

28 December 2007

By: Bogdan Popa, Security and Search Engines Editor



Typing a simple URL  
may get your computer  
infected  
sqpn.com

## [Windows Worm Using Your Computer for Flood Attacks](#)

*Yet another worm targeting the Windows systems*

WORM\_RBOT.HBZ is the latest threat spotted in the wild that targets the Windows systems and attempts to drop its files on most versions of the Microsoft operating system including 98, ME, NT, 2000, XP and Server 2003. The worm was discovered by security company Trend Micro, which wrote that it could easily reach your system because it might be deployed by other malware, or directly, when a user visits a malicious website. Just like other similar worms, WORM\_RBOT.HBZ attempts to create new registry entries to be sure its files are executed every time the operating system is fully loaded. But what's more important is that it automatically scans the network shares to drop its files and spread itself on the network. "It searches the network for certain shares, into which it attempts to drop copies of itself", Trend Micro wrote in the advisory. And this is not enough. The Windows worm wants to open a random port to enable the attacker to connect to the vulnerable system and access its files. This way, the attacker gets complete control over the system and remotely executes commands. "It opens a random port to allow a remote user to connect to the affected system. Once a successful connection is established, the remote user executes commands on the affected system", the security company explained. The surprising fact is that WORM\_RBOT.HBZ uses your computer to launch web attacks over various targets on the Internet. "It launches certain types of flood attack against target sites. It does the said routine to render target sites inaccessible." Now, move your cursor over your antivirus icon placed in the System Tray, right click it and hit Update. This should be pretty useful if you intend to remain secure while browsing the web these days...