Difference Between Virus and Worm

A virus is a harmful executable code that is attached to another executable file and can modify or erase data. When a computer software that is infected with a virus executes, it takes action, such as deleting a file from the computer system. Viruses are incapable of being manipulated remotely.

Worms are similar to viruses, but they do not alter the program. It continues to multiply itself, slowing down the computer system. Remote control of worms is possible. Worms' primary goal is to consume system resources. Worms don't need their host file to be activated. Once a worm has gained access to your computer, usually through a network connection or a downloaded file, it can run, self-replicate, and spread without the need for a trigger event.

Key Difference Between Virus and Worm

Computer viruses and worms are both capable of causing damage to a computer system. Hence, these two aren't exactly the same. Let’s discuss the main Difference Between Virus and Worm in the table below.

Virus	Worm
When a virus infects a file, the harmful code is copied and spreads across the host computer whenever subsequent files are opened.	To penetrate the gadget, a worm just needs a medium. This might be done via the internet, email, online messaging apps, and so forth.
In comparison to a worm, a virus takes less time to spread across the system.	A worm can spread swiftly through a device.

A virus is a destructive executable code that is attached to another executable file and can modify or erase data.	A worm is a type of malware that can replicate itself and spread over a network of computers.
It necessitates the presence of a host in order to spread.	It can replicate from one computer to another without the use of a host.
The primary goal of viruses is to alter information.	Worms' primary goal is to consume system resources.
Virus prevention is provided by antivirus software.	Antivirus and firewall software can identify and eliminate worms.
Viruses are incapable of being manipulated remotely.	Remote control of worms is possible.

Virus vs Worm

Viruses are frequently attached to or hidden in shared or downloaded files, both executable (a program that runs a script) and non-executable (a document or an image file). The virus remains dormant until the infected host file is activated once it is accepted or loaded by a target machine. The virus can only run after the host file has been activated, executing malicious code and replicating it to infect other files on your system.

A worm generates several copies of itself, which it then spreads throughout a network or over the internet. These copies will infect any unprotected PCs or servers that connect to the infected device through a network or the internet.