



[Home](#)[About](#)[News](#)[Events](#)[Distributor Opportunities](#)[Reseller Opportunities](#)[Add To Your Site](#)

Womble Worm Spreads Via Bush Email

Published 20th September 2006

If you receive an email with subject lines 'Bush' or 'FIFA', carrying an attached image, do not open it. Security experts at MicroWorld technologies inform that the email drops a worm named 'Womble.d' in your computer, when you try to open the attachment.

'Womble.d' is a mass mailing worm created in VC++, packed with UPX. It proliferates by gathering email addresses from infected computers and sending self copies to those addresses.

Subject lines of the mail are chosen randomly from a list that contains entities like Bush, FIFA, Incredible!, Paula, Miss Khan, Lola, Look at this, Re:info and alike. Some of the attachments found are, new_picture.jpg, some_info.wmf, firefox_update.pif.zip and seduction_secrets.pif, again chosen from random combinations.

"You may not smell a rat when you get an image file as an attachment from your close buddy. The worm is smart in Social Engineering as it has a varying range of subject lines to pick from, in order to cash in on different tastes and interests that people have, while it's sure to hit the bull's eye at least in some cases," says Arti Taru, Security Analyst, MicroWorld Technologies.

Womble.d exploits 'SetAbortProc Code Execution' vulnerability in Windows, by causing an error in handling specially crafted 'Windows Metafile' file types. The vulnerability can also be exploited when users visit websites hosting malicious files. The security patch for this flaw was released in January 2006 by Microsoft, available at

<http://www.microsoft.com/technet/security/bulletin/MS06-001.msp>.

eScan and MailScan from MicroWorld Technologies, safeguard users against online threats like these by continuously updating themselves with protection for latest Viruses, other malware and Vulnerability Exploits. The solutions also employ highly advanced heuristic methods to tackle disguised and emerging threats.

"This worm points towards the need for comprehensively protecting your Web Access and email communication against even file types normally considered harmless. GIF and JPEG are common place in websites and mail attachments, and nobody really wants to lose one's personal files or the PC itself to a remote attacker, after being lured to dabble with those specially created baits. Your Security Mechanism must stay alert even when your reflexes deceive you," says Govind Rammurthy, CEO, MicroWorld Technologies.

