

## Zotob a serious threat to global users

Fortinet in its review of malicious code activity across the globe in August 2005, covered in detail the Zotob worm .

This network worm appeared in late August after a vulnerability in Windows Plug and Play service was announced. W32/Zotob spreads through the network scanning random IP addresses for the vulnerable systems. Upon finding one, the exploit is triggered, and the newly infected system downloads its own copy of the worm from the originally infected system. The worm is then executed and starts scanning for new targets. Fortinet has also examined Zotob variants that propagate through mass-mailing and other Windows vulnerabilities. Zotob opens a backdoor and functions as a bot-listening to owners' commands through an IRC channel. Some systems infected by Zotob become unstable, rebooting continuously.

There are a few characteristics that make this family of worms a serious threat. First, like MsBlaster and Sasser worms, Zotob requires no user interaction and spreads to all vulnerable machines automatically. Second, the worm's footprint is quite small (10KB) and it can simultaneously connect to hundreds of target computers so it spreads very rapidly. Third, the worm exploits a vulnerability that affects Windows 2000, Windows

XP, and Windows Server 2003, all potential victims as these systems make up a large percentage of Internet-connected computers. Lastly, it can spread to a wide array of networks by randomly guessing IP addresses.

In light of the Zotob mass-mailing worm, where the malware was brought in by infected laptops, deploying antivirus/firewall technology at the network edge is not always sufficient. Network security appliances paired with user education, consistent update policies and desktop antivirus software is nowadays mandatory to avoid being trapped by mobile vectors of intrusion (laptops, USB keys, PDAs, etc).