"TO IMPROVE THE SYSTEM SECURITY FROM VIRUSES"

(Research scholar): Zareen[1]

ansarizareen69@gmial.com

Dr. Praveen Kumar[2]
praveencs10@yahoo.com
(HOD, Research & Development Cell)
(Research scholar): Sabia Perween[3]
sabiaperween179@gmail.com

Department of Computer Science & Engineering, Delhi Institute of Engineering & Technology, Meerut, Uttar Pradesh, India

ABSTRACT

The first virus through network is creeper and to prevent this virus creeper, the first anti-virus is reaper.The first PC virus was "ELK cloner "which is found in 1982. It spread by apple DOS and floppy disk. After seeing the first pc virus then in 1984 FRED COHEN was the first person from south California University who started founding information about this pc virus. He used to try many experiments and wrote a theory on it. Computer virus damages a billions of dollar computers every year.

Keywords: PC Virus, Computer virus, Replication, Network.

1. INTRODUCTION

Virus means a type of software which is used to infect or harm other computer systems. It replicates (multiply) with one another and so on and when this replication continuously starts increasing then at some time the computer system becomes infected and virus occurs.

The first virus through network is creeper and to prevent this virus creeper , the first anti-virus is reaper .The first PC virus was "ELK cloner " which is found in 1982 . It spread by apple DOS and floppy disk .

After seeing the first pc virus then in 1984 FRED COHEN was the first person from south California university who started founding information about this pc virus . He used to try many experiments and wrote a theory on it. Computer virus damages a billions of dollar computers every year .

Due to the virus, which causing and affecting data , steals all the personal information of the people ,the anti-virus software has been develops.

There are many ways by which, these viruses are transferring to another computer .

Fig 1. Virus Enters into the computer

Fig 2. Varieus worms & Malicious Code occur into the computer

a) On using media's such as CD's and USB's.

b) Through E-mail and other social web site

c) As a part of another program.

2. HISTORICAL DEVELOPMENT

Early academic work on self replicating program are on the theory of replication 'John von Neumann s' was the first person who gave the lectures on virus replication, how these replication (multiplication) of virus from one PC to another PC is transferring. He work on this & described to the people how a computer is design in such a way that it is replicating by it self .

Then 'Neumann' produce by himself a computer program, which is the world 's first computer virus, and after that he is known to be the theoretical " father of computer".

SELF MODIFICATION

Most of the anti-viruses programs are try to find pattern of viruses inside the common programs ,they scans program for viruses but unfortunately it fails because it is not having unique signs that human beings have.Such sign of human are sequence of bytes that anti-virus programs looking for because it is a part of virus.

These viruses are become very harmful, even home computers are also affected by these E-mail virus , which is the most common and harmful programs forwarded to E-mail lesser space we can prevent from E-mail viruses by remembering the following points.

a) Never open such attachments are sent by the unknown senders.

b) We should already prepared by installing a anti-virus software on our systems .macro-virus are also contain a code that infects the various applications of systems.It does not harm much ,but the text insert at same points.

3. ENCRYPTED VIRUSES

Basically encryption means to change the message or text in the loading language, so that the hacker could not try to do any change in that message.By cryptography which consists encryption and decryption we can secure the data and text.

In this virus consist a decryption module and encrypted copy of the virus codes. When we send something to the receiver, then the encryption changes to cipher text, cipher text is the text which is not readable to humans and even machines .after this it decrypted the text in plain text which is readable to humans .through this we can save from the virus by encrypt and decrypt our data , but it is sometime gets easier for the hacker to scan all the codes . the old but easy way will be the use of arithmetic operations like addition and subtraction and use of logic conditions like AND, OR, NOT,XOR ring.

4. VULNERABILITIES AND VIRUSES

Vulnerabilities are the loop hole which are found by the attackers to attack on your systems. It is the internal control of system which the user does not know but attackers knows it very well and he tries to hack your all data and software from the system. To protect the vulnerabilities we should immediately installed new- new updates of software .we should try to avoid downloading the unusual links, because these links and websites who asked us to open these websites are try to hack your informations, data and contains a 'viruses' which obviously damage your system, a system consists of worms, which replicates itself and causes a thousands of worms in a system and the virus occurs.

4.1 TYPES OF VIRUSES

a) **Polymorphic virus**

b) **Retro virus**

c) **Stealth virus**

d) **Multipartite virus**

e) **Companion virus**

f) **Phage virus**

a) POLYMORPHIC VIRUS:

Polymorphic virus or code was the first technique that cause a serious threat of virus. it is like regular encrypted viruses. A polymorphic virus infects files, records and data with encrypted copy of itself, and after decrypted. To enable polymorphic code, the virus must has polymorphic has a polymorphic engine. It calculates and infects a file and contains a copy of viruses. It contains a mutate engine, which change the file name and every time we need to input a code on a new device. Polymorphic virus once installed on a system then it infects all the system. This mutation engine suddenly create a new decrypted, so that when the virus move to the next, it appears in a different file.

Virus may contain a copies of original data. But all these copies of data were non-real which shows error to the users. In encrypt all the data files and records of the user. polymorphic engine help to protect from the virus by which we can save your original data & records. To stay alert from the virus we should always update your data, codes and records ,so that we can aware from the unknown virus.

b) RETRO VIRUS:

Retro virus is a type of RNA(ribosome nuclei acid) which vary & transfer through DNA of the cell. It is difficult to identify this virus until it infects the host. In most viruses, DNA is translated into RNA & RNA is translated into protein. Similarly in system it vary from genes to genes. It infects all the data and pass from one system to another system. During installing any data or file records original programs are removed and infecting data are added into the system. It is a type of backdoor that allows someone to infect all the data without going original excess or execution.

The term ‘retro’ refers backward, means it infects the data going through backdoor and the user knows it about this when all his /her data gets damaged & ruined. So , retro virus is very difficult to identify until and unless it reaches to the host.

c) STEALTH VIRUS:

Stealth virus is a computer virus that uses various type of techniques to detect anti-virus software. Stealth virus are nothing new, it is virus that infect the booting sector in storage .when an anti-virus program runs, a stealth virus hide itself in memory, & uses virus tricks and method to boot records. The virus may contain a copy of the original data. The term ‘stealth refers to doing something with avoiding any notices ,files and records. Viruses are mainly used to harm computer system and network through various techniques and view. To avoid from this we should always be alert and careful to the system & we should avoid as much as we can from downloading and clicking on the links which may be further very dangerous for us and for your system.

d) MULTIPARTITE VIRUS:

It is a computer virus that infects and spread in multiple ways. The first virus which include DOS files & PC bios boot sector virus code. Because it contains multiple factor & spread rapidly by replicating themselves as the name tells us that the multipartite virus, tends to work faster as compare to another virus. the drive controller will no longer present in device. The screen content willaapears as if it is spreading.

When multipartite virus occurs then the files suze& all other application continually changes. The execution of program will take a longer loading times& may not execute the programs. The hard drive re-formats with itself. The extensions changes like DOC change to DOT. So, multipartite virus is also very dangerous for user as it multiply the number of worms in seconds & change the system.

e) COMPANION VIRUS:

A companion virus is computer virus which store in a file whose name is similar to another program file that is executed. When file is executed during this execution the virus will damage the computer.such that it will delete the files from the computer.a companion virus is a types of virus which infects all the files stored in a hard drive. It stores in a file whose name is similar to another file program that is running or executed. It is a piece of software that is used with the purpose of infecting other computer file .

Companion virus includes a lot of security threats , which we should follow to aware from the virus. the most importantly thing is to update our anti-virus software programs as soon as possible. To avoid & be safe from unusual vulnerability or dangerous viruses.

f) PHAGE VIRUS:

Phage virus is a type of virus which infects and replicates within bacteria & worms. There are more than 10^31 bacteriphages on the planet. These are most dangerous type of virus which replicates itself & causes a serious problems to our computer systems. These viruses destroy the all other programs, files & data of computer system. Phage virus is also very dangerous in respiratory & digestive system but if we talk about phage virus in computer it infects & destroy all the other files and media stored in a computer system. To be aware from this we should planned carefully before this happens & should be ready for facing & all the dangerous situations and make them to be solve so, we get rid from these types of viruses.

5. OPERATIONS AND FUNCTIONS:

PARTS

A computer virus must contain a search routine, which point or indicate new files or new disks which are worthwhile targets for infection. Secondly every computer virus must contain a routine to copy itself into the program which the search routine locates.

The three main parts of virus are:

5.1INNFECTION MECHANISMS

Infection mechanism (also called infection vector). It is a mechanism which tells us how the virus spread or propagates through various computer system. A virus has a search routine, which locates new files or new disks for infection. This search routine search the infection or viruses in different computer systems.

5.2 TRIGGER

The trigger, which is aalso known as logic bomb, is the compiled version wwhich could be activate at any time within an executable file. When the virus is run that determines the event or conditions and situations for the malicious “payload” which could be activated or delivered as a particular date, time or a particular presence of another program, the capacity and ability of the disk exceeds some limit, & on double clicking on this, opens a particular file . the data of every company is very confidential but logic bombs or trigger are the viruses which work secretly and steal all the data and records by changing theirs original identity & masque themselves as the originals once in hack all the seconds as a unauthorized users

5.3PAYLOAD

Payload is the actual body or that perform the actual malicious purpose of the virus. Payload actually may be notice able (because it cause the system slow down or freeze). Sometimes payload itself is the harmful activity or task & most time non- destructive (damaging) but distributive ,which is known as virus hoax.

6. PHASES

Virus phases is the life cycle of the computer virus, which is used to describe by using an analogy to biology. This life cycle can be divided into four phases.

a) **Dormant phase**
b) **Propagation phase**
c) **Trigging phase**
d) **Execution phase**
e) **Dormant phase**

a) The virus program is free or idle during this stage. The virus are manage to access the target user's computer or software, but during the stage, the virus is does not take any action. Viruses will eventually be activated by the trigger,which states which event will execute the virus. Not all viruses have this stage.

b) **Propagation phase:** The viruses starts propagating,that is multiplying and replicating itself the viruses places a copy of itself into others programs or into certain system on the disk. The copy may not be identical to the propagating version. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

c) **Trigging phase :**A virus moves into this phase when it is activated, and will perform the various operations and functions for which it was intended. The trigging phase can be caused by a variety of different system events, including count of the no. of times that this copy of the various has made copies of itself by replicating and multiplying itself through different computer systems.

d) **Execution phase:** This execution phase is the actual work of the virus, where the payload will be released. It can delete all the files on disk and crashing the systems, or corrupt files or relatively harmless such as popping up humorous or political messages on screen.

7. INTERNET BEST POSSIBLE SOURCES OF VIRUSES

Internet is the most common and basic source of viruses. We know whatever we do on internet is the basic need of each and every person. Through internet various attachments, links, files, PDF, and all other extra data are downloaded. If we don't want to click on such attachment and link, we should be very careful and aware of all source of techniques of internet., There is a cursor that's shows and blink on that specific point and indicate us to click on that point and download them and some people who don't know about the fact are came under their web, and downloaded them on their phone or system and at the time they have done this downlodation, then their systems are hang and corrupted all the data thus viruses downloaded successfully on their system and fetch all the info. And data from their cells and systems.

8. UNIQUE CHARECTERISTICS OF VIRUS

They are unique because they replicate and alive themselves, the cell which multiply is called "HOST CELLS" here host cells means a cell which does not need other source of replication because they are capable of replicating themselves.

It has two properties or characteristics

a) The ability to replicate itself.
b) The ability to attach itself to another computer file.

It has a ability which attach itself to the next computer, it transfer from one computer to another computer file, so this the advantage of virus , but not for the other peoples or users of computer. So the user has to be aware itself to keep themselves safe from "virus", rather than downloading them & attach these viruses in their system or PC's.

9. EXAMPLES OF VIRUSES

a) CODE RED: code red named come from the mountain dew drink which is favoured or supported by the first researcher to analyse the program, this worm come out in july,2001, infecting as many as 360,000 computers in a single day which is a lot. This worm become so dangerous to stop because it is infecting aa millions of computers in a single day. The worm continuously infecting the same computer fromwhich it has been cleaned from, so it became very tough to stop. The worms attack on the Microsoft IS servers, and cause in large amount of denial of services problems as it ate up all the computing resources and IT personal time.

b) THE MORRIS WORM: this worm is wrote by Robert Morris in 1988 while at that time he was still graduate student at cornell.it eventually made the morris the first person convicted under the fraud and abuse of computer act. However, the story of all this ends happily. Thus morris became the professor of computer science at the Orleans university& become an expert on computer viruses. As the name "morris worms" tells the worm is invented & become an expert is by "moris". He find out an searches more about viruses now teaches computer science at MIT. **Popsci**.com takes a look at ten viruses, worms and Trojans.

c) ELK CLONER: elk cloner was the first PC virus written in 1982 by a high school student, elk cloner was spread by apple DOS through floppy disk on every 50^{th} boot, the virus cause the computer to display a poem which was written by the hackers. Whenever we clicked on a misleading banner ad, opened a file sent or downloaded the wrong porn, everyone's dealt with the computer virus directly or indirectly.

10. SOME MOST COMMON MALWARE SEEN IN THE SYSTEM

COMPUTER VIRUSES: a computer virus is a type of computer program which is a type of computer program which is developed with purpose of infecting computers. Generally replication takes place inside the computer system& this replication itself by modifying other computer programs & insert its own code. When replication succeed, the affected areas are said to be effected by term computer" virus .

There are different ways by which virus get transfer from one media or device to another system

a. By using infected media source of transferring info. Like USB or CD's.
b. Virus transmitted by social website and through E-mail .
c. As a part of another program virus enter through this.

As per the above info. E-mail are the most common, highly effected and harmful viruses that affecting the system most.

To prevent E-mail virus we can prevented it by following ways

a) Never open attachment that are received from unknown sender
b) Keep installing the anti- virus software on your system

10.1 WORMS : Worms are the most common viruses which are spread through viruses systems "Worms'' replicates (means multiply, suppose if there are four then they multiply it by four, and becomes 4*4=16 worms and after 16 they again replicate with another 16 worms). This type of replication will continuously increased by one then other and at last they hack or infect the whole system and call the cause serious virus. Worms doesn't need any host app to get transmitted from one system to another that is they does not need any another source to help in replication, they are it self sufficient for transmitting from one PC or system to another PC or system.

10.2 TROJAN HORSES: Trojan horses does not replicate as worms does, but can pass from one system to another. During installation original program get replace by a Trojan horses means when we install something on a system, the programs that are original get change by a "TROJAN HORSES". To prevent the system from Trojan horses their should be a backup of data after installing new software on the system. Trojan horses are the most common type of malware which can be seen in the computer system it does not replicate but it can be transfer from one system to another system through various sources of transferring viruses.

10.3 ROOT KIT : A rootkit is a collection of computer software ,typically ,malicious,which is design to enable access to a computer .the term rootlkit is a combination of two words that is "ROOT"and the word "KIT" is a software components that implemented the tool .rootkit can be automatically installed or an attacker can installed it after obtaining root on access .obtaining these access is a result of direct attack on a system ,that is exploitingor damaging a known vulnerabilities (loop holes)or a password.the removal of a rootkit is very difficult for computer users but some vendors can automatically detect it and remove .according to the experts they believe the only way to remove them is to keep reinstalling the operating system from media which you are trusted .

10.4 SPYWARE: The spyware works as by showing the message on the system .

System Warning

X **Your windows computer could be at risk!**

Details: Viruses spyware &molware can be installed on your computer without yours knowledge whist browsing the internet

Action Required: Install the repair tool to protect & Clean your system of harmful by hacking "Secoure now" as soon as possible!

11. THE VARIOUS TIPS TO PREVENT MALWARE FROM INFECTING THE COMPUTER :

a) Install antivirus or malware software on your system.
b) Keep your antivirus software up to date…
c) Run regularly schedule scans with the antivirus software.
d) Keeps the operating system updating i.e keep current orlatest.
e) Secure your networks.
f) Think,while clicking any other add,or any other title on which the cursor Points you to divert your mind.
g) Use a firewall (which is a piece of hardware or software) through firewall No one can steal the information easily from the system.Firewall provides security and filter the content from network.
h) Use a strong password,so that no one can hack the system and detect the password easily.
i) Keep minimum downloading as much as you can because it is best source through which virus enter.
j) Keep watching your downloads and avoid from suspicious websites.
k) Installanti-spyware and anti-malware programs.
l) Never open e-mail attachments without screening them.
m) Always be in the know of latest update of all anti-virusprogram.
n) Update! Update! Update! As much as you can.updating is the best way of a
o) Awaring to prevent malware from infecting the computer

12. COMPUTER VIRUSES CONCLUSION:

For better and safe calculation anti-virus software should be installed and be helpful for global network freely. It is good to be aware of malware when we surf in the internet and Download files some files that look interesting might hide a malware. Information is the best form of protection, frequently checks the virus. These are the most common source of viruses. To protect system form virus we should use firewall and its (antivirus detection system). There should be tow firewall placed i.e before gateway and after gateway.

- Keep the software up to date so that the hacker cannot harm the computer system
- Don’t click on links which is sanded through emails use free anti-virus software
- Use a strong password so that the unknown user cannot recognize it easily
- Use firewalls and minimize downloading various things on your systems
- Use pop-up blocker to protect your computer system
- The best thing is to keep update the system as much as possible to prevent form viruses

13. REFERENCES

1. Cohen Fred, an undetectable computer virus Achieved 2014-05-25 at the way back machine, 1987, IBM
2. Burger, Ralph 1991 Computer viruses and data protection, PP. 19-20
3. Alan Solomon, Dmitry O Gryaznov 1995. Dr. Solomon's virus encyclopaedia
4. Mark Ludwig 1998. The giant black book of computer viruses.
5. Szor Peter. The art of computer virus was published in 2005
6. Grimes Roger. Malicious mobile code virus protection for windows was published in 2001
7. Ruben king, Neil. J. the best free ant-virus was published in February 17, 2012. He also published Secunia Personal Software inspector 3.0 review and rating in 19 January 2013
8. Eli B. cohen publish the navigating information challenges in forming science. pp. 27 in 2011