Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study and Comparison of Virus Detection Techniques

Ankush R Kakad, Siddharth G Kamble, Shrinivas S Bhuvad, Vinayak N Malavade
Computer Science
India

Abstract- Computer virus is a program that can propagate (replicate) its own copy to other non-malicious program by modifying them without user permission. It is name so because it acts like virus that infects healthy program and antivirus is a program use to detect these viruses to protect the good program form virus. Antivirus tries to remove viruses code and restore original program. An antivirus uses various methods for detecting viruses. As characteristics of different viruses are dif rent there detection method are also different. All type of viruses cannot be detected by any single method. This paper describes what is virus how it is affect the good program and review current methods of virus detection and describe problem facing by current antivirus. Finally end with the conclusion that virus detection by signature scanning simple to implement, economical and commonly used tool for virus detection

Keyword: virus; antivirus; Signature based virus detection; Anomaly Based Detection; Code Emulation;

I. INTRODUCTION

A computer virus is a computer program which can propagate (replicate) itself without the user's consent. It spread at geometric rate, eventually infecting the entire system and spreading to other connected system. Usually, it has malicious intent, e.g. The virus which affects the performance of the system. Virus can be categorized as transient or resident.

A. Transient Virus:

Its life depends on the life of its host. It run when host is executed and it is terminated when attached program end. During its execution, it may infect other program.

B. Resident Virus:

It locates itself in memory. It remains active as a standalone program even if its host program has ended.

Anti-virus software's are used to detect and remove computer viruses or kill the virus and also try to reduce the effect of virus on any data[5]. Existing commercial antivirus software use different virus scanning algorithms e.g.(signature, heuristic).Anti-virus software employed different technique in examine, scanning, and detecting viruses to provide sufficient safety for computer systems. In the next section, we discuss a different type of viruses and scanning methods to find this virus. It helps us to understand the advantages and disadvantages of each method and differentiate them. In the last section, we end with a conclusion and some recommendations.

II. TYPES OF VIRUS

A. Simple virus:

Simple virus replicates itself. It is the easiest to detect. If a user launches an infected program, the virus gain control of the computer and attaches a copy of itself to another program file. After attaching a copy of itself to another program file, virus transfers its control back to the host program, which runs normally.

B. Encrypted Viruses:

The aim of encrypted viruses is change of the virus body with some encryption algorithms to hide it from simple view and make it more difficult to analyze and detect by antivirus. Encrypted viruses contain mainly two parts, the encrypted body of the virus, and a small decryption code program. While the execution of the infected program first the decryption loop executes and decrypts the main body of the virus program. Then, it moves the control to the virus body.[4]

C. Oligomorphic virus:

Virus writer quickly realize that detection of an encrypted virus remains simple for antivirus software as long as the code of encryption itself is long enough and unique enough. To challenge the antivirus product further they decide to implement technique to create mutate decryption. Unlike virus do changes encrypted virus oligomorpheic viruses do change their descriptor is new generation .The simplest technique to change the decryptor is to use a set of decryptor instead of single one the first known virus to use this technique was wahale. Wahale carried a few dozen different decryptor, and virus picked one randomly.

D. Polymorphic Viruses:

In anti-virus software's and tools mostly use signature-based scanning to identify the viruses .To avoid this detection, virus can change some instructions in new generation and overcome the signature scanning. Polymorphic viruses use this concept. When the virus decides to infect new data, it changes some instruction of its body to look different from previous [6].

E. Metamorphic Viruses:

Metamorphic Viruses can increase its code indifferent way so that it appears differently in each infection. This viruses are more difficult to detect for Example involuntary, stimulate, cascade, phoenix, evil, prod, virus101. This virus changes its code at each infection by using various code obfuscation techniques. These techniques are performed on both the data section and the control flow of an assembly program. Control flow obfuscation technique involves unconditional jump instructions and instruction reordering. Data flow obfuscation is achieved by transposition, equivalent instruction substitution, register renaming, and subroutine permutation. This makes it more resistant to code emulation detection technique. Unlike polymorphic viruses, encryption is not used in metamorphic viruses. The metamorphic virus has different boy structures with same functional behavior [2]

III. VIRUS DETECTION METHOD

There is several detection methods there function and working is explain below.

A. Signature based virus detection

Signature based virus detection is the most common technique that is employed in traditional antivirus software for identifying viruses. In this type of Antivirus software signature of some known virus calculated from the content of virus file and that signatures are store in the database of antivirus software.[1] When antivirus software scans for viruses, it compute the signatures of file that present in the system according to contents of the file and compare that signature with the signature present in the database. If signature of calculated file is match with the database present in the antivirus software at that time Antivirus software declare that file as a infected file and delete that particular file.The easiest way to create signature for virus is to use hash algorithm (md5, sha_1), Example of such a virus is given below. To create a signature for virus.exe use the md5 hash algorithms signature of virus.exe can be 48d4533230a1ae1s118c741c0db19.However the accuracy of this type of antivirus scanning is depend on update database. As the antivirus software technology developer, the virus creator also develops ways to hide their viruses. One way is that the virus creator can regularly change the virus codes, in order to hide the viruses from the antivirus software. Another more sophisticated way is to create a virus which can avoid detection by mutating itself each time it infects a new program. Each new mutation essentially performs the same task as its parent. This type virus is called a self-mutating virus [3].

Advantage of Signature based virus detection:

- This type of method is simple to implement.
- Give accurate result.

Disadvantage Signature based virus detection:

- A simple virus has static signature, the virus which consists of a sequence of instructions which are unique at every infections. So it detect only simple virus. Antivirus software which employee this technique required more space to store signature database.

B. Anomaly Based Detection:

Anomaly is defined as something which is not normal. Anomaly based virus detection systems monitor the processes on a host machine for any abnormal activity. If any activity is identified which is not normal, the system inform about the possible presence of malware. It is more reliable because it is also capable of detecting new viruses. The important thing to note is that raising a false signal is not as potential harmful as allowing a new virus [6].

Advantages of Anomaly Based Detection:

- New threats can be detected without having to worry about database being up to date Very little maintenance once system is installed it continues to learn about network activity and continues to build its profiles. The longer the system is in use the more accurate it can become at identifying threats

Disadvantages of Anomaly Based Detection:

- The network can be in an unprotected state as the system builds its profile. If malicious activity looks like normal to the system it will never send an alarm. False positives can become possible with anomaly based detection. Normal usage such as checking e-mail after meeting has the potential to signal an alarm.

C. Code Emulation:

Code Emulation is an extremely powerful virus detection technique. a virtual machine is implemented to simulate CPU and memory activities to mimics the code activity. Some early method of code emulation use debugger interface to trace the code using the processor however such a solution is not safe enough because the virus code can jump out of emulated environment during analysis. Code emulation is a very powerful technique, particularly in dealing with encrypted and polymorphic viruses [4].

Advantage Code Emulation:

- Code emulation can also be applied to metamorphic viruses that use single or multiple encryptions.

Disadvantage Code Emulation:

- Code emulation can become too slow if the decryption loop is very long,

IV. COMPARISION OF VIRUS DETECTION METHODS:

Table I. Comparison of Virus Detection Methods

Methods /Parameter	**Signature based virus detection**	**Anomaly Based Detection**	**Code Emulation**
Strength	Efficient	New malware	Encrypted viruses
Limitation	New malware	Unproven	Complex
Cost	Low	Costly to implement	Costly to implement
Accuracy	More if database is updated	Less	More

We here compare three methods of virus detection that is Signature based virus detection, Anomaly Based Detection, Code Emulation on the basis of parameter which is given in table. Strength of Signature based virus detection is better because it depend on comparing the signature. Anomaly Based Detection is best for the detection of new viruses, while Code emulation is best for detection of encrypted viruses. Limitation of Signature based virus detection that it cannot detect new malware when database is not updated. Limitation of Anomaly Based Detection technique is that some time it delete unaffected file also. Limitation of Code Emulation is that this method is very complex to implement.

Cost of Signature based virus detection is low it require only database to store the signature of viruses. Anomaly Based Detection method require monitoring the activity of process each time which is more costly and time consuming. Code Emulation is costly method it require implementation of virtual machine to detect virus.

Accuracy of Signature based virus detection is more if database is updated. in Anomaly Based Detection is not always possible to get correct result by only monitoring process activity some time it can give wrong result. Accuracy is more in Code Emulation method because It implements virtual machine to detect the viruses.

V. LIMITATION OF CURRUNT ANTIVIRUS*:*

Detection Methods have some major problems. Most of technique is good against known viruses and not very good against unknown or new viruses [2]. Secondly, they tend to take a much more amount of time to scan a system for viruses. Thirdly, a scanner or its virus pattern database must be updated very often to remain effective [2]. In virus detection technique like anomaly base technique it is difficult to detect virus which behave normally [2].

VI. CONCLUSIONS

Among all the methods of virus detection mentioned above, the simplest and most economical for detecting the majority of current viruses is signature scanning. While signature scanning may not be able to detect all possible viruses, but it is still simple and cheap enough to be easily available and useful to the public at large and it has the least impact on existing code and hardware.

REFERENCES

[1] 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

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

[3] Min Feng Rajiv Gupta, Detecting Virus Mutations Via Dynamic Matching, CSE Dept., University of California, Riversidefmfeng,guptag@cs.ucr.edu.

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

[5] SarikaChoudhary,RitikaSaroha,SonalBeniwal,How Anti-virus Software Works??,International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 4, April 2013 ISSN: 2277 128X

[6] BabakBashari Rad, Maslin MasromandSuhaimi Ibrahim Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short SurveyIJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011 ISSN (Online): 1694-0814 www.IJCSI.org.

