International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 08 | Aug 2021 www.irjet.net p-ISSN: 2395-0072

A Survey on "Malware Analysis Techniques, its Detection and Mitigation."

Meet Parekh[1], Gaurav Kulkarni[2]

[1] Student, Dept. of Computer Science and Engineering, ITM SLS Baroda University, Gujarat, India
[2]Assistant Professor, Dept. of Computer Science and Engineering, ITM SLS Baroda University, Gujarat, India

---

Abstract - *Malware which is also referred as Malicious Software. Malware is deliberately intended to make harm PC worker customer or some other PC organizations. Research suggests that impact of malware is getting worse. Furthermore, the variety and volume of their variations seriously sabotage the viability of customary safeguards that ordinarily use signature-based strategies and can't recognize vindictive executable beforehand obscure. Malware family variations share ordinary examples of conduct that show their starting point and reason. Two types of malware analysis are described in this paper. Firstly Static Analysis and secondly Dynamic Analysis. Moreover the methods for its detection and Mitigation are also narrated. This study paper gives an outline of Malware Analysis Techniques and furthermore it's Detection and Mitigation.*

Key Words: Malware, Worm, Trojan horse, Virus, Spyware, Bot, Static Malware analysis, Dynamic Malware analysis, Detection, Mitigation etc.

1. INTRODUCTION

Malware is any piece of programming which is expected to make hurt your framework or organization. Malware is not the same as expected projects such that they the majority of them can spread itself in the organization, stay imperceptible, cause changes to the infected system or network, persistence. They can easily infiltrate the machines causing severe damage to the organization. Consider the situation when the PC becomes contaminated and is at this point not usable, the information inside becomes inaccessible – these are a portion of the malware harm situations. Malware assaults can be followed back to the time, even before the web became inescapable. Moreover as in reality, there are individuals on the Internet with poisonous presumptions that endeavour to drive themselves by taking explanation helps these individuals achieving their objectives. Malware arrives in a wide scope of varieties like Virus, Worm, Trojan-horse, Rootkit, Backdoor, Botnet, Spyware, and Adware and so forth these classes of malware are not totally unrelated importance in this way that a specific malware may uncover the attributes of various classes simultaneously. To dodge recognition, malware creators acquaint polymorphism with the malevolent segments. The malware investigation methods assist the experts with understanding the dangers and expectations related with a noxious code test

2. What is Malware?

Malware is a code that performs pernicious moves; it can appear as an executable, content, code, or some other programming. Assailants use malware to take touchy data, spy on the contaminated framework, or assume responsibility for the framework. It regularly gets into your framework without your assent and can be conveyed through different correspondence channels like email, web, or USB drives. With the ascent of the Internet and the quantity of connected hosts, it is currently workable for a modern aggressor to taint a great many hosts inside the space of hours in the wake of delivering the malware into nature. At the end of the day we can likewise say Software that "intentionally satisfies the destructive purpose of an aggressor is normally alluded to as vindictive programming or malware. Terms, for example, "worm", "infection", or "Diversion" is utilized to group malware tests that show comparable pernicious conduct [1].

3. Need for Malware Analysis

Need for Malware Analysis investigation is utilizations to remove data from the malware test, which can help in reacting to a malware occurrence. The objective of malware examination is to decide the ability of malware, distinguish it, and contain it. It additionally helps in deciding recognizable examples that can be utilized to fix and forestall future contaminations. To distinguish the organization markers related with the malware, which would then be able to be utilized to recognize comparative diseases utilizing network checking [2]. Information is extricated from malware using information removing and observing apparatuses. The methods and cycles expected to effectively accumulate information from malware contrast contingent upon the malware's ability; they adjust to the changing malware scene. This is the reason malware investigation is viewed as a workmanship. Malware can be analyzed in 2 types: static and dynamic [3].

4. Types of Malware

Virus: Virus taints PCs and different documents by repeating itself. It can't exist autonomously so it appends with different records all the more unequivocally executable documents and application and because of its duplicating highlights, it spread across records and even PCs through network.it cause framework execution corruption and disavowal of administration.

Worms: Worms are malicious piece of code that exists independently. They have feature to replicate itself. They

propagate through storage devices and emails; also consume network and computer resources which lead to system degradation in performance [4].

Trojan horse: Programming that claims to be helpful however perform pernicious activities behind the scenes is known as a Trojan horse. The term is gotten from the Greek incident of the tricky Trojan horse that was responsible to capture troy city.

Spyware: It is written code that keeps the eye on host for capturing keystrokes to personal credentials is indicated as spyware. Data that may be fascinating for the aggressor incorporates represents PC frameworks or financial balance accreditations, a background marked by visited pages, and substance of records and messages [5].

5. Malware Analysis Techniques

Malware analysis can be performed in 2 ways: static and dynamic. Static examination includes examining at the malware before running it.

5.1 Static Malware Analysis

Essential static examination comprises of inspecting the executable record without survey the real directions. Fundamental static investigation can affirm whether a document is malevolent, give data about its usefulness, and now and then give data that will permit you to deliver basic organization marks [6]. The location designs utilized in static examination comprises string mark, byte-arrangement n-grams, syntactic library call, control stream diagram and opcode (functional code) recurrence conveyance and so forth. The executable must be unloaded and decoded prior to doing static examination [7].

5.2 Dynamic Malware Analysis

Dynamic analysis alludes to the way toward examining a code or content by executing it and noticing its activities. These activities can be seen at different levels, from the most reduced level conceivable (the paired code itself) to the framework overall (e.g., changes made to the library or record framework). The goal of dynamic analysis is to know the pernicious movement performed by the executable while it is running, without compromising the security of the investigation stage. According to the protective viewpoint, there is a danger of being contaminated by the malware while examining it progressively, since it requires that the malware be stacked into the RAM and executed by the hosting CPU [8].

5.2.1 Advanced Dynamic Analysis

In the high level technique for dynamic investigation, further examination will be embraced of dynamic investigation strategies with troubleshooting on malware, examination the vault and do an investigation on a windows framework [9].Dynamic analysis tools are as follows;

1: procmon- Rocmon, or Process Monitor, is a free tool developed by Windows SysInternals and is used to monitor the Windows file system, registry and process activity real-time.

2: Process Explorer- Interaction Explorer is likewise a free apparatus accessible from Microsoft which ought to be running when performing Dynamic Malware Analysis.

3: Regshot- Regshot is an extraordinary open source utility to screen your library for changes by taking a depiction which can measure up to the present status of your vault. This permits you to see the progressions made to your library after the malware has been executed on your framework [10].

6. Malware Detection Methods

There are three types of malware detection techniques which are described in brief in this survey paper.

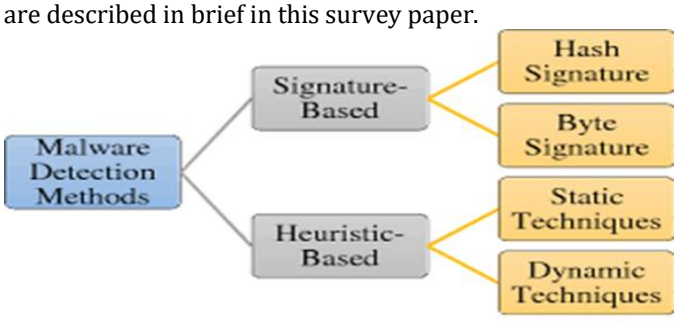

Fig -1: Malware Detection Methods

6.1 Signature based methods

Mark based strategies utilize the examples removed from different malwares to distinguish them and are more productive and quicker than some other techniques [11]. This method is also called pattern matching, string matching, mask matching and fingerprinting matching In signature based detection technique each document is examined, relegated a mark or hash and afterward added to the mark data set where it is utilized to think about the malware occurrences.

6.2 Behavior based method

Behavior based malware discovery strategies notice conduct of a program to close if it is pernicious. In these techniques, programs with a similar conduct are gathered. It consists of various types of components like data collector, interpreter and matcher. The research shows that [12] if we run this method in VM then it sometimes doesn't show all its behavior's which can mislead to wrong malware analysis.

6.3 Heuristic based method

Heuristic analysis is an approach to discovery, learning and problem-solving that uses rules, to find a satisfactory solution to a specific executable file. In this technique, the API framework calls, Opcodes, N-Grams, Control stream Graphs, and half and half highlights are been carried out. Heuristic based detection method uses data mining and machine learning techniques to examine the executable file for the malware analysis.

7. Malware Mitigation Techniques

In today's world attackers are much more adapted to security defense mechanism such as firewalls and antivirus. So

mitigation strategies are very much needed in every industry whether it's a small or large scale corporate industry which will have to focus in these areas like enclave boundary and computing environment [13] there are various strategies which we will be going through in detail.

1: Intrusion Detection System- The goal of IDS is to monitor the network traffic activity in real time. Generally the malicious activity alert is sent to the network administrator.

2: Operating System Hardening- Operating systems should be hardened to improve the ability to withstand attacks.

3: Vulnerability Scanning- Routine scanning should be done in order to prevent any malicious activity happening in any organizations internal network.

As it comes to managing the malware prevention a single device and technology should not be solely relied upon as a part of defence [14]. It's necessary to define operational key points such as accessing malware risk, physical security and logical security where malware detection can be implemented. It is difficult to secure against malware without a viable actual guard plan for all customer, worker, and organization gadgets inside an association's foundation.

8. CONCLUSIONS

Today internet industry is growing rapidly; users and industries need secure and safe environment over the internet. In today's digital world malware has become a great threat to the every organization and individual. Malware can be very deleterious as it causes serious consequences such as stealing the user's information without the end users knowledge, corrupting the data, to spread ransomware and disabling the user's network with the help of malicious attacks. Malware can undoubtedly get to the delicate data of business by foraying into worker machine. It is also possible that malware also causes Hardware failure in rare cases. As the Internet and the smart devices are more deeply indulged in our lives, we are going to face new privacy and security vulnerabilities. This survey paper presents the meaning of malware, how to analyse it and different types of known malware. We have also survey and discussed about the two main types of malware techniques. Also the research shows that Static analysis accuracy in high as compared to the dynamic analysis. The Malware Detection methods are also discussed in detail in this paper. It is likely that the methods discussed in this paper can have a significant impact on the information Technology Industries to prevent malware and to achieve higher mitigation effective strategies. This study also identified different mitigation strategies that can to be used in industries. This study is focused in contribution to the society and various information sector Industries to prevent malware. Finally the detailed study and survey is done on the malware analysis techniques its detection and mitigation.

REFERENCES

[1] Gadhiya, Savan, Kaushal Bhavsar, and P. D. Student. "Techniques for malware analysis." International Journal of Advanced Research in Computer Science and Software Engineering 3.4 (2013): 2277-128.

[2] Monnappa, K. A. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing Ltd, 2018.

[3] Elisan, Christopher C. Advanced malware analysis. McGraw Hill Professional, 2015.

[4] Tahir, Rabia. "A study on malware and malware detection techniques." International Journal of Education and Management Engineering 8.2 (2018): 20.

[5] Egele, Manuel, et al. "A survey on automated dynamic malware-analysis techniques and tools." ACM computing surveys (CSUR) 44.2 (2008): 1-42.

[6] Sikorski, Michael, and Andrew Honig. Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press, 2012.

[7] Talukder, Sajedul, and Zahidur Talukder. "A survey on malware detection and analysis tools." International Journal of Network Security & Its Applications 12.2 (2020).

[8] Or-Meir, Ori, et al. "Dynamic malware analysis in the modern era—A state of the art survey." ACM Computing Surveys (CSUR) 52.5 (2019): 1-48.

[9] YusirwanS, Syarif, Yudi Prayudi, and Imam Riadi. "Implementation of malware analysis using static and dynamic analysis method." International Journal of Computer Applications 117.6 (2015): 11-15.

[10] https://www.hackingtutorials.org/malware-analysis-tutorials/dynamic-malware-analysis-tools/

[11] Bazrafshan, Zahra, et al. "A survey on heuristic malware detection techniques." The 5th Conference on Information and Knowledge Technology. IEEE, 2013.

[12] Arkajit Datta, Kakelli Anil Kumar , Aju. D An Emerging Malware Analysis Techniques and Tools: A Comparative Analysis International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181

[13]https://us-cert.cisa.gov/sites/default/files/publications/malware-threats-mitigation.pdf

[14] Eze, Aru Okereke, and C. Chukwunonso. "Malware analysis and mitigation in information preservation." IOSR Journal of Computer Engineering 20.4 (2018): 53-62.