Vol 6 Issue 2 March 2016

ISSN No : 2230-7850

International Multidisciplinary Research Journal

Indian Streams Research Journal

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.org

Indian Streams Research Journal
International Recognized Multidisciplinary Research Journal
ISSN: 2230-7850 Impact Factor : 4.1625(UIF) Volume - 6 | Issue - 2 | March - 2016

TECHNICAL REVIEW ON COMPUTER VIRUS ATTACK, WORMS AND PREVENTIVE METHODS IN PC USERS

Shyamunder Abuj
Research Scholar, JJT University , Rajasthan, India.

ABSTRACT :

Computer virus is a program that can propagate (replicate) its own copy to other non-malicious program by modifying them without user permission. It is name so because it acts like virus that infects healthy program and antivirus is a program use to detect these viruses to protect the good program form virus. Antivirus tries to remove virus's code and restore original program. An antivirus uses various methods for detecting viruses. As characteristics of different viruses are dif rent there detection method are also different. All type of viruses cannot be detected by any single method. This paper describes what is virus how it is affect the good program and review current methods of virus detection and describe problem facing by current antivirus.

KEYWORD: Worm, FAT, boot sector, virus.

INTRODUCTION:

This research paper targets to find the factors which leads the virus attacks among personal computer users. Today's society has seen a dramatic increase in the use of computers. As a result users of personal computer today need to have comprehensive virus protection mechanisms to face the growing threats of computer viruses. Virus attacks on computer are more harmful that shows up more damage to the computer. It is important to analyze the actions that a virus performs in one's system and also the activities that are possible to occur over time. This helps in protecting our PC with needful security mechanisms to safeguard the secure information. The purpose of this research paper is to introduce to the reader the threats that the computer viruses can create and provide guidelines on how individuals can protect themselves against these viruses. Nowadays many computer viruses are designed to self-replicate and self-install over a very short period of time. They come encoded with specific instructions to destroy and advance through its host computer, and can affect a multitude of programs and applications very quickly. Recognizing the symptoms of a computer virus can help to successfully remove it from the infected computer as quickly as possible; the sooner this is completed, the easier it will be to recover any documents or programs that may be damaged, and prevent the virus from further spreading. After identification of typical factors which leads to computer virus attacks the possible solutions are put forwarded to PC users to surmount this virus attacks and for their future improvement in computer usage.

2 TYPES AND WAYS OF COMPUTER VIRUS ATTACKS

2.1 Boot Sector Virus: These types of viruses effect on the disk and the hard drive that holds small section referred as the sectors. Once the boot sector is attacked they become infected when you reboot the system with the infected diskette it spreads through the hard drive.

2.2 Multipartite viruses: It is a form of hybrid boot sector program virus that affects the programming files. While the infected program is activated it hits the boot record. When the system is restarted it subsequently passes on the infection to other local drive in to computer scattering on the virus to the other programming files instantly.

2.3 Macro viruses: infects a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. A typical effect is the undesired insertion of some comic text at certain points when writing a line.

2.4 Stealth viruses: Have the characteristic of hiding and usually changes file sizes to escape detection. A virus with stealth attributes tends to be found in a boot sector or a program file. Stealth viruses cover their trails by two techniques. The first is to redirect disk reads to other locations and the second technique is making a change in boot tables.

2.5 Program Virus: The program virus is kept hidden in the files or documents, once they are activated or called they start infecting the system by copying the virus to other files and replicating to the system.

2.6 Polymorphic Virus: The Polymorphic virus behaves like a chameleon that changes its virus signature frequently once they get multiplied and ready to affect the next new-fangled file. It is also referred to as binary pattern.

2.7 FAT virus: It is a computer virus which attacks the file allocation table (FAT), a system used in Microsoft products and some other types of computer systems to access the information stored on a computer.

3. LITERATUR REVIEW

John aycock and ken barker (2004), stated that the secure environment in which to work with

computer viruses .This paper introduced the goal of to establish a computer security standard for secure laboratories analogous to that of biohazard laboratories.

Henry & at all (2012), described that the corporate viruses are a major problem which costs business of dollars every year. This paper contains the impact of the computer viruses and work attacks on institutions and industries.

D.Krihna & Arun (2006), proposed that the new feature selection measure, class wise document frequency an n grams computer virus detection. This paper used SVM, decision tree an IBK .The n grams approach lacks semantic awareness because of this it is very difficult to analyze the relevant n grams that we obtain. Abdellatif Berkat(2011),proposed that the n method for detecting computer viruses that is based on the technique of case based reasoning. This detects the ne viruses as well as updating viruses automatically.

Nitesh kumar et.al. (2012), has proposed that developed the metamorphic engine producing morphed copies of the base virus that are highly dissimilar and included some opcode of the normal program. This proves that even with high metamorphism HMM is able to identify common statistical pattern across all morphed copies and their base virus.HMM has prove very difficult to detect.

Hassan Wahshat & et.al (2012), has proposed that described that viruses seems to be the only alive organism in the computer environment and another main goal is survival. This is complex crypting- decrypting engine which is standard for the computer viruses.

Tharam S. Dillon, et al. (2006), has proposed that Decentralized transactions are progressively coming to be prevalent. These transactions look like the early types of the web and from numerous points of view are viewed as the following era of the web. The outcome will be that these e-business transactions approaches will movement to shared correspondences instead of customer the earth. Then again, these distributed interchanges or decentralized transactions experience the ill effects of a few inconveniences, which incorporate the danger connected with every transaction. This paper keeps tabs on the variables that impact Risk in a decentralized transaction.

4. OBJECTIVES

These should be identified on the basis of the problem analysis. That means, after reading the problem analysis it should be immediately clear that the choice of objectives is relevant and justified. The objectives should focus on concepts and problems mentioned in the problem analysis. This research proposal should contain one overall objective describing the general contribution that the research project makes to the subject area as well as one or more specific objectives focusing on discrete tasks that will be achieved during the research. The overall objective may be something that the study will contribute towards but not solve/finish; the overall objective should not be a compilation of the specific objectives. While your problem formulation serves to describe the aim of your thesis, the objectives provide an accurate description of the specific actions you will take in order to reach this aim. As with the problem formulation, the overall objective should be framed in a single sentence,

Objectives are summarized as follow,

1 To study the computer viruses.
2 To Differentiate between front-door and back-door attacks.
3 To study different symptoms of viruses.
4 To identify the reasons which cause virus attacks among the personal computer users.
5 To learn how computer viruses and other malware attack computer systems.
6 To Gain strategies for preventing both types of attacks.

7 To think critically about what computer viruses are capable of doing and the effects of Computer viruses on our society.

5. METHODOLOGIES

Research methodology defines how the development work should be carried out in the form of research activity. Research methodology can be understand as a tool that is used to investigate some area, for which data is collected, analyzed and on the basis of the analysis conclusions are drawn. There are three types of research i.e. quantitative, qualitative and mixed approach.

5.1 Steps in conducting a research

The researcher used questionnaire as a research tool to collect data. 110 questionnaires were issued among university undergraduates, professionals and PC users to collect the data. Among the respondent only 100 respondent's data were considered for the analysis purpose. This sample has been taken from University, professionals and PC users on the basis of convenient sampling method. Researcher had the access for collecting data easily from these categories. Research is regularly directed utilizing the hourglass display structure of research. The hourglass demonstrates begins with a wide range for research, Centering in on the needed data through the system for the undertaking then develops the research as talk and results. The questionnaire composed by the researcher by focusing many aspect of computer virus like reasons for Virus attack.

Preventive mechanisms for virus attacks / Suggestions

It is very much conducive to list out the possible Preventive mechanism to safeguard the computer System. These are the general suggestion for personal computer users to protect their computer system. Keep the operating system updated and ensure that the operating system (OS) is up-to-date. Keep anti-virus software installed on your system and update it regularly. Make sure that your software has the latest to fix new viruses, worms, and Trojan horses. Further make Sure the antivirus program has the capability to scan e-mail and files as they are downloaded from the Internet and run full disk scans periodically. In Addition to scanning for viruses on a regular basis, Install an 'on access' scanner and configure it to start automatically each time you boot your system. This will protect your system by checking for viruses each time when computer accesses an Executable file. Install a firewall and keep it enable especially when the computer is connected with the internet. Unfortunately, when battling viruses, worms and Trojans a hardware firewall may be less effective than a software firewall, as it could possibly ignore embedded worms in outgoing e-mails and see this as regular network traffic. Anti-virus programs are not very good at detecting Trojan horse programs, so be careful about opening binary files and Word/Excel documents from unknown or doubtful sources. This includes posts in binary newsgroups, downloads from web/ftp sites that aren't well-known or don't have good reputation, and executable files unexpectedly received as attachments to E-mail or during an on-line chat session. Do regular backups. Some viruses and Trojan horse programs will erase or corrupt files on your hard drive and a recent backup may be the only way to recover your data. Be extremely careful about accepting programs or other files during on-line chat sessions this seems to be one of the more common means that people wind up with virus or Trojan horse problems. If any other family members (especially younger ones) use the computer, make sure they do not know to accept any files while using chat. Further this research addresses the idea and suggestions to prevent the virus attack very extensively. They highlighted the following with respect to installing and updating antivirus (57%), not using pen drive / USB devices (22), do not open unwanted mails / unsecured sites (13%) and do not

install malicious programs (8%) are the best preventive mechanisms to reduce the virus attacks.

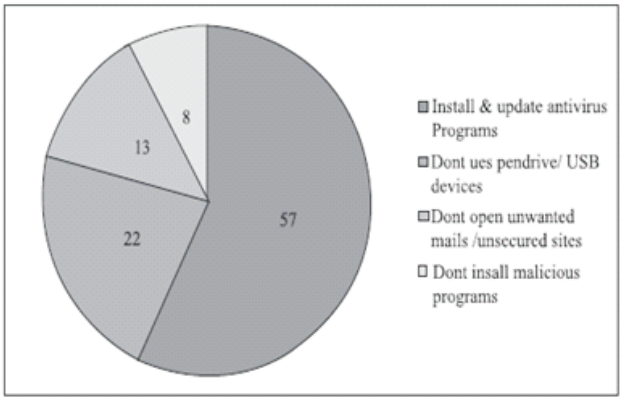

Figure 1: Best Mechanisms For Virus

6.SCOPE AND LIMITATION AND CONCLUSION

Viruses and worms will continue to be an enormous network security problem and New technologies are needed in Early detection, Dynamic quarantining, Intrusion-tolerant networks. There are hundreds of antivirus products but two to be the best: Bit defender's and Kaspersky labs. Bit defender is very strong because it is a combination of signature-based detection, analytic detection, and behavior detection. Products from avast, avira, Eset, F secure, BullGuard, G Data are also perform well.

Detection Methods have some major problems. Most of technique is good against known viruses and not very good against unknown or new viruses. Secondly, they tend to take a much more amount of time to scan a system for viruses. Thirdly, a scanner or its virus pattern database must be updated very often to remain effective. In virus detection technique like anomaly base technique it is difficult to detect virus which behave normally. Viruses can attack files and specific disk sectors. Additionally, invaders can enter the System through various means including disk swapping, email, or file transfers. This research is focusing solely at detecting file infections. A design goal is to modularize detector agents so that they could easily be extended in the future for the scanning of other input sources. The study helps all students, users to gain more knowledge in the computer viruses and troubleshooting some basic parts of the viruses in computer systems like hard disk, folders as well as the system errors and failures. Furthermore, the information serves as the aid to be able to enhance the computer skills of the all users. Etc. The focus of the study is to analyze different viruses, antivirus system for computer hardware. Moreover, it provides recorded information, video tutorial ad user guides in resolving computer problems. These projects provide more importance knowledge for the students in case of viruses, antivirus this project does not cater all the users and students that are not related to computer studies. The study is only limited wherein the topic are selected for the requirement that tackles only the basics computer repair and troubleshooting the memory viruses, folders viruses etc. there are some possibilities that some of the topics covered are not perfectly detailed and efficient. It does not guarantee ach user have to complete information about the virus. The study aims to help and provide a reliable, efficient and beneficial online user, students.

REFERENCES

1.Abdellatif Berkat(2011),"Using case based reasoning for detection computer virus, international journal of computer science ,Vol.No.8,Page No.606-610.

2.John aycock and ken barker (2004),"creating a secure computer virus laboratory", EICAR 2004 conference CD-ROM, Vol.No.2, Page No.1-13
3.A.Coulthard and T.A. Vuori (2002),"Computer Viruses: a quantitative analysis Logistics Information Management", Vol.No.15, Page No.400- 409.
4.Babak Bashari Rad, Maslin Masromand Suhaimi Ibrahim (2011), "Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey", IJCSI International Journal of Computer Science Issues, Vol. 8, Page No.12-18.
5.D.Krishna Sandeep Reddy and Arun K Pujari(2006),"N- gram analysis for computer detection", Springer journal of computer virol,Vol.No.2,Page No.231-239.
6.Frederick B. Cohen and Sanjay Mishra (2011) "Experiments on the Impact of Computer Viruses on Modern Computer Networks", International journal of computer viruses, Vol.No.3, Page No.12-17.
7.Henry ,Godfrd and Alexander(2012),"the economic impact of computer virus-a case of Ghana", journal of emerging trend in computing and information sciences,Vol.No.3,Page No.1235-1239
8.Hassan Wahshat,Yasir Khallil & Takialdin Al Smadi(2007)," computer virus, survey study", International journal of computer science and networking security,Vol.No.7,Page No.308-310.
9.Nitesh kumar dixit, lokesh misha, mahendra singh charan and bhabsh kumar dey (2012)," The new g of computer virus and their detection", International journal of net Yang D., Culture matters to multinationals' intellectual property businesses Journal of World Business, Vol. No. 3, Page No. 281-301.
10.Amara N., Landry R., Traorè N., (2008), "Managing the protection of innovations in
11.Knowledge-intensive business services ", Research Policy, Vol.No.9, Page No.1530-1547.
12.Tafti M.H.A.,(2005), "Risks factors associated with offshore IT outsourcing", Industrial Management & Data Systems, Vol.No.5, Page No. 549-560.
13.Joan C. Hubbard, and Karen A. Forcht (2010), "Computer viruses: how companies can protect their systems", Industrial Management & Data Systems, MCB University Press work security & its application, Vol.No.4, Page No.79-96.
14.Essam Al Daoud1, Iqbal H. Jebril and Belal Zaqaibeh (2008), "Computer Virus Strategies and Detection Methods", Int. J. Open Problems Compt. Math., Vol. 1, Page No. 2.
15.Peltier T., Edison D., (1996), "The Risk of Allowing Outside Staff Access to Your Information System", Information Security Technical Report, Vol. No. 3, Page No.18-28.
16.Pai A. K. & Basu S.,(2007), "Offshore technology outsourcing: overview of management and legal issues", Business Process Management Journal, Vol.No. 1, Page No. 21- 46
17.Spinello R.A.(2007), "Intellectual property rights", Library Hi Tech, Vol. No. 1, Page No.10-22.

Publish Research Article
International Level Multidisciplinary Research Journal
For All Subjects

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication,you will be pleased to know that our journals are

Associated and Indexed,India

- International Scientific Journal Consortium
- OPEN J-GATE

Associated and Indexed,USA

- Google Scholar
- EBSCO
- DOAJ
- Index Copernicus
- Publication Index
- Academic Journal Database
- Contemporary Research Index
- Academic Paper Databse
- Digital Journals Database
- Current Index to Scholarly Journals
- Elite Scientific Journal Archive
- Directory Of Academic Resources
- Scholar Journal Index
- Recent Science Index
- Scientific Resources Database
- Directory Of Research Journal Indexing

Indian Streams Research Journal
258/34 Raviwar Peth Solapur-413005,Maharashtra
Contact-9595359435
E-Mail-ayisrj@yahoo.in/ayisrj2011@gmail.com
Website : www.isrj.org