The Computer Virus

**What is a computer virus?**

* It is a program which attaches itself to, overwrites, or otherwise replaces another program in order to reproduce itself without the knowledge of the PC user.

**Why virus is called a “Virus”?**

* Computer viruses are called computer viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer like a biological virus passes from person to person.

**What can a virus do?**

* It may cause random damage to data files.
* It can occupy disk space or main memory by using CPU processing time and by the time and expense wasted in detecting and removing them.

**Why do people create computer virus?**

* Some people think its funny to create mischief, by creating viruses.
* Some people are intellectual who want the challenge to create a program that replicates itself. Too often, the program replicate itself too well and too fast and accidentally does more harm than the programmer intended.
* Why do people create computer virus?
* Some people are angry, to get revenge they create viruses.
* Some people want to become famous by inventing viruses.
* People who create viruses tend to be immature. Many are teenagers or disgruntled college students.

**Factors that led to the creation of viruses**

* The spread of PC
* The use of computer bulletin boards to download programs.
* The use of the floppy disks.

**The history of computer virus**

**The first computer virus**

* 1983, Fred Cohen invented the first computer virus as an innocent experiment in computer security. He didn't harm anybody, his virus stayed in his lab.

**The first virus that run on PC**

* The Brain was invented in 1986. unfortunately it accidentally escaped from its lab. It was found the next year in the University of Delaware.

**The first destructive viruses**

* The Jerusalem Virus . It was first noticed at the Hebrew University of Israel in 1987. It was believed to have been invented by the programmer in Italy.
* 1988, magazines began running articles saying computer viruses really exists.
* Researchers began to invent anti-virus programs to protect against viruses and destroy them.
* 1989, anti-virus program was distributed to general public .
* The nasty programmers writing viruses began protecting their viruses against the anti-virus programs.

**Virus Mischief**

* Some virus print nasty messages containing four -letter words or threats or warnings to make you worry and waste lots of your time and prevent you from getting work done.
* Some viruses erase some files, or even your entire hard disk.
* Some viruses screw up your computer so it prints wrong answers or stop functioning.
* Some viruses clog your computer, by giving the computer more commands than the computer can handle so the computer has no time to handle other tasks, and all useful computer tasks remain undone.

**What is a “Payload”?**

* The damage done by a virus.
* Some viruses are “benign” their payload is small. Others have big payload.
* If virus destroys all your files, it is said to have a destructive payload.

**2 main propagation tricks**

* **Trojan Horse** – they look like a pleasant gift program, but it secretly contained destructive viruses that destroy your computer.
* **Time Bomb** – They purposely delay damaging your computer until you’ve accidentally transmitted the virus to other computers, then several weeks or months after you’ve been secretly infected others, they suddenly destroy your system and you don’t know why.

**How the virus spreads**

* Sharing programs with other people.
* Piracy (Pirates are people who share programs illegally)
* From major software company

**Viruses can be transmitted by. . . . .**

* Booting a PC from an infected medium.
* Executing an infected program.
* Opening an infected file.
* Common routes for virus infiltration includes. . . . . ..
* Floppy disk or other media that user can exchange.
* Email attachments.
* Pirated software
* shareware

**How infection occurs**

* A virus has to have a chance to execute codes.
* Good vehicles for virus includes part of the disk which contain code executed whenever that disk is booted
* Documents that contains macros
* Whenever you run an infected program, the viruses copies itself to RAM memory chip, stays there and infect every program you try to run and copy.
* It looks for unused spaces, breaks itself up and put pieces of itself into unused spaces. Thus, the virus is undetected.

**Virus Symptoms**

* Slower operation
* Decreased memory
* Disk drive LED lighting up for no apparent reason.

**7 kinds of viruses**

**1. File viruses ( parasitic virus)**

It secretly attached itself to an innocent program so the innocent program becomes infected.

Example

* Yankee Doodle (Bulgaria, Sept. 1989). Every day at 5PM it plays part of the song “Yankee Doodle” on the built-in speaker.
* Die Hard 2( South Africa in July 1994) it makes the computer hang and overwrites ASM files.
* Chernobyl (Taiwan, June 1998) It erases your hard disk on April 26th every year.

**2. Boot-Sector Viruses**

A virus that hides in the boot sector. Whenever the computer tries to boot from a drive containing the infected disk the virus copies itself into the RAM. It makes your computer hang.

Example

* Stoned (New Zealand, Dec.1987) your computer will beep and display message like “your computer is stoned”
* Michael Angelo (Sweden, April 1991) sits quietly on your hard disk until Michael Angelo’s birthday, Each year the virus tries to destroy all data on hard drive by writing garbage everywhere.
* Monkey (USA, Oct.1992) encrypts the HD’s partition table so the HD is accessible just while the virus is in memory.

**3. Multipartite Virus**

It hides in two places: the boot sector and the file system

Stealth polymorphic armored multipartite virus(SPAM virus) –a very smart virus

Stealth virus- makes special effort to hide itself.

Polymorphic virus- changes its appearance each time it infects a file.

Armored virus- protects itself against anti-virus disassembly.

Example

* One Half (Austria, Oct. 1994) It slowly encrypts the hard drive. Each time you turn on the computer, the virus encrypts two more cylinders. When about half of the hard drive’s cylinders are encrypted, the computer says “this is one half, Press any key to continue. . . .”

**4. Macro Viruses**

It hides in macros which are programmed embedded in Microsoft Word and Spreadsheets. The virus spreads when you give somebody a copy of the documents.

Example

* Melissa (USA, March 1999) the virus tries to email copies of the infected document to the first 50 people mentioned in your outlook address book. With the subject “important message from”. It was invented by David L. Smith.
* Example
* Class (USA, Oct 1998) It just displays a stupid message on your screen occasionally.
* Thus (USA, Aug 1999) It lurks there until Dec. 13th when it erases drive C. It is “thus” because the macro program begins with the word thus.

**5. E-mail Worms**

A malicious program that comes as an email attachment and pretends to be an innocent fun.

Example

* Pretty Park (France, May 1999) It shows a drawing of a boy wearing a hat. The boy is Kyle from the “South Park” TV cartoon show

Subject: C:/Cool Programs/Pretty Park.exe

Body: Test Pretty Park.exe ☺

* Free Link (USA, July 1999)

Subject: Check this

Body: Have fun with links, Bye.

It says “This will add a shortcut to free XXX links on your desktop, Do you want to continue?”

* Love Bug (Phil., May 2000)

Subject: I Love You

Body: Kindly check the attached loveletter coming from me

Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs

**Deeds of “ I Love You”**

* It sends copy to your contacts.
* It wrecks graphic files and some programs.
* It makes your computer download from an internet in the Philippines, a program misleadingly called “WIN-BUGSFIX.EXE” (steals your password)

**6. DOS Attacks**

Your computer can attack internet web site server computer by sending so many strange requests to the target computer that it can’t figure out how to respond to them all. It get confused and ignores all other works.

Example

* Trin00
* TFN (Tribe Flood Network)
* TFN 2K

**7. Hoaxes**

An email message that contains a scary incorrect rumor and warns you to pass the message to all your friends. It is not a program, it’s just a document.

Example

* Good Times (USA, May 1994)
* Bad Times (USA, Dec. 1997)
* Email tax (Canada, April 1999)

**Anti-Virus Measures**

* **Preparation-** making back-ups of all software and making a contingency plan.
* **Prevention** – creating user-awareness, implementing hygiene rules, using disk authorization software or providing isolated quarantine PC’s
* **Detection-** the use of anti-virus software to detect, report and disinfect virus.
* **Containment**- identifying and isolating the infected items
* **Recovery-** disinfecting or removing infected items and recovering or replacing corrupted data.

**Applicable and Practical Guidelines to Follow if you suspected that your computer has a virus.**

* Do not attempt to work with an infected file system or let other people do so.
* Switch an infected system off until a competent person deal with it.
* Assume that all the machines are infected check it take appropriate steps if infection is found.
* Avoid spreading infection any further
* Users should not trade disks with others until their system and disks are cleaned.
* If there is an infected machine, don’ use floppy or any removable disks.
* Applicable and Practical Guidelines to Follow if you suspected that your computer has a virus.
* No files should be exchange between machines by any other means until it’s established that this can be done safely.
* Ensure that anyone else in your school are aware of the situation
* Get all floppy disks and removable disks together for checking. Check all backups too.
* Try to get experts help before doing anything else.

**Anti-Virus Software**

These are programs that can be installed in your computer and can scan and remove known viruses which you may have contracted

It can also be a set of automatically scanned diskettes when inserted into the disk drives scan files when downloaded to the internet, or scan email when received.

**What is a Definition Files?**

These are update files for anti-virus software

**Popular Anti-Virus Programs**

* Norton
* McAfee
* Sophos
* AVG
* Avast
* EZ Trust
* PC-cillin
* Nod 32
* Avira