

19 February 2008

By: Marius Oiaga, Technology News Editor

Windows Update
Microsoft

[McAfee on Microsoft's Windows Worm-Update Infections: the Road to Hell](#)

Is paved with good intentions

Microsoft is readying a new [strategy](#) for Windows update based on a technology which shares the same behavior as self replicating malicious code, more commonly known as a variety of malware dubbed worms. The Redmond company's alternative approach to servicing its Windows platform with updates using the same techniques as worm infections, rather than the current model based on a centralized update server delivering patches, is nothing more than the reinventing of the wheel. The fact of the matter is that the concept of converting malicious code and using it for beneficial purposes dates back to the 80s. But for over 20 years now, it has never been successfully implemented. Joe Telfici, director of operations at McAfee's Avert Labs, argues that the road to hell is always paved with good intentions. "Back in 2001 we saw CodeGreen attempt to locate and patch machines infected with the infamous CodeRed worm. In a variety of other cases, one piece of self-propagating code (worm) has tried to patch backdoors or vulnerabilities, but usually in a self-preservation attempt against a rival author rather than for any altruistic purpose. Examples of this include the Linux Cheese worm and a variety of Bagle and Netsky variants that attempted to remove the other during the much-publicized 'Virus Wars' of 2004. The use of self-replicating code to fix other security problems has invariably proved to be a Bad Idea in the real world because we simply do not understand the epidemiology of the complex, heterogeneous universe we call the Internet," Telfici [commented](#). The Network Immunology is a project lead by Milan Vojnovic, a researcher with systems and networks group at Microsoft Research, Cambridge, dealing with sampling strategies for epidemic-style information dissemination. Vojnovic essentially proposes that Windows update spread from computer to computer using the same tactics as self replicating code - worms. McAfee's Telfici did not dismiss the idea, arguing that it would take the load off Microsoft's servers and free up the bandwidth used by the updating process. But at the same time, Telfici stated that the implementation of the project would be equivalent with an unwanted experiment. Vojnovic is "really looking at how the epidemiology of good code versus bad code works. Given that most worms are Windows-based, and Microsoft, by definition, is providing the patches to block those worms that exploit vulnerabilities in their software, this is not irrelevant. While biological analogies to computer viruses are often dismissed, this is one area where a 'computer epidemiology' discipline would be most welcome," Telfici said.