Current Threats & Examples

TwinSPIN
April 8, 2010
University of Minnesota

"What we don't quite understand as seriously as we should is the extent of malicious cyberactivity that grows, that is growing now at unprecedented rates, extraordinary sophistication, and the dynamic of cyberspace, when you look at the technological balance, right now it favors those who want to use the Internet for malicious purposes over those who want to use it for legal and lawful purposes."

Director of National Intelligence Dennis Blair February 2, 2010 in Testimony to the House Intelligence Committee 2010

Affects More Than Computers

• Critical Threats to Our Infrastructure
  – SKADA Systems for Power, Water, Sewer Plus Gas and Oil Pipelines
  – Entire US Power Grid Mapped by Cyber Intruders
  – Smart Grid Risks
• Threats to Our Transportation Systems
  – Compromised or Faulty Flight Control Software
  – “Drive by Wire” Automotive Software & Computer Issues

UAV Video Hack

• UAV Video Feeds “Hacked” in Afghanistan and Iraq by al Qaeda and Taliban
• Used $29.95 File Sharing Program and Battery Powered TV Monitor

Extortion Using Network Attacks

Extortion Examples

• San Francisco Municipal Network Held Hostage by Fired Administrator
• Credit Card Authorizing Site Threatened by DDoS and Syn Flood Attacks
• US Universities Had Data Encrypted and Held for Ransom
• Businesses Data Held for Ransom and/or Threatened DDoS Attacks

Aurora Bot Net Example

• Damaged Google and gmail
• Also Targeted 34 Large US Companies Including Defense Contractors – Substantial Data Losses
• Exfiltrated (Stole) Large Amounts of Data (Est. $2.2 Billion Losses)
• Also Targeted Journalists and a US Law Firm Involved in Suing China
• Exploited a Zero Day MS Internet Explorer Vulnerability
• Used “Old Style” DDNS Command & Control Systems and Multiple Bot Nets
• Appears to Be Chinese with Possible Eastern European “Hired Gun” Support
GhostNet 2.0
• GhostNet Exfiltrated Data from 1295 Computers in 103 Countries
• Primarily Hit India, the United Nations and the Tibetan Government in Exile
• Utilized Cloud Computing and Social Networking (Web 2.0) Tools
• Controlled by Chinese Computers

Hacktivism

Terrorism & Radicalization
EMP Threats

Hacker Profile
• Well Educated with Good Business Skills
• Sells Bot Nets, Hacking Services and Stolen Data to Whoever Will Pay the Asking Price
• Can Expect to make $4 Million a Year (Russia and Eastern European)
• Little Fear of Getting Caught

Trends
• Attacks Moving from Operating Systems to Applications, Social Networking, Mobile Platforms and “Spear Phishing”
• Bot Nets Moving to Cloud Computing (More Difficult to Trace)
• Attacks Increasingly Targeted, Persistent and Technologically Advanced
• Increasing Criminal - Terrorist Cooperation

NIST Security Resources
• FIPS Publication 199 (Security Categorization)
• FIPS Publication 200 (Minimum Security Requirements)
• NIST Special Publication 800-39 (Risk Management)
• NIST Special Publication 800-37 (Security Authorization)
• NIST Special Publication 800-53 (Security Controls)
• NIST Special Publication 800-53A (Security Control Assessment)
• NIST Special Publication 800-60 (Security Category Mapping)
• NIST Special Publication 800-122 (Confidentiality of PII)

George Welles
Imaging Futures, Inc.