ISSN No. 0976-5697

Volume 7, No. 6(Special Issue),November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Network Security: Anti-virus

Gurpreet Kaur,Assistant Professor
Department of Computer Science
Guru Nanak Khalsa Girls College, Baba Sang Dhesian
Phagwara,Punjab (India)

***Abstract*:**
Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. Now days, Computer virus poses a considerable problem for the users of Personal Computers. Here antivirus plays anessential role in protecting users .It provides a key line of defence by detecting, blocking and removing viruses, spyware and malware before it can do lasting damage. This paper tells you how an Anti –Virus detects the viruses and disinfect the file. The main purpose of this paper is to tell how it works and secure the system from different malwares, viruses and worms. It also tells the different types of Anti-Viruses are being used today and why.

Keywords:Viruses, LAN, alert,interception, disinfection.

Introduction

Virus and Antivirus

Virus is a computer program or piece of code when executed replicates by reproducing itself and corrupts the system data it is loaded onto your computer without your knowledge and runs against your wishes. Surfing the internet without proper antivirus security will allow unknown viruses to infect your computer. Besides that, viruses can also replicate themselves,when one of your files is infected; you should check and scan all of your other drives. You may discover that the virus had already replicated itself to some of your folders. Anyhow, all computer viruses are manmade. A simple virus that can make a copy of it over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. Apart from that, an even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. When one computer is infected, the rest of the computers in the network will have a very high chance of getting the virus.

Antivirus

*Antivirus*programs are powerful pieces of software that are essential for computers. It is a computer program that can be used to scan files to detect and eliminate computer virus.It is an essential part of a multi-layered security strategy even if you're a smart computer user, the constant stream of vulnerabilities for browsers, plug-ins, and the Windows operating system itself make antivirus protection important.

Working of an Anti-virus

Antivirus basically uses two techniques to detect and prevent virus:
To Detect the Viruses;
1. It examines the virus dictionary to know about the virus.
2. It monitors the suspicious behaviour of all programs, which might indicate infection.
To prevents viruses; from entering a system there are basically two options.
The first one is to place the computer in a protective shield called a 'bubble'. This means to isolate the machine; disconnect it from the Internet or any other network, not to use any floppy disks, CD-ROMs or any other removable disks, so that no virus will get into your computer and no information will enter the computer, unless it is typed in through the keyboard.

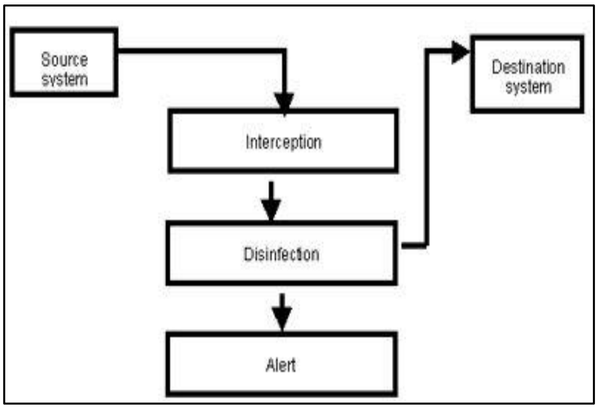

Fig 1: Basic Structure

The second option is to install anantivirus program. These are designed to make you sure that no malicious code can enter your PC.An antivirus program is no more than a system for analysinginformation and then, if it finds that something is infected, it disinfects it. Antivirus Program analysed the information (or scanned) in different ways depending on where it comes from. An antivirus will work differently while monitoring floppy disk operations than monitoring email traffic or movements over a LAN. The principle is the same but there are subtle differences.

According to Figure 1, the information is in the 'Source system' and must reach the 'Destination system'. The sourcesystem could be a floppy disk and the destination system couldbe the hard disk of a computer, or the origin an ISP in which a message is stored and the destination, the Windows communication system in the client machine, Winsock.The information interpretation system works differently depending on whether it is implemented in operating systems or in applications for every concern special mechanisms are needed.The interpretation mechanism must be specific to each operating system or component in which the antivirus is going to be implemented. For example, in Windows 9x, a virtual driver VxD is used, which continually monitors disk activityin Novell. In this way, every time the information on a disk or floppy disk is accessed, the antivirus will intercept the read and write calls to the disk, and scan the information to be read or saved. This operation is performed through a driver in kernel mode in Windows NT/2000/XP or an NLM which intercepts disk activity.special mechanisms between the application and the antivirus must be used. In other words, resources that intercept information and pass it to the antivirus, offering complete integration in order to disinfect viruses.Once the information has been scanned, using either method, if any threat has been detected, two operations are performed:

1.After the scan the cleaned information is returned to the interpretation mechanism, which in turn will return it to the system so that it can continue to move towards its final destination. This means that if an e-mail message was being received, the message will be let through to the mailbox, or if a fileway being copied, the copying of file process will be allowed to finish.

2. A warning message is sent to the user interface. This user interface can vary of course.Forworkstations an antivirus, throw a message can on the display screen, but in server solutions the alert could be sent as an e-mail message, an internal network message, and an entry in an activity report or as some kind of message to the antivirus management tool.As you can see, antivirus programs do not perform miracles, nor is it a software tool that you need to be wary of. It is a very simple security that offers precision and advanced technology.

Scan Engines:This engine scans the information it has intercepted forviruses, and if viruses are detected, it disinfects them.The information can be scanned in two ways. One method involves comparing the information received with a virus database (known as 'virus signatures'). If the information matches any of the virus signatures, the antivirus concludes that the file is infectedby a virus.The other way of finding out if the information being scanned is dangerous, without knowing if it actually contains a virus or not, is the method known as 'heuristic scanning'. This methodinvolves analysing how the information acts and comparing it with a list of dangerous activitypatterns.For example, if a file that can format a hard disk is detected, the antivirus will warn the user. Although it may be a new formatting system that the user is installing on the computer rather than a virus; the action is dangerous. Once the antivirus has sounded the alarm, it is up tothe user whether the danger should be eliminated or not.Both of these methods have theirpros and cons. If only the virus signatures system is used, it is important to update it at least once a day. When you bear in mind that 15 new viruses are discovered every day, an antivirus that is left for two or three days without being updated is a serious danger.The heuristic system has the drawback that it can warn you about items that you know are not viruses. If you have to work with a lot of items that may be considered dangerous, you couldsoon tire of the alerts. Programmers in particular may prefer to disable this option.

Permanent and on demand scans: When describing antivirus programs, it is important to clearly distinguish between the two types of protection on offer. The first is permanent scans, which are more complex and essential. These scans constantly monitor the operations performed on the computer to prevent any kind of intrusion.The other type of protection available is on demand scans. These use the same scan engine as the permanent protection and check any parts of the system whenever the user wants. These are normally used under special circumstances. For example, a user may want to perform an on demand scan when using a new floppy disk or to check information stored on the computer that hasn't been used for a while.

Virus Detection Techniques

Virus detection techniques can be classified as follows:

1. Signature-based detection technique uses the key aspects of an examined file to create a static fingerprint of known malware. The signature could represent a series or stream of bytes in the file. It could also be a cryptographic hash of the file or its sections. This method of detecting malware has been an essential aspect of antivirus tools since their inception; it remains a part of many tools to date, though its importance is diminishing. A major limitation of signature-based detection is that, by itself, this method is unable to flag malicious files for which signatures have not yet been developed. With this in mind, modern attackers frequently mutate their creations to retain malicious functionality by changing the file's signature.

2. Heuristics-based detectionthe most common detection is about detecting new malware by statically examining files for suspicious characteristics without an exact signature match with the help of an Algorithm. For instance, an antivirus tool might look for the presence of rare instructions or junk code in the examined file. The tool might also emulate running the file to see what it would do if executed, attempting to do this without noticeably slowing down the system. A single suspicious attribute might not be enough to flag the file as malicious. However, several such characteristics might exceed the expected risk threshold, leading the tool to classify the file as malware. It is best known method for detecting the new viruses, but the biggest downside of heuristics is it can inadvertently flag legitimate files as malicious.

3. Behavioral detection monitors how the program executes, rather than merely emulating its execution. If a virus has made it past the above detections, the antivirus analyzes the behavior of the running programs. This approach attempts to identify malwareby looking for suspicious behaviors, such as unpacking of malcode, modifying the hosts file or observing keystrokes. Noticing such actions allows an antivirus tool to detect the presence of previously unseen malware on the protected system. As with heuristics, each of these actions by itself might not be sufficient to classify the program as malware. However, taken together, they could be indicative of a malicious program. The use of behavioral techniques brings antivirus tools closer to the category of host intrusion prevention systems (HIPS), which have traditionally existed as a separate product category.

4. Cloud-based Antivirus detection identifies malware by collecting data fromsmall protected computersclients while analyzing it on the provider's infrastructure (in the cloud), instead of performing the analysis locally. This is usually done by capturing the relevant details about the file and the context of its execution on the endpoint, and providing them to the cloud engine for processing. The local antivirus agent or client only needs to perform minimal processing. Moreover, the vendor's cloud engine can derive patterns related to malware characteristics and behavior by correlating data from multiple systems. In contrast, other antivirus components base decisions mostly on locally observed attributes and behaviors. A cloud-based engine allows individual users of the antivirus tool to benefit from the experiences of other members of the community.

5. SandBox detectionis a security mechanism for isolation of running Programs, itcreates an emulated environment for the program to run, monitor and to analyze its behavior, if the program appears to performdestructive then it warns the user before running it on the computer.

Different Types of Viruses

Computer virus is a program code which reproduces itself and spread over the system to harm the data. Viruses has many different ways to attack to the computer such as create copies of itself, damage or corrupt, change data and degrease the performance of the computer system. Computer viruses can be categorized with few designations which are File infector viruses, Boot Sector viruses, Master boot record viruses, Multi-partite viruses, macro viruses, Trojan viruses and Worms. Below is the list to introduce different type of viruses and how they can be occurring into people's computer.

File Infector/Directory Virusesinfects program files by changing their paths that indicate the location of theexecutable code, like .EXE and .COM files. Besides that, it can infect other files when an infected program comes from floppy, hard drive, or from the network. Some file infectors are memory resident. It means that the virus will stay in memory to infect other files. For example, a companion virus might create a hidden PGP.COM file so that when the PGP command is executed, the fake PGP.COM runs first. The .COM file invokes its virus code before going on to start the real PGP.EXE file.

Boot Sector Viruses infect the boot record on hard drive, floppy disk, and Disk drive. All floppy disks and hard disks contain a small program in the boot record that is run when computer starts. The viruses attach themselves to this part of the disk and action when the user attempts to start up from the infected disk. Boot sector viruses have become less common as floppy disk have become rarer. Examples of boot sector viruses are Form, Disk Killer, Michelangelo, and Stoned. For Example the brain virus.

Master boot record viruses very similar with boot sector viruses, except that the viruses infect the MBR which is Master Boot Record. The difference between these two virus types is where the viral code is located. Master boot record infectors normally save a legitimate copy of the master boot record in a different location. Examples of master boot record infectors are *NYB*, *AntiExe*, Polyboot.Band *Unashamed*.

Multi-Partite Viruses it shares some characteristics of boot sector viruses and file viruses. These mean that they can infect .COM and .EXE files, and the boot sector of the computer's hard drive.These are distributed through infected mediaand usually hide in the memory .It is very difficult to repair. If the boot area is cleaned, but the files are not, the boot area will be infected. If the virus is not removed from the boot area, any files that you have cleaned will be infected. Examples of multi-partite viruses include *One Half*, *Emperor*, *Anthrax* and *Tequila*.

Macro Viruses infect files that are created by application programs that contain macros. Currently, thousands of macro viruses are known to exist and include viruses written in the macro language of Microsoft's Excel, Word and AmiPro applications. These types of viruses infect data files. They are the most common and have cost corporations the most money and time trying to repair. Macro viruses can be spread to any machine that runs the application the virus was written in. Examples of macro viruses include W97M.Melissa, WM. NiceDay and W97M.Groov,Bablas.

Trojan or Trojan Horses viruses are defined as a "malicious", security-breaking program. It spread when people are lured into opening a program because they think it comes from a legitimate source. But actuallyconceals something bad. Trojans can be spread in the guise of literally anything people find desirable, such as a free game, movie, song, etc. Victims typically downloaded the Trojan from a WWW or FTP archive, got it via peer- to- peer file exchange using IRC/instant messaging/Kazaa etc., or just carelessly opened some email attachment. Trojans usually do their damage silently. Example for some trojan filenames include: "dmsetup.exe" and "LOVE-LETTER-FOR-YOU.TXT.vbs".Back Orifice is one of the new Trojan viruses that provides a backdoor into our computer when active and connected to the Internet.

Worms is a special type of virus that has ability to self-replicate and use memory area, but cannot attach it to other programs. Unlike viruses, worms require the spreading of an infected host file although worms generally exist inside of other file like Word or Excel documents. Usually the worm will release a document that already has the 'worm' macro inside the document. The entire document will pass in to a computer to another computer, and the whole document can be considered have worms inside. One of the examples for worms' viruses is *PrettyParkWorm.* Melissa is also one of the famous viruses with combination Word macro virus and E-mail worm.

Encrypted Viruses consists of encrypted malicious code, decryptedmodule, uses the encrypted code technique which make difficult for antivirus to detect these. Encrypted Viruses can be detected when they try to spread by decrypted themselves.

How viruses are spread?

Since there are many types of virus in the computing world, there are also many ways how viruses are spread. Viruses come in different forms and their ways of attacks are all different. Sometimes, you won't even know that a virus had already infected your computer. They have the ability to attack your computer without notice but of course, your individual actions are also partly responsible for the attacks of viruses. Let's look at the different ways of how viruses are spread:

Email Attachments:

Since the existence of the Internet, email had become a very common form of communication between many users. In fact, email had become one of the cheapest and most convenient methods of communication. Sadly, viruses can be spread through emails. Viruses may disguise themselves as pictures, screensavers, programs, Word documents and many other file types. These viruses may come in forms of attachment sent to you by unknown users. Electronic greeting cards, links to certain websites and other techniques may be used by virus programmers to infect your computer with the intended virus when you click or open the links.

File Sharing:

In a network, file sharing/exchange is a really good way of sharing resources or important and useful applications. It is a very convenient way of exchanging files and documents between the users of the computers on the network. But sadly, many viruses have the ability to spread themselves through open network shares. When you copy something from a network, you have a slight chance of getting infected by a virus. Any files or folders that are obtained through a network must be scanned by antivirus programs before accessing them.

Downloading Files or Software:

Many files or software can be downloaded for free through the Internet but beware, not all of these files are safe. There may be viruses hidden among these files. If the file you are downloading, or the computer you are downloading from it is infected with a virus, chances are pretty high that your computer might also become infected with the virus. Try to avoid downloading files from another computer unless you have verified with the computer's owner that proper antivirus software is installed and up-to-date.

Instant Messaging:

Instant messaging programs are very famous among computer users. Programs like ICQ, IRC, MSN Messenger, Yahoo Messenger and AOL messenger are very popular. In reality, instant messaging programs are not dangerous in spreading viruses. The biggest risk here comes from accepting files from other users on the network. Strangers whom you just met from these instant messaging programs should not be trusted easily and you must not accept any unknown files from them. Viruses can be hidden among the files you received and it will activate itself when you open the file.

Floppy Disks:

Floppy disks are handy items as it is convenient and useful to transfer files. However, it is also very susceptible to viruses. A clean floppy disk can become infected when it is used in a computer with a virus infection. If an infected floppy disk is used in a clean computer, that computer can also become infected with the virus. When you want to copy some files to or from a computer, make sure that the computer is safe from viruses. This is the same when you want to transfer files from a floppy disk into your own computer. But now, floppy disks are seldom used by computer users. It is replaced by the handy USB key or flash memory as they call it.

Websites:

Nowadays, there are millions and millions of websites on the World Wide Web. Information about nearly everything under the sun can be found through the many web pages in the Internet. Sadly, certain viruses are known to infect web servers, and in theory, if you visit a website that is hosted on an infected server, your computer could become infected with the virus. There is not much prevention that you can do about the way these types of viruses spread. However, this infection method is very rare.

Antivirus Softwares

The following are the various free Antivirus softwares.

- ***McAfee***
- ***Microsoft security***
- ***Essentials***
- ***AVG***
- ***Avira***
- ***Avast***
- ***Malware bytes***
- ***Panda cloud antivirus***
- ***Herd Protect***
- ***King Soft Antivirus***
- ***VirC leaner***

Precautions to escape from viruses:

Antiviruses

Keep your antivirus up-to-date. Without the updates anti malware are unable to protect PCs from the Latest Threats. Scan your computer for "Spyware".

Less Dowmloads

Make sure that your web Browser security settings detects the unauthorised downloads. Alert Messages should be displayed before any download.

Email precautions

Email is a quick and easy way to exchange Information. We have electronic address books instead of little black books. Email frauds commit their crimes in a way similar to con artists who commit their crimes over the telephone. Creators of email viruses prey on you by claiming to be from somebody that they're not. The good news is, you really don't have to be a victim, if you're armed with the right information. The easiest way to prevent a virus is to not engage in the activity that causes it to spread. If you're not willing or able to give up your email entirely, there are a few guidelines to make your email use a lot safer. Don't download files from strangers. Do not execute any program received through email attachment unless you are sure about the sender. If you simply must read the attachment, however, download it to a floppy disk to be on the safe side, and then scan it with your anti-virus software. This is the safest way to handle downloads because the file is not accessible from a network drive or your hard disk. If you get a virus warning sent to you, make sure to check your software provider's website to make sure it's accurate.

Identifying Potential Viruses in E-mail Attachments

Whenever you receive an attachment in MS Outlook / Outlook Express there is generally a picture of a paper clip. Single clicking the paper clip reveals that there are 2 files attached. Notice that the attachment above appears to be a Word Document because of the .doc extension. However, the icon does not appear to be a typical MS Word icon. The typical MS Word icon is a picture of a blue ‘W’, as shown below (at left):

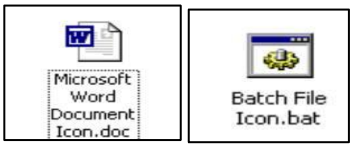

Fig:5 and 6

"Good Attachment" vs. "Bad Attachment"

Notice how the attached file in the e-mail above is called “The Pillarbanquet wine.doc” but has a different icon (depicted above right). In this case, the file is really a batch file, which contains potentially dangerous commands. The entire file name of the above file is "The Pillarbanquet wine.doc.bat". If you clicked on this icon, any commands that are contained within would be executed, including deleting all your files or reformatting your hard drive. Depending on how your computer is configured, it may not be set to show file extensions or extensions of registered files or system files. This means that you may never see certain types of extensions (.bat, .com, .exe, .pif, etc.).

Good Files

Typically, “good” attachments are shown as a picture of their associated program, such as MS Word, Excel, Acrobat Reader, etc.

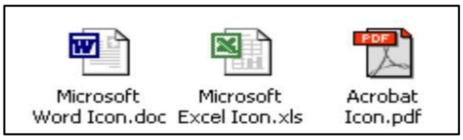

Fig:7

Even "good" files can contain viruses. There are some macro viruses that are embedded in MS Office documents (Word, Excel, etc.). The best bet is to always make sure that your virus definitions are up-to-date.

Bad Files

There are a number of files that can cause problems. Anything that ends with extension like .bat, .com, .exe, .scr, .vbs, .lnk, .pif can cause external commands to be run. Below is a sample of what the icons might look like:

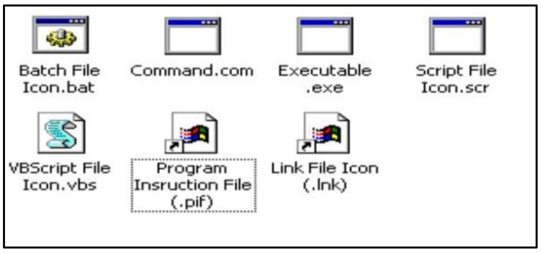

Fig:8

Floppy Disk

Do not boot from a Floppy Disk, it is the most common way virus are transmitted. If you are using floppy while working on your computer remove it from the system when u shut it down or the computer will automatically try to boot from the Floppy, perhaps launching any virus on the hard disk.

Firewall

All PCs connected to the internet should be secured behind hardware and software Based Firewall.

Conclusion

Based on all the information above, it is clear that viruses and antivirus security plays a very important role in the computing world. In these times, new types of viruses are always on the rise and their destructive power is always increasing.

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. Although there is no way for you to protect your computer 100% from infection, you can at least rest a little easier knowing that you're protected, and you can have a back-up plan in case your computer is destroyed by Virus.

Reference:

[1]http://www.webopedia.com/TERM/v/virus.html

[2]http://www.aarp.org/computershowto/Articles/a2002-07-18-virus.html

[3]http://www.hicom.net/~oedipus/virus32.html

[4]http://www.allbusiness.com/articles/content/14211.asp

[5]http://www.jconsult.com/virus/smex38help/WebRoot/at.htm

[6]http://www.ccs.neu.edu/groups/honors-program/freshsem/19951996/awong/types.html
[7]http://de.essortment.com/computervirusp_pfw.htm
[8]http://www.microsoft.com/athome/security/viruses/default.mspx

[9]http://us.mcafee.com/root/landingpages/default.asp?lpname=ms_vso&cid=8448

[10]http://www.symantecstore.com/dr/v2/ec_dynamic.main?sp=1&pn=47&sid=27674&cache_id=0

[11] Adeyinka, O., "Internet Attack Methods and InternetSecurity Technology," *Modeling& Simulation, 2008.AICMS 08. Second Asia International Conference on*,vol., no., pp.77-82, 13-15 May 2008

[12] Marin, G.A., "Network security basics," *Security & Privacy*, *IEEE* , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005

[13] “Internet History Timeline,” www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.h tm.

[14] Landwehr, C.E.; Goldschlag, D.M., "Security issues in networks with Internet access," *Proceedings of the IEEE*, vol.85, no.12, pp.2034-2051, Dec 1997

[15]IFMG 352,LAN DESIGN AND INSTALLATION ANTIVIRUS SECURITY RESEARCH PAPER GROUP MEMBERS: JESLYN CHONG ING WEI,CHING HUI BOON, LIM,PROFESSOR: DR. KUSTIM WIBOWO