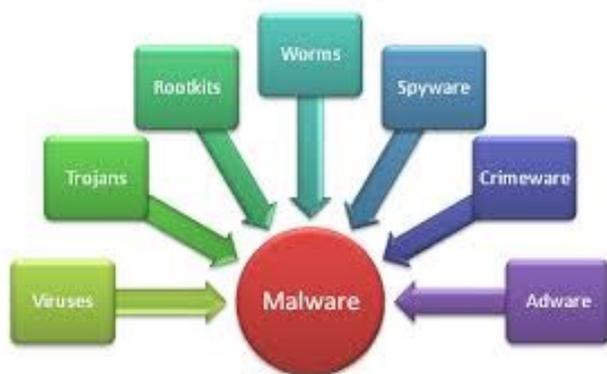


Malware is short for "malicious software."

The word malware is a combination of two words "malicious" and "software". It is a generic term used to describe all of the hostile and intrusive program codes including viruses, spyware, worms, Trojans, or anything that is designed to perform malicious operations on a computer.

The meanings of many of these words have changed over time. Some refer to how the malware infects your system while other words are used to describe what the malware does once it's active in your machine.

Malware is any kind of unwanted software that is installed without adequate consent. Viruses, Worms, and Trojan Horses are examples of malicious software that are often grouped together and referred to as malware.



Malware writers are very Skilled in using tricks to get users to download their malware.

Software that comes bundled with "other software" is often called a Trojan Horse.

For example:

1. An instant messenger software bundled with a program such as WildTangent, a known spyware offender.
2. Peer-to-peer file sharing software, such as Kaaza, LimeWire, and eMule, bundle various types of malware that are categorized as spyware or adware.
3. Software that promises to speed up the Internet connection or assist with downloads (e.g., My Web Search) will often contain adware.

Malware exploits security holes in your browser as a way of invading your machine. It is important to keep computer systems patched with the latest manufacture provided security patches.

Sometimes websites state that software is needed to view the site, in an attempt to trick users into clicking "Yes" thus installing software onto their machines.

Some malware provides no uninstall option, and installs code in unexpected and hidden places (e.g., the Windows registry) or modifies the operating system, thus making it more difficult to remove.

The Differences

Many PC users consider Malware, Viruses, Spyware, Adware, Worms, Trojans, etc. as the same thing. While all these infections harm our computers, they are not the same. They are all types of malicious software and each behave differently.

Spyware is a type of malware that functions by spying on user activity without their knowledge.

Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements.

A **virus** is a form of malware that is capable of copying itself and spreading to other computers.

Bots are software programs created to automatically perform specific operations.

A **Rootkit** is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs.

Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom.

A **Trojan horse**, commonly known as a "Trojan," is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware.

Worms (computer worms) are among the most common types of malware. They spread over computer networks by exploiting operating system vulnerabilities.