan-Downloader.Win	Critical	11.18.2008

Description:
This program is potentially dangerous for your system. **Trojan-Downloa**
personal information from your computer.

Advice:
You need to remove this threat as soon as possible!

Windows Security Alert

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

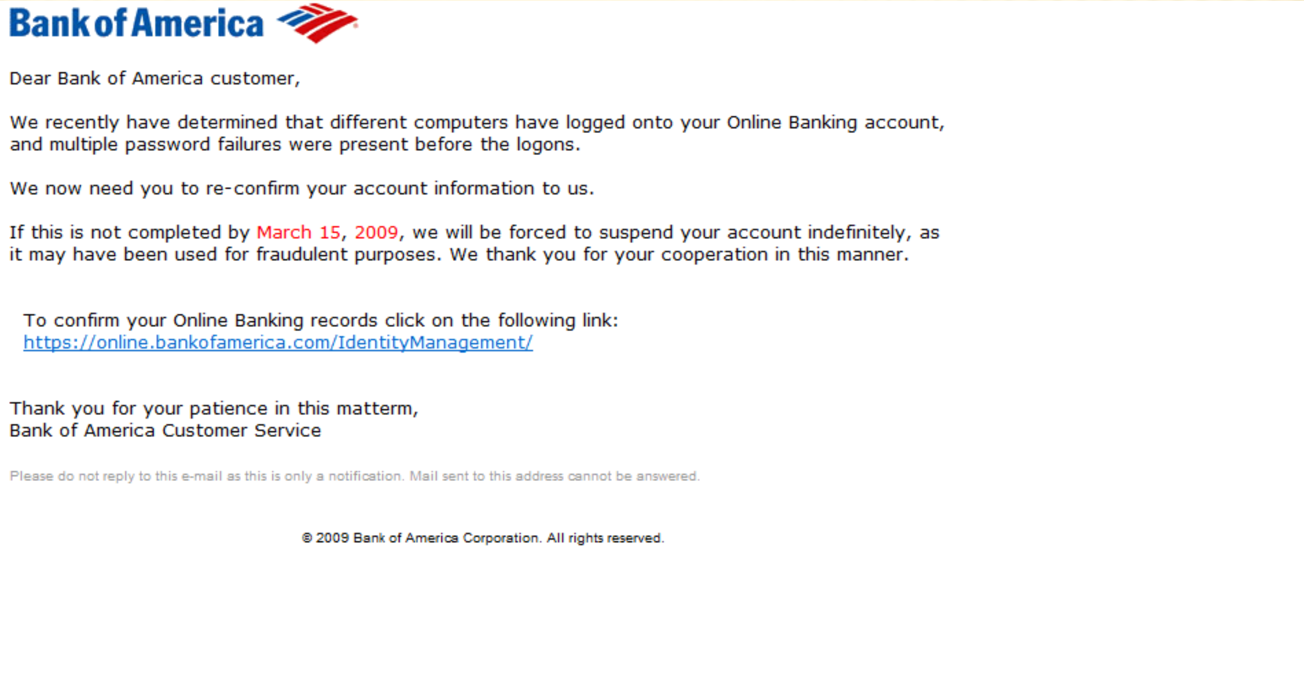
Detected spyware and adware on your computer:	Filename:
☑ Admess.Trojan	tcpservice2.exe
☑ zserv.Transponder.Trojan	ZServ.dll
☑ Wstart.TrojanDownloader	wstart.dll

Spyware is software, which can gather information from user's computer throu
Internet connection and send them to its creator. Gathered information can be
passwords, e-mail addresses and all that data, which is important for you.

Criminal Threats to Internet Users

- Cyber Extortion
  - Individuals threaten to use “Social Networking” power
  - Extortion-based DDoS attacks
  - Scareware/Fraudulent Antivirus Software
- Phishing
  - Comes in different flavors
- Botnets
  - Enable other criminal activity, Spam, distribution of additional Malware (Keyloggers, DNSChanger etc.)

Example of Phishing Emails Sent to Customers of U.S.-based Bank



Bank of America

Dear Bank of America customer,

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons.

We now need you to re-confirm your account information to us.

If this is not completed by March 15, 2009, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

To confirm your Online Banking records click on the following link:
https://online.bankofamerica.com/IdentityManagement/

Thank you for your patience in this matterm,
Bank of America Customer Service

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.

© 2009 Bank of America Corporation. All rights reserved.

Criminal Threats to Internet Users

- Cyber Extortion
  - Recent trend in Health Care Services Industry
  - Threatening to use “Social Networking” power
  - Scareware/Fraudulent Antivirus Software
- Phishing
  - Ongoing case with major U.S. banks, 350 subjects identified, over 50 in a cooperating foreign country
  - 2000 phishing transactions totaling $4 million
- Botnets
  - Enable other criminal activity, Spam, distribution of additional Malware (Keyloggers, DNSChanger etc.)

Coreflood

- Theft of private personal information from innocent users, including users on corporate computer networks

- Actions taken to mitigate the threat posed by Coreflood were the first of their kind in the United States

- DOJ/FBI working with Internet Service providers around the country

Example of Pervasive Malware – Keylogger

- Distributed via spam email, scareware or video codecs using social engineering techniques
- Records all keystrokes of victim
- Captures usernames, passwords, credit card numbers that victims type into webpages
- Information is stored in a hidden text file, compressed and retrieved by hacker

Example of Non-Pervasive Malware – DNS Changer

- Also can be distributed via spam email, scareware or social engineering techniques
- Modifies victims’ trusted Domain Name System (DNS) settings
- Victim computers then “unwittingly” get their domain name resolution from a DNS server controlled by the bad guy
- Bad guy then directs victim computers to his servers running lookalike web pages (i.e., a counterfeit online banking webpage)
- Victim unknowingly enters his banking credentials to what he thinks is the real web page…

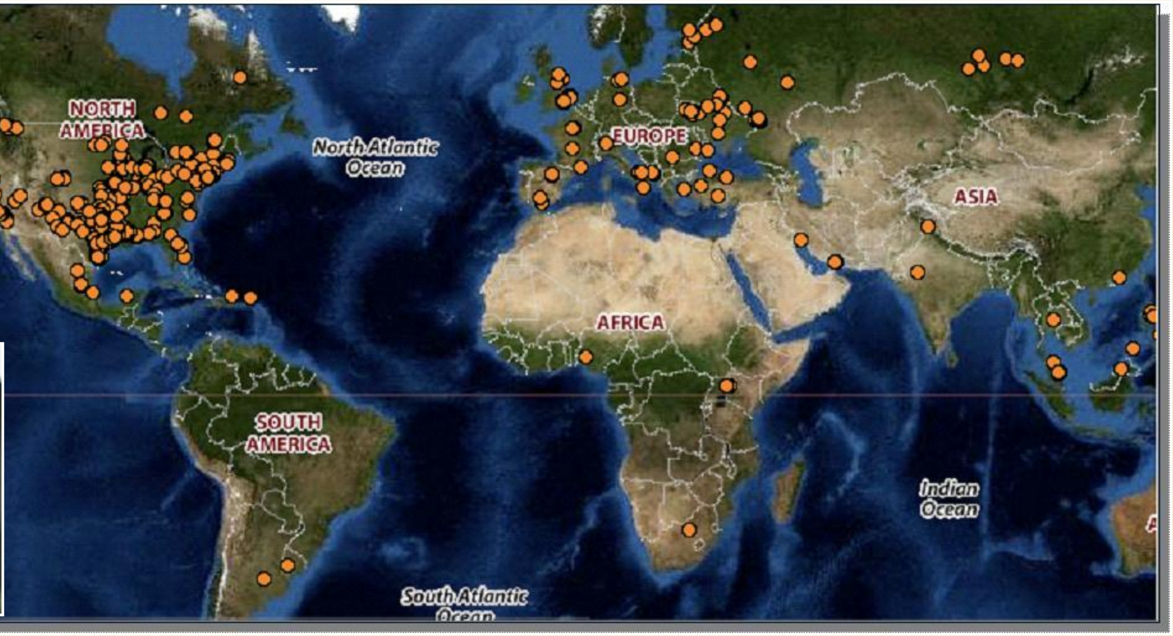
Criminal Threats to Internet Users

- Automated Clearing House (ACH) Transaction Fraud
    - Anyone with authority to pay, transfer funds, manage, control, or effect banking activity can be a victim

Financial Services Intrusion

Scope of the Scheme

- 15,730 attempted transactions worth $10.2M
- 14,544 successful transactions worth $9.7M
- $9.4M (97%) was withdrawn on Nov 8 2008
- 2,136 ATM terminals were accessed in over 28 countries



Cyber Terrorism

- No full-scale cyber attacks.
  - DDoS
  - Defacements
- Growing presence of terrorist organizations on the internet.
  - Internet being used not to just recruit or radicalize, but to incite.
- Growing use of social networking sites to collaborate and promote violence.

Counterintelligence and Economic Espionage

- Espionage used to be spy vs. spy.
  - Today our adversaries can sit on the other side of the globe and have access to an entire network at their fingertips.
- Who are they?
  - Nation-State Actors
  - Mercenaries for Hire
  - Rogue Hackers
  - Transnational Criminal Syndicates

Counterintelligence and Economic Espionage

- What are they after?
  - Technology
  - Intelligence (Policy-maker decisions)
  - Intellectual Property
  - Military Weapons
  - Military Strategy
- They have everything to gain; we have a great deal to lose.

Primary Intrusion Vectors

"The exploitation of Trust"

- The ***trusted*** inbound e-mail.
- The publicly available ***trusted*** web site of appropriate business interest.
- The download of ***trusted*** code from a ***trusted*** and authorized vendor.
- The ***trusted*** outward facing server.
- The necessary ***trust*** of the internal network
- The connections with ***trusted*** business partners.

FBI RESPONSE

- 56 Field Offices with Cyber Squads.
- 75 FBI Legal Attaché Offices and sub-offices around the world.
- Cyber Trained Agents embedded with foreign police agencies.

FBI RESPONSE

- National Cyber Investigative Joint Task Force
- Cyber Action Team
- Threat Focus Cells that are focusing on key threats and trends.
    - These groups consist of agents, officers, and analysts from different agencies.
    - Financial TFC, ICS TFC, Romanian TFC, Botnet TFC, Forums TFC

Threat Focus Cells

- FBI-led government-level working groups targeting high-threat issues, with a view towards the following:
  - Identify the Infrastructure – Understand the mechanics behind the Cyber threat
  - Victim Profiling – Assess how and why specific victims are targeted
  - Subject Identification – Identify malicious actors, methods, criminal histories
  - Consumer Identification – Malicious actors may be ‘sub-contractors’
  - Operational Development – Mitigation strategies

FBI RESPONSE

What the FBI won’t do

- Take over your systems.
- Repair your systems.
- Share proprietary information with competitors.
- Provide investigation-related information to the media or shareholders.