Introduction & History of Computer Viruses

Shivali Bahukhandi, Sandeep Singh Rana

Abstract— In recent years the detection of computer viruses has become common place. It appears that for the most part these viruses have been 'benign' or only mildly destructive. However, whether or not computer viruses have the potential to cause major and prolonged disruptions of computing environments is an open question. In the below mentioned paper i have given the introduction about the topic, definition, common viruses available and how to protect our system from viruses.

Index Terms— computer security, virus, computer virus, worms, computer infection

1 Introduction

In the mid 80's ,the amjad brothers of Pakistan ran a computer store, they wrote the first computer virus in the world, a boot sector virus that was called "Brain", from this discovery the revolution came to the computer industry, in recent decades the term of computer viruses came into boom, even those who are not familiar with the term of computer viruses become familiar with the term by seeing it in the Hollywood movies with the latest technology.

This paper purposes to depict the current situation of computer viruses and the latest trend and the damage caused to the system by the viruses.

2 DEFINITION OF COMPUTER VIRUSES

A computer virus is a program file that is capable enough to make its own code without the knowledge of the user by linking the file to the document. When the file or document that run destroys others files also and spread to the computer slowly and steadily.

Computer viruses are just the same as the viruses or the diseases that attacks the human body, they also directly or indirectly destroys our body the same case is that with the computer viruses.

Execution of host program file results in execution of viruses.

Needs human action to execute.

The structure of Computer Virus can be divided into four phases-

1. Mark
2. Infection Mechanism
3. Trigger
4. Payload

3 CATEGORIES OF COMPUTER VIRUSES

There are following basic categories of viruses-

3.1 Macro Viruses

These viruses infects all the files that contain macros i.e.doc,pps,xls and mdb, they affect the macros ,templates and also the documents that are present in the files

Examples are:

- Relax
- bablas
- Melissa.A
- 097M/Y2K

3.2 Memory Resident Viruses

They attack inside the computer memory, it gets activated when the operating is running and infects all other files, they are hidden in RAM.

Example are:

- CMJ
- meve
- randex
- mrklunky

3.3 Overwrite Viruses

These viruses delete the efficient information available in a file,at the end it leaves the file fully or half useless,it replaces the content but do not change the size of the file

Examples are:

- Trj.Reboot
- way
- trivial.88.D

- *Shivali Bahukhandi is currently pursuing bachelor degree program in Computer Science & Engineering from Shivalik College of Enigeering, Dehradun (Affiliated to Uttarakhand Technical University), Uttarakhand, India.*
- *Sandeep Singh Rana is currently working as an Assistant Professor in the Department of Computer Science & Engineering of Shivalik College of Engineering, Dehradun, Uttarakhand.*

3.4 Direct Action Viruses

These types of virus duplicates and takes action when they are executed, they infect the files in the directory or the folder in it . AUTOEXEC.BAT, they are found in the root directory.

Example : Vienna virus

3.5 Directory Virus

Other name for this type of virus is cluster virus,they infect the directory of computer it does this by changing the path of file location,located in the disk but after affecting it affects the entire directory.

Example is: dir-2 virus

3.6 Web Scripting Virus

Mostly the web pages include complex codes with the purpose to create an interactive and interesting content, these codes are used to create unwanted actions, they comes from infected WebPages.

Example is: JS.Fortnight – a virus that spreads via malicious emails.

3.7 FAT Viruses

They attack the file allocation table (FAT) which is the part to store every information.

Examples is: the link virus
Polymorphic Virus

They do their own encrypting and programming in different style when they infect the computer, they use different encryption and algorithms, it makes it difficult for the antivirus to trace it.

Examples are:

- Marburg
- tuareg
- Satan bug
- elkern

3.8 Worm

This program has the property of self replication causing negative effects on the computer.

Worm Viruses Include:

- lovgate.F
- sobig.D
- trile. C
- PSWBugbear.B
- Mapson

3.9 Trojans

Trojans can un approved tracing of important login details of users online..Email Virus. This is a virus spread through an email.This virus hide in an email and when the receiver receives the mail it is spread widely

3.9 Browser Hijacker

It can be spread while downloading; it affects the browsers functioning of basically redirection of the user to certain sites.
Example is:
the cool web search
Boot Infectors

It include the root sector and the master boot record, they infect the hard disk or the floppy.

4 NAMES OF VIRUSES

There are a number of popular viruses-

4.1 ILOVEYOU

The ILOVEYOU virus is considered one of the most dangerous computer virus ever created. The virus was created by two Filipino programmers, Reonel Ramones and Onel de Guzman. It made use of social engineering to get users to click on the attachment; the attachment was basically a txt file This led to the execution of the E-Commerce Law.

4.2 Code Red

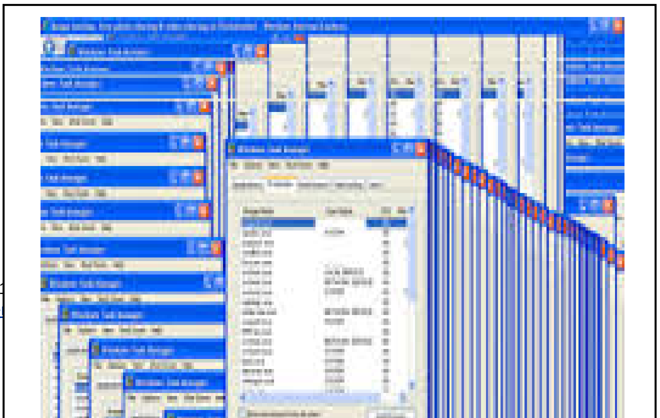
Code Red was discovered in 2001 by two eEye Digital Security employee, it set it goal on computers with Microsoft IIS web server.

4.3 Sasser

It is basically a windows virus created by Sven Jaschan, who also created the Netsky worm; it took advantage of buffer overflow weakness in local Security authority service

4.4 Zeus

It is a Trojan horse made to affect Windows computer to perform various criminal tasks, common task in this is the main in the middle browser key logging and form grabbing



S N	Name of the virus	Year of discovery	Infection caused
1	iloveyou	5 may 2000	It spread by e-mail, arriving with the subject line "**ILOVEYOU**" and an attachment, "LOVE-LETTER-FOR-YOU.txt.vbs".
2	Code red	July 15,2001	It allows the worm to execute arbitrary code and the machine with worm
3	Sasser	April 12,2004	The virus scans different ranges of IP address and connects victims computer primarily through TCP
4	Zeus	July 2007	It is spread mainly through drive by downloads
5	mocmex	17 February 2008	It was the virus that attacked the photo frame
6	Daprosy worm	15 july 2009	It stealed online game passwords.
7	Waledac botnet	January,2010	It was capacable of sending about 1.5 million spam message
8	duqu	1 september,2011	Its nature was same as that of the malware.
9	shamoon	16 aug,2012	It is designed to target computers running on Microsoft windows in the energy sector
10	Cryptolocker	September 2013	It encryptes the files on a user's hard disk
11	Regin	November 2014	Once downloaded,regin quietly downloaded extension of itself, makes difficult to be detected
12	ramsowore	2016	Used for defence purposes.

5 Common Viruses of the year

6 Life Cycle of Computer Virus

Stage I - Creation – The Computer viruses are created by peoples who wish to cause damage to computers.
Stage II -Replication - Computer Viruses duplicates itself and transfers from one pc to another pc
Stage III -Activation -The damage causing viruses activates itself when the conditions are successfully met for it.
Stage IV -Discovery - It takes place once a year at least when the virus have become a threat
Stages V -Assimilation - At this point of time the antivirus developers detect the remedy to cure the virus, this may take time period of one to 6 months also
Stage VI -Eradication - If any user install proper software to delete the viruses it can be successfully deleted, but the fact is that not any virus is deleted completely but its effect is reduced.

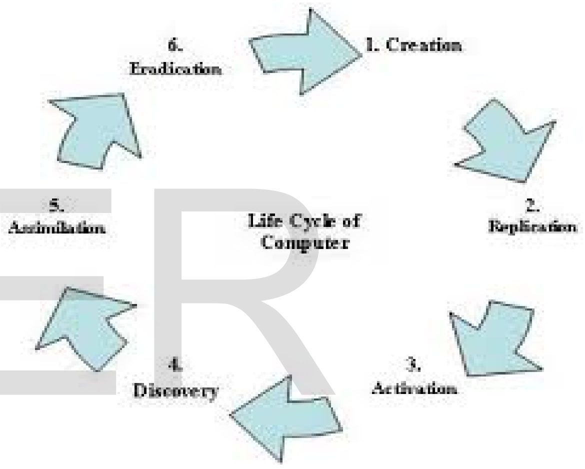


Fig.2. Life Cycle of Computer Virus

7 How to protect our system from Computer Virus?

1. Keep your windows defender activated as it could protect the system from any malicious activity occurring
2. use antimalware app and also keep it updated(basically antimalware app check for viruses, spyware and any other threatening events occurring within the system which could interrupt its processing)
3. use of pop-up blocker is useful
4. we should pay attention to all the notification.
5. if we are using Internet Explorer we should ensure that Smart screen is turned on
6. windows should be updated and it should be the genuine windows
7. make sure that User account is always turned on

8 PROBLEMS OF COMPUTER VIRUS

There are many problems associated with computer viruses some are listed below

1. Computer speed or performance, decreases
2. Computer boots and reboots again and again
3. loosing of data from drives and disks
4. Cause erratic screen behavior.
5. Weird messages comes on screen
6. Browser home page also changes itself.
7. Application softwares changes

9 CONCLUSION

Virus basically destroys our system due to which our efficient information is also lost and multiple copies of the same data is stored due to which more pressure is put on the computer, so we should always keep our firewall and antivirus updated**.**

10 REFERENCE

[1] A System to Support the Analysis of Antivirus Products' Virus Detection Capabilities, Marko Helenius, 2002.

[2] http://www.faqs.org/faqs/computer-virus/

[3] http://www.wildlist.org/WildList/

[4] ASP Press Pittsburg 1990 "A Short Course on Computer Viruses"; Fred Cohen; 1992 all.net/books/ir/csl02-92.html Cohen, Fred; Establishing a Computer Security Incident Response Capability

[5] usvms.gpo.gov/findfact.html,Findings of Fact; United States District Court For The District of Columbia, 1999.

[6] www.symantec.com/avcenter/venc/data/mailissa.html Symantec AntiVirus Research Center, 1999.,

[7] http://www.microsoft.com/com/tech/com.asp

[8] ICSA 1998 Computer Virus Prevalence Survey, 1998.

[9] http://msdn.microsoft.com/library/default.asp?url=/library/enus/netdir/ldap/lightweight_directory_access_protocol_ldap_api.asp

[10] C. Nachenberg, 'Computer Parasitology', Proceedings of The Ninth International Virus Bulletin Conference, 1999. p. 7.

[11] Virus and Malicious Code Protection for Wireless Devices, Trend Micro, February 2001.

[12] Possible Virus Attacks Against Integrity Programs And How To Prevent Them; Vesselin Bontchev, Virus Test Center, University of Hamburg. Feb. 12, 2001; NIPC CyberNotes Issue #2001-03;.

[13] ICSA 2001 Virus Prevalence Survey. pages 822 – 832, NCSA ibid

[14] Fred Cohen, Computer Viruses - Theory and Experiments, Computer Security: A Global Challenge, Elsevier Science Publishers B. V. (North-Holland), 1984, pp. 143-158.

[15] Fred Cohen, Computer Viruses - Theory and Experiments, Computer Security: A Global Challenge, Elsevier Science Publishers B. V. (North-Holland), 1984, pp. 143-158.

[16] Yisrael Radai, Checksumming Techniques for Anti-Viral Purposes, Proc. 1st Int. Virus Bulletin Conf., September 1991, pp. 39-68. Computer viruses: The threat today and the expected future Xin Li 67

[17] Fred Cohen, A Cost Analysis Of Virus Defenses, A Short Course On Computer Viruses, ASP Press, 1990, ISBN 1-878109-01-4, pp. 155-160. pp. 155-160, Fred Cohen, A Cost Analysis Of Virus Defenses, A Short Course On Computer Viruses, ASP Press, 1990, ISBN 1-878109-01-4.