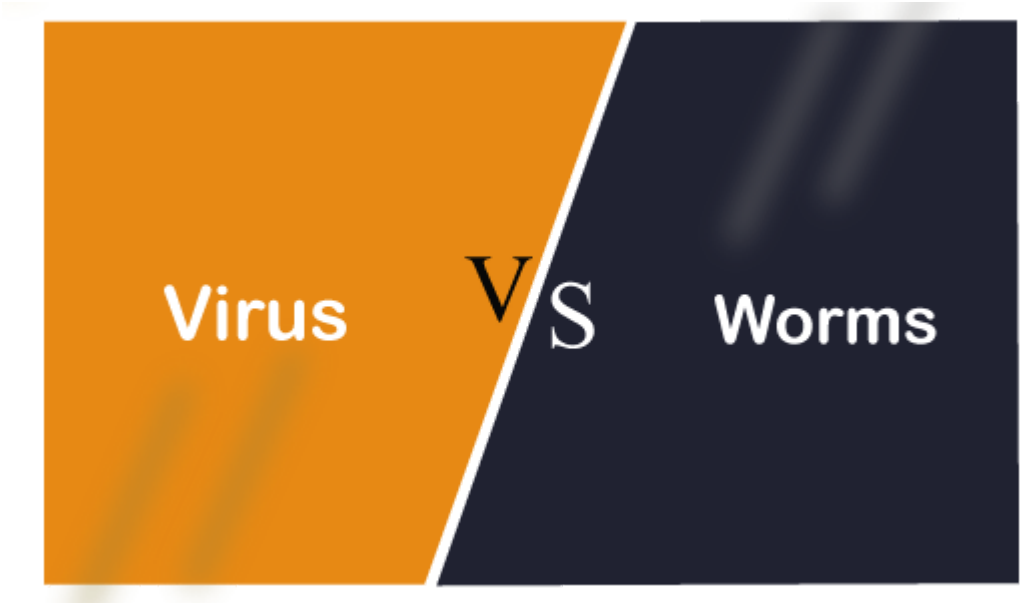
Difference Between Virus and Worm

While discussing the differences between 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.



In this article, we are discussing the significant differences between viruses and worms. Let's first understand both with the definitions:

What is a Virus?

According to the definition, a Virus is a program developed using malicious codes with a nature that links itself to the executable files and propagate 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. However, the virus remains dormant even after arriving on the device with the infected files. 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 human launches the infected file or a program, the virus starts replicating itself.

Typically, the infected program continues to work normally even after the viral infection. However, some viruses can overwrite all the infected program files, destroying the particular program altogether. Besides, the virus attaches itself to new executable files and repeats the entire vicious cycle all over again. This is the reason why the viruses spread at a slower speed. Usually, the viruses are transferred using collaboration apps, email attachments, network share, hard drive, and USB flash drive.

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.

Besides, worms stay within the memory of an infected computer, making a computer think they are part of the system files. This helps worms to avoid any suspicious detection. Unlike a typical virus, worms don't harm the system data. Instead, they tend to consume system resources like CPU, memory, or network bandwidth and make the entire system or network crash. Because of self-replicating nature, worms can even disrupt systems in a series worldwide using a network.

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.

Apart from this, worms can also reach other networks that are attached to the infected system. The most dangerous thing is that the worms can send themselves into other systems using email services.

Key Differences between Virus and Worm

Few key differences between Virus and Worm are listed below:

- Worms usually spread using a computer network, whereas viruses use executable files to spread from one system to others.

- Worms can automatically replicate to different systems, while viruses require human action to replicate.
- The spreading speed of viruses is comparatively slower than worms. Because worms can replicate automatically, they spread at a much faster speed.
- The viruses are designed to corrupt, delete, or modify the target devices' data or software, whereas worms don't harm the stored data but aim to harm the resources.
- Viruses are found in executable files or can attach themselves to executable files to operate on target devices, whereas worms remain independent in an infected device's memory.
- The viruses require hosts to spread from one device to another. Worms, on the other side, don't need any host.
- Viruses usually destroy and damage the stored data, whereas worms can harm the entire network by using maximum resources. For example- by consuming bandwidth, sending mass emails, or deleting or copying files in bulk.

Major Differences between Virus and Worm

The other major differences between a virus and a worm can be explained in a tabulated form, as below:

Attributes	Virus	Worm
Nature	The virus is a malicious program attached to the executable files so that it can spread from one system to another.	A worm is a program made up of malicious code that replicates itself and propagates itself from device to device using a network.
Human Action	Human action is required for viruses. Without human help, they cannot execute and spread.	Human action is not required for the worms. They are designed and developed in such a way that they can automatically execute and spread.
Speed of Spread	The virus spreads at a relatively slower speed than a Worm.	Worms spreading speed is fast, and they can infect multiple devices or networks quickly.

Host Requirement	The host is required to spread viruses. Viruses connect themselves to the host and travel with the host. They spread into devices where the host reaches.	The host is not necessary for the worms to replicate from one device to another. Worms exploit the vulnerability of a network to spread.
Protection Method	To protect the devices from viruses, the user must have installed trusted antivirus software.	To protect the devices from worms, the user is required to use antivirus software and a firewall. Many modern antivirus software come with an in-built firewall system.
Malware Removal	To clean the virus's infection or stop spreading it further, the user must scan the device using antivirus software and remove the infected files. Sometimes, formatting an entire system is the only option to remove the infection completely.	To remove the worm's infection, the user needs a virus removal tool. Also, users must allow only trusted software through a firewall to eliminate the chances of spreading worms. In a complex situation, formatting the system is the best option.
Consequences	Viruses can corrupt, alter, or delete the stored files or programs in the infected device.	Worms do not harm stored files or software; instead, they consume system resources and increase the system's load. This eventually leads to slow processing and system crashes. Also, it can result in network failures.

Which is more dangerous?

The impact of viruses and worms can be mild to severe. Both are developed to harm the computer and other devices. They can steal and damage the data of individuals, organizations, and government institutions. However, worms seem to look more dangerous because of their self-replicating nature. Also, they can spread faster than viruses. Worms can silently spread into multiple devices by detecting the vulnerability and then inset themselves by exploiting that vulnerability.

For instance, let's assume that a worm has attacked us. A worm will infect our emails and transfer itself to all our contacts. It can further replicate itself and spread to all of our contacts' contacts. By doing this, a worm can create an infinite cycle with huge potential damage and harm the resources of all the connected devices or systems.

Viruses, on the other side, cannot replicate themselves. They need human-support to start operating, and they are relatively slower at spreading. This makes them less dangerous than worms.

How to be safe from viruses and worms?

Viruses and worms can cause severe damage to the computer and other devices. It is not enough to only use antivirus software and a firewall system. We are required to follow proper safety guidelines to protect our devices against viruses and worms. Some of the best practices that can be followed to be safe from viruses and worms are given below:

- **Proactive**: Be cautious while opening an email from unknown people or sources. We should avoid clicking on links or attachments, which are part of the email unless we are sure that they are genuine. Several offers and banners look too good to be true (however, they are not in most cases).
- **Updates**: We should keep our software and operating system updated. Outdated software may have vulnerabilities, and attackers may benefit from sending viruses, worms, or other malware into our devices.
- **Ad-blocker**: Malware can cause many advertisements to appear on our computer screens, and those ads can be harmful if we accidentally click on them. Thus, it is best to install good ad-blocking software or browser extension to block all malicious ads.
- **Authorized Store**: We should be careful while downloading software on our devices. It is a best practice to download software from official websites or authorized application store. Many third-party stores are available on the internet, and most of them do not verify software safety.
- **Monitoring**: Analyzing and monitoring the system files and system activities' behavior can help us spot suspicious actions, if any. In case the system suddenly becomes slow, or there are several advertisements on the screen, such activities can be a sign of an anomaly. Scanning a full system using an antivirus can be beneficial in this situation.

← Prev

Next →

Feedback

- Send your Feedback to feedback@javatpoint.com

Help Others, Please Share

Learn Latest Tutorials

Splunk

SPSS

Swagger

Transact-SQL

Tumblr

ReactJS

Regex

Reinforcement Learning

R Programming

RxJS

React Native

Python Design Patterns

Python Pillow tutorial

Python Pillow

Python Turtle tutorial

Python Turtle

Keras tutorial

Keras

Preparation

Aptitude

Aptitude

Logical Reasoning

Reasoning

Verbal Ability

Verbal Ability

Interview Questions

Interview Questions

Company Interview Questions

Company Questions

Trending Technologies

Artificial Intelligence

Artificial Intelligence

AWS Tutorial

AWS

Selenium tutorial

Selenium

Cloud Computing

Cloud Computing

Hadoop tutorial

Hadoop

ReactJS Tutorial

ReactJS

Data Science Tutorial

Data Science

Angular 7 Tutorial

Angular 7

Blockchain Tutorial

Blockchain

Git Tutorial

Git

Machine Learning Tutorial

Machine Learning

DevOps Tutorial

DevOps

B.Tech / MCA

DBMS tutorial

DBMS

Data Structures tutorial

Data Structures

DAA tutorial

DAA

Operating System

Operating System

Computer Network tutorial

Computer Network

Compiler Design tutorial

Compiler Design

Computer Organization and Architecture

Computer Organization

Discrete Mathematics Tutorial

Discrete Mathematics

Ethical Hacking

Ethical Hacking

Computer Graphics Tutorial

Computer Graphics

Software Engineering

html tutorial

Web Technology

Software Engineering

Cyber Security tutorial

Cyber Security

Automata Tutorial

Automata

C Language tutorial

C Programming

C++ tutorial

C++

Java tutorial

Java

.Net Framework tutorial

.Net

Python tutorial

Python

List of Programs

Programs

Control Systems tutorial

Control System

Data Mining Tutorial

Data Mining

Data Warehouse Tutorial

Data Warehouse