Practical No. 6

Aim : Study different approaches for Anti-virus software and write one document.

a. Examine files to look for viruses by means of a virus dictionary

b. Identifying the suspicious behavior from any computer program which might indicate infection

Theory :

1. Introduction

Now a day's computers are very essential part of our life. The uses of computer are increased day by day. A computer people can share information from one computer to another computer with the help of device or media. In the current days there are various ways or method for sharing information because people can carry several gigabytes or terabyte of data from one destination to another destination. We also know history and which devices are used to exchange information in the world. There are several ways a user can go about copying data from one computer to another computer. In the process of exchanging the information using communication media there will be a problem of attack of malware or computer virus. A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge. Viruses are capable of displaying different messages, denying all kinds of access, data thefts, changes in valuable data or files, deleting systems or any files, or it disable hardware.

Therefore. an early detection and prevention mechanism is very important for the security of the computer. Anti-virus software is a critical link in overall security chain. protecting organization's computers from many types of viruses. including worms and Trojan horses. Using Anti-virus software is a good way to detect viruses and it is advisable to use Antivirus software on network operating systems and workstations for adequate protection. Antivirus software is specifically written to defend a system against the threats that malware presents. Anti-virus software may work differently and ranges from large security packages to small programs designed to handle a specific virus. The large number of Anti-virus software available in the market and some are being launched, each one of them offers new features for detecting and eradicating viruses and malware. Therefore people have a choice of different types of Anti-virus i.e. both in the form of freeware software or licensed software. People frequently change their Anti-virus software according to their liking and needs without evaluating the performance and capabilities of the various Anti-virus software available.

Hence there is a need to find parameter for measuring performance of Anti-virus software for finding good and also suitable for the specific needs of the users.

2. Working of Anti-virus

Antivirus software works by comparing your computer applications and files to a database of known malware kinds. Because hackers are continually creating and disseminating new viruses, it will also check systems for the presence of new or undiscovered malware threats.

The antivirus checks files, programs. and applications going in apd out of your computer to its database to identify matches. Similar and identical matches to the database are segregated, scanned. and eliminated.

Most programs will employ three types of detection devices:

- Specific detection. which looks for known parts or types of malware or patterns that are linked by a common codebase
- Generic detection is a type of detection that looks for known parts or types of malware or patterns that are related to a common codebase.
- Heuristic detection is a type of virus detection that looks for unknown infections by spotting suspicious file structures.

3. Computer Virus Pattern

Computer virus analysis has some common patterns that lend efficiency to the analysis process. in order to stay far trong the anti-virus scanners, computer viruses gradually through patters improve their codes to/make them invisible. Simply put, computer virus patterns also referred to as virus signatures for those known by antiviruses are means through which viruses replicate themselves over and over as they infect computer systems. Virus signature is the representative byte-pattern part of virus family, which when a virus scanner recognizes it in a file, it notifies the user that the file is infected. A virus signature is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified variety of viruses may have the same virus signature allowing anti-virus programs to detect multiple viruses when looking for a single virus signature. Because of this sharing of the same virus signature between multiple viruses, anti-virus programs can sometimes detect a virus that is not even known yet. Typically new viruses have a virus signature that is not used by other viruses. but new "strains" of known virus sometimes use the same virus signature as earlier strains. Computer virus authors and antivirus vendors have constantly fought in an evasion of detection game through creation of new virus signatures. Computer malwares have become more and more sophisticated, using advanced code obfuscation techniques to resist antivirus detection. Polymorphie and metamorphic computer viruses are currently the hardest kinds of viruses to detect. Both types of viruses are able to mutate into an infinite number of functionally equivalent copies of themselves. This sophistication comes with the creation of new virus patters that are not easily detectable by the antiviruses available in the market today. Heuristic detection is a scanning mechanism that anti-virus software employs in detecting for virus signatures. The heuristic detection methods encompass more than 250,000 new virus signatures and are most effective for locating new virus signatures. When there are new signatures created each time a new virus comes out these then should be detect during the virus scans since it is necessary to create the new signatures as the new viruses cannot otherwise be detected. Metamorphic type of viruses modify their code to produce an equivalent one during their propagation. These viruses attempt to evade detection through static analysis by implementing code obfuscation techniques. A technique implemented by swapping interchangeable instructions, inserting garbage instructions and introducing conditional jumps to produce the child virus. Here the signature of a virus is broken by changing the order of instructions without altering the control flow. A sophisticated type of this virus will generate code based on the host's operating system by translating the instructions to the corresponding machine code. The detection of these viruses using their signature is challenging since the signature is broken in each version of the virus.

In order to detect such metamorphic viruses, the detection system should be designed to extract the essential instructions of the virus from virus instance. This extracted instruction set should be used to detect the viruses of that type.

4. Need of Anti-virus:

- Antivirus plays an important role in any device. Following are a few of the top protection provided by it.
- Antivirus detects malware and viruses that prominently penetrate company systems.This will help in maintaining the hygiene of the computer.
- The growth of hackers is immense these days. Hackers tend to target sensitive and confidential data from your system. In the presence of antivirus. the activity of data access and more can be detected. Moreover, the data will be protected to a great extent by the antivirus software.
- If you regularly plug in external devices to your PC, the antivirus software will protect your PC/laptop from any potential virus from any external device.
- Through the above-mentioned methods, your PC/ laptop will be protected against viruses to a great extent. As a result, your computer will have a long life.

5.1 Virus Protection:

The main role of an antivirus program is to face viruses and other sorts of malware. The viruses won t only cause damages to your data, it can degrade the general system performance. All of them can happen without your knowledge. The antivirus programming introduced on your PC distinguishes and eliminates this malware before they create any damages to your PC.

5.2 Spyware Protection:

Spyware because the name suggests may be quite a malware that spies on your computer stealing all the confidential information. These details also inelude MasterCard details. passwords. and other financial data. This ultimately results in fraud. The antivirus software has the potential to stop these sorts of spyware attacks.

5.3 Web Protection:

While surfing the web, users can encounter various other sorts of threats. In untrustworthy sites. cyber attackers can gather your MasterCard and checking account details. One among the thanks for overcoming this is often by using antivirus software. Using an antivirus program you'll protect your valuable pieces of information while surfing online.

5.4 Spam Protection:

Viruses also can enter your computer through means of spam emails and ads. These emails and ads can show up repeatedly albeit you haven't any interest in it. Once the virus finds thanks to sneak into your PC it causes irreversible damages. An Antivirus works by the way of blocking these spam emails and ads.

5.5 Firewall Feature:

The firewall provides two-way protection. This suggests that regardless of the information that's sent or received is going to be double-checked here. Hence, hackers cannot enter the system data.

5.6 Cost-Effective:

Even though there are many premium versions of antivirus programs for a monthly/yearly subscription fee, there are some antivirus programs that are completely free from charge. These sorts of antivirus programs offer almost an equivalent level of protection provided by the subscription-based. Albeit you select to afford a premium version, they're relatively inexpensive.

6. Drawbacks of Antivirus:

6.1 System Slowdown:

Using an antivirus program means tons of resources from the memory and therefore the disk drive is getting used. As a result, it can drastically slow down the overall speed of the pc. Moreover, the method of scanning also can cause lags within the network.

6.2 No Complete Protection

If you're employing a free antivirus program, there's no guarantee that it'll provide you the entire protection. Moreover, they're capable of identifying only certain sorts of threats. So as for acquiring a complete level of protection, you've got to use a firewall also.

6.3 Security Holes

When security holes are present inside the OS or the networking software, it'll provide an opportunity for the virus to bypass the antivirus software. Unless the user takes action to stay updated. the antivirus software won't be effective.

6.4 Limited Detection Techniques:

For identifying a possible threat. there is always quite one method available. However. within the case of antivirus programs, it mostly executes the tactic of virus scanning. Sometimes the antivirus programs can offer you false alarms if the scanning matches with the traditional file.

6.5 Frequent Advertisements

Apart from premium versions of antivirus programs, through some means, the free antivirus software must generate an income. Advertising is one of the ways to realize them. Many sometimes these advertisements degrade the user experience.

6.6 No Customer Support

Unless you buy the premium version, there won't be any customer support given to you. Within the event of any problem, the sole thanks to overcoming are through forums and knowledge bases.

7. Identifying the suspicious behavior from any computer program which might indicate infection

A. Unexpected pop-up windows

Unexpected or unusual dialog boxes and windows can be a bad sign. Fake virus warnings claim you have security threats on your computer and usually prompt you to click a link or call a number. "One of the things we always tell people is that, as of right now, there's no way a website can tell you if your computer is infected." Armstrong said. "Sometimes, Skype will pop up a message saying. Urgent security vulnerability.' But Skype can't tell if your computer is infected." Legitimate protection software, such as Windows Defender and virus-scanning programs, will never prompt you to call a customer service number.

B. Random sounds

Infected computers are often programmed to respond with an audio signal to things you can't control. "They'II be things like warning beeps." Armstrong said. *When an error message pops up, a lot of times, it comes along with a warning message. Certain pieces of malware stifle that window so you can't see it. But you might still hear the warning message - a sound in the background that you didn't initiate." If you regularly hear chimes and bells from your computer that seem phantom, your computer may have a virus or malware infection.

C. Unexplained file or folder changes

Your files might be missing, or the icons and content of your files may be different. Your computer won't make these types of changes to your files amless you have a virus or technical problem, though corrupted browser bookmarks should't be regarded as a warning sign. It's common for bookmark icons to become jumbled bs a browser such as Chrome.

D. Slow operation

Pay attention to whether your computer is running more slowly than usual, especially ifits hard drive light (if it has one) is constantly on or its fan is operating at full speed. This suggests the computer's resources are being redirected away from legitimate programs.

"One of the popular scams right now is something called pay per install, Armstrong said. "There are third-party companies out there in places like Russia and China that allow [someone] to go to their forums and sign up to receive a piece of software. They then pay [that person] for every thousand users they can fool into installing the software." Money is a massive incentive for cybercriminals. "So. these people who try to trick you into installing rogue software will put as many things on your computer as possible at the same time to make the most money." Armstrong added. "And with all this spyware and applications running at the same time, you'll see a slowdown in performance."

E. Sudden lack of hard drive space

Have you suddenly run out of space on your hard drive? Self-replicating viruses or worms (often called "disk bombs") can wreak havoc on a computer system by rapidly filling hard drives with copies of itself. In many cases, the files it injects into a hard drive are invisible under default file-browsing settings.

F. Random connections to unknown websites

Another sign of an infection is when your legitimate antivirus software alerts you that an application is trying to connect to a website you've never heard of. In general, your computer doesn't make its own connections: someone has to initiate them. If vou didn't initiate these connections, problematic software could be doing it for you.

G. Unexpected images

You might see pornographic images pop up or replace benign images, such as photos on news sites. A related sign that your computer is infected is the constant appearance of pop-up ads for sites you don't usually visit.

8. Conclusion:

Anti-virus protection is, or should be, an integral part of any Information Systems operation, be it personal or professional. There are number of computer virus are created and these computer virus are affected in day today life. The large number of Anti-virus software available in the market and some are being launched, each one of them offers new features for detecting and eradicating viruses and malware. The antivirus software objective is to behind the viral protection programs is to secure the system using these 3 tasks; Take preventive measure, Detection of the malicious code, Eradication. There are six different brands of Anti-virus software that are being used by the various categories of users in the selected area. Anti-virus software performs frequent virus signature, or definition, updates.

These updates are necessary for the software to detect and remove new viruses. New viruses are being created and released almost daily, which forces anti-virus software to need frequent updates

9. References

[11 Usages of Selected Antivirus Software in Different Categories of Users in selected Districts March 2014 Dr. Bhaskar Vijayrao Patil, Milind Joshi.

2 Review of Viruses and Antivirus Patterns Jan 2017 Muchelule Yusuf. Waniala & Nevole. Misiko Jacob.