e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

MALWARE ANALYSIS AND TOOLS: A SURVEY

Amit Kumar[1], Abhay Pratap Singh*[2]

[1, *2] Research Scholar Department of Computer Science, Gurukula Kangri (Deemed to be University) Haridwar, India.

ABSTRACT

The term malware stands for malicious software. It is a program installed on the system without the consent of the computer user. It is basically installed by the third party for the purpose of stealing some private data from the system, or just for pranks. This turns out to threaten the security of computers, where people utilize computers in daily routine life to manage various necessities, such as education, communications, hospitals, banks, entertainment, etc. The usage of different traditional technologies to detect/identify and defend against this malicious software's called as Antivirus Scanner (AVS), firewalls, etc. But nowadays, malware authors have taken a step towards subsequent malware detectors. They write novel malware every day, which is a huge challenge for malware detectors. This article focuses on basic research on malware analysis and its tools.

Keywords: Malware, obfuscation, Network traffic, Pcaps, Antivirus

I. INTRODUCTION

In this digital era, malware attackers are competing well with malware defenders. Malware defenders encounter thousands of unusual malware samples every day. Malicious code is distributed over the Internet through untrusted or unsafe websites at an alarming rate. The spread of malware has affected the daily life, from e-government [1] to social networks [2], from digital automation [3] to mobile networks [4]. Usually, malware enters the system via downloaded files. Once malware infiltrates the system, it executes malicious activities and destroys the entire system.

Antivirus software can easily detect and defend against certain malicious or harmful software. However, Malware authors used several packers to pack malware in such a way, enabling it to hide and seek through antivirus engine and the malware has won the game. Therefore, antivirus software detection of malware has become a difficult task. In case if the detector detects malware in uninfected files, it is considered a false positive. In addition, if the scanner fails to detect the malware in the infected file, it is considered a false negative. If the scanner detects malware in the infected file, it is called a detect rate. The malware analysis techniques to enable the analysts to recognize the risks and intentions associated with a malicious code sample. The insight so obtained can be utilized to react to novel trends in malware development or take precautionary measures to handle the threats coming in the future. Features obtained from the analysis of malware can be utilized to grouping unidentified malware and categorize them into their presented families.

This paper is a survey study of malware analysis and tools. The rest of the paper is organized as follows: Section 2 describes the malware analysis techniques. Section 3 briefly explains the tools for malware analysis and section 4 concludes the conclusion

II. MALWARE ANALYSIS TECHNIQUES

Malware analysis is a process toward evaluating and inspects the purpose and function of a known malware sample. The primary purpose of malware analysis is to recognize how the malware behaves, how to inspect malware and mitigate it. The several types of malware analysis techniques are discussed below.

2.1 Static analysis

Static analysis defines that the malware analysis is completed without executing the code. This type of analysis is suitable as we do not require executing the binary code; therefore, it needs lesser amounts of resources and time [5]. The binary codes are inspected via disassembling the executable file. Presently, malware writers exploit several methods to avoid static analysis from identifying the malicious code.

2.2 Dynamic analysis

In this type of analysis, malware is executed in a virtual environment, and monitor the traces are known as dynamic analysis [6]. Dynamic analysis can be carried out via monitoring function calls, tracking the information flow, analyzing function parameters, and tracing the instructions. Usually, a virtual machine or sandbox is utilized for this analysis; the doubted application is typically executed in a virtual environment. If

the application behaves unusually it is classified as malicious. In the current scenario, there is behavioral blocking software, which blocks malicious action of the program earlier than attack.

2.3 Hybrid analysis

In this type of analysis, it is the amalgamation of both static analysis and dynamic analysis. The process it follows is that it initially inspects for any malicious signature is there in the code under inspection, and then it evaluates the performance of the code [7]. This type of analysis is also known as behavioral analysis.

2.4 Network traffic analysis

In addition, to inspect the network traffic, normally, we utilized packet-based features and flow-based features to detect malware. The Packet based approach checks the whole payload content besides headers. Packet based traffic analysis is a completely passive approach that can provide more information related to network issues. Flow based features offer important information related to network connection instead of the packet payload. A flow is defined as the source IP, destination IP, protocol, source port, destination port.

III. MALWARE ANALYSIS TOOLS

Malware analysts utilize tools for inspecting the malware to protect and predict future attacks. With the help of open source malware analysis tools, network security researchers will inspect, evaluate and log several variants of malicious triggers while inspecting the cycle of attack. As malware utilizing various online platforms on the dark web, the crypters, botnets, and zero days [8] needed to launch powerful attacks have to turn out to be easier than ever to get. Here, we discuss some open source malware analysis tools that can assist for network security research community.

3.1 Open source based malware analysis tools

Cuckoo Sandbox

It is an open source framework that automatically executes malicious file investigation for Windows, OS X, Linux, and Android and provides widespread and practical input on how each presented file operates in isolated environments. And because it is open source software, developers are constantly writing plugins that offer improved features. Cuckoo is utilized through malware detection and network security firms to assist ease the variant of automatically wading during the store of potentially harmful data.

Zeek

Zeek is also formerly called a bro tool for network analysis framework. It is commonly utilized to identify behavioral threats for network security purposes. Zeek is similar to a network intrusion detection system (NIDS) furthermore; it performs various functions like forensic, incident response, file extraction, and other capabilities as well.

REMnux

REMnux is an open source Linux toolkit considered to aid Malware analyst through malware reverse engineering. This seek Make it simple for forensic researchers and accident handling Witnesses continue to use several free software that can examine Ransomware, even though it might be cumbersome to find or set. This Linux toolkit was developed as a One-stop service for researchers to search for examples reverse engineering malware. It provides researchers to examine the browser based malware, execute forensics on memory, examine several samples of malware, extract and decode doubtful or suspicious items, etc.

YARA rules

YARA stands for yet another recursive/ridiculous acronym is a systematic way to identify malware based on some certain rules or characteristics. Investigators also utilize YARA rules to compose pattern based definitions of the malicious families. This helps network security researchers to recognize and classify actually same types of malware and can be adaptive for utilize inside the cuckoo sandbox. These rules have also been added to several end-mile detection and rejoinder framework to assist them detects the malware samples they encountered, categorize them and distribute their results with users and the society later.

Goggle rapid response

The GRR platform is an incident response system invented via network security researchers at Google, detecting ordinary malicious footprints workstations emphasized on remote live forensics. This types of an application that is installed on the target system to correspond with the agent and a web-server infrastructure.

3.2 Mobile malware based analysis tools

APK Tool

It additionally makes it simpler to manage through a device owing to the project for example file making and completion of some recurring jobs for example making the apk etc. It is a project-similar structure that makes functioning with them easy.

Smali

Smali is a dex format disassembler utilized through Dalvik, which is the Java VM implementation for Android. The syntax is loosely relied on the syntax of Jasmin / dedexer, and follows the inclusive dex format features (annotations, debug data, line details, etc.). Furthermore, code produced through the baksmali is generally considered as written in the Smali language.

Dex2Jar

Dex2Jar is an open source tool for managing with the files Android ".dex" and Java ".class." Android programs are collected into ".dex" (Dalvik Executable) scripts, which in effect are zipped onto the system into a particular.apk file. It can also be utilized to execute some essential de-obfuscation.

Mobile-sandbox

Mobile-sandbox gives static and dynamic malware analysis for Android OS Smartphone's. The system is intended to automatically estimate Android software in two original ways: through combining static and dynamic analysis, i.e., static analysis results are utilized to direct dynamic analysis and enlarge the reports of executed code, and via utilizing various logging methods for native API calls.

3.3 Web based analysis tools

Wireshark

It is a very famous network monitoring tool that is used for analyzing the network traffic. This tool intercepts the network traffic and transforms the binary data into an understandable format for internet users. It contains various filters and features to which allows individual to inspect the network traffic or packets in a detailed way. It is also utilized through management to detect imperfect network apparatus that drop packets, latency problems influenced through machines transmitting traffic about the world, and data exfiltration or even intrusion efforts against any entity.

Malzilla

Malzilla is a valuable malicious famous tool for inspecting the websites including malicious code. Web pages that enclose exploits often utilize a succession of redirects and obfuscated code to create it complicated for someone to follow them. This allows users to retrieve the websites and attain full of their source code, for example, wget, not including visiting the website and potentially destructive their device.

SysAnalyzer

It is an open source tool invented to make available an interactive resource for malware scientists to simply compile, analyze, and keep an eye on the behavior that a binary performed when working on the network. It is also an interactive framework for the malcode run time investigation that tracks several aspects of device and technique states.

Virus Total

Virustotal is an online platform that analyzes or inspects the suspicious files and URLs and helps to identify viruses, worms, Trojans, and all types of malware detected via antivirus engines rapidly. Furthermore, several of techniques for mitigating signals from the studied material, Virus Total inspects products with more than 70 antivirus scanner engines and URL / domain blacklisting services. It can also help identify the malicious content and protect the safeguard from external threats.

Packet Total

It is also an online platform for analyzing and inspecting the PCAPs files and exploring the network traffic. This service is also useful and helpful for virus analysis and incident response. Any person can utilize their web browser to choose a file from his own computer or phone, and put forward it to packet total. Packet total provides a summary or great layout for submitting files where novice users can easily understanding the file structure.

Joy

Joy is an open source software tool for extracting relevant data or information features from live network traffic or packet capture (Pcap) files, utilizing a flow-oriented model related to that of IPFIX or Netflow, and next showing these data features in JSON. It also includes analysis tools that can be useful to these data files. It can be utilized to discover data at scale, particularly security and threat-relevant data

IV. CONCLUSION

This study contributes an overview regarding the malware analysis and tools. Malware analysis is a very complicated process because several malware writers used various obfuscation techniques and write code to evade antivirus software therefore we need to explore tools and malware analysis techniques to easily detect the threats for internet users as well. We had surveyed various malware analysis techniques utilized by malware researchers and also explored several tools which will be useful for identifying and detecting the malicious pattern

V. REFERENCES

[1] S. K. Talukder, M. I. I. Sakib, and M. M. Rahman, "Model for government in Bangladesh: A unique id based approach," in 2014International Conference on Informatics, Electronics Vision (ICIEV), May 2014, pp. 1–6.

[2] Singh, Abhay Pratap. "Improving the malware detection ratio using data mining techniques." Second International Conference on Science, Technology and Management. 2015.

[3] Singh, Abhay Pratap "Ransomware: A High Profile Attack" International Research Journal of Engineering and Technology Vol 4, issue 2, 2017.

[4] S. Talukder, I. I. Sakib, F. Hossen, Z. R. Talukder, and S. Hossain, "Attacks and defenses in mobile ip: Modeling with stochastic game petrinet," in 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). IEEE, 2017, pp. 18–23.

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

[6] Savan Gadhiya, Kaushal, Bhavshar "Techniques for Malware Analysis" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013ISSN: 2277 128X.

[7] 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

[8] Singh, Abhay Pratap. "A Study on Zero Day Malware Attack." International Journal of Advanced Research in Computer and Communication Engineering, Vol 6, issue 1, 2017.