International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume30العدد
July 2022 يوليو
المجلة الدولية للعلوم والتقنية
ISTJ

Study the performance of the Antivirus and Firewalls and their effects on the Computer

Abulgasem. Guunbaej[1] **Khalid Elatrash[2]**
Abdulmanam Abdulwhab[3]

Higher Institute of Marine Science Technology
63gunbaej63@gmail.com

Abstract.
A security issue occurs when your system is compromised by an attacker, hacker, virus, or other type of malware.
The most targeted people in security breaches are the people who surf the Internet, as the breach causes annoying problems such as slowing down and interruption of browsing traffic at regular intervals. The data can be inaccessible and in the worst case, the user's personal information can be compromised. This paper shows the differences in performance between two kinds of systems that, publican used in windows to reduce the effects of the attackers. One of them is anti-various and the next one is the firewalls, the firewalls are safer than anti-virus and the no need to update the software yearly.
Key word: Security, Attacker, malware, firewalls**.**

الملخص

تحدث مشكلة الأمان عندما يتعرض نظامك للخطر من قبل مهاجم أو متسلل أو فيروس أو أي نوع آخر من البرامج الضارة.

أكثر الأشخاص المستهدفين في الخروقات الأمنية هم الأشخاص الذين يتصفحون الإنترنت، حيث يتسبب الاختراق في حدوث مشكلات مزعجة مثل إبطاء حركة التصفح وانقطاعها على فترات منتظمة. يمكن أن يتعذر الوصول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم. يوضح هذا البحث فرق الأداء بين نوعين من الأنظمة التي يستخدمها العشرات في النوافذ لتقليل آثار المهاجمين، أحدهما مضاد

للتنوع والآخر هو جدران الحماية، والجدران النارية أكثر أمانًا من مكافحة الفيروسات ولا حاجة لتحديث البرنامج سنوياً.

1. Introduction.

In the event of programming errors or wrong settings in the web server, it may allow unauthorized remote users to gain access to confidential documents containing personal information or obtain information about the server's host machine, thus allowing system intrusion. These people can also execute commands on the host server machine which can modify the system and launch flood attacks causing the machine to crash temporarily, and flood attacks (DOS) are intended to slow down or paralyze network traffic [1] Also, through Distributed Flood Attacks (DDOS), the attackers uses a number of computers that have been taken to attack another computer or computers, where the DDoS rootkit is installed on a computer using a stolen account [1].

Spying on network data and intercepting information that travels between the server and the browser can become possible if the network or servers are left open and their vulnerabilities exposed [1]. This paper shows the performance of two kinds of systems protection tools that used in windows, one of them is anti-various and the other one is the windows firewall.

2. computer viruses:

Computer viruses are the most common information security problem faced by users and companies. A computer virus is an unwanted program that enters the device without permission and inserts copies of it into computer programs, in other words, the virus is a malicious or intrusive program. Other malicious programs are called worms, Trojans, adware, or spyware [3].

Malicious programs can only be a nuisance by affecting the usage of the computer, slowing it down, causing interruptions and crashes at regular times and affecting

various programs and documents that a user might want to access. More dangerous malware can become a security issue by obtaining your personal information from your emails and other data stored in your device [2].

As for adware and spyware, they are often annoying and lead to advertisement pop-ups on your screen. Spyware also collects your personal information and provides it to third parties who request it for commercial purposes.

You can protect your computer and yourself by using appropriate anti-malware programs that may be unwanted and potentially devastating [1].

First Classic Viruses, which are programs that aim to sabotage the system and cause malfunctions and errors in it mainly

And there is a new type of virus that uses the method of file injection, where it adds part of its code to the file, infects it and becomes part of it system resources and much more.

3. Types of Viruses

The viruses can be divided into:-

3.1. File Viruses

These types of viruses follow at least one of these methods to infect the system

A) Injected viruses infect executable files, and in this case, when an antivirus detects it, it gives you the option to correct (Disinfect, Cure, Repair, …etc), as it varies according to the type of antivirus you are using, and among the most famous of these viruses are the famous Sality virus and Mabezat virus, and unfortunately most viruses are this type [2]

B) they make copies of themselves in famous paths of the device, %System Root%, %Temp% , %user profile%,…etc. %system drive,%.

C) Virus that use system file feature.

These viruses spread in the nineties of the last century, but with the progress of 32-bit processors and the decreasing use of floppy disks, their number dwindled, although

technically it is possible to create such viruses based on the Cd and on flashes [4].

3.2. Macro viruses

These viruses infect the files of text editors such as MS Worde - MS Excel- Power Point as soon as you open such viruses; other files are infected with this device. An example is a virus, as soon as you open it on the device, all Office files that are running on the device are erased, even if they are stored [3]

3.3. Script Viruses

which are viruses that use code for symbolic languages (JavaScript, Visual Basic Script, Php, patch files, … etc(and it infects the system and leads to converting the codes into operations that disturb the system) [4].

3.4. Trojans Viruses

Backdoor Trojan, which are the most dangerous because they take the powers of a system administrator and operate in complete secrecy and without the user's knowledge [3]. And it uses a local network or the Internet to control the victim's device and track the behavior of the system administrator tools (Remote Administrator Tool (RAT)). The difference between Trojans and administration programs is that Trojans download and run without the user's knowledge, while the administration tools are clear and give you a message that they monitor the system and this type TCP/IP is used to control the protocol, which is the same protocol used by the messenger and to manage Internet cafes and some programs. The backdoor Trojan dangers lie in the following [1]:-

-Send and receive files to and from the victim's device.
-Access to private files and the ability to delete and modify them

-Directing the user to a website without his will and changing the home page as well.
-Theft of private information and passwords.
-Running software and hardware related to the device (printer, camera, etc).

4. Firewall

An Internet firewall is a program or device that screens and filters viruses, worms, hackers, and aggressors trying to access your computer over the Internet [3]. Installing a firewall is the most effective way, and the most important initial step you can take to protect your computer before you go to the Internet for the first time and keep it running at all times.
And because the internet is a public network, any connected computer can find and connect to any other connected computer. A firewall is a barrier between the internet and your own computer or network. Think of it as a highly dedicated security guard who stops anyone coming into your computer if they're not on the guest list, and anyone leaving if they don't have permission [3].

5. Types of firewalls

5.1. Personal firewalls

Personal firewalls should be installed on each computer that is connected to the internet and monitors (blocks where necessary) internet traffic. They are also sometimes known as 'software firewalls' or 'desktop firewalls' [4].
Windows Firewall is a basic personal firewall. It is free, included with Windows operating systems. In Windows 10 and 8, the Firewall defaults to active, so you do not need to worry about configuring it yourself.
If you wish, you could replace Windows Firewall with another personal firewall of your choice, including the type incorporated in some internet security packages, or standalone firewall software which can be downloaded from the internet, some of which is free of charge [2].

5.2. Hardware firewalls

Medium-sized and large businesses may need a hardware firewall – in addition to personal firewalls – depending on the configuration of their IT infrastructure. The internal or external IT support resource will be able to recommend, source, install and configure the most suitable one for the business needs.

6. Antivirus program:

In addition to the firewall program, the antivirus program must be obtained before entering the Internet for the first time. The anti-virus program scans the device for new viruses that it has infected and then cleans these viruses to ensure that no further harm is done to the device [4].

Just as with a firewall, the antivirus software should be kept running at all times so that once your computer is turned on, the software will start detecting viruses, ensuring that they are dealt with as quickly as possible. Antivirus software also detects viruses on disks inserted to the computer, e-mail you receive, and programs that you downloads to the computer from the Internet [2]

In the event that a virus enters the device, the anti-virus program will alert you and then try to repair the infected file, and this program isolates the viruses that it cannot repair and try to rescue and repair any infected files that it can fix. Note that some anti-virus programs require you to send the virus information to the anti-virus company, so that they can enter it into their database if it is a new virus [5]

The antivirus software's can be found online to buy or at software store and it's a good idea to check if your internet service provider (ISP) provides such software. It is worth noting, that if your computer is infected with viruses, it is dangerous to purchase online protection software because the spyware can eavesdrop on your credit card information and steal it even if you enter it on a secure web page [5].

The antivirus software must be compatible with your computer and the software you have. The most used

antivirus programs are programs provided by McAfee, Norton Antivirus from Symantec, Cisco System and Microsoft [2].

To illustrate more keep your hardware and software up to date**:**

Because viruses are constantly changing, it is important that you keep your computer's operating system, firewall software, and antivirus software up-to-date so that they are kept updated. The antivirus will automatically ask you to update the software and you must make sure that you have updated. Note that many virus-scanning programs can be obtained once a year and we advise you to upgrade the program after that in order to ensure that your device includes the latest update [4].

7.Results

From the study that the researcher has done and checked for windows, the researcher has been founding the flowing results.

- Firewall safer than anti viruses especially in windows 10 because it has already installed as a package in the windows.
- No need to check the date and the period of time of your system with firewall, on other hand in anti-virus we need to check the date.
- In anti-virus we need to check the update, but we don’t have to check it in firewall.
- Antivirus: It is suitable for ordinary users who do not connect to the Internet and do not download or purchase via the Internet. It protects your computer from viruses only. It can be said that it is an internal protection program, meaning that if you connect a flash drive, a memory card or an external hard, it can search for viruses and protect you from them and get rid of the Short Cut Virus and Autorun if it is a strong anti-virus, and it also does not consume a lot of

device resources and therefore will not cause a noticeable slowdown for the computer unless the computer specifications are weak.

- Firewall: We can liken it as a powerful firewall for every hacker who wants to penetrate to the computer or penetrate it, and it is integrated into most antivirus programs now and is present in Windows Defender, but there are some independent programs for the firewall such as zone alarm free firewall and Outpost program, which acts as an assistant program for the antivirus you are using.

8. Conclusion

The study proved that dealing with the firewall is better in terms of cost and is considered uncomplicated for users in light of the presence of the Internet or not, and the existing antivirus requires the presence of the Internet, as the presence of reliable protection without the Internet is very difficult.

9. References

[1] "Firewall as a DHCP Server and Client"، *Palo Alto Networks* ، اطلع عليه بتاريخ 08 فبراير 2016، *في 06 أغسطس 2017*.

[2] "WAFFle: Fingerprinting Filter Rules of Web Application Firewalls" ،*2012* ، *في 25 أغسطس*

[3] https://technoarabi.com/antivirus-vs-internet-security-firewall/date: 2/5/2022 time 20:00

[4] https://kutub.freesite.host/tag date: 10/5/2022 time 10:00

[5] https://www.getsafeonline.org/personal/articles/firewalls/ date: 7/5/2022 time 18:00