

Computer Viruses

Maria Thomas

Department of computer science, Carmel college mala
Thrissur, India

Abstract: The purpose of this paper is to discuss various types of computer viruses, along with their characteristics, working, effects on the computer systems and to suggest measures for detecting the virus infection in a computer system and to elaborate means of prevention. The first PC virus was a boot sector virus called (c) brain. In this paper presentation includes what is a virus, history of virus, how does a virus infected computer, how can we detect a virus infected computer, how do we protect our computer against viruses, specific types of viruses and also what is an anti virus

Key words:- PC: personal computers, VIRUSE: vital resources information under siege, E-mail: electronic mail

I. INTRODUCTION

A computer virus is a special kind of computer program which Spreads across disks and networks by making copies of it, usually surreptitiously. Can produce undesired side-effects in computers in which it inactive. As long as the virus is active on the computer, it can copy itself to other files or disks that are accessed. Infections spread from machine to machine, and from organization to organization, in a number of ways. Viruses can be transmitted by Booting a PC from an infected medium, executing an infected program.

II. COMPUTER VIRUSES

A virus is a program designed by a computer programmer (**malicious hacker**) to do a certain unwanted function. The virus program can be simply annoying like displaying a happy face on the user's screen at a certain time and date. It can also be very destructive and damage your computer's programs and files causing the computer to stop working. The reasons why hackers create viruses are open for speculation.

A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge. Viruses have harmful side effects. These can range from displaying irritating messages to deleting all the files on our computer. It is estimated that there are 53,000 computer viruses in existence; with new one's being detected almost every quarter of minute. The "I LOVE YOU" virus infected up to 45 million computer, causing ten billion dollar worth of damage worldwide.



III. HISTORY

A program called "elk cloner" is credited with being the first computer virus to appear "in the wild" that is, outside the single computer or lab where it was Created. Written in 1982 by rich skrenta, it attached itself to the apple DOS3.3 Operating System and spread by floppy disk. This virus was originally a joke, created by the High School student and put on to a game. The game was set to play, but release the virus on the 50th time of starting the game. Only this time, instead of playing the game, it would change to a blank screen that read a poem about the virus named Elk Cloner. The computer would then be infected.

The first PC virus was a boot sector virus called © brain, created in 1986 by two brothers, Basit and Amjad Farooq Alvi, operating out of Lahore, Pakistan. The brothers reportedly created the virus to deter pirated copies of software they had written. However, analysts have claimed that the Asher virus, a variant of brain, possibly predated it based on code within the virus.

IV. HOW DOES A VIRUS INFECTED COMPUTER

A virus infected program has to before it can infect your computer. Viruses have ways of making sure that this happens. They can attach themselves to other programs and as soon as you launch the infected program, the virus code runs. You might receive an infected file on a disk, in E-mail attachment, or in a download from the internet. As soon as you launch the files, the virus code runs. Then the virus can copy itself to other files or disks and make changes on your computer. There are some examples shown here how a virus infected computer looks like

V. SYMPTOMS OF A COMPUTER VIRUS

Computer virus symptoms are a not cast in stone, but rather a moving target. Just like with the human viral conditions, they evolve through generations – which in computer technology terms may mean weeks or even days. Some symptoms may not necessarily mean an infection – for example, if you are sneezing, you do not necessarily have a

flu, it may be just an allergy – which means different cause, and different treatment methods. Same with computers – if your system seems to be slower than usual, it may be a symptom of a virus, but it may also be a symptom of “program overload” – when you have too many programs running at once, and it crashes your computer system’s performance. With that in mind, let’s go over some of the most common symptoms that can alert you to the potential virus within your computer system, or even your computer network, presented here in no particular order.

A. HARDWARE TROUBLES

If your hardware – computer, printer, etc. – started acting up on its own, without you requesting any action by means of keyboard or mouse, you are likely having a virus in your computer system. When you work on the computer, especially if you are performing some actions by using programs, your hard drive is expected to be making some noises.

B. NO RESPONSE

We all had the frozen iceberg for a computer before. Lockup alone may not necessarily mean you have a virus – it could also be a symptom of a desperate need for a cleanup but if it presents itself in array of other symptoms, be on a lookout for a virus.

C. SLOW PERFORMANCE

As in the previous paragraphs – you must account for specifics of certain files and programs when making a judgment of the slow performance: one PDF document may take much longer time to open simply because it is of a much larger size, and it will not be indicative of the computer virus. However, keep in mind that some viruses can reproduce and multiply your files and overcrowd disk space, overloading disk usage.

D. SLOW STARTUP

Another important symptom of a computer virus is a slow startup. Do not confuse it with wishful thinking. As a collective, we are impatient beings. My point exactly! When considering the startup process – think of the typical (however slow you may feel it is) to the actual startup time

E. CRASHING.

When your computer crashes spontaneously, be careful. After computer restarts, you may notice it does not seem to run normally. If it self-restarts frequently, every few minutes – beware of a virus. This symptom alone may indicate that your system is infected. If your computer crashed, best course of action – Do Not Resuscitate and call your IT support company.

F. MISSING FILES

When you notice that applications on your computer do not work correctly, you may also notice some of your files are missing. That includes different types of files. Some may be the files that you created, such as images or documents you had saved on your drive. You may physically notice absence of those when you actually look for them and can’t

seem to find them anywhere. As a result of computer virus infection your computer may also be missing system files.

G. DISKS OR DISK DRIVES ARE NOT ACCESSIBLE

If you are losing the network connection – or worse yet cannot connect to the USB drive you just plugged in, or you go to My Computer and only see one drive instead of your usual X number of drives, you may be in trouble. If you cannot connect to all, some of the drives or cannot access your CD-ROM, it may be one of the symptoms indicating your computer is infected.

H. EXTRA FILES

You may visually notice extra pop ups and extra programs that seem to be running on your computer, especially on startup. You may notice (if you check for it) that your disk space suddenly quadrupled in size without you making 200 copies of your vacation photos folder on your C: drive.

I. PRINTER ISSUES

If you cannot get your documents to print correctly, or cannot print at all, you may be dealing with a virus.

J. UNUSUAL ERROR MESSAGES

This may include gibberish messages, messages you hadn’t seem before, undesired ad messages and such. Special attention must be paid to messages that disguise themselves as anti-virus warning messages.

VI. SPECIFIC TYPES OF VIRUS

A. BOOT SECTOR VIRUS

Boot sector viruses were the first type of PC virus to appear. They spread by modifying The boot sector, which contains the program that enables your computer to start up. When you switch on, the hardware looks for the boot sector program-which is usually on the hard disk, but can be on floppy or CD-and runs it. This program then loads the rest of the operating system into memory. A boot sector virus replaces the original boot sector with its own, modified version. When you next start-up, the infected boot sector is used and the virus become active.

B. PARASITIC VIRUS (file virus)

Parasitic virus is also known as file viruses; attach themselves to a program when you start a program infected with a file virus, the virus is launched first. To hide itself, the virus then runs the original program. The operating system on your computer sees the virus as part of the program you were trying to run and gives it the same rights. These rights allow the virus to copy itself, install itself in memory or release its payload

These are common signs to infection- but they might also indicate hardware or software problems that have nothing to do with a virus.

C. E-MAIL VIRUS

An E-mail virus is a virus which uses e-mail messages as a mode of transport. These viruses often copy themselves by

automatically mailing copies to hundreds of people in the victim's address book.

D.MACRO VIRUS

A macro virus, often written in the scripting languages for Microsoft programs such as word and excel, is spread in Microsoft office infecting and spread sheets.

E.LOGIC BOMB

A logic bomb employs code that lies inert until specific conditions are met. The resolution of the conditions will trigger a certain function. An example of logic bomb would be a virus that waits to execute until it has infected a certain number of hosts. A time bomb is a subset of logic bomb, which is set to trigger on a particular date and time.

F.TROJAN

A program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information or make the system more vulnerable to future entry or simply destroy programs or data on the hard disk. A Trojan is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the computer. Trojan often sneaks to a free game or other utility

There are two common types of Trojan horses. One, is otherwise useful software that has been corrupted by a cracker inserting malicious code that executes while the program is used.

Examples include various implementation of weather alerting programs, computer clock setting software, and peer-to-peer file sharing utilities. The other type is a standard-alone program that masquerades as something else, like a game or image files, in order to trick the user into some misdirected complicity that is needed to carry out the program's objectives.

G.THE TROJAN HORSE

Trojan come from Greek mythology, in which the Greeks battled the Trojan. After years of being unable to break into the fortified city, the Greeks built a wooden horse, filled it with soldiers and pretended to sail away. After the Trojan brought the horse into city, the Greek soldiers crept at night, opened the gates of troy to the returning soldiers, and troy was destroyed.

H.WORM

A worm is another type of self-replicating program. Worms have the ability to spread over a network. The definitions of viruses and worms are not mutually exclusive. Worms always have a mechanism to spread over a network; viruses always infect other (whether those programs are boot sectors, binary files or macros). My Dom or I LOVE YOU is two examples of worms.

I.MOBILE PHONE VIRUSES

As computing platforms, mobile devices are also susceptible to virus attacks. Thus far, there are only a few viruses, worms, and Trojan for handheld computers and

smart phones. But the number will likely increase with the increase of functionality of mobile application development environment with extensive software development documentation and tools also allow hackers to create viruses for these platforms more easily.

Viruses can infect mobile in several ways. Like viruses for desktop PCs, viruses for

For mobile devices can as well spread via email messages and shared files, and by exploiting software vulnerabilities. Additionally, the malicious code can also be sent from a PC to the mobile device during synchronization with PC etc.

VII.HOW WE CAN PROTECT OUR COMPUTER AGAINST THE SYMPTOMS

The best way to prevent viruses is to have up-to-date anti-virus and delete it if you have allowed the anti-virus software to run in auto-protect mode. This means that the anti-virus software will automatically scan when you download, open, or install files. In addition to having updated anti-virus software, you can also prevent virus from infecting your computer by using caution when viewing e-mail attachments or downloading files from the internet.

VIII.ANTI-VIRUS MEASURES

The fight against computer viruses involves five kinds of counter-measure:

Preparation includes making backups of all software (including operating systems) and making a contingency plan.

Prevention includes creating user awareness, implementing hygiene rules, using disk authorization software, or providing isolated 'quarantine' PCs.

Detection involves the use of anti-virus software to detect report and (sometimes) disinfect viruses.

Containment involves identifying and isolating the infected items.

Recovery involves disinfecting or removing infected items, and recovering or replacing corrupted data.

XI.WHAT IS A ANTI-VIRUS

Anti-virus is the name given to software that detects and removes viruses in a computer system. It is a program that either comes installed on your computer or that you purchase and install yourself. It helps protect your computer against most viruses, worm, Trojan horses, and other unwanted invader that can make your computer "sick". Viruses, worm, and the like often perform Malicious acts, such as deleting files, accessing personal data, or using your computer to attack other computers. You can help keep your computer healthy by using antivirus software. Remember to update Your antivirus software regularly. These updates are generally available through a subscription from your antivirus vendor.

X.THE FOLLOWING IS A LIST OF SOME RECOMMENDED ANTI-VIRUS PROGRAM

A.NORTON ANTI-VIRUS

This program is very popular and effectively protects your computer from viruses. It gained recognition for its high quality and wide range of features designed to safeguard your home or office computer.

B.MacAfee

MacAfee virus scan programs will detect, block and remove any virus or spyware that threatens your computer. The McAfee anti-virus software is known for its breadth of protection.

C.PC- cillin Internet Security

This program offers effective anti-virus safeguarding and also includes spam, spyware, wireless, and firewall and privacy data protection. In addition, it features parental control and a year of free teaches support via their toll-free number.

D.F- Port for windows

This product consistently receives excellent performance reviews for its detection capabilities and is also praised for its user-friendly appeal. It's a good product for novice computer users. Note that E- port should be used in conjunction with a firewall.

X.CONCLUSION

Computer viruses have two basic forms one is a **boot sector** viruses which infect the section of a disk that is first read by the computer. This type of virus **infects** the boot or master section of any disks that it comes in contact with. The second is a **program virus** that infects other programs when the infected program is run or executed. Some viruses infect both and others change themselves (polymorphic) depending on the programs they encounter.

REFERENCE

- [1] computer basics- your guid:Elamaramkareem
- [2] www.powersolution.com/top-10-computer-virus-symptoms-checklist/