Vol 8. No. 1 – March, 2015
African Journal of Computing & ICT

www.ajocict.net

Users' Perception of the Effects of Viruses on Computer Systems – An Empirical Research

S.S. Oyelere
Department of Computer Science
Modibbo Adama University of Technology
Yola., Adamawa State Nigeria.
E-mail: Solomon.oyelere@mautech.edu.ng

L.S. Oyelere
Windows Click Computers
SMIT Commercial Area
Modibbo Adama University of Technology
Yola., Adamawa State, Nigeria
E-mail: lydialuggu2005@gmail.com.

ABSTRACT

A computer virus is a piece of software which attaches itself to another program causing undesirable effect on the program. It is attached similar to the way in which biological virus affect other organisms. The synonymous way it works with that of the human virus gave rise to the term computer virus. Computer viruses infect personal computers (PCs) and server. Some viruses create mere annoyance, but others can do serious damage: delete or change files, steal important information, load and run unwanted applications, send documents via electronic mail (e-mail) or even cripple a machines operating system (OS). Random sampling technique on respondents was performed while the data used for the study is collected from primary sources using a well-structured questionnaire. Data collected were logically analyzed using descriptive tool such as percentages and charts and inferential statistical tool such as chi-square. Based on the administered questionnaires the result indicated that viruses can infect computer system through a number of ways such as exchange of flash drive, hard disk and network medium.

Keywords: Virus, Antivirus, Computer system, Security, Program

African Journal of Computing & ICT Reference Format:
S.S. Oyelere & L.S. Oyelere (2015). Users' Perception of the Effects of Viruses on Computer Systems – An Empirical Research
Afr J. of Comp & ICTs. Vol 8, No. 1. Pp1-121-130..

I. INTRODUCTION

The importance of virus free computer system cannot be over looked due to many factors surrounding and facilitating system management such as cost of implementing a computer based information system, cost of gathering data, processing it and producing a meaningful information, risk of losing important information and lots more. Viruses therefore constitute a reasonable percentage of various threats that computer based information system faces. In recent time, especially in the early part of 21st century, the word virus was closely associated with the state of health of human beings i.e. the biological virus. Presently the word comes up both in biological and health sciences as well as computer sciences. However, it is distinguished in the computer field as "computer virus". Although its biological counterpart preceded it, it is not less important too. In the field of computer science, its effect cannot be undermined, as it has become a major threat to many computer professionals and users. The rapid development of information technology has undoubtedly brought about the advent of the computer virus. This project work would look into the heart of computer virus infection and prevention.

1.1 What is a computer virus?

A computer virus is a unique type of program that has the ability of self-replicating and it stores a copy of itself in another part of a computer system (usually on hard or floppy disk). According to [1] computer virus are instructions that are hidden within a computer program and are designed to cause faults or destroy data. A computer virus is capable of perpetuating itself with the basic objective of performing certain activities that could range from annoyance to serious vandalism. This means that the virus will try to replicate itself and carry out certain operations without letting the computer user even know of its ability to be inconspicuous in its existence.

Also the activities of any virus in its existence depend on the imagination, skill and knowledge of its author [2]. In some cases, however, a virus is referred to as a program which exploits loopholes in the way the computer perform its various operations. The target is usually the computer operating system - which manages computer resources. The operating system performs file management, processor management, and device memory and information management.

This shows that attacking the operating system, virus has attacked every part of the computer at large. Computer viruses have a lot of similarities with their biological counterpart and basic similarities arise even from their definitions. A biological virus is a submicroscopic organism that invades living cells and reproduces only within the living cell. Most precisely, they are defined as obligate intracellular parasite containing either DNA or RNA (the hereditary material) and they cause diseases as a result of their replication assembly and releasing of infectious particles.

From the foregoing both forms of virus require a host for activation and survival. The computer virus requires a 'host' program in order to be activated while its biological counterpart must invade a living cell. The computer virus requires an executable path to penetrate a computer and spread. There is need for a way of protecting a system from infections by making sure that only legitimate, virus-free code is executed. And this is also true for the biological virus, which requires a mode of transmission, which could either be water or air.

Both the computer and biological viruses replicate and spread to other parts within their different host. They also both attempt to do this inconspicuously, providing side effects that are undesired by the host. The computer virus often causes direct harm to the infected system by performing hostile acts such as erasure of files, obliteration of the boot block etc. they are both disseminated. Computer viruses are products of people known as virus authors. These people write and distribute their programs both intentionally and un-intentionally. The programs are written for various reasons as for terrorist action, to demonstrate skills, smartness, and experimentation.

In order to inactivate a virus, it must be captured and analyzed. Analysis involves full disassembly and extraction of hexadecimal pattern for future identification. Virus researchers that produce antivirus products do these.
The biological virus is even more difficult to inactivate and this is because of its host during replication and often it is difficult to find drug that will inactivate the virus without affecting the host [3].

There are various examples of both viruses [4]. The BRAIN, JERUSALEM, MELISSA, TEQUILA, MALTESE, AMOEBA, LEHIGH, VIENNA, I LOVE YOU, KISS ME, TIMER, BRONTOK, are typical examples of the computer virus while some examples of the biological virus are SMALL POX, CHOLERA, POLIOMYELITIS, TUBERCLOSIS, and HIV.

From the foregoing, computer viruses can be characterized as follows;

i. Self-replication
ii. Side effects
iii. Executable path
iv. Disguise

Henceforth, in this research work, the word virus refers to the computer virus and all references to the biological viruses will be stated closely.

1.2 Stages of virus infection

The existence of a computer virus typically encompasses four stages. That is to say this class of programs differs from the conventional computer programs in four aspects namely [5]:

a. Dormancy
b. propagation or replication
c. Trigger
d. Damage

Upon infecting a new machine or a new program, the virus may remain dormant to avert suspicion. A virus penetrates a computer system when it is executed and running a contaminated program does this. The duration of dormancy varies with the type of the virus. While some awaits a certain number of executions of the host program, others await a certain period of time of elapse; yet some others watch out for a date in the year before delivering the payload i.e. before it is triggered.

When a computer system becomes infected, it now starts to replicate itself. A virus may be a fast infector or a slow infector. A fast infector spreads rapidly within a computer by infecting everything that is accessible. If a fast infector is in memory, every file that is opened gets infected. On the other hand, a slow infector does the opposite. The logic is that, if it spreads slowly, it is less likely to be noticed and killed. A classic slow infector aims to deceive a change detector as an antivirus measure. It therefore infects only those files that are intended to be changed.

As the system becomes infected and the virus self-replicates, most viruses try to determine whether they have infected an executable file by testing for some infection signature or virus maker. When an uninfected program is detected, the virus infects it by copying itself to the file. Therefore when an infected program is executed, the virus code receives control and performs the work appropriate for the stage that it is in. it then returns control to the host program to carry out its normal operations. In this way, the virus can hide its existence all the way through to the triggering stage. The triggering stage is the stage in which the payload is executed. It triggers the side effects of the virus. It is at this stage that the user usually notices that his PC is infected. The triggering damage done by viruses can be categorized into different groups according to the severity of the damage.

Computer virus poses a serious ache to any computing installation. However, it is important to emphasize at this stage that computer viruses are not alone in the menace on the computer system. Other common forms are Trojan horse, logic bombs, and worms. There are bound to be more active virus writers and there will also be a continuous development and improved sophistication in virus writing. Therefore an understanding of the various techniques will enhance the production of antivirus software that will successfully combat the survival of viruses. As in most situations in life, prevention in the case of viruses remains the best options for protection. Common preventive measures include scanning of the newly acquired software, scanning the disks, frequent backups, cold booting the system when a storage occurrence is noticed.

The problem at hand deals with issues pertaining to computer system information security. Computer virus still seems to be infancy stage in developing African countries despite the fact that some measures have been taken on the control of viruses by introducing anti-viruses. Based on the above facts there is need to study the effect of virus on a computer system and its tremendous impacts.

This research work intends to plough out some basic facts about the computer virus and its effect on computer system. However, the objectives of this research work are;

i. To demonstrate the effect of computer virus
ii. To enlighten computer users on what attract the virus to the computer system
iii. To also enlighten computer users on how to control the effect of computer viruses
iv. To provide a framework for discussing a wider variety of virus related issues.

The very aim of this research work is to provide a security measure against threats facing information technology. The design will benefit the management of any organization, individual users, professional, and enhanced computer system life span.

In other to achieve the objectives of this research work, the following questions are to be considered:

i. Have you ever experienced virus infection before?
ii. Does your system get infected with virus through flash drive or external memory?
iii. Does your computer system get infected with virus anytime you browse in the café?
iv. Do you encounter hardware component failing to function as a result of virus infections?
v. When virus affects your system, does it corrupt the operating system?

2. RELATED LITERATURE

The boot sector code is run whenever you start up the computer with a diskette in drive A as opined in [2], they realized that they could replace this code their own program and that this could be memory resistant program and that it could install a copy of itself on each floppy diskette that it accesses in any drive. The program copied itself, they called it a virus. Today's computer virus was conceived and demonstrated by Fred Cohen in 1983. Worm originated from John Shoch and Jon Hupp when conducting an experiment on mobile software at Xerox PARC in 1979 [6].

According to [7], Franz Suloboda became aware that a virus was being spread in a program called Charlie. He called it the Charlie virus, he made a lot of noise about the virus and badly bitten as a result. At this point, there are two version of the story. Burger claim that he obtained a copy of this virus from Swoboda, but Swoboda denied in any case he obtain a copy and give it to belt FX, who disassemble it (this was the first time anyone had disassemble a virus).

Swoboda include the dissemble in his book after patching out a couple of areas to make it less infecting and changing the normal pay load of Vienna is to cause one file inn eight or reboot the computer (virus patches the first time bytes of the code). Swoboda replace this reboot code write file spaces. The effect was that patches hang the computer instead of rebooting this isn't really an improvement [7].

There is contribution in [8] that in US Cohen had completed his doctoral dissertations which was on computer viruses, Cohen provide that you cannot write a program that can with 100% certainty look at file and decide whether it is a virus, of course no one thought that you could, but make good use of an existing mathematical theorem and earned a doctorate, he also did some experiment he released that a virus on a system and discovered that it traveled further and faster than anyone had expected.

Virus was defined as any binary file that meets the following criteria [9]:

1. It requires direct human intervention in order to spread. Unlike a worm, which spreads automatically, a virus requires a user to download and double-click a binary file, or transfer it using an infected medium, such as a floppy disk
2. It has a payload, which can be destructive behavior (deleting or altering files), or annoying messages left on the screen, or both
3. A virus spreads quickly to all documents in an operating system. A virus never spreads itself to other systems automatically.

In [1], the origin and history of virus was revealed. It was opined that people create viruses. A person has to write the code, test it to make sure it spreads properly and then release the virus. A person also designs the virus's attack phase, whether it's a silly message or destruction of a hard disk.

The differences between computer virus and worms was enumerated [10]. A worm is a computer program that has the ability to copy itself from machine to machine. Worms normally move around and infect other machines through computer networks. Using a network, a worm can expand from a single copy incredibly quickly. For example, the Code Red worm replicated itself over 250,000 times in approximately nine hours on July 19, 2001. A worm usually exploits some sort of security hole in a piece of software or the operating system. For example, the Slammer worm (which caused mayhem in January 2003) exploited a hole in Microsoft's SQL server. Worms used up computer time and network bandwidth when they are replicating, and they often have some sort of evil intent.

There are numerous types of computer viruses some of which are as follows [12];

- Macro virus
- Multipartite virus
- Stealth virus
- Files infected virus
- Cannabin virus
- Boot virus
- Trojan horse virus
- Amercing virus
- Internet virus

Macro virus; written using a simplified macro programming language, these viruses affect Microsoft office applications, such as word and excel and count for about 75 percent of virus found in the world. Multipartite virus; this is a portion of the infected boot files and the boot sector, a double whammy that can re-infect your system dozens of times before it's caught. Polymorphic virus; these are charges code whenever it passes to another machine; in theory these viruses should be more difficult for anti-virus scanners to detect; but in practical they are usually not that well written. Stealth virus; thee destroy the component of the system and recovery from the damage caused these virus is extremely difficult, if not impossible. File infector virus; these are viruses that add code to files that run program so that the virus is activated it spread to another program files.

Cannabin virus; this is the type of virus that infect floppy disk boot record. It means that record that is been store into the floppy disk that contact how your operating system starts when you turn on your computer. A boot sector virus replace the disk original boot sector with its own carrying the virus into the memory once is in the memory, the virus can spread to the disk.

Trojan horse virus; these are program that are not described in their specification. The use run what they think is a legitimate program allowing it to carry out hidden, often harmful infections. For example Tro/Zulu claim the millennium bug but actually over writes the hard disk. Trojan horse is sometimes used as a means of infecting a user with a computer virus.

Amercing virus; this popular viruses infect the exe files only. This means that no access to this files or extensions, when you need it. Internet virus; these are virus which attack any net user immediately. Affect computers when connected to the internet.

2.1 Control of computer virus: computer antivirus

Standard antivirus software normally carryout the detection of viruses, anti-virus arte program designed to detect, clean virus and rehabilitate the damage caused by viruses. There are numbers of anti-virus software available to detect and remove virus from the computer for example virus scan from Dr Solomon, MACFEE, Norton and PC-Cillin, etc. anti-virus software checks the RAM and the files and virus and report it. Each anti-virus software can only detect and clean virus that have been programmed to clean only, most compiler industries making anti-virus software offers periodic upgrade that are equipped to detect and remove the virus that has been since the last upgrade.

The following steps were enumerated to check viruses [11]. Establish routines: Unless organizations and single-users have established internal routines for data handling, the chance for running a virus-free computing environment is not likely to succeed. We have seen that when strategies and routines for data handling are initiated at management level, the organization is less exposed to virus infections. And when they occur, routines make it easier to root out the infected files before they spread.

When people think of anti-virus solutions, they normally think of scanners. Scanners are the most readily available types of anti-virus solution, but they are not the only type. A virus can be detected using either generic methods or specific methods. Generic methods look for virus-like behavior rather than specific viruses. As a result, even new viruses can be detected, and there is little need for frequent updates to the tool that is being used. Because generic methods look for behavior rather than specific viruses, the name of the virus is normally not given. Instead users are simply warned that a virus is likely to be present. Some shy away from this method because it can give false alarms. Examples of generic detection methods are: check summing and integrity checking, heuristics, decoys, behavior blocking.

Specific methods, on the other hand, rely on having prior knowledge of the virus. In this case the tool is able to both detect that the virus is present as well as identify it. As a result, frequent updates to the tool are necessary. Most users like to know what they're "up against" if a virus is found, and the best way to do that is to determine the exact nature of the beast. For this reason, many users prefer this method, but they do not ultimately appreciate how often the tool must be updated. Examples of specific detection methods are: on-demand and scheduled scanning, on-access (real-time) scanning.

3. RESEARCH DESIGN AND CONTEXT

This section presents the description of the research design, area of the study, population of the study, sample size, sampling techniques, instrument for data collection, validity and reliability of instrument, method of data collection, and method of data analysis. The study analyzes the effect of virus on computer system of Modibbo Adama University of Technology (MAUTECH) Yola Adamawa State Nigeria by sampling the opinion of computer literate individuals selected at random. The research study which is based on analyzing the effects of virus in computer system is carried out of some selected number of staff and students of MAUTECH. The sample size for this research is fifty five (55) numbers of respondents which includes student, lecturers and non-academic staff. The sampling technique for this research is carried out randomly such that the respondents cut across the different opinions in the university. The data to be used for this study is collected from the primary source using a well-structured questionnaire. The questionnaire is administered to staff and students of MAUTECH. The questionnaire is supervised by the researcher to determine whether the questionnaires were able to measure what they are supposed to measure. Data collected purposely for this research work is logically analyzed through the use of both descriptive and inferential tools. Descriptive tool such as percentages and tables is utilized while inferential statistical tool such as chi-square is employed.

4. RESULTS

This section covers the presentation and analysis of data collected for the purpose of the study. The results were based on the various data obtained from the use of questionnaires. These findings provide solution to the problems outlined in the statement of the problem of this research work.

Section A: Demographic data

As shown in figure 1, 45% are female while 55% are male, thus indicating that there were more male respondents compared to females.

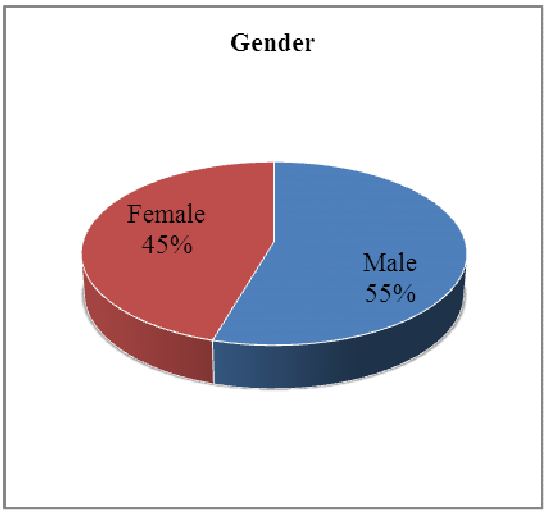

Fig. 1: Gender demographic profile of respondents

This shows that there are more male than female in the university environment. Figure 2 shows the different age groups that participated in the research.

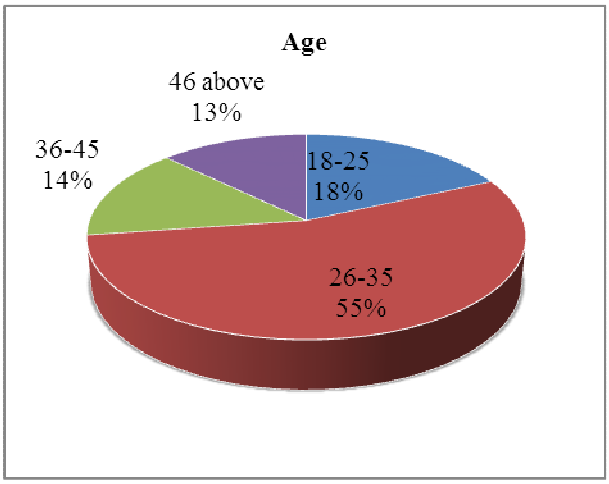

Fig. 2: Age demographic profile of respondents

Majority of the respondents were between 26-35 years old which has 55%. In figure 3, the occupation information of the respondent is presented.

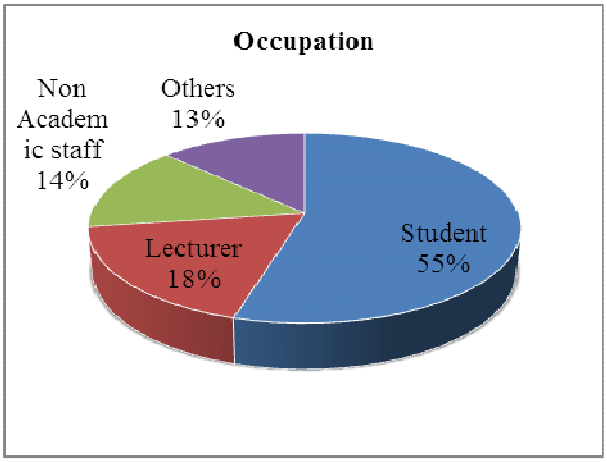

Fig. 3: Occupation profile of respondents

It could be identified that most of the respondents are student while 18% are lecturers, 14% are non-teaching staff. The various educational levels of the respondents are presented in figure 4.

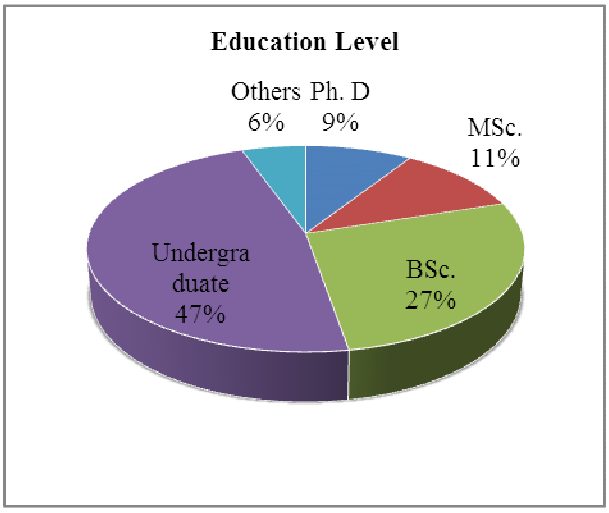

Fig. 4: Education profile of respondents

It can be deduced that most of the respondents are students at undergraduate level. Bachelor degree holders also form a measurable percentage of the respondents.

Section B: Topical questions

The first aspect shows whether computer is use for desktop publishing in the research area as presented in figure 5.

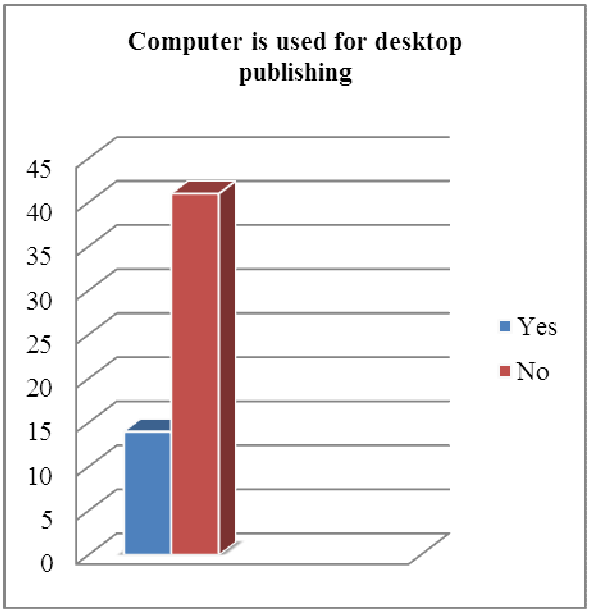

Fig. 5: The use of computers

From figure 5, most of the computers are not used for desktop publishing while few people do use their systems for desktop publishing. This indicates that respondents used their systems for other use. On whether virus infections have been encountered, the result is presented in figure 6.

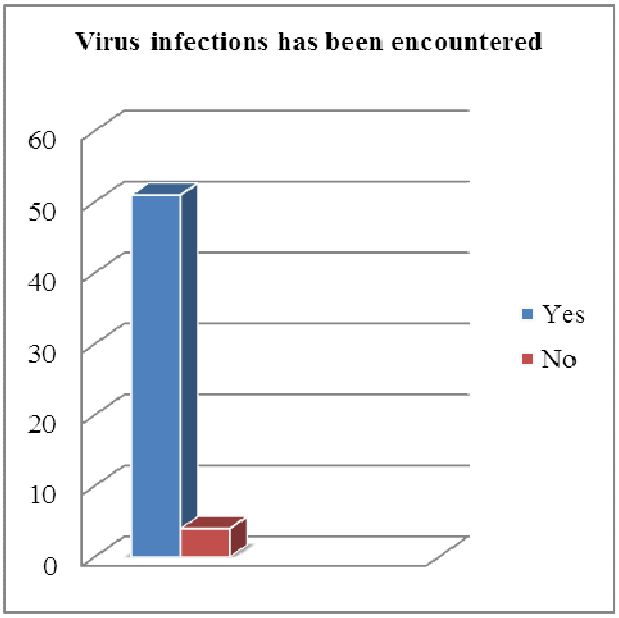

Fig. 6: Virus infections encounter

This shows that most of respondents have experienced virus infections while only few opined otherwise. This implies that virus infections are common. The aspect of finding out whether boot sector, Trojan horse, file infections are normally experienced is presented in figure 7.

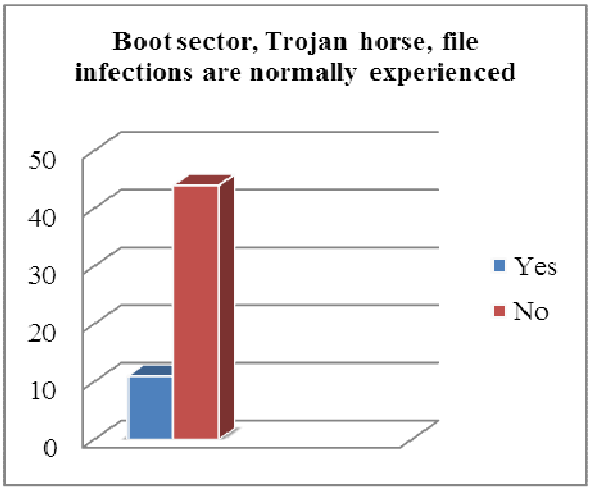

Fig. 7: Experience with boot sector, Trojan horse and file infections

From the analysis of response, only small percentage of the respondents do normally experienced boot sector, Trojan horse, file infection while most of the respondents replied the opposite. This means that most virus infections are not caused by boot sector, Trojan horse, file infection. Figure 8 reveals whether computer systems get infected with virus through flash drive.

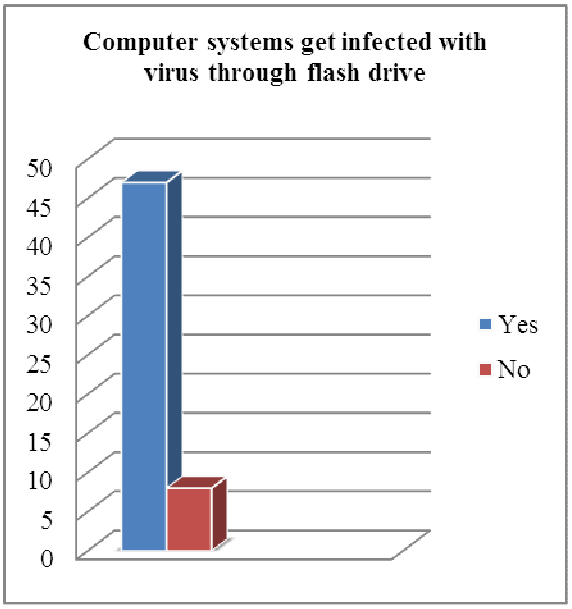

Fig. 8: Experience with virus infection through flash drive

Among the 55 respondents, most are of the view that system get virus through the use of flash drive while only few replied the opposite. This means that flash drive transfer virus to computer systems. Figure 9 shows whether the computer system get virus infections with the use of external memory drive.

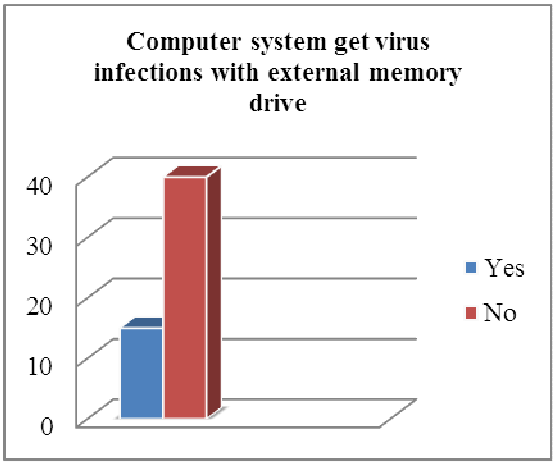

Fig. 9: Experience with virus infection through external memory drive

From figure 9, few of the respondents' computer get virus through external drive while most of the respondents' computer did not get virus through external drive. This means that the use of external drive should be encouraged among computer users. Figure 10 shows whether there is difficulty in booting the system infected with virus.

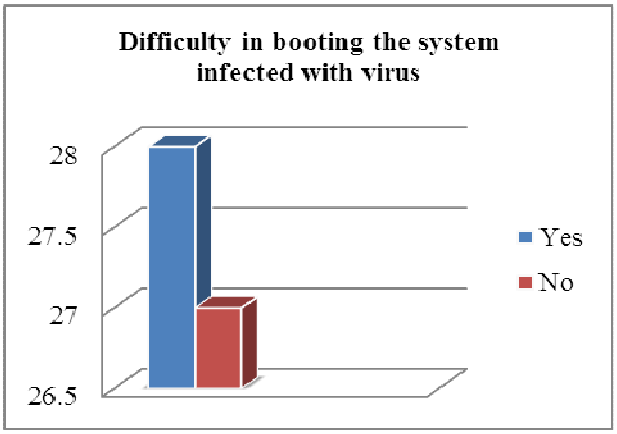

Fig. 10: Difficulty booting virus infected computer system

Most of the respondents stated that there is difficulty in booting system when infected with a virus while only few responded otherwise. This implies that substantial measures should be taken on virus infected system. The next aspect of this research work as presented on figure 11 shows whether hardware component fail to work as a result of virus infection.

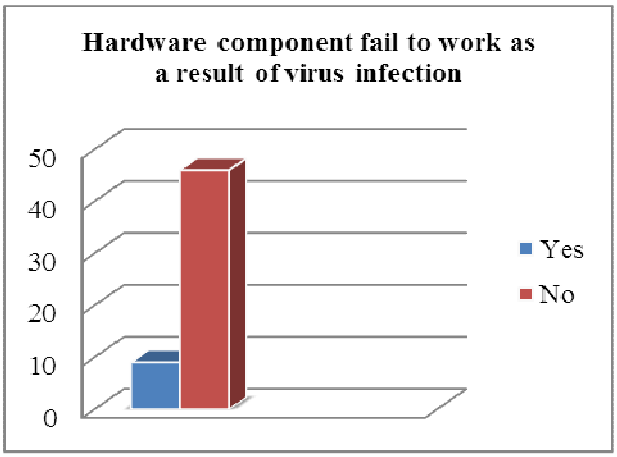

Fig. 11: Hardware component failure on virus infection

Larger populations of the respondents are of the opinion that virus infection does not cause hardware failure while few of the respondents did not share this opinion. This suggests that virus infection do not cause system hardware failure. Figure 12 shows whether virus infection corrupt the operating system.

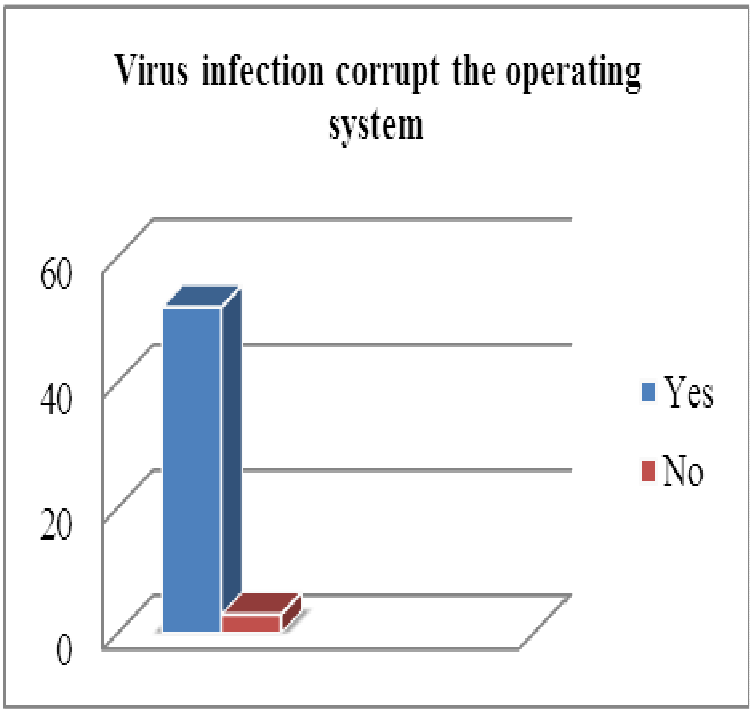

Fig. 12: Virus infection corrupt the operating system

From figure 12, most of the respondents agreed that virus do corrupt the operating system of a computer while few disagreed. Therefore, it means that stronger anti-virus need to be installed on computer system to prevent the operating system from corrupting. Figure 13 reveals whether if sound is heard or unexpected message is displayed on the screen when virus affects the system.

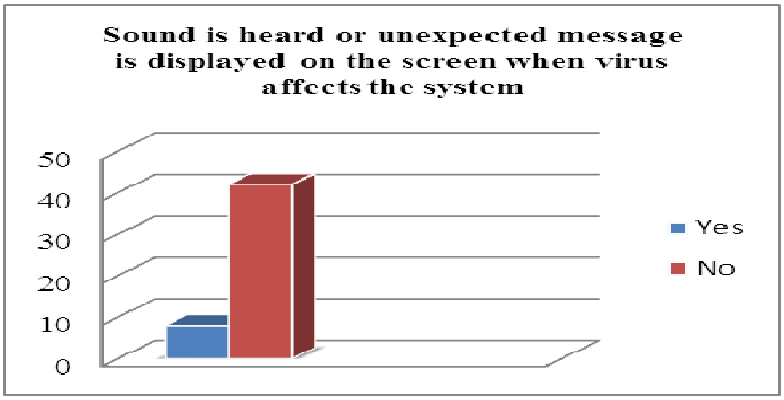

Fig. 13: Sound is heard or unexpected message is displayed on the screen during virus infection

Majority of the respondents are of the opinion that virus infections do not make sound or display unexpected message on the computer screen while a few of the respondents of the opposite. This implies that virus infections show other symptoms other than sound and unexpected messages. Figure 14 shows the response on whether anti-virus terminate virus to an extent.

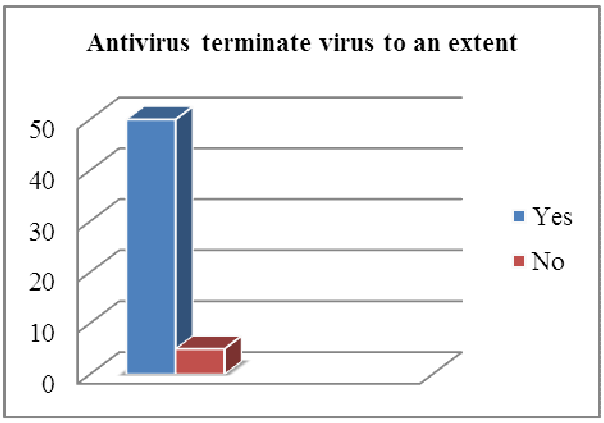

Fig. 14: Antivirus terminate virus to an extent

In the total of 55 respondents, most of the respondents are of the view that any time they run an updated antivirus software on their system it terminate the virus to an extent while few respondents does not share this view. This implies that updated anti-virus software is one of the major remedy to virus infection on computer system.

Hypothesis testing

In order to test the hypothesis stated, the expected frequency is calculated based on the responses of the most relevant questions from the questionnaire and these were compared with the observed frequency using a chi square test with a degree of freedom at 5% level of significance [13].

Decision rule

Reject the null hypothesis H_0 if chi-square calculated is greater than the table value. Otherwise, the attribute hypothesis H_1 alternative is accepted.

Hypothesis one

H_0: System does not get infected with virus through the use of flash drive.

H_1: System gets infected with virus through the use of flash drive.

Since the calculated chi-square is greater than the table value, we therefore reject the null hypothesis (H_0) and accept the alternative hypothesis (H_1) which states that a system get infected with virus through the use of flash drives.

Hypothesis Two

H_0: Virus does not corrupt the operating system

H_i: Virus corrupts the operating system

Since the calculated chi-square is greater than the table value, we therefore reject the null hypothesis (H_0) and accept the alternative hypothesis (H_i) which states that Virus corrupt the operating system.

4.1 Research findings

Following the statistical analysis that was employed, and the responses obtained from questionnaire, it was observed that some of the effect of virus in a computer system includes difficulty in system booting, hardware components fail to function, loss of data and corruption of the operating system. The common kind of virus that affects computers systems are; boot sector, worms, Trojan horse and file infections virus. Furthermore, based on the research findings so far it is discovered that system can be affected with virus through downloading from the internet café, using of flash drive or external memory. However, despite the problems faced by the respondents, they are of the opinion that the presence of antivirus on a system may reduce the extent of damage and the effects of virus possible attack.

5. DISCUSSION

This study is an eye opener to many people who have little or no knowledge about virus and antivirus. The research will correct various misconceptions and provide basic ideas in understanding the subject. This research work has made us to understand that;

i. Viruses are not bugs, dirt, dust, or corrupted programs
ii. Viruses may attack more than one component at a time
iii. Computer viruses problems are not mystical; it is purely the work of somebody somewhere, a code developed by a computer professional.

Some viruses may be powerful than a particular antivirus due to the following reasons:

i. If the antivirus is weak, it has to be upgraded since some virus writers might have weaken the strength of the existing codes of the antivirus by writing more powerful codes that supersede that version of the antivirus
ii. Some antivirus only work for a particular system type and a particular operating system
iii. Some antiviruses are virus specific; they can only identify a particular virus and not all viruses
iv. Biological viruses operate on human beings and the medium of spreading is human body, but computer virus operates on computer systems and the media for spreading it are flash drive, external hard-disks, shared networks, internet files and e-mails, all aimed at destruction.
v. The effects of virus attack on the host computer ranges from loss of information to the destruction of files, folders, hard disk, operating system blocks and start-up programs.
vi. The presence of anti-virus on a system may reduce the extent of damage and the effects of virus possible attack.

6. CONCLUSION

There is certainty that the future will witness the development of more sophisticated codes for viruses. These viruses may be difficult to detect and if detected, could prove stubborn to erase or remove from the computer system. This will no longer be seen as malicious act but as significant impact on the future of computing, knowing well that viruses are legitimate software. It becomes an intellectual challenge to become a virus and antivirus developer. This may in one way or the other limit the growth of information technology due to fear of loss of capital to the users. Many people may prefer to give-up the fate they had on computer system. In order to help people stand the test of time, the researcher has considered this research study as a way of exposing viruses and its characteristics to the wider world. Implementing the recommendation obtained in this study will go a long way to prepare both the computer experts and users for the future war against viruses, which may defile even the use of weapons such as antivirus. Implementing antivirus software might be expensive considering compatibility of some antivirus to the existing hardware and operating system, but the benefits outweigh its cost. Information as a great tool for management decision must be well secured. The following are recommendations: computer user is encouraged to report every virus attack they encounter to computer specialists so as to make materials available for upgrading the existing antivirus and writing new ones; it was carefully observed in the course of this research work, that when users delete a virus from a component, they tend to forget that the virus might have infected one or two other components other than the one seen, thus giving room for the virus to bounce back which (to the user) is caused by inefficiency of the antivirus, but certainly not. The user only needs to make sure that all drives and diskettes are properly scanned at any suspicion.

REFERENCES

[1] Collins, H. 1990. *The Computer Virus Protection Handbook*. Arnold Ltd London.
[2] Solomon, A. and Dmitry, O. 1994. *Dr. Solomon's Virus Encyclopedia*. 3rd Edition. S & S International. Berkhamsted, London.
[3] Gram, J. 1998. *Windows Internet Server 4* (second edition) University of North Carolina.
[4] Jan, A. 1993. *Computer Virus and Antivirus Warfare* (2nd Revised). Hemstend Ellis Horwood.
[5] Kaushik, S. Pang Diwan 1990. *Information Technology* (tenth edition) University of Essex. Associates, 4423
[6] Shoch J. & Hupp J. The 'worm' programs? early experience with a distributed computation. *Communications of ACM*, Volume 25, pp. 172-180, March 1982.
[7] Brien, J. A. O. 1996. *Management Information System* (third edition) University press New York.
[8] John, D. Macfee 1987. *Computer Industry Association Microsoft* (second Edition) academic press New York.
[9] Aryen, G. 1999. *Quick Start Instruction for McAfee Associates Programs*. McAfee.
[10] Snorre, F., Sylvia M., Kenneth, W., and Carl, B. 2003. *The Norman Book on Viruses*. Helsinki Inc. Switzerland.
[11] Solomon and Gyaznor 1984. *Research manual* (third edition) University press New York.
[12] Cheeney Street, Santa Clara, USA.
[13] French, C. S 1996. *Data Processing and Information Technology* (tenth Edition) University of Oxford press Oxford.
[14] S.U. Jen 2002. *Fundamentals of Research Methodology*. 1st Edition. Paraclete Publishers Yola.
[15] Fred Cohen in 1983.