

8 February 2008

By: Marius Oiaga, Technology News Editor



Fake Critical Windows Vista Update Installs Malware

Via a spoofed Microsoft Update site

Attacks that are using Windows Updates in order to spread malware and compromise Microsoft platforms are nothing more than an integral part of the luxuriant threat environment that preys on unsuspecting users. But generally the attacks masquerading as Microsoft Updates are nothing more than social engineering tricks devised to essentially convince the end user to become an active participant in the compromising of the system. In this context, the level of authenticity of emails allegedly delivering Windows updates is rather low, as such a practice was never deployed by the Redmond company. In this context, attackers are now seeking to replicate as closely as possible the actual experience that Windows users do associate with the Redmond company. Such as the Microsoft Update. The actual Microsoft Windows Update site can be found [here](#) and it is sensitive to the context of the operating system, meaning that when a Vista user will visit the website, the page will change to reflect the platform. Security outfit F-Secure has warned Windows users of the existence of a spoofed Microsoft Update site that spreads malware. The fake Microsoft Update website urges users to immediately install a Critical security update for Windows 2000, Windows Server 2003, Windows XP and Windows Vista. The social engineering scheme is put together to effectively scare the user into installing malware on their machine. "Watch out for this one. It's not the real Microsoft Update site. Note the real URL (cfm48.com) and the spelling errors ('Please intall'). If you click the Urgent Install button, you'll get a file called WindowsUpdateAgent30-x86-x64.exe, which is not signed by Microsoft. (i.e. Click the button - Download a Trojan-Dropper.) The dropper is now detected as Trojan-Dropper:W32/Agent.DYD, and the dropped malware was already detected as Backdoor:W32/Agent.CVU; this is functionally the same as the earlier Backdoor:W32/Agent.CTH," a F-Secure security expert revealed.