IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Avoiding Computer Viruses and Malware Threats

Eng. Jasim M. A. ALBazzaz[1], Nassar E. ALMuhanna[2]

The Public Authority for Applied Education and Training, Higher Institute for Communication and Navigation

Computer Department, Kuwait[1, 2]

Abstract: The paper introduced the concept of the computer viruses and its harm and problems due to virus infection. It introduced the different types of viruses and the evolution of viruses. We discussed the need of anti-virus software and its performance indicators. Detecting viruses and malicious software is a complex problem, for that providing antivirus software is one of the most widely used tools for detecting and stopping viruses and malicious software. We discussed the Cloud Antivirus that uses a powerful combination of virus monitoring technologies to immediately protect your computer from all malware in the cloud computing environment. Finally, the paper put forward prevention recommendations to avoid viruses and malware threats.

Keywords: Computer Virus, Trojan horse, Worm, Malware, Anti-virus, Cloud Computing.

I. INTRODUCTION

Computers are very essential in our life, and since the first days of appearance of early viruses, there is a big contest between virus creators and anti-virus experts. A computer virus is a program that recursively and explicitly copies its evolved version. Computer Virus is a program file capable of reproducing its own special code and attaching that code to other files without the knowledge of the user. A virus copies itself to a host file or system area. Once it gets control, it multiplies itself to form newer generations.

Figure 1. Viruses, Trojan horses and worms

II. VIRUS, TROJAN HORSE, WORM, BACK DOOR, SPYWARE, ADWARE, MALWARE

- Computer Virus: a virus is a program or programming code that replicates by being copied or initiating its copying to another program, hard drive boot sector or data file. Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette. A computer virus is a self replicating program that can infect other programs by modifying them or their environment. Viruses often require a user action (e.g., opening an email attachment or visiting a malicious web page) to spread.
- Trojan horse: a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. A Trojan horse is a program in which posses various intentional undocumented feature whose effects few users of the software would appreciate were these undocumented features to manifest themselves. Unlike computer virus, which attaches itself to other program, a Trojan horse is a self-contained program can be included in software that you download for free or as attachments in email messages without knowing it.
- Worm**:** a worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. A worm is an independent program that is able to spread itself to other computers commonly across network connections. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks. A worm is a type of virus that can spread without human interaction. Worms often spread from computer to computer and take up valuable memory and network bandwidth, which can cause a computer to stop responding. Worms can also allow attackers to gain access to your computer remotely.
- Back door: A back door is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

that the program can be accessed for troubleshooting or other purposes. However, attackers often use back doors that they detect or install themselves. In some cases, a worm is designed to take advantage of a back door created by an earlier attack.

- ❖ Spyware: Spyware is any technology that aids in gathering information about a person or organization without their knowledge.
- ❖ Adware: adware is any software application in which advertising banners are displayed while the program is running.
- ❖ Malware: Malware is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission.

III. SYSTEM INFECTION

The computer system gets infected due to different reasons such as installing free applications, sharing files, accessing their system through network connections, sending and receiving E-mail messages.

There are common problems occur due to the virus attacks which means that the system is infected. The following are some primary indicators that a computer may be infected with a virus:

- Slow computer speed or system performance.
- Computer system freezes, stops responding or keeps on rebooting.
- An entire disk drive is erased or became inaccessible.
- A partition of the hard drive disappears.
- Unexplained messages and pop-ups appear on the screen as shown in figure (2).

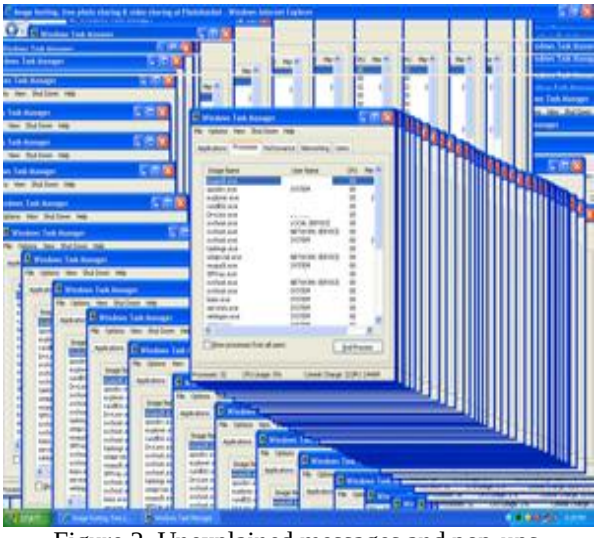

Figure 2. Unexplained messages and pop-ups

- Menus and dialog boxes are seen in distorted form.
- A program disappears from the computer even though it has not been intentionally removed.
- Out-of-memory error messages are received even though the computer has sufficient RAM.
- Windows Task Manager is unable to start.
- Slow internet connection.
- Internet browser homepage changed.
- Application software seems to be changed and does not work correctly.
- Unexplained printing problems occur.

IV. EVOLUTION OF VIRUSES

The numbers of new viruses are increasing each year and that viruses are becoming more sophisticated and malicious. Since the first viruses were written, each new class of viruses has incorporated new features that make the viruses more difficult to detect and remove.

Thus, there is some doubt that a virus could run on enough hosts to allow it to evolve. (Note that "evolve" implies a change in functions or attributes; not represents changes in structure).

The microcomputers in widespread use do not contain built-in security measures such as those on larger systems, thus the preventive measures for viruses and related threats depend on users' willingness to purchase, install, and use them.

Moreover, the process of educating users and helping them to be more aware of the problem is slow, and people are, as in other things, prone to lapses of good judgment where computer security is concerned.

Consequently, there is no reason to assume that current defenses against viruses will be generally more effective in the future than they are at present. Perhaps as part of the effort to develop better defense measures, we need to understand that computer crime is no different from theft or fraud.

At the same time, computer users should continue to learn more about viruses and how to prevent them. We need to promote the use of current defence methods and measures as applicable, and support efforts for systems and measures that offer better security.

V. ANTI-VIRUS SOFTWARE

An anti-virus software program is a computer program that can be used to scan files to identify and eliminate computer viruses and other malicious software (malware). The working area of anti-virus software has increased and now antivirus programs are the security tools designed to combat these threats preventing infections caused by many types of malware, including worms, Trojan horses, root kits, spyware, key loggers and adware.

In the crowded anti-virus software market, the most popular anti-virus software are Bitdefender Anti-virus, Kaspersky Anti-virus, Mcafee Anti-virus, AVG Anti-virus, Norton Anti-virus and F-Secure Anti-virus.

Anti-virus software does up to three tasks:

- ❖ Detection: Detecting whether or not a code is a virus or not.
- ❖ Identification: Once a virus is detected, which virus is it? The identification process distinct from detection.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

- Disinfection: Disinfection is the process of removing detected viruses; sometimes called cleaning.

VI. PERFORMANCE INDICATOR OF ANTI-VIRUS SOFTWARE

There are different performance indicators identified for measuring the performance of Anti-virus software which are as follow:

- Virus Definition Update - Update virus library.
- Anti-virus Upgrades - Anti-virus programs also may become need to be upgraded. Even if you are fully up-to-date on your Anti-virus updates, you may need to keep the software itself fully updated to the latest version.
- On-Access Scanner - The purpose of the On-Access Scanner is to scan files and folders as they are being accessed and catch any infections. In order to function properly, the scanner must constantly run in the background of your computer.
- On-Demand Scan - The purpose of this option is to scan particular drive, folder or files.
- Scheduled Scanning – Schedule a scan to be carried out automatically when the system restarts; when it boots, before the operating system is active.
- Auto Clean Infected File Scanning - Scan any removable media that is attached to your computer such as USB flash drives or external hard drives.
- Scanning of Compressed Files - Scan files in multiple layers of compression.
- Email shield - Checks incoming and outgoing email messages and will stop any messages containing a virus from being accepted or sent.
- Web shield - Protects your computer from viruses while using the internet during browsing or downloading files.
- Anti-virus Technical Support – Expert team of Anti-virus support specialists will make sure the Anti-virus software is up to date and ensure your PC is secure.

VII. CLOUD ANTI-VIRUS

Traditionally anti-virus engines have intercepted files in multiple layers (entry vector, file system and execution). In each layer, each file is scanned by multiple technologies.

Cloud anti-virus is anti-malware technology that uses agent software on the protected endpoint, while offloading the majority of data analysis to the provider's infrastructure. Cloud anti-virus is usually combined with malware detection techniques which are found in traditional anti-virus products for identifying malware. Cloud anti-virus employs agent software on the protected endpoint that is much lighter than the installed components of traditional anti-virus tools. This implies that cloud anti-virus imposes less strain on the system's resources.

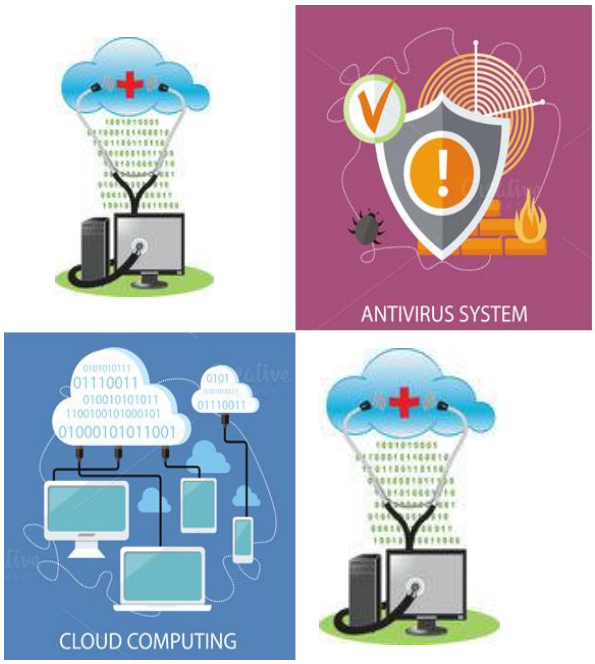

Figure 3. Cloud Anti-virus

It is cloud-based in the sense that files are scanned on a remote server without using processing power of the user's machine. Instead of having performing malicious analysis locally, the agent captures the relevant details from the endpoint and provides them to the cloud engine for processing. The processing of the data collected by agents on protected end-points is analysed by the servers of the anti-virus service provider. If malicious activities are observed on some endpoints in association with files not previously considered malicious, cloud anti-virus updates its perspective on those files.

This cloud based approach saves the time as well as money and space. So this method of deployment and detection of virus is more effective way as compared to the traditional antivirus software system and provides better protection against threats in the cloud computing environments without problems and with high efficiency and flexibility.

VIII. CLOUD ANTI-VIRUS VS PC ANTI-VIRUS

Both competitors in the cloud antivirus vs. PC antivirus have their limitations. Possibly the best solution to the cloud antivirus and PC antivirus is incorporating both types of protection in one system. The cloud service would be the lightweight intelligent internet security device, while the standard PC antivirus software could serve as a backup. This combination ensures to protect your system.

IX. VIRUS PREVENTION RECOMMENDATIONS

Prevention is the best remedy for avoiding virus infections and threats. A virus can compromise personal information and even destroy a computer completely. It becomes a major hazard and security risk.

DOI 10.17148/IJARCCE.2016.51161

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Although the anti-virus software attempt to become updated and overcome the malwares threats, however we have to accept that virus authors are one step more ahead, because they decide how to attack first and anti-virus technologies have to only defence against their attacks. Therefore, there are many weaknesses in both viruses and anti-virus technologies, which must be studied well. We need to prevent virus, Trojans, worms and malware from getting onto our systems and make sure that the system continuously protected from viruses. There are many measures, which may help in prevention and protection from computer viruses are recommended:

- Install reliable anti-virus software from a reputable vendor and keep protection tools up to date which constantly update its virus library and version to be reliable.
- Do not install multiple anti-virus programs on your computer at the same time. This will most likely cause the programs to conflict with each other and may actually reduce the security of the computer system.
- Use a virus scan before you open any new programs or files that may contain executable code. This includes software that you buy from the store as well as any program which downloaded from the Internet.
- Never download and operate software or program with unknown source and review software being installed.
- Avoid suspicious web sites and never browse abnormal websites and be careful during web browsing.
- Never open unknown e-mail in mailbox without prevention consciousness to ensure E-mail safety. (Never open e-mail attachments without scanning them first).
- Install antivirus chip on the network interface card.
- Create bootable disc and repair disc to avoid data loss.
- Make sure you back up your data (files) on disk so that in the event of a virus infection, you do not lose valuable work.
- Shut down the computer immediately after discovering virus.
- Use firewall that can maintain the network security. A firewall is a program that screens incoming internet and network traffic. Along with the virus program, it can help prevent unauthorized access to the computer. Firewall can be divided into two kinds, virus firewall and network firewall. Virus firewall can monitor the file operation in computer system and inspect if there is any virus. While network firewall has the function of screening data packages between computer and internet to effectively avoid attack from network.
- Use the combination of both is the Cloud Anti-virus and PC Anti-virus when working in the cloud environment.

X. CONCLUSION

Computer viruses are big issues for all users. We have looked at the concept of computer viruses and discussed the types of malware. We looked to PC anti-virus and cloud anti-virus software to provide system protection. In this paper, we provided some virus prevention recommendations to avoid the risk of virus attacks. Providing an anti-virus is an important part of your system security, but it cannot detect or stop all attacks. While current measures for dealing with computer viruses have proven to be effective, one should not be left with the impression that the problem of viruses has been solved. Ultimately, you are the best defense, not just technology.

REFERENCES

[1] http://searchsecurity.techtarget.com/
[2] Jeffrey Horton, Jennifer Sberry, "Computer Viruses- An Introduction", University of Wollongong.
[3] The New Age Of Computer Virus And Their Detection , International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012.
[4] Usages of Selected Antivirus Software in Different Categories of Users in selected Districts, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 3, Issue 5, May 2014.
[5] Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey, International Journal of Computer Science Issues (IJCSI), Vol 8, Issue 1, January 2011.
[6] John Aycock, " Computer Viruses and Malware ", 2006.
[7] Computer Virus: Their Problems & Major attacks in Real Life, International Journal of P2P Network Trends and Technology (IJPTT), Vol. 3, Issue 4, May 2013.
[8] Study on Computer Trojan Horse Virus and Its Prevention, International Journal of Engineering and Applied Sciences (IJEAS), Vol. 2, Issue 8, August 2015.
[9] https://zeltser.com/what-is-cloud-anti-virus/
[10] Malware Detection in Cloud Computing, International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 5, No. 4, 2014.
[11] Jon Oberheide, Evan Cooke, Farnam Jahanian, " CloudAV: N-Version Antivirus in the Network Cloud", University of Michigan.
[12] Imran Khan, "An introduction to computer viruses: problems and solutions", Library Hi Tech News, Vol. 29 Issue 7, pp. 8 – 12.
[13] Eugene H. Spafford, " Computer Viruses as Artificial Life", Purdue University.
[14] John P. Wack and Stanley A. Kurzban, " Computer Virus Attack", National Institute of Standards and Technology (NIST).

BIOGRAPHIES

Eng. Jasim M. A. Albazzaz, Computer Engineer from Kuwait University , Experience 3 years in the Information center in the Kuwait university, 16 years in the public Authority for Applied Education & Training in The Higher Institute for Telecommunication and Navigation- Computer Department.

Eng. Nassar E. Almuhanna, Computer Engineer from Wright State University, 16 years in the public Authority for Applied Education & Training in The Higher Institute for Telecommunication and Navigation- Computer Department.