

27 December 2007

By: Marius Oiaga, Technology News Editor

[Kaspersky: Windows Vista Firewall Is Full of Leaks](#)

Users need third-party protection



According to Microsoft, Windows Vista is the most secure Windows operating system available on the market. The Redmond company has now been shy about downplaying the relevance of previous Windows iterations in order to push Vista to the foreground in terms of security. It is in fact an old drum that Microsoft has been beating repeatedly even before Vista hit the shelves, in an effort to focus consumers on the latest Windows platform. Unlike Mac OS X and Linux, Windows is, by no means, a landmark of the security landscape. Vista came to fix this aspect. According to Russian antivirus maker, Kaspersky, Microsoft did good, but not enough. "Even the latest operating systems, such as Windows Vista, cannot block all types of leaks on their own (although, from Windows XP SP2 onwards, Windows has included a firewall. Firewall functionality was significantly expanded in Windows Vista). According to the results of testing conducted in March 2007 by Guillaume Kaddouch, Windows Vista Ultimate 64-bit using default settings blocked only 9 leak tests (the leak tests blocked are shown in green in the results table)", revealed Kaspersky's Nikolay Grebennikov, Deputy Director of the Innovation Technologies. In Kaspersky's perspective, leak tests used to evaluate Vista's firewall point to the holes in Microsoft's latest operating system, holes that recommend the implementation of third-party security solutions. Grebennikov predicted that even with the added mitigations in Vista, such as User Account Control, Internet Explorer Protect Mode, and PatchGuard, the operating system is still vulnerable in its default configuration. "Even Windows Vista requires third-party protection programs to provide the necessary level of protection from leaks. In the future, malicious programs will implement new methods in order to bypass protection mechanisms in the new operating system as well as existing protection mechanisms. This is why the importance of the firewall as an additional level of protection will only increase. Clearly, malware writers will increasingly use leak technologies to bypass firewalls. This means that leak tests will become a crucial method for testing the reliability of a computer's protection", Grebennikov added.