Computer Viruses in India-A Questionnaire Survey

Divya Singhal
Department of Electronics and Communication
M.B.M Engineering College
Jodhpur(342003),India

ABSTRACT

One of the big challenges in India in confronting computer viruses is to educate users effectively. This paper presents the results of a questionnaire survey, carried out in India in 2014 specifically in Jodhpur(Raj),India investigating the knowledge of people and attitudes towards computer viruses and virus protection and addressing the problems faced by users. Out of 127 questionnaires distributed through online and hard copies, to the people who used computers in daily life, a total of 96 respondents had taken part in answering the questionnaires. The main aims of this analysis was to examine the computer virus awareness among users in Jodhpur(Raj), India and the impact computer viruses has caused. The result of a questionnaire analysis shows that the viruses have a big impact to the users especially when they were unable to perform their daily routine work .The study also shows that users have just an average knowledge of computer viruses so we enlightened them about various symptoms and prevention techniques of virus attacks. The study also educates them about basic requirements of good antivirus software.

Keywords- computer virus, awareness, antivirus

1. INTRODUCTION

A COMPUTER VIRUS is a malware, when executed, try to replicate itself into other executable code; when it succeeds, the code is said to be infected. The infected code, when run, can infect new code in turn. The self-replication into existing executable code is the key defining characteristic of virus.[3]So it is a program that can copy itself and infect a computer without permission or knowledge of the user.[1]Computer viruses have become real threats for computer users in the past few years However, only a few researchers have tried to map out how great the problem actually is. [2]

In comparison of early 90's where the number of known computer viruses was about 1,000 to 2,300 viruses, today this number is escalated to more than 1,00,000. Studies and researches show that a computer connected to the Internet may experience an attack every 39 seconds. In order to handle a computer virus incident properly, this area needs an in-depth research. [2]

Several important aspects of computer viruses problem should be first acknowledged and later followed by an in-depth research in order to understand the actual problems. Hundreds of different PC viruses are written every day, and their numbers are increasing rapidly. Summarized from article [7], human factors contributed to the security breach and dissemination of malicious code. In spite of the latest technological improvements, it was human or user, who plays roles in interacting and configuring devices or programs which contributes to the dissemination of malicious code.

The new exposed problems are fixed by the software vendors who provide patches and updates for the system. In the mean time, hackers take advantage of this situation as malicious programs are installed on user machines which steal secret data and provide it to unauthorized person for financial and other types of gains.

The contaminated machines can also be made a part of a huge botnets which are groups of computers infected with malicious code and unknowingly controlled by a malicious master. These systems can be used to launch Denial of Service attacks on servers, or be used in an attempt to intrude the computers of government agencies.[3]

Unfortunately, our current ability to defend against new viruses is extremely poor and the basic approach of detection, characterization, and containment has not changed significantly over the last five years. The complexity of modern malware is making this problem more difficult.

2. METHOD

This questionnaire analysis was conducted to determine the respondents' experience, knowledge, and suggestion on the matter related to virus problem. The analysis on the virus impact on computer users were conducted in the Jodhpur (Raj), India and ninety-six (96) respondents from various professions, from different background and gender were involved in this questionnaire analysis. All the participants were aged from 16 or over and had access to the Internet, with over 90% of them going online every day.

The survey analyzed the respondents 'opinions towards virus spread and antivirus issues, how virus affected their daily operation, how they get to know about virus, how they react to virus incident or outbreak and the usage of anti-virus software, the damage computer viruses have caused and opinion towards having a system that is capable to help them in handling virus incident. The questionnaire was distributed through online and hard copies. Both experienced and novice computer users took part in the survey. The survey was based on voluntary participation open to people of all professions.

3. RESULT

Based on survey conducted the results can be summarized as following-

1) The first question gathered the information of respondents' experiences facing the virus problem. Majority of the respondents had experienced virus problems and it affected their daily work routine. Further analysis shows that viruses have infected 94 percent of the respondents and 6 percent have never being infected yet during their experience with computers.

2) Most of the respondents that had encountered virus threats were monthly attacked by virus. Shockingly 12 percent do not realize when they faced virus problems. The actual figure is shown in Figure 1.
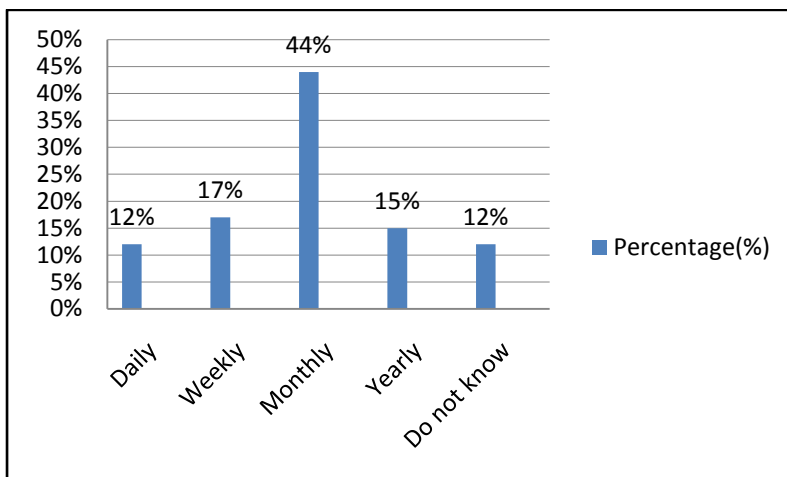

Figure 1: The Frequency of Occurrence of Virus threat

3) Majority of the respondents i.e. 32 percent verify that because of virus problems they are unable to open files or folders and 18 percent are unable to do their daily work. Specifically, the details of impacts caused by virus activities are shown Figure2.
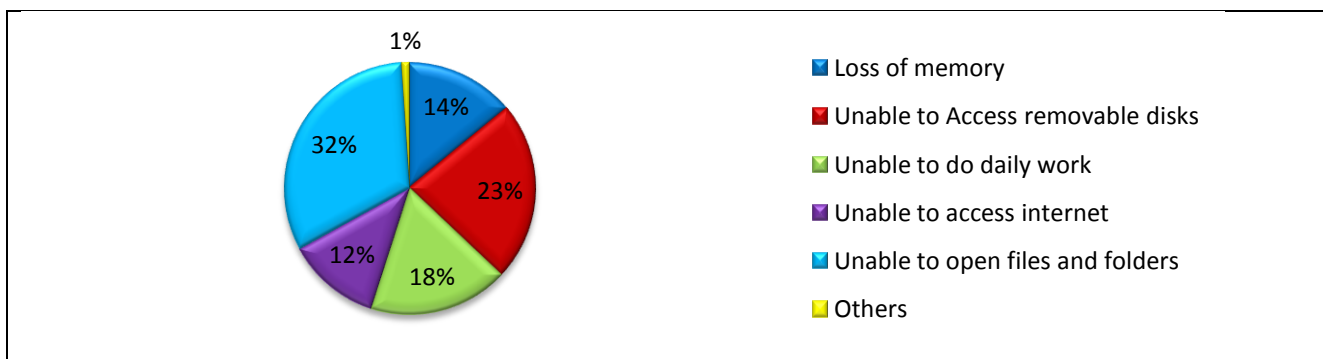

Figure 2: Effects of Virus Activities

4) The forth question was asked to study respondents actions in eradicating the virus problems. Majority of the respondents prefer to solve the virus problems themselves and succeeded doing it.. The details can be viewed on Figure 3.The virus problems have been solved successfully by a majority of the respondents. While the others failed to solve the virus problems themselves. This is a huge figure, associating the effect of virus might cause to the loss of money in the business environment due to the lack of productivity and unavailability to conduct business or business transactions online.
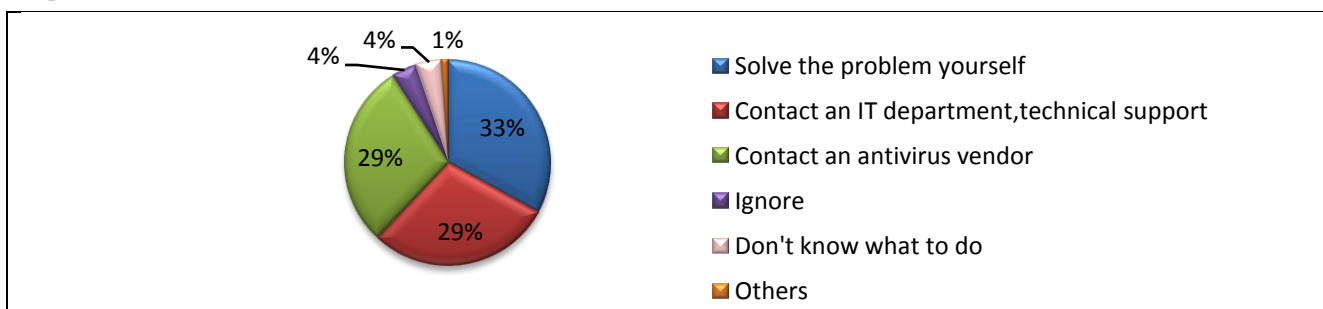

Figure 3: Method used to Solve Virus Problem

5) The next question was asked to analyze the respondent's awareness towards the antivirus functionality and capabilities. Majority of the respondents had knowledge and understanding of the antivirus and were confident that their antivirus software was capable to clean viruses found on their machine. It was found out that most of the respondents have antivirus software installed on their machine. Only 4 percent of the respondents did not install the antivirus software. However, 96 percent of the respondents had anti-virus software. This indicates the importance of antivirus software's to prevent virus attacks. The statistics are shown in Figure 4.
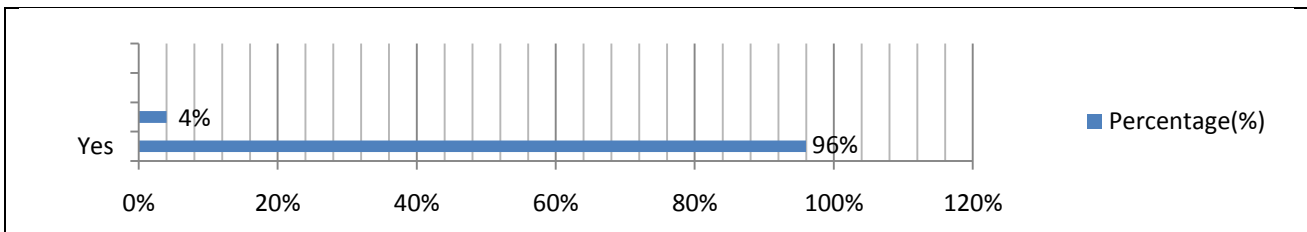
Figure 4: Percentage of people having antivirus installed

6) The next question was asked about the money they spend on antivirus software's. Maximum people (36%) were spending between Rs500-1000 annually on their antivirus software's and 32% of respondents where downloading it free from internet.
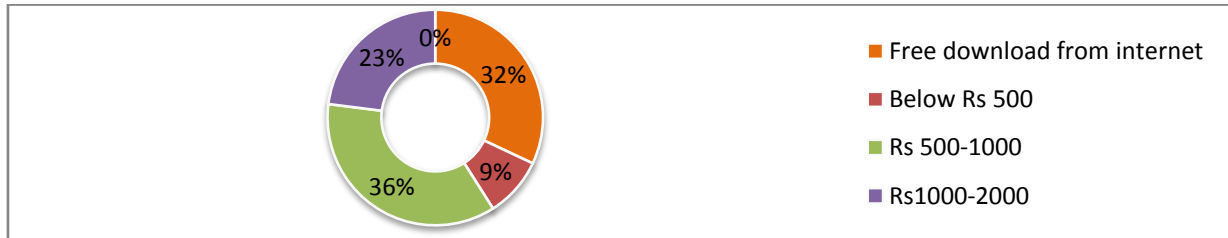

Figure 5: Amount spend on antivirus software's annually

7) When the respondents were asked how frequently they updated their antivirus software's and the results found were an eye-opener as maximum of the respondents updated their antivirus monthly, while 5% never updated them.
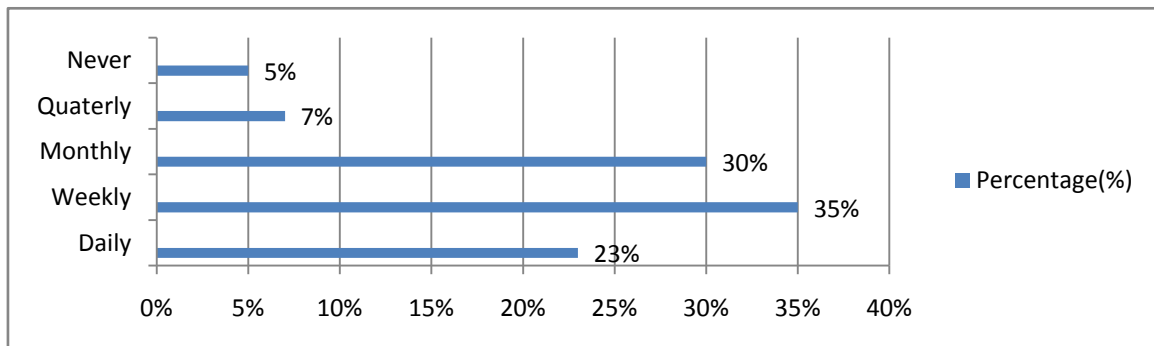

Figure 6: Frequency of updating antivirus software

8) The next question was about their satisfaction with the antivirus software they are using. Majority of the respondents were satisfied with their organizations role for prevention and eradication of virus. 68% were satisfied by the protection offered by the antivirus software. Though, 16% were not satisfied with the protection offered by their antivirus.
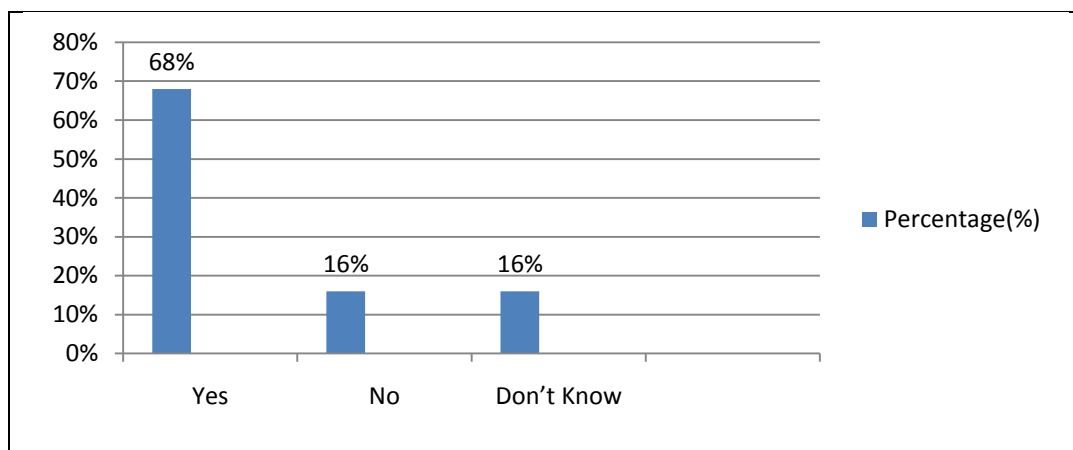

Figure 7: Satisfaction of people by virus protection offered by antivirus.

9) The next category was to analyze respondent's media channel of receiving the virus information. Maximum of the respondents received information from various websites while 14% received it from different sources like friends, teachers etc.
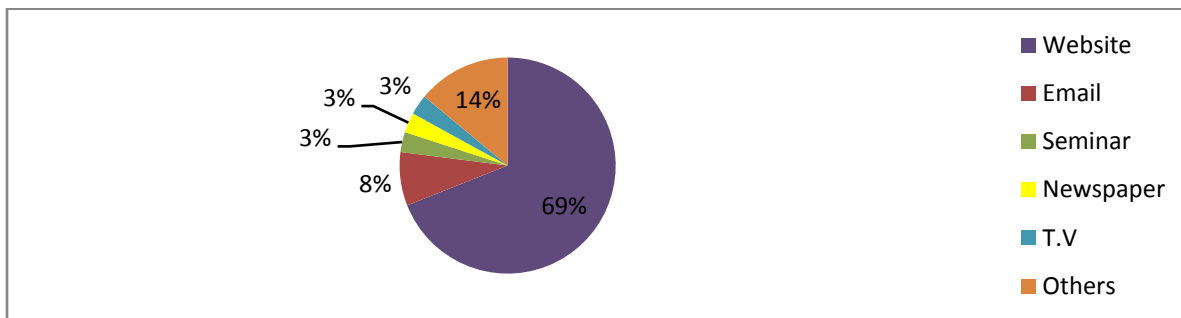

Figure 8: Source of Information on Virus

10) Of all these, 64% percent of the respondents do take the information on viruses seriously. Majority of the respondents stated the information they received about viruses would prepare them against viruses' spreads and equipped them with the latest status of virus. And they are being kept up to date with the virus pattern.
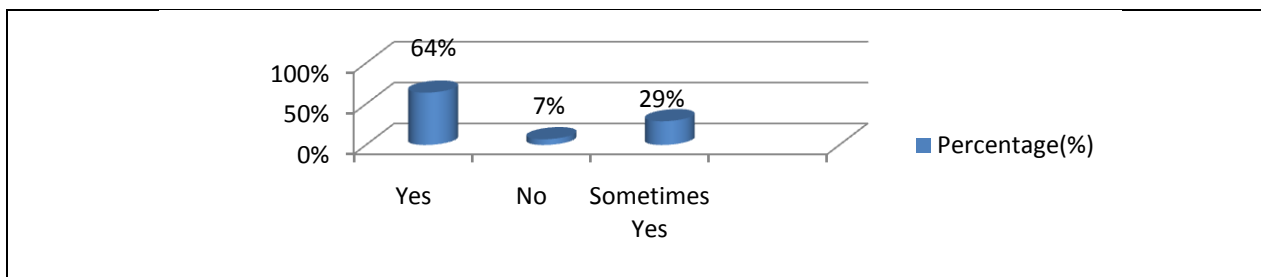

Figure 9: Percentage of respondents taking information seriously

11) Respondents were then requested to rank their own level of knowledge regarding viruses. Average level of knowledge is highly ranked and followed by good level of knowledge. These 2 groups contribute to the major of the respondent's level of knowledge.

The small differences between these 2 groups indicate the need to educate the respondents about viruses, which is one of the objectives for this research. Only minority (3% percent) of the respondents has a very good knowledge about viruses.

Table 1: Knowledge level regarding viruses

Knowledge level	Percentage (%)
Very Good	3%
Good	31%
Average	51%
Poor	15%

12) The final questions were asked to identify that if people were interested to have a system that is capable of providing them knowledge of viruses and antivirus.

As the outcome, it was found out that 98percent of the respondents were very much interested to have a system that is capable to help them when encountering virus incident.
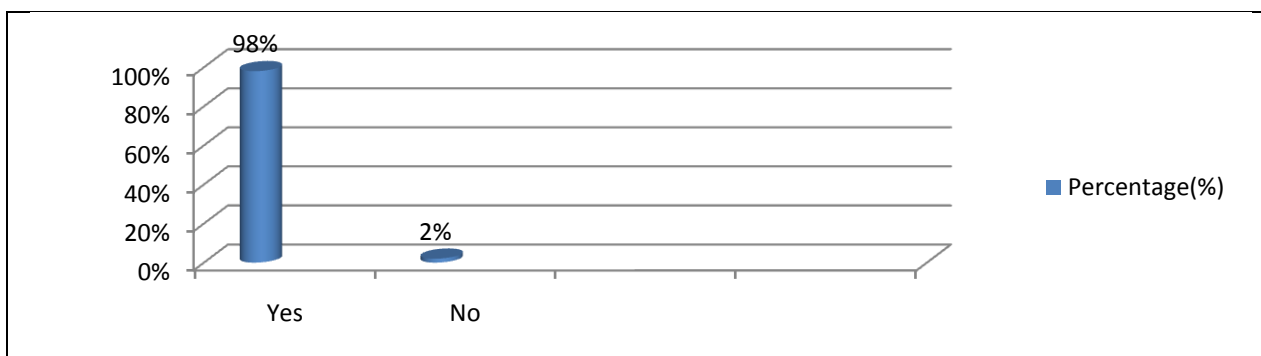

Figure10: Percentage of respondents interested to gain knowledge about virus and antivirus

4. COMPARING WITH OTHER SURVEYS

Based on the survey conducted by Madihah Saudi [2] in Malaysia maximum of their respondents had a good knowledge of viruses which is different than this survey where maximum had just an average knowledge of viruses. According to the survey done by Computer Crime and Security Survey 2005 which was conducted at Australia [9]and CSI/FBI 2005 Computer Crime and Security Survey which was conducted at United States of America [10],majority of the respondents agreed that the virus impact caused loss of money which is totally different with this report where maximum of respondents were unable to access files and folders due to virus attack. The similarity between Computer Crime and Security Survey 2005 which was conducted at Australia [9] and CSI/FBI 2005 Computer Crime and Security Survey which was conducted at United States of America [10] and this paper, is that all surveys showed an agreement that anti-virus is used as defense methods of combating viruses with 96 percent, 99 percent and 96 percent respectively. The same goes to questionnaire survey conducted by Marko Helenius[11] in Finland , Madihah Saudi [2] in Malaysia and AV- Comparatives IT security survey 2013 [12] where 90 percent of the government organizations , 98 percent and 97 percent of the respondents respectively are using anti-virus program as defensive method. One more similarity between this report and AV- Comparatives IT security survey 2013 [12] is that most of the respondent do not attempt to contact security software manufacturer in event of virus attack.

5. DISCUSSION

5.1 How Virus Gets Into Your Computer?

- You obtain a virus by running an infected program or opening an infected data file. Viruses normally infect program files, which are identifiable by the COM or EXE program extension.

- Some viruses can also infect batch files such as BAT and CMD files. Occasionally, viruses infect data files. Usually affected data files are Microsoft Office files such as Word DOCs and Excel XLS files. MP3 files have also been mentioned as possible virus sources, although few viruses that exploit MP3 files exist.

- Viruses are spread by passing files from one user to another. You can obtain them via e-mail, by downloading files from the Internet, or by sharing files over the network or via removable storage devices such as floppy disks.

- Many viruses infect systems if you download and install an infected program. You can obtain the virus-infected file by downloading it from the Internet, opening an infected e-mail attachment, or using a file-sharing network. You don't always have to open an infected attachment from an e-mail to obtain a virus. Some viruses can infect early versions of Outlook by merely opening an infected e-mail.

- One key way to get a virus, especially a worm, is by not keeping your system patched against the latest security threats. Hackers discover new vulnerabilities in systems, which vendors, such as Microsoft, constantly patch against. Without the latest updates, your system can be vulnerable to old attacks. [4]

5.2 Identifying an Outbreak

- Sometimes viruses will trigger windows to appear and disappear randomly on your system as they do their work. These will be very rapid but may include an odd warning or request for you to click OK.

- Some viruses can create small data files that fill up hard drive space or allow programs to be downloaded to your workstation, turning your workstation into a network server for pirated files or pornography. If you see a sudden decrease in free drive space, you might have a virus.

- Viruses can corrupt or damage data files and programs. This can cause you to lose important data or experience error messages and blue screens on your operating system. These can also be indications of hardware failure, although hardware failure is much less likely on newer systems.

- Your computer crashes more frequently or sometimes your computer may also shutdown automatically this can also be an indication of virus attack.[4]

- Your keyboard doesn't work properly or unexplained printing problems occurs, may be a symptom of virus attack.

5.3 How to Prevent Virus Attack?

- Update your operating system regularly. It blocks security holes that can be exploited by viruses or hackers.

- Update your Anti-Virus. Don't rely on the automatic updates. Open the Anti-Virus program, check when the last update was performed and if necessary check for updates manually. Make sure the program and the virus definitions are both constantly updated.

- Update all Software. Try to keep all your software updated. Every program nowadays has an online connection, which can mean a gateway for spyware adware etc to get in. This is mostly true for browsers. So make sure you have the latest version.

- Don't click on links sent to you by e-mail by an unfamiliar sender as this is a common way for malicious website to hook you in. Instead go to the browser and type in the websites name in directly.

- Avoid Bad websites like adult sites, piracy sites and file sharing sites. Any website where you get a continuous number of pop up pages on any link you press is generally bad and should be avoided.

- Be careful when installing Programs. Always research any programs you wish to install. Do not install a program just because it appears to suit your

needs. If it is a good program there will be many reviews and recommendations.

- Avoid Clicking Popup adverts. If you're careful and you know the website is legitimate then it can be okay, but a lot of the time they're not and are to be avoided. Specifically ones that say they will improve your computer.

- Be Vigilant .If you get a windows pop up that looks like it's scanning your hard drive for viruses or errors, yet you have never seen this program before close it instantly..

- Run Virus cleanup regularly. Most antivirus programs have a scheduler that will schedule a regular scan of your computer. Make sure this is enabled, and check regularly to see if it has been run.[6]

5.4 Which Anti-Virus Program Is Better?

- Reliability and convenience of work - absence of anti-virus "hang ups" and other technical problems, requiring special technical knowledge from a user. Reliability of anti-virus programs is the most important criterion, because even the "absolute anti-virus" may become useless, if it is not able to finish the scanning process and hangs, leaving a portion of your disks and files unchecked, thereby leaving the virus in the system undetected.

- Quality of detection of all major kinds of viruses, scanning inside document files, spreadsheets (Microsoft Word, Excel, Office97), packed and archived files. Absence of false positives. Ability to cure infected objects.

- Availability of anti-virus versions for all the popular platforms (DOS, All windows platform, Novell NetWare, OS/2, Alpha, Linux etc.), not only on-demand scanning, but also scanning on-the-fly capabilities, availability of server versions with possibility for network administration.[5]

- There are hundreds of antivirus products but two to be the best: Bitdefender's and Kaspersky lab's. Bitdefender 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 also perform well.[8]

6. CONCLUSION

Computer viruses have been around almost as long as computers. Computer viruses have dramatically increased in complexity over the years. The purpose of this survey was to know the user knowledge and attitude towards a computer virus. Based on the survey conducted we found that most of the respondents complaint about virus attack and most of them used antivirus software to safeguard their computer. This showed that people were aware about the problems caused by viruses and also the importance of antivirus. The viruses have

a big impact to the users especially when they were unable to perform their daily routine work due to viruses. We also concluded from the survey that male respondents had better knowledge about viruses and used antivirus software's than female respondents. We found that people had average knowledge regarding viruses so we provided them knowledge about various symptoms and prevention techniques of virus attacks, how to know that they have been attacked by virus and which is better antivirus software.

7. ACKNOWLEGDMENTS

8. REFERENCES

[1] Computer Virus Strategies and Detection Methods Essam Al Daoud,, Iqbal H. Jebril2 and Belal Zaqaibeh Int. JOpen Problems Compt. Math., Vol. 1, No. 2, September2008 pg 122- 9)

[2] User Knowledge and Attitude of Computer Viruses inMalaysia Madihah Saudi , Shaharudin Ismail, Muhammad Najib Masdan International Journal Of Learning, Volume 13, Number 8, 2006 Pg 111-122)

[3] Computer Viruses and Challenges for Anti-virus Industry Deepak Kumar , Narender Kumar , Aditya Kumar International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 2 February , 2014 Page No. 3869-3872.

[4] Computer Viruses: How to Avoid Infection http://www.msubillings.edu/cotfaculty/security/al-viruses.pdf pg 1-6)

[5] Behavioral And Performance Analysis Model For Malware Detection Techniques A.Edwinrobert,.Dr.M.Hemalatha International Journal Of Computer Engineering & Technology (Ijcet) Issn 0976 – 6367(Print) Issn 0976 – 6375(Online)Volume 4, Issue 1, January-February(2013),pp.141-151

[6] Bits & PC's 10 Step Guide to Protect Against Viruses (2012,march 4) http://www.bapcs.co.uk/10-step-guide-to-protect-against- viruses

[7] Dancho Danchov. 20 Jul 2004. Reducing "Human Factor" Mistakes. Article in MISC Network Security.(2003,July23)(online)http://www.windowsecurity.com/articles/Reducing_Human_Factor_Mistakes.html

[8] How Anti-virus Software Works?? Sarika Choudhary Ritika Saroha Mrs. Sonal Beniwal International Journal of Advanced Research in Computer Science and Software Engineering (Volume 3, Issue 4, April 2013 ISSN: 2277 128X pg 483-4)

[9] AusCERT, AFP, AHTCC, NSW Police, NT Police, Queensland Police, SA Police, Tasmania Police, WA Police, Victoria Police. 2005. Computer Crime and Security Survey 2005. (online).http://www.auscert.org.au/render.html?it=2001.

[10] Lawrence A. Gordon, Martin P. Loeb,William Lucyshyn and Robert Richardson. 2005. CSI/FBI 2005 computer crime and security survey. (online). www.cpppe.umd.edu/Bookstore/Documents/2005CSI Survey.pdf

[11] Marko Helenius. 1994. Computer Viruses in Finland - A Questionnaire Survey. Master Thesis of Sciences, University of Tampere. (online).http://www.cs.uta.fi/~cshema/public/vru/docume nts/survey.zip.

[12] AV- Comparatives IT security survey2013 (online) http://www.av-comparatives.org/images/docs/security_survey2013_en. pdf