Antivirus Security System

By Adhora Roy
Senior Author: mPower Technology.

INTRODUCTION:

In this era of modern technology, computers play a very important role in our daily lives. Computers play its functions in private homes, offices, workspaces, hospitals, schools, and everywhere else. It is undeniable that computers are very important nowadays but of course, no matter how great the technology is, there will still be some flaws and problems. The existence of computer viruses revolutionized the way the computer works and what type of security measures are supposed to be taken to prevent this serious problem. So we provide Nod32 key for solving all virus problem.

WHAT IS A VIRUS?

A computer virus is a program or piece of code that 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 itself 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.

Even though all the computer viruses are manmade, not all of them are dangerous. Viruses, as purely replicating entities, will not harm your system as long as they are coded properly. Any system damage resulting from a purely replicating virus happens because of bugs in the code that conflict with the system's configuration. In other words, a well-written virus that only contains code to infect programs will not damage your system. Your programs will contain the virus, but no other harm is done.

WHAT IS ANTIVIRUS SECURITY?

Antivirus securities are the measurements of prevention that protects a computer from the infection of viruses out there in the huge computing world. A computer has to be armed to protect itself from the attacks of viruses. Antivirus security comes in many different forms. There are antivirus programs which can help detect and prevent viruses from coming in. Antivirus programs such as McAfee and Norton Antivirus are quite popular in the computing world for their abilities to protect a computer from viruses. Installing antivirus software into a new computer is very important, especially for new users.

Besides that, personal knowledge on computer viruses is important too. Anyone who has a computer should check out the latest news about viruses and antivirus security programs. Let’s take a look at the many different types of virus in the next section of this paper.

Different Types of Viruses

Computer virus is a program which reproduces itself. 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 Viruses- it infects program files which contain executables code, like .EXE and COM files. Beside that, it can infect other files when an infected program is 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- bring infect to 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.

Master boot record viruses – it is 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*, and *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. It is very difficulty 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 – compare with the rest, this is the newest type of virus and tend to be a least damages. The first macro virus, written in Microsoft's Word macro language, was discovered in August, 1995. 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.

Trojan 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 actually conceals 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 - A worm is a special type of virus that can replicate it and use memory, 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.

As a conclusion, computer viruses are getting more popular in nowadays. They can spread and hide anyway in the computer file without our knowing and against our wishes. A simple virus can make a thousand copies stay in the computer file. A dangerous virus is capable to transmit themselves through the network and even break

the security system if without a well protection for the computer systems. This is very important for people to know about differences of viruses and how did a computer to get infected by those viruses. The second thing for prevent the problem occur is doing a safe computing system. This is very important that for every people must have a good anti-virus protection in order to prevent the problems occurred.

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 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 obtained 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.

Computer Virus Prevention

In this modern century, no matter what your circumstances were, whether you were annoyed or infected, panicked or fascinated, the virus took over the world's computers by storm. There are many computers in this world attacked by viruses. Email systems were blocked, files disappeared, and users were left puzzled about the fact that they got and somehow they had been fooled again. The clever disguise of the virus took many people by surprise. The worst thing is people have no idea when the virus will attack their computers. What went wrong? With all the talk and hype about virus protection, how could we have been fooled again?

The best way to treat a cold or a virus is to avoid catching it in the first place. The same goes for your computer. You can help to prevent viruses from infecting your computer or spreading to other computers. Here are some ways you can help to inoculate your computer against computer viruses.

Anti-Virus software is a necessity nowadays. If you don't have it, now is the best time to shop for it! In stead of the recent virus attacks, many of anti-virus companies are giving away free 30-day-trials. You have to download the antivirus before your computer catches a virus. There are two famous antivirus software, McAfee's Virus Shield and Norton Antivirus you can shop on the internet. Be sure that the operating system you're using, such as Windows '98, is compatible with the program you choose. Once you get your software, make sure you update it at least once a week, and that you have it set to scan for viruses when your computer boots up. Most of these programs have an "auto

update" feature that you can schedule to automatically update your software any time the computer is on, even if you're not home. If a particularly notorious virus has been released recently, update it daily for about a week. It may be a pain, but it's worth it;

Antivirus Softwares

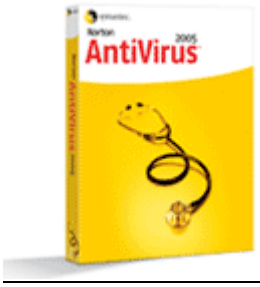
1. **McAfee**

   McAfee's advanced retail desktop solutions include premier anti-virus, security, encryption, and desktop optimization software. McAfee's managed Web security services employ a patented system and process of delivering software through an Internet browser to provide these services to users online through its Web site http://us.mcafee.com, one of the largest paid subscription sites on the Internet with over two million active paid subscribers.

   McAfee gives you two ways to protect your PC against nasty viruses and worms like Sasser, Mydoom and Lovsan/MSBlaster. You can purchase McAfee VirusScan for real-time virus protection or McAfee Web Essentials for 2-in-1 protection from viruses and hackers.

McAfee VirusScan	McAfee Web Essentials
• Protects your PC from over 87,000 viruses.	• Protects against viruses, worms, Trojans, and hackers.
• Detects spyware and adware protecting loss of data and privacy.	• Detects and quarantines spyware, web dialers, adware and more.
• Scans e-mail, downloads, CD-ROMs, & Instant Message attachments.	• Free updates and upgrades during your subscription.
• WormStopper detects and stops mass-mailing worms.	
• Detects and attempts to clean malicious code.	
• Free updates and upgrades during your subscription.	

2. Norton Antivirus



Symantec's Norton AntiVirus™ 2005

Symantec's Norton AntiVirus 2005 is the latest version and it is the world's most trusted antivirus solution. It removes viruses, worms, and Trojan horses automatically without interrupting your work. New Norton™ Internet Worm Protection blocks certain more sophisticated worms (such as Blaster and Sasser) before they enter your computer. Norton AntiVirus can also detect spyware and other non-virus threats.

Norton™ Internet Worm Protection stops certain damaging Internet worms at their attempted point of entry. QuickScan tool automatically searches for and removes viruses whenever new virus protection updates are downloaded. PreInstall Scan quickly detects and removes infections that can interfere with installing and launching Norton AntiVirus. It will scans and cleans both incoming and outgoing email messages. It can blocks viruses in instant message attachments. It will detect spyware and certain non-virus threats such as adware and keystroke logging programs. On the other hand, it will download new virus protection updates automatically to protect against new threats.

Email precautions

Like the telephone, email is one of the quickest and most convenient forms of communication today. We send them through the office, to our children, and to our clients. We use it because it is quick and easy. 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. 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):

"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 will have a picture of their associated program, such as **MS Word, Excel, Acrobat Reader**, etc.

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 in .**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:

Knowledge on Virus prevention

- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- Do not open any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.
- Do not open any files attached to an email if the subject line is questionable or unexpected. If the need to do so is there always save the file to your hard drive before doing so.
- Delete chain emails and junk email. Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
- Do not download any files from strangers.
- Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.
- Update your anti-virus software regularly. Over 500 viruses are discovered each month, so you'll want to be protected. There updates should be at the least the products virus signature files. You may also need to update the product's scanning engine as well.
- Back up your files on a regular basis.