ISSN No. 0976-5697

Volume 3, No. 1, Jan-Feb 2012

International Journal Of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online AT www.ijarcs.info

Computer Virus and Methods of Virus Detection Using Performance Parameter

Dr. Milind. J. Joshi
Shivaji University Kolhapur,
Kolhapur [M.S.], INDIA
milindjoshi@unishivaji.ac.in

Mr. Bhaskar V. Patil*
Bharati Vidyapeeth University Yashwantrao Mohite
institute of Management, Karad [M.S.], INDIA
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 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. These threats can be minimized using number of network security tools and antivirus software, but all are not equally compatible for each type of attack hence the study is undertaken. It runs random access of memory of a computer.

This research paper highlights the phases of computer virus, History of computer virus, working of antivirus software, computer virus detection methods, and parameter for finding best antivirus software in all generations.

Keywords: Antivirus, Computer Virus, Security threats, detection methods, and System scan.

I. 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, Spy ware and Hackers, it has become mandatory to protect yourself against them.

In order to prevent such data looses many organization came forward and designed network security tools and antivirus packages. Antivirus packages are mainly used to prevent and remove the viruses, Trojans, worms etc, where as firewalls are used to monitor incoming and outgoing connections.

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 organizational 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. However, there is much software released every day to detect and avoid these viruses. Antivirus packages are mainly used to safeguard. Antivirus software is class of program that reaches a hard drives and floppy disk, pen drives for any known or potential viruses. It runs random access of memory of a computer.

There are number of venders providing antivirus packages which are differ in various features such as installation time, size, memory utilized, boot time, user interface launch time and full system scan time etc.

II. 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. This is a typical structure of a computer virus which 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.

III. 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: 1Year 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

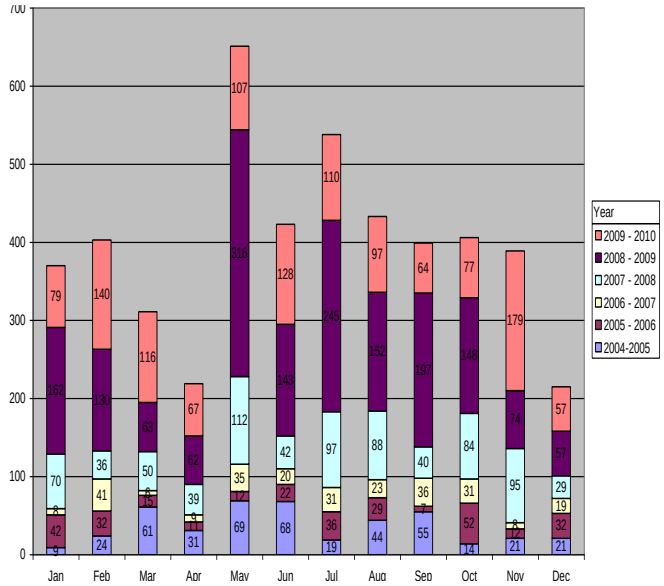

Figure: 1Year wise Total Number of Computer Virus

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.

IV. INFORMATION ABOUT ANTIVIRUS

Organization need to provide security skeleton to prevent the data didding due to malicious code. In order to provide the security the organizations go through the security audit and most of the organization chose the internet security software as well as design their personal firewall and antivirus.

Antivirus solutions are now a common component of computer system. However, security issues pertaining to the anti-virus software itself have not captured enough attention of anti-virus vendors and computer users.

"Antivirus" is protective software designed to defend your computer against malicious software. Malicious software or Malware includes: viruses, Trojans, key loggers, hijackers, dialers, and other code that vandalizes or steals your computer contents. Anyone who does a lot of downloading, or accesses diskettes from the outside world on a regular basis should develop an antivirus strategy.

Antivirus software is equipped with features that not only check your files in your system, but also check your in-coming and out-going e-mail attachments for viruses and other malicious programs [5]. The most important weapon in your antivirus is a clean, write-protected bootable system diskette. Booting from a clean write-protected diskette is the only way to start up your system without any viruses in memory. An effective defense against viruses is a clean backup of your hard drive. Many antivirus packages will attempt to disinfect infected programs for you so that the virus is no longer in your system.

Antivirus products are categorized into three parts such as Internet Security, Total Security, and Antivirus. Antivirus: products are the products which are primarily focused on detecting and remediation viruses and spy ware. Internet Security product provides all the virus and spy ware removal features of an AV, as well as additional functions to provide greater Internet protection. These features may include protection against phishing, root kit detection, firewalls and scanning of web pages and HTTP data. Total Security: products provide data migration and backup features on top of all security features common to IS products [3].

Antivirus software is class of program that reaches a hard drives and floppy disk, pen drives for any known or potential viruses. It runs random access of memory of a computer.

V. HOW TO CHOOSE ANTIVIRUS SOFTWARE

There are number of antivirus software vender from the year 1988 to remove and immunize computers from the Brain virus. By 1990 there were several anti-virus products available including Anti-virus Plus, Certus, Data Physician, and Turbo Anti-virus. In 1991 Symantec released Norton Anti-virus which remains a major anti-virus brand through 2010 for the security purpose. There are two types of antivirus program developed i.e. standalone program and online scanner. In standalone program user must download program from particular website or purchase license program from vender. And in online scanner customer can protect or secure computer with the help of online scanner. Most antivirus software companies offer a standalone program that will only install a virus-scanning package on your computer. This software will look specifically for viruses in all their varieties, is generally easy to update and will keep your computer running well and relatively safely.

In addition to the stand-alone program, many companies are now offering antivirus software suites that bundle firewalls, spam filtering and anti-spy ware tools into the total package. If you use instant messengers or peer-to-peer file sharing services, an antivirus software suite is a better choice, because it protects you from hackers who try to access your computer directly.

Before you can really look for the features you need in antivirus software, you should understand what each feature can and cannot do.[11] E-mail attachments that are infected with a virus of any kind Corrupt Web sites that try to infect your computer when you visit them Internet worm viruses that roam around looking for unprotected computers Spy ware that can be installed with a downloaded attachment or program, or are installed from a worm Viruses that spread through your computer using features in your software and documents

If there's a single thing that keeps most people from purchasing antivirus software, it's the fact that there are so many options available. How are you supposed to know what

you're even looking for? Break it down into basic choices that help you along. Following are the basic and most important criteria for choosing antivirus software [11] [8].

a. ***Price***- Pay for the best antivirus software that you can afford; there are cheaper (and free) options out there, but they never equal the flexibility and updates provided by the premium software.

b. ***Ease of use***- The best antivirus software Web sites offer screenshots and often full installation guides. To get the most out of your purchase, it should be extremely easy to set up and use.

c. ***Technical support***- Make sure that any antivirus software you're considering offers multiple support options, including e-mail and a toll-free help line. FAQ and support documents are fringe benefits, but they should never be the sole form of support.

d. ***Reviews***- Look for independent reviews of antivirus software on the Web written by people who aren't affiliated with the software company in any way.

VI. COMPUTER VIRUS DETECTION METHOD

Anti-virus software companies design their products to detect and remove viruses; there is more to making a smart choice than comparing detection rates and/or product prices. The software must also be effective against the majority of common and damaging viruses, yet be as inconspicuous to productivity as possible. The anti-virus software is necessary for everyone in the enterprise means that it must work alongside a variety of applications, and probably on multiple computing platforms within the location.

Effective anti-virus software must be capable of performing three main tasks: *Virus Detection, Virus Removal* (File Cleaning) and *Preventive Protection.* Detection is the primary task and the anti-virus software industry has developed a number of different detection methods. There are five methods for detecting computer virus which are as follow [9];

a. Integrity Checking or check summing
b. Interrupt Monitoring
c. Memory Detection
d. Signatature Scanning
e. Heuristic or Rule-based Scanning

a) ***Integrity Checking Or Check Summing*** **-** An integrity checker records integrity information about important files on disk, usually by check summing. An integrity check program with built-in intelligence is the only solution that can handle all the threats to your data as well as viruses. Integrity checkers also provide the only reliable way to discover what damage a virus has done. These methods require software update at specific interval.

b) ***Interrupt Monitoring*** **-** Attempts to locate and prevent a virus “interrupt calls” (Function requests through the system’s interrupts).

c) ***Memory Detection***- In this detection methodology antivirus software are depends on recognition of a known virus’ location and code while in memory; generally successful.

d) ***Signature Scanning***- In these detection method of antivirus software are recognizes a virus’ unique “signature,” a pre-identified set of hexadecimal code, making it highly successful at virus identification. It is totally dependent on maintaining current virus database signature files from vendor and scanning engine refinements; May make false positive detection in valid file.

e) ***Heuristic or Rule-based Scanning***- These detection methods are faster than traditional scanners, method uses a set of rules to efficiently parse through files and quickly identify suspect code.

All five techniques can usually perform on-access or on-demand scans, for both network servers and workstations. Today, all effective products leverage a combination of detection methods because of the large number of virus types and their many tricks for invasion and disguise.

VII. WHERE DO VIRUSES COME FROM

There are number of different ways for attacking computer virus to your computer. The most common way for attacking is internet, because the growth of internet increases day by day. There are some common ways to come computer viruses which are as follow;

a Global Access Networks and Email
b Email Conferences, File Servers, FTP and BBS
c Local Access Networks
d Pirated Software
e General Access Personal Computers
f Repair Services

a) ***Global Access Networks and Email***-Today one of the primary sources of viral infection is the Internet. The unsuspecting user of an infected by macro virus editor software sends infected letters to addressees, who in their turn send new infected letters and so on.

This is the most common case of virus spreading registered by anti-virus companies. Often enough an infected document file or Excel spreadsheet may get into business mailing lists of large companies.

b) ***Email Conferences, File Servers, FTP***- General access file servers and email conferences are also one of the main sources of virus spreading. Virtually every week there appear messages that some user infected his computer with a virus which had been downloaded from FTP server, or emailed to some Usenet group.

c) ***Local Access Networks***- The third way of "fast infection" is via local access networks. If no necessary safety measures are taken, an infected workstation after logging on to a network infects one or several system utility files on a network

d) ***Pirated Software***- Illegal copies of software, as it has always been, are one of the main "danger zones". Often piracy software on diskettes and even on CDs contains files, infected with all kinds of viruses.

e) ***General Access Personal Computers***- Computer systems installations in educational institutions also present danger. If one of the students infected such an installation with virus, brought by him on a diskette, then all the other students using this computer will also get the parasite on their diskettes.

f) ***Repair Services***- Cases like that are seldom but still possible, when a computer is infected while being repaired. Repair personnel are also humans and are prone to negligence to basic rules of computer security. Having once forgotten to write protect one of his floppies, such person will pretty soon spread the viruses to computers of his clients and most likely will lose them.

VIII.PARAMETER FOR ANTIVIRUS REVIEW

There are number of antivirus software developed by their vendors. The main objective of the antivirus software’s is to detect and remove the malicious codes which are

created day by day increase. The parameter of antivirus software review are increases because different of computer virus are created. These are not detected by older technique. Antivirus software is categories in to first generation scanner, second generation scanner, virus specific detection and code emulation technique. The bellow table shows that common computer virus detection technique [9] [12].

a) ***Wildcards:*** Use of wildcards allows excluding some constant byte values or ranges of values from comparison.

b) ***Mismatches:*** It allows negligible values for non-specified quantity of bytes inside a string, regardless of their position.

c) ***Generic Degree:*** when a virus has more than one variant, the variants are analyzed to extract one unique string that indicates all of them. This kind of string scanning uses this common pattern to find any previously identified variants of a virus family.

d) ***Bookmarks:*** Use of Bookmarks is a simple way to ensure a more reliable detection and decrease the risk of false positive.

e) ***Hashing:*** In anti-virus scanners, hashing is exploited in order to decrease the number of searching strings within the file.

f) ***Top-and-Tail Scanning:*** Because virus codes are sited usually at the beginning or end of the victim files, scanning only the first and the last parts, instead of whole file is a useful idea to raise the speed of signature detection procedure more. This procedure is known as top-and-tail scanning.

g) ***Entry-Point and Fixed-Point scanning*****:** These techniques also help the scanning engines to execute more rapidly. They use the concept of the program execution entry-point, which is achievable by the headers of executable files.

h) ***Smart Scanning:*** Smart scanning refers to a defense optimizing method for the newer generation of viruses, which try to conceal their code within a sequence of worthless instructions

i) ***Skeleton detection:*** It is especially effective in order to detection of macro viruses. It does not utilize strings or checksums for detection purpose[9]

j) ***Nearly Exact Identification:*** The purpose of nearly exact identification is more accurately detection of the viruses. One common method is to employ two strings as the signature of the virus, rather than only one. The virus is nearly exact identified, if both strings are existed in the file. Therefore, it makes disinfection process more reliable and risk-free, and ensures that the detected virus is not probable to be an unverified alternative of the primary version of the virus that maybe requires non- similar disinfection manner. Combination with bookmarks makes this technique more dependable.

k) ***Exact Identification:*** The exact identification technique utilizes non-variable bytes in the virus code as many as required to find a checksum of all bytes in the virus program, which contains constant value. The variable bytes of the virus body are ignored and a map of every constant byte is produced.

l) ***Heuristics Analysis:*** The heuristics analysis is a useful method for detection of new unknown malware. It is especially helpful for detection of macro viruses too. It can be so worthwhile for binary viruses, as well, but it may extremely produce false positive output that is a major drawback of scanners.

m) ***Virus-specific Detection:*** this kind of detection is not a regular method, but it denotes any special method that is specifically designed for a given particular virus. This approach is also called algorithmic scanning.

n) ***Filtering:*** This technique is used to optimize the performance of anti-virus engine regarding of scanning speed. It is especially useful in virus-specific detections because those are very time-consuming and high complexity in performance.

o) ***Static Decryptor Detection:*** the method can be a bit faster when it is employed together with an efficient filtering. It can also be employed to find other kinds of encrypted virus, such as oligomorphic or polymorphic viruses.

p) ***X-RAY Scanning*****:** X-ray scanning attacks the encryption of the virus rather than searching for the decryptor. It works based on a previously identified plaintext of the virus, and applies all encryption methods singly on special parts of files, such as top or tail of the file or supposed entry-point, to find the given plain text in decrypted virus body.

q) ***Code Emulation:*** It simulates the computer central processor, main memory, storage resources and some necessary functions of operating system by a virtual machine to run the malware virtually and investigate its behavior and performance.

r) ***Dynamic Decryptor Detection:*** It is a method made of joining static decryptor detection and code emulation. It is helpful when the decryption loop is very long and time-consuming and code emulation merely is not suitable

s) ***A false positive*** occurs when a virus scanner erroneously detects a 'virus' in a non-infected file. False positives result when the signature used to detect a particular virus is not unique to the virus - i.e. the same signature appears in legitimate, non-infected software.

t) ***A false negative*** occurs when a virus scanner fails to detect a virus in an infected file. The antivirus scanner may fail to detect the virus because the virus is new and no signature is yet available, or it may fail to detect because of configuration settings or even faulty signatures.

From the above table shows that [Table 2: Common computer virus detection technique] YES shows that the method can support the property or may affect on the property positively. And NO shows that shows a weakness of the method. Hashing technique in first generation scanner can improve the scanning speed and supports complete disinfection of the infected hosts, but it cannot used for detection of variants of a virus family or unknown virus or micro virus. It has no effect on false negative and false positive alarms.

Table: 2Common computer virus detection technique

Generations	Scanning technique		Promise Perfect detection	Scanning speed improvement	Virus family detection	New or unknown virus detection	Encrypted or polymorphic virus	Metamorphic virus	Micro virus	False positive	False negative
First generation scanner	Simple scanning		Yes	No	No	No	No	No	No	Low	Low
	Optimizing technique	Wildcards	Yes	No	Yes	No	No	No	No	Low	Low
		mismatch	Yes	No	Yes	No	No	No	No	Low	Low
		Generic degree	Yes	No	Yes	No	No	No	No	Low	Low
	Bookmarks		Yes	No	No	No	No	No	No	Very Low	Low
	Speedup technique	Hashing	Yes	Yes	No	No	No	No	No	Low	Low
		Top and tail scanning	Yes	Yes	No	No	No	No	No	Low	High
		Entry point or Fixed point	Yes	Yes	No	No	No	No	No	Low	Low
Second generation scanner	Smart scanning		Yes	Yes	Yes	No	No	Yes	Yes	Low	Low
	Skeleton detection		Yes	No	No	No	No	No	Yes	Low	Low
	Nearly exact identification		Yes	No	No	No	No	No	No	Very Low	Very Low
	Exact identification		Yes	No	Yes	No	No	No	No	Zero	Zero
	Heuristic analysis		No	No	Yes	Yes	No	Yes	Yes	Very High	Low
Virus specific detection	General		Yes	No	Yes	No	Yes	Yes	Yes	Low	Low
	Optimizing technique	Filtering	Yes	Yes	No	No	No	No	No	Low	Low
		Static descriptor detect	No	No	No	No	Yes	No	No	Very High	Very High
		X- ray scanning	Yes	No	No	No	Yes	No	No	Low	Low
Code emulation	Generic Detection		Yes	No	No	No	Yes	No	No	Low	Low
	Dynamic descriptor detection		No	Yes	No	No	Yes	No	No	Low	Low

IX. CONCLUSION

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. Nowadays, 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. Anti-virus software in use today is fairly effective - but only if it's kept updated and the user takes precautions such as not opening unfamiliar documents or programs. Despite all this, anti-virus software cannot protect against brand new viruses, and few users take the necessary precautions. The bottom line is, **there are no anti-viruses guaranteeing 100 percent protections from viruses.** Antivirus software is a constantly evolving field, and as the knowledge base deepens, vendors can further refine these methods and develop even more effective future solutions.

X. 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

XI. REFERENCES

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

[2] Dr. Klaus Brunnstein, "Antivirus to Anti malware Software and beyond", 22nd National Information Systems Security Conference , 1999.

[3] Paul Royal, Mitch Halpin, David Dagon, Robert Edmonds, and Wenke Lee. "Poly Unpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware." In The 22th Annual Computer Security Applications Conference (ACSAC 2006), Miami Beach, FL, pp.289-300 December 2006.

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

[5] Felix Uribe, "Protecting your Personal Computer against Hackers and Malicious Codes" ,AusCERT, pp 1-10 ,2008 http://www.auscert.org.au/AntiMalware

[6] K. Lai, D. Wren, T. Rowling, "Consumer Antivirus Performance Benchmarks" PassMark Software, September 2010

[7] The Wild List Organization International, www.wildlist.org, 2010

[8] Phebe Durand, "How to choose Antivirus software" www.life123com

[9] Scott Gordon, "Current Computer Virus Threats, Countermeasures and Strategic Solutions", McAfee – Network Security & Management, NAI White Paper, pp 1-16, 1997.

[10] Babak Bashari Rad, Maslin Masrom and Suhaimi Ibrahim, "Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011, pp 113-121, 2011.

[11] Vinod P., V.Laxmi, M.S.Gaur, "Survey on Malware Detection Methods", Hack.in 2009**,** 3rd Hackers' Workshop on Computer and Internet Security, pp74-79,2006.