+ what’s new on the ether +

Computer Security Response Team

http://security.depaul.edu/
security@depaul.edu

26 February 2004

Summary

This presentation is intended to outline the major threats impacting computer use on the University network. This presentation specifically addresses computer and operating level security and does not address application security. CSRT feels that without a secure network, access to applications such as PeopleSoft and other ERP applications cannot be safe from malicious use.

A Quick Recap of 2003

Malware matured from ‘‘single-function’’ worm, virus, etc. to blended threats ... i.e. those threats that occur over multiple attack vectors

Blended threats...

- circumvent existing network security technologies
- often [generously] includes a backdoor(s)
- offers the best ‘‘bang for the buck’’

Approximately 35 major malware outbreaks in 2003

Few peaks, many valleys

The votes are in!

Malware Favorites of 2003 -- Annoyances

- W32.Sobig.F :
  - Large infection rates via email in a small period of time
- W32.Klez.I :
  - Released April, 2002, was alive and well in 2003
- W32.Nachi :
  - The “savior” from W32.Blaster
  - Exploited WebDAV
- W32.BugBear :
  - BugBear scanned milllions of hosts for several months

Malware Favorites of 2003 -- Major Threats

- W32.Slammer :
  - Wire-speed scanning for MS-SQL servers
  - Millions of infections within minutes
  - Outages ranging from edge to backbone networks
  - Interruption of financial, airline and other industry
- W32.Blaster :
  - Exploited Microsoft RPC vulnerabilities
  - Required a single OS patch be installed
  - Warmed up many organizations to the idea of network filters

Other Malicious Activity

Malware wasn't the only malicious activity

- DDoS attack against DALnet IRC servers
  - Pinned down DALnet IRC servers for 2+ months!
- DDoS attacks of ranging from 200Mbps to 3Gps
  - Not burst...sustained
- Large Bot infection rates
  - Botnets scaled to 20,000+ hosts
- Several compromised open source projects
  - Backdoored/trojaned source code distributed

What We Learned

Several lessons were learned in 2003

- A heterogenous network is a safe network
- Defense-in-depth is a requirement, not an option
  - Host firewalls and frequent patching
  - A/V scanners and daily A/V signature updates
  - Network filters
  - Traffic analysis for recognition of attacks
- Incident logging and trend analysis
- Worms are good for finding unpatched hosts!

Flash-forward to the present

Statistics

Between 31 Jun 2003 and 31 Dec 2003: 153 incidents

Between 01 Jan 2004 and 23 Feb 2004: 60 incidents

We estimate there will be 500+ incidents this year

CERT/CC Statistics

Number of Incidents Reported

- 2000: 21,756
- 2001: 52,658
- 2002: 82,094
- 2003: 137,529

Number of Vulnerabilities Reported

- 2000: 1,090
- 2001: 2,437
- 2002: 4,129
- 2003: 3,784

Concentration of Attacks

The focus is now, largely, on spam, proxies and bots

- Spammers support the underground, financially
- Proxies allow spammers to relay mail via "throw-away" hosts
- Coordinated bots can DDoS anti-spam sites and allow spammers to leak spam past spam checking applications

Concentration of Attacks (cont'd)

- Malware is continuing to become more intelligent by attacking through multiple vectors, including VPN tunnels!
- DDoS attacks are getting more malicious and frequent
- ‘‘Come and Get It’’ exploits and phishing scams are increasing the risk of identity theft

The Underground Community

Remember, the underground is a self-sustaining ecosystem consisting of...

- An economy
- Enemies and Allies
- Large computing resources
- Drop points (for carded items)
- Dossier’s on many of the best ‘‘whitehats’’ that would rival a CIA profile