



[Home](#) | [Forums](#) | [Archives](#) | [Search](#) | [Speedtest](#) | [Advertising](#) | [Contact](#) | [About & Link](#) | [Sitemap](#) | [RSS](#)

Links

- [Home](#)
- [Online](#)
- [Discussions](#)
- [Blogs](#)
- [Podcast](#)
- [Downloads](#)

Categories

- [Telecoms](#)
- [Broadband](#)
- [ADSL](#)
- [3G & Cellular](#)
- [MyWireless](#)
- [iBurst](#)
- [Gaming](#)
- [Hardware & Software](#)
- [International](#)
- [Business & General](#)

Sponsor

News Partners

[Home](#) ▸ [Hardware & Software](#)



Back-door worm targets vulnerability in Microsoft Word

By ICTWorld, 8 September 2006



A new variant of a Trojan Downloader is actively exploiting a recently found vulnerability in Microsoft Word 2000, claims MicroWorld Technologies. The malware infection is said to be caused when the victim opens an infected Word 2000 file in Windows 2000.

The flaw is associated with a forced Memory Corruption error in the text editing software. A Trojan Dropper named 'Win32.Mdropper' exploits this vulnerability when users download and open a specially crafted Word file carrying this malware, and proceeds to drop 'Worm.Mofeir', a network worm with back-door capabilities.

Worm.Mofeir then opens a back door channel to contact the remote attacker. Using the back door, the intruder can open a terminal access to the system, download code from the Internet and run, send and delete files.

“Almost everybody uses Microsoft Word and it is one of the most widely exchanged file types in the form of e-mail attachments since the early days of the Internet,” points out Dinesh Shah, product manager at MicroWorld Technologies.

Related Articles

- [Speak to me](#) 09/12/06
- [Professional PCs for superheroes](#) 09/12/06
- [EU, Microsoft in Vista launch spat](#) 09/08/06
- [Latvians having a laugh at Microsoft](#) 09/08/06
- [Intel slashes 10,500 from workforce worldwide](#) 09/06/06
- [Japan's Matsushita recalls 6,000 laptop batteries](#) 09/05/06
- [Daily online update on piracy](#) 09/05/06
- [Malware challenge shows IT still needs a business reality check](#) 09/05/06
- [CA anti-virus flags Windows component in mix-up](#) 09/05/06
- [Laptop sales will outstrip PCs](#) 09/05/06

Sponsor

[Financial Mail](#)

[Business Day](#)

[Business Report](#)

[MoneyWeb](#)

[ICT World](#)

[Finweek/Fin24](#)

[BiA Online](#)

[Mail & Guardian](#)

“Most anti-Virus products consider Word files to be harmless, and hence the hack will be hugely rewarding for the malware writer if he can inject the malicious code into a Word document, and initiate a multi-layered onslaught there on.”

Shah says there was a similar attack in May this year, by a back-door worm named GinwuiA via MS Word files, and, more recently another one called Win32.Papi that found its way to user computers through Japanese text editing application Ichitaro. He urges computer users not to open MS Word files from unknown senders, until Microsoft releases a patch for the flaw, as there may be fresher attacks targeting it.

© 2006 MyADSL, All Rights Reserved..



DataPro
INTERNET SOLUTIONS FOR THE REAL WORLD

**Click and switch to
DataPro ADSL for
A faster, more reliable
internet experience**

News Discussions

Advertisement