

26 November 2008

By: Marius Oiaga, Technology News Editor



Win32/IRCbot.BH and Win32/Conficker.A used in attacks against Windows 7 and Vista SP1

## [Widespread Malware Attacks Target Windows 7, Vista SP1 and XP SP3 Vulnerability](#)

### *Infections confirmed*

Microsoft confirmed not only that malware attacks designed to take advantage of a Server Service vulnerability, affecting both Windows client and server versions of the platform, were no longer isolated and targeted cases, but also that infections with malicious code had been detected.

On November 25, [Bill Sisk](#), Microsoft Security Response Center communications manager, and [Ziv Mador](#), senior program manager and response coordinator, revealed that the company was aware of a new wave of attacks, targeting a vulnerability rated as Critical, for which [Microsoft Security Bulletin MS08-067](#) had been released in October as an out-of-band patch.

The security update was designed to integrate with a variety of Windows operating systems, including [Windows Vista SP1, Windows XP SP3 and even Windows 7](#). "During the weekend, we started receiving customer reports for new malware that exploits this vulnerability. During the last two days, that malware gained momentum and, as a result, we see an increased support call volume," Mador revealed.

"Recently we've received a string of reports from customers that have yet to apply the update and are infected by malware. These most recent reports have a common malware family, and the folks in the Microsoft Malware Protection Center (MMPC) have provided detailed information regarding this latest threat," Sisk added.

Microsoft pointed out that there were two pieces of malware associated with attacks exploiting the Server Service vulnerability: [Win32/Conficker.A](#) (also TA08-297A, CVE-2008-4250, VU827267 W32.Downadup (Symantec)) and [Win32/IRCbot.BH](#) (Win32/IRCBot.worm.Gen (AhnLab); Win32/IRCBot!generic (CA); WIN.IRC.WORM.Virus (Dr.Web); Exploit-DcomRpc.gen (McAfee); Mal/IRCBot-B (Sophos); Purple Exploit).

The first is a worm that exploits computers with vulnerable SVCHOST.EXE across a network, the latter is a Backdoor Trojan horse, which gets its commands from an attacker via an IRC server. Backdoor:Win32/IRCbot.BH is used by boots attempting to exploit MS08-067.

Worm: Win32/Conficker.A "mostly spreads within corporations, but also was reported by several hundred home users. It opens a random port between port 1024 and 10000, and acts like a web server. It propagates to random computers on the network by exploiting MS08-067. Once the remote computer is exploited, that computer will download a copy of the worm via HTTP, using the random port opened by the worm. The worm often uses a .JPG extension when copied over, and then it is saved to the local system folder as a random named dll," Mador revealed.

According to Microsoft, Win32/Conficker.A even patches the very API vulnerability, which it uses to infect machines, in order to prevent any further exploits to take advantage of the security hole. Mador explained that the majority of infection reports were generated in the U.S., but that the worm was also detected in Germany, Spain, France, Italy, Taiwan, Japan,

Brazil, Turkey, China, Mexico, Canada, Argentina and Chile. At the same time, Win32/Conficker.A completely avoids to exploit and infect Ukrainian computers.