

30 March 2007

By: Marius Oiaga, Technology News Editor



## [Sophos: What You Get When You Download Internet Explorer 7](#)

### *Update*

Security company Sophos describes in detail what users will get when they download and install Internet Explorer 7. However, Sophos did not focus on the final version of Internet Explorer 7 as delivered by Microsoft via its official download web page or through Automatic Updates. Instead, Sophos has analyzed [Internet Explorer 7 Beta 2](#), the version that is aggressively promoted through a spam campaign. "The emails, which claim to come from admin@microsoft.com and have the subject line "Internet Explorer 7 Downloads", display an image which invites users to download beta 2 of Internet Explorer 7. However, users who click on the image will download a file called ie7.0.exe which is infected by the W32/Grum-A worm," revealed Sophos. According to Sophos, this is not the first time that malware poses as a download from Microsoft. This is no more than a social engineering method designed to provide enough incentive for unsuspecting users to download the Grum worm. "Worms like this are only succeeding in spreading because so many people have still not learnt to be suspicious of unsolicited emails, even if they claim to come from well-known companies like Microsoft," said Graham Cluley, senior technology consultant for Sophos. "The problem is that to the casual observer the email looks genuine, and the image displayed looks near-identical to the imagery that Microsoft is using on its website to promote Internet Explorer 7.0. Clicking on the image, however, doesn't download the real beta - but malicious code straight from the hackers." "The Grum worm is an appender virus for the Windows platform. If executed, Grum will copy itself to winlogon.exe and infect files that are referenced by Run keys. The worm also modifies the registry, edits the HOSTS file, injects a thread into system.dll and patches ntdll.dll and kernel32.dll system files. "There have been many occasions when virus writers have coded attacks that have presented themselves as communications from Microsoft," continued Cluley. "For instance, in 2003 the Gibe-F worm (also known as Swen) posed as a critical security update from the software giant, and two years ago hackers directed Internet users to a bogus website masquerading as Microsoft's update page."