Legal Foundation and Enforcement: Promoting Cybersecurity

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection

February 19, 2008

Mark L. Krotoski
Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division

Legal Foundation & Enforcement Overview

- Laws
- Global Enforcement Reach
- Investigation
- Prosecution/Criminal Justice System
- Effective Networks/Cooperative Partnerships

Legal Foundation & Enforcement

- What is the role of the legal foundation and enforcement in cybersecurity?

- Cornerstone
  - Provide framework to investigate, prosecute and deter cyber crime
  - Promote Cybersecurity
  - Confidence In Legal Systems
  - Encourage Commerce

Legal Foundation: Laws

- Challenges/Barriers
  - New methods of attack
  - More sophisticated crime
  - Organized Crime
  - International Dimension

Recent Trends

- Increasingly Sophisticated Web Site Attacks That Exploit Browser Vulnerabilities - Especially On Trusted Web Sites
- Increasing Sophistication And Effectiveness In Botnets
- Cyber Espionage Efforts By Well Resourced Organizations Looking To Extract Large Amounts Of Data - Particularly Using Targeted Phishing
- Mobile Phone Threats, Especially Against iPhones And Android-Based Phones; Plus VOIP
- Insider Attacks
- Advanced Identity Theft from Persistent Bots
- Increasingly Malicious Spyware
- Web Application Security Exploits
- Increasingly Sophisticated Social Engineering Including Blending Phishing with VOIP and Event Phishing
- Supply Chain Attacks Infecting Consumer Devices (USB Thumb Drives, GPS Systems, Photo Frames, etc.) Distributed by Trusted Organizations

Source: http://www.sans.org/press/top10menaces08.php

Greater Sophistication

"Today's attackers are increasingly sophisticated and organized, and have begun to adopt methods that are similar to traditional software development and business practices."

- Increased professionalization and commercialization of malicious activities
- Threats that are increasingly tailored for specific regions
- Increasing numbers of multi-staged attacks
- Attackers targeting victims by first exploiting trusted entities
- Convergence of attack methods

Source: Symantec Internet Security Threat Report: Trends for January – June 07 (Published September 2007)

Malicious Code By Type

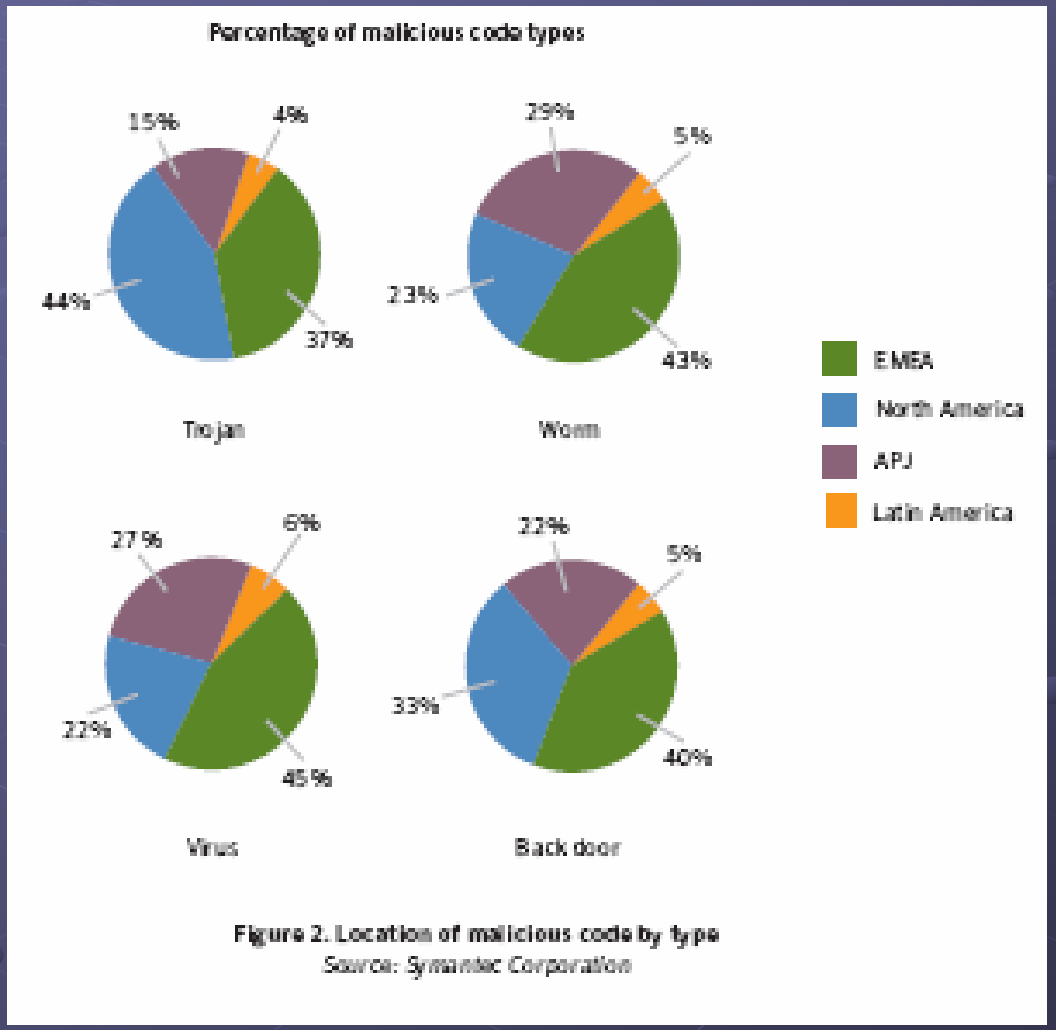


Figure 2. Location of malicious code by type
Source: Symantec Corporation

Legal Foundation: Laws

- Laws
  - Updated
  - Sufficient for present cybersecurity needs
  - Address core substantive and procedural areas
- Global Enforcement Reach
  - Address domestic Needs
  - International Cooperation
  - Coordination

Legal Foundation: Laws

- Convention on Cybercrime
- www.COE.int/cybercrime
  - Framework
  - Substantive Crimes
  - Procedural Rules
  - International Cooperation
- CCIPS Review Of Law Drafts
  - Betty.Shave@USDOJ.gov
  - (202) 514 1026

Investigation

Questions to ask:

- What is the ability of investigators to:
  - Follow criminal leads?
  - Collect and preserve evidence?
  - Find, apprehend the perpetrators?
- Where other countries are involved, how long will it take?

Investigation

- Specialized Training
  - Obtaining Electronic Evidence
- Cooperation
  - Mutual assistance processes

Prosecution

- Enforce Criminal Law
  - Admit evidence in court
  - Deterrence
  - Punishment
- Criminal Justice System
  - Train judges

Effective Networks/Cooperative Partnerships

- International Partnerships
- Governments
  - National
  - State and Local
- NGOs
- Industry/Private Sector
  - Assisting investigation
  - Reporting crime

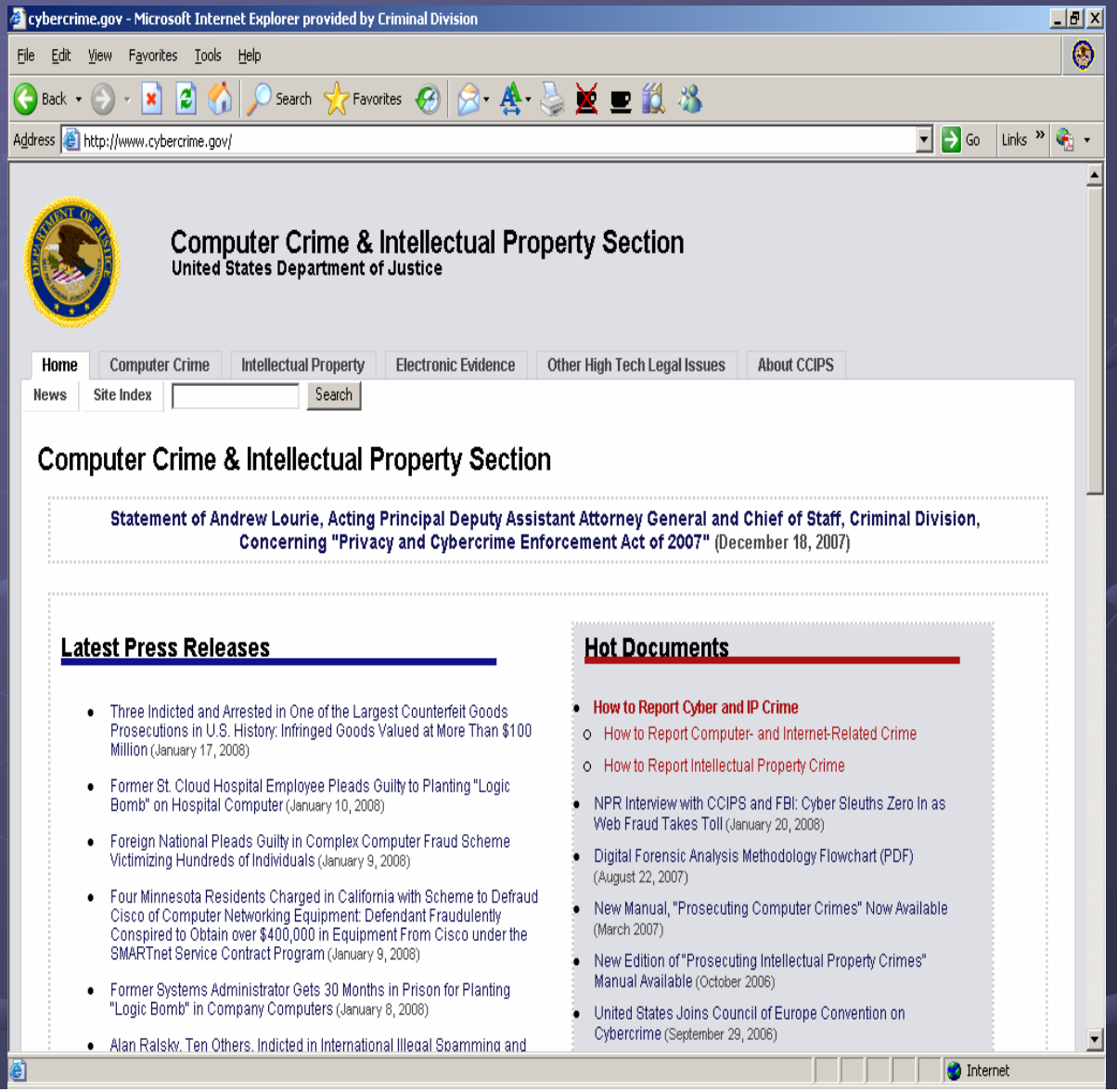
Conclusion

- Legal foundation and enforcement are essential for effective cybersecurity

- Assessment
  - How effective is the present legal foundation and enforcement?
  - What areas for improvement?
  - How to enhance regional and international cooperation?

Cybercrime.gov

- Public Page
- Latest News Releases
- Policies & Programs
- Legal Resources
- Contact Info
- Cases



Legal Foundation and Enforcement: Promoting Cybersecurity

Questions ?

Mark L. Krotoski
Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division
Mark.Krotoski@usdoj.gov

Five Pillars

(1) Developing a national cybersecurity strategy
(2) Establishing national government-industry collaboration
(3) Creating a national incident management capability
(4) Deterring cybercrime
(5) Promoting a national culture of cybersecurity