ISSN: 2278-3369

International Journal of Advances in Management and Economics
Available online at: **www.managementjournal.info**

REVIEW ARTICLE

Computer Virus and Antivirus Software –A Brief Review

Bhaskar V. Patil*, Rahul J. Jadhav

Bharati Vidyapeeth University Yashwantrao Mohite institute of Management, Karad (M.S.), India.

*Corresponding Author: Email: ***bhaskarpatil28381@yahoo.co.in***

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 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. The large number of Anti-virus 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 Anti-virus software according to their liking and needs without evaluating the performance and capabilities of the various Anti-virus software available. This research paper highlights the basix concepts of computer viruses and antivirus software. And also describe the details types of computer malware or miclinious code and working of anti-virus software.

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

Interoduction

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. Anti-virus software is a critical link in overall security chain, protecting organization's computers from many types of viruses, including worms and Trojan horses. Using Anti-virus software is a good way to detect viruses and it is advisable to use Anti-virus software on network operating systems and workstations for adequate protection. Anti-virus software is specifically written to defend a system against the threats that malware presents. Anti-virus software may work differently and ranges from large security packages to small programs designed to handle a specific virus. [2]

The large number of Anti-virus 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 Anti-virus i.e. both in the form of freeware software or licensed software. People frequently change their Anti-virus software according to their liking and needs without evaluating the performance and capabilities of the various Anti-virus software available. Hence there is a need to find concepets 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 danger-

ous 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? [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. [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. [15]

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. [10]

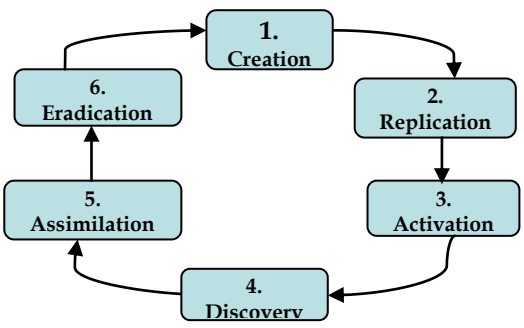

Figure 1: Life cycle of computer virus

- **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 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, Anti-virus 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.

Typically, each virus will only infect one type of target - though some security analysts believe that future viruses will be capable of affecting more than one type of target. To get an overview over the malware-field a classification of the different types of malware would be of great help. The malicious code are mainly classified in to five main category which are namely as virus, worms, Trojan or Trojan horse, Obfuscation Technique based virus. Each main category of malicious code

is classified in different sub categories which are shown in bellow figure. Figure 2 classification of malicious code. [14-16]

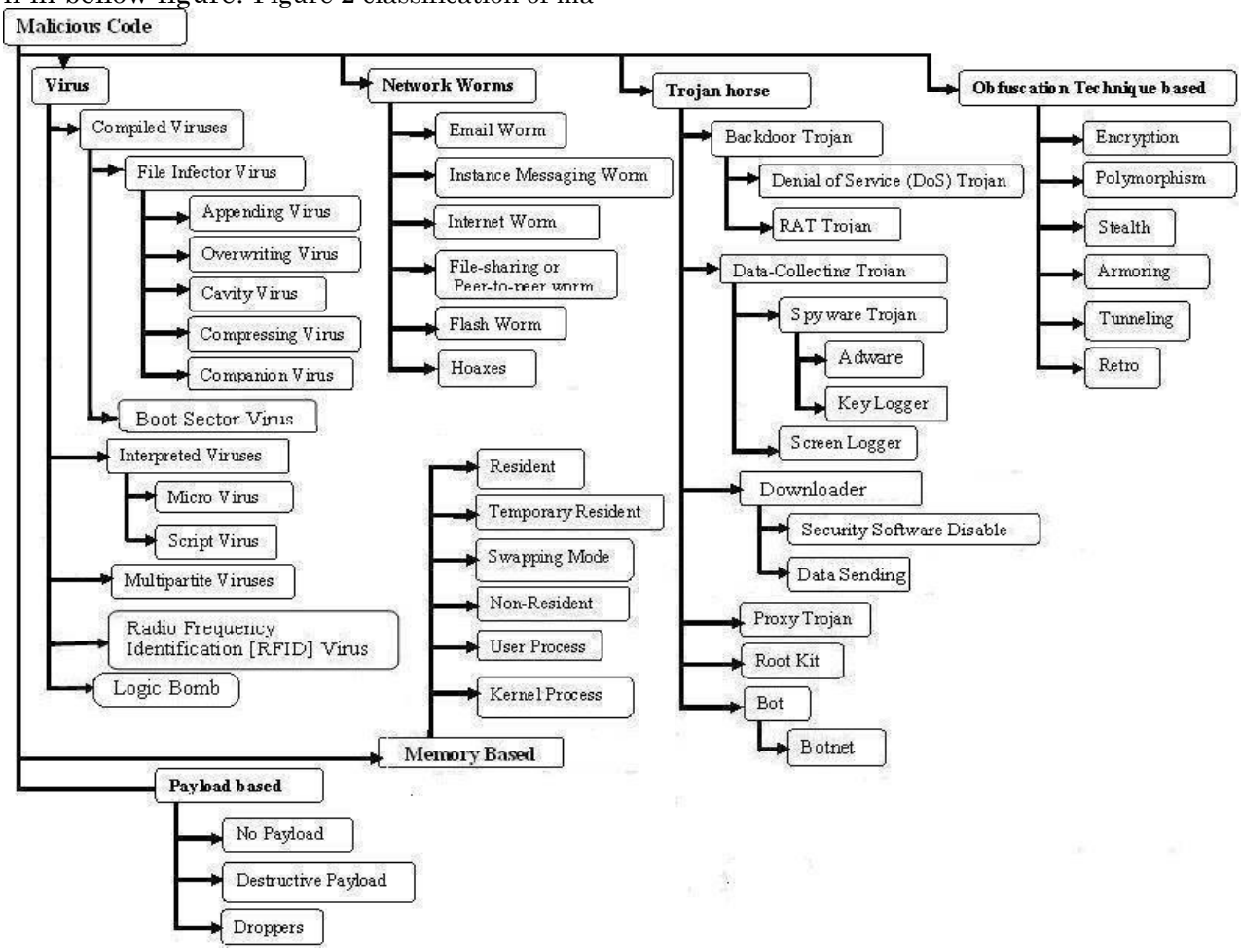

Figure 2: Classification of malicious code

Main Objective of Anti-Virus

Anti-virus is a program code which is used to capture or notify the malicious code and performs some certain functions according to the description written by the programmers. The main objective behind the viral protection programs is to secure the system using these 3 tasks; [1][6]

- Take preventive measure
- Detection of the malicious code
- Eradication

To perform these tasks this Anti-virus software uses many resources from the computer system, so the ideal situation is to perform the aforementioned tasks without putting extra loads on the processing unit modules.

Working of Anti-Virus Software

The use of computers and Internet are increasing day by day for different purposes with more and more users. At the same time these computers and networks are facing number of problems posed by malicious codes like virus, Trojan, etc.

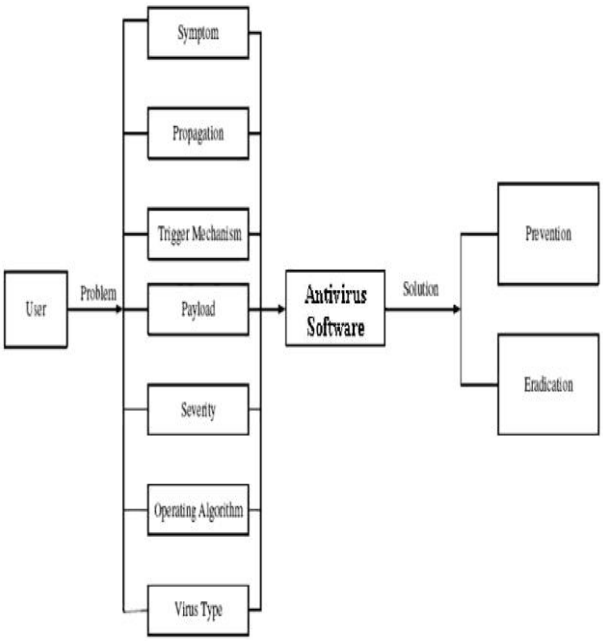

Figure 3: Prevention from different attack

The problems which are shown in the above figure which are Symptoms, Propagation, Trigger Mechanism, Payload, Security, operating algorithm. These different problems are analyzed by Anti-virus software programs, which provide solutions for prevention and eradication of computer viruses.

Conclusions

Now a day's computers are very essential part of our life. In today's world of extreme competition on the business front, information exchange and efficient communication is the need of the day. The internet is the highway that connects you to millions of computer together globally, forming networks in which any computer can communicate with any other computer as long as they are both connected to internet. This fantastic world of computers and their worldwide network has been replete with incidences of malicious attacks of a virus created by people who get the thrills of spotting loopholes and making an entry into others computer systems. '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 history of worst computer virus attacks dates back to 1998 and since then the world of computers has witnessed several computer attacks which were shocking in their times. Now (since 2010 onwards) computer attacks are not shocking any more, the world of computers has learnt to take into its stride computer attacks and has also learnt to deal with malware. Viruses are classified as Compiled virus, Boot Sector Virus, Interpreted Virus, Multipartite Virus, and Radio Frequency Identification [RFID] Virus. There are different computer viruses and their variants that are created and they find their way into other computers through networks and media. But there is some mechanism to find particular viruses and their categories.

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. 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 Original 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 E-mail 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. Robin Wielputz, Evolution! From Creeper to Storm, Seminar on Malware, Bonn-Aachen International Center for Information Technology, 2007.
16. Konrad Rieck, Thorsten Holz, Carsten Willems, Patrick D¨ussel, and Pavel Laskov, Learning and Classification of Malware Behavior, PASCAL EPrints, 2008.