

23 November 2007

By: Bogdan Popa, Security and Search Engines Editor



## [One More Windows Infection, Damage Potential - High!](#)

### *WORM\_AGENT.AFBF in the wild*

It seems like this is the Windows infections day as a new threat was discovered by security vendor Trend Micro, the infection targeting most versions of Microsoft's operating system. Windows 98, ME, NT, 2000, XP, Server 2003, they're all affected by WORM\_AGENT.AFBF, the new worm which seems to be distributed through popular instant messaging applications. The security company reported that WORM\_AGENT.AFBF comes with a medium distribution potential and a high damage potential although the overall risk rating is set too low. However, the worm can easily reach a user's computer because it can be downloaded from a website without approval but it can also be installed by another malware. But what's more important is that the Windows infection can easily open a new port on an affected computer which can be used later for other exploitations and even for remote controlling the system. "It opens random ports and listens for commands coming from a remote malicious user. It then executes the said commands on the affected system. This routine compromises system security and opens the affected machine to further attacks," Trend Micro noted. "This worm then sends copies of itself to target recipients using certain instant messaging applications." At this time, the worm targets only Windows Messenger and MSN Messenger so if you're a user of Yahoo Messenger, Google Talk or any other instant messenger, you're not affected by it. However, it can easily expand its targets so don't disable your antivirus while you're chatting on the web! Trend Micro already discovered 279 infected computers, most of them, 169, coming from United States. The other infected systems were reported to be in Spain, Canada and Thailand. Just like usual, it's recommended to update your antivirus database and to avoid opening and downloading untrusted files coming from unknown sources.