# 3 Malware Detection and Analyzer

**Prakash Chand Thakuri Anmol Garg Rohit Kumar Shivam Panwar**

**Department of CSE Department of CSE Department of CSE Department of CSE**

**SET, Sharda University SET, Sharda University SET, Sharda University SET, Sharda University**

***Abstract*- Malwares are the malicious software which are designed to harm the system. Malware is capable of corrupting, executing itself, and executing the system remotely without the knowledge of the user. In addition to denial-of-service attacks, malware can breach security principles such as confidentiality, integrity, authentication, and secrecy. The ability to replicate is one of the most crucial qualities of most viruses, as it assures its survival. In some cases, the virus can damage the Ram, SSD, or hard disk of the computer. When the malware enters a system, it multiplies drastically and crashes the operating system by sending the large amount of process to CPU. This paper focus on Malware and it’s various detection types.**

***Index Terms***- Malware, Malware Detection, Signature-based, Anomaly-based, Anti-Virus, Obfuscation, static, dynamic, Algorithm,

1. **Introduction**

Malware has had a tremendous impact on the world as we know it. The rising number of computer security incidents since 1988 suggests that malware is an epidemic [1]. A recent report from the popular anti-virus company MC-Fee says “malware continues to grow” [2]. Every day, the Kaspersky Institute registers over 450,000 new malicious programs (malware) and potentially unwanted applications (PUA) [3]. The graph of creation of new malware is so high as passing of times [4]. So, the researcher and anti-virus companies are trying to make anti-malware mechanism to protect the system despite the fact that there is not the permanent solution to stop this because malware can be created and modified as per requirement seeing the flaws of the system.

Malware detection is a word used to describe whether a program has malicious intent [5]. It is made up of two words: detection and analysis [6]. The focus of this work is on the analysis aspect of malware detection. It can be used on both the client and the server, similar to cloud-based technology.[7].

Many technical solutions have been developed, including the use of cloud computing [8], network-based detection systems [9], web, virtual machine, agent, and hybrid approaches, as well as other technologies. The primary purpose of this review article is to look into the present state of malware detection and detection systems with proper mechanisms. The research encompasses malware analysis as well as techniques and technology for developing anti-malware software.

1. **Types of Malwares:**
2. **Virus:** It is a type of malware in which the malicious code is attached which attacks the system and cause the damage.
3. **Worms:** It is a type of malware which get the details of infected machine.
4. **Trojans:** It is malicious software which is used to control the system.
5. **Spyware:** It is not a malicious but used to steal your personal information, credit card information etc.
6. **Rootkits:** It allows the user to gain the access to the user’s computer without knowing.
7. **Adware:** It is unwanted software that displays advertisement.
8. **Ransomware:** It is malicious software that seize the data until and unless the targeted victim pays the money.

Malware is comprising of two things: malicious and software. As per the G. McGraw and G. Morrisett, “any code added, changed or removed from a software system in order to intentionally cause harm or subvert the intended function of the system is considered to be the malware” [10]. Likewise, Virus has been defined as “a generic term that encompasses Virus, Trojans, Spywares and other intrusive code” [11].

A Malware can corrupt, alter, execute itself, and execute the system remotely without the knowledge of the user. In addition to denial-of-service attacks, malware can breach security principles such as confidentiality, integrity, authentication, and secrecy.

The ability to replicate is one of the most crucial qualities of most viruses, as it assures its survival. In some cases, the virus can damage the Ram, SSD, or hard disk of the computer. When the malware enters a system, it multiplies drastically and crashes the operating system by sending the large amount of process to CPU.

Essentially, the main motive of malware creators are to create undetectable software that can perform its purpose without being detected by anti-malware or firewall systems.

1. **Who are the Users and Creators of Malware?**

Malware writers go under many different names. Black hats, hackers, and crackers are some of the most well-known terms. An external/internal danger, a foreign government, or an industrial spy could be the actual people or groups that use the aforementioned designations. [12].

Malware is injected into software during two stages of its lifecycle. The pre-release phase and the post-release phase are the terms used to describe these phases. The only form of hacker capable of introducing malware into software before it is released to end-users is an internal threat or insider. An insider is a trustworthy creator of software that will be distributed to end users within a company. During the post-release phase, when the software is available to its intended audience, all other persons or organisations that take on the hacker role insert malware.

Malware has the power to corrupt, alter, execute itself, and execute the system remotely without the knowledge of the system administrator. In addition to denial-of-service attacks, malware can breach security principles such as confidentiality, integrity, and secrecy. In order to get around malware detection, black hats typically use one or both of the following techniques: obfuscation and behaviour addition/modification [13]. Obfuscation is a technique

1. **The Malware Detector**

A malware detector, as stated in the introduction, is the implementation of a malware detection technology (s). By detecting harmful behaviour, the malware detector tries to assist secure the system. The malware detector may or may not be installed on the same computer as the one it is attempting to safeguard. The malware detector protects users by employing manifested malware detection technique(s) and serves as an empirical method of assessing malware detection approaches' detection capabilities. Malware detection techniques are divided into two categories. Signature-based and anomaly-based can be further subdivided into specification-based and anomaly-based.

1. **Malware Detection Techniques**

Malware detection techniques can be broadly divided into two categories: anomaly-based detection and signature-based detection. A technique that employs knowledge of what constitutes normal behaviour to determine the maliciousness of a software under examination is known as anomaly-based detection. The term "speculation-based detection" refers to a specific sort of anomaly-based detection. Specification-based techniques rely on some kind of specification or rule set of what constitutes acceptable behaviour in order to determine whether or not a programme is malicious. Programs that deviate from the specification are regarded abnormal and, in most cases, harmful. Signature-based detection determines the maliciousness of a software under investigation by analysing what is known to be harmful. As one might expect, a signature-based detection method's success is determined by how well the malicious behaviour is characterised or sig-natured.

* 1. **Malware Analysis Techniques**

Graphical user interface, diagram

Description automatically generated

**Fig 1**

**Basic Analysis:**

* Static Analysis:
  + Examines malware without running it
  + Tools: Virus-Total, strings, a disassembler like IDA Pro
* Dynamic Analysis:
  + Run the malware and monitor its effect
  + Use a virtual machine and take snapshots
  + Tools: Reg-Shot, Process Monitor, Process Hacker, Capture-BAT

**Advanced Analysis:**

* Static Analysis:
  + Reverse Engineering with disassembler
  + Highly complex
* Dynamic Analysis:
  + Run code in Debugger
  + Examines internal state of running malicious executable

Static analysis is the analysis that use syntax or structural properties or bytes of the program to determine the malware behaviour on the intended software. Signature-based detection would only leverage structural information to determine the malicious behaviour, whereas dynamic requires the run time approach.

1. **How a Malware Works? (Algorithm)**
2. **Initiation of the attack**: The attacker first analyses their victim and sent the malicious mail, phishing links to get the information about it.
3. **Instantiation:** Now the malware would make a bridge between the attacker and the victim to retrieve the data.
4. **Activation:** The third stage is the activation state in which attacker uses remote access to retrieve the data from the victim.
5. **Encryption:** Encryption means converting the plain text to the cipher text. Ransomware that also targets the backup system may delete or encrypt the backups to prevent the recovery.
6. **Ransome Request:** The attacker asks for the money to decrypt the data. The malware converts the
7. **Algorithm of Tool (Malware Analyzer)**

Step:1 The tool takes the path of an exe file.

Step:2 Verification of the file if it is an exe or not.

Step:3 Analyze the file

Step:4 Prepare the P.E report of the file

Step:5 On the basis of P.E file it analyze the file.

1. **Portable Executeable File**

The P.E file is the report file which is essential data structure encapsualting necessary information for the windwos OS loader to manage the wrapped executable code. The P.E file consists of following things:

1. API
2. Real Virtual Address
3. Image Address
4. DLLS Report
5. Number of Sections
6. Virtual Size
7. **General Overview on working of Signature Based malware detection**

This detection system uses the continuous sequence of bytes for inspection of the malware sample to find the malicious behavior on it. It generally does by also comparing hashes, virtual address sections or strings. In case of cloud based or network signatures it analyze the network traffics and other factors.

1. **Capabilities of the Tool:**
2. **Hashes:** They are the strings of characters and generated by the formula.
3. **String:** The combination of the characters.
4. **Real Virtual address:** It is virtual address of the memory which is embedded in the file.
5. **Address of Entry point:** It is the address of entry point of the file where the coding of the file started.
6. **No. of sections:** It refers to how many sections does a exe file has.
7. **DLL:** DLL refers to“Dynamic linked library” which is a window’s file used to run the OS.

If the tool give all the necessary information about the software like Image address, Relative Virtual Address, (.txt file), (.data file), Virtual Address, resources and many other than the software is not a Malware.

After analyzing the notepad, I-tunes, disk-cleanup all the necessary information have been collected but Ns malware has not provided full PE file report then we can conclude that it is Malware.

1. **Conclusion**

This paper presented a quick review of the types, pattern and function of malware and it’s detection system focusing the signature based techniques as the center of presentation.

It provides an updated study for most of the familiar malware types and detection techniques. Although the development of new created malware is so rapid so this study can be considered as a key reference for the researcher and the developers.

**12.Final Analysis**

* + 1. **Tool Interactivity**

**Text

Description automatically generated**

**Fig:2**

* + 1. **Generated P.E file of Notepad**

Table

Description automatically generated

**Fig:3**

* + 1. **Generated P.E file of I-tunes**

Table

Description automatically generated

**Fig:4**

A screenshot of a computer

Description automatically generated with medium confidence

**Fig:5**

1. **References**

[1] CERT/CC. Carnegie Mellon University. <https://www.usenix.org/legacyurl/18th-large-installation-system-administration-conference-151-technical-paper-11>

[2] Mcafee and Lab, 2013 Threats Predictions. 2013

[3] [Malware Statistics & Trends Report | AV-TEST](https://www.av-test.org/en/statistics/malware/)

[4] [Malware Statistics & Trends Report | AV-TEST](https://www.av-test.org/en/statistics/malware/)

[5] Christodorescu, M., et al., Semantics-Aware Malware Detection, in Proceedings of the 2005 IEEE Symposium on Security and Privacy. 2005, IEEE Computer Society

[6] [(PDF) Malware Detection and Analysis (researchgate.net)](https://www.researchgate.net/publication/342491461_Malware_Detection_and_Analysis)

[7] https://sourcedefense.com/glossary/client-side-malware/

[8] Ahmed, M., et al. NIDS: A Network Based Approach to Intrusion Detection and Prevention. in Computer Science and Information Technology - Spring Conference, 2009. IACSITSC '09. International Association of. 2009

[9] http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9599-case-network-based-malware-detection.pdf

[10] . McGraw, G. and G. Morrisett, Attacking Malicious Code: A Report to the Infosec Research Council. IEEE Software., 2000

[11] Xufang, L., P.K.K. Loh, and F. Tan. Mechanisms of Polymorphic and Metamorphic Viruses. in Intelligence and Security Informatics Conference (EISIC), 2011 European. 2011

[12] M. Christodorescu, S. Jha, S. Seshia, D. Song, and R. Bryant. Semantics-aware malware detection. In Proceedings of the 2005 IEEE Symposium on Security and Privacy, pages 32–46, 2005

[13] M. Ciubotariu. Netsky: a conflict starter? Virus Bulletin, May 2004.

[14] M. Debbabi, E. Giasson, B. Ktari, F. Michaud, and N. Tawbi. Secure self-certified cots. In Proceedings of the 9th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, pages 183–188.