

14 January 2009

By: Marius Oiaga, Technology News Editor

Security  
Microsoft

## [Free Microsoft Security Tool Kills Worm Targeting Critical Windows Flaw](#)

### *The Win32/Conficker*

Microsoft has updated the Malicious Software Removal Tool, a free security tool the company is offering Windows users to fight specific malware, in order to defend themselves against a prevalent worm that targets a Critical Windows vulnerability. Back in October 2008, the Redmond company made available an out-of-band security bulletin (MS08-067) designed to resolve a Critical flaw in the Windows Server service (SVCHOST.EXE) affecting all supported versions of Windows. At that time, Microsoft warned that even Windows Vista SP1, Windows Server 2008 and Windows XP SP3 were vulnerable, and also released a patch for the [pre-release version of Windows 7](#).

"The malware utilizes several layers of polymorphism and packing to hinder analysis and detection. Beyond that, infected users may have difficulty locating [Conficker](#)'s dropped files. It replaces the access rights for its registered key under HKLM\SYSTEM\CurrentControlSet\Services, allowing only Local System account to read, traverse or change discretionary ACL (Access Control List). Similar behavior goes for its system32 DLL file - all the NTFS permissions, except file execute, are stripped for all users," explained [Cristian Craioveanu and Ziv Mador](#), from the Microsoft Malware Protection Center.

Microsoft continues to advise users to patch the Windows Server service vulnerability with the patches released through the [MS08-067](#) bulletin. According to the software giant, unpatched computers are sitting ducks for the [variants of the Win32/Conficker worm](#), and additional pieces of malicious code that are associated with exploits targeting the flaw. US, Mexico, France, UK, Spain, Canada, Italy, Brazil, Korea, Germany, Malaysia, and the Czech Republic account for the largest numbers of infection reports.

"To help customers who are affected, we decided to add capabilities to detect and remove this worm to the January version of the MSRT. This version is released today and is available here. If your computer or environment is impacted by this malware, you may want to run the MSRT to help disinfect it. The first step would be to install the update on all your computers and replace passwords of network shares with stronger ones. Then use the MSRT to remove the worm from infected computers. Infected computers may not be able to access Windows Update and therefore the administrator may need first to download the tool using a clean computer, and then distribute it to the other machines, for example by copying it to a share, write-protecting the share, then running the tool from there," Craioveanu and Mador added.