In Brief

SECOND US TEENAGER ARRESTED FOR BLASTER

Another teenager has been arrested in America for creating one of the MS Blaster variants. The suspect, who's identity is being withheld, is reported to have created RPCSDBOT. This latest arrest follows the identification by police of Jeffrey Lee Parson from Minneapolis, US and Dan Dumitru Ciobanu from Romania for creating other MS Blaster variants. However the original worm author has still not been arrested.

FIREWALLS STOP 90% OF ONLINE ATTACKS

Two dummy European banking websites, one with a firewall and one without, have experienced massive variances in the number of attacks, according to research from PanSec and PSINet. The unprotected website suffered 19,128 attacks in 8 weeks compared to the protected website, which was only attacked 1,672 times.

...Continued from page 1 (top)

MS Blaster's knack of targeting IP addresses within the same subnet as the infected machine meant it rapidly took control of subnets, which perimeter-based defences had no awareness of.

Also the RPC DCOM vulnerability was present in two of the most popular Windows platforms, XP and 2000 and the flaw was only a month old, meaning many systems were still unpatched.

Turn to page 4 for the complete analysis of MS Blaster.

Virus authors faster to the kill

Virus writers are churning out exploit code faster than ever, targetting the severest vulnerabilities.

There is an aggressive targeting of the most dangerous vulnerabilities to release malicious code in a shorter window frame, meaning that patches are less likely to be installed in time shows research from Symantec.

"There is definitely a more aggressive approach to building exploits for vulnerabilities", said Jeff Ogden, director of managed security services, EMEA.

He believes that research in hacker groups is getting better, "therefore they can write exploits for vulnerabilities quicker."

"Blaster took 26 days for the exploit to be released. That is an unbelievable statistic considering three years ago the mean time from vulnerability to exploit was well over 12 months. The mean value now is below 40 days," he said.

Other statistics from the latest Internet Security Threat Report from Symantec show that the number of blended threats is creeping up. 60% of malicious code submissions were blended threats in January to June 2003.

Ogden believes you need more than one particular piece of technology to stop a blended threat. "A firewall, alone, may not stop a blended threat but if you have a combination of a firewall, IDS and an antivirus system, then this should help stop them, he said."

There is a 400% jump in malicious code using peer-to-peer and instant messaging vectors to spread. The main reason there is such a radical leap is these applications are becoming rapidly more widespread, believes Ogden.

For this same reason, Symantec also predict that more Linux attacks are on the way.

The rate of new vulnerabilities has stayed nearly the same, with a 12% increase in newly discovered holes. In the last study, there was a 400% leap in new vulnerabilities.

Ogden said: "Organizations…are gathering more data than they used to. Vendors are looking for countermeasures for vulnerabilities so they have to be more open about the vulnerability in the first place."

Snapshot Attack Statistics for January - June 2003 (Symantec)

- 12% rise in newly discovered vulnerabilities.
- 20% increase in blended threats.
- 40% rise in exploits using IM & P2P applications.
- 19% increase in overall attack activity
- 23% decline in severe attacks.
- 50% rise in malicious code with backdoors.