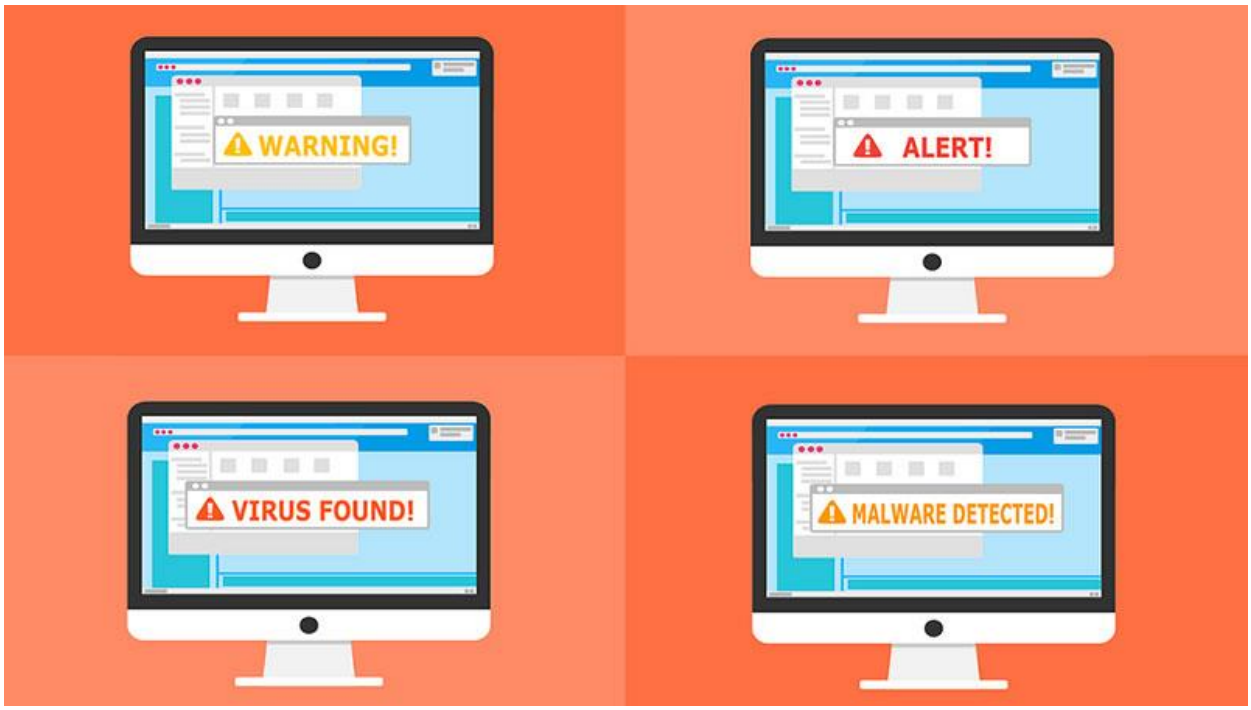
Types of Malware | Malware Classification

Well, you might have heard or come across the term malware, viruses, etc. It is a common misconception that malware is a virus. In this article, you will know the common types of malware that infects most of the people. If you are using a computer and accessing the internet, you probably need an anti-malware or antivirus to keep your computer protected from malware, you will know why in this blog post.

Before we go through the types of malware, let's understand "what is a malware" first.



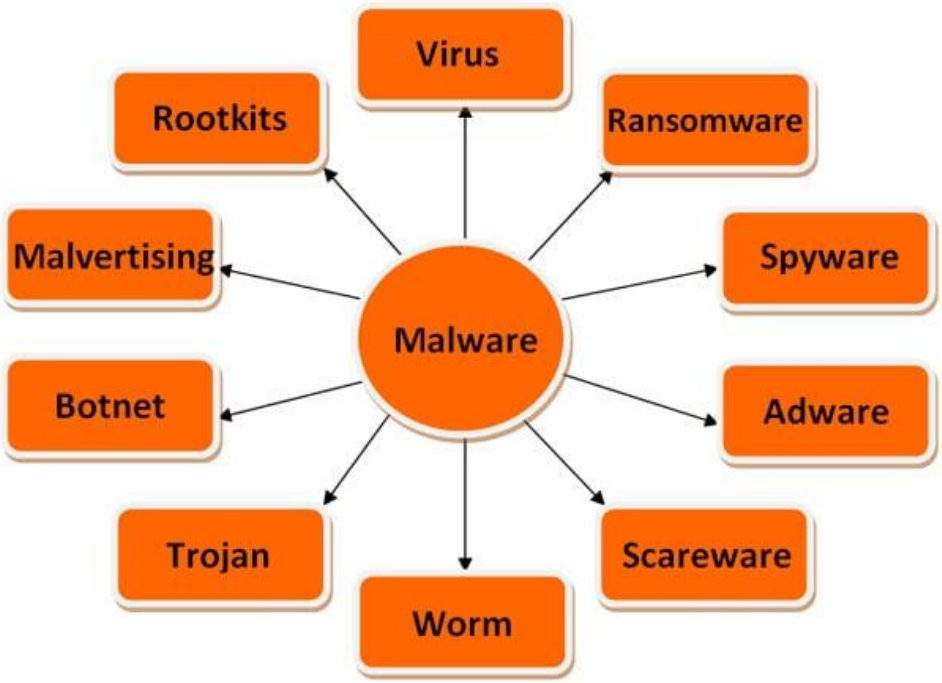
What is Malware?

Malware is the short form of **malicious software**. Any kind of software or program that is capable of performing malicious activities on your computer is called a malware. The malware can perform a simple task like showing a user some advertisements to even harm the computer hardware.

Malware is a broad term and literally represents all types of suspicious programs out there.

When it comes to categorizing the malware, one can classify it based on the activity the malware does and how they infect the host computer. The common types of malware that are widely used by hackers or cyber threats are the viruses, worms, trojans, spyware, adware, ransomware, rootkits and the list continues. But one type of malware can be bundled with other types as well and that is what most of the hackers target.

Different types of malware:



Virus:

It is a program often an exe file that is triggered by some user action either by running the executable manually or it can be embedded into MS office applications like excel or word in form of macros; so when a user opens a word/excel file, the exe is executed and replicates itself to other files present in the computer.

The virus needs user action every time to spread inside the host computer.

It can steal a user's personal data, store some files in your computer, show unwanted ads, or even infect your browser to access multiple information and there are many more.

The attacker can embed viruses on the software you download over the internet from untrusted sources. Once the program runs on any computer, it starts infecting the files and folders. If the infected files or folders are copied to another computer either through network transfer or through a storage device, then it becomes easier for the virus to spread. When a user opens a virus affected file unknowingly, the virus spreads itself.

To remove a virus, you need to have an antivirus with the latest virus signatures which are capable of removing the virus. These days due to the enormous number of viruses, the antivirus may not have the signature to remove it properly. As a result, the antivirus ends up quarantining the infected files or deleting the whole file rather than removing the virus.

Worm:

Unlike a virus, the worm has an extra capability to spread itself when put in a network. Of course, it needs a host action at the beginning to be activated, and then it keeps on self-replicating in the network of computers. The worm is smart enough to exploit the vulnerability of a computer and that is how it spreads in a network. A worm can often inject a virus, spyware into your computer to do a number of malicious activities.

Due to the self-replicating nature of the worm, it is easier for the anti-malware programs to understand the malicious behavior of the worm and can remove it easily. But if not taken care of at the earliest, it can infect the whole network within a few minutes.

The difference between a virus and a worm is that the worm is self-replicable and needs user action at the beginning to start an infection whereas a virus needs user action every time in order to spread.

Basically, the virus and worm are the types of malware that can self-replicate whereas there are other types that deceive the user to perform manual action and the malware exists as long as the user is using the application. A trojan is such an example.

Trojan:

Trojan horse, commonly known as trojan is not a virus because it can't replicate itself and spread in the computer. Hackers often embed trojans in some computer applications or software. When you install and start using the application, the trojan starts doing its job, let's say for an example it utilizes your CPU or network bandwidth to do whatever it is programmed to do. There are no such limitations that this malware can't do. Even a hacker can have a backdoor entry to your computer. That's where all the anti-virus, anti-malware companies come into the picture.

Often you might have seen warning messages while browsing over the internet that your computer is affected by a virus and it prompts a user to install antivirus software to remove it. In fact, the downloaded antivirus is a house for trojans. The so-called antivirus does its job and in the background, the trojan keeps running.

The ram cleaner, speed booster notifications in untrusted websites are a trap. So, be careful while downloading any software from any unknown sources.

Spyware:

You've guessed it right. Spyware is a program that spies on your activities and shares with the hacker. The typical malicious activity that this spyware can do is to get the passwords, bank account details, credit card details, etc.

You might have heard of keylogger software that records whatever you type using your keyboard. Keylogger is famous spyware that we know. The activity of the spyware is not limited to only spying; it may bring other malware along with it.

To give an example, the spyware can track and steal the user's browsing details, and based on that it serves customized advertisements. In some organizations, the administrator also puts the spyware to keep track of their employees. But without user consent, it is treated as malware.

Adware:

The adware is programmed to show advertisements on your computer, be it desktop notifications, browser pop up, etc. There are certain types of malware, specifically adware that changes the browser homepage and fills it with affiliate advertisements.

The adware most of the time does not harm your computer except showing targetted or irritating advertisements. But this adware can come with other malicious scripts as well.

These adware installs software on your computer or can install an extension in your browser. The adware if integrated with spyware can damage your privacy and steal your confidential information. The hackers often spy on the user to understand the browsing history and based on that they show targeted advertisements.

If your computer is infected with adware, you can go to your control panel or your browser extension panel to remove the unwanted programs/plug-ins. Most of the time, this works. If you feel the computer is still infected by adware, you can get anti-malware software to clean this adware.

Malvertising:

Even both the malvertising and adware target to show advertisements to the user is different based on how they operate; so don't get confused between this two malware. The malvertising type malware intercepts the ad code of the publisher's website and shows some phishing websites instead.

Often the hackers target the ad networks that serve ads on the publisher's website. The hacker replaces the ad code of the ad network with a phishing website to drive traffic wherever they want.

The user may not figure out as he is clicking on the legitimate advertisement banner and in the backend, the redirection happens and some other landing page appears for the user. Users can be tricked to enter personal details in the phishing websites and it can end monetary losses or again multiple spam emails if the hacker gets the email id.

Sometimes, malvertising can run cryptocurrency mining scripts on users' browsers which consume the CPU of the computer.

It can be difficult to trace the malvertising but the use of adblocker or proper anti-malware with web-protection can help to block the phishing websites.

Scareware:

As the name suggests, the scareware type malware targets end users and show some vulnerability to scare the users which often prompts users to install some software. The infected software downloaded becomes a way for hackers to achieve whatever they need.

The common examples of scareware are

- A pop up appears and shows that your computer is infected with a virus and prompts to clean it. Upon clicking the clean/remove button, either it downloads software or redirects to a malicious website.
- Sometimes browsing the internet through VPN, a pop up appears with a notice along with your IP address and can scare users that police can catch you if you don't install a VPN software

Ransomware:

The ransomware basically encrypts some of the important files in your computer and demands a ransom amount in return to decrypt it back. It also possesses the capability to lock down the entire computer.

The source of the ransomware can be any documents received from untrusted email id or any clickable link on the internet. Once downloaded, the ransomware looks for some important files on your computer and does its job. Once it finds any important file and encrypts it, the hacker sends a notice to the user to pay a ransom amount, else the hacker threatens to destroy the file.

WannaCry is famous ransomware that affected many computers. And asked its owner to pay a ransom amount in Bitcoin within 72 hours. Since bitcoin is not traceable, you can understand the brain behind this malware. In recent news, maze ransomware attacked some IT companies.

The hackers mostly target companies, financial institutions or government organizations to take control of the important data. Even after paying the ransom amount, there is no guarantee, you will get back your data. So, to get rid of any kind of ransomware attack, you need to have antivirus software that has anti-ransomware features. The best way to keep your data important data safe is to store them offline in external hard drives.

Rootkits:

Rootkits are very powerful malware that often hides inside the root of a computer, which means it is capable of penetrating into the deepest layer of the operating system where the anti-malware may not remove it.

Since the rootkits have access to the core of the OS, it can control the anti-malware software and can add itself to the exclusion list of the antimalware while searching for potential malware. In most cases, the computer may need formatting in order to clean this type of malware.

Since the rootkits have access to the operating system, it can override the hardware; and can cause overload and hardware failure as well.

A better way to remove rootkits is to have the software updated and the operating system patched every time there is an update available. By keeping the software up to date, we can minimize the chances of rootkit attacks.

Botnet:

A bot may not be a malicious program all the time but if used in a wrong way can harm a single computer or a network of computers. The botnet represents a network of computers affected by bots.

The botnet has the capability to compromise the system security by spamming the servers, stealing server data, and even cause a **Distributed Denial-of-Service (DDoS)** attack which makes the entire server unavailable.
You might have seen websites ask to solve CAPTCHA in order to access their system. This is the first level of security to prevent botnet attacks.

These are the different types of malware that are common to us and you should know.

But recently the malware attack has gone to the next level by using many transformation techniques. Based on the transformation technique of the malware, all the malware can be considered of two types.

1. Polymorphic malware
2. Metamorphic malware

Let's dig into details.

Polymorphic malware:

If you are from a programming background, you might be aware of polymorphism. Polymorphic malware got its name from polymorphism which means many forms.
The polymorphic malware keeps on changing the behavior which makes it difficult to detect by malware. The current anti-malware software tries to detect the malware based on their signature and due to the regular changing of signature of the polymorphic malware, it almost becomes undetectable.

This type of malware has become common these days and most of the viruses, worms, trojans are already following the polymorphic pattern.

Metamorphic malware:

As compared to polymorphic malware, the metamorphic malware is capable of changing the entire code which makes it much more difficult to trace. Every time the metamorphic malware infects a system, the whole code of the malware transforms to form a completely different malware using various permutations and combinations.

If compared with the metamorphic malware, the polymorphic malware is a little bit easier to detect as some code remains the same, and others are mutated.
In the current world, there are not many examples of metamorphic malware as it is difficult to develop.

The only way to get rid of these cyberthreats is to turn-on real-time protection and keep the anti-malware or antivirus software up to date. And in case of heavy infection, formatting the whole computer is a better solution.
You might have got a pretty decent idea on different types of malware by now; do you wonder how to know if your computer is infected by malware?

The malware may do many activities that can harm your computer. Here are some common symptoms that malware can exhibit.

Signs of malware:

1. High RAM/CPU usage
2. Computer becomes slower
3. Some unknown files/folders are created
4. Unwanted programs get installed in the control panel
5. Some unknown programs run in the background and appear in task manager which after killing the process, automatically starts

Now that you know what are malware and its types and the malware symptoms; you should know how to delete or get rid of malware from your computer or phone.

How to get rid of malware:

It is always better to prevent the malware attack than try to remove it after infection. Once the malware infects a computer it becomes difficult to remove it.

1. While browsing over the internet, make sure not to click on any suspected links from unknown sources.
2. Do not visit untrusted websites specifically when there is no https connection.
3. Do not open any email attachments from unknown senders.
4. Enable firewall all the time.
5. Update software and operating systems with the latest patches.
6. Have one anti-malware/antivirus installed on your computer with features like internet security, anti-ransomware, anti-trojan, etc.
7. Keep the antivirus software up to date whenever there is any update available to get the latest virus signatures.

Conclusion:

In this internet world, it may be difficult for us to get rid of malware completely but with a premium antivirus/anti-malware and little precaution, we can lower the risk of getting our computers exposed to malware.

I would suggest going for a paid antivirus as they keep their virus/malware signature up to date.

Any free antivirus program may already contain malware within it. So, be careful. Happy learning. ☺