Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

How Anti-virus Software Works??

Sarika Choudhary*
M.tech (Network Security)
School of Engineering & Sciences
BPS Mahila Vishwavidyalaya
Sonepat, Haryana
India

Ritika Saroha
M.tech (Network Security)
School of Engineering & Sciences
BPS Mahila Vishwavidyalaya
Sonepat, Haryana
India

Mrs. Sonal Beniwal
Astt. Prof. of Computer Science
School of Engineering & Sciences
BPS Mahila Vishwavidyalaya
Sonepat, Haryana
India

Abstract— The study of this paper will tell you that how an anti-virus detect the viruses and disinfect the files. The main motive of this paper is to tell how it works and secure your system different type of malwares, viruses and worms.

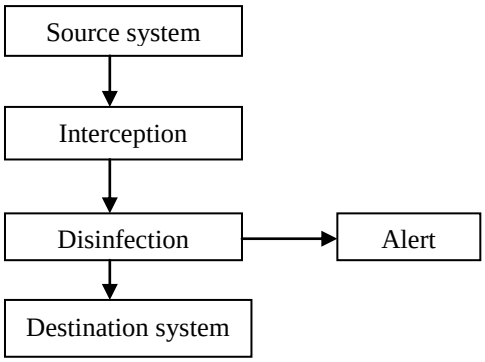
Keywords— viruses, LAN, alert, interception, disinfection.

I. INTRODUCTION

In early eighties, the main important worry for computer users was that viruses or malicious code were taking place into their systems. So we had to take important steps towards this. So there are basically two options:

1. Your system in a protection bubble that means isolated system; disconnect from the internet or any other transmission media neither use CD-ROMs nor any other removable disks. So by doing this we have a perfect data processing machine but there is no data to process. If there is no information that can enter in your system so you may have a perfect system there are no viruses.
2. You can install antivirus software so that there is peace in user's mind that no virus can enter into their system. The main point is that how the program does work to prevent from viruses entering your computer.

An antivirus software is a set of programs that is used to analyse your information and then, if finds any infected file, it disinfects it. There are various ways to analyse or scan any information based on where it comes from. For e.g. it operate differently when monitoring the CD-ROMs and when scanning the e-mails and monitoring over the LANs. Principles for all antiviruses are same but there are subtle differences.



The information starts from the source system and must reach to the destination system. Source system could be anything like floppy disk, hard disk etc. and destination system could be hard disk of a computer or any ISP (Internet Service Provider) which stores the messages sends them when a client needed. The information interpretation system varies depending upon special mechanism or whether it is implemented in operating system. This interpretation mechanism is specific for each OS or depending on component in which antivirus program is implemented. For e.g. in windows 8 a virtual driver is used which monitors the activity of disks. Therefore, every time the information is accessed through floppy disk or hard disk then antivirus program will intercept the read and write call to the disk and then scan the information so that anybody can read it safely. All these operations worked through the kernel in windows XP/2000. All antivirus software's have different interpretation mechanism. It is not only made for the OS but also other applications too. Sometimes interpretation mechanism is not available by the antivirus program or by any application. So, it uses other resources. Resources that secretly take information and pass it to the antivirus and then it scan the information and disinfect the file. Once the information has been scanned using any method then two operations performed:

1. The clean information is sent to the interpretation phase so that it can continue towards the destination system.

2. Alert message is sent to the user interface. User interface can vary for e.g. in an antivirus for workstations, message can be displayed on the screen directly and an antivirus for server, the alert message could be sent to the mailbox.

It doesn't perform any miracle. It is a very simple and efficient security assistant that provides advanced technology. Even when you copy some bytes in your system then antivirus must checks for 70,000 viruses without interfering to the normal activity of the computer and user can't realize these activities. It provides a high level security.

II. SCAN ENGINES

Most important function of any antivirus is virus scan engine. It scans the information and if the viruses are detected, it disinfects them. The information can be scanned in different ways.

- **Size:** it can easy detect if the file is infected or altered. Some viruses append their malicious code at the end of the file. An antivirus scanner (scan engine) scans it and compares it before and after sizes. If there is no modification done by the user so it suspects that there is some malicious activity running.
- **Pattern Matching:** every virus has a unique signature that they use to infect the files or computers. This signature could be some lines in assembly language that overwrite the stack pointer and then jump to the new line of code. An antivirus program compares the information with a virus database (virus signature). If information matches any of the virus signatures then antivirus shows that the file is infected by the virus.
- **Heuristic:** if any information being scanned is dangerous and without knowing that is it contains a virus or not? This method is known as heuristic scanning. It analyse that how an information acting and comparing it with the list of dangerous activities. For e.g. if an antivirus program notices that a program is trying to open every EXE file on your computer and infecting it by writing a copy of the original program into it. So an antivirus program detects this program and declares it a dangerous activity or unknown type of virus and sound the alarm. Then it is up to user weather the danger should be eliminated or not.

These methods have their pros and cons. If the antivirus program uses virus signature mechanism then it must update it at least once a day because 15 new viruses we discovered every day. If an antivirus left for two or more days without updating it cause a serious danger.

III. PERMANENT AND ON DEMAND SCANS

When an antivirus program is describing, it is very important to clearly distinguish between two type of protection offers:

- First one is permanent scan which is complex. This type of scan constantly monitors the operations that are performed on the system for preventing any kind of intrusion.
- Second one is on demand scan. This type of scan uses the same scan engine used by the permanent scan but it checks some part of the system whatever and whenever the user wants. For special action/ operations this type of scan is used.

IV. CONCLUSIONS

In this paper we discussed about how antivirus software works. There are different ways for detecting the viruses from the system. This type of deep knowledge can help us to choose the best antivirus for your system so that you can provide an efficient security to your PC.

There are hundreds of antivirus products but two to be the best: Bitdefender's and Kaspersky lab's. Bitdefender is very strong because it is a combination of signature-based detection, analytic detection, and behavior detection. Products from avast, avira, Eset, F secure, BullGuard, G Data are also perform well.

REFERENCES

[1] http://www.searchsecurity.techtarget.com/
[2] http://www.antivirusworld.com/
[3] http://www.sans.org.com/
[4] http://www.helpnetsecurity.com/
[5] http://www.askscience.com/
[6] http://www.howtogeek.com/
[7] http://www.antivirusware.com/
[8] http://www.brighthub.com/

