How Anti-Viruses Works

This is an article on *How Anti-Viruses Works* in *Operating System*.

Anti-Virus is a software or a program that can scan your files and data in your computer prevent you from firmwares and viruses...

How Does it works

Anti-Virus uses 2 different techniques to accomplish its tasks :-

1. Examining Files and comparing its signature/structure to that of viruses present in a database or a text file...This is called a virus-dictionary..
2. Identifying some suspicious behavior from any Program or Software sitting on the system

Virus-dictionary Method

In a Virus-dictionary Method a Anti-Virus starts by examining a file and checking up the dictionary of known viruses...

Every Binary/ELF/.exe has its own signature if they have different functionality...
Actually by signature we means some data in the bin file..This is a set of opcodes which the computer understands..These are different in every unique program..

When the Anti-Virus gets the signature of the file it then checks for the same signature in the dictionary of known-viruses(reported signatures) if it matches any signature in the dictionary then it is reported as a virus and the required task is performed(Dis-infection , removal ,etc etc..)

For this method to be successful , The virus-dictionary needs to be updated as a new virus-signature is reported.

This Method is quite common in most of the anti-viruses out there but it is not so successful now as its really easy to bypass this protection by using binders (These are the program that binds one program to another) , packers (Packs the signature , simply compresses the opcodes and make it difficult to detect) , encoders (These are the main cause of concern for the Anti-Virus developers out there as its quite a powerful approach , the encoders change the opcodes to something similar which provides the same functionality...It drastically changes the bin signatures and makes it almost undetectable..)

Another con of this Method is that it takes a lot of time and system resources to scan and compare all the files sitting on our system..

The Suspicious – Behaviors Method

In this method the anti-virus simply check for some suspicious – behavior happening on the system.. For checking this the anti-virus today has many modules like :-

1. Network Traffic Monitors
2. System Files Monitors
3. Process Monitors etc etc..

Network Traffic Monitors

Network Traffic Monitors simply monitors the incoming and ongoing network traffic from the system to other systems or the internet...

For eg :-

If there is a trojan sitting on the system..It will certainly listen for the attackers call ..As it receives the attackers call (in the form of a TCP , UDP etc packets) It simply send down the data to the attacker system (most of the trojans) This fluctuates the network traffic and Anti-Virus catches the trojan and performs the required task..

System Files Monitors

The System files Monitors simply checks for the files sitting on the system ..

Eg :-

If there is a virus sitting on a system and it checks for some system files and tries to dlete them then this will Report as a suspicious behaviour to the anti-virus..Then the anti-virus performs the required task..

Process Monitors

The Process Monitors check the process tree of the system and checks if there are some hidden programs running..If it finds something suspicious it reports the anti-virus core and then the required task is performed..

Eg :-

There is a key-logger sitting on the system. Most of the key-loggers have hidden processes and simply reads the key-strokes a user makes..This would be undetectable without the use

of Process Monitors..

Actually these were only the features on a basic anti-virus Most of the anti-virus today have Millions of protection systems and features and its not in the scope of this article..

Source: http://www.go4expert.com/articles/anti-viruses-t24942/