Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 04 (2025)

A Survey Paper on Malware Analysis Technique

M A Prasanna [1]

[1] *Assistant Professor, Department of CSE, Ramakrishnan College of Technology, Samayapuram, Trichy, Tamil Nadu, India*

Abstract:- Nowadays, information will become insecure due to illegal transaction over an internet. To steal an information from sender to receiver, in between an information is attacked by a third-party tool or by a person with knowingly or unknowingly. Malignant knowledge is often attacked by the third party person through any form of topology within the computer network. Among different forms of malware analysis there are three types of information evaluative methods identified that involve hybrid millet alongside static malware and dynamic malware. There are various approaches to identify the malicious system in a network. This paper deals with signature-based approach and heuristic based approaches to identify the threat inside the network.

Keywords*: Static malware, dynamic malware, hybrid malware, signature-based, heuristic-based, machine learning based.*

1. Malware – An Introduction

In Technology world like using apps, web applications are used world-wide and threats is vulnerable to any attack on various server in the computer network based on the topology design. The topology design such as LAN, WAN, WIFI…. etc. If any machine is affected in the computer network called the Bot.If the group of machines is affected in the computer network is called as Botnet. Another name for Bot is called as Malware. Bot is kind of software used in Kali Linux software to check any threats is identified by computer server.

1.1. Definition of Intruder

Another name of an intruder called as threats inside a malware program. Intruder attacks the computer system without any system's guidelines.

Those software place inside the computer program called as malicious threat program.

1.2. Types of Intruder in Malware

Virus: It is a new program that inside an existing program without the user's knowledge. Those machines seem to be malfunction in the network.

Trojan: Trojan is a type of threat program that sends the copies of threats and an information is tiptoe in the network. Those tiptoe code sends a numerous copy in network based on the topology used. Tiptoe code runs like a horse in a topology of the computer network.

Worms: Another name for worms called as creepy-crawly. It is a program which sends a self-copy inside the computer network and the network bandwidth utilization. That program mentions the destination machine for further operation.

Crypto-ware: This is another name for spyware. It is a user unknowingly to installed third party antivirus software in a computer machine. That virus is spreading along various topology in a computer network.

RAT: RAT means Remote Administration Toolkit. It is the type of toolkit in which trojan horse antivirus software with high privilege when kernel operating system runs.

1.3. Define RAT IN MALWARE

RAT, the abbreviation for remote access trojans, are identified to be an attacker enabling malware for computer attackers to gain remote access to infected computers. The attacker on the established run of RAT, the attacker is capable of sending commands to the compromised systems for accessing and collecting data back in response to the commands. “2022 Security Report Demo Endpoint RAT Protection”.

Once machine is affected by any topology in a computer network. RAT is responsible for identify the user threats, “Distributed Denial of Service attack”, “man-in-the-middle attack”, and “Denial of Service attack”, over the firewall in the computer network.

There are three approaches in RAT IN MALWARE ATTACK.

i. Static attack
ii. Dynamic attack
iii. Hybrid attack.

2. Three Approaches in Malware Analysis

There are three approaches in malware analysis technique.

Static malware analysis is a method of examining malware without running it. It involves studying the malware's code, file structure, and metadata to learn about its characteristics, purpose, and capabilities:

- **File structure**: Analysts examine the file's structure and content to check if it complies with its expected format.
- **Strings**: Analysts identify strings in the malware.
- **Signatures**: Analysts search for known signatures.
- **Metadata**: Analysts study the malware's metadata.
- Dynamic malware analysis is a cybersecurity technique that involves running malware in a controlled environment to observe how it behaves in real time. This process helps security teams understand how malware works, detect harmful activity, and create mitigation techniques.

These are heuristic focused and signature oriented approach for machine learning.

2.1. Signature Based Approach:

This approach is practically applied for detection of Malware in an exceptional manner. It involves having knowledge of the malware in prior level for being able to detect and requires needing to keep updating for maintaining functionality against new viruses. This approach is unable to detect zero day malwares however. Despite the fact that the malware of the same family is probable to go and be detected on a zero day malware basis. Despite this it is a strongly implemented approach in commercial purpose due to its speed and efficiency in several manners.

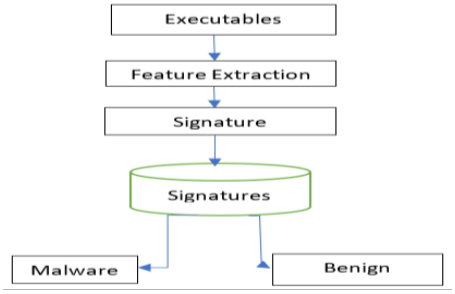


Figure 1

Figure 1 represents the signature based method that initially implements the executables to be selected. This could involve any form of executable file such as.exe files and it is following this sent over to feature extraction from that executable file unlock with all features being extracted out following the process of signature being checked for determination of malware or benign presence.

2.2. Analysis on Signature-Based Approach

As a form of antimalware approach signature based reduction is considered for a capacity to recognise Malware infection existence and instances through matching at a rate of at least the pattern of 1 byte code of the software at fault alongside with databases of present signatures of the recognised malicious programs that also are known as blacklists.

2.3. Heuristic Based Approach

In the recent time heuristic focused approach for recognition has been quite commonly used [2] and it is considered a rather unpredictable form of strategy for discovery that uses multiple cheese and Encounters such as ml methods and rules [3]. In spite of this it was noted that there is a high exactness rate for distinguishing zero day malware in a particular manner and involves identification of convoluted malware and the heuristic based range. Figure number 2 is noted to be providing the identification blueprints.

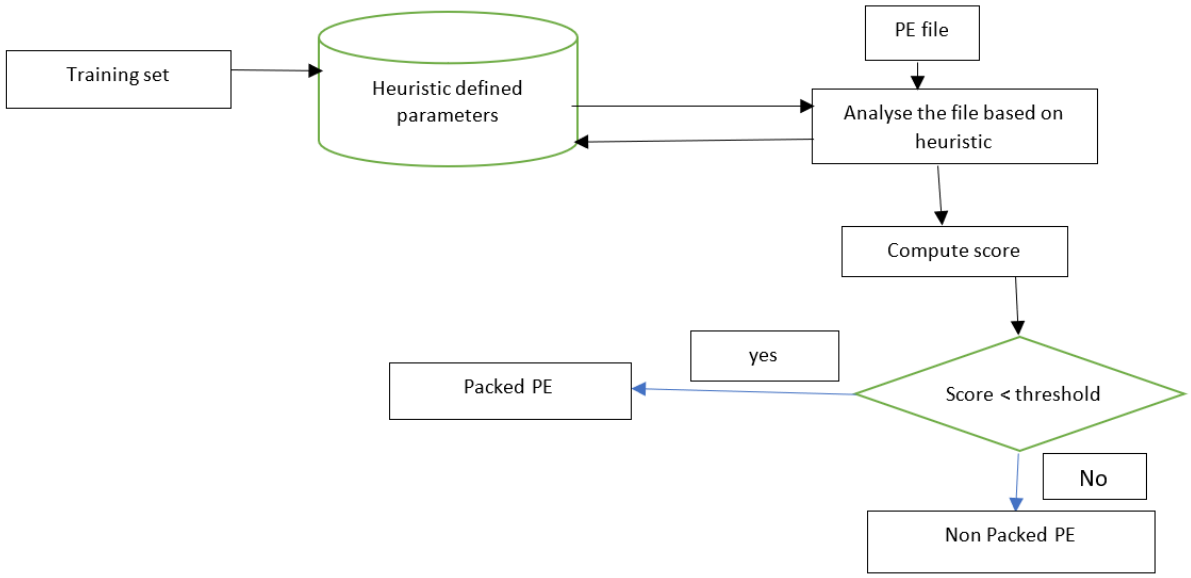


Figure 2

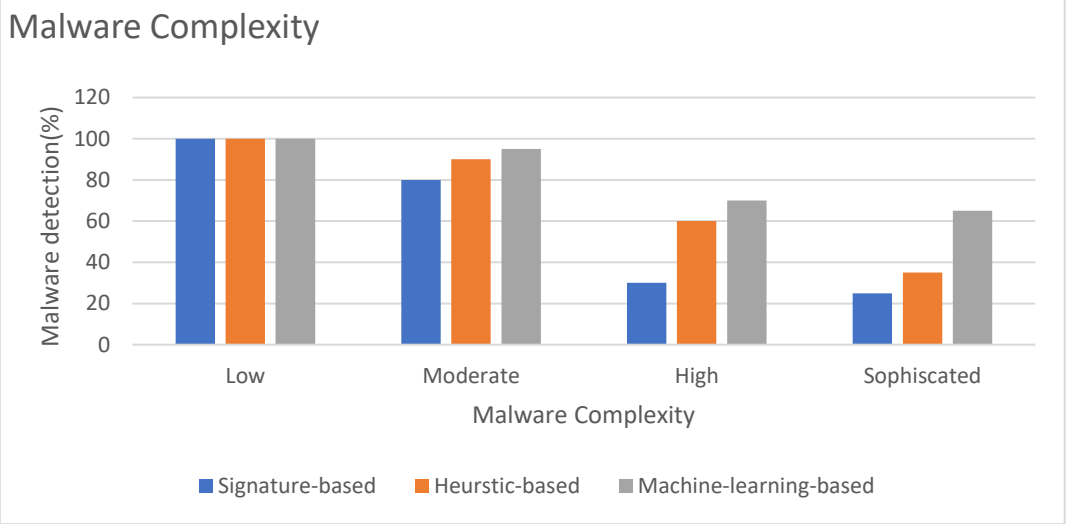
2.4. Analysis on Heuristic Based Approach

Heuristic evaluation is identified to be a methodology involving detection of viruses through the evaluation and investigation of suspicious property associated phones. Analysis has been noted to involve integration within advanced security solutions through facility companies such as Kaspersky Labs, for new threat detection before cause of harm without necessity of particular signatures.

2.5. Machine Learning Based Approach

Machine learning based approach is used by applying multiple forms of machine learning algorithms and activities that are mostly consistent with a collection of algorithmic factors that are capable of providing an output sans the particular programming required. Among multiple tasks that are capable of being executed in machine learning there are classifications and clustering alongside regression full stop. It is noted that this approach has been implemented for a considerable amount of years in the past [5]. A few of the more popular machine learning algorithm involve “linear regression” and “K nearest neighbouring (knn)”, along with “logical regression”, “Naïve Bayes”, “Random forest”, “Gradient Boosting”, “isolation forest”, “multi-layered perceptron (MLP)” etc.

2.6. Evaluation of Malware Detection Approach using Graphical Representation



Fiogure 3

3. Malware Analysis Technique

The analysis technique of malware is essential for the development of efficient techniques for deduction of malware. It is identified as a procedure for evaluation of the functionality and purpose of malware for the goal of malware analysis focusing on comprehension regarding specific fees of malwares working can contribute in building a defence for protection of organisation network system this involves three forms of malware analysis capable of attaining the same target of explaining the operation of malware and impact on system with the tools and time and skill necessary for performance of analysis being different from each other.

3.1. Static Analysis

Code analysis is another name for static analysis and it often includes the environment of program evaluation procedure through investigation of software code of malware being maintained in terms of observations and accessibility regarding knowledge associated to malware working functions. This technique involves rivers engineering to be performed through use of disassemble tool and decompile to followed by debugger and fourscode analyser to such as IDA Pro and Ollydbg, for the purpose of comprehending the malware structure [9]. In the initial level of before programming executed the static information is identified within the executables that includes header data and sequence of bites utilised for determination of the maliciousness of file. This assembly technique is a technique for static analysis. This involves this assembly of executable files such as with instruments including XXD, Hexdump and NetWide command, that can be used for getting the program file for assembly language. Using this file the opcode is extracted out as a feature to statistically evaluate applications and behaviour for detecting malware.

3.2. Dynamic Analysis

Dynamic analysis is also considered to be known as behavioural analysis due to the factor that it includes evaluation of infected files at the time of execution leading to analysis of the dynamics. It is recognized as something that is needed [2]. Infected files have been identified to be evaluated in simulated environments such as simulators and emulators along with virtual machines and sandboxes etc. [6]. The Malware researchers utilise processes such as “SysAnalyzer”, “Process Explorer”, “ProcMon”, “RegShot”, along with other tools that help in identifying the general behaviour of the file [9]. The dynamic analysis of a file is identified to be utilised by evaluating the file and its detection post execution within the real environment at times of execution of the file it is noted that the interaction and behaviour of the system with the effect of machines are being monitored. The benefits that dynamic analysis is capable of securing is the accuracy of analysis of the known and unknown new malware. These analysis is easy in terms of detection of unknown malware since it can also contribute in the

analysis of obfuscated and polymorphic malware however involves the observation of behaviour and indicates a quite time consuming ordeal that needs long preparation time.

3.3. Hybrid Analysis

Hybrid analysis technique is preposition as a way of overcoming the boundaries of Static and dynamic analysis techniques. It initially appraises the signature specifications of any malware code and is followed by after that combining it with the other behavioural limits for refining whole malware analysis. Because of this approach hybrid analysis has been noted to overcome existing challenges of both dynamic and static analysis [6]. The dynamic and static analysis are also needed to be differentiated in the Table 1 inform of benefits and hindrances the Table 1 also embodies a contrast of a static and dynamic analysis amongst the analysis.

4. Conclusion

In conclusion the brief research had been about analysis of Malware and the features that these approaches hold. Within these multiple approaches identified in the study the signature-based approach is considered to be mostly acceptable in case of malware uses.

References

[1] Symantec Corporation, Internet security threat report2013, Volume 18
[2] Ammar Ahmed E. Elhadi, Mohd Aizaini Maarof and Ahmed Hamza Osman, Malware Detection Based on Hybrid Signature Behaviour Application Programming Interface Call Graph, American Journal of Applied Sciences 9 (3): 283-288, 2012, ISSN 1546-9239, 2012, Science Publications
[3] Asaf Shabtai, Robert Moskovitch, Clint Feher, Shlomi Dolev and Yuval Elovici, Detecting unknown malicious code by applying classification techniques on OpCode patterns, Security Informatics 2012, 1:1, http://www.securityinformatics.com/content/1/1/1.
[4] Imtithal A. Saeed, Ali Selamat, Ali M. A. Abuagoub, A Survey on Malware and Malware Detection Systems, International Journal of Computer Applications (0975 – 8887) Volume 67– No.16, April 2013
[5] Jonathan joseph bloun, adaptive rule-based malware detection employing learning classifier systems, Thesis-Master of science in computer science, Missouri University of science and technology, 2011.
[6] Kirti Mathur, Saroj 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, Volume 3, Issue 4, April 2013.
[7] Matthew G. Schultz, Eleazar Eskin, Erez Zadok, and Salvatore J. Stolfo, Data Mining Methods for Detection of New Malicious Executables, in Proceedings of the Symposium on Security and Privacy, 2001, pp. 3849.
[8] Muazzam Ahmed Siddiqui, Data Mining Methods For Malware Detection, Thesis, B.E. NED University of Engineering and Technology, M.S. University of Central Florida, 2008
[9] Pham Van Hung, An approach to fast malware classification with machine learning technique, Keio University,5322 Endo Fujisawa Kanagawa 252-0882 JAPAN, 2011
[10] Raja Khurram Shahzad, Niklas Lavesson, Henric Johnson, Accurate Adware Detection using Opcode Sequence Extraction, in Proc. of the 6th International Conference on Availability, Reliability and Security (ARES11), Prague, Czech Republic. IEEE, 2011, pp. 189195.
[11] R. K. Shahzad, S. I. Haider, and N. Lavesson, Detection of spyware by mining executable files, in Proceedings of the 5th International Conference on Availability, Reliability, and Security. IEEE Computer Society, 2010, pp. 295302.
[12] R. K. Shahzad and N. Lavesson, Detecting scareware by mining variable length instruction sequences, in Proc. of the 10th Annual Information Security South Africa Conference (ISSA11), Johannesburg, South Africa. IEEE, August 2011, pp. 18.
[13] Robiah Y, Siti Rahayu S., Mohd Zaki 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.
[14] Robin Sharp, An Introduction to Malware, Spring 2012. Retrieved on April, 10, 2013

[15] Ronghua Tian, An Integrated Malware Detection and Classification System, Changchun University of Science and Technology, Thesis, August, 2011
[16] Sunita Beniwal, Jitender Arora, Classification and Feature Selection Techniques in Data Mining, International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 6, August – 2012, ISSN: 2278-0181
[17] 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.
[18] Yi-Bin Lu, Shu-Chang Din, Chao-Fu Zheng, and BaiJian Gao, Using Multi-Feature and Classifier Ensembles to Improve Malware Detection, JOURNAL OF C.C.I.T., VOL.39, NO.2, NOV., 2010.
[19] A survey paper on malware detection techniques by Nahush Shetty1, Raja Praveen2 1Jain University, India, nahushshett01@gmail.com 2Jain University, India, raja.jainuniversity@gmail.com
[20] D. Spinellis, Reliable identification of bounded-length viruses is NP-complete, IEEE Trans. Inf. Theory, vol. 49, no. 1, pp. 280–284, Jan. 2003.
[21] Adkins, L. Jones, M. Carlisle, and J. Upchurch, Heuristic malwaredetection via basic block comparison, inProc. 8th Int. Conf. MaliciousUnwanted Softw., Amer. (MALWARE), Oct. 2013.
[22] Nirav Bhojani Department of Computer Science and engineering Institute of Technology, Nirma University Ahmedabad, India 14MCEI05@nirmauni.ac.in, Malware Analysis
[23] E. Gandotra, D. Bansal, and S. Sofat, Malware analysis and classification: A survey, J. Inf. Secur., vol. 5, no. 2, pp. 56–64, 2014.
[24] Jyoti Landage ME, Dept of Comp Engg Sinhgad College of Engg, Vadgaon, Pune, Prof. M. P. Wankhade Professor, Dept of Comp Engg. Sinhgad College of Engg, Vadgaon, Pune, Malware and Malware Detection Techniques: A Survey, International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 12, pp. 61-68, 2013