

Forum:[Hack Forums](#)

Thread: [Malware and Prevention \[Beginner Edition\]](#)

Vyxn - April 21, 2018, 5:23 pm

[img]http://#/boQdjD.png[/img]

Overview

This guide will give you some idea and may help you on protecting your own personal computer from any type of malicious software. The information written here is intended for user who have not idea about this topic. All information here was gained from my own experiment and experience. Term definitions were came from lots of sources.

Demistifying Malware

The technology of today's world is changing really fast, so does malware. But what is malware in the first place?

Malware is a combination of malicious software which is a software that is written or intended doing harm to electronic data. The first recorded malware was from 1971 when Bob Thomas try the Theory and Organization of Complicated Automata of [John von Neumann](#) ([Click this for more details](#)). Malware has many many types and some of them are still active and scattered over the internet and waiting to be executed.

This are some types of the malware you may encounter:Computer VirusThe most common one and 11/10 you already knew about it. It is a type of malware which when executed, it propagates itself by creating a copy of itself. Some computer viruses may not be harmful, and some of the causes are real damages to the system.

WormsThe second most known type of malware is the worm which is also duplicate itself. Unlike virus, worm program doesn't requires the spreading of an infected host file. It does automatically travel from one computer to another.

Trojan HorseThis bad boy will deliver you a not-so-good experience. The words came from ancient greek story where a big wooden horse used as a gift. The receiver don't have any idea that this big wooden box contains a ton of soldiers that will later on invade their city and will result to their downfall.

For this story, I know you'll get what the trojan horse means in terms of computing. It tries to mimic a legitimate program or files but when executed, the malicious script will start to ruin your system.

RansomwareThis type of malware was in the news last year and created a massive damage (

[WannaCry \(2017\)](#) & [Petya\(2017\)](#)). Ransomware is a software that when executed, it will encrypt your files to make it unusable. The program will prompt some message after the encryption done showing the step to do to decrypt your files. Some ransomware wants you to pay a certain amount, but some of them just want you to teach you a lesson or have some fun ([PUBG Ransomware](#)).

Spyware This scary ass little shit does gather information to the infected victim without their knowledge. Most spyware runs in stealthy which means, it doesn't appear on their screens or no visual interfaces. The presence of this program may result to an unauthorized payment or identity theft.

Adware Adware or advertising-supported software is a program that generates profits to whoever made the program. Some of this program interrupts your work with some randomly annoying popup ads even you don't surf on the internet. Some of them where hidden in the background, eating your resources while the developer of the program are earning revenues.

Signs of Malware Infections

While some of the listed types of malware does an obvious signs, some are not.

Here's are some list that you may encounter: Slow computer performance While this may also be caused by an outdated software/hardware, this may also be caused by a malware infestation. Some malware has its own purpose, some of them just want to eat your resource to use for their own like malware with cryptocurrency miner. If the malware is written poorly, it will consume your system resources abnormally.

Suspicious Error Message Prompt This may also be caused by an outdated software/hardware, but I'll discuss what is this if malware is a suspect. This message may cause by corrupted files due to a malware infestation or a start of the infestation. Corruption of file may cause by computer viruses and other types of malware. Start of infestation is what you should really be aware of. If you read about Trojan Horse, a fake error message is one of its features and part of its social engineering mechanics to infect users.

Unusual setting changes A system updates may result in this but can also be caused by malware. Some of you may usually encounter about their browser with tons of extensions, and you have no idea where it came from, random website redirections, cannot access the internet properly because their dns was changed, registry changes, antivirus are disabled and more.

Random popup ads This is the ads that will pop up on your screens even you are not surfing the internet. The result may not only be an annoyance but be a more destructive damage due to the ads that may contain more malware.

System crashesAnother sign of malware infestation was the random system crashes. The reason was the malware made to do this, the malware is poorly written, and some malware uses this for their defence mechanism. When you try to end the process of this kind of malware, it triggers an error like BSOD (Blue Screen of Death), so you won't be able to disable them completely.

Malware Prevention

You know prevention is better than cure, right? Even though there's really no secure computer environment but at least this guide will lessen the percent of you being infected.

BE UPDATED!This will talks about your system and about yourself. Of course, on your system, you use this software that helps you on everyday task but this software may be an open gate to a malware so be sure to update it whenever there's an available. Update your operating system and your beloved security solutions. After the complete update, scan your computer with your antivirus/antimalware solution. ?

Screenshot of Update settings from Windows 10

For yourself, be updated about the news happening on the internet. Read about the latest exploits and hacking, so you know what to avoid. Don't forget to subscribe to a legit and accurate tech news site/blog.

INSTALL/EXECUTE CAREFULLYThe easiest way to get infected is by installing a random application from an unknown source. If you're using a Windows Operating system, there's a feature called [SmartScreen](#). SmartScreen filters all programs and will do its action by warning the user to block the specific program.

Settings of Smartscreen from Windows 10

Always get the software from its website and not on the random junk site. Cracking a program will also give a sweet load of malware so say no to cracking, dude.

Read the installation wizard before installing a piece of software. Even though you have downloaded some program on its website, some free programs have crapware/malware that will be installed if you don't uncheck them before you press the install button. Always choose custom installation. ?

Example of installation wizard with additional package to be installed.

Don't run if you're not sure what is it.

I'd like to thank our leader, [?BowmanBot?](#) for being a great leader. ?

?BowmanBot? - April 22, 2018, 7:11 pm

Great guide for beginners. Easy to follow and well put together.

Keep up the keep work!

Wake - April 27, 2018, 9:31 pm

Very informative thread. Will be redirecting new members to here to answer any questions they may have.

Makaveli The Don - April 28, 2018, 5:32 pm

Great thread. Thank you for your contribution Vyxn. Keep it up! ?

SIM-1729678 - April 29, 2018, 1:07 pm

Great thread, keep up the good work.

Marwiz - June 1, 2018, 3:59 am

This is a good and very informative thread, great work.

Mr.7 - July 10, 2018, 12:52 am

good information.

how can we prevent DOS and DDoS attacks.tell me how to implement the secure firewall for single system.

how to find the DoS and DDoS attacks while occuring on our system

delta248 - July 10, 2018, 10:10 am

(Jul 10, 2018 12:52 AM)Mr.7 Wrote: [\[CITE\]](#) good information.

how can we prevent DOS and DDoS attacks.tell me how to implement the secure firewall for single system.

how to find the DoS and DDoS attacks while occuring on our systemdos attacks arent malware!!1

To prevent a DoS attack, you can try various things - rate limiting, blocking certain attack patterns, etc.

But a DDoS attack... It depends. You can sometimes use the things mentioned above, and other times you can try balancing the load between a network of devices, but sometimes the attack might be too much. Since you're not setting up a web server (that's what I understood from what you said), things like CloudFlare aren't going to really help. But you can always try?

And discovering such an attack? when your internet is down and it isn't the isp you can always see it

Internet speed or lack of thereof, firewall logs, etc. are the things you'll probably need to have in mind.