Computer Viruses

What Are Computer Viruses?

Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation.

This definition is rather broad, because it contains everything from small viruses that duplicate your files and are just a mere annoyance to the dangerous ones that put a lock on your files and refuse to give you access to them until you pay a certain amount of money to its creator.

Virus attaches itself to files stored on floppy disks, USBs, email attachments and hard disks. A file containing a virus is called infected file. If this file is copied to a computer, virus is also copied to the computer.

Besides stealing information, computer viruses oftentimes:

- delete information off of your computer,
- corrupt files and make your computer act wonky and weird,
- use your e-mail address to spread itself to other users,
- take your files hostage until you pay a certain amount of money to the creator of the virus in order to release them.

In short: Computer viruses are small software programs created for malicious purposes that involve stealing information. They can easily hide themselves into small files such as images and attachments and infect your computer, after which they can multiply and send themselves as attachments using your e-mail address to other people in your list. The damages each virus can do to your computer varies according to the category it fits in. While some may corrupt your files, multiply them or delete them, others go as far as deleting everything from your hard disk or taking your data hostage until you pay a certain fee.

Activation of Viruses

When the computer virus starts working, it is called the activation of virus. A virus normally runs all the time in the computer. Different viruses are activated in different ways. Many viruses are activated on a certain date. For example, a popular virus “Friday, the 13th” is activated only if the date is 13 and the day is Friday.

Causes of Computer Viruses:

The following are the main causes of a Computer Virus.

Infected Flash Drives or Disks

Flash drives and disks are the main cause of spreading viruses. Flash drives and disks are used to transfer data from one computer to other. A virus can also be copied from one computer to other when the user copies infected files using flash drives and disks.

Email Attachments

Most of the viruses spread through emails. Email attachment is a file that is sent along with an email. An email may contain an infected file attachment. Virus can spread if the users opens and downloads an email attachment. It may harm the computer when it is activated. It may destroy files on the hard disk or may send the virus automatically to all email addresses saved in the address book.

Infected websites

Thousands of insecure websites can infect computer with viruses. Most of the websites with suspicion materials are infected, so by visiting these websites the user’s computer also gets infected by virus. These websites are developed to spread viruses. The virus is transferred to the user’s computer when this material is downloaded. These websites may access the computer automatically when the users visit them.

Networks

Virus can spread if an infected computer is connected to a network. The internet is an example of such network. When a user downloads a file infected with virus from the internet, the virus is copied to the computer. It may infect the files stored on the computer.

Pirated Software

An illegal copy of software is called pirated software. Virus can spread if user installs pirated software that contains a virus. A variety of pirated software is available in CDs and from the internet. Some companies intentionally add virus in the software. The virus is automatically activated if the user uses the software without purchasing license.

Types of computer viruses

Basic types of viruses:

Boot viruses: Boot viruses attack the boot sectors on your hard drive and interfere with your computer's basic operation, making your operating system run strangely or even corrupt it all together .

Macro viruses: Macro viruses tend to attack data files, like word documents and spreadsheets, causing you to loose files or cause your word or excel software to not work properly .

Trojan viruses: Trojan viruses pretend to be other software, hence their name as in the Trojan horse. Trojan viruses pretend to be a legitimate piece of software, but in reality can attack your hard drives, deleting files and re-writing system files, causing your computer to become unstable, particular when operating system files are deleted .

As a general rule, computer viruses only attack files in your computer. They do not attack your computer's hardware, like the monitor, mouse or keyboard .

However, some viruses will attack the files that operate your computer's hardware, causing hard drives to reformat, video drivers to be deleted or your operating system to stop running. While this may cause your monitor to stop working properly, it doesn't mean you need to get a new monitor .

Structure of a Virus

A computer virus has three parts:

Infection mechanism: How a virus spreads, by modifying other code to contain a (possibly altered) copy of the virus. The exact means through which a virus spreads is referred to as its infection vector. This doesn't have to be unique - a virus that infects in multiple ways is called multipartite.
Trigger: The means of deciding whether to deliver the payload or not.
Payload: What the virus does, besides spread. The payload may involve damage, either intentional or accidental. Accidental damage may result

from bugs in the virus, encountering an unknown type of system, or perhaps unanticipated multiple viral infections.

File Infectors

Operating systems have a notion of files that are executable. A file infector is a virus that infects files which the operating system considers to be executable; Where is the virus placed?

Beginning of a File

Very simple executable file formats like the .COM MS-DOS format would treat the entire file as a combination of code and data. When executed, the entire file would be loaded into memory, and execution would start by jumping to the beginning of the loaded file. In this case, a virus that places itself at the start of the file gets control first when the infected file is run.

End of a File

Appending code onto the end of a file is extremely easy. A virus that places itself at the end of a file is called an appending virus. How does the virus get control? There are two basic possibilities:

- The original instruction(s) in the code can be saved, and replaced by a jump to the viral code. Later, the virus will transfer control back to the code it infected. The virus may try to run the original instructions directly in their saved location, or the virus may restore the infected code back to its original state and run it.

- Many executable file formats specify the start location in a file header. The virus can change this start location to point to its own code, then jump to the original start location when done.

Anti-virus programs:

The broad definition for anti-virus programs is that they are one or multiple programs that have been designed with the specific purpose of preventing and destroying the malicious software (also known as the computer viruses) they detect on the user’s computer. These programs are very smart and they use all sorts of tricks in order to catch and destroy the malicious software on the user’s computer. They go as far as creating ‘bait files’ that the viruses will attack and thus get destroyed or quarantined. Things to remember when purchasing an anti-virus program:

- **Make sure it’s a full paid version** – the free ones just search your computer for patterns of malicious software they are already familiar with and they don’t do anything about the viruses they find on your computer. The full and paid version of the anti-virus program will use a variety of techniques to catch, destroy or quarantine the viruses on your computer.
- **Make sure you have an Internet connection** –the anti-virus programs need a constant internet connection in order to stay up to date on the virus definitions and make sure that they catch all of the malicious software / programs that can be found in your computer.
- **Don’t download anything that you don’t trust to be virus free**. No matter how pretty that wallpaper looks like or how much you want that new song, unless you know and trust the website, don’t ever download anything off of the internet. Oftentimes, those that create such malicious software hide it in plain sight – in .mp3 or .jpg files and once it reaches your computer, it’s very difficult to get rid of it.
- **Do some research before purchasing a certain anti-virus program**. As you probably know by now, the competition is fierce in the anti-virus industry, do some research, see what other people experienced with the same program and then decide whether to buy it or not.

How do anti-virus programs work?

The science behind anti-virus programs is not that difficult to understand. As mentioned previously, they were created with the sole purpose of stopping the malicious software from damaging the computers of the users. They employ a variety of techniques in order to detect, quarantine and eventually destroy the viruses, some of which include:

- **Scanning the downloaded files;** This means that the anti-virus program starts to scan the documents you are downloading into your computer as soon as they appear in your computer or as soon as you click the “Download” button on the website you want to download the said file from.

- **Scanning the programs before you execute them;** When you double click a program in order to start it up, even if you don’t notice it because it happens so fast, the anti-virus program on your computer will scan it very quick in order to make sure that there is no malicious software attached to it and that you can safely open it. If it is, then the anti-virus program will stop the program from starting up in order to protect your computer.
- **Scanning the entire computer;** If you tell your anti-virus program to scan your entire computer, it will take each file, one by one and run it through a series of programs in order to determine whether the said file contains malware or malicious software. This type of scanning takes much longer than usual obviously because the amount of files the anti-virus must go through is huge.