

[Articles](#)[News](#)[Reviews](#)[Releases](#)[Downloads](#)[Contact Us](#)[White Papers](#)**Sponsors:**

Is your network open to attack? Find out with the #1 sold network security scanner: GFI LANguard Network Security Scanner! [Download your FREE trial version today.](#)

Check your website security with a FREE [website security audit](#) by [Acunetix](#). Audit your web applications for [SQL injection](#), [cross site scripting](#) & more with [Acunetix Web Vulnerability Scanner](#)

Software security section is sponsored by GFI, a leading developer of network security, content security and messaging software - [Free trial!](#)

**Trojan And Backdoor Spread Via Vulnerability In Microsoft Word**

Monday, 22 May 2006 12:36 EST

Security Experts at MicroWorld Technologies inform that a new vulnerability has been identified in Microsoft Word XP and 2003. It's currently being exploited in a targeted zero-day attack using a combination of a Trojan and a Backdoor. As a precautionary measure, MicroWorld warns users against opening MS Word documents from unknown senders.

'Trojan-Dropper.MSWord.1Table.bd' spreads via targeted emails identified to be sent from China and Taiwan. Once you to download and try to open the infected file, it shows an error message. If you click on 'Retry', the malicious file is replaced by a clean one immediately!

By this time, Trojan-Dropper has already slipped into your computer, which then goes ahead and downloads 'Backdoor.Win32.Gusi'. This backdoor can open a direct channel that connects to the remote attacker suspected to be sitting in China, to receive and execute commands. With its rookit capability, this backdoor can smartly hide itself as well.

Microsoft has already identified the vulnerability and will be releasing a patch soon. A security response from the corporation reads "Microsoft is investigating new public reports of a "zero-day" attack using a vulnerability in Microsoft Word XP and Microsoft Word 2003. In order for this attack to be carried out, a user must first open a malicious Word document attached to an e-mail or otherwise provided to them by an attacker. Microsoft will continue to investigate the public reports to help provide additional guidance for customers as necessary."

Security Expert from MicroWorld Technologies, Arti Taru says "We strongly recommend users not to download and run MS Word files from strangers, obtained via emails and file sharing networks. Though the Trojan and Backdoor in question have already been identified, fresher attacks are anticipated with newer breeds and variants."

AntiVirus and Content Security solutions eScan and MailScan from MicroWorld proactively protect users from all kinds of malware with a fusion of signature detection and a highly intelligent behavioral analysis. To stop viruses and suspicious programs at the gateway level of connectivity, MicroWorld uses a unique, patent pending technology named MicroWorld Winsock Layer.

**News**

[Verid Debuts Enhanced Identity Fraud Security Features](#)

May 22, 2006, 15:32 EST

[Five Ways to Screw Up SSL](#)

May 22, 2006, 13:29 EST

[Skype URI Handler Command Switch Parsing Vulnerability](#)

May 22, 2006, 13:18 EST

[Custom Trojans: The Next Big Thing](#)

May 22, 2006, 13:06 EST

[Sunbelt All-in-One Messaging Security](#)

May 22, 2006, 12:42 EST

[SafeWord PremierAccess 4.0](#)

May 22, 2006, 12:39 EST

[UK Business Hit By Email That Uses Anti-Spyware Company To Spread Trojan](#)

May 22, 2006, 12:38 EST

