

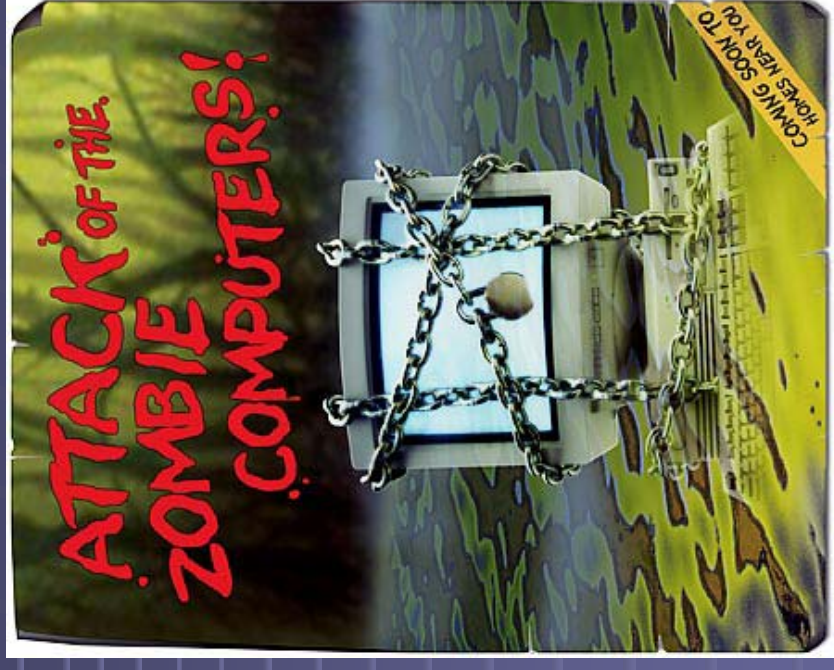
Malware

Law Enforcement and Industry Challenges

Anthony V. Teelucksingh
Computer Crime and Intellectual Property Section
United States Department of Justice

The Problem

- Use of malware for financial fraud, identity theft, and other criminal conduct
- Primary example is the bot computer
- Not only a law enforcement problem



Widespread and Growing

- Malware (botnets) has become the “plumbing” for the commission of numerous computer crimes
 - Fraudulent “ad-ware” installs
 - Identity theft
 - Credit card and bank fraud
 - Trade secret theft
 - Denial of Service attacks
 - Spam
- Rate of compromise appears to be increasing
- Financial theft is quickly becoming the dominant motive for malware attacks

Who is targeted for infection?

- Consumer machines without corporate firewalls, security procedures, low awareness
 - DSL/cable means high bandwidth
- Corporate machines
- University machines
- Financial institutions

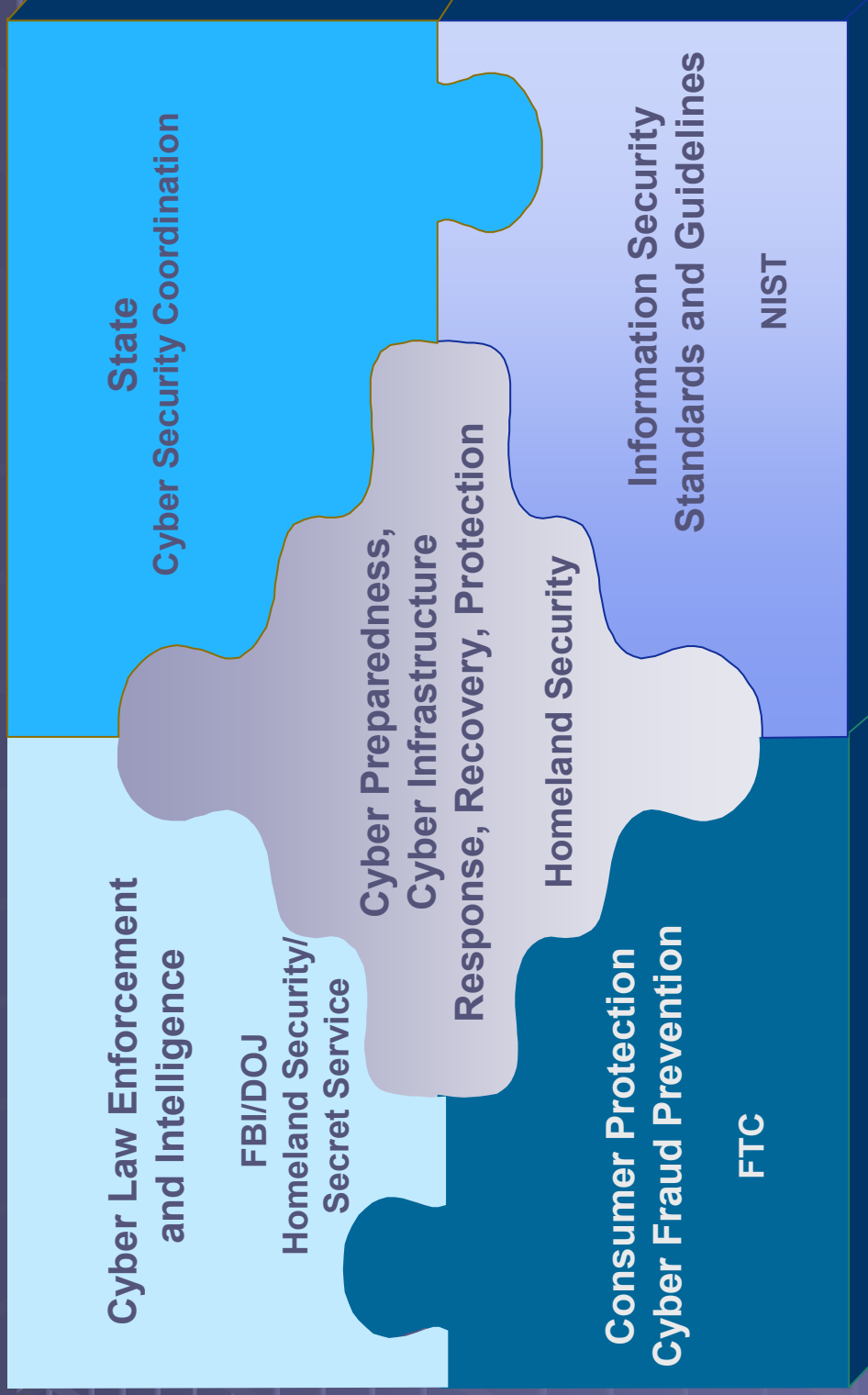
The Challenge

- Identify the individual(s) responsible for
 - Releasing malware on the Internet
 - Creating and maintaining botnets
- Organized groups increasingly behind malware transmission
 - Located in different economies with diverse legal systems
 - Conduct may not be criminalized in every jurisdiction
 - Technical challenge to coordinate the “takedown” of the botnet infrastructure
- Remediation of the infected machines

What do we need?

- Enact criminal laws applicable to malware attacks
- Legal tools that authorize investigation
 - Council of Europe's Convention on Cybercrime
- Training
 - Investigative techniques and best practices
 - Judge and prosecutor training
 - Commit adequate personnel and resources
- Information sharing
 - Criminal leads and referrals
 - Criminal intelligence sharing
- Cooperation
 - Prompt exchange of evidence and other data
 - Joint investigations where appropriate

Government's key cyber roles



Domestic Cooperation (U.S.)

- INFRAGARD
 - goal to improve and extend information sharing between private industry and the government, including law enforcement, when on threats to critical national infrastructures
 - Industry members pledge confidentiality on shared information
 - Key vector for providing law enforcement with industry data on attacks and losses
 - 84 Chapters with more than 16,000 members (8/06)
- Multi-stakeholder response teams, including US-CERT, law enforcement, and executive branch leadership

International Cooperation

- Botnet Task Force
 - Consists of law enforcement members from approximately 25 (and growing) economies, and cooperative industry members, i.e. Microsoft, various ISPs, anti-virus researchers
 - Many APEC economies participate
 - Next meeting is in Sydney, Australia (June, 2007)
 - Purpose is to share criminal intelligence on botnet problem
 - Provides training on malware investigations
 - Includes academic partners and CERTs
- FIRST (Forum on Incident Response and Security Teams)
 - Now includes a law enforcement module
- G-8 24-7 network for hi-tech investigative assistance
- Regional agreements
 - ARF on Cybersecurity

Enforcement Examples

- Numerous domestic investigations underway
 - Two convictions for bot activity
 - Pursuing additional cases this year
- Significant enforcement action overseas
 - Moroccan and Turkish borderers and virus writers arrested and prosecuted
 - Dutch takedown of a botnet in excess of 1 million machines
 - Additional actions expected this year

Further Information

<http://www.cybercrime.gov/intl.html>

anthony.teelucksingh@usdoj.gov



WWW.CYBERCRIME.GOV

Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice