Viruses and Worms

- While discussing the virus and worm, it is important to first understand the larger category of malicious programs, called "Malware".
- Malware can be defined as a special kind of code or application specifically developed to harm electronic devices or the people using those devices.
- Viruses and worms are both types of malware; however, there are significant differences between them.

What is Virus?

- A Virus is a program developed using malicious code with a nature that links itself to the executable files and propagates device to device.
- Viruses are often transferred through the downloaded files and the shared files.
- They can also be attached with a scripting program and non-executable files like images, documents, etc.
- After the user executes the infected program, the virus gets activated and starts replicating further on its own.

Viruses can harm the system by the following means:

- Filling up the disk space unnecessarily
- Formatting the hard disk drive automatically
- Making the system slow
- Modify, or delete personal data or system files
- Stealing sensitive data

How does a virus spread?

- The virus does not have the capability of spreading itself.
- It requires the host and human support to spread.
- The virus is developed in such a way that it attaches itself to the executable files.
- It further spreads when the infected executable file or software is transferred from one device to another.
- As soon as a human launches the infected file or a program, the virus starts replicating itself.

What is a Worm?

- Worms are the type of virus that can self-replicate and travel from device to device using a computer network. That means worms don't need any host to spread.
- They are standalone computer malware that doesn't even require human support to execute.
- Usually, worms use computer networks by exploiting vulnerabilities, and that makes them spread more quickly.

How does a worm spread?

Unlike viruses, worms don't require host files to spread. This means that worms do not attach themselves with executable files or programs. Instead, worms find a weak spot in the system and enter through a vulnerability in the network. Before we detect and remove worms from our system, they replicate and spread automatically and consume all the network bandwidth. This can result in the failure of the entire network and web servers. Because worms can spread automatically, their spreading speed is comparatively faster than other malware.

Basis	WORMS	VIRUS
Definition	A Worm is a form of malware that replicates itself and can spread to different computers via Network.	A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.
Objective	The main objective of worms is to eat the system resources. It consumes system resources such as memory and bandwidth and makes the system slow in speed to such an extent that it stops responding.	The main objective of viruses is to modify the information.
Host	It doesn’t need a host to replicate from one computer to another.	It requires a host to spread.
Harmful	It is less harmful as compared.	It is more harmful.
Detection and Protection	Worms can be detected and removed by the Antivirus and firewall.	Antivirus software is used for protection against viruses.
Controlled by	Worms can be controlled by remote.	Viruses can’t be controlled remotely.
Execution	Worms are executed via weaknesses in the system.	Viruses are executed via executable files.

Basis	WORMS	VIRUS
Prevention	● Keep your operating system and system in updated state ● Avoid clicking on links from untrusted or unknown websites ● Avoid opening emails from unknown sources ● Use antivirus software and a firewall	● Installation of Antivirus software ● Never open email attachments ● Avoid usage of pirated software ● Keep your operating system updated ● Keep your browser updated as old versions are vulnerable to linking to malicious websites
Types	Internet worms, Instant messaging worms, Email worms, File sharing worms, Internet relay chat (IRC) worms are different types of worms.	Boot sector virus, Direct Action virus, Polymorphic virus, Macro virus, Overwrite virus, File Infector virus are different types of viruses
Examples	Examples of worms include Morris worm, storm worm, etc.	Examples of viruses include Creeper, Blaster, Slammer, etc.
Interface	It does not need human action to replicate.	It needs human action to replicate.
Speed	Its spreading speed is faster.	Its spreading speed is slower as compared to worms.
Comes from	Worms generally come from the downloaded files or through a network connection.	Viruses generally come from the shared or downloaded files.

What is a Trojan Horse?

- The name of the **Trojan Horse** is taken from a classical story of the Trojan War.
- It is a code that is malicious in nature and has the capacity to take control of the computer.
- It is designed to steal, damage, or do some harmful actions on the computer.
- It tries to deceive the user to load and execute the files on the device. After it executes, this allows cybercriminals to perform many actions on the user's computer like deleting data from files, modifying data from files, and more.
- Now like many viruses or worms, Trojan Horse does not have the ability to replicate itself.

Types of Trojan Horse?

Now there are many Trojans which are designed to perform specific functions. Some of them are: –

- **Backdoor trojan:** A trojan horse of this kind gives the attacker remote access to the compromised machine.
- **Ransom trojan:** This kind of trojan horse is intended to encrypt the data on the compromised system and then demand payment in exchange for its decryption.
- **Trojan Banker:** It is designed to steal the account data for online banking, credit and debit cards, etc.
- **Trojan Downloader:** It is designed to download many malicious files like the new versions of Trojan and Adware into the computer of the victims.
- **Trojan Dropper:** It is designed to prevent the detection of malicious files in the system. It can be used by hackers for installing Trojans or viruses on the victim’s computers.
- **Trojan GameThief:** It is designed to steal data from Online Gamers.

Uses of Trojan Horse?

- **Spy:** Some Trojans act as spyware. It is designed to take the data from the victim like social networking(username and passwords), credit card details, and more.
- **Creating backdoors:** The Trojan makes some changes in the system or the device of the victim, So this is done to let other malware or any cyber criminals get into your device or the system.
- **Zombie:** There are many times that the hacker is not at all interested in the victim's computer, but they want to use it under their control.

Prevention from Trojan Horse: The most basic prevention method: –

- Do not download anything like the images, and audios from an unsecured website.
- Do not click on the ads that pop up on the page with advertisements for online games.
- Do not open any attachment that has been sent from an unknown use.
- The user has to install the antivirus program. This anti-virus program has the capacity to detect those files which are affected by a virus.

What are Backdoors?

- A backdoor is an undocumented way to bypass existing cybersecurity measures and gain access to the computer system or device. Software and hardware developers sometimes install backdoors into their own products to retain access for troubleshooting purposes.
- Backdoor installation helps software developers solve various problems, for example, retrieve data from a device to aid a criminal investigation or restore users’ lost passwords. But the backdoors might also be exploited by hackers, but how?

How does a Backdoor attack work?

Backdoor attacks work in two ways.

- In the first scenario, hackers use a backdoor to circumvent normal security measures and gain unauthorised access to a computer system and its data.
- In the second one, they exploit system vulnerabilities to gain access into it and implant backdoor software. Once the backdoor is in, attackers can easily re-enter the system whenever they like, even if the vulnerabilities are fixed.

Types of Backdoor Attack

1. Administrative backdoors: Lots of software developers include backdoors in their programs to give them easy administrative access to various areas of their own systems. Doing so can help them to troubleshoot user problems and fix vulnerabilities quickly. However, if these backdoors are discovered by cybercriminals, they can be used to launch cyber attacks.

2. Malicious backdoors: A malicious backdoor is one created for a malicious purpose. This process may involve hackers installing backdoor malware through a targeted phishing email. If the hacker can eventually gain access to the code of an operating system, they can add backdoors to allow for easy access in the future.

Types of Backdoor Attack

3. Accidental backdoors: Many backdoors are just the result of human error. When a developer leaves a weak point in their internet security systems, it can go undetected for a long time. If bad actors find the flaw first, they can use it as a backdoor to the operating system or application.

4. Hardware backdoors: While most backdoor attacks involve hackers gaining remote access to networks and devices through software flaws, it's also possible to include hardware backdoors in the physical structure of a device. A good example is the Clipper chip that the NSA proposed. However, this approach is high risk for a cybercriminal because it requires physical access to a targeted device.

How to protect yourself from Backdoor Attack

Here are some steps you can take to protect yourself.

- Don’t use your work device for personal internet activity
- Report any unusual or suspicious incidents
- Use a VPN, especially while travelling
- Use strong passwords
- Enable firewalls
- Monitor network traffic