***Journal of Advanced Computer Science and Technology**, 1 (4) (2012) 316-324*
©Science Publishing Corporation
www.sciencepubco.com/index.php/JACST

Computer Virus: Their Problems & Major attacks in Real Life

Milind. J. Joshi[1], Bhaskar V. Patil[2]

[1]Shivaji University Kolhapur, Kolhapur [M.S.], India
Email: milindjoshi@unishivaji.ac.in
[2]Bharati Vidyapeeth University Yashwantrao Mohite institute of Management, Karad [M.S.], India
Email: bhaskarpatil28381@yahoo.co.in

Abstract

Today's enterprise networks are distributed to different geographical locations and applications are more centrally located, information represents the most important asset. With the growing number of data communication services, channels and available software applications, data are processed in large quantities and in a more efficient manner. This technological enhancement offers new flexible opportunities also measure security threats poses in the networks. These threats can external or Internal, external threats divided as hacking, virus attack, Trojans, worms etc.

There are thousands and thousands of different viruses these days which improve every day. Although the wild spread of new and strong viruses, it still infects and spread only with user's permission. This research paper highlights the phases of computer virus, computer virus, history of worst computer attack, type of computer virus with effect on computer & few examples of virus on their types, working of computer virus, and problem occur due to virus in computers.

Keywords: *Network, Virus, Security threats, Hacking, Attack of Computer Virus, Major attacks & Life Cycle of Computer Virus*

1 Introduction

Today enterprise networks are distributed to different geographical locations and applications are more centrally located. Every company's data is most valuable asset and must be treated as such. With the ever growing number of malicious threats; such as Viruses, Spyware and Hackers, it has become mandatory to protect yourself against them. The most powerful way for communication and data transfer is internet, because the speed of internet goes increased day by day. People can transfer large amount of data within few minute from one location to another location worldwide.

Computers are used extensively to process the data and to provide information for decision making therefore it is necessary to control its use. Due to organisational cost of data loss, cost of incorrect decision making, and value of computer software hardware organisations suffer a major loss therefore the integrity of data and information must be maintained. There are thousand and thousand of different viruses these days which improve every day. From these virus performance of computer goes slowly, entire disk will be crashed, programs are modified and more.

2 Information about Virus

A computer virus is self replicating program containing code that explicitly copies itself and that can infects other program by modifying then or their environment [1]. Harmful program code refers to any part of programme code which adds any sort of functionality against the specification. [2] A virus is a program which is able to replicate with little or no user intervention, and the replicated program(s) are able to replicate further. [4] Malicious software or malware for short, are “programs intentionally designed to perform some unauthorized - often harmful or undesirable act." Malware is a generic term and is used to describe many types of malicious software, such as viruses and worms. A typical structure of a computer virus contains three subroutines. The first subroutine, infect-executable, is responsible for finding available executable files and infecting them by copying its code into them. The subroutine do-damage, also known as the payload of the virus, is the code responsible for delivering the malicious part of the virus. The last subroutine, trigger-pulled checks if the desired conditions are met in order to deliver its payload.

The structure of Computer Virus can be divided in to four phases; [6]

Mark cans prevent re-infection attempts.
Infection Mechanism causes spread to other files.
Trigger is conditions for delivering payload.
Payload is the possible damage to infected computers.

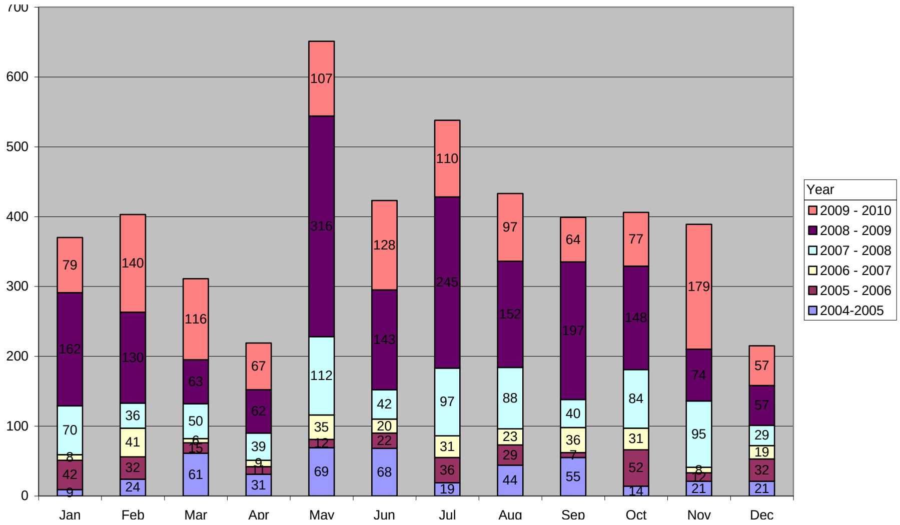
3 History of Computer Virus

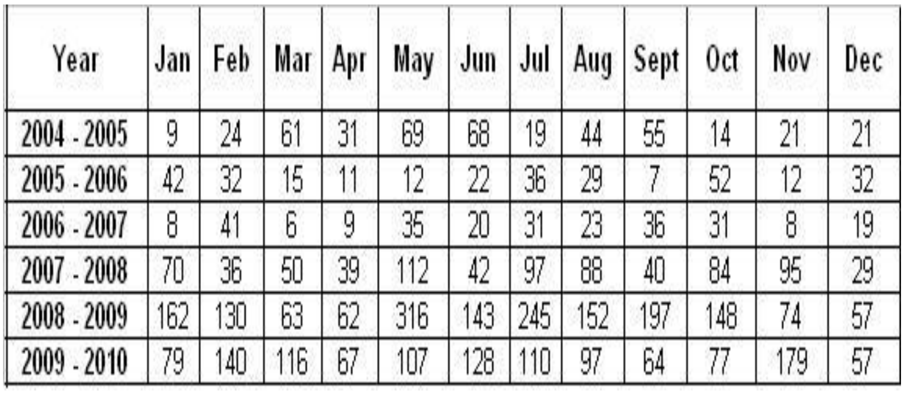
There are thousand and thousand of different viruses these days which improve every day. However, there is much software released every day to detect and avoid these viruses. Although the wild spread of new and strong viruses, it still infects and spread only with user’s permission.

There are endless arguments about the "first" virus. There were a number of malware attacks in the 1970s and some count these among the virus attacks. The description of the malware, however, would indicate these were worms and not viruses by general definition. Just to be complete, however, the questionable entries from the 1970s are included here with that Computer Knowledge considers virus history to start in 1981. And in year 1995 to 2000 the total number of computer virus are created. And in 2001 to 2010 them are increases up to 1221 number of newly create computer virus.

The new computer virus are created from year 2005 to year 2010 are shown in table 1. The table shows that for every month computer virus are created. [7]

Table 1: Year wise total no. of virus





Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec
2004 - 2005	9	24	61	31	69	68	19	44	55	14	21	21
2005 - 2006	42	32	15	11	12	22	36	29	7	52	12	32
2006 - 2007	8	41	6	9	35	20	31	23	36	31	8	19
2007 - 2008	70	36	50	39	112	42	97	88	40	84	95	29
2008 - 2009	162	130	63	62	316	143	245	152	197	148	74	57
2009 - 2010	79	140	116	67	107	128	110	97	64	77	179	57

Fig. 1: Year wise total number of computer virus

From the above chart 1 showing in year first and last four month less number of computer viruses is created. In remaining four month computer virus are created much more as compare to first and last four month of every year.

4 Types of Computer Virus

There are thousands of different kinds of viruses but they form distinct groups. They all operate differently and affect our computers and the information contained on them in different ways. From the Table [Table: 2 Types Of Computer Virus] shows that the different types of computer virus, what it does, how a particular computer virus are get affected with some example of commuter virus.

Table 2: Types of Computer Virus

Virus Type	**What it Does**	**How Affects our PC**	**Example of Virus**
Resident Viruses	To live as a resident in the RAM memory	it interrupt all of the operations executed by the system	Randex, CMJ, Meve, and MrKlunky
Program or File Virus	Infects executables such as EXE, BIN, COM, SYS)	Destroys or alters programs and data.	Sunday and Cascade
Boot sector Virus	Infects boot sectors on hard and floppy disks	Destroys or alters programs and data.	Disk Killer, Stone virus.
Multipartite Virus	A hybrid of a program and boot sector virus	Destroys or alters programs and data.	Invader, Flip, and Tequila
Macro Virus	Triggers on a command in Microsoft Office	Commonly affects Word & Excel	DMV, Nuclear, Word Concept
Stealth Virus	Uses various tactics to avoid detection.	Destroys or alters programs and data.	Frodo, Joshi, Whale
Polymorphic Virus	Uses encryption to foil detection, so that it appears differently in each infection.	Destroys or alters programs and data.	Involuntary, Stimulate, Cascade, Phoenix, Evil, Proud, Virus 101
Email Virus	If the recipient opens the e-mail attachment, the word macro is activated then	spread only with the opening of the attachment in the email	Melissa, ILOVEYOU, Love Bug
Spyware	It makes unnecessary alterations to your PC & changes your experience of it.	a computer system is causing it to slow down	7FaSSt, Elf Bowling
Trojan Horses	Programs that do things that are not described in their specifications.	It allows other computer users to take control of your PC over the internet	A2KM. Nitrogen , 91Cast, 8sec!Trojan
Worms	negative effects on your system, they are detected and eliminated by antivirus	It replicate themselves as stand-alone programs	Lovgate.F, Trile.C, Sobig.D, Mapson.
Directory Virus	It inserts a malicious code into a cluster and marks it as allocated in the FAT.	It prevents FAT allocation from being allocated in the future	Spam Laws, DIR II virus

5 Histories of Worst Computer Virus Attacks

Virus attacks are not shocking news anymore. But here is the list of the worst of those attacks which shocked many at that time in history. The history of computer virus attack is as follow;

[5.1] **Melissa -**It was created by David L. Smith in 1999 and is based on a Microsoft Word macro. He intended to spread the virus through e-mail messages. The virus prompts the recipient to open a document and by doing so the virus gets activated. The activated virus replicates itself and will be transferred to 50 persons whose address is present in the recipient's e-mail address book. The increase in e-mail traffic due to the virus forced some companies to block e-mail programs until the virus attack was controlled.

[5.2] **MyDoom -** It was creates a backdoor in the OS of the victim's computer. The MyDoom virus had two triggers. One of them began a denial of service (DoS) attack on Feb. 1, 2004. In Feb. 12, 2004 the second trigger was initiated which stopped the virus distributing itself. Later that year, MyDoom virus outbreak occurred for a second time, which targeted several search engine companies. The virus would send a search request to a search engine and will use e-mail addresses obtained in the search results. Such a type of attack slowed down search engine services and caused some website crash.

[5.3] **ILOVEYOUILOVEYOU -**It was a standalone program which was capable of replicating itself. The virus initially traveled through the e-mail, same way as Melissa virus. The email had a subject which says that the message was a love letter from the secret admirer. Attachment with this e-mail caused all the trouble. The file LOVE-LETTER-FOR-YOU.TXT.vbs contained the worm.

[5.4] **Nimda -**It was spread through the Internet rapidly and became one of the fastest propagating computer virus. The Nimda worms aimed on the Internet servers and its real purpose was to slow down the Internet traffic. Nimda could travel through the Internet in multiple methods which included the email. The Nimda virus caused several network systems to crash as the system's resources were taken away by the worm. The Nimda worm was one of the dreaded distributed denials of service (DDoS) attack virus.

[5.5] **The Klez Virus -**It was appeared in late 2001 and infected a victim's computer through an e-mail message. The virus replicated itself and was sent itself to all the contacts in the victim's address book. The modified version of this virus could take any name from the contact list of the victim and can place that address in the "From" field. This technique is called spoofing. By spoofing the e-mail appears to come from a source when it's actually coming from somewhere else.

Spoofing will prevent the user's chance to block email from a suspected recipient.

[5.6] **SQL Slammer / Sapphire SQ -**It was caused a damage of affected networks included Bank of America's ATM service, Continental Airlines etc. A few minutes after the infection of the first Internet server, the number of victims of the Slammer virus doubled every few seconds. After Fifteen minutes of the first attack, half of the servers that act as the pillars of the Internet were affected by the virus.

[5.7] **Sasser and Netsky -** It was exploited Microsoft Windows vulnerability. The infected system will look for other vulnerable systems and instruct those systems to download the virus. A random scan of the IP addresses was done to find potential victims. The virus made it difficult to shut down the computer without turning OFF the system. The Netsky virus spread through e-mail and Windows networks. The virus causes a denial of service (DoS) attack on the affected system.

[5.8] **H. Leap-A/Oompa-A -**It was one of the viruses which aimed at Mac systems. The viruses used the iChat instant messaging program for its propagation among vulnerable Mac computers. The Leap-A virus was not able to cause much harm to computers, but showed that even a Mac computer can be affected by malicious softwares.

[5.9] **Code Red and Code Red II -** It was exploited operating system vulnerability found in Windows 2000 and Windows NT machines. A buffer overflow problem was the vulnerability. Due to this if the OS receives more information than its buffers handling capacity; the adjacent memory will be overwritten. The original worm initiated a distributed denial of service attack to the White House website. That means all the infected computers with Code Red try to contact the Web servers at the same time, thereby overloading the machines. The infected machine no longer obeys the owner, allowing a remote user to control and access the machine.

[5.10] **Storm Worm -**It was got this particular name because of the fact that the e-mail messages which carry the virus carried a subject "230 dead as storm batters Europe." Some versions of this Worm turn computers into bots or Zombies. The infected computers become vulnerable to further attack by the person behind the attack.

6 Working of Computer Virus

Computer viruses have a life cycle that starts when they're created and ends when they're completely eradicated. The following diagram [Diagram 1: Life Cycle] points are describes in each stage [9].

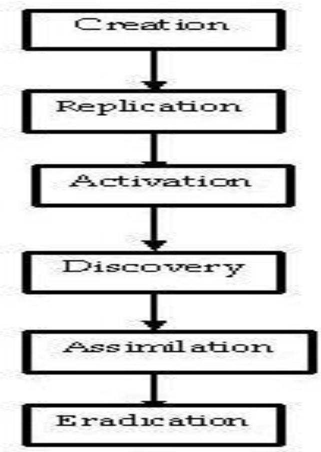


Fig. 2: Life Cycle of Computer Virus

Stage I - Creation – The Computer viruses are created by misguided individuals who wish to cause widespread, random damage to computers.

Stage II -Replication - Computer Viruses replicate by nature means it copies itself from one PC to anther PC.

Stage III -Activation - Viruses that have damage routines will activate when certain conditions are met. Viruses without damage routines don't activate, instead causing damage by stealing storage space.

Stage IV -Discovery - This phase doesn't always come after activation, but it usually does. Discovery normally takes place at least a year before the virus might have become a threat to the computing community.

Stages V -Assimilation - At this point, antivirus developers modify their software so that it can detect the new virus. This can take anywhere from one day to six months, depending on the developer and the virus type.

Stage VI -Eradication - If enough users install up-to-date virus protection software, any virus can be wiped out. So far no viruses have disappeared completely, but some have long ceased to be a major threat.

The same or different developer develops a different strain of a new virus and process begins afresh.

7 Problems of Computer Virus

Many common computer problems are easy to fix but hard to diagnose. Once you figure out what is wrong with the computer, a solution is easy to find. Most of the time, it will either be a problem of: viruses, malware, spyware or a computer running slow. There are some common problems occur due to the virus attacks which are given bellow;

[7.1] Computer speed or performance has slowed

[7.2] Computer system freezes and blue screens of death

[7.3] The computer keeps on rebooting again and again
[7.4] An entire disk or drive is erased
[7.5] Cause erratic screen behavior
[7.6] Unexplained messages appear on the screen
[7.7] Many viruses do nothing obvious at all except spread!
[7.8] Your browser home page changed itself
[7.9] Application software seems to be changed
[7.10] Operating system software appears to be modified
[7.11] Unexplained printing problems occur

8 Conclusions

A computer virus is software intentionally written to copy itself without the computer owner's permission and then perform some other action on any system where it resides. Now a days, viruses are being written for almost every computing platform Anti-virus protection is, or should be, an integral part of any Information Systems operation, be it personal or professional. There are number of computer virus are created and these computer virus are affected in day today life. These viruses erase important data. before finding the solution against the computer virus people must know the basic thing of computer virus like which are the type of computer virus are created now a days, working of computer virus, problem occurs from computer virus.

Acknowledgments

The researchers are grateful to the authors, writers, and editors of the books and articles, which have been referred for preparing the presented research paper. It is the duty of researcher to remember their parents whose blessings are always with them.

References

[1] Dr. Solomon's Virus Encyclopedia, 1995, ISBN 1897661002

[2] Dr. Klaus Brunnstein 1999, from Antivirus to Antimalware Software and Beyond http://csrc.nist.gov/nissc/1999/proceeding/papers /p12.pdf

[3] Paul Royal, Mitch Halpin, David Dagon, Robert Edmonds, and Wenke Lee. PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware. In The 22th Annual Computer Security Applications Conference (ACSAC 2006), Miami Beach, FL, December 2006.

[4] Rainer Link, Prof. Hannelore Frank, August, 2003, Server-based Virus-protection On Unix/Linux

[5] Felix Uribe, Protecting your Personal Computer against Hackers and Malicious Codes
[6] K. Lai, D. Wren, T. Rowling, Consumer Antivirus Performance Benchmarks
[7] The Wild List Organization International, www.wildlist.org
[8] Digg, Worst Computer Virus Attacks in History, September, 2009
[9] Gaurav Sharma, A LOOK INTO COMPUTER VIRUSES