ARCHIVE MAY 2000

Yet another mutant of the infamous love bug is now unleashed, even more dangerous than the one before. This one changes its name each time it is opened, and then resends to everyone in an Outlook address book, before severely damaging your hard disk.

Since most of these viruses have a common weakness, this is what you should do IMMEDIATELY:

- Always be suspicions of any attachment - whoever it appears to be from. These viruses send me
- Always look carefully NOT at the name of the attachment, but at the bit at the end of the name - a
- Update your virus software online.

These three simple steps will dramatically reduce vulnerability to the current batch of viruses.

McAfee has a brilliant virus library

For more see below on latest mutation from Sophos.com.

Name: VBS/NewLove-A

Aliases: VBS/Loveletter.ed, VBS/Loveletter.Gen, VBS_SPAMMER,

VBS.Loveletter.FW.A, NEWLOVE.A, VBS/Spammer.A,

VBS.Loveletter.FW, Spammer, Newlove

Type: Visual Basic Script worm

Sophos and the FBI issued an alert on 19 May 2000 about a new polymorphic email-aware worm which has been reported in the wild. The worm, called VBS/NewLove-A is a Visual Basic Script virus that mutates its appearance in an attempt to avoid detection by anti-virus products.

If you are infected it will chooses a random filename and attempts to forward a mutated version of itself to everybody in your Microsoft Outlook address book. The name of the file it forwards is determined by randomly choosing one of the filenames in your WindowsRecent folder, appended with ".Vbs" (eg EXPENSES.XLS becomes EXPENSES.XLS.Vbs). The filename attached will have one of the following extensions: Doc.Vbs Xls.Vbs Mdb.Vbs Bmp.Vbs Mp3.Vbs Txt.Vbs Jpg.Vbs Gif.Vbs Mov.Vbs Url.Vbs Htm.Vbs The message has the subject line: "FW: <filename>" where filename is name of the file it is forwarding, with the extension ".Vbs" removed. So, if the attached infected file is README.DOC.Vbs then the subject line will be "FW: README.DOC". Because of this VBS/NewLove-A does not use the same filename or subject line on different infections. The email message has no message text. The virus attempts to reduce all files on local and remote drives to zero. This means that Windows may stop working correctly, and that your system will not start up properly upon reboot.

Users who have disabled Windows Scripting Host (WSH) on their computers will not be infected by this virus. Details on how to disable WSH are published at: http://www.sophos.com /support/faqs/wsh.html

Users who are blocking any Visual Basic Script filename (the infected message always arrives with end suffix of ".Vbs" on the filename) will not be affected. Due to the way in which the virus mutates, it rapidly increases in size on each infection. This means that your mail server may become increasingly slowed down by larger and larger amounts of email.

Sophos researchers are working on a method of detecting this virus, and will be issuing an update.