

26 March 2008

By: Ionut Arghire, Hardware Editor



## [Symantec Suspects D-Link Routers for Bot Attack Vulnerability](#)

*D-Link's devices may be vulnerable to worm or bot attack*

Researchers at Symantec Corp. said yesterday that there is a worm or bot at large and that it may be infiltrating D-Link's devices through a three-years-old vulnerability. On Monday night, the security company warned its DeepSight threat notification customers about a worm or bot which, according to "reliable reports", was installing itself on D-Link routers. The vulnerability was first discovered in 2005 and it's based on the SNMP (Simple Network Management Protocol) service. "It looks like they're exploiting the SNMP vulnerability to reset and reconfigure the administrative password on the routers," said Oliver Friedrichs, director of Symantec's security response team. The attacks are suspected to be changing the settings of the router to redirect users to malicious sites instead of the requested URLs. Yet, Friedrichs also said that the first announcement was misleading, as there hasn't been a confirmation of the attacks. There is an increase in attack activity and it seems to come from these routers, but no worm or bot sample has been collected so far. "We suspect that it's a bot," Friedrichs said. The TCP port 23 can be scanned for an active SNMP service and the attack may infiltrate through it. Port 23 should not be opened to the Internet connection, but users having a router with only one Ethernet port are unwillingly exposing their services, as Petko Petkov, a penetration tester from the U.K., advised. The attacks on routers are more often late and they are targeting especially wireless network devices used by small business or consumers. Attackers are searching for new places to infiltrate, install and hide their malware, and they "are increasingly looking beyond the desktop," according to Friedrichs. On the other hand, Petko Petkov said that all the embedded-devices tested by him and his partner, Adrian Pastor, appeared to be vulnerable to all sorts of vulnerabilities. He also added that there is enough research material "out-there" to help anyone creating a worm or a bot Trojan to attack routers on a massive scale. "It is a matter of putting the pieces of the puzzle together," Petkov added. For now, the port 23 scanning activity seems to be moderate, but Symantec researchers will continue to investigate. Also, it is not yet known whether the vulnerability has been patched, nor which models of D-Link routers are targeted. Friedrichs advises users to make sure that the SNMP service of their routers was not exposed to the Internet.