

Name

Hamza Ali

Class

7:7

BSIT 1st Semester

Roll No

7:7

IT-G1-143

Assignment

7:7

Intro to ICT

Topic:-

"Computer Viruses and their
Types."

-: Computer Viruses:-

A computer virus is a type of ~~harmful~~ software, or malware that infects computer and corrupts their data and software.

Virus is also a programs that are develop for damage the computer components and other sensitive information resources.

Many viruses pretend to be legitimate programs to trick users into executing them on their devices.

-:-Types of Viruses:-

There are nine main virus types, some of which could be packaged with other malware to increase the chance of infection and damage. The nine major categories for viruses on computer are:

1. Boot Sector Virus

The computer drive has a sector solely responsible for pointing to the operating system so that it can boot into the interface. A boot sector virus damages or controls the boot sector on the drive.

Attackers usually use Harmful USB devices to spread this computer virus.

The virus is activated when users plug in the USB drive

and boot their machine.

2. Web Scripting Virus

Most Browsers have defenses against malicious web scripts, but unsupported browsers have vulnerabilities allowing attackers to run code on the local device.

3. Browser Hijacker

A computer virus that can change the settings on your browser will hijack browser favorites, the home page, URL and search preferences.

The site could be a phishing site or an adware page used to steal data or make money for the attacker.

4. Resident Virus:

A virus that can access computer memory and sit dormant until a payload is delivered is considered a resident virus.

This malware may stay dormant until a specific date or time or when a user performs an action.

5. Direct Action Virus

When a user executes a seemingly harmless file attached to malicious code, direct-action viruses delivers a ~~photo~~ payload immediately. These computer viruses can also remain dormant until a specific action is taken or a timeframe passes.

6. Polymorphic Virus

Malware authors can use polymorphic code to change the program's footprint to avoid detection. Therefore, it's more difficult for an antivirus to detect and remove them.

7. File Infector Virus

To persists on a system, a threat actor uses files infector viruses to inject malicious code into critical files that run the operating system or important programs. The computer virus is activated when the system boots or the programs run.

8. Multipartite Virus

These malicious programs spread across a network or other systems by copying themselves or injecting code into critical computer resources.

9. Macro Virus

Microsoft Office files can run macros that can be used to download additional malware or run malicious code. Macro viruses deliver a payload when the file is opened and the

macro runs.

10. Network Virus:

Network Viruses are extremely dangerous because they can completely cripple entire computer networks. They are often difficult to discover, as the virus could be hidden within any computer on an infected network. These viruses can easily replicate and spread by using the internet to transfer to devices connected to the network.

11. Trojan Horse

A Trojan Horse is a type of program that pretends to be something it is not to get onto a device and infect it with malware.

A Trojan Horse virus is a virus disguised to look like something it is not. For Example,

Viruses can be hidden within unofficial games, applications, file-sharing sites, and bootlegged movies.

12. Worm

A computer worm is not a virus. Worms do not need a host system and it can spread between systems and network without users actions, whereas a virus requires users to execute its code.