

30 November 2006

By: Marius Oiaga, Technology News Editor



[The First Viruses for Windows Vista](#)

There has been much speculation about whether Vista would render existing malware extinct; the news is now in - it won't!

The first viruses for Windows Vista are in traditional malware threats. We might not see the first piece for malicious code designed especially for Vista for some time. But this makes little difference and is even less relevant in the context in which the latest operating system from Microsoft is vulnerable to old threats. November 30 is the day that marks a Microsoft milestone with the launching of Windows Vista. But adjacent events from the security industry are raining on Microsoft's parade. First off, Symantec has published a security report in which it reveals that Windows Vista is susceptible to attacks via the Teredo Protocol. And Sophos is joining in. According to Sophos, Windows Vista is vulnerable to no less than three of the top ten global malware threats: W32/Stratio-Zip, W32/Netsky-P and W32/MyDoom-O. "Sophos experts note that on the launch date of Microsoft's Windows Vista operating system, three of the top ten - including Stratio-Zip - are capable of bypassing the product's security defences and infecting users' PCs. The Vista-resistant malware - W32/Stratio-Zip, W32/Netsky-P and W32/MyDoom-O - comprise 39.7% of all malware currently circulating," stated Sophos via a press release. "There has been much speculation about whether Vista would render existing malware extinct, and the news is now in - it won't," said Carole Theriault, senior security consultant at Sophos. "While Microsoft should be commended for the huge security improvements it has made in Vista, running separate security software is still essential to eliminate the risk of infection. On top of this, cyber criminals will already be looking at creating Vista-specific malware. Users need to think carefully about whether their current solution is going to offer sufficient protection against such emerging threats, given that some vendors continue to experience problems adapting their software for the Vista operating environment." W32/Stratio-Zip, W32/Netsky-P and W32/MyDoom-O are all worms designed for Windows, and all proved to be - as Sophos has put it - Windows Vista resistant. "The figures, compiled from Sophos's global network of monitoring stations, show that the W32/Stratio-Zip worm has overtaken W32/Netsky-P as the most widely circulated piece of malware, accounting for one third of the total number of reports," disclosed Sophos.