Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Survey on Malware Detection Techniques

Pranit Gaikwad, Prof.Dilip Motwani [2], Prof.Vinayak Shinde [3]

[1,3]Department of Computer Engineering, SLRTCE, Mira Road
[2]Department of Computer Engineering,VIT, Mumbai

Abstract— Malware is a worldwide pandemic. It is designed to damage computer systems without the knowledge of the owner using the system. Software's from reputable vendors also contain malicious code that affects the system or leaks information's to remote servers. Malware's includes computer viruses, spyware, dishonest ad-ware, rootkits, Trojans, dialers etc. Malware detectors are the primary tools in defense against malware. The quality of such a detector is determined by the techniques it uses. It is therefore imperative that we study malware detection techniques and understand their strengths and limitations. This survey examines different types of Malware and malware detection methods.

Keywords- Malware, malware detection, signature-based, reverse engineering ,obfuscation

I. INTRODUCTION

Malware is a term for any malicious software which enters system without authorization of user of the system. By merging the words 'malicious' and 'software' the term is created as Malware. Malware is a very big hazard in today's computing world. It continues to grow in volume and evolve in complexity. As more and more organizations try to address the problem, the number of websites distributing the malware is increasing at an alarming rate and is getting out of control. Most of the malware enters the system while downloading files over Internet. It scans for vulnerabilities of operating system and perform unintended actions on the system finally slowing down the performance of the system once the malicious software finds its way the system. Malware has ability to infect other executable code, data/system files, boot partitions of drives, and create excessive traffic on network leading to denial of service. When user executes the infected file; it becomes resident in memory and infect any other file executed afterwards. If operating system has vulnerability, malware can also take be in charge of system and infect other systems on network. Such malicious programs are also known as parasites and favorably affect the performance of machine generally resulting in slow-down.

This paper is organized as follows. Section II in brief describes various types of malware. Section III is a review of malware detector .Section IV analyzing the malware detection techniques explains structural and functional aspects of polymorphic and metamorphic malware. Section V abstracting the Obfuscation technique and finally section VI concluding the paper.

II. MALWARE TYPES

Malware can be broadly classified into following categories.

A. Viruses

Computer virus refers to a small program with harmful intent and has ability to replicate self. Mode of operation is through appending virus code to an executable file. When file is run, virus code gets executed. The original virus may evolve into new variants by modifying itself as in case of metamorphic viruses. A virus may spread from an infected computer to other through network or corrupted media such as floppy disks, USB drives. Viruses have targeted binary executable file such as .COM and .EXE files in MSDOS , PE files in Windows etc., boot records and/or partition table of floppy disks and hard disk, general purpose script files, documents that contains macros, registry entries in Windows, buffer overflow, format string etc.

B. Worms

Worms are self replicating programs. It uses network to send copies of itself to other systems invisibly without user authorization. Worms may cause harm to network by consuming the bandwidth. Unlike virus the worms do not need the support of any file. It might delete files, encrypt files in as crypto viral extortion attack or send junk email.

C. Spyware

Spyware is a collective term for software which monitors and gathers personal information about the user like the pages frequently visited, email address, credit card number, key pressed by user etc. It is internet jargon for advertising supported software. It is a way for shareware authors to make money from product, other than by selling it to the users. There are several large media companies that approach software authors to place banner ads in their products in exchange for a portion of the revenue from banner sales. It generally enters a system when free or trial software is downloaded.

D. Adware

Adware or advertising-supported software automatically plays, displays, or downloads advertisements to a computer after malicious software is installed or application is used. This piece of code is generally embedded into free software. The problem is, many developers abuse ad – supported software by monitoring Internet users' activities .The most common adware programs are free games, peer-to-peer clients.

E. Trojans

Trojan horses emulate behavior of an authentic program such as login shell and hijacks user password to gain control of system remotely. It is a malicious program disguised as something benign. Once installed on a system, they can cause data theft and loss, and system crashes or slowdowns. Other malicious activities may include monitoring of system, damages system resources such as files or disk data, denies specific services.

III. THE MALWARE DETECTOR

A malware detector is the implementation of some malware detection techniques. The malware detector attempts to help protect the system by detecting malicious behavior. The malware detector may or may not reside on the same system it is trying to protect from malicious code. Using manifested malware detection techniques malware detector performs its protection, and serves as an experimental means of evaluating malware detection techniques detection capability. Malware detectors take two inputs. One input is its knowledge of the malicious behavior. In anomaly based detection, the inverse of this knowledge comes from the learning phase. So anomaly-based detection knows what is anomalous behavior based on its knowledge of what is normal. Since anomalous behavior subsumes malicious behavior, some sense of maliciousness is captured by anomaly based detection. If the malware detector employs a signature-based method, its knowledge of what is malicious comes from its warehouse, which is usually maintained manually by people who were able to classify the malicious behavior and express it in a form willing for the signature warehouse, and ultimately for a machine to read. The other input that the malware detector must take as input is the program under inspection. Once the malware detector has gaining the knowledge of what is considered malicious performance and the program under scrutiny, it can utilize its detection technique to decide if the program is malicious or benign.

IV. MALWARE DETECTION TECHNIQUES

Techniques used for malware detection largely categories into three parts: Static Analysis, Dynamic analysis and Hybrid analysis. Static analysis detection techniques are again divided into Signature based detection and Heuristic detection [5].

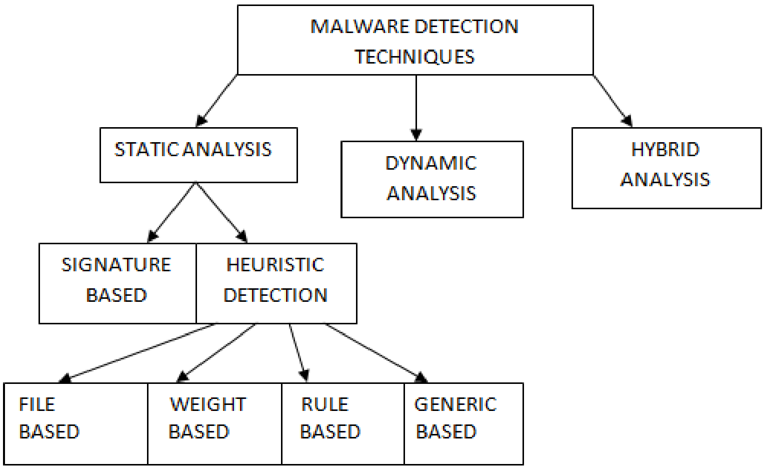

Figure 1. Malware detection techniques

4.1. Static analysis detection technique

It is the procedure of evaluate software without executing it. Using reverse engineering tools and techniques, static analysis can break down application. so as to re-build the source code and algorithm that the application has created. For performing Static analysis program analyzer, debugger and disassemble are used [6]. There are various static analysis techniques are as follows:

4.1.1. Signature based detection technique

This technique is also called as pattern matching mask or fingerprinting technique. A signature is a bit of sequence injected in the computer program by malware writers, which idiosyncratically identifies a particular malware. For recognizing a malware in the code, the malware detector search for a formerly specified signature in the code. Commercial antivirus scanners are looking for signatures which are typically a sequence of bytes within the malware code to declare that the computer program scanned is malicious. There are three categories of malwares: basic, polymorphic, metamorphic malwares.

4.1.2.Heuristic detection technique

This technique is also known as proactive technique [7]. Instead of searching for a particular signature in the code, in this technique the malware detector searches for the instructions that are not present in the application program. The effect will be is it becomes easy to detect new variant of malware that had not yet been discovered. Various heuristic analysis techniques are:

File based heuristic analysis

This type of heuristic detection technique is also known as file analysis. In this technique, the file is analyze like the contents of file, purpose of file, location of file , working of file. If the file or program contains commands to delete or damage other file, than it is painstaking as malicious.

Weight based heuristic analysis

In this technique each application is weighted according to the danger it may possess .Application program is considered as malicious when weighted value exceeds the predefined threshold value.

Rule based heuristic analysis

The analyzer, here, extracts the rules defining the application. These rules are then matched with the previously defines rules. If the rules are mismatched, then the application contains malware.

Generic signature analysis

In this signature, variants of malware are detected. A variant of malware means, the malware are different in behavior but belong to same family like "identical twins". This technique uses previously defined antivirus definition, to discover new variants of malware.

4.2. Dynamic analysis detection technique

The process of analyzing the behavior or the actions performed by the application while it is executing is called dynamic analysis [8] . Dynamic analysis can be done through monitoring function calls, tracking the information flow, analyzing function parameters and tracing the instructions. Generally a virtual machine or sandbox is used for this analysis; Doubted application is usually run into a virtual environment. If the application behaves unusually it is categorized as malicious. Nowadays, there are behavioral blocking software, which blocks malicious action of the program before their attack

4.3. Hybrid analysis detection technique

This technique is the combination of both static analysis and dynamic analysis [9].The procedure it follows it that it first checks for any malware signature if present in the code under inspection and then it monitors the behavior of the code. Hence this technique combines the advantages of both the above techniques.

V. OBFUSCATION TECHNIQUE

Obfuscation is the technique, generally used by malware authors, to make source code harder to read, understand and reverse engine, and to conceal the malicious intent of the malware [5] .

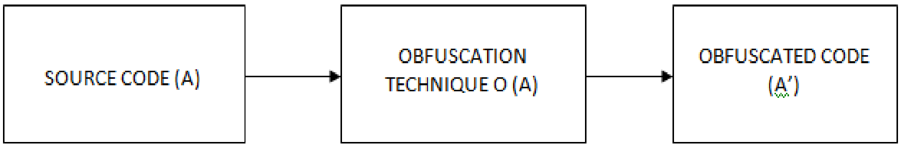

Figure 2. Obfuscation techniques

A' contains malicious code which is difficult to reverse engine, but it holds functionality and performs comparable to A.

Basically six techniques are used for Code Obfuscation

Dead – Code – Insertion

It is the simplest form of code obfuscation technique which can be done by inserting NOPs (No Operation Performed) or some push statement followed by pop statement in the code.

Subroutine Reordering

As the name suggests, this technique randomly changes the order of subroutines in the program, hence generates K' different malwares, where K is the number of subroutines.

Code Transposition

In this technique, the order of instruction is changed by using statements like jmp and unconditional branch statements, which makes the code different from its naive code. Code transposition can be done in such a way that one generate the new variants by reordering the independent instructions, which is difficult to implement and harder to identify the malware.

Instruction Substitution

This technique replaces some of the code statements with the equivalent statements. For example MOV with either Push or Pop.

Code Integration

In this technique new brief is inserted into the source code of the program in order to make the code malicious.

Register reassignment

The registers of the code is replaced by the unused registers. The program code and its behavior remains the same in this technique.

VI. CONCLUSION

In this paper we had surveyed a learning about various types of malware and a succession of malware detection techniques have been presented. Detection of malware's changing their signatures frequently has posed many open research issues. Challenge lies in the development of good disassemble, similarity analysis algorithm so that the variants of malware's can be detected software. In particular, a light has been thrown on various obfuscation techniques.

REFERENCES

[1] 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 vol. 3, 422-428,2013.

[2] Vinod P. V.Laxmi,M.S.Gaur: Survey on Malware Detection Methods, 3rd Hackers" Workshop on Computer and Internet Security, Department of Computer Science and Engineering, Prabhu Goel Research Centre for Computer & Internet Security,IIT, Kanpur, pp-74-79, March,2009.

[3] F. Adelstein, M. Stillerman, and D. Kozen, "Malicious code detection for open firmware", In Proceedings of the 18th Annual Computer Security Applications Conference,2002.

[4] A. H. Sung, J. Xu, P. Chavez and S. Mukkamala: Static Analyzer of Vicious Executables (SAVE),Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC"04), IEEE.J.Rabek, R.Khazan, S.Lewandowski and R.Cunningham. Detection of injected, dynamically generated, and obfuscated malicious code. In Proceedings of the 2003 ACM Workshop on Rapid Malcode, pages 76–82, 2003.

[5] D. Uppal, V. Mehra and V. Verma, "Basic survey on Malware Analysis, Tools and Techniques " , International Journal on Computational Sciences & Applications (IJCSA)Vol.4, No.1, 103-112,February 2014

[6] Bergeron, J., Debbabi, M., Desharnais, J., M., E., M., Lavoie Y.&Tawbi, N. (2001). Static Detection of Malicious Code in executables programs. International Journal of Req Engineering.

[7] G. McGraw and G. Morrisett. Attacking malicious code: A report to the infosec research council. IEEE Software, 17(5):33–44, 2000.

[8] SavanGadhiya,KaushalBhavshar "Techniques for Malware Analysis" Volume 3, Issue 4, April 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Softwar Engineering.

[9] Robiah Y, SitiRahayu S., MohdZaki M, Shahrin S., Faizal M. A., Marliza R. "A New Generic Taxonomy on Hybrid Malware Detection Technique " (IJCSIS) International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.