

IT Backbones - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links



Give your mouse a heart!

search 

Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- [Home](#)
- [About](#)
- [Contact](#)
- [Submit PR](#)
- [Search News](#)
- [What We Can Offer You](#)
- [IT Events](#)
- [Time & Money](#)

## Backdoor Worm Targets Vulnerability In Microsoft Word

Published 8th September 2006

New variant of a Trojan Downloader is actively exploiting a recently found vulnerability in Microsoft Word 2000, informs Security Experts at MicroWorld Technologies. The malware infection is 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 you download and open a specially crafted Word file carrying this malware, and proceeds to drop 'Worm.Mofeir', a network worm with Backdoor capabilities.

Worm.Mofeir then opens a backdoor channel to contact the remote attacker. Using the backdoor, 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’s one of the most widely exchanged file types in the form of email attachments since the early days of Internet,” points out Dinesh Shah, Product Manager at MicroWorld Technologies. “Most AntiVirus products consider Word files as harmless and hence it 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. That’s precisely why we see this stepped-up level of attacks trying to find and force flaws in Microsoft Office Applications.”

Mr Shah says there was a similar attack in May 2006, by a Backdoor named Ginwui.A 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 can be fresher attacks targeting it.

MicroWorld Solutions eScan and MailScan relentlessly protect home and corporate users from all kinds malware threats including targeted attacks of this nature, using a potent combination of fastest malware detection, proactive algorithms and a unique Technology named MWL(MicroWorld Winsock Layer).

“Of late there’s been slew of zero-day attacks of this nature, targeting a range of popular software applications. But the most remarkable aspect of almost all these attacks is that the malware used in them are close variants of older worms, for which MicroWorld already had protection in place. Because we believe that even the most insipid piece of malware code needs to be guarded against, as you never know where, when and how it will be used!” observes Sunil Kripalani, Vice President - Global Sales and Marketing of MicroWorld Technologies.

## Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)

---

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.