The Impact of Computer Virus

1 author:

Aboobucker Ilmudeen
South Eastern University of Sri Lanka
56 PUBLICATIONS   **404** CITATIONS

Some of the authors of this publication are also working on these related projects:

Project   7th International Symposium 2017 (IntSym2017)- SEUSL - 07th & 08th December 2017 View project

— A. Ilmudeen[1] —

The Impact of Computer Virus Attacks and Its Preventive Mechanisms among Personal Computer (PC) Users

(1) MIS Unit, Department of Accountancy & Finance, Faculty of Management and Commerce, South Eastern University of Sri Lanka, Oluvil, Sri Lanka.(e-mail: ilmudeen16@gmail.com)

Abstract: The purpose of the research is to explore the impact of computer virus attack and provide guidelines on how individuals can protect their personal computer (PC) against virus attacks. It is important to address the virus attacks and its preventive mechanisms among the personal computer users in this electronic global world. After identification of typical factors which leads to computer virus attacks the possible solutions are put forwarded to personal computer users to surmount this virus attacks and their future improvement in computer usage.

Key words: virus, attacks, personal computer, preventive mechanisms

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 a 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.

Types and Ways of Computer Virus Attacks

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.

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.

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.

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.

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.

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.

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.

Literature Review

A virus is by definition a computer program that spreads or replicates by copying itself (F-Secure Corporation 2001). Computer virus attacks have become serious worldwide issue and can quickly spread through the Internet, causing even more damages (Joseph Wen 1998). Unlike other threats computer viruses able to infect from program to program, file to file and computer to computer very rapidly without direct human intervention. (Joseph Wen 1998) mentioned in his research that a computer virus can cause the loss or alteration of programs or data, and can compromise their confidentiality. (Joseph Wen 1998) stated that the vital part of a virus is a set of instructions that when executed spreads itself to other unaffected programs or files. Based on the intention of the virus developer these instructions can do any harmful activities like displaying a message, erasing files or altering stored data, replicating itself

and taking up system resources such as disk space , memory, Central Processing Unit (CPU) time and network connections. (Joseph Wen 1998). In general most of the viruses are stay active in memory until we shut down our computer system. But when we turn off the computer we just temporarily remove the virus from memory, but not permanently remove from the file or disk it has infected. The next time when we use the computer system the virus program is activated and starts its vandal activities continuously. Typically there are many well-known techniques can be used by viruses to destruct the computer system. Basically a typical virus make two functions thus first it copies itself into uninfected programs or files, second it executes other malicious instructions the virus developer included in it. (Babak Bashari Rad *et al,* 2011) mentioned in their research that, there is a great fight between virus developer and anti-virus experts and it is becoming more difficult issue in day by day and in future too. (Essam Al Daoud *et al,* 2008*)* mentioned that anti-virus softwares are advancing their methods and techniques to detect viruses, on the other hand the virus developers are looking for new tactics to break them. Specially computer virus developers apply many strategies to escape from the detection such as space filling, compressing and encryption. On the other hand the antivirus softwares are trying to detect the viruses by using alternative static and dynamic methods. In general PC users today need to have a fully-fledged virus protection mechanisms to face the growing threat of virus attacks.

Some of the Warnings of Virus Infected Computer

The virus infected computer shows the followings symptoms such as computer performance slowed down and it takes a long time to start, it gets restarted frequently on itself, it displays more prompt messages with unusual errors and collapse of operations and strange sounds or music plays from speakers unexpectedly, failure in application functionality to meet up to the mark, crushed data that are change in format and difficult to reopen, files and documents do not get opened at times with error or unknown file formats, email account automatically send messages with the virus to our contacts, the command CTRL+ALT+DEL no longer works, antivirus no longer update, receives an e-mail message that has a strange

attachment, an anti-virus program is disabled for no reason and it cannot be restarted, the computer may not allow re-installation of the anti-virus, new icons that you did not place on the desktop appears, a program disappears from the computer without uninstallation, operating system does not start because certain critical system files are missing, receive error messages listing those files, programs that used to run now stop responding frequently, and a partition completely disappears....etc

Statement of the Problem & Research Question

Researcher conducted an preliminary interview among the Personal Computer (PC) users with regard to their computer usage and its interruption. People are using computers for several purposes like internet surfing, social media, e-commerce, e-learning, preparing documents, entertainment...etc. It is notable that most of the personal computer users are using internet based activities and it has high possibility to virus infection from the internet. Researcher's interview revealed that computer virus attacks are occur in numerous ways due to the user's lack of knowledge about virus infection, unprotected system, antivirus not installed ...etc. Research question is raised as "what are the reasons for computer virus attacks and what possible preventive mechanisms to safeguard the personal computer user's system.

Objectives of the Research

As people increasingly use Internet technology as a way to connect with globe the possibility of acquiring computer virus is greater. Computer viruses have become an ongoing worldwide problem and can travel quickly through the Internet and causing even more destruction. Individuals today need to have a comprehensive virus protection policy to face the growing threat of these old and new viruses. Objectives of this research are:

• Identify the reasons which cause virus attacks among the personal computer users.

• Suggest the possible preventive mechanism to safeguard their computer resources from virus attacks.

Methodology

Data Collection

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. The questionnaire composed by the researcher by focusing many aspect of computer virus like reasons for virus attack, virus infection damages in PC, possible symptoms in an infected PC, type of antivirus production, preventive mechanism for virus infection....etc.

Data presentation and analysis

The collected data were entered to the SPSS 16.0 and researcher conducted the relevant descriptive analysis. This was made using SPSS.

Results and Discussion

Majority of the respondents replied that viruses have high impact on personal computer usage. From the collected data 68 respondents revealed that their PC infected by virus attack more than 6 times within last three months. From this research the respondents reveal the reasons for PC's virus infections are with respect to using pen drives(43%), not having antivirus(29%), visiting harmful sites(12%), free from antivirus updates(11%), does not have licence version of software(5%) and too much of internet surfing(9%).

Program file infection has been recognized as a serious issue by the PC users and it affected the PC severely. Further hard disk infection, system file infection and boot sector infections also highlighted by the respondents. All respondents indicated that Internet browsing has virus attack and majority of them using the trial version (70%) of antivirus software as a protection mechanism. Among the licence version of antivirus users approximately AVG and Kaspersky
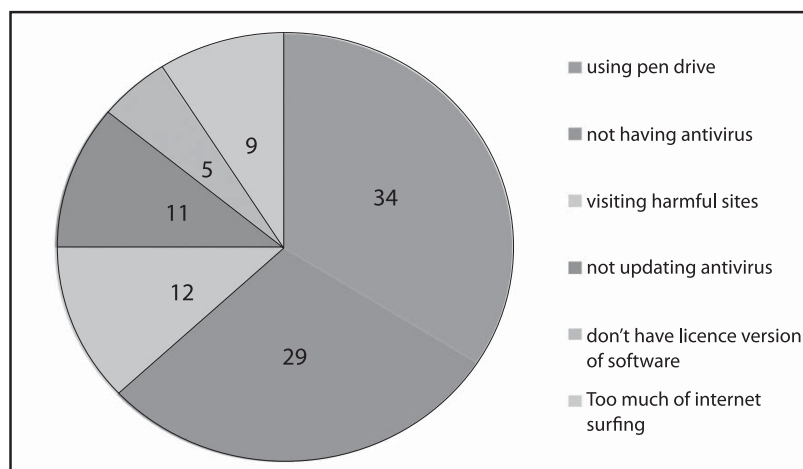
Figure 1 : Reason for virus attack

are the same status and Norton places second antivirus for Srilankan users. When it comes to symptoms recognized when virus infected system slows down in performance (48%) places first place, failure in application functionality and unwanted messages & error messages lays second place (20%). Further as a preventive mechanism for the virus attack most of the respondents (57%) select the best mechanism to protect PC from virus attack installing antivirus & update it frequently and using license version antivirus are the best way to protect the system. 22% of the respondent replied that not using pen drive is also the good mechanism to prevent virus infection to the system.

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
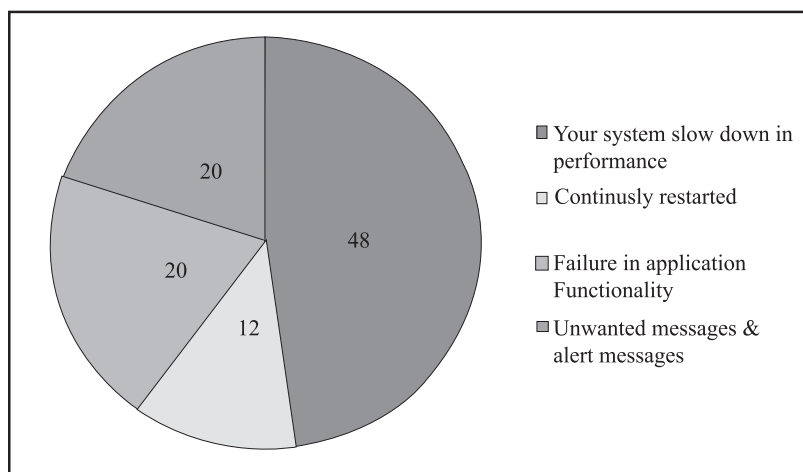

Figure 2 : Symptoms recognized when virus infection

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 specially 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 a

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.
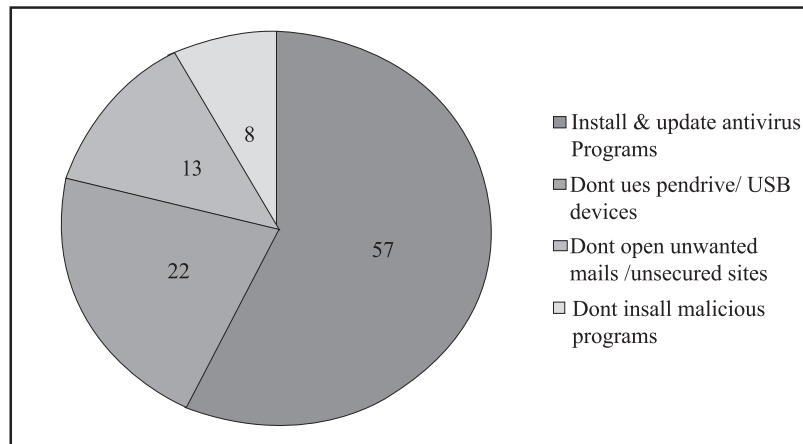

Figure 3: Best Mechanisms For Virus Attacks

Conclusions and Recommendations

All respondents replied that virus attack has high impact on their personal computer usage. This research reveals number of lucrative mechanisms which would help to the personal computer users to protect their computers from the virus attacks. The simplest recommendation for this research is the virus prevention and detection mechanisms. It is the easiest and least expensive ways for the virus attack by practicing such as keep the antivirus program up to date for the latest threats, patching OS loophole, application software loophole and browser loophole frequently, avoid unsafe internet surfing such as visiting doubtful websites, surfing on the cracked websites and downloading from unsafe websites, do not open the mail straight away, preserve it and use checking poisonous software and when receive the suspicious e-mails delete them immediately. By following these safety measures the personal computer users can save valuable resources and their computer system. When a virus is found, it should be addressed immediately to take appropriate action. The PC users revealed the symptoms they felt when their PC infected like the system slows down in performance (48%) places the first place, failure in application

functionality and unwanted messages & error messages (20%) lays second place and system continuously restarted (12%) placed in third place. From this research the respondents revealed the reasons for PC's virus infections are with respect to using pen drives(43%), not having antivirus(29%), visiting harmful sites(12%), free from antivirus updates(11%), do not have licence version of software(5%) and too much of internet surfing(9%). Further this research highlighted installing and updating antivirus (57%), not using pen drive / using 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.

Limitations & future research avenue

This research is only focusing the virus attacks among personal computer users. In this global world business firms are facing high threat due to the virus problem. So business firms are ignored to this research. Researcher permits other researchers to carry out research in this area by eliminating these limitations.

References

A.Coulthard and T.A. Vuori (2002), Computer Viruses : a quantitative analysis *Logistics Information Management*, Volume 15. Number 5/6. 2002. PP.400-409, ISSN 0957 - 6053

Ajayshivaa (2007). *Symptoms of virus attacks* [Online] February 28, 2007. Available from : http://www.astahost.com/info/tiposc-symptoms-virus-attack.html. [Accessed: 20th May 2013]

Babak Bashari Rad, Maslin Masrom and Suhaimi Ibrahim (2011), Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey, *IJCSI International Journal of Computer Science Issues*, Vol. 8, Issue 1

Essam Al Daoud1, Iqbal H. Jebril and Belal Zaqaibeh (2008), Computer Virus Strategies and Detection Methods, *Int. J. Open Problems Compt. Math*., Vol. 1, No. 2,

Frederick B. Cohen and Sanjay Mishra (1992) "*Experiments on the Impact of Computer Viruses on Modern Computer Networks*"

F-Secure Corporation (2001) , "*Computer Viruses – from an Annoyance to a Serious Threat*". White Paper

Joan C. Hubbard, and Karen A. Forcht (1998), Computer viruses: how companies can protect their systems, *Industrial Management & Data Systems*, MCB University Press ISSN 0263-5577

Joseph Wen H (1998), Internet computer virus protection policy, *Journal of Information Management & Computer Security* 6/2 66–71 MCB University Press. ISSN 0968-5227

Kendria (2011). Types of viruses and their effects on your PC [Online] April 7, 2011.Available from : http://techgyo.com/index.php/types-viruses-effects-pc. [Accessed: 22th May 2013]

Isha Singh (2010). 8 Symptoms of Computer Virus [Online] 2010/12/13. Available from: http://hellboundbloggers. com//symptoms-of-computer-virus. [Accessed: 10th May 2013]

Prabhat K. Singh, Arun Lakhotia. (2002), "Analysis and Detection of Computer Viruses and Worms: An Annotated Bibliography". *Center for Advanced Computer Studies University of Louisiana*, V. 37(2)

ShenYanmei and XieHong (2010) *Computer Virus Preventing and Controlling Method Discussion,* Third International Symposium on Electronic Commerce and Security Workshops, *Guangzhou, P. R. China*

Shukor Sanim Bin Mohd Fauzi (2003) *A Study On Computer Viruses Attacks And The Way To Cure Them*. A Thesis Submitted in partial fulfillment of the Requirements of University Technology Mara, for the Degree of B.Sc (Hons) Information System Engineering. Shah Alam

Sujandharan Venkatachalam (2010) *Detecting Undetectable Computer Viruses*, Master's Thesis, A Project Report Presented to the Partial Fulfillment of the Requirements for the Degree Master of Science in Computer Science The Faculty of the Department of Computer Science. San Jose State University

Appendix: Reason for virus attack

		Frequency	Percent	Valid Percent	Cumulative Percent
	using pen drive	34	34.0	34.0	34.0
	not having antivirus	29	29.0	29.0	63.0
	visiting harmful sites	12	12.0	12.0	75.0
	not updating antivirus	11	11.0	11.0	86.0
	don't have licence version of software	5	5.0	5.0	91.0
	Too much of internet surfing	9	9.0	9.0	100.0
	Total	100	100.0	100.0	

Symtom_felt_when_virus_infected					
		Frequency	Percent	Valid Percent	Cumulative Percent
	Your System slow down in performance	48	48.0	48.0	48.0
	Continuously restarted	12	12.0	12.0	60.0
	Failure in application functionality	20	20.0	20.0	80.0
	Unwanted messages & alert messages	20	20.0	20.0	100.0
	Total	100	100.0	100.0	

Best_mechanisms_against_virus_attacks					
		Frequency	Percent	Valid Percent	Cumulative Percent
	Install & update antivirus programs	57	57.0	57.0	57.0
	Don't use pen drive / USB devices	22	22.0	22.0	79.0
	Don't open unwanted mails / unsecured sites	13	13.0	13.0	92.0
	Don't install malicious programs	8	8.0	8.0	100.0
	Total	100	100.0	100.0	