

# Cyber Security Emerging Trends



**Wayne Jones**

Cyber Security Program Manager

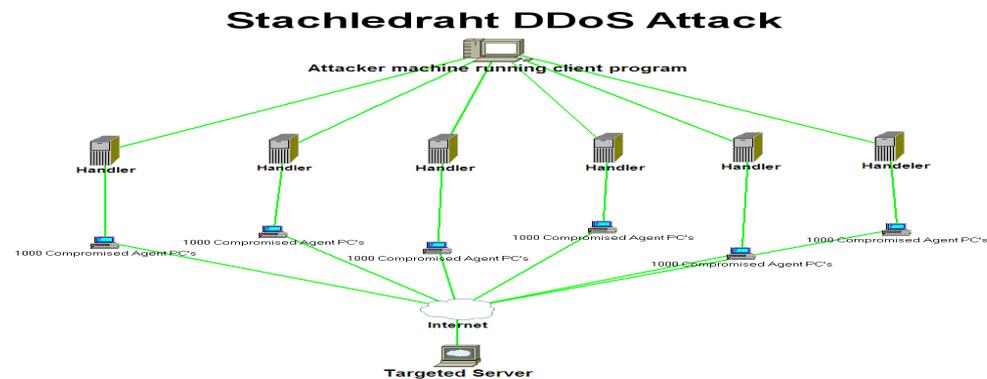
May 6, 2008

- Emergence of more sophisticated website attacks **caused by explosion of Web 2.0 development**
- Increasing prevalence of Botnets
- New generation of identity theft **conducted by organized criminal activity**
- Increasingly malicious spyware



# Threat Types

- ✓ Trojans
- ✓ Viruses
- ✓ DDoS (Distributed Denial-of-Service)
- ✓ Internet server attacks
- ✓ Zero-day exploits
- ✓ Phishing targeted through sophisticated constructed social engineering campaigns



# Threat Targets

- Individuals
  - Bots
    - Spam Campaigns
    - DDoS Attacks
  - Trojans
    - Keyloggers
    - Applications to facilitate data leakage
- Organizations
  - Spear Phishing
  - Server Compromise
  - Database services
  - Storage area networks

# Recent Threats

- Spyware
  - Fraudulent Software
  - Ad Revenue
- Steal information from websites
  - Customer Credentials
  - Confidential Business Information
- Peer-to-Peer (P2P)
  - Malware Distribution
  - Unauthorized personal info retrieval



# Past 'Spyware' Threats



- DesktopScam
- SpyFalcon
- 180search Assistant
- Virtumnde
- Looking-For.Home Search Assistant

- ID Theft
  - FTC Survey in USA 8.3 Million Victims in 2005
  - Gartner states about 15 million Americans were victims of fraud stemming from identity theft between mid-2005 and mid-2006
  - 2005, ID Theft complaints at 37% filed
    - Internet Auctions – 12%
    - Foreign Money Orders - 8%
- Internet related complaints
  - 46% of all fraud reports
- Data Breaches
  - Over 218 million data records of US residents have been exposed due to security breaches since early 2005.



# What are the threats we are seeing today?



- Phishing
- Vishing
- Malware Keyloggers
- Trojan Bankers
- Social Spheres
- All of the Above
- I don't know

- Database targeting
- Identity Theft
  - Phishing
  - Vishing
  - Malware Keyloggers
  - Trojan bankers
  - Social spheres
    - Chat rooms
    - Social networking websites



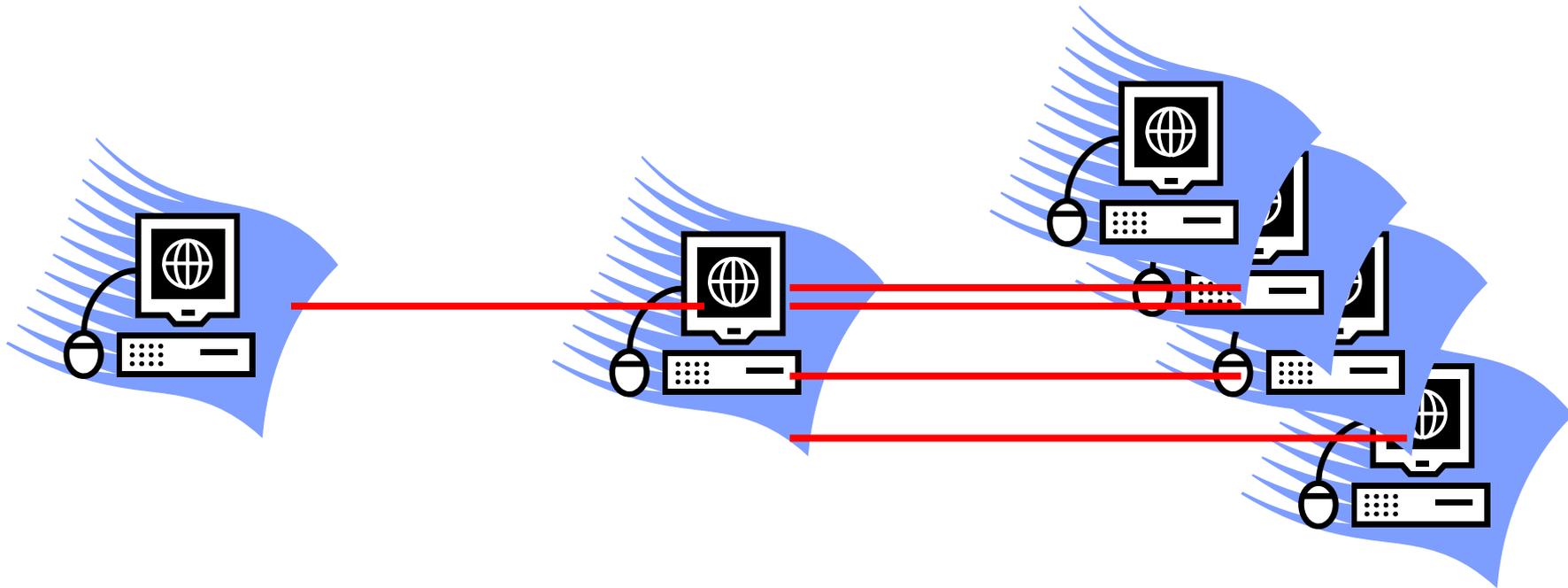
# Current 'Spyware' Threats



- Trojan.FakeAlert
- Trojan-Downloader.Zlob.Media-Coder
- VirusHeat
- Trojan-Clicker.Small.PN

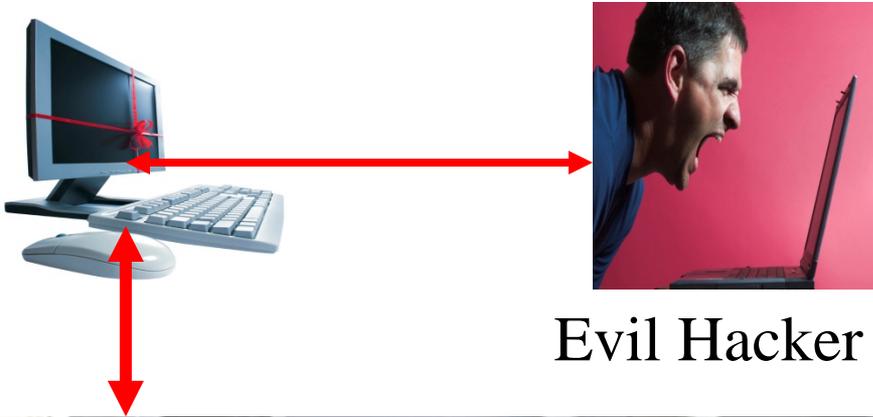
# What is the highest percentage of email borne malware?

- Worms
- Phishing or Fraud
- Downloaders
- Scams
  - Greeting Card
  - Credit Card



Each of the infected computers is “listening” on a pre-designated port for commands from the Phisher. “The phisher then uses a program which automatically distributes email by sending mail through the computers which are infected.”

# Spam-Sending



Thousands. Tens of Thousands



# Remediation: Organization

- Security
  - Application development
  - Systems administration
    - Training
    - **Monitoring**
- Support honeypot projects
  - Share list of attacking IP addresses
    - Analyze and report suspicious log file entries
  - MX Records
    - Permits tracking of spammers

# What approach should we take

- Embrace security as part of the business, which means security must no longer be done in a silo and an afterthought
- Incorporate security early-on in the SDLC (acquisition is too late)
- Look to mature organizational security through the use of best practice guidelines or control frameworks
- Move day-to-day security into operations and work to eliminate redundancy

# Capabilities Needed

- Participation by key stakeholders in the organization for risk and response and recovery
- Commitment to assess, prioritize and implement measures to mitigate risk
- Situational awareness
- **Monitoring**
- Analytical and forensic capabilities
- Incident response capability



# Contact Information



Wayne Jones

Cyber Security Program Manager (CSPM)

National Nuclear Security Administration  
(NNSA)

Office of the Chief Information Officer

Cyber Security

[wayne.jones@nnsa.doe.gov](mailto:wayne.jones@nnsa.doe.gov)