Infectious Malware-Analysis and Protective Measures

Harjit Singh

Assistant Professor, Department of Computer Science, Punjabi University
Neighbourhood Campus, Dehla Seehan (Sangrur), Punjab, India
hjit@live.com

Abstract: ***Everything Malicious on a Computer is not always Virus; it is Malware i.e. Malicious Software. The viruses are developed by programmers who want to disturb the working of your computer and even want to intentionally cause damage to it. The motive can be to corrupt executable files, corrupt important documents including movies or music files and above that making the system totally unstable. These viruses mostly don't work in secrecy similar to spywares, these are specially designed to target the critical components on the computer and arise serious problems. These viruses work similar to human viruses in the sense that they reproduce themselves, and circulate by attacking the shared files. Other Destructive but Non-Virus Programs are Spyware, Worm, Trojan Horse, Logic Bomb. All these are different from Virus. Malware- General term for any type of unwanted software that infects your computer. This can include viruses and other Non-Virus programs that are destructive in nature. When trying to assess whether a computer system has fallen victim to a virus, logic bomb, worm or Trojan Horse, the main factor to consider is whether the malicious program has the ability to reproduce or not. Only viruses can make copies of themselves and attach the copy to new files.***

Keywords: Virus, Malware, Spyware, Worm, Trojan Horse, Logic Bomb, Virus vs. Spyware, Virus vs. Worm, Virus vs. Trojan Horse, Virus vs. Logic Bomb, Symptoms of Virus Infection, Destructive Non-Virus Programs, Virus History, Types of Virus, Life Cycle of Virus.

1. Introduction

A computer virus is not much different from a biological virus in the sense that it does not live independently; it must choose a host program or document to survive and propagate. These are also programmed like other programs and are designed and developed to propagate themselves on a computer.

It can have the motive to corrupt executable files, corrupt important documents including movies or music files and above that making the system totally unstable. These viruses mostly don't work in secrecy similar to spywares, these are specially designed to target the critical components on the computer and arise serious problems. These viruses work similar to human viruses in that they reproduce themselves, and circulate by attacking the shared files.

A virus can be very much capable to do infections on every computer application or attacking and damaging the important documents gradually. The virus automatically does not try to copy itself to other computers without human intervention. When humans try to send email attachments, use pen drives or other media to copy files to other computers, they provide their role in propagating the virus to other computers and so on.

Everything malicious on a computer is not always virus; it is malware i.e. malicious software. A virus is a specific category of malware. The computer virus performs similar behavior to a human virus and attacks and resides in the host program or application from where it tries to spread itself to other “hosts”. It is different from other type of malware in the sense that it reproduces itself and continuously works to find new host programs or documents to infect. Some viruses are very harmful while some other viruses will simply display a message on a given date.

2. How do we know?

If we are working on our computer and it starts behaving abnormally, we can get the idea that there is something wrong at the bottom. To be sure about a virus, we can examine:

- Programs start freezing frequently.
- We are unable to access certain documents.
- Improper booting behaviour of computer.
- The CAPS LOCK takes time to respond or stops responding.
- Increase in executable files’ size.
- Abnormal message display frequently.
- Screen displays abnormal pictures and disturb.
- PC plays unusual sounds.
- Your friends are receiving unusual emails sent from your email account but you are sure that you did not send any such emails.

3. Destructive non-virus programs

These perform similarly but do not try to attach themselves to other applications or files. In real these are non-virus programs which can destroy themselves and can even be the host of some virus and help to spread it:-

- Spyware
- Worm
- Logic Bomb
- Trojan Horse

“Malware” is the term used to describe any and all malicious software. Each one can be compared with Virus as below:-

3.1 Virus vs. Spyware

Spyware and viruses are commonly confused but are two totally different things. If you have only an anti-virus suite running on your computer, you are still very vulnerable to spyware attacks.

Virus- Self replicating, spreading computer program that is harmful to your computer. Viruses erase data, corrupt files, and cause usability problems to the computer that they infect. Spyware- Software that unknowingly collects and/or transmits user data, using it to display annoying adverts or relay sensitive personal data about the user to someone else.
Spyware is a type of malware that when installed on computers, collect information about users without their permission. The presence of spyware is usually hidden from the user, and also can be difficult to detect. Usually, spyware is installed secretly on the user's computer. There is also some spyware such as key loggers that are installed by the owner of a public computer (such as Internet Cafe) for the purpose of secretly monitoring other users.

While the term spyware suggests software that secretly monitors the user's computing, the functions of spyware extend well beyond simple monitoring. Spyware programs are able to collect your personal information, such as Internet surfing interests and sites that you visit frequently. These can also intervene with user control of the computer system such as installing extra unwanted software and redirecting the browser to another URL.

Spyware may be responsible to change settings of computer system which results in the slow connection speed, change in home pages, or even loss of Internet connection or functionality of other software.

The term adware commonly refers to a software application that displays unwanted advertisements, without taking any consent from the user. Most adware applications behave like spyware because they display those advertisements that are related to what they find from spying on users.

When a user visits web sites, these sites may be capable to install Gator on user’s machines in a stealthy way which provides income to the site owners through advertisements display. The user is shown many pop-up advertisements.

3.2 Virus vs. Worm

Viruses are computer programs that spread themselves from one file to another file on a computer. It does not intentionally try to spread itself from that computer to other computers in the network. In most cases, that’s where humans play a role. Worms rely very less on human behavior to spread themselves from one computer to another computer. It has the capability to copy itself from one computer to another computer over a network. It doesn’t require any help from human. Also they can act as carriers for viruses.

Viruses are far from the only malicious programs that try to disrupt a computer system. Worms are created to penetrate the programs and modify or destroy the important data. Often what people think is a virus infection is, actually a worm program. This is not as much serious since worms cannot replicate themselves. But the damage done by a worm program can be equivalent to the damage caused by a virus, especially if it is not discovered in time. For example, a worm program may issue instructions to a computer of a bank to transfer funds to a specific bank account. It may continue to transfer funds even if we destroy the worm. However, if it is discovered that a worm has invaded, the system can be recovered much easier because there will be only one copy of the worm program to destroy. It is because the worm program did not have replicating capability. Using this capacity it may again infect many times.

Worm is a self-propagating program that spreads over a network. Unlike viruses, worm may not depend on other programs or user actions for replication, dissemination, or execution. Worms spread by locating other susceptible hosts on the network, then copying their program instructions to those hosts.

3.3 Virus vs. Trojan Horse

For propagation, a virus inserts a copy of itself into another program and becomes a part of that program. These are developed to spread themselves from one file to another on a computer system.
Trojan horse is a program that does not replicate itself, and it does not infect other files. It masquerades as a safe and useful program. The most common type of Trojan Horse provides backdoor access to a computer system.
Trojan Horse is developed to be undetectable easily. Trojan Horse program installs itself on a computer when the user opens an email attachment or computer file containing the Trojan, or clicks on a hyper link that directs the user’s web browser to a Web site from which the Trojan is downloaded automatically. Once installed, it can be controlled from remote locations by hackers for criminal activities, such as extracting money, passwords, or other sensitive information. It can also be used as a zombie program which can be used to disseminate spam, phishing emails or other malware to other computers over the network.
A Trojan Horse is a destructive program that has been hidden in some useful software application. It can carry worm and virus programs. Trojan Horses are not viruses technically because they do not replicate themselves and spread as viruses do. There is a mythical story based on which Trojan Horse is so named. The Greek warriors concealed themselves in an attractive wooden horse and that horse is left outside the gates of the besieged city of Troy. The Trojans thought it as a friendly peace offering by Greek

and took it in. The Greek warriors then jumped out and cause disaster. Trojan Horse program works on the same principle. This program may seem both desirable and safe, inviting the computer user to copy or download it and run.

3.4 Virus vs. Logic Bomb

Viruses use various tricky methods to invite the user to install them on his/her computer. They usually try to copy and spread themselves. Viruses are not usually developed to attack at a specific computer. Logic Bomb is a program that is secretly inserted into the computer system and remains hidden until they are triggered. These often do not spread themselves. They are usually directed at a specific target. They are usually timed to activate so that they can do maximum damage. A logic bomb can be developed to wipe out records at a specific time. Logic bombs can be written literally decades before they explode.

Logic bombs can be used by the suppliers, who set up a computer system, causing data to be destroyed if their bills are not paid.

4. How virus works?

Many viruses are hidden in the code of genuine software programs, we can call host programs. These viruses are called file infector viruses, and when the host program is run, the code for the virus is also executed, and the virus loads itself into the computer memory. From there, the virus searches for other programs on the computer that it can infect. When such a program is found, it adds its code to the new program, and so on (Figure 1).

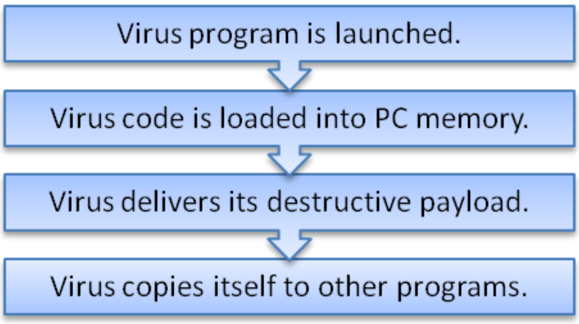
Virus program is launched.
Virus code is loaded into PC memory.
Virus delivers its destructive payload.
Virus copies itself to other programs.

Figure 1: Procedure of virus infection

Even if a virus program is not reproducing itself, it can be damaging too. A virus infected program may damage some important files on the system. It may be capable to replace the boot sector code with its own code to make the hard disk unusable. You may see some strange messages on your screen or may listen strange sounds in our ears. Your email account may be hacked by a virus to replicate itself to other computers belonging to your near and dears.

The viruses are specially designed to put their code to other applications or files when they are run. These are also programs like others but are developed to damage the systems as much as possible.

5. Historical Background

Humans became aware about the computer viruses in 1949 even much before the computer systems were so common. The paper presented by John von Neumann in 1949 was based on theory of automata, and in this paper the author provided details about the possibility of computer programs that could be able to reproduce themselves base on automata theory. The viruses we observe today are actually based on the fact presented by John von Neumann. But until then all this stuff was on papers because it was a theoretically proven concept but not implemented practically. Then the absence of implementation is completed at Bell Labs in 1950s in the form of a computer game that was played by two different players. A type of computer organisms was produced by two different players to hijack the mainframe computer system. In reality, the viruses we observe today, do the same thing but on personal computers.

Then in 1980s, personal computer systems start to become common in real world. Simultaneously, the computer viruses also start to become common in real world. But in those times, the viruses were made to automatically spread to other computers. Human activities with computer systems were responsible for their spread on other systems through the use of floppy diskettes. In those times floppy diskette was a very common medium to share files from one computer system to another.

The first specially developed virus was spread using a floppy diskette and attached in 1981 on Apple II computer. The developers named it Elk Cloner but it was not a damaging virus. Instead it was designed to display a suspicious message to the user to tell him/her that it will hijack the disks and chips of his/her computer system.

Table 1: Some historical malware

Virus	*Year*	*Description*
Elk Cloner	1981	Infection on diskette of Apple II without damage.
demo	1983	Virus experiment and demonstrated by Len Adleman.
Brain Virus	1986	Very first virus to infect ms-dos files.
Trojan Horse	1986	Very first Trojan horse was developed for PC.
Michelangelo	1992	Very first virus circulated globally.
Melissa	1999	Very first e-mail hosted malware.
Love Bug	2000	First virus that shutdown many thousands of corporate email systems.
And the progress continues………………………		

6. Types of Viruses

A virus is actually a piece of programming code that embeds itself into our usable applications and remains hidden but performs some tasks that we cannot expect from those applications. The other categories of malware programs may be harmful similar to virus programs but they do not attach their code to other application programs. These malware programs cannot be categorised as virus programs. Different viruses programs are:-

- Boot-Sector (MBR) Viruses
- File-Infector Viruses
- Macro-code Viruses
- Script Viruses

6.1 Boot-Sector (MBR) Viruses

Boot sector is the part of a floppy diskette and master boot record is a similar type of part on hard disk drive. These viruses store themselves in boot sector or master boot record and are run automatically when the system start up. The virus has the tendency to infect any other diskettes that are inserted into the floppy drive once it is loaded in the main memory. The virus then propagates to another computer's hard disk's master boot record when same an infected floppy diskette is inserted into another computer system. These viruses mainly spread using floppy diskettes, so these types of viruses are very limited.

The working of these viruses is very straight forward. The boot sector code is replaced with the infected code and real code is copied somewhere else on the diskette or hard disk being marked it as bad sector. These types of viruses were very difficult to trace due to their capability to take overall control of the computer system at boot up. But now the use of floppy diskettes is no more, so these types of viruses are also very rarely found.

6.2 File-Infector Viruses

Capturing another program to embedding itself into that code is the common behaviour of this type of virus. A traditional type of virus the mysteriously hides itself into another program's coding. In most cases, the virus attacks the executable programs which may be software tools, video games or some other application programs.

It is very common for Microsoft platforms because "Windows" uses special extensions for executable applications. On execution of an infected application, the virus is loaded in memory at a separate memory space than the host application. If we close the host application, even then the virus remains active.

The working of this type of virus matches with boot-sector virus programs in that replacing the initializing code with the infected code and then launch with the host program. The real initializing code of host program is copied to some other part of the disk. Embedding more code in host program increase the size of that program and it is a very simple symptom to detect if the program has been infected or not. Even some viruses of this type are capable to copy the original file with some other extension and embed into the original file and make that file hidden in order to remain in the system secretly.

These types of viruses were very common in the beginning when internet was not so common and macro-viruses were not invented. In those times, most of the infections were done by these types of viruses.

6.3 Macro-code Viruses

Many application programs use macro coding to create some customized menus or buttons which helps the users to automate some lengthy or repeatable tasks. These codes are very small in size and work within the application program to perform some specific tasks. In Microsoft office applications, visual basic for applications is a very popular macro coding language which is used by users to code a set of instructions to perform specific task that can then be linked to a menu item or toolbar button for easy execution. This coding facility is used to write macro-code viruses which can change your documents and get the control to automate email sending to your contacts.

In this sense, we may consider these viruses more dangerous than other types of virus programs. It is because, documents and other files are not having fixed size and we cannot consider the size of a document to investigate that if the document is infected from a macro-code virus. These just do their duty when a document is opened.

A very special property of these viruses is that the code in which they are written, depends only on the application for which they are written. The virus can spread itself to other platforms, means it becomes a platform independent virus. It is very dangerous.

6.4 Script Viruses

Websites are made up of web pages and these web pages use scripting languages to perform certain tasks. A very popular scripting language is JavaScript. It is basically used to run some initialization tasks when a web page is opened in the browser. The browser runs the code. Today, we surf the web on daily basis and a web page may have a script virus hidden in it. So this type of virus is very common now-a-days and infects many computers daily.

Any file that is able to run the script stored in the web page can be infected by script virus.

7. The Life of the Virus

The virus takes birth when the virus programmer generates its code. Once it is born, it starts its journey towards infecting other computers through various means such as pen drive, network, floppy diskette etc. The host application starts up to launch the virus into memory and activate it. The virus starts delivering its payload. From its behavior it is detected and documented in anti-virus programs. The anti-virus programs detect the virus and remove it. Hence the virus died. The virus programmers creates new one.

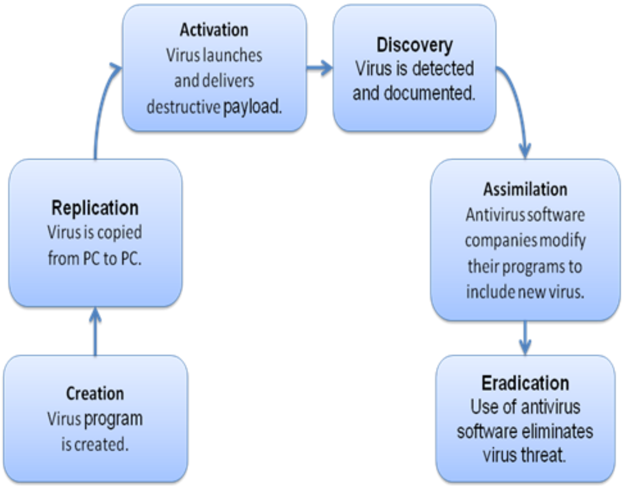
Activation
Virus launches and delivers destructive payload.
Discovery
Virus is detected and documented.
Assimilation
Antivirus software companies modify their programs to include new virus.
Eradication
Use of antivirus software eliminates virus threat.
Creation
Virus program is created.
Replication
Virus is copied from PC to PC.

Figure 2: The Life of the Virus

8. Reducing Chances of Infection

To reduce the chances of infection, the following steps should be carefully taken into consideration:

8.1 Always operating the computer using Normal User Account.

Computer system should not be used with Administrative Account for normal operations. Normal user account has limited privileges, so virus will work under restrictions imposed by the limited privileges. Using administrative account the virus will have full control over the systems.

8.2 Restricting file downloading to known or secure sources.

Downloading an unknown file from an unknown website is the surest way to catch a virus. It should not be tried unless it is absolutely required.

8.3 Using an up-to-date anti-virus program.

Antivirus programs work by scanning the files on the computer and check for any previously identified virus. These are memory resident programs and scan new files downloaded and e-mail messages received. They are a good first step of defence, but they should be kept up-to-date with information about the very latest viruses. Most antivirus programs download updates automatically when a connection to internet is made.

8.4 Enabling macro virus protection in applications.

Most current Microsoft applications include macro disable feature that keep the program from running unknown macros. It prevents the system from being infected by macro viruses.

8.5 Not opening unexpected email attachments.

The majority of viruses today arrive in the mailbox as attachments to e-mail messages. An unexpected email attachment should not be opened unless it is absolutely required.

8.6 Creating backup copies of all important data.

The non-infected versions of most critical data files need to be backed up regularly. This habit can help to get copies of important data in case the entire system gets infected and could not be reverted back.

9. Conclusion and Suggestions

Computer malware is the malicious code specially written to spread itself to other computer systems and to put its payload at target machines using various means. The malware lived along with computer systems from the beginning and resulted in lot of damage year by year. The malware is found in various categories and to protect the computers from damage we should take protective measures. We should take care when we download unknown files from the internet and open emails in our inboxes. These may be very dangerous to us. We should also install reliable antivirus programs to protect from any harm. Some of the free Anti-Virus programs available to download are:-

Avira Free Antivirus : http://www.avira.com
AVG Antivirus Free: http://www.avg.com
Avast Free Antivirus: http://www.avast.com
PC Tools Antivirus Free: http://www.pctools.com

References

[1] Computer Associates Virus Information Center (www3.ca.com/virus/).
[2] Computer Security Resource Center Virus Information (csrc.ncsl.nist.gov/virus/).
[3] F-Secure Security Information Center (www.datafellows.com/virus-info/).
[4] IBM Antivirus Research Project (www.research.ibm.com/antivirus/).
[5] McAfee AVERT (www.mcafeeb2b.com/naicommon/avert/).
[6] Sophos Virus Analyses (www.sophos.com/virusinfo/analyses/).
[7] Symantec Security Response (www.symantec.com).
[8] What You Can Do About Computer Viruses 17.
[9] Trend Micro Virus Information Center (www.antivirus.com/vinfo/).
[10] Virus Bulletin (www.virusbtn.com).
[11] Viruslist.com (www.viruslist.com).
[12] The WildList Organization International (www.wildlist.org).