

25 June 2007

By: Marius Oiaga, Technology News Editor



Windows Live
Messenger
Microsoft

[New Worm Attacks Windows Live Messenger - Seeds Itself via BitTorrent](#)

And breaks up bootnets harvesting bots

W32/Impard-A is everything but the kitchen sink type of malware. Security company Sopot revealed that W32/Impard-A is essentially a worm targeting the Windows platform (Windows Vista is not mentioned particularly) also featuring IRC backdoor capabilities. The worm spreads via either Windows Live Messenger, AIM or an eventual BitTorrent application on the compromised computer. Richard Cohen, security expert with SophosLabs CA revealed that the worm comes with multi-lingual support and is pushed through a social engineering scheme. "It's controlled by a remote user over IRC, and is capable of sending itself via AIM and MSN, storing itself as a file called IMG009.jpg-www.imagehosting.com inside a zip file called C:RECYCLERmyphoto.zip, and then sending this zip with a message that promises pictures, written in the same language as the infected computer. This sort of social engineering tries to maximize the chance that recipients will believe it to be legitimate and open the attachment, though this is shot in the foot somewhat by the fact that many of the the phrases have been cut off abruptly," Cohen stated. The promise of the sender's photos is nothing more than an incentive to execute the malformed file in order to catalyze the infection. Once on an infected machine, W32/Impard-A can also start seeding itself through BitTorrent. The worm itself will initialize a torrent to a chosen location if it detects a "bittorrent.exe" file on the infected computer. Sophos also informed that the worm will detect and remove alternative bots on the computer. "It scans through each running process and looks for signs that it might be a bot. If any catch its attention, it first attempts to terminate that process, then to send the file over IRC to its own controller, and finally to delete it. This clean-up isn't for altruistic reasons, but sees the author staking the infected computer as his territory, while also sending himself the offending bot to add to his own personal arsenal," Cohen added.