



Biting the hand that feeds IT

Ads by Google

[Lexar Enterprise Products](#)

Enterprise Personal Storage Devices
Secure and Control your USB
Devices
www.Lexar.com/

[Lock Down Windows XP](#)

Secure your confidential data. Free
security guide download.
www.newboundary.com

[Create your own Website](#)

It is Free and Easy like Weblog Now,
a version start . Please test
atwiki.com

[MS Information Security](#)

Learn security assurance with a MS
from University of San Francisco
cps.usfca.edu

[The Register](#) » [Security](#) » [Anti-Virus](#) »

Original URL: http://www.theregister.co.uk/2006/05/22/trojan_exploit_word_vuln/

Trojan exploits unpatched Word vulnerability

By [John Leyden](#)

Published Monday 22nd May 2006 11:42 GMT

Hackers have developed malicious code designed to exploit an [unpatched](#) (<http://secunia.com/advisories/20153>) vulnerability in Microsoft Word 2002 and 2003.

Maliciously-constructed Word documents containing the Mdropper-H Trojan have begun to circulate on the net in messages that pose as internal emails. The malware contains a number of objects (such as PowerPoint slides and Excel charts) along with [Backdoor-Ginwui](#) (<http://www.symantec.com/avcenter/venc/data/backdoor.ginwui.html>), which opens a back door that allows hackers to control compromised Windows PCs.

**Vendor Whitepapers
Free to Download**

[The Evolution of Wide Area File Services](#)

[Enterprise VoIP Security](#)

[Securing your Online Data Transfer with SSL](#)

[Building the 'Thin Branch'](#)

"This threat originated in Asia but is not spreading widely because it seems to be targeted at specific large organisations," Symantec Security Response senior director Vincent Weafer said. "Symantec has seen similar types of targeted attacks in the past which leveraged exploits in office applications, such as Word. This event illustrates the

trend toward zero-day targeted attacks."

Microsoft [says](http://blogs.technet.com/msrc/archive/2006/05/20/429612.aspx) (<http://blogs.technet.com/msrc/archive/2006/05/20/429612.aspx>) it is working on a patch designed to fix the underlying vulnerability in MS Word, though it's unclear when an update will be ready.

The SANS Institute has published an advisory on how to [defend](http://isc.sans.org/diary.php?storyid=1347) (<http://isc.sans.org/diary.php?storyid=1347>) against Mdropper-H attacks. ®

Related stories

[Unpatched Word flaw menaces civilisation](http://www.theregister.co.uk/2006/12/06/unpatched_word_flaw/) (6 December 2006)

http://www.theregister.co.uk/2006/12/06/unpatched_word_flaw/

[Another day, another zero-day MS exploit](http://www.theregister.co.uk/2006/09/28/0-day_powerpoint_threat/) (28 September 2006)

http://www.theregister.co.uk/2006/09/28/0-day_powerpoint_threat/

[Patch Tuesday omits critical Word fix](http://www.theregister.co.uk/2006/09/14/ms_patch_tuesday/) (14 September 2006)

http://www.theregister.co.uk/2006/09/14/ms_patch_tuesday/

[Trojan targets 0-day Word vuln](http://www.theregister.co.uk/2006/09/05/ms_office_trojan/) (5 September 2006)

http://www.theregister.co.uk/2006/09/05/ms_office_trojan/

[Flaw finders lay siege to Microsoft Office](http://www.theregister.co.uk/2006/07/22/bug_hunters_crawl_over_ms_office/) (22 July 2006)

http://www.theregister.co.uk/2006/07/22/bug_hunters_crawl_over_ms_office/

[French MoD questions OpenOffice security](http://www.theregister.co.uk/2006/07/20/openoffice_france_mod_report/) (20 July 2006)

http://www.theregister.co.uk/2006/07/20/openoffice_france_mod_report/

[When PowerPoint presentations attack](http://www.theregister.co.uk/2006/07/17/powerpoint_trojan/) (17 July 2006)

http://www.theregister.co.uk/2006/07/17/powerpoint_trojan/

[MS June update fixes dangerous Word flaw](http://www.theregister.co.uk/2006/06/14/ms_june_patch_tuesday/) (14 June 2006)

http://www.theregister.co.uk/2006/06/14/ms_june_patch_tuesday/

[Online attack holds files to ransom](http://www.theregister.co.uk/2006/05/31/virus_ransoms_files/) (31 May 2006)

http://www.theregister.co.uk/2006/05/31/virus_ransoms_files/

[MS advises users to play safe with Word](http://www.theregister.co.uk/2006/05/24/ms_word_security_workaround/) (24 May 2006)

http://www.theregister.co.uk/2006/05/24/ms_word_security_workaround/

[Cybercops and zero day vulns](http://www.theregister.co.uk/2006/04/24/infosec_blog_three/) (24 April 2006)

http://www.theregister.co.uk/2006/04/24/infosec_blog_three/

[Unofficial zero-day patches gain corporate support](http://www.theregister.co.uk/2006/04/04/0-day_patch_survey/) (4 April 2006)

http://www.theregister.co.uk/2006/04/04/0-day_patch_survey/

[Patches released for zero-day IE threat](http://www.theregister.co.uk/2006/03/29/ie_patches_released/) (29 March 2006)

http://www.theregister.co.uk/2006/03/29/ie_patches_released/

[UK.gov repels zero day WMF attack](http://www.theregister.co.uk/2006/01/24/uk_gov_wmf_attack/) (24 January 2006)

http://www.theregister.co.uk/2006/01/24/uk_gov_wmf_attack/

[Zero-day WMF flaw underscores patch problems](http://www.theregister.co.uk/2006/01/13/security_wmf_microsoft/) (13 January 2006)

http://www.theregister.co.uk/2006/01/13/security_wmf_microsoft/

[Zero-day holiday](http://www.theregister.co.uk/2006/01/05/secfocus_zeroday/) (5 January 2006)

http://www.theregister.co.uk/2006/01/05/secfocus_zeroday/

© Copyright 2007