EPH - International Journal of Science And Engineering
ISSN (Online): 2454 2016
Volume 02 Issue 04 December 2016

DOI: https://doi.org/10.53555/eijse.v2i4.6

THE BENCHMARKING MODEL FOR IDEAL ANTIVIRUS SOFTWARE FOR ALL USERS

Dr. Bhaskar V. Patil[1]*, Dr. Prof. Milind. J. Joshi[2]
*[1]*Bharati Vidyapeeth University Yashwantrao Mohite*
[2]*Shivaji University Kolhapur, Kolhapur [M.S.], INDIA institute of Management, Karad [M.S.], INDIA*
Email: milindjoshi@unishivaji.ac.in

Corresponding Author:-
Email: dr.bhaskar.vijay.patil@gmail.com

Abstract:-

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 Antivirus 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. The large number of Antivirus software available in the market and some are being launched, each one of them offers new features for detecting and eradicating viruses and malware. People frequently change their Antivirus software according to their liking and needs without evaluating the performance and capabilities of the various Antivirus software available. This research paper highlights the basic concepts of computer viruses and antivirus software. And also suggest the benchmarking model for ideal antivirus software for all types of user.

Keywords: - *Network, Virus, Security threats, Attack of computer Virus, Antivirus software.*

I. INTRODUCTION

Now a day's computers are very essential part of our life. The uses of computer are increased day by day. A computer people can share information from one computer to another computer with the help of device or media. In the current days there are various ways or method for sharing information because people can carry several gigabytes or terabyte of data from one destination to another destination. We also know history and which devices are used to exchange information in the world. There are several ways a user can go about copying data from one computer to another computer. In the process of exchanging the information using communication media there will be a problem of attack of malware or computer virus. [1]

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 are capable of displaying different messages, denying all kinds of access, data thefts, changes in valuable data or files, deleting systems or any files, or it disable hardware. Therefore, an early detection and prevention mechanism is very important for the security of the computer. Antivirus software is a critical link in overall security chain, protecting organization's computers from many types of viruses, including worms and Trojan horses. Using Antivirus software is a good way to detect viruses and it is advisable to use Antivirus software on network operating systems and workstations for adequate protection. Antivirus software is specifically written to defend a system against the threats that malware presents. Antivirus software may work differently and ranges from large security packages to small programs designed to handle a specific virus. [2] The large number of Antivirus software available in the market and some are being launched, each one of them offers new features for detecting and eradicating viruses and malware. Therefore people have a choice of different types of Antivirus i.e. both in the form of freeware software or licensed software. People frequently change their Antivirus software according to their liking and needs without evaluating the performance and capabilities of the various Antivirus software available. Hence there is a need to find concepts of computer viruses with detailed types of it because if you know the exact viruses' types then you find the exact solution on that computer virus.[3] Computer Virus In august 1981, the first IBM personal computer was introduced for small group of people. Now today huge numbers of interconnected networks are used for communication and exchange information around the world. Then internet came and its magnitude of places to stuffs, button to click and email to send, it began to grow into a dangerous environment for unsuspecting computer users. Email provided a speedy method for a virus to propagate and consume new host. [4] A computer virus becomes series problem for people. The researcher is going to write research about these problems. First what is a computer virus? [4][5]

VIRUS stands for-Vital Information Resources under Siege. As defined A computer virus is a self-replicating program containing code that explicitly copies itself and that can 'infect' other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus. It is a set of instructions that manipulate the functions of your computer's operating system. 'Virus' is actually a generic term for software that is harmful to your system. They spread via disks, or via a network, or via services such as email. Irrespective of how the virus travels, its purpose is to use or damage the resources of your computer. The first viruses were spread as part of computer programs, or by hiding in floppy disks. Most modern viruses are spread by Internet services, in particular email. 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. [6][12]

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. [7][13]

II. 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 points are describes in each stage. [8][9]

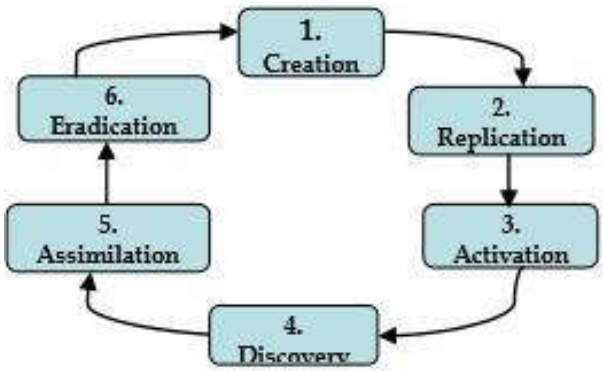


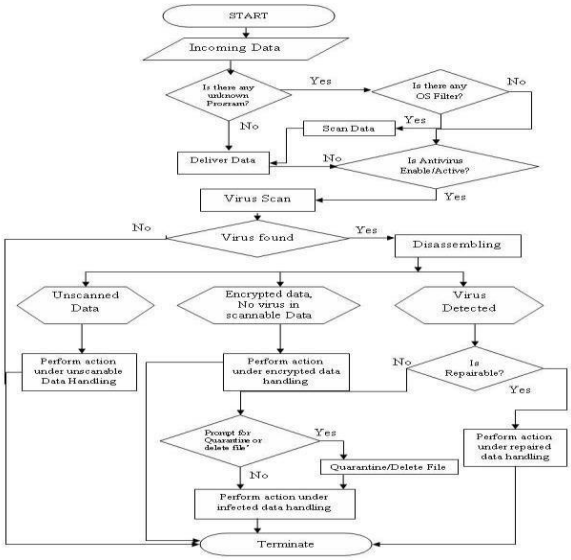
Figure 1: Life cycle of computer virus

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 I V -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. Viruses can not disappear completely, but some have long ceased to be a major threat.
Classification of Computer Virus Now a day's numbers of computer viruses are created. Computer viruses are just a type of malicious software called Malware. Malware are designed to infiltrate damage and/or prevent the normal use of a computer system.

They are commonly divided into number of classes, depending on the way in which it is introduced into the target system and the sort of policy breach which it is intended to cause. As it is hard to define malware in a proper way, it can also be difficult to classify malware into distinct categories. Malware is constantly evolving and is also combining different ideas and techniques. For the purpose of this guide, a payload is a collective term for the actions that a malware attack performs on the computer once it has been infected.

III. Antivirus protection software
Antivirus software can defend you against viruses, Trojans, worms and – depending on the product – spyware and other types of malware. Most people know that Antivirus software is a necessity and most computers come with some form of Antivirus program already installed. Antivirus software uses a scanner to identify programs that are, or may be, malicious. Scanners can detect; Known



Viruses, previously unknown viruses, suspicious files. This type of software can detect and block viruses before they have a chance to cause any harm. A good Antivirus program can scan for viruses on your hard drive or any program, files, or documents. If it finds any viruses, it can remove the virus, quarantine it or delete the file safely from your computer. To be affective, your Antivirus protection software needs to be updated regularly, preferably automatically. Detection of known viruses depends on frequentupdating with the latest virus identities. [11]

IV. The benchmarking model for an ideal antivirus software
Figure II: Benchmark Model for Ideal Antivirus Software
Basically, in any Antivirus software, the scanning process should start with accepting data for virus scanning. At this step, user must be given an interface to select the data for scanning. This selected data will be termed as 'Incoming Data' from this step onwards, by the Antivirus software. [15]

Now, after accepting data for scanning, at first instance, the software will check whether there are any unknown programs submitted for virus scanning. If Any, Then Antivirus software will check, whether there are any Operating System filters components/files submitted as a part of incoming data. If there is no such unknown program found, then the control of scanning process will move to the next step, i.e. Deliver data.

If any operating system filter found, then the researcher suggests having a provision for specific scanning of such components of operating system. As operating system is an interface between user and computer, there is a need of specific virus scanning of such data items. In absence of such operating system components, the data will be sent to the next step of scanning process. [10][15]

At the next instance, there is need for checking whether status of Antivirus software is 'disable' or 'enable'. If disable, then there should be a provision for making it 'enable'. If it is in 'enable' state, then virus scanning process will start.

As a part of virus scanning process, each data component submitted for virus scanning, will be scanned to check whether it is infected by any kind of virus attack, such as malware, Trojan, adware, spyware, boat, etc. Each Antivirus package contains its own virus definition, which must be updated regularly.

Normally there are two outcomes of virus scanning process, 'virus found' and 'virus not found'. In case of 'virus not found', then it will display the scanning process summary along with a message of 'No virus found'. Hereby the scanning process will be terminated.

In case of 'virus found', next step in the scanning process is 'disassembling'. In disassembling process, all infected files will be classified into three categories, a) files infected with virus, b) Encrypted data, in which no virus in scanable data c) completely unscanned data. For infected files, it will check whether the file is repairable or not. If yes, then perform action under repaired data handling and display the scanning process summary and process will be terminated. If infected files are not repairable, then Antivirus software should ask the user to quarantine or delete the infected file. Based on the user response, perform quarantine or delete action on infected files, display process summary and process will be terminated. If user does select 'quarantine' or 'delete' option, then Antivirus software will perform action under infected data handling, display process summary and process will terminate. For encrypted data, in which no virus found in scanable data, perform action under encrypted data handling, display process summary and process will terminate.

For 'Unscanned data', perform action under unscannable data handling, display process summary and process will be terminated.

V. 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 Antivirus 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. Also there are number of antivirus software for different types of users like total security, internet security, personal antivirus etc. These types of antivirus software working same but all antivirus vendors are giving same mechanism for virus scanning with different features. This benchmark model gives ideal types of antivirus software with colleting all features. With the help of this benchmarking model all Antivirus vendors developed product for all types of users.

VI. 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.

VII. References

[1]. Paul Mobbs, Computer Viruses, Association for Progressive Communications, March 2002.
[2]. Jacob M. Rutledge, Research report Virus, 2010.
[3]. Chuck Hauge, Anatomy of Computer Viruses CPH Solutions 2006.
[4]. Paul, Sophos Plc, Computer Virus Demystified. PDF, ISBN 0-9538336-0-7.
[5]. Thomas M. Chen, Trends in Viruses and Worms, The Internet Protocol Journal, 23-33.
[6]. Kiran Karki, Malik H Muzaffar, Virus and Antivirus.
[7]. Francesco Gennai, Marina Buzzi, Computer viruses and electronic mail.
[8]. Matt Bishop, An overview of computer virus in research environment, Technical Report PHC- TR91 156.
[9]. Robin Sharp, An Introduction to Malware, Spring 2011.
[10]. Pele Li, Mehdi Salour, And Xiao Su, San, A Survey Of Internetworm Detection And Containment, Ieee Communications, The Electronic Magazine Of Orig inal Peer-Reviewed Survey Articles, 1st Quarter 2008, Volume 10, No. 1.
[11]. Bharath Madhusudan, John Lockwood Design of a System for Real-Time Worm Detection, Applied Research Laboratory, 2005.
[12]. Ruiqi Hu and Aloysius K. Mok, Detecting Unknown Massive Mailing Viruses Using Proactive Methods, UTCS Technical Report RTS-TR-04-0, 2004.
[13]. Lap Fan Lam, E-mail Viruses Detection: Detect Email virus by network traffic, Thesis in TCC402, 2002.
[14]. Protecting Your Computer and Your Identity, Security Awareness, Office of Enterprise Security Dept. of Information Technology, 2007.
[15]. K. Lai, D. Wren, T. Rowling, Consumer Antivirus Performance Benchmarks