

29 January 2008

By: Marius Oiaga, Technology News Editor



[Is That a Worm in Your Windows Live Messenger, or Are You Just Happy to See Me?](#)

Microsoft warns of new IM threat

Windows Live Messenger accounts for the largest community for any IM client worldwide. At the end of 2007, in November, as Microsoft was unveiling Windows Live 2.0, the next generation of its suite of software and services in the cloud, the company estimated that Windows Live Messenger had an install base of approximately 300 million users. In this context, it failed to come as a surprise the fact that Windows Live messenger was the most attacked instant messaging platform in 2007, according to statistics provided by [FaceTime Communications](#). And with such a high profile, it is bound that the trend will continue into 2008. Roger Halbheer, Chief Security Advisor Microsoft EMEA, informed that the company was tracking a new Trojan that is currently spreading via Windows Live Messenger. Halbheer however failed to specify the versions of Microsoft's instant messaging client that are impacted by the malicious code. As such, all users of Windows Live Messenger should consider themselves at risk because of the new threat. "Worm:Win32/Pushbot.BD is a worm that spreads via MSN Messenger and AIM when commanded to by a remote attacker. This worm contains backdoor functionality that allows unauthorized access and control of an affected machine," reads the description of Win32/Pushbot.BD as posted on the [Microsoft Malware Protection Center](#). "Worm:Win32/Pushbot.BD can be ordered to spread via MSN Messenger and AIM by a remote attacker. It sends a message to all of the infected user's contacts. The message is provided by the controller via the IRC backdoor, and it has been observed to include a URL pointing to a copy of the worm executable on the domain 'www.mymmsnpics.net'." "Once it has compromised a Windows copy, Worm:Win32/Pushbot.BD proceeds to make a copy of itself in %windir%svchost.exe. The file is then modified and set with the following attributes: read-only, hidden and system, making removal not an easy task. Additionally, the registry is modified so that the worm is executed at Windows start. These details reveal that users running Windows Vista with standard privileges and the User Account Control enabled are protected from the malware. Under Vista with standard user privileges, Win32/Pushbot.BD will not be able to write itself in the protected areas of the operating system, nor to modify the registry without explicit user consent.