USC-OIA Special Virus Report

Volume 1, Issue 3 **Fall 2002**

Virus Guidelines

Kara Kelly, Information Security
USC Office of Information Assurance

What are Viruses?

- A virus is a malicious program or piece of computer code that replicates itself and may cause damage to a computer system.
- Viruses will quickly use all available memory and bring the system to a halt.
- Some viruses have destructive payloads, hide within other files and are activated when a user opens an infected file.

How do Viruses Infect Computers?

- To infect a computer, a virus needs to be able to execute its code.
- Viruses transmit via executable code in EXE, COM and DLL files, boot sectors of floppy disks, or macros inside data files such as Word, and via emails, floppy disks, and CD ROMs.

Protection Against Computer Viruses

- Install good anti-virus software and run daily virus pattern updates
- Subscribed to an email virus alert service such as Symantec's that warns about new viruses. (http://nct1.symantecstore.com/virusalert)
- Do not open e-mail attachments from unknown people.
- Disable Active Scripting in Internet Explorer: Select "Tools," then "Internet Options." Click the "Security" tab. Click "Internet Tab" then click "Custom level." Go to "Scripting" then "Active Scripting" and click "Disabled" button.
- Turn of Windows Scripting Host so no VBS files will be able to run
- Do not propagate virus hoax and chain mail.
- Before passing around any floppy disk always run a virus check before hand
- Write-protect floppy disks before inserting them into other users' computers. To write protect a floppy disk go to the back bottom right of the disk and move the slider from the "unlocked" position (shown as an open lock) to the "locked" position (shown as a closed lock). If the slider is removed the disk will remain permanently locked. If the disk is being passed to other computers, it's a good idea to permanently lock the disk, especially if it's being used to install a program. Always remember to run a virus check before passing any disk to another computer.

continued on page 2

Inside This Issue

continued from page 1

What are the different types of computer virus?

Macro viruses - Common viruses that make use of the macro functionality in Microsoft Office within Word, Excel, Access, PowerPoint or Project and infect all subsequent documents opened or created**.**

Visual Basic Script (VBS) Viruses - Viruses that often pretend to be something that they are not such as the Anna Kournikova virus and in some cases can infect simply by opening or previewing infected email with Outlook or Outlook express. Remember to turn of Windows Scripting Host so no VBS files will be able to run.

Boot Sector Viruses – Viruses that infect the boot sector of a floppy disk. Any files on the disk or subsequently saved to it will also be infected. Always remember to run a virus check before passing any disk to another computer.

Hoaxes - Hoaxes are not actual viruses but emails pretending to be warnings about viruses, get-rich-quick schemes, etc. Hoaxes rely on users to forward them to other users. For a list of hoaxes refer to http://www.symantec.com/avcenter/hoax.html.

Jokes - "Joke" programs will not perform any malicious action on your computer. Joke programs are often annoying programs, which attempt to display something humorous or only pretend to perform a malicious action. For a list of Joke programs refer to http://www.symantec.com/avcenter/jokes.html

Virus Links

The links listed below are a good source of information

Symantec - http://www.symantec.com/

Trend Micro - http://www.trendmicro.com/

CERT - http://www.cert.org/ - Publishes Virus alerts and fixes and is located at Carnegie Mellon University.

USC-CIAS glossary - http://www.usc.edu/infosec/resources/glossary.html

Latest Virus Report

Klez.H - The Klez.H worm uses a technique known as "spoofing" in which it randomly chooses addresses 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.

The worm obtains the email addresses that it places in the FROM: field from the infected user's address book and this causes a non-infected user to appear as the person who has sent this worm's malicious email. It does this to hide the real sender of the infected email. The actual email address of the sender is found in the "headers" From field.

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

As the virus can use its own SMTP engine, there have been several other examples of messages that appear to be "postmaster bounce messages". For example, if a user's email address is janedoe@anyplace.com, a user could receive a message that appears to be from postmaster@anyplace.com, indicating that the user attempted to send email and the attempt failed.

The email message that this worms sends is composed of "random" subject strings.
The virus subject lines that our office has most commonly seen are:

- Worm Klez.E immunity;
- Undeliverable mail--"[Random word]";
- Returned mail--"[Random word]";
- a [Random word] [Random word] game;
- a [Random word] [Random word] tool;
- a [Random word] [Random word] website;
- a [Random word] [Random word] patch;
- [Random word] removal tools;
- meeting notice
- meeting request
- how are you;
- japanese girl VS playboy;
- eager to see you;
- spice girls' vocal concert;
- japanese lass' sexy pictures.

continued from page 2

Please ensure that any antivirus applications are installed, running, and current and that Virus definitions are updates on a daily basis. Please refer to Symantec Norton Antivirus at http://www.symantec.com/avcenter/venc/data/w32.klez.h@mm.html for removal instructions. .

CREDITS and REFERENCES: Information from the following sources was used in the preparation of this notice:

Symantec
http://www.symantec.com/avcenter/venc/data/w32.klez.h@mm.html

Trend Micro
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_KLEZ.H&VSect=T

FOR INFORMATION ON THESE AND OTHER TOPICS REFER TO THE WEB SITE AT WWW.USC.EDU/INFOSEC

Return Address
Street Number and Name
City, State 98765-4321

BULK RATE
US POSTAGE
PAID
PERMIT NO.
00000

ADDRESS CORRECTION REQUESTED

Mailing Address
Street Number and Name
City, State 98765-4321