+ 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

Does All of This Effect the University?

Since 01 Jan 2004...

- 3 major incidents involving spam
  - One of which involved a total loss of email communications for staff lasting several hours
- 14 incidents of 30+ bots (each)
- 5+ DDoS attacks coordinated via botnets
- 12 incidents of warez servers (80+ unique hosts)

Finding Compromised Hosts

Our favorite tactic is using ngrep, a search utility for slicing up network traffic and displaying well-known patterns... this finds FTP control channels on non-standard ports.

```
pluto# ngrep -qd em0 'USER|PASS' tcp and not
       port \( 21 or 25 or 110 or 119 or 80 \)
T 10.62.221.111:3871 -> 140.192.256.43:1663 [AP]
  USER bebess..
T 10.62.221.111:3871 -> 140.192.256.43:1663 [AP]
  PASS qsdmlwkxvn..
T 10.198.113.73:3941 -> 140.192.256.45:81 [AP]
  USER hoboslayer..
T 10.198.113.73:3941 -> 140.192.256.45:81 [AP]
  PASS 5492402..
T 192.168.230.129:2890 -> 140.192.256.5:27999 [AP]
  USER GaryZelda..
T 192.168.230.129:2890 -> 140.192.256.5:27999 [AP]
  PASS b3taw1n..
T 10.168.230.129:31131 -> 140.192.256.27:444 [AP]
  USER l33ch....
T 10.168.230.129:31131 -> 140.192.256.27:444 [AP]
  PASS p|-|uckU....
```

[ad nauseum]

```
$ telnet 140.192.256.45 27999
220-.:.
220-.::::::::::. e1137 FTP Server loading . WinSock ready .::::::::::
220-.::: _____________________________________________________
220-.:::|
220-.:::|                Welcome to
220-.:::|               ~ 1337 Ftp ~
220-.:::|_____________________________________________________
220-.::: _____________________________________________________
220-.:::|
220-.:::|     SERVER INFO:
220-.:::|    /Current Date: Wednesday 25 February, 2004
220-.:::|    /Current Time: 11:29:28
220-.:::|    /Server Uptime: 1 Days  1 Hours  47 Minutes  32 Seconds
220-.:::|_____________________________________________________
220-.::: _____________________________________________________
220-.:::|
220-.:::|     SERVER STATISTICS:
220-.:::|    /Current Users Online: 12
220-.:::|    /Total Users Ever: 241
220-.:::|    /Times Accessed Today: 24
220-.:::|_____________________________________________________
220-.:::|
220-.:::|     UPLOADED:
220-.:::|    /Total Kilobytes: 141432 Kb
220-.:::|    /Total Files: 13
220-.:::|_____________________________________________________
220-.:::|
220-.:::|     DOWNLOADED:
220-.:::|    /Total Kilobytes: 4204796 Kb
220-.:::|    /Total Files: 319
220-.:::|_____________________________________________________
220-.:::|
220-.:::|     CURRENT STATS:
220-.:::|    /Current Bandwidth: 114.000 Kb/sec
220-.:::|    /Average Bandwidth: 53.751 Kb/sec
220-.:::|    /Free Disk Space: 47693.59 MB
220-.:::|_____________________________________________________
220-.:.
```

```
$ telnet 140.192.256.43 1663
220-Serv-U FTP Server v4.1 for WinSock ready...
220-============================================
220-            Midnight-FxP Server
220-============================================
220-.....: Your Current IP :... 140.192.256.135
220-============================================
220-.....: Server stats:
220-.....: 18 total:..Total User
220-.....: 3:..Aktuelle User Online
220-.....: 449 Kb:..wurden geleeched
220-.....: 2656673 Kb:..wurden geupped
220-.....: 4:..Files wurden geleeched
220-.....: 201:..Files wurden geupped
220-.....: 12.500 Kb/sec:..Durchschnitlicher Speed
220-.....: 0.000 Kb/sec:..Aktueller Speed
220-.....: 1193.72MB MB:.. Free Space auf Pladde
220-.....: Server läuft seid:.....
220-.....: 2 Tagen
220-.....: 11 Stunden
220-.....: 2 Minuten
220-============================================
220-             Hacked by T-ViRuS
220-============================================
220
```

Finding Compromised Hosts (cont'd)

pluto# ngrep -qd em0 '#justgreatmoviez|#XDCC|#SICK-XDCC' tcp port 6667

Using nmap's -sV options and looking for IR-Offer, Serv-U, and other likely-used-for-warez FTP servers on non-standard ports

Also, gaining intelligence through colleagues, groups such as FIRST, Unisog and Nanog and mailing lists generally are the quickest avenue to discovering 0-day exploits, ongoing attacks, etc.

Finding Vulnerabilities

We ran two audits on 2004-02-23

All of our tests are run using

- Open source scanners
  - nmap
  - nessus
- Exploit code
- Home-grown utilities

Finding Vulnerabilities (cont'd)

How well did we fair?

Target: Resnet

- 1526 hosts were online
- 933 major vulnerabilities
- 3849 minor vulnerabilities
- 5678 general (in)security notes

- Resnet gets a 61%, a grade of an F

Finding Vulnerabilities (cont'd)

Target: Information Services Desktops

- 179 hosts were online
- 61 major vulnerabilities
- 352 minor vulnerabilities
- 565 general (in)security notes

- IS gets a 34%, a grade of an F-

- These facts are taken attacks executed from the Internet. The hosts attacking each vulnerable host have the same access permissions as anyone else on the Internet.

How Can We Fix This?

The Low Hanging Fruit

Typically, low-hanging fruit accounts for 80% of vulnerabilities.

Our low-hanging fruit is...

- Open-shares on the network
- Unpatched hosts
- Lack of upstream network protection

Short Term Solutions?

Short term solutions are...

- Deploy ‘‘shielding’’ network ACLs on all business critical networks
- Institute better incident response procedures coordinated via CSRT
- Audit business critical resources weekly and provide trend analysis
- Increase awareness through user-education programs

Long Term Solutions

Long term solutions are...

- Implemented network access controls at key transit points and throughout the edges on Resnet
- Research other operating platforms (i.e. not Microsoft)
- Deploy more security sensors for better network forensic analysis
- Eliminate plain-text logins to any/all IS resources

Thank You

End of presentation.

Questions?