

28 February 2007

By: Marius Oiaga, Technology News Editor



Symantec Has Bombarded Vista with 2,000 Instances of Malware

The impact of malicious code on the "Quasi Immaculate" Vista

Symantec has bombarded Windows Vista with malicious code. Literally! A total of 2,000 instances of malicious code have been executed under the Windows Vista framework and the operating system emerged quasi immaculate, but immaculate nonetheless. While Symantec has a long history of downplaying the security contribution of Windows Vista, the fact of the matter is that testing Windows Vista's capacity to fend off existing malware has backfired against the Cupertino-based security company. Symantec has thrown everything it has at Windows Vista. Backdoors, Keyloggers, Rootkits, Mass mailers, Trojan horses, Spyware and adware and also uncategorized binaries were all executed on Windows Vista. Symantec stated that it has used its own virus repository as well as those of security partners as sources for the binaries. "The results showed that 3 percent of backdoors can successfully execute and survive a system restart on Windows Vista without modification. Other categories include keyloggers, of which 4 percent can successfully execute and survive a system restart, mass mailers (4 percent), Trojans (2 percent), spyware (2 percent), and adware (2 percent). Symantec believes that these percentages would increase dramatically with only minor code changes to make these threats Windows Vista-aware, in turn allowing them to run successfully within the new Windows Vista security model," Symantec revealed. Symantec informed that the tests were designed to verify the extent to which the security technologies in Windows Vista are able to mitigate the threats of legacy malicious code. It is important to note that the instances of malicious code used were not adapted to the Windows Vista security model. "This research demonstrates that, while Windows Vista has made improvements that restrict the exploitation of vulnerabilities and reduce the likelihood of complete system compromise, some legacy threats survive and go unhindered by the improvements. This suggests that authors of existing threats need only update their code with minor changes in order to adapt to Windows Vista and continue to run within its confines. If the new security technologies introduced in Windows Vista were a silver bullet, we would expect that no legacy threats would survive," Symantec concluded.