7 computer viruses you should be careful

Serious virus infections can wreak havoc on the entire system. They can delete files, steal data and easily spread to other devices on your network.

Like viruses on the human body, computer viruses come in many forms and can affect your computer in many different ways.

Obviously, your computer will not need to rest or use antibiotics like humans, but serious virus infection can wreak havoc on the entire system. They can delete files, steal data and easily spread to other devices on your network.

Here are 7 types of computer viruses you should pay attention to.

7 computer viruses you should be careful

1. 1. Boot Sector Virus
2. 2. Virus Direct Action
3. 3. Resident virus
4. 4. Multipartite virus
5. 5. Polymorphic virus
6. 6. Virus overwrite
7. 7. Virus spacefiller

1. Boot Sector Virus

From a user perspective, Virus Boot Sector is one of the most dangerous viruses. Because they infect the master boot record, they are difficult to remove, and often require the entire system to be formatted. This is especially true if the virus has encrypted the boot sector or damaged the code too badly.

They are often spread by mobile means. They peaked in the 1990s when floppy disks were popular, but you can still find them on USB drives and in email attachments. Fortunately, improvements in the BIOS structure have reduced their popularity over the past few years.

2. Virus Direct Action

Virus Direct Action is one of the two main types of viruses that infect files (the other is resident viruses). Virus Direct Action does not install itself or 'hide' in your computer memory.

It works by attaching to a specific file type (usually EXE or COM files). When someone executes the file, it will "revive", searching for other similar files in the directory to spread to.

On the positive side, viruses often do not delete files or interfere with the performance of the system. In addition to making some files inaccessible, it only has minimal impact on a user and can be easily removed with an antivirus program.

3. Resident virus

Resident virus is a virus that infects files. Unlike direct action viruses, they install themselves on computers. This allows the virus to continue to function even when the source of the virus infection has been removed. Therefore, experts say they are more dangerous than the 'cousin' - the direct action virus.

Depending on how the virus is programmed, detecting them can be very complicated and even removing them is even more difficult. You can split resident virus into two groups: Fast infector (fast spread) and slow infector (slow spread). Fast infector causes destruction as quickly as possible and is therefore easier to detect; while slow infector is more difficult to recognize because their signs develop very slowly.

In the worst case scenario, the resident virus can even attach to your own antivirus software, infecting every file that the software scans. You often need a single tool, such as an operating system bug fix, to remove them completely. An anti-malware application will not be enough to protect you.

4. Multipartite virus

While some viruses can only be spread through a certain method or transmitted via a single payload, multipartite viruses can perform both methods. A virus of this type can spread in many ways and can perform various actions on the infected computer, depending on variables, such as the installed operating system or the existence of some files. certain.

The multipartite virus can simultaneously infect both boot sectors and executable files, allowing them to act and spread quickly.

Such two-way attacks make them difficult to remove. Even if you clean up all the program files in the computer, if the virus is still in the boot area, it will regenerate immediately after you restart the computer.

5. Polymorphic virus

According to Symantec, the polymorphic virus is one of the most difficult to detect or remove viruses with an antivirus program. Symantec claims anti-virus companies need to "spend days or months to create detection habits, necessary to capture a single polymorphic virus".

But why is it difficult to protect the computer from polymorphic viruses? The answer lies right in the name of this virus. Antivirus software can only list one variant of the virus. But a polymorphic virus changes its sign (binary model) every time it is cloned. For an antivirus program, it looks like a completely different kind of software, and therefore, can be removed from the blacklist.

6. Virus overwrite

For end users, the overwrite virus is one of the most annoying viruses, even if it's not particularly dangerous for your entire system.

That's because it will delete the content of any file that it infects. The only way to remove the virus is to delete the file, and therefore, the user loses the entire contents of the file. It can infect both standalone files and entire software.

Virus overwrite is often difficult to detect and spread via email, making them difficult to identify for average PC users. The heyday of this virus was in the early 2000s with Windows 2000 and Windows NT, but you can still find them now.

7. Virus spacefiller

Also known as 'cavity virus', spacefiller virus is smarter than most other viruses. The typical mode of operation of a virus is to simply attach it to a file, but the spacefiller viruses try to penetrate the free space that can sometimes be found in the file itself.

This method allows it to infect a program without damaging the code or increasing its size, so it does not need stealth detection techniques that other viruses rely on.

Fortunately, this virus is relatively rare, although the development of Windows Portable Executable files is opening up a new door for them.

As always, taking the necessary steps to protect yourself is better than being infected with the virus before finding a solution.

To get started, you need to use a highly rated antivirus software suite. Also, do not open emails from untrusted sources, do not trust the USB for free from conferences and exhibitions, do not allow strangers to use your system and do not install software from random websites !