



<b>DE LA SALLE LIPA</b> INFORMATION SERVICES DEPARTMENT Services Directorate		Document #: VTW-090206	Version: 1	Revision: 000
Title: <b>*** VIRUS-TROJAN-WORM ALERT ***</b>			Page: 1 of 3	
Date Issued: 09 February 05		Date Effective: 09 February 05		

<b>PROFILE</b>	
Name	Win32:VB-CD2
Type	Worm/Trojan
Propagation	Email Attachments
Affected OS	Windows
Side effects	<p>Sends itself to email addresses found on the infected computer</p> <p>Modifies data on the computer</p> <p>It kills processes of miscellaneous antivirus and security programs and deletes files of them. The worm is destructive, tries to delete files of certain types every 3-rd day in month</p>
Aliases	Net-Worm.Win32.Mytob.dc
<b>DETAILED DESCRIPTION</b>	
<p>W32:VB-CD2 is a mass-mailing worm.</p> <p>When executed, the worm creates one of the listed files:</p> <ul style="list-style-type: none"> <li>• %windows%\Rundll16.exe</li> <li>• %system%\New winzip file.exe</li> <li>• %system%\sample.zip</li> <li>• %system%\winzip_tmp.exe</li> </ul> <p>and files:</p> <ul style="list-style-type: none"> <li>• %system%\scanregw.exe</li> <li>• %system%\update.exe</li> <li>• %system%\sample.zip</li> <li>• %system%\winzip.exe</li> </ul> <p>The worm is <b>autostarted</b> with Windows using the registry key</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run          Its item „ScanRegistry” has the value “%System%\scanregw.exe /scan”</p> <p>The worm collects mail addresses from documents on the infected computer. The infected mail has <u>one of the following Subjects</u>:</p> <p><b>*Hot Movie*</b>  <b>A Great Video</b>  <b>Arab sex DSC-00465.jpg</b></p>	

eBook.pdf  
Fuckin Kama Sutra pics  
Fw:  
Fw: DSC-00465.jpg  
Fw: Funny :)  
Fw: Picturs  
Fw: Sexy  
Fwd: image.jpg  
Fwd: Photo  
give me a kiss  
Miss Lebanon 2006  
My photos  
Part 1 of 6 Video clipe  
Re:  
Re: Sex Video  
School girl fantasies gone bad  
The Best Videoclip Ever  
the file  
Word file  
You Must View This Videoclip!

The infected attachment is in the file named

007.pif  
04.pif  
677.pif  
document.pif  
DSC-00465.Pif  
eBook.PIF  
image04.pif  
New\_Document\_file.pif  
photo.pif  
School.pif

Sometimes, the attachment is MIME encoded and uses one of the names

3.92315089702606E02.UUE  
Attachments00.HQX  
Attachments001.BHX  
Attachments[001].B64  
eBook.Uu  
Original Message.B64  
SeX.mim  
Sex.mim  
Video\_part.mim  
WinZip.BHX  
Word\_Document.hqx  
Word\_Document.uu

In such case, special tool is needed to unpack and execute the worm.

On every 3-rd day of month, the worm **tries to delete** data files with the extensions \*.dmp, \*.doc, \*.mdb, \*.mde, \*.pdf, \*.pps, \*.ppt, \*.psd, \*.rar, \*.xls, \*.zip

MORE INFO at <http://www.avast.com/eng/win32-vb-cd-alias-kamasutra.html>