Cyber Security

Takin’ Care of Your Business

Agenda

- Espionage and Counterintelligence
- Extremist/Criminal Organizations
- The Threat to US Technology
- Cyber Threat Awareness for Business
- Why Do I Care
- TEST

FBI PRIORITIES

FBI boss says cyber crime, not terrorism, is top of Feds' todo list

FBI Director James Comey
February 2014
RSA Conference

What is counterintelligence?

Identifying, Penetrating and Neutralizing the

“SPY”

“Foreign Intelligence Activities” directed against a country’s national interests

Can also be an economic or scientific competitor!

COUNTERINTELLIGENCE THREATS

ISSUE THREATS

- Espionage (National Defense Information)
- Proliferation (Weapons of Mass Destruction)
- Economic Espionage
- National Information Infrastructure Targeting
- Infiltrating the U.S. Government
- Perception Management
- Foreign Intelligence Activities

Espionage:

Methods used to target technology

Unsolicited e-mails

Researchers and facilities relocated overseas

Front companies

Circumventing export control laws

Liaison with universities that have ties to defense contractors

Recruitment by foreign intelligence services

Visiting scientific and research delegations

Attending & hosting conferences

Hacking

Threat to US Technology

According to National Counterintelligence Executive (NCIX):

- 10 Core Countries involved in collection efforts against sensitive and protected US technologies – China and Russia most aggressive
- Foreign businessmen, scientists, engineers, and academics were active collectors
- The global economy gives foreigners unprecedented access to US firms and sensitive technologies
- Collectors increasingly make use of methodologies such as cyber attack and exploitation, which obfuscate their identities and goals

WHAT THEY ARE AFTER

- Classified information/research and development
- Inside information on federal and state government's policies and intentions toward their country
- Cutting edge U.S. manufacturing practices
- Business negotiation position – tax incentives, lowest price, capital improvements
- Business plan, plan for entering new markets, costs, liabilities, structure, contacts
- Personal information on key employees for targeting

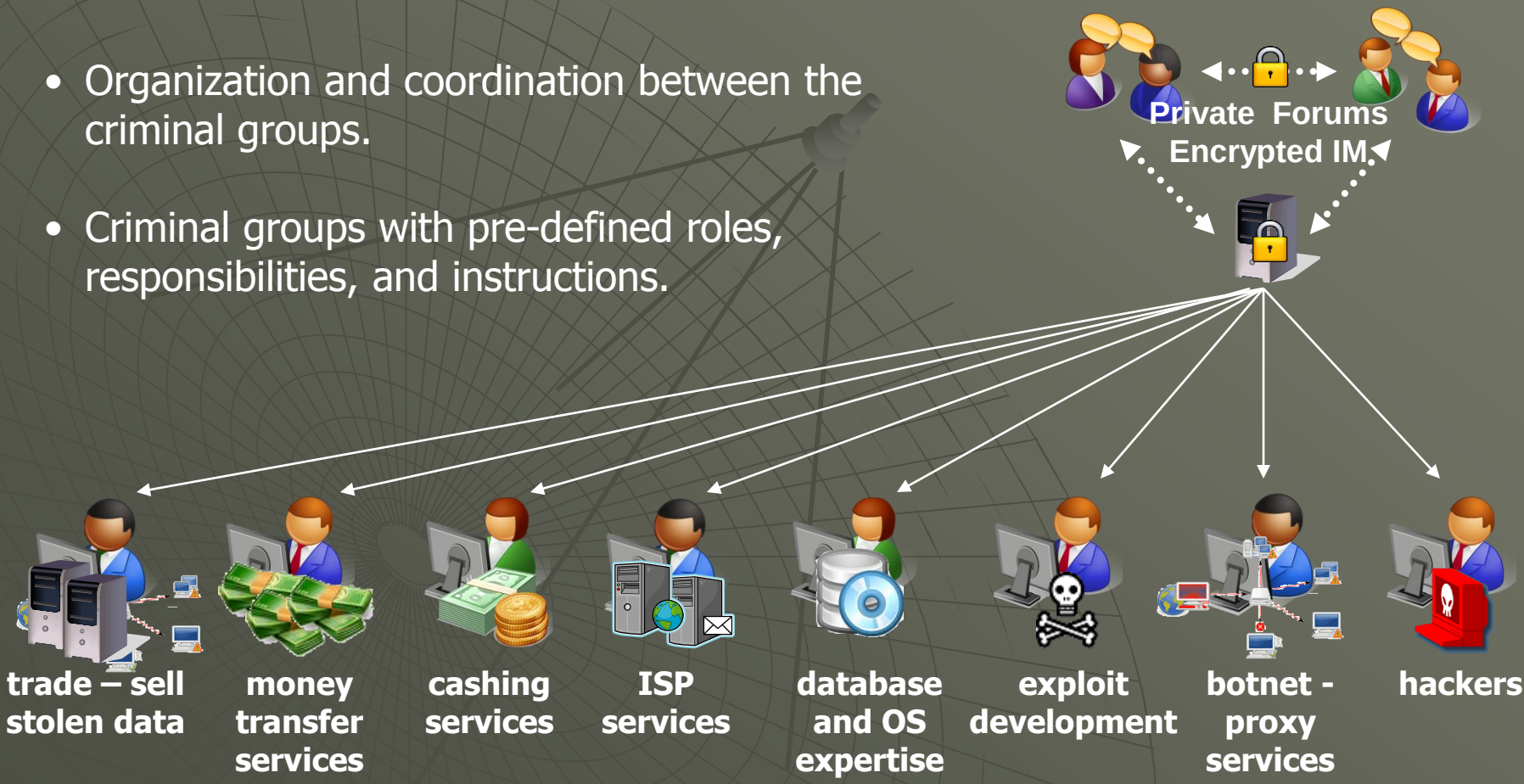
KEY FACTS:

- American businessmen and women traveling to a foreign country or engaged in international business are at an increased risk to be targeted by foreign competitors and by FIS
- FBI estimates that every year billions of U.S. dollars ($) are lost to foreign competitors who deliberately target economic intelligence in flourishing U.S. industries and technologies
- Many foreign government's believe that technology is the most important contributor to increasing their power relative to the U.S.
- The vast majority of foreign espionage is directed toward private sector, non-classified research and technology, products and trade negotiations.

The Eastern European Criminal Model

The Criminal Enterprise

- Organization and coordination between the criminal groups.
- Criminal groups with pre-defined roles, responsibilities, and instructions.



EXTREMIST USE OF CYBERSPACE

- The Internet offers an ability to exchange private communications and broadcast propaganda with anonymity, often over large distances when face to face meetings are not possible

- Can be used to distribute training resources, conduct training operations, fund raising and money laundering activity

USG vs. The Cyber Threat

- Over 12,000 cyber incidents against USG networks in 2007, over 18,000 in 2008
- A recognition that the offensive capabilities currently outpace defensive measures
- Sophisticated Cyber threats require a consolidated response: 01/08/2008 Executive Order "The Cyber Initiative;" current administration continues cyber emphasis
- US Cyber Command: DoD's command to direct operations in the cyber domain; effective October 2010
- Public/private partnerships and outreach are key to a successful defense

Foreign Cyber Threat- Methods

- Insider with network access
- Removable storage media
- Laptop computers and travel
- Remote access
- Network Intrusions and Botnets
- Email- spear phished and unsolicited
- Supply Chain
- Virtual Worlds and online networking

Social Engineering and the Trusted Insider

- Employees victims of social engineering
- Senior financial manager spearphished resulting in malware download
- Scientist inserts thumb drive after Asian trip resulting in data exfiltration

Example of a Potential Foreign Intel Threat

- BusinessWeek, 04/10/2008: Booz Allen Hamilton executive received email containing malicious code
- Email appeared to originate at the Pentagon, and was consistent with the executive's work
- Code would have established keylogging capability, backdoor functionality to a computer in China
- USG and defense contractors are targeted frequently- check out the article online, "The New E-spionage."

WHY WE CARE
Continuing Cyber Threats

- **Spear Phishing** – emails appear to come from a trusted source and seek unauthorized access to confidential data
- **Whaling** – spear phishing directed towards the executives of a company – often contain malware which can copy keystrokes to gain sensitive information
- **Social Engineering** – use of a ruse that relies on human interaction; tricking someone to break security procedures. Easiest and most common way a hacker can access your network

(Continued)

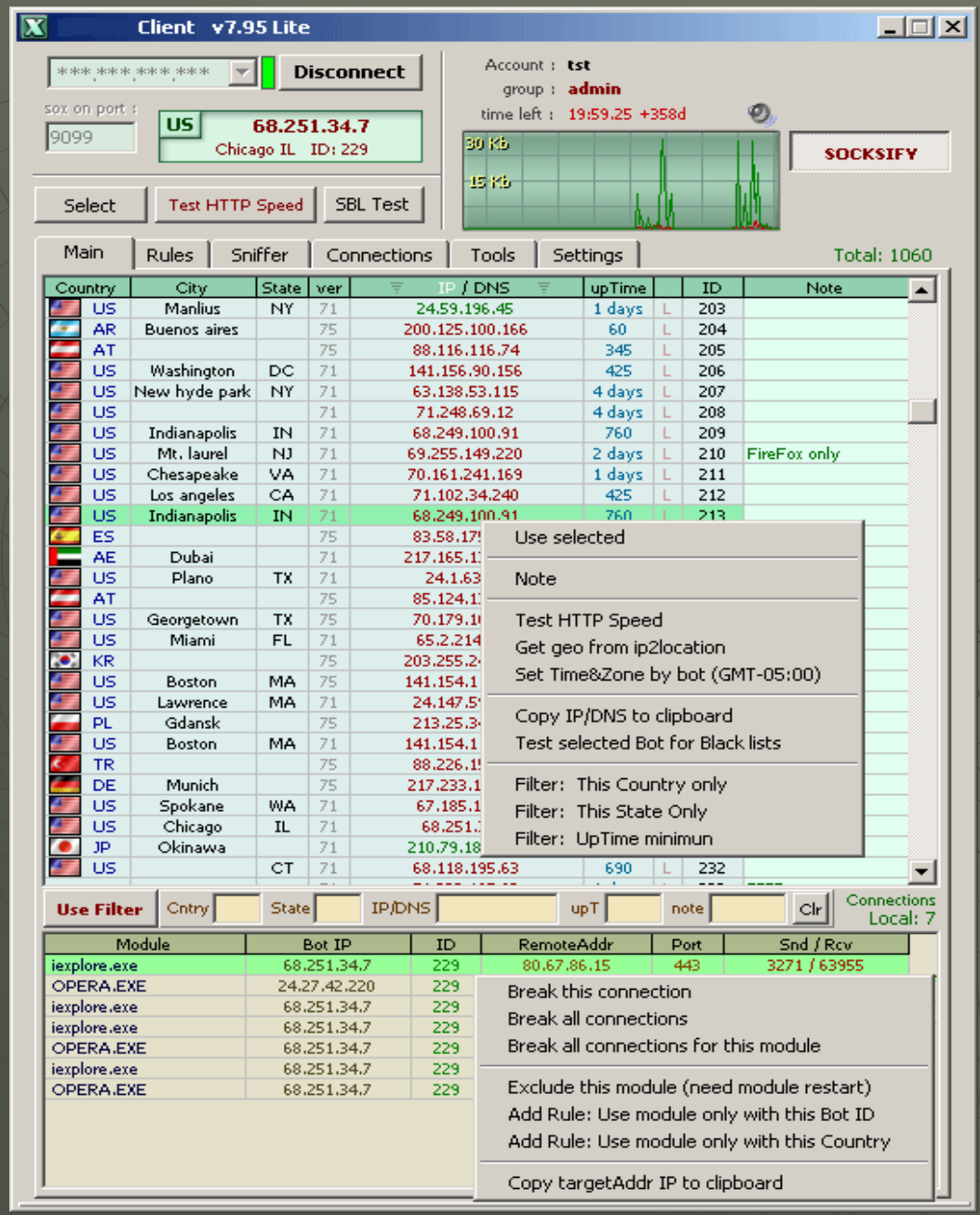
- **Spotting the Spear Phished Email:**
- "From" address may be inaccurate or misspelled
- May contain poor syntax or grammar
- May be "job-centric"!
- Contains a hyperlink or attachment
- Hyperlink or attachment may not match content of message
- May cause slow system performance, hangups
- If in doubt, pass to IT Security for review

(Continued)

BOTNETs – A network of compromised computers remotely controlled and used to create and send spam or viruses or flood a network with messages as a denial of service attack.

An effective force multiplier- recall the Russia-Georgia conflict of 2008

Can your organization perform its research if denied access to your network, or your data was compromised?



Botnet Tools: so easy!

Cyber Threats

Laptop computers and travel:

- Based on destination, laptop may be targeted for exfil or compromise
- Take only what you need on the laptop
- Safes are not safe
- Use caution in use of removable media
- Use caution in use of network connections, particularly wi-fi
- Consider use of a travel image

Cyber Threats

Remote access

- Convenient- for you and a hacker
- Follow organizational IT guidance on remote access if used
- Keep home stuff on home computer, work stuff on work computer
- At home, are you the only user of the work computer?

Cyber Threats

Supply Chain:

- Even "USA" manufactured equipment contains foreign built boards
- Computers, routers, WAPS, keyboards, Removable media, software subject to compromise
- Product assurance a daunting task; as a consumer or user be aware of where your equipment was made, research product
- If in procurement, ask the tough questions with end use in mind (R & D or admin?)

Cyber Threats

Unsolicited Email:

- You're "kind of a big deal" on the internet
- Unsolicited contacts a real threat to research, and it's through the front door.
- Academic exchanges are great- even essential- for progress, but be aware of the tipping point where queries or relationships turn sensitive- you'll know it when you see it in your area of research

Cyber Threat - Virtual Worlds

Virtual worlds provide opportunities for extremists, criminals and FIS to conduct malicious activities that pose moderate national security and cyber threats

Cyber Threat – The Virtual Worlds

Virtual World – A computer simulated environment in which multi-national users interact with other users across the Internet using avatars (a 2- or 3-D representation of a user).

Online Gaming- World of Warcraft, Club Penguin, Virtual Magic Kingdom, Xbox and game consoles

Networking Sites- Facebook, LinkedIn

Online Resume - Monster, Careerbuilder

Cyber Threat - Virtual Worlds

Activities include:

Committing financial crimes
Identity theft
Trade of child pornography
Spreading malware
Launching certain types of cyber attacks
Covert communications
Recruiting members into extremist or criminal groups, training, spreading propaganda, and conducting intelligence and espionage activities.

Cyber Threat - Virtual Worlds

Your Online Presence:

Google yourself and your organization to gauge your cyber profile

Online resumes, research papers and biographies sell your skills to FIS as well as the academic community

Be cautious of new contacts- you can Google them too, and make a phone call if warranted

Cyber Threat- Network Defense

- Defense in Depth vs “Hard Shell”
- Disable physical ports not in use
- Monitor outbound traffic anomalies
- Maintain current software patches
- Enable logging, archive it remotely
- Consider laptop and media scrub policy

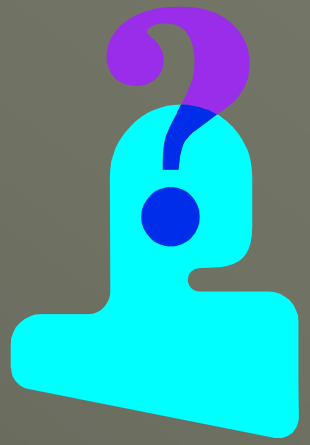
Cyber Threat- Network Defense

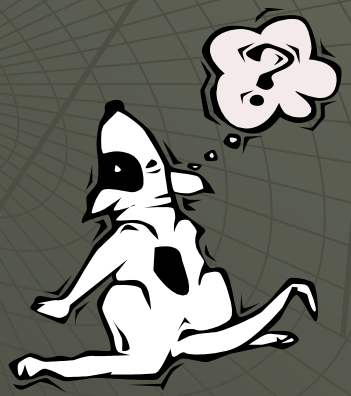
- Use and update antivirus programs
- Employee education
- Implement and enforce computer user policy and banner at user login to remind employees of policy
- Consider pros/cons of remote network access
- Use Web proxies where possible

Cyber Threat- Network Defense

- Consider white list of applications used on network
- Consider air gapping R and D networks from other business lines
- Employ IDS
- Encrypt

QUESTIONS





TEST

1. The FBI says cyber crime is second only to terrorism in terms of national priorities.
2. Most of the data sought is classified government information.
3. Mixing home and work on the same computer is a good idea.
4. Phishing defines attacks against the senior most executives and officers of a company

5. Conferences are a good place to collect competitor data.
6. Collectors increasingly make use of methodologies such as cyber attack and exploitation, which obfuscate their identities and goals.
7. Business losses by cyber sources are not significant

8. New thumb drives are safe.
9. Home wifi networks are safe within the home.
10. Patching computer systems is a critical step to protecting information.