Computer Viruses

What is a Computer Virus?

- Computer virus refers to: a program which damages computer systems and/or destroys or erases data files.
- Computer virus: A program inserted into a computer system to perform some sort of malicious purpose.
- Once it's running, it spreads by inserting copies of itself into other executable code or documents.
- Some have no purpose besides to spread and self replicate.
- As of April 2012, Symantec security company had upwards of 18 million Virus Definitions

Typical things that some current Personal Computer (PC) viruses do

- Display a message
- Erase files
- Scramble data on a hard disk
- Cause erratic screen behavior
- Freezing the PC
- Many viruses do nothing obvious at all, except spread!

Executable Viruses

Traditional Viruses.

- pieces of code attached to a real program.
- run when that program gets executed.
- loads itself into memory and looks around to see if it can find any other programs on the disk.

Boot Sector Viruses

- A boot sector virus infects boot sector of computers. During system boot, boot sector virus is loaded into main memory and destroys data stored in hard disk.
- infect the boot sector on floppy disks and hard disks.
- load itself into memory immediately, and it is able to run whenever the computer is on.

E-mail Viruses

- Moves around in e-mail messages.
- Replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.
- Example: Melissa virus, ILOVEYOU virus

Different names of "Viruses"

- Malware is the proper definition of a computer virus
- Adware, Spyware, Worms, Ransomware, Trojan Horses.

First “Computer Virus”

- John von Neumann- 1949
- Theory of self-reproducing automata
- His design for a self-reproducing computer program is considered the worlds first computer virus.

Some Famous virus

Jerusalem Virus

- First detected in Jerusalem 1987
- Believed to have been made in Italy
- Affected the DOS operating system
- Infects .EXE and .COM files
- On every instance of Friday the 13th, deletes every program file that was executed.

Happy99

- Written by French virus programmer “Spanska”
- First appeared mid-January 1999
- Spread through emails.
- Automatically attaches to all send emails after infection.
- Besides spreading and advertising itself, no real damage to computer

ILOVEYOU worm

- Created by two Filipino computer programmers
- May 5th 2000
- Attacked tens of millions of Windows PC's
- Programmed in Visual Basic Script
- Spread via email
- Estimated $5.5-8.7 Billion in damages worldwide
- Considered one of the most damaging worms ever

Flame

- Discovered in 2012, espionage malware
- Has the ability to record audio, Skype conversations, screenshots, keyboard activity, network traffic, and convert the host computer to a Bluetooth beacon and download contact information from Bluetooth enabled devices
- Targets Middle Easters countries, has been detected elsewhere

Actions to prevent virus infection

1. Always update your anti-virus software at least weekly.
2. Back up your important files and ensure that they can be restored.
3. Change the computer's boot sequence to always start the PC from its hard drive.
4. Don't share Drive C: without a password and without read-only restrictions.
5. Empty floppy drives of diskettes before turning on computers, especially laptops.
6. Forget opening unexpected e-mail attachments, even if they're from friends.
7. Get trained on your computer's anti-virus software and use it.
8. Have multiple backups of important files. This lowers the chance that all are infected.
9. Install security updates for your operating system and programs as soon as possible.