International Journal of Computer Science
and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 6, Issue 4, Jun - Jul 2017; 11 - 20

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

SIDE EFFECTS OF COMPUTER ANTI-VIRUSES

AHMED SALEEM ABBAS

Research Scholar, Department of Software, College of Information Technology,

Babylon University, Babylon, Iraq

ABSTRACT

In this paper, a deep study on computer antiviruses, advantages and disadvantages will be conducted and more focus will be on the side effects of antivirus on overall computer system performance, then end user feedback on the most common antiviruses will be analyzed and the results will be displayed and discussed. Finally, we proposed a number of steps to overcome these problems and reduce the discussed side effects.

KEYWORDS: Computer Antiviruses, Computer System Performance, End-Users Feedback

INTRODUCTION

In this paper, we try to determine all disadvantages of Antiviruses and all the side effects on the computer performance, but at the first, computer virus must be well defined. The computer viruses are types of malicious software programs, these programs when executed, copy their own source code or infecting other computer programs through modifying them. [1] Infecting computer programs can be also having same infection on the hard drive, especially in boot sector, or infects data files. When these replications are executed, the affected parts are then named as infected by a computer virus. The "virus" is the most popular term, but sometime used in a wrong way to refer to other types of malware. Malware is the computer viruses with many forms of malicious programs, as: Trojan horses, adware, worms, Ransomware, rootkits, key-loggers, malicious Browser Helper Object, spyware and other malicious software. The majority of danger comes from computer worms rather than computer viruses. Most Viruses perform some type of unwanted actions on infected host computers, such as consuming the time of central processing unit or cause losing in hard disk space, accessing private information, corrupting data, spamming their e-mail contacts, logging their keystrokes, showing political messages, funny messages, or any other unwanted messages on the user's screen, or even make the PC useless [2, 3, 4]. The economic damage that happened in the few years ago, is coming from many reasons, but main one of them are the computer viruses [5] because, they are the reason of system failure, corrupting data, wasting computer resources, increasing maintenance costs.

Anti-virus (known as AV) or anti-malware software, also named as antivirus software, is PC software used to discover, isolate and delete unwanted programs. [6]

Anti-virus software was developed to discover and delete computer viruses. Now, with the propagation of other types of malware, AV program starts to support computer with some types of protection from these threats as: browser hijackers, backdoors, worms, rootkits, Trojan horse, dialers, adware, and others. [7]

The most common antiviruses are Kaspersky, Panda, Norton, NOD32, Microsoft Security Essentials, AVG, Avast, VIPRE, BitDefender and AntiVir. In this paper, we will collect all side effects of these antiviruses from different point of views, and then conclude the best way to protect our personal computer and private data.

MOST COMMON ANTI-VIRUS PROGRAM

In this section, we will mention many available AV programs in the market and give a brief description for each one of them as the following:

Avira Antivirus is an antivirus program produce, which fast detect malware and it has multiple daily definitions of update, also it is considered as one of the light-weight AV programs. It is appropriate for Win7 & 8. The free version does not have the ability to protect PC against malicious URLs and rogues. The Avira Premium edition is offering more protection and features.

- **NOD32:** It is an antivirus program that widely common, developed by ESET. The GUI of basic and advanced versions makes user satisfies. NOD32 has proven to detect faster than others because of the capability of using a sophisticated heuristic detection algorithm. The end-user can install it on Win7, 8, &10.
- **Kaspersky:** It is a common antivirus, because of its ability to quickly detect Trojan Horses, most rogues and malware. End-user can install it in Win7, 8, & 10.
- **Norton:** It is an antivirus program that supports many operating systems as wins 10. This AV program is providing popular protection through network mapping and identity protection.
- **Avast:** It is the boot-time scanner, e-mail scanner and Network Shield. The ability to detect viruses of this AV program is very good and it can be installed in any versions of Windows. This AV is installed as free or paid editions.
- **VIPRE:** It is an antivirus that has attracted end-users for its good user interface, many licenses for home site, good support, and the good ability to detect malware. VIPRE has supported all operating systems from 2000 until now.
- **AVG:** It is the anti-virus that has the stylish GUI, easy to use, Link Scanner property, and the future of e-mail scanners, these properties lead to make users make their decision to use the AVG program.
- **BitDefender:** The free version of it only provides malware removal, on-demand scanner, with the ability to quarantine and schedule scans. You have to use the paid edition to get real-time protection and other useful features.
- **Microsoft Security Essentials:** It offers real-time protection, e-mail attachment scanner, and some basic options of any antivirus. It is updated multiple times a day and it is considered as one of the light-weight AV program. The free antivirus of Microsoft will run on all Windows systems, but there is one condition that it has to pass the Windows Genuine Validation.
- **Panda:** It is an AV program that is very useful in Cloud protection; it has the ability to do the real-time protection, on-demand scanner, and other features. For full features, the paid version of it is available. Panda can work properly with Win 7, 8, &10.

MOST COMMON ANTI-VIRUS PROGRAM

In this section, a dissection about antivirus software advantages and disadvantages will be conducted; all these

positive and negative aspects will be explained.

The Benefits of Anti-Virus Software

When the end-user setup the anti-virus software on his personal computer, he gains the protection from viruses, spyware, Trojans, adware, worms, and others. Many users click on the attached files in emails or the suspect links, or they visit untrusted websites, so, by having the anti-virus program, the probability of getting infected can be decreased.

The virus is not only has the ability to do damage to the valued data, it also can make the PC useless by destroying the main functions and processes and the result of that is, the reduction of computer's performance.

AV program will protect end user while he surfs the web, also it isolates and prevents hackers from accessing to personal things as: bank account access or credit card information.

The firewall property attached to many AV programs to block any unwanted (i.e. unauthorized) incoming connections, and to prevent hackers attacking end user system.

When the viruses attack your personal computer, they can delete important personal images and files, slow down your processing speeds, and they lead to physical problem to your computer that cannot be fixed. The AV program can protect your computer from the identity theft and spyware. Identity theft is a major problem for the victims and it can cause many problems as receive bad marks on the user's credit report and lost money.

The spyware is a type of software that is designed to attack computer and spy on the users of it, the spyware looking for and get all personal information that stored on a personal computer, this can be: passwords, data about financial issues, the number of credit card and social security. The hackers can use the information in a wrong way that can harm the victim.

The AV program protects your PC from Spam, which is annoying you. In most time, the spam is the result of a virus stored on your computer; you can recognize that situation when your PC gets many emails and ads, that you have no interest on it.

Side Effects of AV Software

In this section, we will talk about the side effects of the popular antiviruses from the end user point of views; the first one of them is it sometimes attacking your active trusted programs. Some solution used as try an exceptional option, but even this utility is disabled in some antiviruses, and if it was enabled the anti-virus also attack your beloved program.

Misunderstand problem, When end user installs anti-virus, he thinks his PC will be fully protected, but AV cannot work as a firewall and it will not protect PC from hackers, So, the end user need to set up firewall software or install a full version of internet security suite, and he can also use router to support the firewall.

Performance problem, AV Program slows down the network or PC, Installing anti-virus software can use up a lot of hard disk space, and the running of it lead to allocate a lot of computer memory space and slowing down the end user PC.

Update problem, many of AV software are unable to discover old viruses, because many users forget that they have to update the database of their virus scanner's until their PC infected and that is too late. Sometimes, update delays

because of antivirus company itself.

Security problem, most of time new security holes appeared, and these are used to exploit in networking software and operating system that would give the viruses another entry point (way) to overcome the anti-virus software and infect end-user PC.

As far the limitation problem in detection techniques is concerned, there are many ways to discover a virus, but the main drawback to some AV is that they may not use all the techniques of virus detection. Virus scanners are the one of the best popular methods of detection. Scanning defined as, it is the searching process on a personal computer to discover the previous known code patterns of viruses. Another detection technique is to discover changes that made in files, as executable files (*.exe).s

Conflicts problem, since the anti-virus programs aren't having the same effect, the end user may try to set up more than one AV program. So, he must be very careful because these programs may actually not work properly and conflict with one another.

Free antivirus problem, most of free AV programs that available on net have many problems and defects and the developer of like these programs put notes to customers and tell him: “if you want to overcome these problems purchase the full product”, the problem is that the customer doesn’t understand the real problems that can be happened because of free AV like these.

A cost problem, the cost of the anti-virus program and its update is expensive in comparison of the monthly income for customers, who live in most countries as Asia, Africa, and Middle East.

A spyware problem, sometimes the anti-virus programs are could not discover the spy or they are the real spy on your personal computer specially the free programs.

Online advertising (Ads) problem, also named as Internet advertising, it is a form of marketing that uses the web to deliver marketing messages to consumers. Consumers view these messages as an unwanted noise with few benefits and try to block them for many reasons; these ads appear many times in free Anti-viruses.

EXPERIMENT

We made a questionnaire form to get the opinion of 200 users of Anti Virus Software, where all of the users were students in software engineering department – college of Information Technology – Babylon University, their age between 20 to 26 years old. This questionnaire was to ask them about the type of use AV program, what are the problems they faced when using it? What are the benefits from using it? Also, we asked them, if the AV program is free or not, and which developer that develop this Antiviruses?

RESULTS

The Resulted Statistics from questionnaire administered to 200 users of Antivirus, where all of the users are students at software engineering department – college of Information Technology – Babylon University, whose age between 20 to 26 years old, we found the following as shown in Figure (1) that illustrate the using ratio of the AV programs.

From this figure, we found that about 22% from users are using the Avast Antivirus, about 20% using the

Kaspersky Antivirus, about 14% using AVIRA Antivirus, about 6% using the Norton Antivirus and same ratio (6%) using ESET SMART SECURITY, and the others range from (1% to4%), the details of this figure was shown in Table (1).

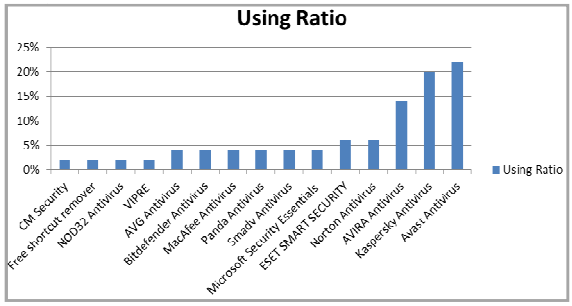

Figure 1: AV programs Using Ratio

Table 1: AV programs Using Ratio

Anti-Virus	Using Ratio
Cm security	2%
Free shortcut remover	2%
Nod32 antivirus	2%
Vipre	2%
Avg antivirus	4%
Bitdefender antivirus	4%
Macafee antivirus	4%
Panda antivirus	4%
Smadv antivirus	4%
Microsoft security essentials	4%
Eset smart security	6%
Norton antivirus	6%
Avira antivirus	14%
Kaspersky antivirus	20%
Avast antivirus	22%

In Figure (2), the percentage of each side effect, according to customer (end user) point of views is illustrated. From this figure, we found that about 27.27% is the occurrence ratio of free anti-virus problem, about 14.29% of users they complain from Online advertising (Ads) problem, 14.29% of users they fell down in Conflicts problem, and about 10.39% of users suffer from Performance problems, 9.09% they complain from Update problem, about 7.79% from users complain from the cost of anti-viruses, and finally about 6.49% of users suffer from Misunderstand problem, the rest of details is shown in Table (2) and the definition of each problem was discussed in previous section.

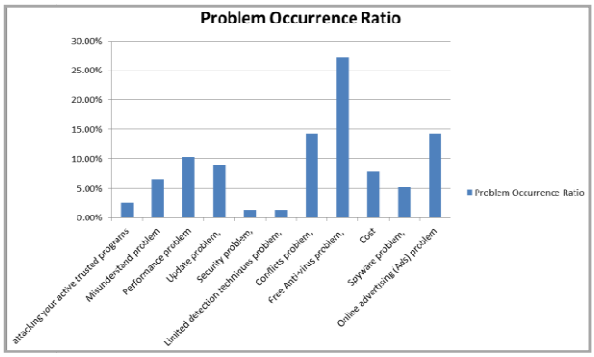

Figure 2: Problems Occurrence Ratio

Table 2: Problems Occurrence Ratio

Problem Name	Problem Occurrence Ratio
Attacking your active trusted programs	2.60%
Misunderstand problem	6.49%
Performance problem	10.39%
Update problem,	9.09%
Security problem,	1.30%
Limited detection techniques problem,	1.30%
Conflicts problem,	14.29%
Free Anti-virus problem,	27.27%
Cost	7.79%
Spyware problem,	5.19%
Online advertising (Ads) problem	14.29%

In Figure (3), we can see the percentage of each problem in each anti-virus separately, we show three only. In Figure (4), we show the comparison between the percentage of problems for each antivirus with each other's, where these result from the end user point of view.

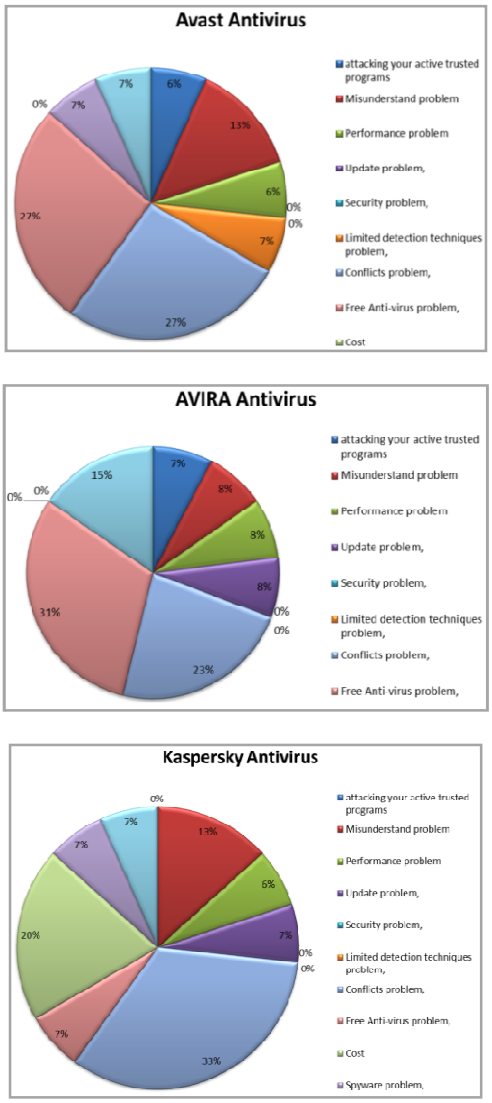

Figure 3: The Most Problems in Each Antivirus Program Separated from Program, Another's according to End Users Questionnaires

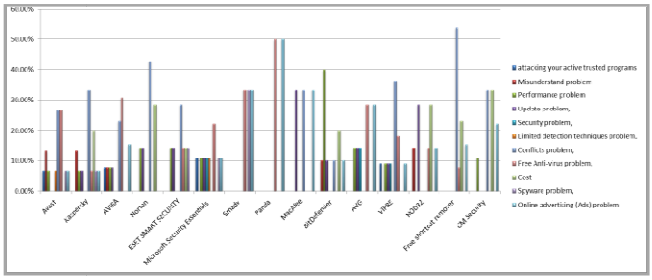

Figure 4: The Percentage of Most Problems in each Antivirus Program

SUGGESTED SOLUTION TO OVERCOME ANTIVIRUS SIDE-EFFECTS

An antivirus can protect an end user PC, from the moment the system is started and until it is turned off. To cure end-user from antivirus side-effects, the real issue here is the extent to which it can expand this protection, which is restricted to the perimeter of its signature database. Everyone will know by now that cyber-threats are continuously evolving, faster than any antivirus is able of adapting to. In other words, the end-user can only be ready against known viruses; otherwise, the antivirus infect end-user PC, so determinedly administer to his information system will only give him a false sense of security. Not being capable to get real protection against attacks that are specially coded and targeted, foreign to the existing signature database of virus, that cause the result of all scans are null.

The problem is that, a cyber-threat can only be formally identified by the development of antivirus, once it has already successfully infected several entities and spread randomly among the masses. That is, until someone finally takes notice of its existence and alerts software suppliers, proving once more that the process has its flaws. In this case, other methods employed by antivirus software editors come to the surface. Sandboxes, for instance, are a container used by antiviruses, placed around a running application, ensuring none of the mess inside gets spreads throughout the "playground". It is the quarantine meant to prevent untrustworthy applications from violates the integrity of the end-user operating system.

Then, there is also heuristic analysis; basically, the programming commands of a suspiciously behaving program are executed within a specialized virtual machine (VM), which is an environment that simulates a completely separate computer from the real-world machine. It then proceeds to play out the scenario of what expected response that particular file may have. If viral activities are detected, the user receives a message alerting him or her with concern to its potentially unsafe nature.

Most of the attacks often leave behind signs of their passing, much like the symptoms before catching the flu. If we were to perhaps pay enough attention to these signals, however weak, and catch on to them beforehand, we might just be able to put a stop to the threat before it becomes a full-blown epidemic, the suggested solution is by analyzing many of system events and logs, in real time, on a daily basis, and to identify occurring anomalies in a system's behavior, determining at the same time which ones are most likely to pose security threats.

Living without antivirus software is the one of suggested solutions. As end users, they do not set up any one of anti-virus on their computers, because of one simple reason they are convinced that, these AV programs may lead to more harm things than good, and that they make a false sense of security - causing some users to doing some riskier behavior.

As a software engineer, I cannot see my time lost due to bad software, and the AV software also has errors (bugs). As an example: one major antivirus program, lead to a lot of problems by deleting non-harm programs and user data.

AV software has to intercept many system functions to monitor, discover and prevent unwanted activity - even if the software is without bugs, which it isn't, it will slow down end-user computer, and allocate system resources and memory space. Also, after all that the end user must now pay a repeating bill in order to just feel safe.

How can the end-user live without antivirus software? He can do that by following these steps:

The end – user has to learn how to tell the things that belongs to his PC, what should be running and download, then learn to use the: Auto-runs, Process Explorer, and Root-Kit Revealer, all of these are available free, They're essential tools with high quality.

Install a good quality H/W firewall between the internet connection and the other part of your network, and then block all incoming ports.

Most of the time, run your PC as a non-admin user. This is named as Least User Access. Windows users most of time logs in with full administrative privileges and that made those users to be as a reason of security risks. So, the 'log in' as admin only in one case when it is necessary to change system configuration or to install any trusted software from a known company.

You have to make good judgment when you want to install new software, open an email, or visit a web site.

In a Periodic way run a free, online AV scanner to check your operating system to be sure that you have no infection.

Email or Web Browser, our advices for you: you have to think before open any email, if the email contained some bogus. You have to check the attachment size, recipient address, subject, sender address, if the recipient or sender is suspected, and then you have to do not open it.

For a web site, Check before visiting - go to Special site to check, if the site is in the list of malware sites or not. There are many checking sites like: www.stopbadware.org and SiteAdvisor.com.

Configure your web browser to use the highest level of security by set the Internet Zone to maximum security, then manually add selected, trusted sites to the Trusted Sites Zone you have to do this also for normal internet browsing.

Usual update your Internet Explorer and Outlook Express with the latest version, and configure your Outlook to read all emails by default in plain text. Also disable the preview panel if you need to read email in HTML.

Use the up to date browser as the default browser (like: Mozilla, FireFox, or Chrome).

CONCLUSIONS

From this work, we conclude that there are no antivirus programs clear from side effects or disadvantages, so our advice is that, we have to educate the users of the personal computer to learn how to protect their valuable data and their programs and systems from any attacks without fully dependent on Antivirus. Then after some time, the end-users will get good experience to do that without using any Anti-Virus program.

ACKNOWLEDGEMENT

I would like to thank colleagues those support me to accomplish this paper also to acknowledge all AV program users those share their opinions with me to produce this work.

REFERENCES

1. Stallings, William (2012). “Computer Security: principles and practice”. Boston: Pearson. p. 182. ISBN 978-0-13-277506-9.
2. Aycock, John (2006). “Computer Viruses and Malware”. Springer. p. 14. ISBN 978-0-387-30236-2.
3. Toxen, Bob (2003). “Real World Linux Security: Intrusion Prevention, Detection, and Recovery”. Prentice Hall Professional. p. 365. ISBN 9780130464569.
4. Alan Solomon “All About Viruses (VX heavens)". Web.archive.org. 2011-06-14. Archived from the original on January 17, 2012. Retrieved 2014-07-17.
5. Ludwig, Mark (1998). “The giant black book of computer viruses”. Show Low, Ariz: American Eagle. p. 13. ISBN 978-0-929408-23-1.
6. Naveen, Sharanya. "Anti-virus software". Retrieved May 31, 2016.
7. Henry, Alan. "The Difference between Antivirus and Anti-Malware (and Which to Use)". Paper, G. W. Juette and L. E. Zeffanella, “Radio noise currents in short sections on bundle conductors (Presented Conference Paper style),” presented at