Anti-Virus: software to keep users safe from virtual threats

Tasmiah Sarif Nayna
University Teknologi Malaysia
Software engineering (semester-1)
Skudai, Johor, Malaysia
tasmiahnayna12@gmail.com

Abstract—The first known computer virus appeared in 1971 and was dubbed the "Creeper virus”. The first known that appeared "in the wild" was "Elk Cloner", in 1981, which infected Apple II computers [1]. For as long as computers have been and will be in existence, whether it is connected to the Internet or not, there will always be a need for antivirus software. Because there will be always the present of created new viruses randomly. Although not every threat into a computer is meant to cause damage or steal valuable information, on the other hand it doesn’t mean that the attack isn’t dangerous. All type of virus can create weakness in the computer and operating system. Sometimes because of the virus attack the computers become slow and useless. Antivirus software is an important tool to help prevent such attacks. However not every type of cyberattack can be prevented with antivirus software, but it can be a great asset when trying to prevent overstepping into a computer

Keywords- Malware,virus,security,cloud,prevention,scan, computer

I. Introduction

Antivirus is a software which is created to detect, delete and prevent viruses. Once antivirus is installed it can perform automatically in the background against the viruses that can harm computers. In particular, modern antivirus software can protect users from: malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware.[2]

Moreover, antivirus protection software are designed to evaluate data such as web pages, files, software and applications to find and uproot malware as quickly as possible. It scans the device regularly so that any threat can be removed as soon as possible. It gives automatic updates everyday once it is installed. Nowadays it is common to conduct work online and new threats emerge continuously. As a large amount of important information is passed between computers worldwide, the risk of Trojan horses, viruses, malware, spyware and other digital threats has increased. As computer has become a part of our daily life this malware problem is also taking a part into it. That is why the cyber security and malware detection market is raising rapidly.

II. Anti-Malware Software

All antivirus programs can be divided into the following three categories**:**

a) Standalone Antivirus Software

Independent antivirus software is a tool dedicated to detecting and deleting certain viruses. It is often referred to as portable antivirus software because it can also be installed on a USB drive and used by administrators to perform emergency scans of infected systems. However, most portable programs are not designed to provide real-time protection and download new virus definitions every day, which is why they cannot replace Internet security suites with multiple additional features.

Over the years, several types of antivirus programs have been developed. When setting up an umbrella, it is important to understand the more common antivirus programs available.

b) Security Software Suites

The security software suite is not just an antivirus program. In addition to being able to detect and remove viruses, they also have the ability to resist all other types of malicious software and provide round the clock protection for our computers and files. Most of these packages contain anti-spyware, firewall and parental control functions. Some of them also include other features such as password managers, VPNs and even standalone antivirus programs bundled with the suite.

c) Cloud-Based Antivirus Software

Cloud-based antivirus software is a fairly new type of antivirus technology that can analyze files in the cloud instead of the computer to free up computing resources and speed up response. These programs usually consist of two parts-the client installed on the computer, which runs regular virus and malware scans without taking up too much memory, and processes the data collected by the client and checks whether it matches the virus. Web service. Malware database.

A. Identification of malware:

a) Signature-based detection

Substantially, when a malware arrives in the hands of an antivirus firm, it is analyzed by malware researchers or by dynamic analysis systems. Then, once it is determined to be a malware, a proper signature of the file is extracted and added to the signatures database of the antivirus software.[3]

b) Heuristics

the Vundo trojan has several family members, depending on the antivirus vendor's classification. Symantec classifies members of the Vundo family into two distinct categories, Trojan. Vundo and Trojan.Vundo.B.[4]

c) Rootkit detection

Anti-virus software can attempt to scan for rootkits. A rootkit is a type of malware designed to gain administrative-level control over a computer system without being detected. Rootkits can change how the operating system functions and in some cases can tamper with the anti-virus program and render it ineffective. Rootkits are also difficult to remove, in some cases requiring a complete re-installation of the operating system.[5]

d) Real-time protection

Real-time protection, on-access scanning, background guard, resident shield, auto protect, and other synonyms refer to the automatic protection provided by most antivirus, anti-spyware, and other anti-malware programs. This monitors computer systems for suspicious activity such as computer viruses, spyware, adware, and other malicious objects in 'real-time', in other words while data loaded into the computer's active memory: when inserting a CD, opening an email, or browsing the web, or when a file already on the computer is opened or executed.[6]

III. THE USE AND EFFECTIVENESS OF ANTI-MALWARE SOFTWARE

Over the years, several types of antivirus programs have been developed. When setting up an umbrella, it’s important to understand the more common antivirus programs available.

Malware signature antivirus

Malware can install viruses and spyware on computers or devices without our knowledge. Malware can steal login information, can use computer to send spam, can damage the computer system, and essentially provide cybercriminals with access to our device and the information stored on it, can even monitor and control our online activities.

Malware signatures Antivirus software detects malware signatures, which are digital fingerprints of malware. Antivirus protection can scan specific malicious code, identify specific viruses and disable these programs.

Although the antivirus protection of malware signatures is the key to detecting and eliminating known viruses, one of its limitations is that it cannot deal with new viruses. The antivirus product does not contain these new virus signatures at all.

System monitoring antivirus

This anti-virus protection function can monitor software and computer systems for suspicious or atypical behaviors of users. When a user connects to an unfamiliar website or tries to access a large number of files, or when data usage increases significantly, an alert is generated. The alert make us aware.

Machine learning antivirus

It monitors "normal" computer or network behavior. Machine learning antivirus software can restrict the activities of programs or computers as long as they look suspicious. This type of antivirus protection is beneficial because it works in conjunction with other antivirus applications to provide multiple layers of protection.

One example of machine learning is the design of Microsoft’s latest antivirus software, which can gather data more than 400 million computers running on Windows 10 to discover new malware. (Note: To be clear, this is diagnostic data that a consumer can opt out of reporting.) . This automation is key in its ability to stay on top of the latest viruses.[7]

IV. IMPORTANCE OR BENEFITS OF ANTIVIRUS

Users are also curious about the benefits of antivirus. Knowing these benefits might help one convince to invest in an antivirus program.

- **Protection from viruses**

  This one is a primary function of an anti-virus program. This program protects the computer from viruses, malware, spyware, and other unknown threats, and eliminates these malicious programs before they damage the device system. An effective antivirus software will list good and bad files to detect whether the program is harmful**.**

- **Prevention of phishing attacks**

  It can protect the computer from phishing attacks. These attacks include unauthorized attempts by third parties to access computer data to steal or infect data and make it impossible for the owner to use it

- **Scanning removable devices**

  Antivirus software can quickly scan any removable devices connected to the computer to identify potential threats. For example, using Comodo, it will automatically put unknown executable files into a virtual container. The container allows the program to run for use by the computer owner, but it prevents the program from accessing the computer's data and other resources.

- **Protection against online threats**

  With continuous access to the Internet, a computer user has to fight off numerous cyber threats. Therefore, a good antivirus can block them from accessing the computer.

- **Firewall protection**
  It monitors the data that enters and exits the network system through the Internet, monitors suspicious data, and prevents suspicious data from being transmitted**.**
- **Blocking spam sites and ads**
  It monitors data entering and leaving the network system through the Internet, monitors suspicious data, and prevents suspicious data from being transmitted**.**
- **Faster computer**
  It deletes unwanted folders and files from the computer, improving its performance speed
- **Protection from identity theft**
  Spyware attacks are designed to steal personal information from computers. These can include bank data, social security numbers, passwords, credit card numbers and other important data. Some sophisticated spyware can even run silently in the background, waiting for computer users to purchase goods online and enter their credit card information for payment. Spyware will be recorded and used as if it were recorded, thereby contributing to identity theft. Antivirus software even prevents spyware from accessing computer data, thereby enabling safe shopping and online banking.
- **Convenience**
  Simply running an antivirus program is more convenient than wasting time trying to find, delete, and restore damaged data.
- **Restore damaged files**
  If a file has been infected by a computer virus, anti-virus software will attempt to remove the virus code from the file during disinfection, but it is not always able to restore the file to its undamaged state.[8]

CONCLUSION

All in all, using an antivirus program can protect your computer from virus attacks. It helps prevent data and information from being attacked. An antivirus program is a software that is installed on a computer and used to scan the PC for any viruses, which may damage the computer. Many powerful antivirus programs have high-quality protection, such as Norton and MacAfee. In addition, the program can detect any virus in two ways: footprints and features. There are many malicious programs masquerading as things that can help you to actually harm you. They may cause performance delays, so much so that you may automatically give up defences. This is why it is absolutely important to only use the best antivirus software on the market. The best defence is prevention first. Otherwise, it's too late and you may not get the redo.

REFERENCE

[1] "Elk Cloner". Archived from the original on January 7, 2011. Retrieved December 10, 2010.

[2] Henry, Alan. "The Difference Between Antivirus and Anti-Malware (and Which to Use)". Archived from the original on November 22, 2013.

[3] Automatic Malware Signature Generation ArchivedSeptember 21, 2015, at the Wayback Machine. (PDF) . Retrieved on January 3, 2017.

[4] Symantec Corporation (February 2009). "Trojan.Vundo". Archived from the original on April 9, 2009. Retrieved April 14,2009.

[5] "Terminology – F-Secure Labs". Archived from the original on August 24, 2010

[6] Kaspersky Lab Technical Support Portal Archived March 12, 2006[Date mismatch], at the Wayback Machine

[8] "Why F-PROT Antivirus fails to disinfect the virus on my computer?". Archived from the original on September 17, 2015. Retrieved August 20, 2015.

[9] "Actions to be performed on infected objects". Archived from the original on August 9, 2015. Retrieved August 20, 2015.

[10] Thomas Chen, Jean-Marc Robert (2004). "The Evolution of Viruses and Worms". Archived from the original on May 17, 2009. Retrieved February 16, 2009.