IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Review Study About Malware Analysis

Gauri Santosh Vedpathak, Department of IT, GMVCS Tala, University of Mumbai

Sakshi Pravin Dalvi, Department of IT, GMVCS Tala, University of Mumbai

Kaustubh Pradip Mekde, Department of IT, GMVCS Tala, University of Mumbai

Hrishikesh Sanjivan Khaire, Department of IT, GMVCS Tala, University of Mumbai

Prof. Avni Anup Amburle
Assistant professor GMVCS
University of Mumbai

**Abstract :-** The malwares being designed by attackers are polymorphic and metamorphic which have the ability to change their code as they propagate. moreover, the diversity and volume of their variants severely undermine the effectiveness of traditional defences which typically use signature-based techniques and are unable to detect the previously unknown malicious executables. The threats malware pose to the people around the world are increase rapidly. A software that sneaks to your computer system without your knowledge with a harmful intent to disrupt your computer operations. Due to the vast number of malwares, it is impossible to handle malware by human engineers. Therefore, security researchers are taking great efforts to develop accurate and effective techniques to detect malware. Studies suggest that the impact of malware is getting worse. Two types of malware analysis are described here. One is Static Malware Analysis and other is Dynamic Malware Analysis. Static Malware Analysis has some limitations. So, Dynamic Malware Analysis is preferable for Malware Analysis.

**Keywords :-** Malware, Static Malware Analysis, Dynamic Malware Analysis, malicious, malware detection method.

## I. INTRODUCTION

Now a day, Internet becomes an essential part of the daily life of many people. On internet many services are available and are also increasing day by day. More and more people are making use of these services. The treat tat malware cause to the computing world is growing rapidly. According to the AV-TEST institute, 48 million various malware samples were developed in the first quarter of 2017[1]. Due to the vast number of malware, it is impossible to handle malware by human engineers. Thus, security researchers use malware detection system to detect malware. Software that "deliberately fulfils the harmful intent of an attacker" is referred to as malicious software to malware. These are intended to gain access to computer system and network resources, disturb computer operations, and gather personal information without taking the consent of system's owner, thus creating a menace to the availability of the internet, integrity of its host, and the privacy of its users. Malwares come in wide range of variations like virus, worm, Trojan-horse, Rootkit, Backdoor, Botnet, spyware, Adware etc. These classes of malwares are not manually exclusive meaning thereby that a particular malware may revel the characteristics of multiple classes at the same time.

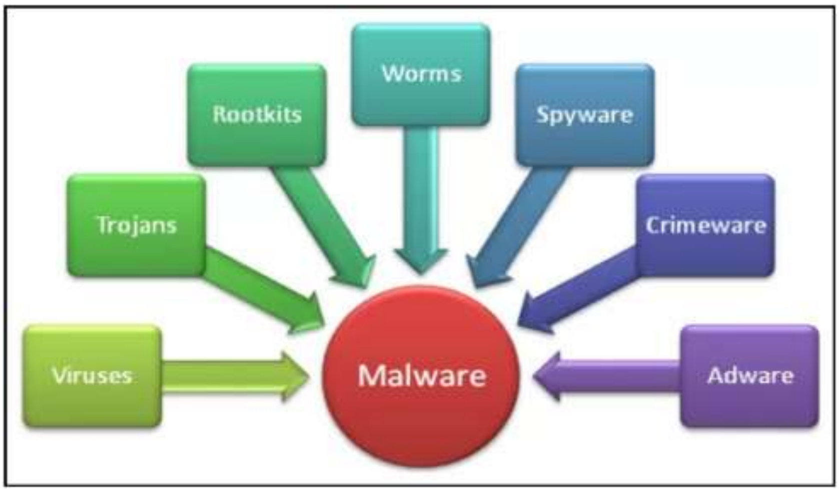
### What is Malware Analysis?

Malware Analysis is the process of determining the purpose and characteristics of a given malware sample such as virus, worm, or Trojan horse. This process is a necessary step to be able to develop effective detection technique for malicious code. The tools used for malware analysis can basically be broken into two categories: static and dynamic analysis. The static analysis tools attempt to analyse a binary without actually executing the binary. Live analysis tool will study the behaviour of a binary once it has been executed. Automated malware analysis is a virtually interactable problem. It is simply not possible for one program to determine the exact behaviour of another program.

### Types of Malware :

Malware is a software that inserted into the system without user knowledge. It can harm the computer system by compromising computer functions, stealing data or evading access controls. The following list presents the common categories of malware:

- **Virus:** A malicious software that duplicates itself by injecting its code into other programs, virus can spread from one program to another and from computer to another.
  .
- **Worms:** Are malicious programs that replicate themselves in a computer and destroy the files and data on it. Worms might also encrypt files or send junk emails. Unlike viruses, worms carry themselves in their own containers.
- **Trojan Horse:** While acting as a legitimate programs, Trojans perform unknown and unwanted activities. Trojans allow attackers to gain access to the effective computer and extract user confidential information like password and banking details.
- **Spyware:** Spyware is a software that continuously spies on the users activities. It is used to gather information about the users like webpages regularly visited and credit card number without their knowledge, then sends that information back to the attackers.
- **Rootkit:** Rootkit is a collection of malicious software that is programmed to access a computer system and allow other types of malware to get into the system.
- **Ransomware:** A harmful software that allows the hacker to lock the computer and restrict the victim access to the vital information. Ransomware encrypts the important data on the infected computer or network then ask for payment to lift restriction.
- **Adware:** Advertising-supported software is a type of malware that continuously brings advertisements to the computer. Usually, adware is bundled with free playing games.
- **Botnet:** A malware that remotely controls a group of devices like PCs, smart phones and internet of things devices are infected and controlled by a cybercriminal. Botnet is typically used for spam emails campaigns or denial of service attacks. Users are often unaware that their system are infected by a botnet malware.
- **Crimeware:** Crimeware is an umbrella term for any malware with common purpose of obtaining money or secret information. Crimeware addresses a growing problem in security management, as growing number of malicious code threats attempt to steal sensitive information.



## II. METHODOLOGY

- **Signature-Based Detection:** Signature-based detection uses the unique digital footprint, known as a signature of software programs running on a protected system. Antivirus programs scan software, identifies their signature and compares it to signature of known malware. Antivirus products use a large database of known malware signatures, typically maintain by security research team operated by the antivirus vender. This database is frequently updated and the latest version is synchronized with protected devices. When antivirus program identifies software that meets a known signature, it stops the process and either quarantines or deletes it. This is simple and effective approach to malware detection and is important as the first line defence.

- **Checksumming:** This method is a type of signature analysis that involves calculating cyclic redundancy check (CRC) checksums. Checksumming helps verify that files are uncorrupted. The main drawback of signature-based detection is creating a massive database generating false positives, which checksumming amins to address. Hackers often use polymorphic malicious advertisements to avoid detection by signature-based identification methods. Polymorphic viruses can change themselves when replicating, eliminating consistent search strings-usually, the hacker encrypts random decryption command sets in the form of non-constant keys in the virus code. Thus, when the security team identifies a malicious signature, the malware no longer contains the code fragment and cannot be found. The absence of a detectable signature in the variable code requires other malicious code detection techniques, such as:

  - **Statistical analysis:** analyses the frequency of processor commands to determine if a file is infected.

  - **Cryptanalysis:** known-plaintext cryptanalysis decodes encrypted viruses using an equation system (like the classic cryptographic technique of decoding text without a decryption keys, applying the algorithm to encodes fragments to decode the overall body of the encrypted virus.

  - **Heuristics:** a malware detection team scans and analyses behavioural data to identify anomalous activity. The team must research for malicious code associated with suspicious behaviour, such as a code served to thousand of users within a few minutes. The security team can then prioritize and further investigate suspicious incidents.

  - **Reduce masks:** The malware detection team can use elements within the encrypted virus body to circumvent the need for an encryption key when obtaining static code. The static code produced can revel the malware’s signature or mask.

- **Application Allowlisting:** Application allowlists (aka whitelists) are the opposite of the attack signature approach. Instead of defining which software the antivirus program should block, it maintains a list of approved application and blocks everything else. This solution is not perfect but can be highly effective, especially in high-security environments. It is quite common for legitimate applications to have security vulnerabilities, or introduce unneeded features that increase the attack surface. In some cases, the application itself is benign, but its use could expose the device to threats – for example, in some environments, there may be a need to block web browsing and email. Application allow listing works best with devices that are strictly task-focused, such as web servers and internet of things (IOT) devices.

## III. CONCLUSION

Malware is causing a critical threat to our computer systems, internet and data. The challenges that malware authors pose by developing complicated malware that frequently change their signature to evade detection, and by releasing more sophisticated version of malware that use new obfuscation techniques, have brought many issues to anti-virus software and security researcher.

## REFERENCES:-

[1] AV-TEST, “The AV-TEST Security Report,” 2017.

[2] C.T. Lin.N. J. Wang, H, Xiao, and C. Eckert, “Feature selection and extraction for malware classification,” J. Inf. Sci. Eng., vol. 31, no. 3, pp. 965-992, 2015.

[3] R. Mosil, R. Li, B. Yuan and Y. Pan, “Automated malware detection using artifacts in forensic memory images,” in 2016 IEEE Symposium on Technologies for Homeland Security, HST 2016, pp. 1-6.

[4] M. Karresand, “Separating Trojan horses, viruses, and worms – A proposed taxonomy of software weapons,” in IEEE System, Man and Cybernetics Society Information Assurance Workshop, 2003, pp.127-134.

[5] A. Zaki and B. Humphrey, “Unveiling the kernel: Rootkit discovery using selective automated kernel memory differencing,” Virus Bull., no. September, pp. 239-256, 2014.

[6] A. Alshamrani, S. Myneni, A. Chowdhary, D, Huang
A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities
IEEE communication Surveys and Tutorials, 21(2) (1019), pp. 1851-1877.