The FBI and the Internet

Special Agent Robert Flaim
Federal Bureau of Investigation

Unclassified
Presentation Goals

- To give you a better understanding of:
  - The FBI Cyber Division, its priorities, and its mission
  - The use of technology within the FBI Cyber Division to solve Federal violations
FBI Priorities

1. Protect the US from terrorist attacks
2. Protect the US against foreign intelligence operations and espionage
3. Protect the US against cyber-based attacks and high-technology crimes
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational and 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 Cyber Division

- Created Fall 2002
- Primary goal - to enhance the FBI’s capability to protect the US against cyber based attacks and high tech crime
- Cyber Squads active in all 56 FBI field offices
FBI Cyber Priorities

- Criminal cyber threats
  - Intrusions
  - Intellectual Property Rights
  - Child pornography
  - Internet Fraud and identity theft (phishing, spam)
  - Other computer based or computer facilitated criminal activity

- Threats from terrorist organizations to computer networks and architecture
Cyber Division

Two Different Approaches

- **Traditional**
  Crime that has migrated to the Internet

- **Non-Traditional**
  Activity that was not a concern prior to the World Wide Web and the Internet
Cyber - Traditional

- Cyber Crime Investigations
  - Child pornography
  - Phishing, spam
  - Terrorism
  - Fraud
  - Slave trade
  - Theft of Intellectual Property (IPR)
  - Stalking
  - Sale of drugs or other contraband
Cyber - Non-Traditional

- **Computer Intrusion Investigations**
  - Distributed Denial of Service (DDoS) attacks
  - Malicious code (viruses, worms, trojans)
  - Botnets and Pharming
  - Malicious intrusions into computers/ networks
- **National Security Threats**
  - Cyber Terrorism

Unclassified
Use of Technology

• The FBI uses many of the same publicly available technologies to identify, monitor, capture, and prosecute the criminals the criminals use, such as:
  – Domain & IP WHOIS queries
  – DNS
  – VOIP
  – Email, Instant Messenger, & IRC
  – Encryption
  – Google
  – And many others
Technology Use Example

WHOIS ⇄ Directory Services
WHOIS

- IP and domain name WHOIS information is an integral tool for all cyber investigations
- These tools provide gap analysis, target profiling, and sometimes even identification
- Speed and accuracy in getting the data is key
WHOIS - Investigative Use

- Mytob/Zotob worm
- 9/11 and Anthrax Investigations
- Multiple kidnappings
- Child pornography – Innocent Images
- Many other including phishing, botnets, pharming, IPR, Internet gambling, and Internet fraud related investigations
ICANN Luxembourg 2005

• Law Enforcement session
• Reps from Australia, Spain, Malawi, UK, Japan, Interpol
• Importance of accessible and accurate WHOIS
International Association of Chiefs of Police

- 27 September 2005 issues Resolution advocating continued access to publicly available databases.
- Consult with law enforcement to assist in the resolution of potential conflicts, i.e., privacy regulation, business concerns, data-mining prevention efforts before removing to restricting access to this information
