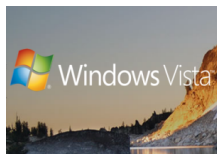


17 September 2007

By: Marius Oiaga, Technology News Editor

Windows Vista  
Microsoft

## [Windows Vista Immune to Skype Worm by Default](#)

### *How the User Account Control pays off*

At the beginning of the past week, Skype warned users of its peer-to-peer instant messaging client, that a Windows worm was running wild through its network. The piece of malicious code was dubbed Win32/Pykbub.C (Computer Associates); Worm.Win32.Skipi.b (Kaspersky); W32/Pykse.worm.b (McAfee); W32/Pykspa.D (Norman); Mal/Behav-103 (Sophos); Worm.Win32.Skipi.b (Sunbelt Software); W32.Pykspa.D (Symantec); WORM\_SKIPI.A (Trend Micro) and [Win32/Pykspa.A](#) by Microsoft. According to the Microsoft Malware Protection Center, protection against the worm was added to its security solutions via definition updates. "Worm:Win32/Pykspa.A is a worm that sends instant-messages on behalf of a user logged into Skype, an Internet chat client application. Messages sent contain a link to a remote Web site hosting a copy of the worm. Worm:Win32/Pykspa.A terminates processes, and redirects Web browser connections for various security-related Web sites to random IP addresses. Worm:Win32/Pykspa.A may be introduced to a system in two ways: clicking a link referencing a remote Web site hosting a copy of the worm or mounting an infected removable drive with "autorun" feature enabled", the Microsoft Malware Protection Center revealed. The Redmond company also detailed the worm's actions, once the user clicked on a malicious link provided via the Skype instant messaging client. And for the most part, the malware has to write itself to the registry and to the system32. While Microsoft does not reference Windows Vista in any special manner, running the company's latest operating system with the User Account Enabled offers a default barrier against Win32/Pykspa.A. This is because UAC limits all users to standard privileges as opposed to administrative rights. In such a context, the worm would fail to write itself to either the registry or to system32, with the UAC safeguarding both. Still, Microsoft does not refer to the UAC as a security mitigation, but as a feature designed to train users and software developers to work exclusively with standard privileges. The end purpose however is to increase security by limiting access to critical areas across the operating system.