Have you ever wondered that what is the method that a virus scanner easily catches the virus and is rarely mistaken?

Firstly, what is a virus in your definition?

According to me, a virus is a program that has the capability to self -replicating with the function of deleting files, changing settings and causing other malicious activities on its own. The rapid growth leads to excessive network traffic and prevent network from functioning properly making it difficult for real traffic to work efficiently.

Moving on to our main topic that what is a virus scanner?

Our most obvious defense against viruses is essentially is a software that tries to prevent virus from infecting into our systems. It scans the incoming e-mails and other incoming traffic depending on what kind of scanner we have. Most of them have the ability to scan the portable media devices like the USB drives and stuff.

There are basically 2 ways in which we can broadly classify the virus scanner on the basis of how they work: -

The first method is that a file contains all the known viruses and periodically updates this file. It is a short file with generally a name of a.dat file. The current file keeps on updating with the most recent file on vendor’s website about new virus definitions.

The system here is that the virus scanner compares this file with the incoming files. Like scanning our email with the specific lines and content since known virus files have specific phrases on subject line and on body of messages they are attached to.

The problem here is that there are many false positives meaning it mistake a file that is not virus to be a virus.

Therefore, comes the second method into role. This type of scanner monitor your system for certain type of behavior that includes automating e-mail software, altering system registry, change system files and an attempt to write on a drive’s boot sector.

The new virus scanner technology combines these both in one. That is scanning system files and identify files that are critical to system and then monitoring those program that seems to modify these files. If any attempt is made to modify the critical files, the user is warned.

ON GOING VIRUS SCANNER – they constantly run-in background and check PC for any sign of virus.

ON DEMAND- they run only when you launch them.

SCANNING CRITERIA FOR DIFFERENT DOMAINS:

1. HEURISTIC SCANNING: This is one of the most advanced form of virus scanning. This best way to find a virus that is not known. It uses rules to determine whether a file is behaving like a virus or not. This is not fool proof as it may suspect a file that is not virus.
2. INSTANT MESSAGE SCANNING: This new feature to virus scanner industry is really appreciable. It scans instant message communications looking for the sign of known trojan horse file(virus).
3. FILE SCANNING: This deals with viruses that are copied over the network, deposited on shared drives or are there in the system before the virus scanner was installed. It takes times and cannot find viruses that are not known.
4. EMAIL AND ATTACHMENT SCANNING: An email should be scanned before opening it making very less chances of infection. It examines email and attachments on computer before passing it to an email program.

We should always buy a virus scanner that has most of the approaches so that you have a tough security barrier for your system.

***----------THANK YOU----------***