A Comprehensive Study on Malware Detection and Prevention Techniques used by Anti-Virus

Conference Paper · April 2021

DOI: 10.1109/ICIEM51511.2021.9445322

2 authors:

Rohith Cheerala
Lovely Professional University
3 PUBLICATIONS **31** CITATIONS
SEE PROFILE

Gagandeep Kaur
Lovely Professional University
13 PUBLICATIONS **178** CITATIONS
SEE PROFILE

A Comprehensive Study on Malware Detection and Prevention Techniques used by Anti-Virus

Cheerala Rohith
School of Computer Science Engineering
Lovely Professional University
Punjab, India
cheerala.11606529@lpu.in

Gagandeep Kaur
School of Computer Science Engineering
Lovely Professional University
Punjab, India
Gagandeep.23625@lpu.co.in

2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) | 978-1-6654-1450-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICIEM51511.2021.9445322

***Abstract*—This paper aims to explain and discuss advanced technology used by anti-virus. In this era of the digital world, technology is developing rapidly day by day. Along with technology, Along with the development, cyber risk also increasing; thousands of cyber attacks are taking place every day. Mal- ware (Viruses, worms, Trojans, rootkits, ransomware, Adware, Spyware) is one of the most common cyber-attack. An operating system that has been infected with malware (malicious software) can experience damage. As the name implies, malicious software is a computer program that can infect applications or documents stored in storage media and systems and manipulate applications and data on a computer. In 2020 there are 700 million newmalware emerged and attacked billions of electronic devices. To prevent malware attacks, we need anti-virus/AntimalwareSoftware. In this paper, we discussed various methods of how anti-virus work? What are the advanced techniques used by anti-virus software in this digital era? Comparison between various anti-virus and their methods of detecting malware**

***Index Terms*—Malware, Virus, detection, Anti-virus, Cyber attacks, Cyber crime, Cyber-Security.**

I. INTRODUCTION

As all of us know, anti-virus scans, identifies, and deletes malware from your computer and makes it work properly. Typically, anti-virus uses many types of techniques in virus removal solutions, such as scanning files and matching files to existing virus dictionaries/databases to find matches and to identify unusual computer activity, such as slow performance of computer functions and many more

- How antivirus a suspected malware file.
- How It prevent malware from developing multiply in computer systems.
- Read the identity of the suspected malware file with the creation of an antimalware application.
- How It performs Scaning technique and prevent attack, using (Signature detection programs, Virus Blocking techniques, Cyclic Redundancy check etc.)

II. ANTI VIRUS METHODS

A. *Signature Detection Programs*

This programs look for signature specific to a particular virus in RAM and files and, if detected, issue a corresponding message. The disadvantage of such anti-virus programs is that they only find viruses that the developers of such programs know. This Antivirus are memory-resident programs that capture “dangerous Virus” situations and notify the user. Virus- prone calls include writing to executable files, writing to the boot sector of a disk, and so on. They are directing calls that are characteristic of viruses during their reproduction. Oneof the advantages of blockers is their ability to detect and blocking a virus at the initial stage of their growth [12].

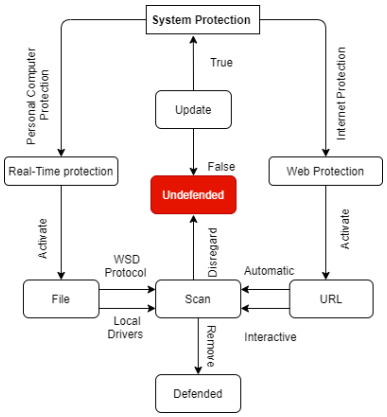

Fig. 1. Working procedures for anti-virus while detecting malicious activity.

B. *Data Analyzing*

Data analyzing includes auditors. The consequences are manifested in data changes that should not be changed. The fact of a data change is a sign of malware for the auditor. Auditors check the integrity of the data and decide on malwarepresence in the computer environment in the event of a breachof integrity.

C. *Virus Blocking Techniques*

These are memory-resident programs that intercept “Dangerous virus” situations and notify the user. Dangerous Virus calls include writing to executable files, writing to the MBR of disks or hard disks, attempting to stay in programs. That is calls that are virus-specific during replication. This include detecting and stopping the virus in the earliest stages of reproduction. Disadvantages include the existence of methods to circumvent blockers protection and many false-positive results [15].

D. *Cyclic Redundancy Check*

978-1-6654-1450-0/21/$31.00 ©2021 IEEE

The operation of Cyclic Redundancy Check is grounded on calculating the checksums of the files on the disk. These Cyclic Redundancy Check amounts are then saved in the anti-virus database and some other information: the length of the file, the date it was last modified. These scanners check the database's data with the actual calculated values. Suppose the information in the file recorded in the database discards the actual values. In that case, CRC scanners indicate that the file has been modified or infected with a virus [8]. CRC scanners cannot catch a virus when it appears on the system, but only after a while when the virus has spread to the computer. CRC scanner cannot detect a virus in new files (email, floppy disks, files recovered from a backup, or extracted from an archive) because their database does not contain information about them. Also, regular viruses take advantage of the flaw in CRC scanners, infecting only recently created files, and thus remaininvisible to them [18].

E. Analytical Scrutinize

These programs are among the most reliable tools for virus protection and remember the initial state of programs, directories, and disk system areas when the computer was not infected with a virus. Then, they occasionally or at the user's request, compare the current state with the original. The detected changes are displayed on the display screen. When comparing, we check the file's length, the cyclic controlcode (the checksum of the file), the modification's date and time, and other parameters. These programs have advanced algorithms, detect stealth viruses, and even clean up changes to the program's scanned version from the changes introducedby the virus. Filters or "Guard" are small resident programs used to detect suspicious activity typical of viruses while your computer is operating [16].

F. Process Analyzing

The heuristic analyzer identifies a series of operations, has a specific "danger" for each of them, and decides based onrisk all of that. This sequence is part of a malicious code. An Additional kind of process based anti-virus is behavior blockers. In this case, the dubious code is executed until theset of actions instigated by the code qualify as dangerousor safe behavior. In this case, the code is partially executed because more straightforward data analysis methods can detect the malicious code's termination. The technologies used inanti-virus programs can be divided into two groups:

- Signature analysis technologies
- Probability analysis technologies

G. Signature Analysis

It is a popular method for detecting viruses and is used in almost every anti-virus. The anti-virus software needs virus signatures to perform the scan, which is stored in the anti-virus database. Because signature analysis involves checking file signatures for viruses, the anti-virus database must be updated regularly to keep the anti-virus up to date. The working principle of signature analysis itself determines the limits ofits functionality, only the ability to detect known viruses. The signature-based scanner is userless against new viruses. The presence of virus signatures includes the ability to heal infected files detected by signature analysis. However, not all viruses are curable - most Trojans and worms are not curable because of their design characteristics. These are integrated modules that cause damage [16].

H. Probabilistic Analysis Technologies

However, probabilistic analysis technologies can be divided into three categories:

- Heuristic analysis
- Behavioral analysis
- Checksum analysis

1) *Heuristic analysis:* It is a technology-based on probabilistic algorithms that result in identifying suspicious objects.During the heuristic analysis, the file structure and compliance with the virus patterns are checked. The most common heuristic analysis is to verify the data of a file to modify already known virus signatures and their combinations. This helpsdetect new versions of hybrids and previously known viruses without further updating the anti-virus database. Heuristic analysis is used to detect unknown viruses, and consequently, no cure is required. This technology is not able to 100 percent determine the virus in front of it or not. Like all probability algorithms, it has false-positive results.

2) *Behavioral Analysis:* Behavioral analysis is a technology in which an inspected object's nature is decided based on an analysis of the operations it performs. Behavioral analysis can be applied very narrowly in practice. Scripts and macros are the most famous behavioral analyzers. The suitable viruses almost always perform several similar operations. Protection built into the BIOS can also be classified as a behavior analyzer. When an attempt is made to change the computer's MBR, the parser blocks the operation. It displays an appropriate notification to the user. Behavioral analysts can also track experiments with direct access files, make changes to the floppy disk boot record, format hard disks. Behavioral analyzers do not use additional objects, such as virus databases, to operate and cannot distinguish between known and unknown viruses. Similarly, the behavior of devices that implementbehavioral analysis technologies does not involve treatment [17].

3) *Checksum analysis:* Checksum analysis is a way to track changes in computer system objects - concurrency, mass, the exact change in the file length - we can conclude that the system is infected checksum analysts (also known as "change checkers"), like behavioral analysts. Similar technologies are used for on-access scanners - the checksum is removed from the file during the first scan and cached. The amount is removed again before the following scan of the same fileis compared. If there is no change, the file is considered uninfected.

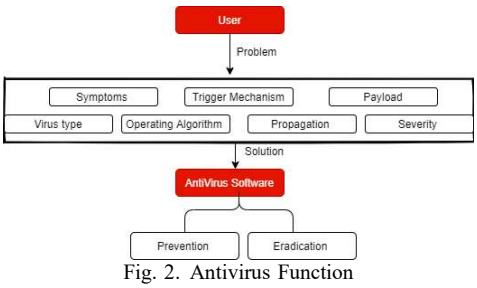

Fig. 2. Antivirus Function

I. *Antivirus Complexes*

Anti-virus complexes a set of anti-viruses using the same anti-virus kernel or kernels to solve practical problems related to the security of anti-virus systems on computer systems. The anti-virus complex necessarily includes tools to update anti-virus databases. The anti-virus package may also include behavior analyzers and change monitors that do not use the anti-virus engine. The following types of anti-virus complexesare distinguished:

- Antivirus to protect complex workstations.
- Antivirus is involved in protecting file servers.
- Antivirus is involved in protecting mail systems.
- Antivirus is complex to protect gateways.

1) *Monitoring Antivirus:* "Monitors" (or filtering programs) are anti-virus programs that use a virus signature database to detect viruses. The anti-virus monitor is in the computer's memory and scans only programs that have been tampered with by the user or the operating system. Anti-virus monitors typically scan all files for the following manipulations:

- Launching the program for implementation.
- Change the properties of the file.
- Opening document (Microsoft Office)
- Copy or move a file.
- Edit the file.

Screening programs are helpful because they help the user recognize the virus in the initial stage of its existence before the virus spreads in the form of an epidemic.

2) *Heuristic Analyzers:* - Programs that run scanned programs under their control and detect virus-specific actions. As a result, heuristic analysts are just as easy to find "polymorphic" viruses as common viruses that do not usea masking mechanism, in addition to being able to detectviruses that were not previously known to the makers of an anti-virus program. The technique contains mimicking a program's execution by the processor and sliding fictitious control resources into the virus. In this way, a virus that is deceived under the control of an anti-virus program decrypts its code. The scanner then compares the decoded code withthe codes in the scan database.

J. *Basic Methods for detecting viruses*

Anti-virus programs have evolved in parallel with the development of viruses. As new technologies for creating viruses appeared, the mathematical devices used to develop anti-virus products became more sophisticated. The first anti-virus algorithms were based on a comparison with a reference value. The idea of the algorithm is to use statistical methods. The mask must be small for the file size to be acceptable and large enough to avoid false-positive results (when the "friend" is perceived as a stranger, and vice versa). The first anti-virus program based on this principle knew several viruses and could cure them. These programs were created as follows: the developer, after receiving the virus code (the virus code was initially static), compiled a unique mask using this code (10–15-byte sequence) and entered it into the database of the anti-virus program. The anti-virus program scanned the files. This sequence (signature) was chosen tobe unique and not to occur in the standard data set. Most anti-virus programs used the approaches described until the mid-1990s when the first polymorphic viruses appeared that changed their bodies according to unpredictable algorithms. The signing method was then supplemented with a so-called processor emulator, making it possible to find encrypted and polymorphic viruses which don't have a constant signature in a specific form [15]. The principle of processor emulation is shown in the figure. One. Suppose a conventional chain usually consists of three main elements: CPU OS Program. The emulator is about reproducing the program's work in some virtual space and reconstructing its original content. The emulator can constantly interrupt the program's execution,monitor its activity without disturbing anything, and call the anti-virus program. The second mechanism that emerged in the mid-1990s and was used by all antiviral viruses is heuristic analysis. A processor is an emulation tool that allows it to squeeze out the analyzed program's operations does not always allow these operations to be searched but allows individual analyses to be performed. A hypothesis such as "virus or not" to be put forward. Virus?" In this case, decision-making is based on statistical approaches. The appropriate program is called a heuristic parser. To reproduce, the virus must performany specific operation: copying to memory, writing to sectors. The

heuristic analyzer (part of the anti-virus engine) containsa list of such operations, looks at the program's executable code, determines what it does, and decides based on that. Is this program a virus or not? However, the percentage of virus absence, not even known to an anti-virus program, is tiny. This technology is now widely used in all anti-virus programs.

III. An Overview Of The Most Popular Personal Antiviruses

The review includes the most popular personal anti-virus for personal use by five known developers. It must be observed that some of the businesses reviewed below offer many kinds of personal programs that differ in terms of functionality and, accordingly, price. Our review examined one product from each company, selecting the most functional version, commonly referred to as Personal Pro. Other personal anti-virus options can be found on the appropriate websites.

A. Features of Antivirus Programs

Detection programs allow viruses to be searched and detected on randomly accessed memory and external media and issue a corresponding message after detection. There are universal and unique detectors. Universal detectors check the immutability of files as they work by counting and comparing them to a checksum standard. The disadvantage of universal detectors is that it is impossible to determine the causes offile corruption. Detectors scan for known viruses based on their signature. The trouble with these detectors is they can not detect all known viruses. A detector that detects multiple viruses is called a poly detector. The disadvantage of such anti-virus programs is that they only find viruses that thedevelopers of such programs know about. AV programs find files infected with viruses and "cure" them, i.e., remove the virus strain from the file and restore them to their original state. At the beginning of their work, they look for viruses in RAM, destroying them, and only then continue to "heal" the files. Due to the constant emergence of new viruses, detector programs are rapidly becoming obsolete. Their versions need to be updated regularly. Auditor programs are among the mostreliable anti-virus tools. The scanners remember the initialstate of programs, directories, and disk system areas whenthe computer was not infected with a virus. Then, from timeto time or at the user's request, compare the current state with the original state. The detected changes are displayedon the display screen. When comparing, we check the file's length, the cyclic control code (the checksum of the file), the modification's date and time, and other parameters. Auditor programs have advanced algorithms that detect stealth viruses and can distinguish changes to the program's scanned version from those performed by the virus. Filters are small resident programs used to detect suspicious activity typical of viruses while your computer is running.

B. Kaspersky Anti-Virus

Anti-virus products can be classified according to several aspects simultaneously, for example, anti-virus technologies used, product functionality, target platforms. Anti-virus technologies used:

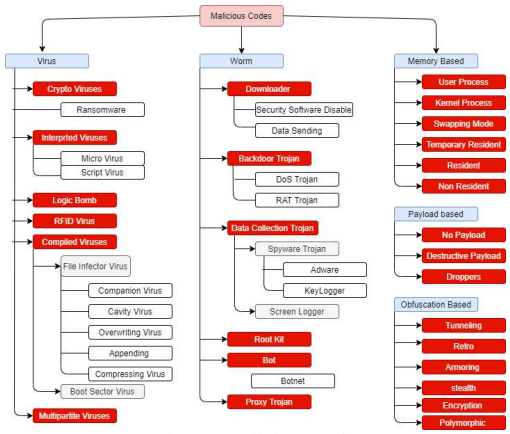

Fig. 3. Malicious code

- Classic antivirus products (products that use a signature-recognition method only).
- Proactive antivirus products (products using proactive antivirus technologies only).
- Combined products (both classical and signature-based protection methods and proactive products are used).

By product functionality:

- Antivirus products (antivirus products only).
- Combined products (products that provide not only protection against malware but also spam filtering, encryption and data backup, and other features).

According to target platforms:

- Antivirus products for the Windows family of operating systems.
- Antivirus products for the macOS family.

Antivirus products for enterprise users can also be classified according to protection objects:

- Antivirus products to protect workstations.
- Antivirus products to protect file and terminal servers.
- Antivirus products to protect mail and Internet gateways.
- Antivirus products to protect virtualization servers.

C. Norton Antivirus (Manufactured by Symantec)

One of the most famous and popular anti-viruses. The virus detection rate is very high (close to 100). The program uses a mechanism that allows the detection of new unknown viruses. Norton Antivirus includes LiveUpdate, which allows

you to update your program and set of virus signatures over the Internet at the touch of a button. The Antivirus Wizard pro- vides detailed information about the detected virus and offers achoice: automatic or more careful removal of the virus step by step, which allows you to view each of the actions performed during the removal process [13]. This program's disadvantage is its complexity (although it is practically unnecessary tochange the default settings).

D. *McAfee Virus Scan (Manufactured by McAfee Associates)*

This is one of the best-known anti-virus packs. It eliminates viruses extremely well, but it is inferior to previous packages when new types of viruses are detected. You can scan allfiles or just software; you can or may not distribute files compressed by the scan process. It has many functions for using the Internet [7].

E. *Antiviral Toolkit Pro (Manufactured by Kaspersky Lab)*

This anti-virus is recognized worldwide as one of the most trusted. Despite its ease of use, it has all the arsenals needed to fight viruses. The heuristic mechanism, redundant scanning, scanning of archives, and compressed files are not a full ability. Kaspersky detects the appearance of new viruses and releases anti-virus database updates promptly. There is a resident monitor to monitor executable files [6].

IV. CONCLUSION

Anti-virus is a specialized program designed to protect the operating system from viruses, spyware, hacker attacks, and other unauthorized access to steal valuable personal data or unauthorized computer management. Anti-virus programs canbe classified according to the protection technologies used, the product's functionality, and the target platform. Anti-virus detectors find files infected with anti-virus, and if detected,a message is displayed. It treats infected programs or media, destroys the virus code, restores the program to the state in which it was before the virus infection. The auditors analyze the state of the files and compare it with the original state of the file. If discrepancies are detected, the user is notified. It canbe download directly to RAM and intercept and report viral calls to the system. The advantages of such programs include the ability to detect unknown viruses. Vaccine programs modify programs and media so that it is not reflected in programs' operation, and the virus considers programs and media already infected. Under current conditions, it is almost impossible to prevent infection with viruses because it is unnecessary to use computer networks, flash drives, pirated software, and more. Statistics show that every computer is infected with a virus. That is why the leading and most reliable preventive measure is data backup. There are many anti-virus programs, but there is no 100 percent protection against computer viruses. After all, dozens of new computer viruses appear in the world every day. The process of developing anti-viruses takes some time. The virus program causes the most damage and significant damage.

REFERENCES

[1] Bettany, A., Halsey, M. (2017). Windows Virus and Malware Trou-bleshooting. Berkeley, CA: Apress. doi:10.1007/978-1-4842-2607-0

[2] Bitdefender. (2018, February 6). Retrieved from Bitdefender Total Security 2018 User's Guide https://download.bitdefender.com/resources/media/materials/2018/userguides/en EN/ bitdefender ts 2018 userguide en.pdf

[3] ESET. (2018, March 3). Retrieved from ESET Smart Security Premium User Guide: https://download.eset.com/com/eset/apps/home/essp/windows/latest/eset essp 11 use rguide enu.pdf

[4] Futuremark. (2018, April 20). Retrieved from PCMARK: https://www.futuremark.com/benchmarks/pcmark

[5] P. Singh, A. Kaur, G. S. Aujla, R. S. Batth and S. Kanhere, 2020"DaaS: Dew Computing as a Service for Intelligent Intrusion Detectionin Edge-of-Things Ecosystem," in IEEE Internet of Things Journal, https://doi.org/10.1109/JIOT.2020.3029248 https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky Se-curity Bulleti n 2016 Statistics ENG.pdf

[6] Kaspersky. (2015, June 20). Retrieved from Kaspersky Total Security User Guide: https://media.kaspersky.com/usa/documentation/kts2016 userguide en.pdf? ga=1.11 7583625.1421756489.1435137987

[7] McAfee . (2017, September 4). Retrieved from How did my system get infected when I have McAfee software installed?: https://service.mcafee.com/webcenter/portal/cp/home/articleview?locale=enGBarticleId=TS100771

[8] Microsoft. (2017, November 20). Retrieved from Windows Defender Antivirus in Windows 10 and Windows Server 2016: https://docs.microsoft.com/enus/windows/security/threat-protection/windows-defender-antivirus/windowsdefender-antivirus-in-windows-10

[9] Microsoft. (2018, March 30). Retrieved from Shop Windows 10 : https://www.microsoft.com/en-us/store/b/windows?activetab=tab:shopwindows10

[10] X. Ren, G. S. Aujla, A. Jindal, R. S. Batth and P. Zhang, "Adaptive Recovery Mechanism for SDN Controllers in Edge-Cloud supported FinTech Applications," in IEEE Internet of Things Journal (2021). https://doi.org/10.1109/JIOT.2021.3064468

[11] Nayyar, A., Batth, R.S., Ha, D.B., Sussendran, G., 2018, Opportunistic Networks: Present Scenario- A Mirror Review, International Journal of Communication Networks and Information Security 10.

[12] Souppaya, M., Scarfone, K. (2013). Guide to Malware Incident Preven- tion and Handling for Desktops and Laptops. Gaithersburg, MD: Na- tional Institute of Standards and Technology. doi:10.6028/NIST.SP.800-83r1

[13] Thamsirarak, N., Seethongchuen, T., Ratanaworabhan, P. (2015). A Casefor Malware that Make Antivirus Irrelevant. Hua Hin, Thailand: IEEE. doi:10.1109/ECTICon.2015.7206972

[14] Zeltser, L. (2011, October). How antivirus software works: Virus detection techniques. Retrieved from SearchSecurity: http://searchsecurity.techtarget.com/tip/Howantivirus-software-works- Virus-detection-techniques

[15] Eytan, D., 2021. True CDR. [online] odix Content Disarm and Reconstruction (CDR). Available at: ¡https://www.odix.com/news/blog/true- cdr-the-next-generation-of-malware-prevention-tools/¿

[16] Aslan, O., Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. IEEE Access, 8, 6249–6271. https://doi.org/10.1109/ACCESS.2019.2963724

[17] "Techniques for Detecting Malware and Malicious Ad Code — GeoEdge", GeoEdge, 2021. [Online]. Available:

https://www.geoedge.com/university/techniques-for-detecting-malware-malicious-ad-code/.

[18] Rubenking , N. J. (2018, March 7). The Best Antivirus Protection of 2018. Retrieved from PCMag: http://uk.pcmag.com/antivirus-reviews/8141/guide/the-best-antivirusprotection-of-2018

[19] Wang, C., Batth, R.S., Zhang, P., Aujla, G.S., "VNE solution for network differentiated QoS and security requirements: from the perspective of deep reinforcement learning". Computing (2021). https://doi.org/10.1007/s00607-020-00883-w

[20] G.S Shahi, R.S Batth, S. Egerton, 2020 "MRGM: An Adaptive Mecha- nism for Congestion Control in Smart Vehicular Network", InternationalJournal of Communication Networks and Information Security.

[21] Pfleeger, C. P., Pfleeger, S. L., Margulies, J. (2015). Security in Computing. Upper Saddle River, N.J: Prentice Hall

[22] Garnaeva, M., Sinitsyn, F., Namestnikov, Y., Makrushin, D., Liskin, A. (2016). Kaspersky Security Bulletin Overall Statistics for 2016. Retrieved from kasperskycontenthub.