MyDoom More Bad News for SCO

January 27, 2004
By Larry Seltzer


eWEEK Special Report:
Securing Windows

The rapidly spreading MyDoom worm (a k a Novarg.A by Symantec Corp. and MiMail.R by Trend Micro Inc.) is poised to perform a denial of service (DOS) attack against The SCO Group Inc.'s Web site (www.sco.com).

The new worm has many of the standard malware worm behaviors of recent attacks in addition to the DOS attack, and this is not the only recent DOS attack against SCO's Web site. As is shown by performance monitoring of access to the Web site by the British security analysis firm Netcraft Ltd., the recent performance problems at the site may or may not be related to the worm, and we had no trouble getting to the site. MyDoom also opens TCP ports in the range of 3127 to 3198 to create an open proxy server for remote access by attackers.

RELATED LINKS

- SCO Offers Cash Reward to Find MyDoom Author
- With Friends Like These, Linux Doesn't Need Enemies
- MyDoom E-Mail Worm Spreading Quickly
- Windows 'Bagel' Worm Spreading Fast
- Secret Trojan Network Could Produce Superworm

Read Steven J. Vaughan-Nichols' column, "With Friends Like These, Linux Doesn't Need Enemies."

Symantec's analysis of the worm says it "can perform a Denial of Service against www.sco.com using a direct connection to port 80. Creates 64 threads which send GET requests. The DoS is active between February 1, 2004 and February 12, 2004." This indicates that the sporadic attacks so far are indicative of clock errors in some systems, and the real attack is set to begin Sunday.

Unless a defense is in place by then, the attack could be significant. According to Ken Dunham, director of malicious code at iDefense Inc., "MyDoom is spreading at a very high rate, reminiscent of SoBig.F in August of 2004. MyDoom is going to be one of the more notable worms for all of 2004."


eWEEK Special Report:
The Battle over Unix

SCO's recent legal actions have made many enemies in the open-source community and other areas. The company has come under significant verbal attack, in addition to technical attacks such as this one.

Check out eWEEK.com's Linux & Open Source Center at http://linux.eweek.com.