THE IMPACT OF COMPUTER VIRUS ATTACKS AND ITS PREVENTIVE TECHNICS AMONG COMPUTER USERS

[1.] Abdulrahman Shuaibu Aliyu
abdurrahmanshuaibu29@gmail.com
08032089324
[2.] Muhammad Aminu Umar
muhamiumar@gmail.com
[3.] Babandi Usman
babandee@gmail.com
[4.] Uba Yusuf Magaji
ubayusuf33@gmail.com

[1 & 2] Department of Computer Science Education
Federal College of Education (Technical) Bichi, Kano.
[3 & 4] Department of Computer Science
College of Science and Technology,
Jigawa State Polytechnic, Dutse.

Abstract
Computer viruses reproduce and spread from computer to computer through storage medium and network having a detrimental effect, such as system corruption and/or data destruction. It is very difficult to prevent every computer from being attacked by viruses. Virus infects computers and other storage devices by replicating themselves in to a file and other executable programs. This paper discusses types of computer virus as well as the prevention and detections technics of computer viruses. It recommends that proper awareness of the virus attack, sensitizing the users, about suspicious website's, unnecessary downloads from untrusted websites, the purchase of licensed software, proper security implementations and the regular update of computer applications as well as the operating system as some measures to avoid these viruses attack.

***Keyword**: Virus, Detection, malicious, executable, Ransomware, threats.*

Introduction

Today's society has seen the expansion and increase of the use of computer devices. This paper aims to find some factors that lead the virus attacks and some preventive technics among the users. For this reason, the users of personal computer (Pc) today need to have a protection mechanism for the virus to face the growing computer viruses. It is important to analyze the detection and preventive those are possible to take care up. This will help for the protection of our PC (Khan & Delhi, 2014).

A virus spreads from one computer system to another through copying itself to an existing executable code. It will run when attached to executable code. The virus can be spread from one computer network to another through authorizations by the user. Every program that gets affected will also act as a virus and the spreads continue to other networks (Osborn et al., 2012a)

Ransomware is also a new type of intrusion attack with the aim of collecting a ransom from its Victim. There are three types of ransomwares which are: The first is Scareware. This type of virus does not cause any real danger to the victim; it scares the victim to be paying for a ransom. The scareware threatens to expose the victims' illegal acts to authority, family, and friends. It was also called Leak ware. The second type of Ransomware is called locker-ransomware. This type of virus locks the victim by displaying a login screen and the ransom must be paid for the password to unlock the system. This type of ransomware is less dangerous compared to scareware because sometimes the attack can be resolved through restarting the computer in a safe mode. The third type of ransomware is called Crypto ransomware; this type of virus is extremely dangerous because it will encrypt the victim files making it impossible to access without decryption key (Kok et al., 2019a).

The purpose of this paper is to introduce the readers to the guidelines and the measures on how to protect their information against unwanted access. Now a day's many computer viruses are designed to lock in your information and ask for ransom.

Related Literatures

According to Schneider, 2020, a computer virus as an executable program that attached itself to other applications programs for it spread. For example, a computer operating system when it starts up the virus will be activated to execute. The virus will check out other programs in your pen drive or any other storage medium and install itself, whenever the infected external storage is installed, the virus will be executed.

It was opined by Osborn et al, 2012b, that Institutions spend enormous amount of Money because of Computer malware activities. The malware became often advancing causing damages to the victim. The type of malware that takes more attention was called crypto ransomware. It attracts more interest especially from the cyber criminals some of these types of malwares are Wanna Cry, Notpetya and Petya. (Zhao, Liang. 2021).

A signature approach is used for detecting ransomware whereby a distinctive sequence of byte in the ransomware code, the sequence of call functions and damage massage content are saved in a database through scanning executable files by the anti-malware (Alshaikh et al., 2020).

It is not easy to find a favorable or a desirable solution in the cyber security infrastructure to halt the growth of cybercrimes, because of no system or technology which is perfect against cyber threats. The experts who supply cyber security may leave defects in the system due to inadequate monitoring of software development, maintenance, and ethical standards by the programmers. Therefore, the threat of the cyber security system can never be avoided completely because of some system loopholes which they always exist (Uddin et al., 2020)

Purpose of this Paper

Computer viruses are a worldwide problem that is distracting and disturbing computer users. It travels through the internet so quickly causing damage to files and data. PC users need to have a good virus protection policy to face the developing threat of the old and new viruses. The main purpose of this paper includes:

a. To show the strategies which viruses use in attacking computers.
b. To show the possible counter measures to protect computers from virus threats.

Types of Viruses/Malwares

There are several types of viruses/malwares, which differ in their prevention, and the way they attack computers as opined by (Hama Saeed, M. A, 2020).

1. Boot Sector Virus: This virus affects the MBR (Master boot record) of a storage media of your computer. Any type of media can trigger this virus regardless of it being bootable or not. These viruses infect the storage device by infusing their piece of code into the partition table of your hard disk. Then it gets access to the main memory of your system when the computer starts booting. Booting issues, failure to find the hard disk, and precarious system performance are basic problems that may appear after getting infected. Present-day operating systems go with a built-in safeguard for the boot sector that makes it hard to track down the MBR.

2. Overwrite Virus: This virus has influenced a wide scope of operating systems such as Macintosh, Windows, Linux, and DOS. They remove the data and supplant the existing code with the malicious code. Overwrite virus it overwrites the file content by making no changes in the size or type. It can be detected easily as the original program quits working. When the file becomes infected, it cannot be restored, and all your data can be lost.

3. Web Scripting Viruses: It penetrates browser security and allows hackers to inject client-side malicious scripting into the website page. Web scripting viruses are easy to spread as compared to other viruses. A web scripting virus is a programming code written in the core of an application, controlling the elements and behavior of that application.

4. Direct Action Virus: The direct-action virus penetrates the main memory, infects all project files, folders defined in Autoexec.bat path, and afterward removes itself. This type of virus can likewise crush the data present in a hard disk or USB device attached to the system. These types of viruses are always changing their location. They do not erase system files however they affect the system's performance.

5. Polymorphic Virus: The virus uses different algorithms and encryption keys every time they attack a program or make a duplicate of it. Because of various encryption keys, this virus turns out to be extremely difficult for the antivirus program to discover them. This virus is self-encrypted which makes it difficult to get detected by scanners.

6. Directory Virus: The Directory Virus infects the file by changing the DOS index data. For this situation, rather than pointing to the original program, DOS points to the virus code. This virus is also called a cluster virus. DOS first loads and executes the virus code before running the original program code when you run a program. It turns out to be exceptionally difficult to find the first file in the wake of getting infected.

7. Macro Virus: A macro virus is written in the macro languages, and it runs automatically when the file is opened and can without much of a stretch spread to different files as well. It relies upon the application instead of the operating

system. Macro viruses are commonly covered up with files that are received via emails. Programs like MS Word can allow embedding macro viruses in documents.

8. Memory Resident Virus : This virus exists in the main memory (RAM) and gets started whenever you start your computer. They infect all programs that are currently running on your system. It distributes memory, runs its own code when any program is executed, and blocks original scripts.

9. Multipartite virus: This virus infects and propagates in different manners relying on the operating system of your computer. It stays in the memory and affects the hard disk. When it gets into the computer, the applications' content is altered when infected. You will start to see low performance and the low availability of virtual memory.

10. Companion Virus: Not at all like typical viruses, do they alter the current file. It makes a duplicate of a file with an alternate extension (ordinarily .com) that runs alongside the real program. For instance, if you have a file with a name abc.exe, the companion virus will make another hidden file named abc.com. Also, when the system calls the file abc, the .com extension runs before the .exe extension. This virus affects your computer performance, for example, by removing the files.

Some Sign of Computer Virus

The following symptoms such as slow performance and taking time to boot up. Also, frequent restarting and unusual error messages appearing. The collapse in its operation's strange sounds. If you see a program that shows up on your computer that you do not recall downloading, practice caution, and start taking necessary actions.

It is good to uninstall or remove any software you do not trust and to run a virus scan using any system security software to detect any potential dangers. Pop-ups that show up when your program is closed are a solid sign of a virus. So, if you see any of these signs, make a quick move to remove the virus. The failure in some applications functionalities, antivirus program also disables and not allowing the reinstallation of the antivirus program. Another sign that your computer may have been infected with a virus is if applications on your computer start acting unusually. If your applications crash for no clear reason, your computer may have a virus (Isha Singh, 2010).

Methods of Virus detection

The program scans and informs the user during internal scanning. The virus writes its code at several locations and the scanner tries to remove the virus code and restore the normal operation of the program. The key to anti-virus software is detection. Once an infected file has been found, it can sometimes be corrected. If not, the file can at least be quarantined so that the viral code will not be executed again. Scanners can find viruses that are not yet executed - this is critical for e-mail worms, which can copy themselves rapidly if not stopped. Also, false alarms have become extremely rare with the software available today. Finally, scanners are also particularly good at detecting and removing viruses that they have signatures for.

The generic method is one of virus detection technic the Anti-virus software makers develop a set of rules to differentiate viruses from non-viruses. Should a program or code segment follow these rules, then it is marked a virus and take care of it accordingly. This method allows detection of any kind of virus.

Interception is a good generic detection technic to stop logic bombs and Trojan horses. Logic bombs will trigger a sequence given an event and it is detractive, such as the date being set to a certain date. When not detected by scanners, interception software will usually detect the destructive and unusual sequences of events caused by logic bombs and Trojan horses. Interception software detects virus-like behavior and warns the user about it. (Norton, 2021)

Virus Prevention Technics

It is highly recommended Anti-virus software be constantly updated with new lists of viruses. Currently, when a new virus is found but it can only be done through execution samples are sent to virus analysis centers. These centers analyze the virus and extract a unique string from the virus that will show it. This and other information about the virus are added into a database that users can then download from the company website. Do not open emails from unknown sources. Most of the time Windows viruses are triggered when users click on spam links without even knowing the sender in the first place. It is needed to Install advanced antivirus program.

It is also highly recommended to routinely back up your computer's data. Set up a back-up time on your system and it will automatically do it for you.

It is needed to use a security system and antivirus software installed and working does not mean it will protect you from all threats. It is equally important to have a security system enabled in your computer system. Windows and Macs both have a built-in security system installed; you just need to enable it so makes sure you do that for best protection. (ESSIC, 2011)

6. Conclusion

The malicious virus copies information that is confidential. It may be client information of a personnel. It may also include company information which is related to the employees' records such as username and password or some sensitive information related to the business. It can pick up useful information from any other client in the network.

7. Recommendation

It is recommended to focus on prevention and detection. Prevention is the best and least costly way for reducing the risk of virus infections.

To protect our computer from these threats it is good that we have an antivirus program installed. An antivirus program will do little good if one does not keep one's definitions up to date. New viruses are being shown all the time, so it is vital to keep your antivirus program up to date on the latest threats. In addition to this measure, organizations could adopt the following: Creating the awareness of the attacks of computer virus, sensitizing users on the need to avoid opening suspicious websites, visiting cracked websites, and downloading files only from trusted websites. Organizations/users should avoid free software because it is dangerous and buy licensed software.

References

Alshaikh, H. Ramadan, N, & Ahmed, H. (2020). Ransomware Prevention and Mitigation Techniques. *International Journal of Computer Applications, 177(40), 31–39.* https://doi.org/10.5120/ijca2020919899

ESSIC. (2011). *How Antivirus Software Works. 1–5.* http://helpdesk.umd.edu/

Hama Saeed, M. A. (2020). Malware in Computer Systems: Problems and Solutions. *IJID(International Journal on Informatics for Development), 9(1), 1–8.* https://doi.org/10.14421/ijid.2020.09101

Isha Singh (2010). Symptoms of Computer Virus (online) 2023/03/29. Available from: http://hellboundbloggers.com//symtoms-of-computer-virus

Khan, I, & Delhi, N. (2014). An introduction to computer viruses: *Problems and solutions Library Hi Tech News Emerald Article: An introduction to computer viruses: problems and solutions Article information: March.* https://doi.org/10.1108/07419051211280036

Kok, S. H. Abdullah, A, Jhanjhi, N. Z., & Supramaniam, M. (2019). *Prevention of crypto ransomware using a pre-encryption detection algorithm. Computers, 8(4), 1–15.* https://doi.org/10.3390/computers8040079

Norton, T. (2021). Virus and Malware prevention method: http://www.pckrisk.com/computer- technician-blog/general-information/7022-how-to-remove-virus-no-imternet-access.

Osborn, H., Mba, Q., Pg, M. I. S., & Law, C. (2012a). The Economic Impact of Computer virus a case of Ghana. *International journal of science and research 3(8), 1235–1239.*

Osborn, H., Mba, Q., Pg, M. I. S., & Law, C. (2012b). *The symptoms after virus infected computer:* http://creatingwords.com/work/ghostwritting/computer/warningsi.

Schneider, W. (2020). Session XIII Tutorial: Computer Viruses. *Behavior Research Methods, Instruments, & Computers, 21(2), 334–340.*

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cyber security hazards and financial system vulnerability: a synthesis of literature. *Risk Management, 22(4), 239–309.* https://doi.org/10.1057/s41283-020-00063-2

Zhao, Liang. (2021). Network Security and Computer Virus Prevention on the Internet. https://doi.org/10.1007/978981-16-1726-3_148.