

Industry News

[Security News](#)

[Security companies](#)

[Jobs forum](#)

[Knowledge base](#)

[White papers](#)

[Research library](#)

[Security books](#)

[Special reports](#)

[Security links](#)

[Security events](#)

[Classifieds](#)

[Directory](#) **GET LISTED!**

Product News

[Access Control](#)

[Biometric Systems](#)

[CCTV](#)

[Intruder Alarms](#)

[IT Security](#)

[Manned Guarding](#)

[Perimeter Protection](#)

[Physical Security](#)

[Remote Monitoring](#)

[Security Services](#)

[Fire, Health & Safety](#)

[Other Security Products](#)

Security Markets

Posted in [Security News](#) - [IT and Computer Security](#) - on 22/05/2006 

Trojan and Backdoor spread via Microsoft Word vulnerability

A new vulnerability has been identified in Microsoft Word XP and 2003. It is currently being exploited in a targeted zero-day attack using a combination of a Trojan and a Backdoor. As a precautionary measure, users are warned 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 try 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

Article search

Directory search

Now you can [add your company](#)



**DOWNLOAD YOUR
FREE EVAL TODAY!**

NICE
Insight from Interactions™

- Bank and financial services security
- Buildings and office security
- Education and school security
- Entertainment and events security
- Homeland and Government security
- Hospital and healthcare security
- Infrastructure and utilities security
- Manufacturing and industrial security
- Public sector security
- Residential and home security
- Retail security
- SME security
- Sports and recreational security
- Transport and logistics security

variants.”

 Print version |  Send to a friend |  View related articles

NEW: Interested? Want to know where to buy this? Request a quote!

Other News & Resources

[Security News](#) [Company News](#) [Knowledge base](#) [Research Library](#) [Security Events](#) [Jobs and Recruitment](#) [Products and Suppliers Directory](#)

[Access Control](#) [Biometric Systems](#) [CCTV](#) [Intruder Alarms](#) [IT Security](#) [Manned Guarding](#) [Perimeter Protection](#) [Physical Security](#) [Remote Monitoring](#) [Security Services](#) [Other Security Products](#)

Special reports: Technology, Market data, Company profiles

[Basel II compliance](#) [Energy market security](#) [Enterprise IT Security market](#) [Fleet card security](#) [IT Security threats](#) [RFID Security](#) [VoIP security](#) [Wireless LAN security](#)

Security links

[ISO 27001 Masterclass](#)

Led by the authors of the Open University's post-graduate information security text book. Spaces are limited, so book early.

Search for Company / Industry Research:

IT Security white papers and research library

[RSS XML feed
for this page](#)

The latest Security news:
CCTV, remote monitoring,
access control, biometric,
smart cards, IT and network
security, intruder alarm,
perimeter protection,
manned guarding, physical
security, fire, health and
safety, available via an
XML RSS feed.

Secu

Need a
[reference book?](#)

Find it on Amazon:



[Advertise on Security Park](#)

Reach Security Park's audience of 220,000 Security Professionals (far ahead of other Security magazines, in print or online), for a fraction of the cost of print advertising.

[Free e-mail newsletter](#)

Free subscription
click [here](#)

[Access Control](#) [Authentication](#) [Data Management](#) [Data Security](#)
[Digital Signatures](#) [Email Security](#) [Identity Management](#) [Internet Security](#)
[Intrusion Prevention](#) [Network Security](#) [Remote access security](#) [Security Management](#) [Security Policies](#) [Security Software](#) [Security Threats](#) [Virus Detection](#) [Software Virus Protection](#) [VPN](#) [Vulnerability Assessment](#) [Wireless Security](#)

EDITOR'S CHOICE:

Develop an ISO 27001/BS7799-compliant Information Security Management System

The hardest, most exhausting part of achieving ISO 27001 / BS7799 certification is the documentation of the Information Security Management System (the ISMS). That's why many organizations turn to outside consultants. But consultants are expensive and don't necessarily leave an organization owning the ISMS. The logical alternative is to buy a set of model pre-written policies and procedures:

The [ISMS Documentation Toolkit](#) is a unique product, costing less than a day of a consultant's time and packaged with 12 months of online drafting support and advice. It makes it easier for organizations of all sizes, anywhere in the world, to succeed with a ISMS project. You should buy this toolkit products and use it in your business. Follow this link and buy the [ISO 27001 / BS7799 ISMS Documentation Toolkit](#).

Security books, guides, standards and toolkits

[RFID and Smart Cards books, guides and reference documents](#)
[Biometric books, guides and reference documents](#) [CCTV books, guides and reference documents](#) [Intruder alarms and intrusion detection systems books, guides and reference documents](#)
[Monitoring and surveillance books, guides and reference documents](#) [IT Governance, ISO 27001 ISO 17799 and BS 7799 toolkits](#) [Fire, Health & Safety books, guides and reference documents](#)

[feedback](#) | [advertise](#) | [terms & conditions](#) | [copyright](#) | [privacy policy](#) | [CMS and Web design by www.Areza.com](#)