An Analysis of Computer Virus and Detection Methods Comparison

Chetan N. Rathod [1], Bhumika K. Charnanand [2]
[1]Vivekanand College for BCA, Surat
[2]Smt. Z.S. Patel College, Surat

Abstract:

Large organisations today have to manage big data that is dispersed throughout the globe. A virus is a type of programme that seriously compromises the system. Because of this, security is now a top concern for all businesses. These days, the most valuable resource for anyone is data which requires a variety of maintenance measures to safeguard those assets. Maintaining system security is becoming increasingly difficult as different types of viruses, such as malware, trojans, hackers, and adware, become more and more common. The prevalence of the internet in our daily lives is growing, and with it comes the ever-growing risk of various threats. Different viruses can be caught by different mechanisms, which calls for careful analysis. This paper presents a brief overview of different types of virus detection techniques and the effects they have on the system. This will assist in comprehending the advantages and disadvantages of every virus following the survey. A conclusion and some advice on how to avoid the virus in a sizable virtual world are provided at the end.

Keywords:

Virus, Virus Detection, Signature-Based Virus Detection, Anomaly-Based Detection, Trojan

Introduction:

A computer virus is a programme that has the capacity to replicate itself without the help of a human, and once it has, it can continue the process indefinitely [2].Consequently, a programme that refers to something that operates against the specified specification is considered harmful code[3].Numerous malicious code or programmes exist that are intended to carry out unauthorised or unlawful tasks that can seriously damage the system. Malicious software comes in many forms and is commonly referred to as viruses, trojans, worms, and so on. Three different subroutine types can be found in a computer virus. Similar to how a typical virus causes illness in our bodies, computer viruses are designed to spread throughout the system without leaving any behind signs. Through attachment to other system programmes, such as some application software, the virus affects the system. As a result, it occasionally enters the system and affects the boot media or hard drive. These viruses are extremely deadly. The most dangerous effects occur when a virus takes control of an application, such as the browser, modifies its settings, or modifies the system date. In these cases, it can be challenging for a user to identify the issue. Viruses can also occasionally delete a significant amount of data, and in the worst case, they can corrupt or crash the entire system. A wide variety of viruses exist. Viruses infect systems by acting like parasites. These programmes come in the form of files with the extension.exe or.com that manage other programmes. Upon clicking the.exe file on the computer, a virus may infiltrate the system, causing it to malfunction and necessitate a fresh format.

Boot sector virus

Numerous boot sector virus formats exist. They are significantly more numerous than all kind of computer viruses. The most dangerous one up to presently. A well-known boot sector virus is Michelangelo. They're hard to find. This kind of virus has no effect on the system's regular functionality silently and consistently impacts the removable media, such as floppy discs. The virus takes over the machine. Consequently, when the bootable media loads the virus before the operating system loads, take control of the system. It targets RAM, which targets the hard drive, causing the system to restart.

Trojan Horses

It is a dangerous code that attempts to enter the system through a backdoor without the normal user's knowledge, just like any other software programme. Reformatting is actually required at that point because, after a certain amount of time, the user sees an error and is unable to access the disk's normal data. Occasionally, the antivirus programme is unable to identify the Trojan horse. Many notable individuals have stated that Trojan horses do not behave like other viruses because they inflict damage much more quickly than other viruses [4].Nuker, Back Office, and Netbus are a few examples.

Stealth Viruses

Similar to stealth viruses, which are so powerful that they are difficult for radar or other anti-virus software to detect, we may be familiar with the name of stealth aircraft, which are designed specifically to hide from radar. This is what makes them so powerful—even though they could be on boot media or in any other area of the system, no scanner can find them. It stays in the computer memory that is always keeping an eye on the system. A virus infects a file when a user opens it on the computer. The virus then automatically erases the infection from the system, rendering the user untraceable. As a result, the computer will boot normally but slowly. It also deletes some data, which causes the system to slowly shut down. They are difficult to detect in the boot sector because they keep moving it around.

When a user clicks on an advertisement on a computer, this type of software affects the system. When someone clicks on the advertisement, the virus that has been injected into it will infect the computer. As a result, it infiltrates the system together with some malware and other dangerous apps that can quickly take over the system with the aid of this adware [5].For instance, Adblaster, DeskAd, and Clickbank

Adware

When a user clicks on an advertisement on a computer, this type of software affects the system. When someone clicks on the advertisement, the virus that has been injected into it will infect the computer. As a result, it infiltrates the system together with some malware and other dangerous apps that can quickly take over the system with the aid of this adware [5].For instance, Adblaster, DeskAd, and Clickbank

Metamorphic Virus

This type of virus targets networks that are difficult to monitor. They alter both their structure and code, which results in the emergence of a new virus that does harm but that no one can precisely identify because their signatures have changed and are no longer technically able to match [6] [7].After a while, it reverts to its initial structure before altering its internal composition once more and taking on a new form to create a new virus[2].

Other virus

Numerous other malware and viruses exist, including botnets, logic bombs, rabbits, and scare ware. There are numerous methods for obtaining the virus, and a multitude of antivirus programmes are at one's disposal. The most widely used security programmes employ potential scanning and require daily updates in order to function properly. The various tools installed in the system identify and eliminate the virus following a thorough scanning of the system. The antivirus service is better the more expensive it is.

The dangers posed by operating system viruses:

Every operating system has some vulnerabilities. Any virus simply takes advantage of the holes in the system to access both the system's application and system software, and it then spreads relentlessly until the entire system collapses. However, operating systems such as UNIX are still difficult for viruses to infiltrate and gain access to their roots, whereas Microsoft Windows is more vulnerable to a wide variety of viruses. Numerous quick updates in Linux render the system totally uninhabitable by viruses. Samba and NFS servers are two instances of Linux versions that maintain the document in an undocumented manner. Malicious code can occasionally be used to access Linux servers, attacking their scripts to allow any guest login to access them.

Techniques for detecting viruses:

There are various methods for detecting viruses, and these work as follows:

Signature-based Virus Detection

This is the most widely used technique for virus identification in all modern anti-virus software. The antivirus programme calculates the signature of a known virus based on information found in the virus file, and it stores all of these signatures in its database.[8] During the virus scan, the programme computes the signature that is already in the system based on the file's data and compares it with the signature that is already in the database. The antivirus software marks a file as infected and deletes it if the signatures match those in the database. This type of software's accuracy is contingent upon the frequency of database updates [10]. However, virus writers come up with new ways every day to modify the code, preventing antivirus software from detecting the virus and allowing it to continue hiding. Sometimes a virus mutates itself after infecting a file, making it difficult to trace and sometimes impossible to identify. Every time, the mutation carries out the same type of operation as its parent. Another name for this type of virus is self-mutating virus [9].There is very little possibility of a false alarm with these kinds of techniques. The only prerequisite is to maintain an up-to-date database with every virus signature. The signature that is in the database determines the ideal outcome. A new virus is typically not detected by it because its signature is not stored in the database. Here, the input file's signature is obtained by following the opcode pattern.

Anomaly based virus detection

This type of detection technique searches the host computer for any unusual activity. The system sounds an alert and warns users of the potential for malware or viruses if any suspicious activity is found [10].False alarm rates can occasionally be higher, but this is advantageous for users as it increases the risk of contracting a new virus. In this case, setting off the alarm is not as risky as letting a fresh virus infect the system. Any hacker group may occasionally be able to access the alarm system and turn abnormal behaviour into the norm [11]. Consequently, in this instance the system is unable to identify the anomalous behaviour [10]. An anomaly is defined as something that is abnormal. It is not even necessary to worry about the database being updated when a new type of malware or virus is discovered. Monitoring network activity only requires minor maintenance; the more a system is used, the higher the risk of contracting a virus. As the system develops its profile, there are moments when the network is unsafe. Any virus activity that appears to be normal won't raise an alarm. Therefore, even minor checks, like routing checks or email checks, can trigger a signal alarm which is among the drawbacks of these kinds of detection methods.

Code emulation

The best method for detecting viruses is this one. To mimic CPU and memory activities for the code activity, a virtual machine is present. This type of code is not safe enough because it jumps out of the environment during analysis. Instead, it uses a debugger interface to trace the code along with the processor. This type of method is more effective at combating encrypted and polymorphic viruses [12].

Virus specific detection

Sometimes the specific algorithm is unable to identify the virus. In these situations, the detection process is implemented using a virus-specific detection algorithm. Although this type of technique is not widely used, it is employed in specific situations to infect a particular type of virus. We refer to this type of detection as algorithm detection method. However, algorithm scanning is generally not used in favour of virus-specific detection because it can be misleading [13]. Its portability, stability, and platform-related issues are among its many shortcomings. Because of this, simple virus scanning languages have been developed, allowing for clear reading and seeking operations.

Filtering

By using this technique, the anti-virus program's scanning speed can be increased. This is employed in some virus detection techniques due to their lengthy processing times and intricate workings. Based on the signature, the virus can identify the infected file as.com,.exe, script, boot sector, and many other file types as it spreads executable files infect both.exe and.com files. The scanning time is reduced by using only the signature.

Solution for Virus Issues:

In addition to employing antivirus software, there exist additional protocols that aid in safeguarding against viruses. Among them are

- Virus scans that are scheduled and updated should be performed at least once a week on every computer in the company.
- Software patches can be downloaded from websites and kept up to date with certain updates.
- Use licenced versions of all software; avoid using tools, patches, or cracked software as they may contain malware or viruses.
- Never grant someone administrative access as this could make them more susceptible to infection.
- Avoid using free antivirus software as it does not support the entire functionality of the programme; a paid version is required.
- Maintain enough data backups in case you need to restore the system because of an infection.
- If the system has already been infected with a harmful virus, the best course of action is to format the system.

Comparison

Every technique for detecting viruses has its own set of benefits and drawbacks. It is a useful tool for signature-based detection since it matches the signature in the database. For the best outcome, it is both highly effective and extremely simple. Its inability to identify newly discovered viruses arises from an outdated database. On the other hand, anomaly-based detection works well for any aberrant system function and can identify novel virus types without requiring database updates. It occasionally fails to remove the unaffected files as well. There is no better method for detecting encrypted viruses in the system than the code emulation technique, which is highly effective for polymorphic or encrypted viruses. However, these kinds of techniques are more complex. The technique of code emulation is highly expensive to implement. When a specific algorithm is needed to identify a certain type of virus, a virus detection method is employed. Numerous methods are ineffective against unidentified viruses [14].Additionally, it takes longer to scan the system, which occasionally prevents viruses from being found. However, many known viruses can be found with ease, though not all viruses can be detected with ease. It can be very challenging to identify viruses that behave normally using the anomaly base technique [14].

Conclusion

Even though antivirus software is updated every day, virus authors continue to update and modify their code, leaving the system more open to intrusions. The latest methodologies for anti-virus software are only released into the market after a virus has infected a system. This suggests that significant advancements in virus detection techniques are still needed. Large networks now need to be watched out for malware, virus, trojan, and other types of attacks. In order to prevent the virus from erasing any important data belonging to any organisation, it must first be removed. In the latest technologies, it is also necessary to reduce time complexity and take hardware quality into account before implementing high-quality software, as this lowers the likelihood of being infected by malicious software. Businesses should put more of an emphasis on research and development because, in the current environment, tech expertise is needed.The anti-virus companies should provide basic security training to the general public on their systems.It may lessen the likelihood of contracting an infection.

Reference:

[1] Dr. Prof. Milind. J. Joshi , Mr. Bhaskar V. Patil ,Shivaji University Kolhapur, Kolhapur M.S.], INDIA,Computer Virus: Their Problems & Major attacks in Real Life,ISSN: 2249-2615

[2] Dr. Solomon's Virus Encyclopedia, 1995, ISBN 1897661002

[3] Dr. Klaus Brunnstein 1999, from Antivirus to Antimalware Software and Beyond http://csrc.nist.gov/nissc/1999/proceeding/papers /p12.pdf

[4] H. Shravan Kumar, "Seminar Report on Study of Viruses and Worms",Indian Institute of Technology Bombay, 2005.

[5] K. Mathur, S. Hiranwal, "A Survey on Techniques in Detection and Analyzing Malware Executables", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3, Issue 4, April 2013

[6] Hossein Bidgoli, Handbook of Information Security, Volume 3,1st Edition, John Wiley & Sons, ISBN-10: 0471648337, ISBN-13: 978-0471648338, December, 2005

[7] S. Venkatachalam, M. Stamp, "Detecting Undetectable Metamorphic Viruses", Proceedings of the 2011 International Conference on Security & Management (SAM 2011), pp. 340-345, 2011,ISBN-10: 1-60132-196-1.

[8] D.RAKESH, L. PADMALATHA,PATTERN MATCHING ALGORITHM USING FILTER ENGINE AND EXACTMATCHING ENGINE, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)VOL. 1 ISSUE 7, SEPTEMBER – 2012

[9] Min Feng Rajiv Gupta, Detecting Virus Mutations Via Dynamic Matching, CSE Dept., University of California

[10] Ankush R Kakad, Siddharth G Kamble, Shrinivas S Bhuvad, Vinayak N Malavade , Study and Comparison of Virus Detection Techniques , Volume 4, Issue 3, March 2014 , ISSN: 2277 128X

[11] Jan Hruska. Computer Viruses and Anti-VirusWarfare. Ellis Horwood, Chichester, England,

[12] Wing Wong, ANALYSIS AND DETECTION OF METAMORPHICCOMPUTER VIRUSES, A Writing Project Presented toThe Faculty of the Department of ComputerScienceSan Jose State University.

[13] Szor, P., The Art of Computer Virus Research and Defense, Addison-Wesley Professional, 2005.

[14] ESSAM AL DAOUD1, IQBAL H. JEBRIL2AND BELALZAQAIBEH, COMPUTER VIRUS STRATEGIES AND DETECTIONMETHODSESSAM ,INT. J. OPEN PROBLEMS COMPT. MATH., VOL. 1, NO. 2, SEPTEMBER 2008.