



4

Computer Virus

Connect

- How do you feel when you are sick?

I have fatigue

- Do you work quickly or become lazy?

.....

- How do you feel after taking the medicine?

.....

Learn

You will learn about:

- | | | |
|-------------------------|-----------------------------------|---------------------------|
| ✦ Introduction to virus | ✦ Different forms of virus attack | ✦ Ways to prevent a virus |
| ✦ Types of virus | ✦ Symptoms of virus attack | |

Task

Have you ever noticed your computer behaving in an odd manner, slowing down or shutting down abruptly? If you have noticed any such occurrences, your computer system is at risk. What can be the risk? It may be infected by some computer virus(es). In that case, it needs proper medication. Now, read more about the symptoms and its medicine.

VIRUS

The full form of **VIRUS** is Vital Information Resources Under Seize. A **computer virus** is a program that reproduces itself (Fig. 4.1). It may be attached to other programs or it may create copies of itself. It may damage or corrupt data, change data, or degrade the performance of your system by utilizing resources such as memory or disk space. It can also hack your computer system and share the information with the hacker's systems.

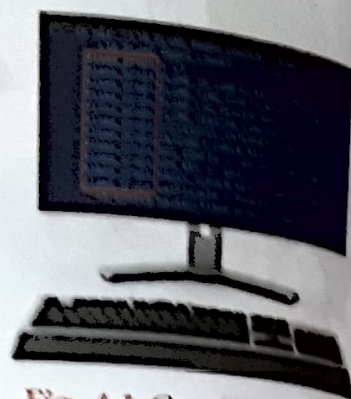


Fig. 4.1 Computer virus

TYPES OF VIRUS

A computer virus may be categorized as:

BOOT SECTOR VIRUS

Boot sector virus infects the computer by copying the code to the boot sector. It replaces the valid contents with its own infected version. When the computer starts, the virus is loaded into the computer memory. Then it easily infects the disks.

For example, Parity Boot, which displays the message PARITY CHECK and freezes the operating system. Other examples include Disk Killer, Stoned virus.

PROGRAM FILE VIRUS

Program file virus infects the files on the computer system. It resides in the root of a host file and then begins its operation when the file is executed. When the file is opened, it overwrites the file. It can also infect files with .exe, .com, .sys file extensions. For example, Sunday, Cascade.

MACRO VIRUS

Macro Virus infects Microsoft Word or Microsoft applications that provide support for Macros. Whenever the application runs, the virus gets activated and damages the formatting of the document. Since these files are sent through mails, a computer network can be easily infected by these viruses. They are relatively harmless. For example, Melissa, W97M.

MULTIPARTITE VIRUS

Multipartite Virus is called a **multi-part** virus or **hybrid** virus. It infects computer systems multiple times and at different times. It can infect both program files and boot sectors, thus causing more damage than any other kind of virus. In order to **eradicate** the entire virus, it must be removed from the system. The first multipartite virus was the Ghostball virus and was discovered in 1989 by Fridrik Skulason.



Eradicate: to get rid of

DIFFERENT FORMS OF VIRUS ATTACK

Viruses, Worms, Trojans, Spyware, Adware, Keyloggers and Ransomware are all forms of malware. Malware is an umbrella term used to refer to a variety of forms of virus. Malware is a combination of two words malicious and software and is developed for the purpose of harming the computer system.

WORMS

Worms infect and multiply without targeting and infecting specific files already present on the computer. They may show up via email, network or instant message software and then create more emails or messages to get spread. They often do not cause much damage by deleting files on the computer. There are many worms that attempt to disable firewalls, antivirus software and other security elements. They delete start up registry keys, terminate active processes and cause other similar damages.



Fig. 4.2 Worms

TROJAN HORSE

Trojan horse, also known as a Trojan, is a program or file that a user unknowingly allows or invites into his or her computer system. The user is tricked into believing that the program or file is just a normal software. In reality, the program or file contains malware. The malware takes control over the system, or provides a way for an outsider to reach in and control it. In many cases, Trojan horse installs software called a **keystroke logger**. This software permits them to capture and store all keyboard activities and mouse clicks. This may not sound dangerous, but such a malware can easily hack your account names and passwords, credit card numbers or bank account information stored in the computer system.

Tech Fact

Creeper

The first virus named Creeper was detected on APRANET in 1987. The virus on APRANET displayed a message "I'M THE CREEPER: CATCH ME IF U CAN".

The Concept virus

The Concept virus got accidentally shipped on a CD-ROM supplied by Microsoft in 1995. It was the first virus to infect Microsoft Word documents shared via email.

The Melissa virus

The Melissa virus, written by David L. Smith, was the first successful email-aware virus and inserted a quote 'from The Simpsons into Word documents'. Smith was later sentenced to jail for causing over \$80 million worth of damage.

The Morris worm

In 1998, Robert Morris, a university student, released a worm that affected 60,000 computers connected to the Internet, slowing them down to a stop.

OSX/RSPlug Trojan

In November 2007, the first malware for Apple Macs was discovered. The launch of the OSX/RSPlug Trojan increased fears that Apple's platform may be targeted more by hackers in future.

II SPYWARE

Spyware is a program that is put in someone's computer, to secretly gather information about the user and spread it to those who are interested with harmful intentions. Spyware can get into a computer as software virus or as a result of installing a new program.

It uses a lot of computer memory and in turn makes it slow. Adware and tracking cookies are examples of spyware.

Adware displays ads on your computer. It is the least dangerous among all the other forms.

Keyloggers records everything you type on your computer in order to obtain sensitive information such as log-in names, passwords and send it to the source of the keylogging program.

Ransomware is a type of malicious software. It blocks access to your computer and threatens to pay a ransom. There is no guarantee that paying the ransom will return access or the data will not be deleted.

Explore

Activity 1

- A. Do smartphones also get infected by viruses? Find out about the first virus that infected a mobile phone.
- B. Find out about Friday the 13th virus.

II SYMPTOMS OF VIRUS ATTACK ON A COMPUTER

Computer viruses are created by humans who have intentions to create problems for others. But, by creating computer viruses, they also make the users aware of the need to pay attention to their computer systems.

You will encounter irritating pop-ups when you browse the web. Some pop-ups will check system clock regularly and activate at a particular date and time. The most harmful ones will erase all your files. Others will attack the system memory and BIOS. This will make the operating system impossible to boot.

The computer virus enters the computer system without the knowledge of the user. The action which virus performs on the computer is called **payload**. The different effects of payload or symptoms of virus attack on a computer are:

- Deletes files
- Formats the hard disk
- Degrades performance
- Large scale emailing, often received in the Spam box
- Causes system instability
- Releases confidential information such as passwords or credit card numbers
- Compromises security settings

Tech Fact

A computer virus cannot infect files through CDs. Also, they do not infect any hardware.

Activity 2

Checkpoint

Match the columns.

1. Malware	a. Pen drives
2. Virus usually spread through	b. McAfee
3. Virus does not affect	c. Malicious software
4. Antivirus software	d. Peripheral devices

HOW DOES MALWARE GET INTO A COMPUTER?

The most common way for malware to get into a computer is through the Internet. Sometimes, the malware is embedded in the software or game that you download from the Internet. When the program is installed, the malware gets installed simultaneously. Then, it infects the computer with its effects.

Virus also enters through infected pen drives. It will begin to work immediately when you open the pen drive or its contents. Some viruses become active only till the infected application is running. Some viruses become active every time you switch ON the computer. Common method for a worm to enter the computer is through an email. The worm might attach itself to an email. Usually, the message will have an enticing header. The user will click it and the program will start to run.

There are some malware running from Web-based scripts. All the users have to visit many websites while running the Internet. So, when the users visit the website, the script activates itself and self-installs in the PC. The facts about computer worm viruses show that these are among the most dangerous types of malware. They can really harm and damage the computer to a great extent.

WAYS TO PREVENT A VIRUS

As the saying goes, 'Prevention is better than cure'. Before the computer system encounters a virus infection, following measures can be taken:

- Install **antivirus software**, which will detect, prevent and remove malware. After installation, run its update feature regularly. By keeping it updated, it will be able to detect the threat immediately.
- It is recommended to update the computer with the latest version of antivirus, as new viruses are being detected. When you run an **antivirus program**, it scans for the database of viruses. This database of viruses is called **virus definitions**. The database and the reports related to the malware are also stored in the antivirus for records. You can also see the infected files placed on your computer. Be careful the next time for such files.



Fig. 4.3 Antivirus program

Activity 3

Explore

In order to install any antivirus software, you either need to purchase or download it from the Internet. To install an antivirus software, follow the steps:

Step 1: Run the installation file.

If you have the latest CD-ROM, run the **Install.exe** file on the CD drive to start the installation process.

Step 2: Follow the steps in the Installation wizard.

Step 3: Select the antivirus installation language and click **Next**.

The wizard prompts you to read and accept the license agreement.

Step 4: Click **Yes**.

The next screen gives you the chance to change the program installation drive. If you wish to install another location, click **Browse** and select the location.

Step 5: The computer memory scan starts. Once the scan is complete, click **OK**.

Step 6: Once all the files have been copied, restart the computer and click **Finish**.



- Always backup your files. If the network has been infected, clean it first before backing up the files or attaching any external device to it.

Tech Help

Data backup is a process of keeping a duplicate copy of the original files. It is said to be the best prevention and cure for data loss. It is an activity of copying files or databases so that the data will be preserved in case of any accidental or intentional deletion of the data.

- Scan the pen drive before use. Download only from secured websites.
- Even though email services have virus scanners, run a thorough scan on any attachment you get. If you get an .exe or script attachment from someone you do not know, delete it. When browsing the web, keep your antivirus scanner ON. This will keep malicious scripts away.

Activity 4

Explore

Make a list of the latest antivirus software available in the market.

Tech Fact

The first antivirus programs appeared in 1987 from G. Data Software for the Atari ST software. Later, in the same year, VirusScan was introduced by John McAfee, which later became the McAfee antivirus program.

HACKER

Hacker is a term used to describe a person who is a clever programmer. The hacker tries to break into your computer system to get information or destroy it.

A hacker enjoys learning details of a programming language or system. Thus, hacking involves the act of becoming an expert to get into someone else's computer.

Activity 5

Discuss

Do you think a programmer is a good one if he/she creates viruses that are used to attack other systems?

Recap

- ✧ Malware is a malicious software.
- ✧ The different types of virus attacks are virus, worm, Trojan horse and spyware.
- ✧ The full form of VIRUS is Vital Information Resources Under Seize.
- ✧ The first virus named Creeper was detected on APRANET in 1987.
- ✧ It is recommended to update the computer with the latest version of antivirus.
- ✧ Data backup is said to be the best prevention for data loss.