

Virus Alert

As of the writing of this column there are over 61,000 known viruses in the world. The Klez virus has been infecting more computers this past month than I have seen in all of my years in the computer industry. It was “discovered” on April 17th, 2002.

Here is what Symantec (The Norton Antivirus people) have to say about the Klez virus:

- **Payload:** This worm infects executables by creating a hidden copy of the original host file and then overwriting the original file with itself. The hidden copy is encrypted, but contains no viral data. The name of the hidden file is the same as the original file, but with a random extension.
 - **Large scale e-mailing:** This worm searches the Windows address book, the ICQ database, and local files for email addresses. The worm sends an email message to these addresses with itself as an attachment.
 - **Releases confidential info:** Worm randomly chooses a file from the machine to send along with the worm to recipients. So files with the extensions: ".mp8" or ".txt" or ".htm" or ".html" or ".wab" or ".asp" or ".doc" or ".rtf" or ".xls" or ".jpg" or ".cpp" or ".pas" or ".mpg" or ".mpeg" or ".bak" or ".mp3" or ".pdf" would be attached to e-mail messages along with the viral attachment.
- Because this worm uses a randomly chosen address that it finds on an *infected* computer as the "From:" address, numerous cases have been reported in which users of *uninfected* computers received complaints that they sent an infected message to someone else.

For example, Linda Anderson is using a computer that is infected with W32.Klez.H@mm. Linda is not using an antivirus program or does not have current virus definitions. When W32.Klez.H@mm performs its emailing routine, it finds the email address of Harold Logan. It inserts Harold's email address into the "From:" portion of an infected message that it then sends to Janet Bishop. Janet then contacts Harold and complains that he sent her an infected message, but when Harold scans his computer, Norton AntiVirus does not find anything - as would be expected - because his computer is not infected.

If you are using a current version of Norton AntiVirus and have the most recent virus definitions, and a full system scan with Norton AntiVirus set to scan all files does not find anything, you can be confident that your computer is not infected with this worm.

As you can see, viruses are becoming more stealthy and smarter than ever before. So if your computer is acting “funny” and maybe becoming extremely slow, consider that you may be infected with a computer virus. I read one article that stated that 1 in every 30 emails is infected with the Klez virus. This indicates just how prevalent and serious this latest virus is.

For more information on viruses please visit www.securityresponse.symantec.com.

