COMPUTER VIRUSES AND ITS MANAGEMENT

Edited by:

Dr. Gajanana Prabhu B.

Assistant Professor

Department of P G Studies & Research in Physical Education

Kuvempu University

What is computer virus?

- Computer virus refers to a program which damages computer systems and/or destroys or erases data files
- Computer viruses are called 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.

- The term 'computer virus' was first formally defined by Fred Cohen in 1983.
- Computer viruses never occur naturally. They are always induced by people.
- Once created and released, however, their diffusion is not directly under human control.
- After entering a computer, a virus attaches itself to another program in such a way that execution of the host program triggers the action of the virus simultaneously.
- It can self-replicate, inserting itself onto other programs or files, infecting them in the process.

- Not all computer viruses are destructive though. However, most of them perform actions that are malicious in nature, such as destroying data.
- Some viruses wreak havoc as soon as their code is executed, while others lie dormant until a particular event (as programmed) gets initiated, that causes their code to run in the computer.
- Viruses spread when the software or documents they get attached to are transferred from one computer to another using a network, a disk, file sharing methods, or through infected e-mail attachments.
- Some viruses use different stealth strategies to avoid their detection from anti-virus software.

Definition of Virus

- A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.
- A virus is a small piece of software that piggybacks on real programs in order to get executed
- Once it's running, it spreads by inserting copies of itself into other executable code or documents

Characteristics of a Virus

- Viruses have four essential characteristics.
- SELF REPLICATION: First, viruses are notable for the ability to replicate itself to infect computers, much like its biological counterpart. By replicating itself it is able to spread across computer systems and networks to infect as much as it possibly can.

- EXECUTABLE PATH: Second, before the virus can do anything, it must be executed. If it cannot be executed, it is harmless. To get itself to replicate it hitches a ride by attaching itself to an executable program. It has to modify the program involved to also execute the virus code. The virus is usually attached to a common executable such as the operating system, which is automatically executed on startup. It may also attach itself to a commonly executed file that a specific company may use.

- SIDE EFFECTS: Third, viruses do not just contain self-replicating code; they also contain what is called a payload. The payload is similar to a warhead on a missile; it is the side-effect of the virus. The payload has the potential to be malicious, but it does not have to be.
- DISGUISE: Lastly, the virus will be able to disguise itself before it is noticed by its side-effects. There are two methods of disguise, encryption and interrupt interception.

WHAT VIRUSES MAY DO TO A COMPUTER

- Delete files.
- Varies messages in files or on programs.
- Changes volume label.
- Randomly overwrites sectors on the hard disk.
- Marks clusters as bad in the FAT (file allocation table)
- Replaces the MBR (master boot record) with own code.
- Create more than one partition.

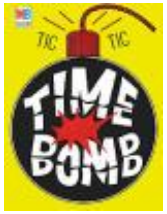
- Causes cross-linked files.
- Causes a "sector not found" error.
- Cause the system to run slow.
- A directory may be displayed as garbage.
- Directory order may be modified so files, such as COM files, will start at the beginning of the directory.
- Causes keyboard keys to be remapped.

Signs Your Computer is Infected

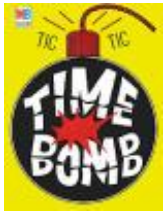
- Functions slower than normal
- Responds slowly and freezes often
- Restarts itself often
- See uncommon error messages, distorted menus, and dialog boxes
- Notice applications fail to work correctly
- Fail to print correctly

Types of Computer Virus

- Time Bomb
- Logical Bomb
- Worm
- Boot Sector Virus
- Macros Virus
- Script Virus
- Trojan Horse



Time Bomb



A **time bomb** is a virus program that performs an activity on a particular date

Logical Bomb

A **logical bomb** is a destructive program that performs an activity when a certain action has occurred.

Worm Virus

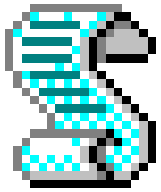
A **worm** is also a destructive program that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped

Boot Sector Virus

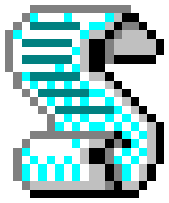
A **boot sector virus** infects boot sector of computers. During system boot, boot sector virus is loaded into main memory and destroys data stored in hard disk

Macro Virus

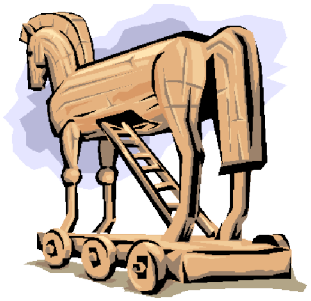
A **macro virus** is associated with application software like word and excel. When opening the infected document, macro virus is loaded into main memory and destroys the data stored in hard disk



Script Virus

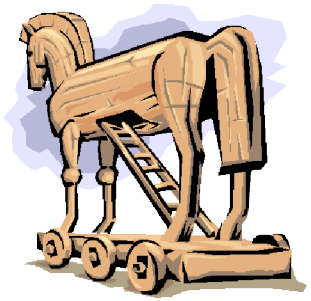


Commonly found script viruses are written using the Visual Basic Scripting edition (VBS) and the JavaScript programming languages



Trojan Horse

Trojan Horse is a destructive program. It usually pretends as computer games or application software. If executed, computer system will be damaged.



Trojan Horse

Trojan Horse usually comes with monitoring tools and key loggers

Actions to prevent virus infection

- **Update** anti-virus software at least weekly.
- **Back up** important files and ensure that they can be restored.
- Computer's boot sequence should always **start the PC from its hard drive**

Actions to prevent virus infection

- **Don't share Drive C**: without a password and without read-only restrictions.
- **Empty floppy drives of diskettes** before turning on computers, especially laptops.

- **Do not** open unexpected e-mail attachments, even if they're from friends.
- **Install** computer's anti-virus software and use it.
- **Keep** **multiple backups of important files**. This lowers the chance that all are infected.

- **Install security updates** for your operating system and programs as soon as possible.
- **Keep** learning more about computer. This will help in spoting viruses.

THANK YOU