A PROJECT REPORT

ON

"MALWARE ANALYSIS USING SANDBOX"

Submitted to

BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)
DEPARTMENT OF ENGINEERING AND TECHNOLOGY, NAVI MUMBAI

In Partial Fulfilment of the Requirement for the Award of
BACHELOR'S DEGREE IN
INFORMATION TECHNOLOGY
BY

Aditi Thakur	**2043110234**
Shubham Jha	**2043110236**
Pranav Taskar	**2143110241**
Nargis Shah	**2143110253**

UNDER THE GUIDANCE OF
Prof. Reshma Kanse

DEPARTMENT OF INFORMATION TECHNOLOGY
BHARATI VIDYAPEETH DEEMED TO BE UNIVERSITY DEPARTMENT OF ENGINEERING AND TECHNOLOGY, NAVI MUMBAI

2023-2024

A PROJECT REPORT
ON

"MALWARE ANALYSIS USING SANDBOX"

Submitted to

BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)
DEPARTMENT OF ENGINEERING AND TECHNOLOGY, NAVI MUMBAI

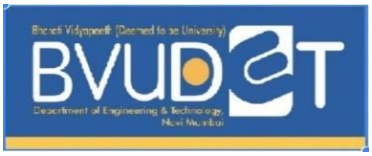
In Partial Fulfilment of the Requirement for the Award of

BACHELOR'S DEGREE IN INFORMATION TECHNOLOGY

BY

ADITI THAKUR	**2043110234**
SHUBHAM JHA	**2043110336**
PRANAV TASKAR	**2143110241**
NARGIS SHAH	**2143110253**

UNDER THE GUIDANCE OF
PROF. RESHMA KANSE



DEPARTMENT OF INFORMATION TECHNOLOGY
BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)
DEPARTMENT OF ENGINEERING AND TECHNOLOGY, NAVI MUMBAI

2023-2024

DEPARTMENT OF INFORMATION TECHNOLOGY
BHARATI VIDYAPEETH DEEMED TO BE UNIVERSITY
DEPARTMENT OF ENGINEERING AND TECHNOLOGY, NAVI MUMBAI

2023-2024

CERTIFICATE

This is certify that the project entitled

"MALWARE ANALYSIS USING SANDBOX"

submitted by

Aditi Thakur	**2043110234**
Shubham Jha	**2043110236**
Pranav Taskar	**2143110241**
Nargis Shah	**2143110253**

is a record of bonafide work carried out by them, in the partial fulfilment of the requirement for the award of Degree of Bachelor of Technology in INFORMATION TECHNOLOGY at **BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY) DEPARTMENT OF ENGINEERING AND TECHNOLOGY, NAVI MUMBAI.** This work is done during academic year 2023-2024.

Date: / /

(Prof. Dr. Kamal Mehta)	**(Prof. Reshma Kanse)**	**Name of external**
HOD, Information Technology	**Project Guide**	**External Examiner**

Acknowledgements

We would like to express deepest appreciation towards Prof. Dr. Mohan Awasthy, Principal, DEPARTMENT OF INFORMATION TECHNOLOGY, **Bharati Vidyapeeth Deemed To Be University Department Of Engineering And Technology, Navi Mumbai**, and Prof. Dr. Kamal Mehta, Head of Department of Information Technology, who invaluable supported us in completing this project.

We are profoundly grateful to Prof. RESHMA KANSE, Project guide for his/her expert guidance and continuous encouragement throughout to see that this project rights, its target since its commencement to its completion.

At last, we must express our sincere heartfelt gratitude to all the staff members of the department of IT who helped me directly or indirectly during this course of work.

ADITI THAKUR
SHUBHAM JHA
PRANAV TASKAR
NARGIS SHAH

ABSTRACT

As the threat landscape of cyberattacks continues to evolve, the need for robust malware analysis tools becomes imperative. This project introduces an innovative Malware Sandbox, designed to enhance cybersecurity through dynamic analysis of malicious software. The sandbox employs cutting-edge technologies to dissect and scrutinize suspicious files in a controlled environment, providing a deeper understanding of their behavior and potential threats. Key features of the Malware Sandbox include dynamic code analysis, behavior monitoring, and threat intelligence integration. By executing malware in an isolated environment, the sandbox allows for real-time observation of its actions, enabling the identification of malicious activities such as file system modifications, network communication, and system registry alterations. Additionally, the integration of threat intelligence feeds ensures that the sandbox stays updated with the latest information on emerging threats, enhancing its detection capabilities.

The project prioritizes user-friendly interfaces, ensuring seamless interaction for both security professionals and researchers. Keyword-driven searching and detailed reporting mechanisms facilitate efficient analysis and reporting of findings. The Malware Sandbox supports a variety of file types, making it adaptable to diverse cyber threats. This initiative represents a crucial step forward in the ongoing battle against cyber threats, providing a proactive defense mechanism to safeguard digital environments. The combination of dynamic analysis, behavior monitoring, and threat intelligence integration establishes a comprehensive solution for identifying and mitigating malware risks effectively.

Keywords: behavior monitoring, cybersecurity, dynamic analysis, malware, sandbox, security professionals, threat intelligence, threat landscape.

Contents

List of Figures

Chapter 1

Introduction

1.1 Introduction

A malicious computer program is one that causes damage to the machine on which it is run. An important part of examining the features and actions of malware is malware analysis. Malware analysis is a laborious, time-consuming procedure that requires a lot of manual labor. Identifying the kind of the Malware frequently speeds up the analysis process and enables the researcher to learn more about the capabilities of the binary. Typically, researchers use tools like strings and dependency walkers among other static analysis techniques to identify the malware's category. However, while millions of new malware samples are produced every day, manually classifying them is not a practical option.

Malware analysis helps the researchers to find out the functionality of the malware. Malware analysis comprises of two major types:

1. Static Malware analysis
2. Dynamic Malware analysis

Types of malware:

1. **Backdoor:** A malware backdoor is a type of malicious software that creates a secret entry point into a computer system or network, allowing attackers to gain unauthorized remote access. Typically installed through various means such as email attachments or exploiting vulnerabilities, the backdoor operates stealthily, evading detection by security software. Once established, attackers can remotely control the infected system, executing commands, stealing data, or even using it as a launchpad for further attacks. Malware backdoors are designed to maintain persistence, making them challenging to detect and remove. They pose significant risks to individuals, organizations, and critical infrastructure, emphasizing the importance of robust cyber security measures to mitigate such threats.
2. **Downloader:** Downloader malware, often known as simply **"downloaders"**, is a malicious software type crafted to surreptitiously download and execute other harmful payloads on a victim's system. Serving as the initial stage of a cyberattack, downloaders enable attackers to establish a foothold on the compromised device, facilitating further malicious activities. They operate covertly, employing tactics like obfuscation and encryption to evade detection by security measures and users. Once installed, downloaders establish a connection to a remote server controlled by the attacker, retrieving additional malware payloads to execute. These payloads can encompass various types of malware, including **trojans, ransomware, spyware, and adware.** Downloaders exploit vulnerabilities in software or leverage social engineering tactics, such as phishing emails or fake software updates, to infiltrate systems. Given their ability to

deliver diverse and damaging payloads, downloader malware poses significant risks to individuals, businesses, and organizations, emphasizing the importance of robust cybersecurity measures and user awareness to thwart such threats.

3. **Keylogger:** Keyloggers are a type of software or hardware specifically designed to record every keystroke made on a computer or mobile device. They are typically used covertly to monitor and capture users' keystrokes, including sensitive information such as usernames, passwords, credit card numbers, and other personal data. Keyloggers can be deployed for various purposes, ranging from legitimate uses such as parental control or employee monitoring to malicious activities such as identity theft, espionage, or unauthorized access to systems. Software-based keyloggers are often installed surreptitiously through malware or phishing attacks, while hardware keyloggers are physical devices inserted between the keyboard and the computer. Detection and prevention of keyloggers typically involve using antivirus software, employing strong security practices such as two-factor authentication, and regularly monitoring system activity for signs of unauthorized access or data exfiltration. Overall, keyloggers represent a significant privacy and security threat, highlighting the importance of proactive cybersecurity measures to protect against them.

4. **Trojans:** A Trojan, derived from the mythical Greek horse, is a deceptive form of malware that masquerades as legitimate software to infiltrate computers or networks, often through social engineering tactics like phishing emails or malicious downloads. Once executed, Trojans can perform a variety of malicious actions, including stealing sensitive data, modifying system settings, spying on user activities, or recruiting infected devices into botnets for further attacks. Their ability to operate stealthily and evade detection makes Trojans a significant cybersecurity threat, emphasizing the importance of employing robust antivirus software, keeping systems updated, and practicing caution when interacting with unknown or suspicious content online to mitigate the risk of infection.

5. **Ransomeware:** Ransomware is a kind of malicious software that encrypts files on a victim's computer or network, making them unreadable. The virus then demands payment, typically in cryptocurrency, to unlock the files and allow access again. Ransomware attacks typically involve encrypting a wide range of files, including documents, photos, videos, and databases, using strong encryption algorithms that are difficult to break without the decryption key held by the attackers. Once files are encrypted, the attackers display a ransom note, often with instructions on how to make the payment and receive the decryption key. Ransomware infections can occur through various means, including phishing emails, malicious attachments, compromised websites, or exploiting vulnerabilities in software or networks. Attacks utilizing ransomware can have serious repercussions, including data loss, monetary loss, and operations disruption for people, companies, and even vital infrastructure. Prevention measures include regular data backups, keeping software up-to-date, using reputable antivirus software, and educating users about phishing and other common attack vectors.

1.2 Motivation

In the dynamic landscape of cybersecurity, the relentless evolution of malware poses an escalating threat to individuals, organizations, and nations alike. As malicious actors employ increasingly sophisticated techniques, it becomes imperative for the cybersecurity community to enhance its capabilities in understanding, detecting, and mitigating these threats. This project on malware sandbox analysis aims to address this critical need, providing a comprehensive exploration of the intricacies involved in analyzing and combating malware through the lens of sandbox technology.

Rising Sophistication of Malware: Malicious software is continuously evolving, exhibiting heightened complexity and adaptability. The motivation behind this project stems from the urgent requirement to delve deep into the anatomy of modern malware. By employing malware sandbox analysis, we seek to unravel the sophisticated techniques employed by malware to evade detection, infiltrate systems, and compromise data integrity.

Enhancing Cybersecurity Resilience: Cybersecurity is a cornerstone of contemporary digital ecosystems. Understanding the behavior and characteristics of malware is fundamental to fortifying the defenses against cyber threats. Through meticulous sandbox analysis, this project aspires to contribute to the development of robust cybersecurity measures, thereby bolstering the resilience of systems and networks against diverse malware attacks.

Proactive Threat Intelligence: The proactive nature of malware sandbox analysis is a pivotal factor in its significance. By dissecting malware within a controlled environment, we gain valuable insights into its functionalities, propagation methods, and potential impact. These insights not only aid in immediate threat mitigation but also contribute to the formulation of threat intelligence, empowering cybersecurity professionals to anticipate and counteract emerging threats.

Facilitating Incident Response: In the unfortunate event of a security breach, swift and effective incident response is crucial. Malware sandbox analysis plays a pivotal role in expediting incident response efforts by providing in-depth information about the nature of the attack. This project seeks to explore how the integration of sandbox analysis into incident response frameworks can significantly reduce the time to identify, contain, and eradicate malware.

Educational Value and Knowledge Dissemination: Beyond its practical applications, this project also aims to serve as an educational resource. By comprehensively documenting the methodology and findings of malware sandbox analysis, it contributes to the collective knowledge base of the cybersecurity community. This educational aspect is crucial for fostering a well-informed and proactive cybersecurity culture.

1.3 Problem Statement

The problem at hand is to develop an advanced and systematic approach to malware sandbox analysis. This approach should address the limitations of current methodologies by providing a detailed behavioral profile of malware, robust signature development, seamless incident response integration, and effective knowledge dissemination. Standardizing the evaluation of sandbox technologies and ensuring ethical compliance in the acquisition of malware samples are crucial aspects that need to be addressed to enhance the overall effectiveness of malware analysis and fortify cybersecurity measures

against evolving threats.

1.4 Objectives

The objectives are as follows:

- Conduct thorough analysis to profile the behavioral characteristics of diverse malware specimens within controlled sandbox environments.
- Derive robust signatures based on behavioral patterns, contributing to the creation of a comprehensive malware signature database.
- Assess and compare the efficiency, accuracy, and scalability of different malware sandbox technologies.
- Implement the seamless integration of malware sandbox analysis into incident response frameworks to enhance the speed and effectiveness of threat mitigation.
- Extract actionable threat intelligence from sandbox analysis, supporting proactive cybersecurity measures.
- Document the entire malware sandbox analysis process and implement the creation of educational materials for effective knowledge dissemination.

Chapter 2

Literature Survey

2.1 Literature Review

Ref. No	Paper Title	Journal/Published In/ISSN/Author(year)	Goal of Research Paper	Techniques	Gaps
1	Analyzing and comparing the effectiveness of malware detection: A study of machine learning approaches	Heliyon / Muhammad Azeem, Danish Khan, Saman Iftikhar, Shaikhan Bawazeer, Mohammed Alzahrani (2024)	To explore malware detection and classification elements using modern machine learning approaches	K-Nearest Neighbors, Extra Tree, Random Forest, Logistic Regression, Decision Tree, neural network Multilayer Perceptron	Deep learning models limitations in malware detection and classification.
2	A Literature Review on Malware and its Analysis	IJCRR Vol 05 issue 16/ Aparna Verma, M.S.Rao, A.K.Gupta, W. Jeberson, Vrijendra Singh(2013)	To examine available literature on malware analysis and determine how research has evolved	Literature review	Lack of specific focus on advanced malware analysis techniques.
3	Sandbox Environment for Real-Time Malware Analysis of IoT Devices	Research Gate/ Gaurav Pramod Kachare, Gaurav Choudhary, Shishir Kumar Shandilya and Vikas Sihag (2022)	To propose a sandbox environment concept model for analyzing advanced malware in IoT devices securely	Sandbox environment, machine learning algorithms (Convolutional Neural Networks), static malware analysis, real-time malware analysis, network analysis	Lack of detailed evaluation of the proposed sandbox environment model

Ref. No	Paper Title	Journal/Published In/ISSN/Author(year)	Goal of Research Paper	Techniques	Gaps
4	Malware Detection and Prevention using Artificial Intelligence Techniques	Md Jobair Hossain Faruk, Hossain Shahriar, Maria Valero, Farhat Lamia Barsha, Shahriar Sobhan, Md Abdullah Khan, Michael Whitman, Alfredo Cuzzocreak, Dan Lo, Akond Rahman and Fan Wu	To emphasize Artificial Intelligence (AI) based techniques for detecting and preventing malware activity	Artificial Intelligence (AI), Machine Learning, Deep Learning	Limited discussion on specific AI algorithms or methodologies used for malware detection and prevention
5	A Pilot Comparative Analysis of the Cuckoo and Drakvuf Sandboxes: An End-User Perspective	Military Technical Courier/ Slaviša Ž. Ilić, Milan J. Gnjatović, Brankica M. Popović, Nemanja D. Maček (2022)	To conduct a comparative analysis of the Cuckoo and Drakvuf sandboxes in terms of their usefulness for human analysts in malware analysis	Sandbox analysis	Lack of detailed technical analysis beyond the evaluation based on web console reports
6	A Study on Ransomware and its Effect on India and Rest of the World	International Journal of Engineering Research and Technology (IJERT)/ ISSN: 2278-0181/ Naveen Kumar C.G and Dr.Sanjay Pande M.B (2017)	To study the recent attack of ransomware, its history, impact on India and the rest of the world, and mechanisms to prevent ransomware	Literature review, analysis of ransomware attacks	Lack of empirical data or case studies to support the discussion on the impact of ransomware
7	A Comparative Study of Behavior Analysis Sandboxes in Malware Detection	ResearchGate/ Joshua Tommy Juwono, Charles Lim, Alva Erwin(2015)	To compare the accuracy of two behavior analysis sandboxes in detecting malware using commonly used machine learning algorithms	Dynamic analysis, machine learning algorithms (Random Forest, Support Vector Machine), malware detection	Lack of detailed discussion on the limitations or challenges faced during the experiment

Ref. No	Paper Title	Journal/Published In/ISSN/Author(year)	Goal of Research Paper	Techniques	Gaps
8	An Analysis of Faculty and Staff's Identification of Malware Threats	Dr. Todd Emma, Dr. Brian Bennett, Dr. Megan Quinn(2016)	To analyze faculty and staff members' ability to identify malware threats, particularly focusing on eight common malware categories in higher education systems	Survey, scenario-based assessment	Lack of detailed methodology description and statistical analysis of the survey results
9	An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability	Journal of Cybersecurity/ Lena Yuryna Connolly, David S. Wall, Michael Lang, Bruce Oddson (2020)	To assess the severity of ransomware attacks experienced by organizations and identify factors influencing the severity	Quantitative and qualitative analysis of 55 ransomware cases	Lack of detailed breakdown of the quantitative and qualitative data analysis methods used
10	Introduction to Malware and Malware Analysis: A brief overview	International Journal of Advance Research in Computer Science and Management/ISSN: 2321-7782/ Anusmita Ray and Dr. Asoke Nath (2016)	o discuss the various issues in malware and malware analysis	Static analysis, Dynamic analysis	Limitations of static analysis, Sophistication of malware attacks outpacing software development pace

Ref. No	Paper Title	Journal/Published In/ISSN/Author(year)	Goal of Research Paper	Techniques	Gaps
11	Malware Detection Issues, Challenges, and Future Directions: A Survey	Applied Sciences/ ISSN: 2076-3417/ Faitouri A. Aboaoja, Anazida Zainal, Fuad A. Ghaleb, Bander Ali Saleh Al-rimy, Taiseer Abdalla Elfadil Eisa and Asma Abbas Hassan Elnour (2022)	To provide a comprehensive review of malware detection models, focusing on analysis and detection approaches, feature representation, and associated data types	Signature-based, Behavioral-based, Heuristic-based	Lack of detailed taxonomy for malware detection approaches beyond generic categories, Neglect of feature representation methods in some review papers, Addressing challenges and future research directions needed
12	Automating Linux Malware Analysis Using Limon Sandbox	Monnappa K A	To introduce Limon, a Python-based sandbox for automated Linux malware analysis, and to discuss its features and capabilities	Static Analysis, Dynamic Analysis, Memory Analysis	Lack of detailed discussion on specific malware analysis results or case studies, Potential challenges or limitations of Limon not addressed
13	Computer Viruses	International Journal of Engineering Research and Technology (IJERT)/ ISSN: 2278-0181/ Maria Thomas(2015)	To discuss various types of computer viruses, their characteristics, modes of infection, effects, detection methods, prevention measures, and types of antivirus software	Historical Analysis, Description of Virus Types, Detection Methods, Prevention Strategies	Limited discussion on advanced virus detection techniques (e.g., heuristic analysis, behavior analysis), Potential challenges in virus detection and prevention not addressed

Ref. No	Paper Title	Journal/Published In/ISSN/Author(year)	Goal of Research Paper	Techniques	Gaps
14	Malware Analysis Through High-level Behavior	Xiyue Deng and Jelena Mirkovic	To investigate malware's network behavior during execution, propose a behavior classification approach based on observed network traffic, and apply the approach to diverse malware samples to understand current trends in malware behaviors	Malware Network Behavior Analysis, Behavior Classification, Fantasm Platform on DeterLab Testbed	Limited discussion on the effectiveness of the proposed behavior classification approach in real-world scenarios, Potential challenges in applying the approach to a larger dataset of malware samples not addressed
15	A Study on Malware Analysis Leveraging Sandbox Evasive Behaviors	Takahiro KASAMA(2014)	To discuss techniques employed by malware and malware authors to evade analysis and detection, categorize evasion techniques against sandbox analysis, and propose countermeasure techniques against evasive malware	Malware Evasion Techniques, Sandbox Analysis, Countermeasures, Behavior-based Malware Detection	Limited discussion on the scalability and practical implementation challenges of proposed countermeasure techniques, Potential limitations in the effectiveness of the proposed behavior-based malware detection method in real-world scenarios

Ref. No	Paper Title	Journal/Published In/ISSN/Author(year)	Goal of Research Paper	Techniques	Gaps
16	Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges, and Future Directions	IEEE/ NOR ZAKIAH GORMENT, ALI SELAMAT, LIM KOK CHENG AND ONDREJ KREJCAR (2023)	To conduct a thorough systematic literature review (SLR) and provide a taxonomy of machine learning methods for malware detection, addressing shortcomings in performance accuracy, analysis type, and detection approaches	Systematic Literature Review, Taxonomy Development, Machine Learning Methods	Lack of discussion on the scalability and real-world applicability of the proposed taxonomy, Limited exploration of emerging machine learning techniques for malware detection, Potential biases in the selection and analysis of the chosen research works
17	Malware Detection and Analysis	Namratha Suraneni(2022)	To discuss various forms of malware, concealment strategies, attack mechanisms, detection methods, and classification models	Malware Analysis Techniques, Malware Detection Techniques, Classification Models, Image Analysis	Limited discussion on specific machine learning algorithms for malware detection, Lack of empirical evaluation of proposed detection methods, Limited exploration of emerging malware concealment strategies

Ref. No	Paper Title	Journal/Published In/ISSN/Author(year)	Goal of Research Paper	Techniques	Gaps
18	Malware Analysis Sandbox Testing Methodology	THE JOURNAL ON CYBERCRIME and DIGITAL INVESTIGATIONS/ Zoltan Balazs (2015)	To propose a practical approach for detecting sandbox-aware malware and circumventing sandbox detection techniques	Malware Analysis Sandbox, Anti-sandboxing	Limited discussion on the practical implementation details of the proposed approach, Lack of empirical evaluation of the proposed method's effectiveness, Potential limitations in scalability and adaptability to evolving sandbox detection techniques
19	Malware Automatic Analysis	César Augusto Borges de Andrade, Claudio Gomes de Mello, Julio Cesar Duarte	To propose an automated approach for identifying malware using sandbox and machine learning techniques, aiming to overcome the impracticality of manual signature-based scanning	Malicious code analysis, Sandbox techniques, Machine learning	Lack of detailed discussion on the specific sandbox and machine learning techniques employed, Limited exploration of the potential limitations and challenges of the proposed approach, Potential issues related to scalability and adaptability in real-world environments

Ref. No	Paper Title	Journal/Published In/ISSN/Author(year)	Goal of Research Paper	Techniques	Gaps
20	Malware Analysis: An Introduction	Dennis Distler (2007)	To provide a detailed introduction to malware analysis for security professionals, addressing the common malware issues in computer security	Malware types, Incident response plan basics, Malware analysis goals, Static and behavioral analysis techniques, Tools for analysis, Malware acquisition methods, Methodology for malware analysis, Real-world malware analysis example, Defense mechanisms against malware	Lack of detailed discussion on specific malware types and their characteristics, Potential oversight of emerging malware trends and advanced evasion techniques, Limited exploration of the legal and ethical considerations in malware analysis
21	Malware Analysis and Classification: A Survey	Journal of Information Security/ Ekta Gandotra, Divya Bansal, Sanjeev Sofat (2014)	To provide an overview of techniques for analyzing and classifying malware to address the challenges posed by polymorphic and metamorphic malware	Static Analysis, Dynamic Analysis, Machine Learning, Classification, Clustering	Limited discussion on specific machine learning algorithms used for malware classification, Lack of detailed case studies or empirical evaluations of the proposed techniques, Potential oversight of emerging malware evasion techniques

Ref. No	Paper Title	Journal/Published In/ISSN/Author(year)	Goal of Research Paper	Techniques	Gaps
22	A Study of Ransomware Attacks: Evolution and Prevention	JOURNAL OF SOCIAL TRANSFORMATION AND REGIONAL DEVELOPMENT/ Aini Khalida Muslim, Dzunnur Zaily Mohd Dzulkifli, Mohammed Hayder Nadhim, Roy Haizal Abdellah (2019)	To examine the evolution of ransomware and propose preventive measures against it, based on secondary data collected from telemetry data by Symantec	Data Collection, Analysis of Telemetry Data, Examination of Ransomware Evolution, Proposal of Preventive Measures	Limited discussion on specific preventive measures proposed, Potential oversight of emerging ransomware variants and evasion techniques, Lack of detailed analysis on the effectiveness of proposed preventive measures

Table 2.1: Literature Review

Chapter 3

Proposed Methodology

3.1 Proposed system

Malware sandbox analysis focuses on in-depth analysis of specific malware categories: phishing attacks, worms, and keyloggers. It leverages a combined approach of dynamic execution, network behavior monitoring, and user interaction simulation to provide detailed insights into their functionalities and potential dangers.

Key Features:

- **Targeted Sandbox Environment:** Utilizes dedicated virtual machine (VM) configurations tailored for each malware category (e.g., web browser VM for phishing attacks, network-oriented VM for worms). Integrates plugins and tools specific to each type, like web capture tools for phishing analysis or network traffic monitors for worm propagation studies.
- **Advanced Network and User Interaction Simulation:** Simulates realistic user interactions and network environments to trigger malware functionalities and expose hidden tactics. Captures detailed data on network communication, web browsing behavior, and keystroke logging to understand attack vectors and data exfiltration techniques.
- **Behavior Profiling and Threat Scoring:** Analyzes captured data using machine learning algorithms to identify patterns and anomalies specific to each malware category. Assigns dynamic threat scores based on observed behavior, providing a risk assessment and prioritization for further investigation.
- **Automated Reporting and Visualization:** Generates comprehensive reports with screenshots, network diagrams, and keystroke logs for each analysis session. Utilizes interactive dashboards to visualize malware behavior and highlight critical events, facilitating efficient incident response.
- **Threat Intelligence Integration:** Connects to relevant threat intelligence feeds to enrich analysis with known indicators of compromise (IOCs) and attack patterns. Correlates observed behavior with existing threat data to identify potential variants and improve detection accuracy.
- **Scalability and Performance:** Employs containerization technology for efficient allocation of resources and concurrent analysis of multiple samples. Optimizes VM configurations and monitoring tools to handle resource-intensive malware without performance degradation.
- **Deployment and Maintenance:** Available as a cloud-based service or on-premise deployment for flexible implementation. Offers automatic updates and security patches to ensure continuous effectiveness against evolving threats.

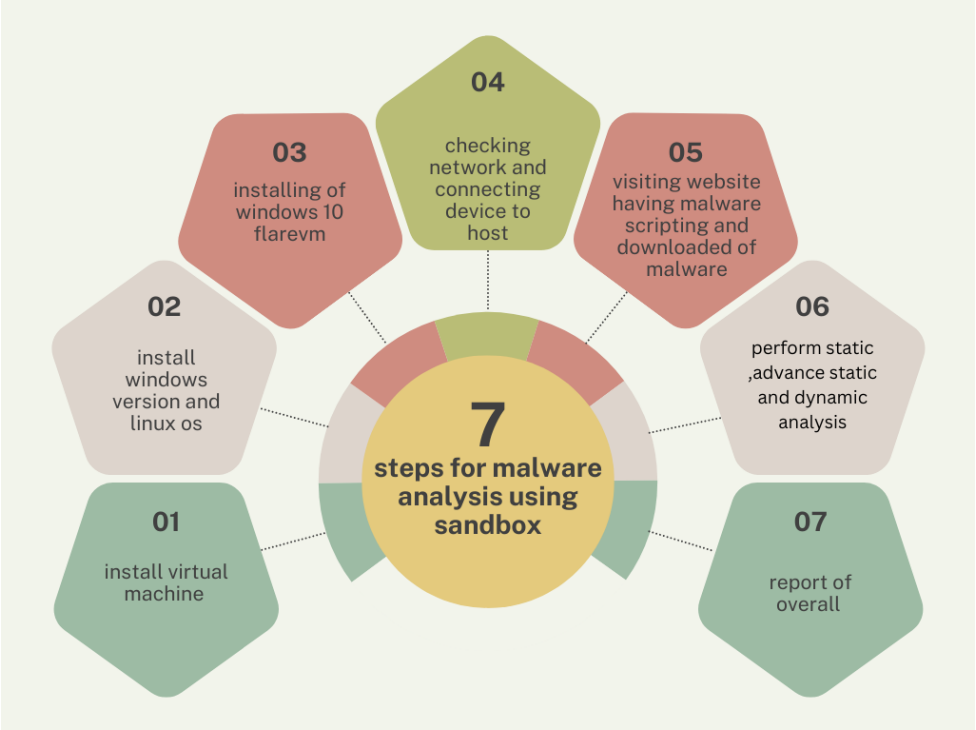


Figure 3.1: Procedure for Proposed System

Chapter 4

Software Requirements Specification

4.1 Software Requirement Specification:

1. Virtual Box
2. Windows 10 Flare VM
3. Remnux Linux
4. Pestudio
5. Cmdr
6. Wireshark
7. Terminal
8. Cutter
9. Procmon
10. VirusTotal
11. Wayback Archive

4.2 Hardware Requirement Specification:

1. System : Intel I5 Processor and above.
2. Hard Disk : 1TB
3. Ram : 6GB

Chapter 5

Requirement Analysis

5.1 Requirement Analysis

1) Comprehensive Behavioral Profiling: Implementing a thorough behavioral profiling mechanism to capture diverse aspects of malware behavior within the sandbox environment, including file system interactions, network communications, system calls, and registry modifications.

2) Robust Signature Development: Developing robust signatures based on behavioral analysis to detect similar variants of malware, contributing to threat intelligence databases for proactive defense measures.

3) Seamless Incident Response Integration: Integrating the malware sandbox analysis system seamlessly with incident response procedures and security operations centers (SOCs) to enable rapid detection, analysis, and response to potential threats identified through sandbox analysis.

4) Timely Threat Intelligence: Establishing mechanisms for timely dissemination of threat intelligence derived from malware sandbox analysis, including sharing indicators of compromise (IOCs), behavioral patterns, and mitigation strategies with relevant stakeholders in the cybersecurity community.

5) Standardized Evaluation Framework: Developing a standardized framework for evaluating the effectiveness and efficiency of malware sandbox technologies, encompassing criteria such as detection rate, false positive/negative rates, scalability, and ease of deployment.

6) Ethical Compliance in Sample Acquisition: Ensuring ethical compliance in the acquisition of malware samples for analysis by adhering to legal and ethical guidelines, obtaining consent when necessary, and safeguarding privacy rights during the collection and use of malware samples.

7) Scalability and Performance Optimization: Designing the solution to be scalable and capable of handling large volumes of malware samples efficiently, optimizing performance to minimize analysis time while maintaining accuracy and reliability.

Chapter 6

System Design

6.1 System Design

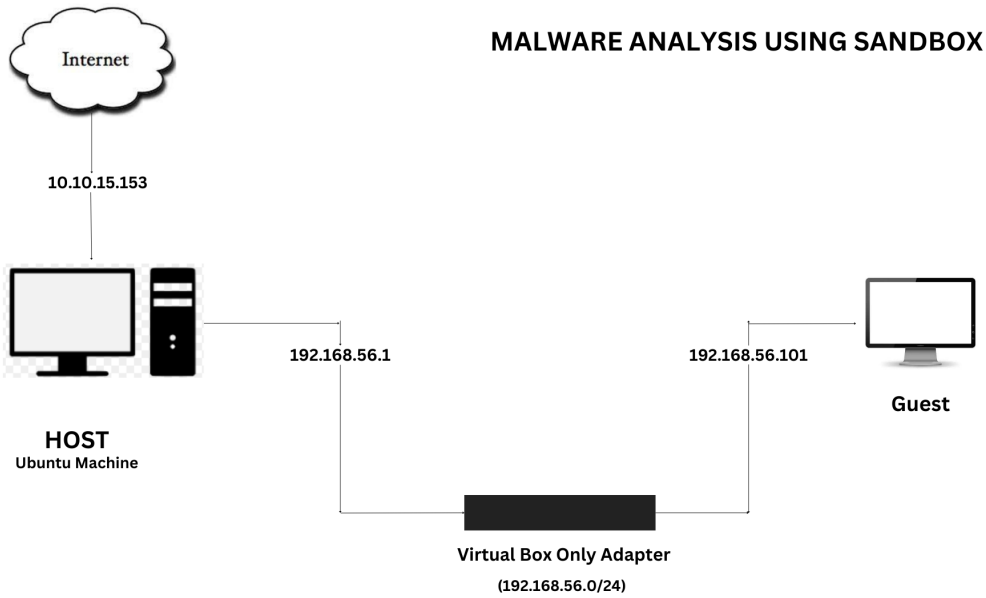


Figure 6.1: System Design

6.2 System Framework

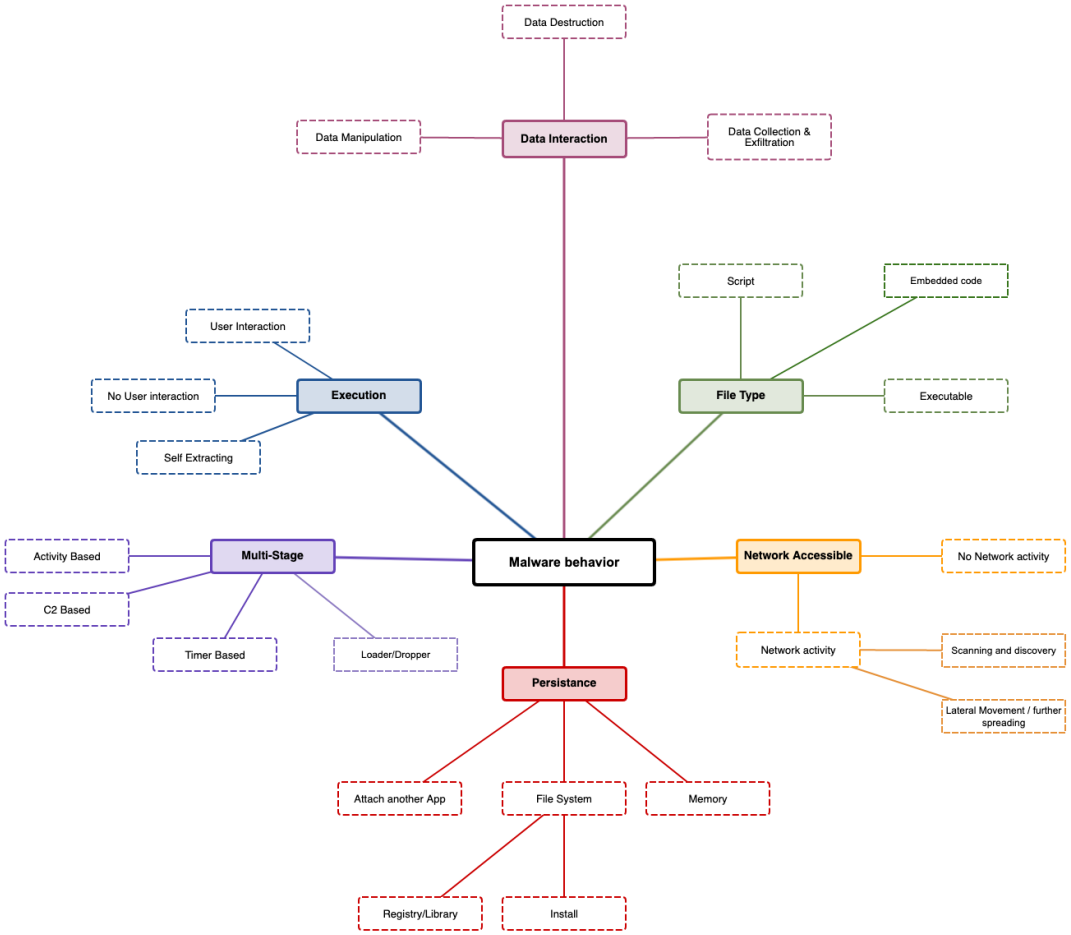


Figure 6.2: System Framework

6.3 Activity Diagram

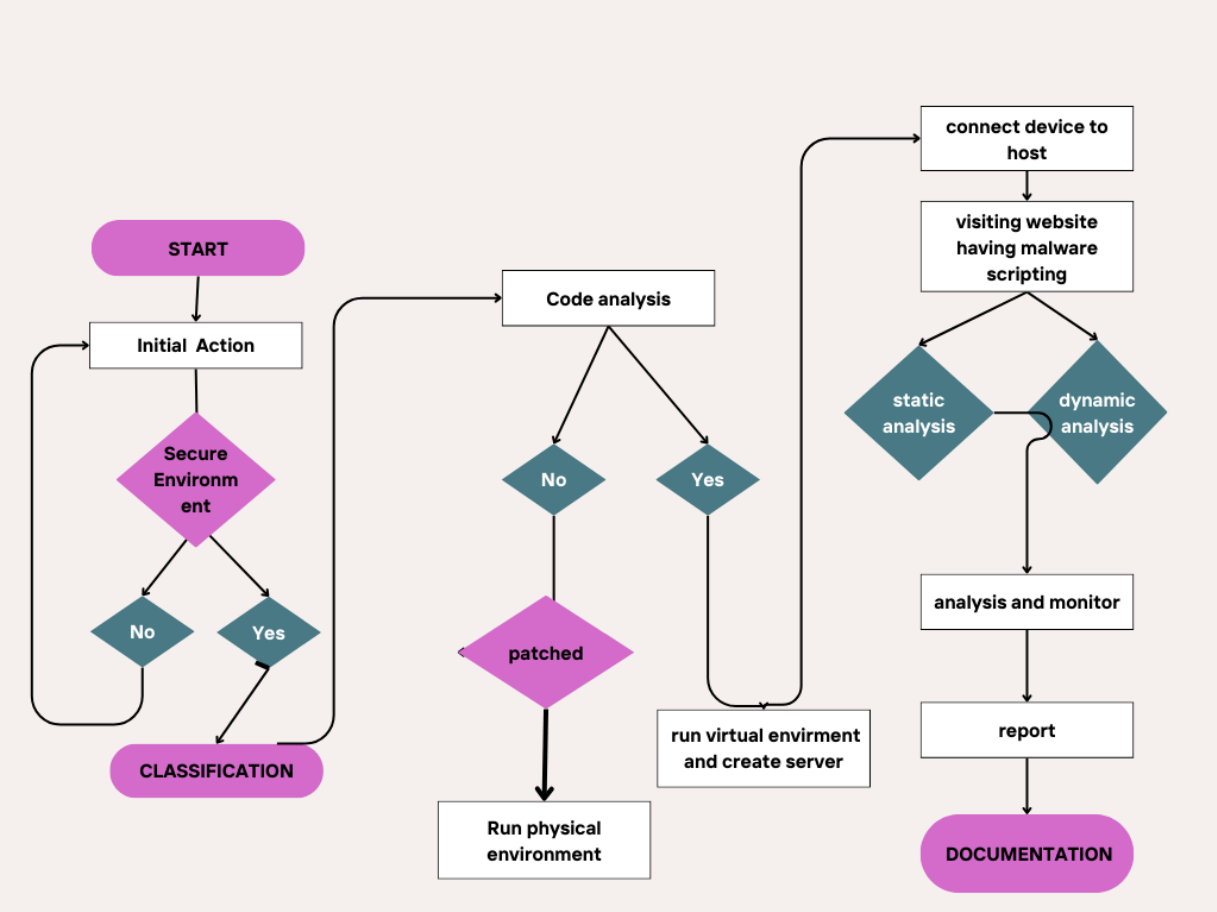


Figure 6.3: Activity Diagram

6.4 Use Case Diagram

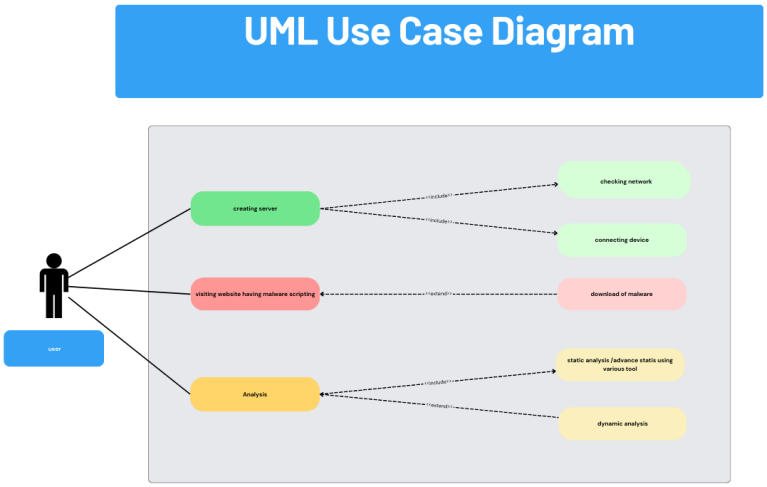


Figure 6.4: Use Case Diagram

6.5 Block Diagram

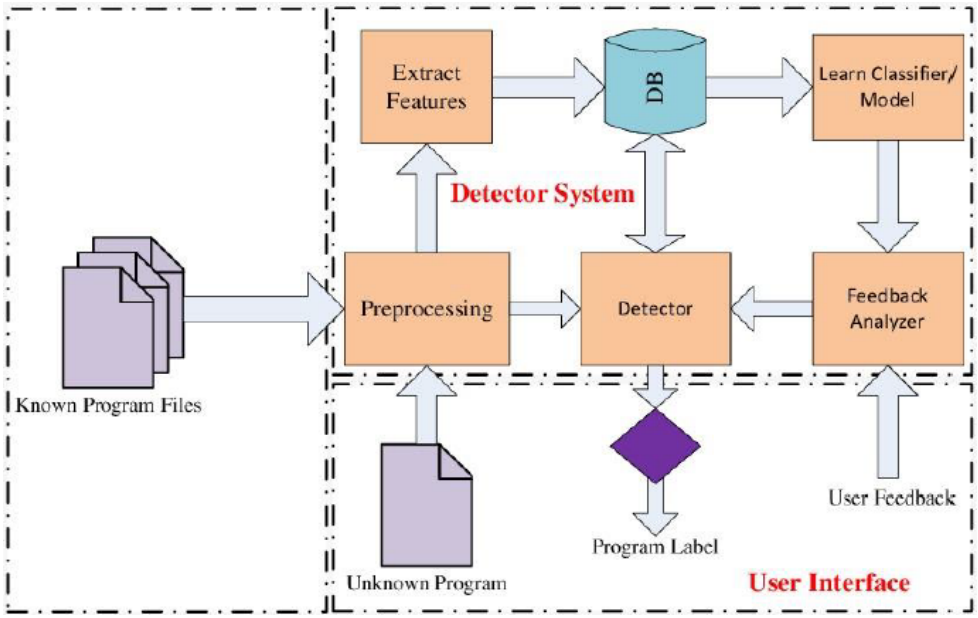


Figure 6.5: Block Diagram

Chapter 7

Project Planning

Establishing a malware analysis lab requires meticulous planning to ensure effectiveness, security, and compliance. Here's a comprehensive project plan to guide the setup and operation of such a lab.

1. **Define Objectives:**
   - Clearly outline the purpose of the lab, such as identifying and analyzing new malware threats, understanding their behavior, and developing countermeasures.
2. **Team Formation:**
   - Assemble a multidisciplinary team including malware analysts, reverse engineers, network security specialists, and legal/compliance experts.
3. **Infrastructure Setup:**
   - Procure hardware (servers, workstations, networking equipment) and software (malware analysis tools, virtualization platforms) needed for analysis and research.
   - Implement robust security measures to isolate the lab environment from the rest of the network and the internet to prevent accidental leaks or infections.
4. **Tool Selection:**
   - Evaluate and select appropriate tools for static and dynamic malware analysis, including sandboxing, disassembly, and debugging tools.
   - Consider open-source and commercial options based on functionality, scalability, and budget constraints.
5. **Malware Sample Acquisition:**
   - Establish procedures for safely obtaining malware samples from reputable sources, such as threat intelligence feeds, malware repositories, and honeypots.
   - Implement strict protocols to ensure legal compliance and minimize the risk of handling malicious code.
6. **Analysis Workflow:**
   - Develop standardized procedures and workflows for analyzing malware samples, including sample submission, initial triage, static and dynamic analysis, and reporting.
   - Document analysis findings, including indicators of compromise (IOCs), behavioral characteristics, and mitigation strategies.
7. **Training and Skill Development:**
   - Provide ongoing training and skill development opportunities for lab personnel to stay abreast of the latest malware trends, analysis techniques, and defensive strategies.

- Encourage collaboration and knowledge sharing within the team and with external partners and industry peers.

8. **Incident Response Integration:**
   - Integrate the malware analysis lab with the organization's incident response plan to facilitate rapid detection, analysis, and containment of malware-related incidents.
   - Establish communication channels and escalation procedures to coordinate response efforts across different teams and departments.

9. **Compliance and Legal Considerations:**
   - Ensure compliance with relevant laws, regulations, and industry standards governing the handling of malware samples and sensitive information.
   - Implement appropriate data protection measures and obtain necessary permissions for storing and analyzing malware samples.

10. **Continuous Improvement:**
    - Regularly review and update the lab's processes, procedures, and technologies to adapt to evolving threats and organizational requirements.
    - Collect feedback from stakeholders and leverage lessons learned from past analyses to enhance the effectiveness and efficiency of the lab.

11. **Documentation and Reporting:**
    - Maintain detailed documentation of all activities, analyses, and findings conducted in the lab, including metadata, timestamps, and analysis artifacts.
    - Produce comprehensive reports summarizing analysis results, key insights, and recommendations for remediation and future prevention.

12. **Collaboration and Information Sharing:**
    - Foster collaboration with external stakeholders, such as industry peers, law enforcement agencies, and security vendors, to exchange threat intelligence and best practices.
    - Participate in information-sharing initiatives, such as ISACs (Information Sharing and Analysis Centers), to stay informed about emerging threats and vulnerabilities.

Chapter 8

Implementation

8.1 Implementation Details

1. **Set up a virtual machine** It is best to run malware in a completely isolated environment to prevent infection of the host operating system. Although having a separate computer is preferable, you can set up multiple virtual machines with various operating systems. Numerous virtual machines (VMs) are available on the market, including Microsoft Hyper-V, Parallels, Oracle VM VirtualBox, KVM, VMware, and Xen.

2. **Examine the items** Malware nowadays is intelligent; it can tell if it is operating on a virtual machine or not. For this reason, it's imperative to discard artifacts. Verify the code, eliminate any detection, and more.

3. **Switch to an alternative network** Using an alternate network system is an additional safety measure. It's critical to keep other machines on your network from becoming infected. Purchase a VPN service, then configure it properly. The traffic leak cannot originate from a legitimate IP address.

4. **Give each resource a reasonable amount of work** Making a system appear as genuine as feasible is our aim in order to deceive any malicious program into running. A reasonable number of resources should be allocated, such as more than 4GB of RAM, at least 4 cores, and at least 100GB of disk space. That is a prerequisite for pretending to be a genuine system. Furthermore, remember that malware examines the hardware settings. A malicious object recognizes a virtual machine by name and ceases operation if it is found anywhere.

5. **Set up frequently used applications** Installing Windows without making any changes will result in a malicious object being detected and examined. Install a few standard programs that every user should have, such as Word and browsers.

6. **Launch several files** Here, we must demonstrate that this is a legitimate computer that is someone's property. To gather logs and a few temporary files, open a few documents. Numerous virus kinds verify this. Regshot and Process Monitor are useful tools for recording changes to the file system and registry. Keep in mind that while these apps are operating, virus can find them.

Below are the trojans multiple hash keys across various tools and the file type.

```
File Name - invoice_2318362983713_823931342io.pdf.exe
general, executable program>
file > sha256,69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169
dos-stub > sha256,6960FDC23907135D89201041AB3E8A222D0D9D327C4A16ADA1037BB1DAA11197
dos-header > sha256,5D85EEA79E3B682F8FE35296C9C506B0960112F39CC275078E096295EFF02644
rich-header > sha256,CD3CD6CDB421DA509FDE21CB41B183E51E145371F844B5DE628A3A2E873ABFF6
section > .text > sha256,8309B5D320B3D392E25AFD57793E6BB9D54A3AEACA697759963B008F3367B352
section > .data > sha256,510A0F9FAF189356CA7819AC6A5CBE1DA1D94EA110158E1C4D3BCB753C458BA5
section > .itext > sha256,4CDD5D9821CC0790A1D7031EF6CD3DFA9E68B967279D3BD2F0DE781EBCB95389
section > .pdata > sha256,70CC3E025CCED228E4EBB21E54B904A2E0CCEC85C0B0E292A1E12E7C819DB0AE
section > .rsrc > sha256,CB1CB914AD7F61C98BFB6506306E31A8D94DF71B078C69405E9FBD8DD289C54F
section > .reloc > sha256,7C2F4C4DB94369F90B2A41459CB3FB96EB9E9FF0D8631B7C6562467F0D8924B9
manifest > sha256,781AA123142F5551ABCD8D75E34CB3E24686341235276240580E4F3244616C9D
,
special, imphash > md5,n/a
```

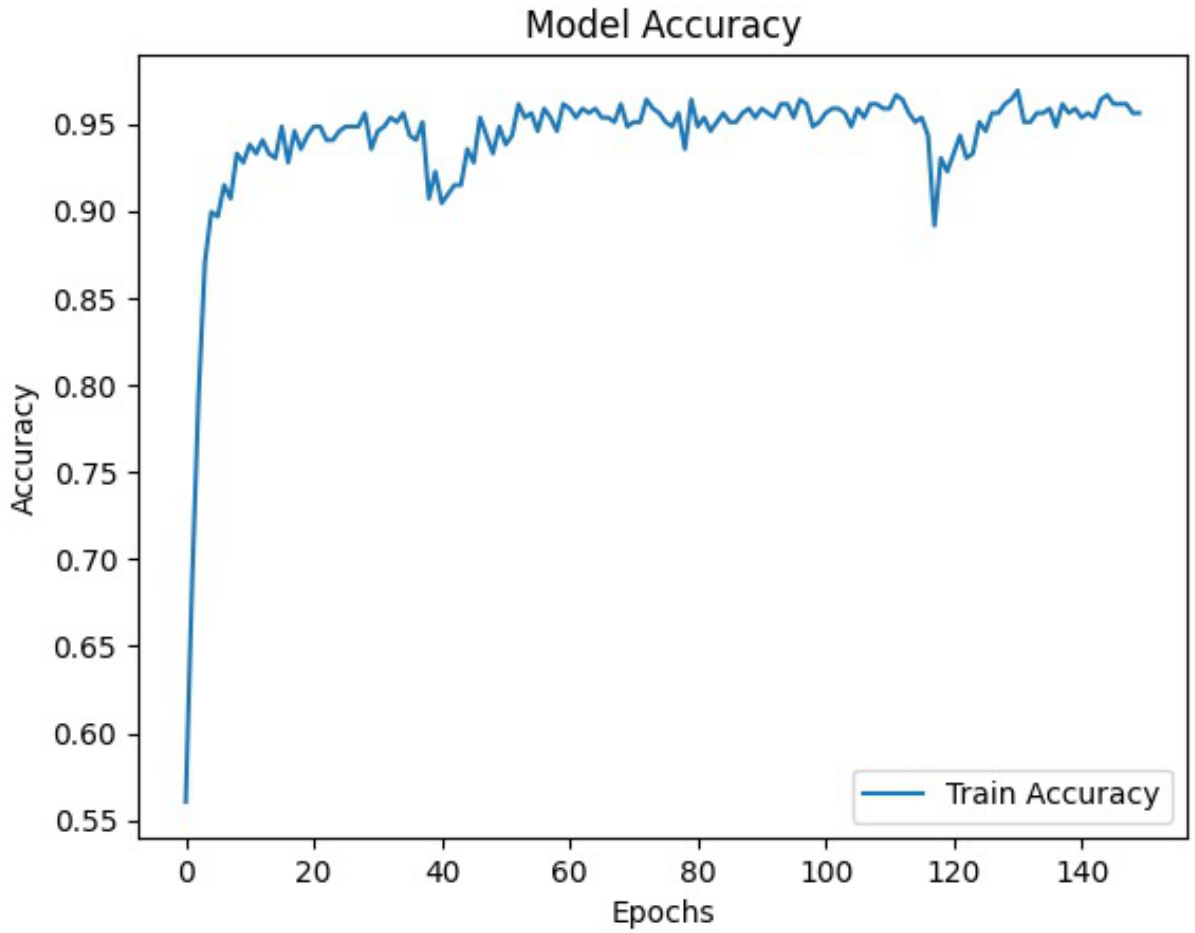


Figure 8.1: Accuracy Graph - 1

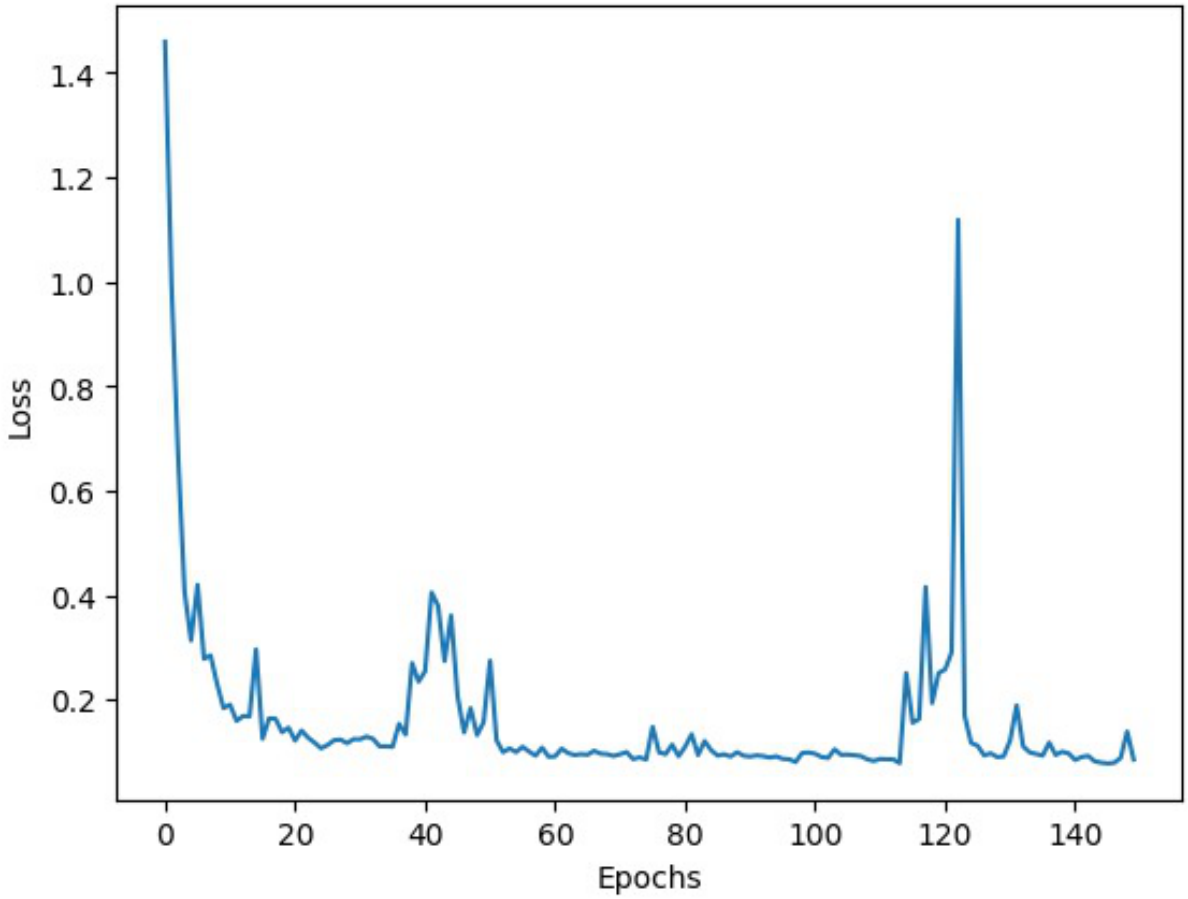


Figure 8.2: Accuracy Graph - 2

Chapter 9

Screenshots of Project

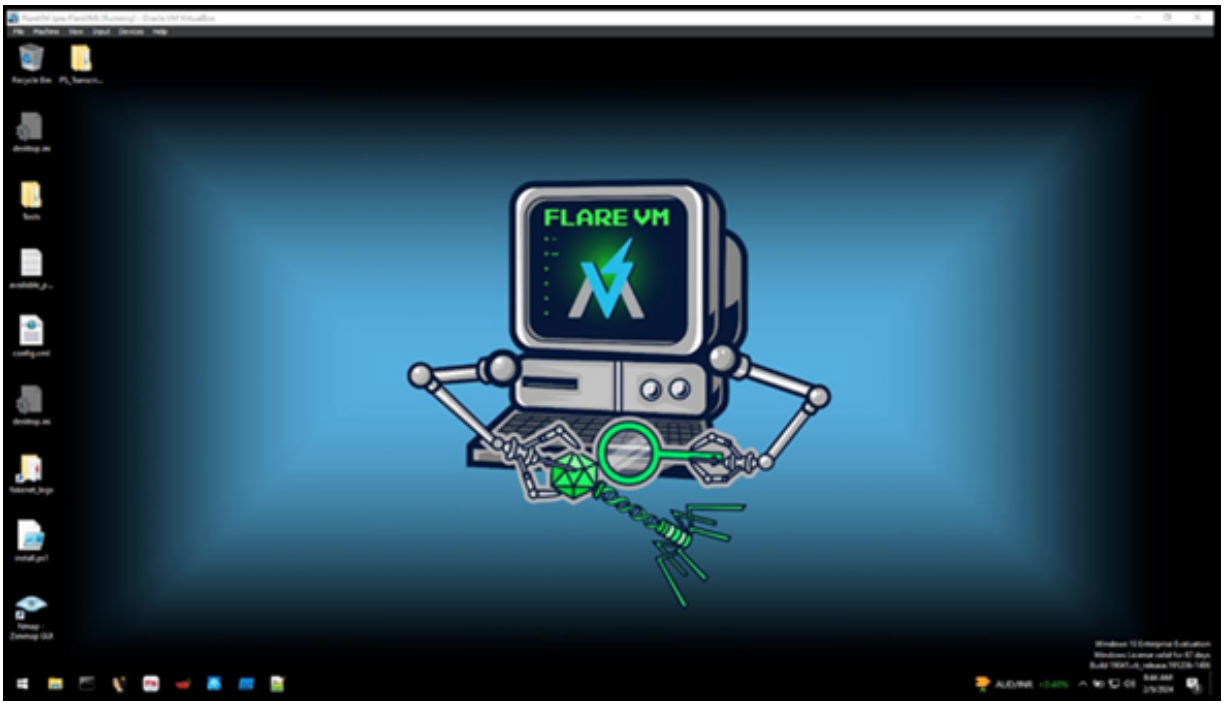


Figure 9.1: FLARE VM

Figure 9.2: REMnux

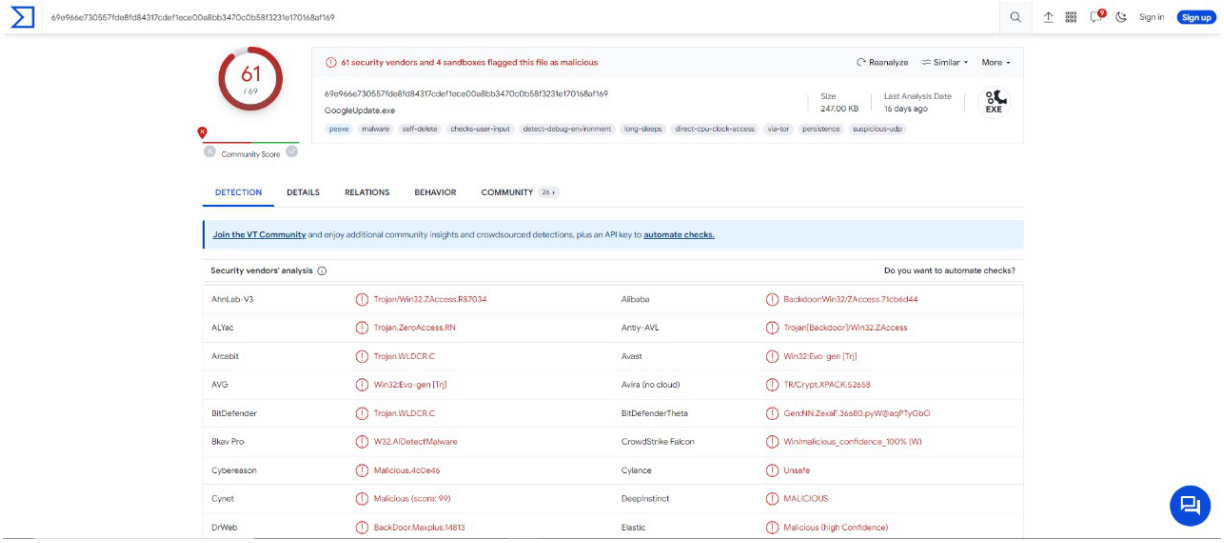


Figure 9.3: VirusTotal Report

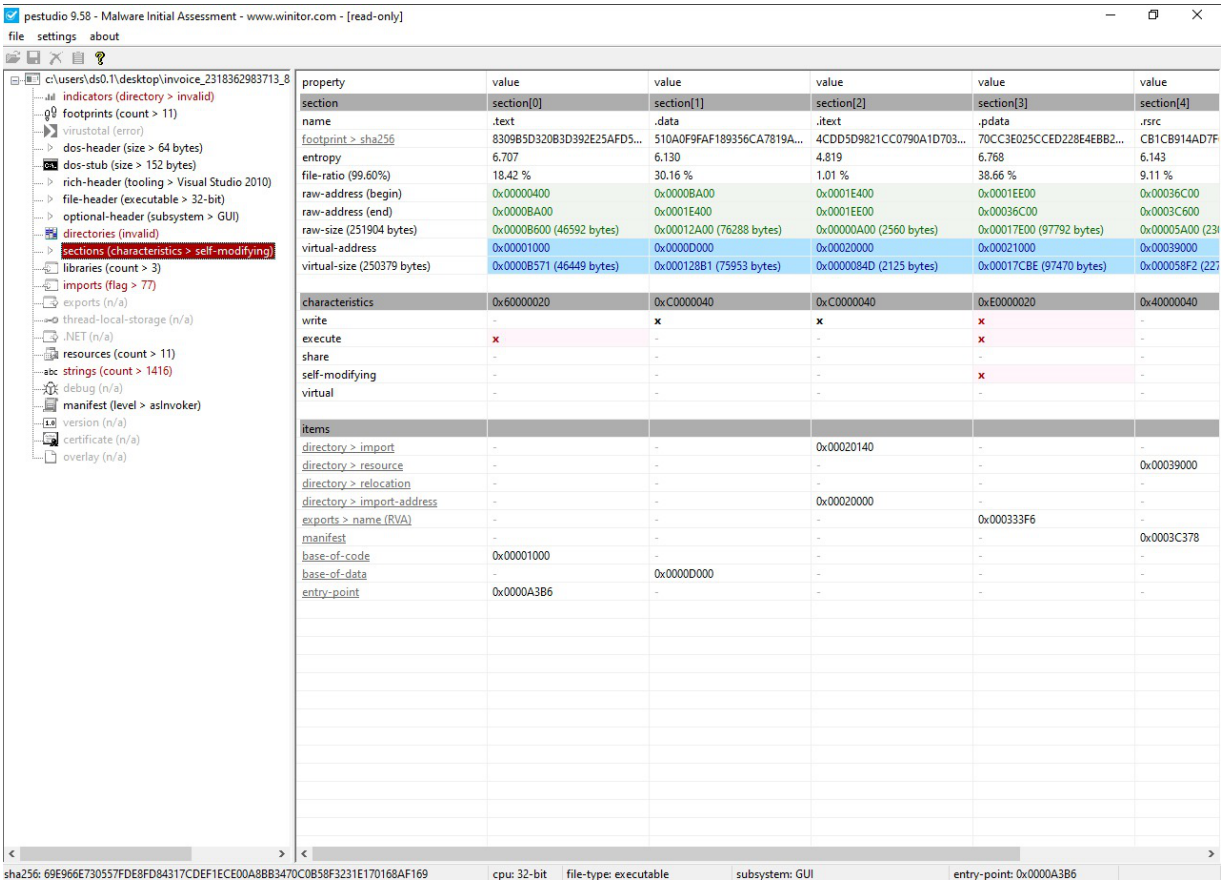


Figure 9.4: Pestudio Analysis(1)

names	
file	c:\users\ds0.1\desktop\invoice_2318362983713_823931342io.pdf.exe
debug	n/a
export	corect.com
version	n/a
manifest	n/a
.NET > module	n/a
certificate > program-name	n/a

Figure 9.5: Pestudio Analysis(2)

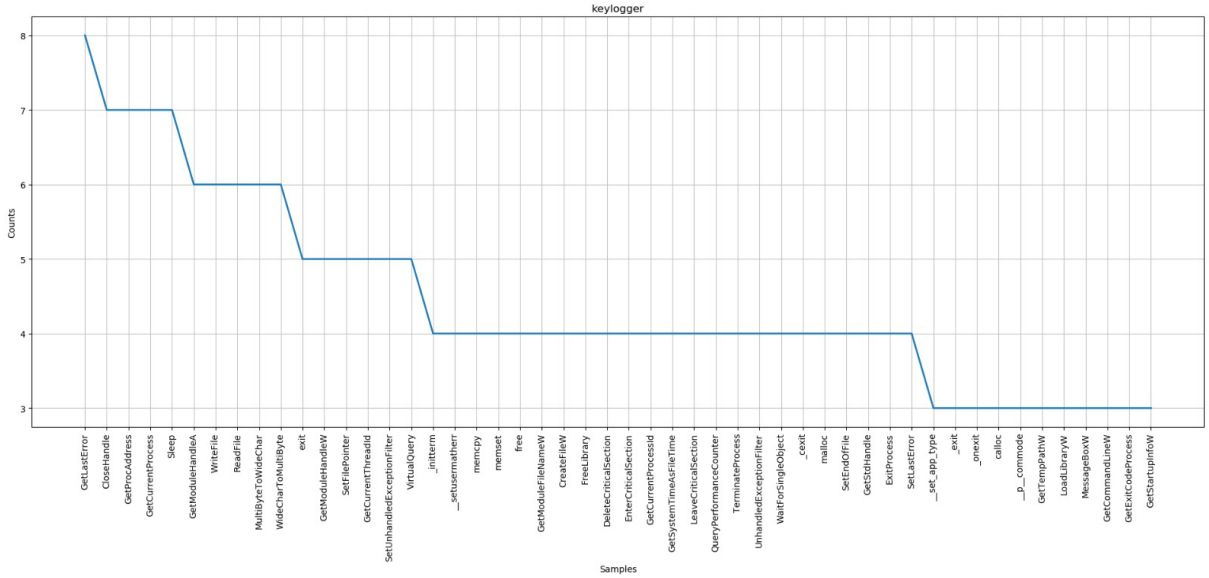


Figure 9.6: Static Analysis of Keylogger

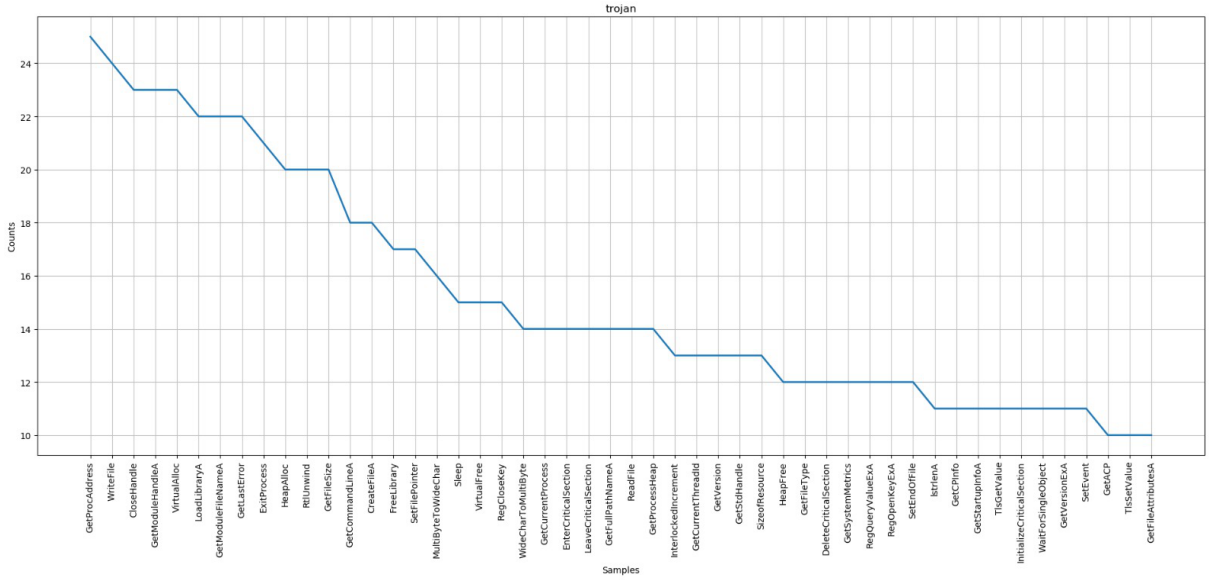


Figure 9.7: Static Analysis of Trojan

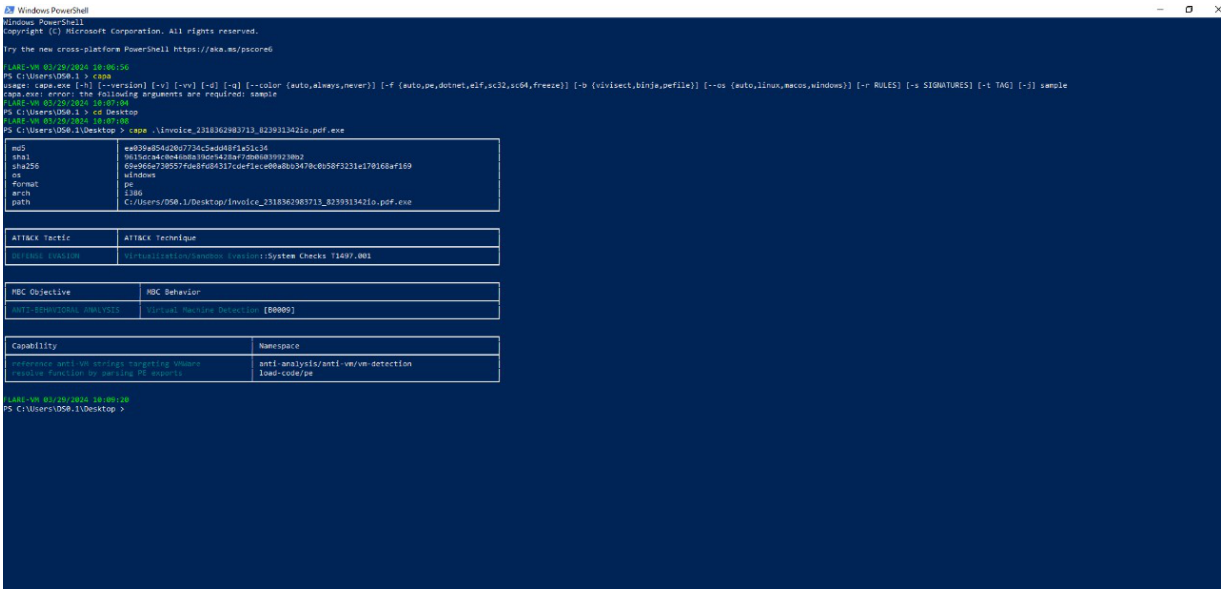


Figure 9.8: Capa Advanced Static Analysis(1)

Figure 9.9: Capa Advanced Static Analysis(2)

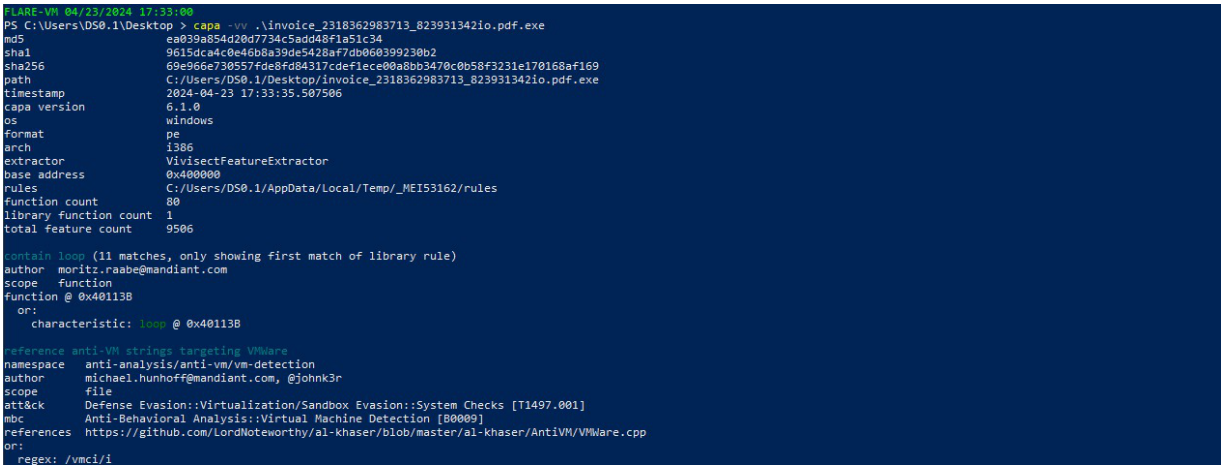


Figure 9.10: Capa Advanced Static Analysis(3)

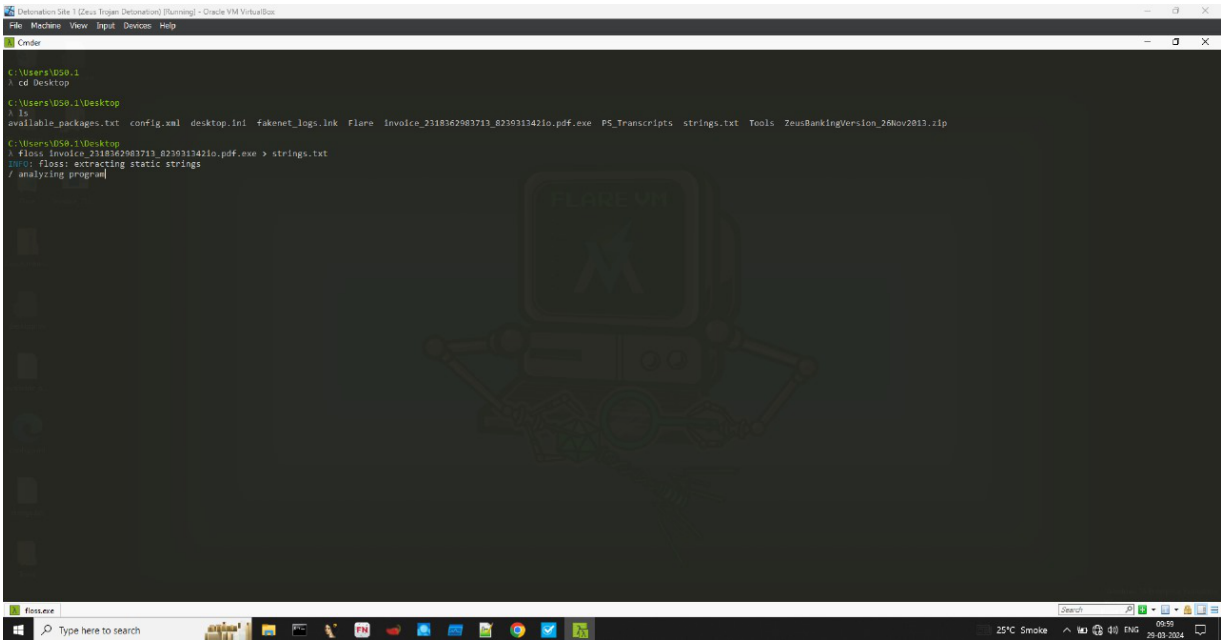


Figure 9.11: Cmdr string Acqisition(1)

Figure 9.12: Cmdr string Acqisition(2)

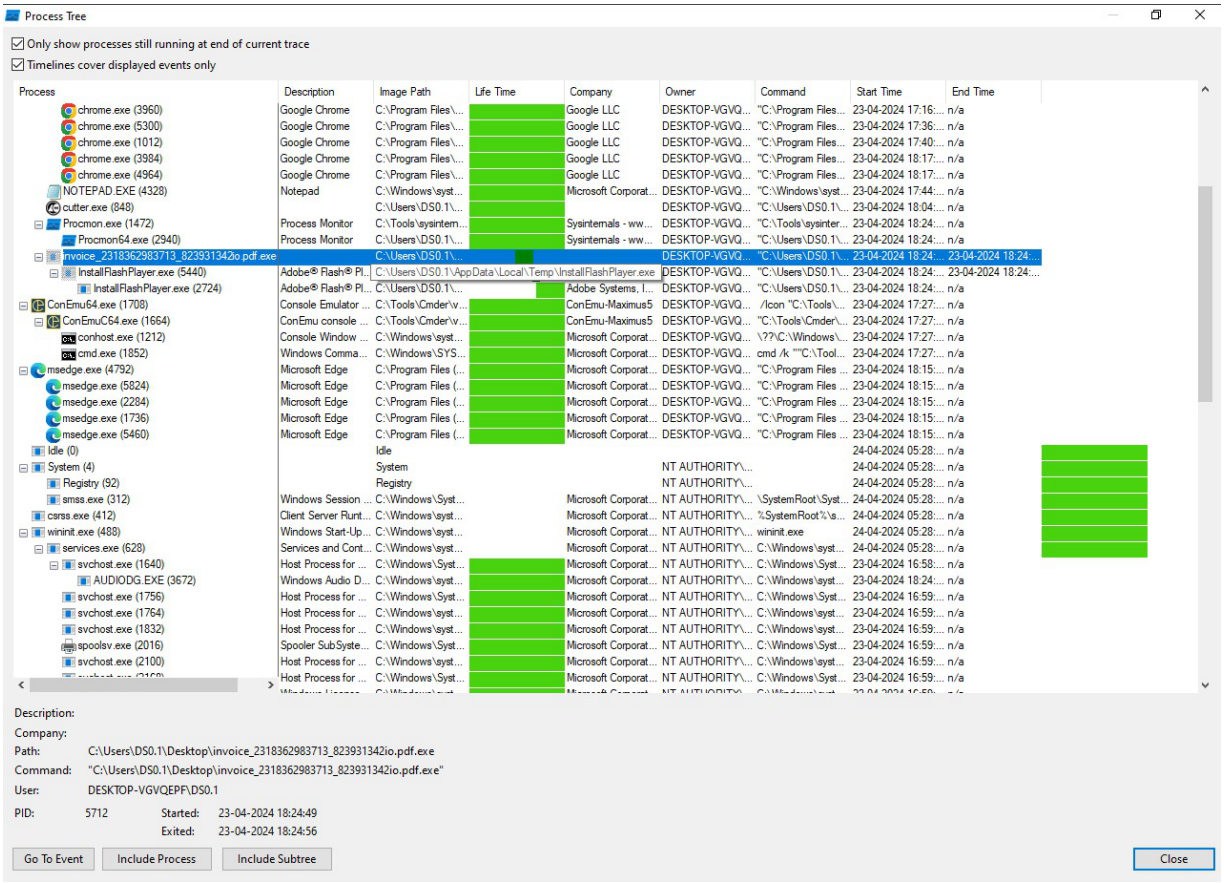


Figure 9.13: Procmon (Process Monitor) SysInternals Behavioural Analysis and Monitoring of Activity Process(1)

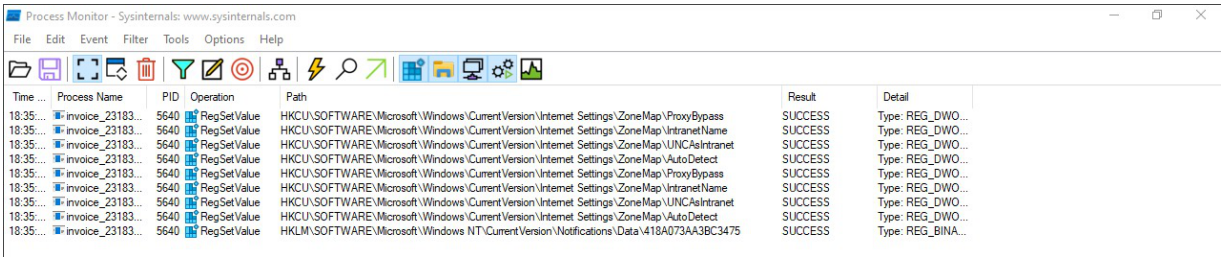


Figure 9.14: Procmon (Process Monitor) SysInternals Behavioural Analysis and Monitoring of Activity Process(2)

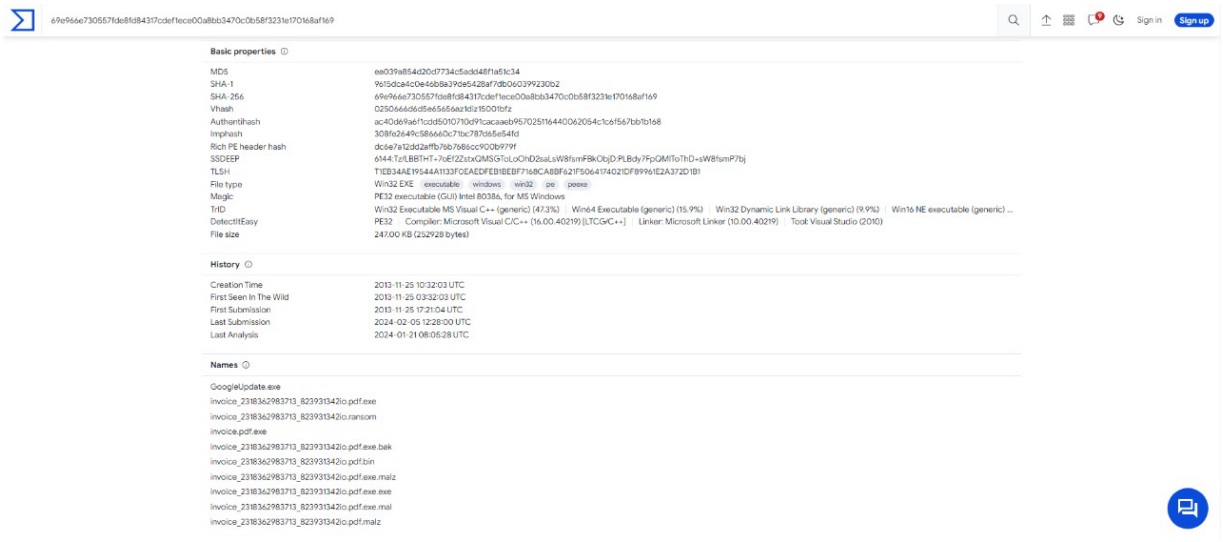


Figure 9.15: VirusTotal for generation of initial hashes across multiple platforms

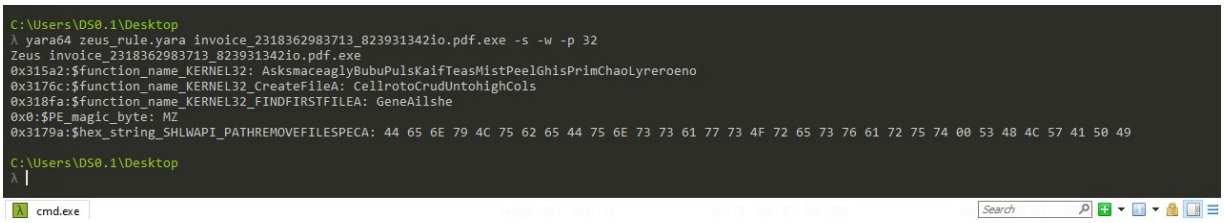


Figure 9.16: Yara64 rule for network checks of similar packets, signatures and scritps

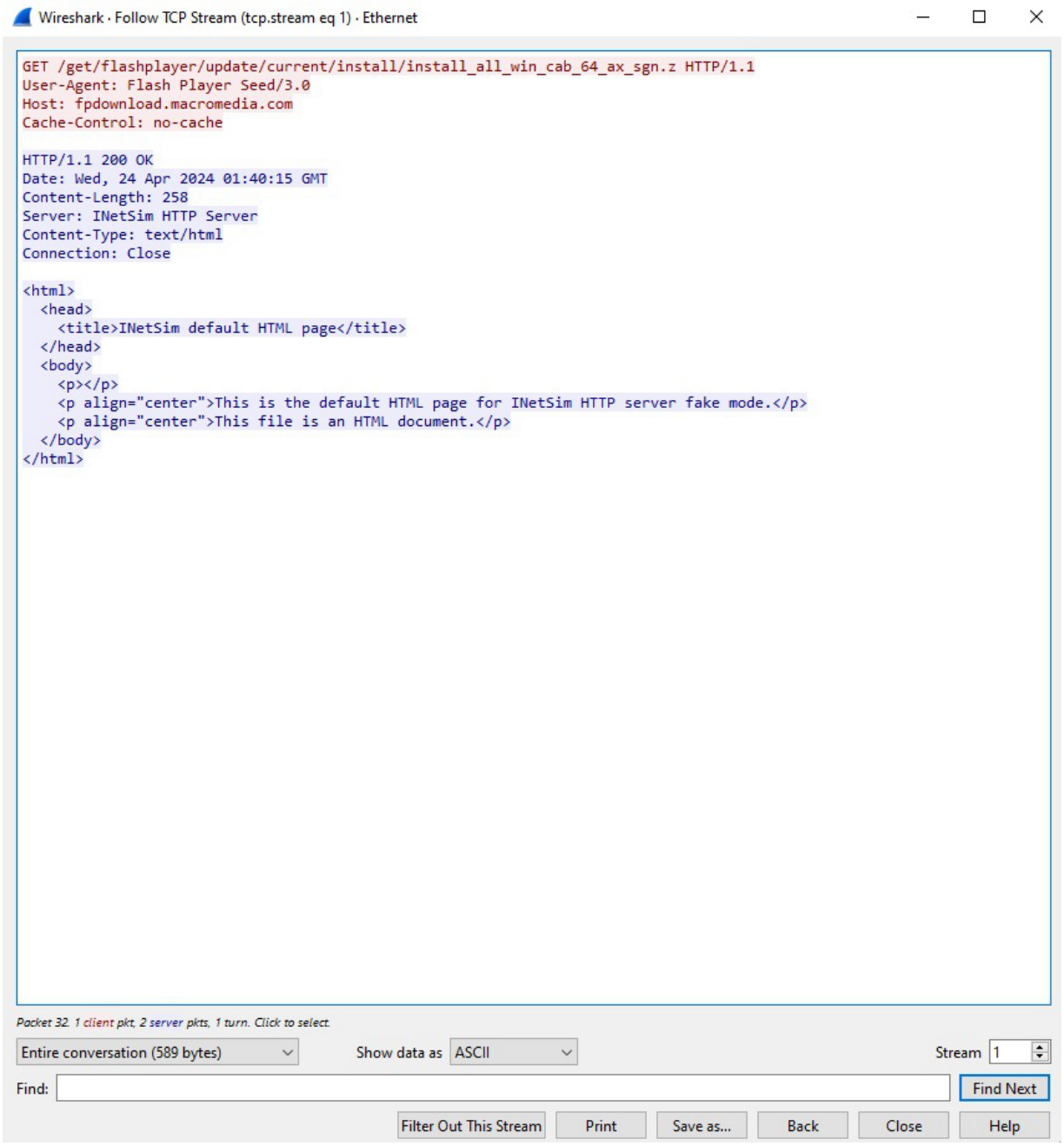


Figure 9.17: Wireshark Visualization of original packets and in-depth analysis

Chapter 10

Conclusion

10.1 Conclusion

In conclusion, the diverse array of research studies in malware analysis reflects a continual pursuit of effective strategies to tackle evolving cybersecurity threats. Each study, whether focused on behavioral profiling, deep learning classification, or unique feature extraction methods, contributes distinct insights to the multifaceted challenge of malware detection and mitigation. These endeavors collectively underscore the dynamic nature of the cybersecurity landscape and the ongoing need for innovative approaches to counteract sophisticated malicious activities.

Our proposed approach, centered on extracting imports without executing malware, offers a promising avenue for efficiency gains in the analysis process. By enabling bulk labeling and sidestepping the time-intensive task of individually executing malware samples, this approach has the potential to enhance scalability and resource optimization in the context of large-scale malware datasets. As the cybersecurity field continues to evolve, the integration of such diverse methodologies contributes to a more robust and adaptive defense against the ever-changing landscape of cyber threats.

References

[1] Muhammad Azeem, Danish Khan, Saman Iftikhar, Shaikhan Bawazeer, Mohammed Alzahrani (2024) *Analyzing and comparing the effectiveness of malware detection: A study of machine learning approaches* Heliyon 10 e23574

[2] Aparna Verma, M.S.Rao, A.K.Gupta, W. Jeberson, Vrijendra Singh (2013) *A Literature Review on Malware and its Analysis*; JCRR Vol 05 issue 16

[3] Gaurav Pramod Kachare, Gaurav Choudhary, Shishir Kumar Shandilya and Vikas Sihag (2022) *Sandbox Environment for Real-Time Malware Analysis of IoT Devices*; COMS2

[4] Md Jobair Hossain Faruk, Hossain Shahriar, Maria Valero, Farhat Lamia Barsha, Shahriar Sobhan, Md Abdullah Khan, Michael Whitman, Alfredo Cuzzocreak, Dan Lo, Akond Rahman and Fan Wu; *Malware Detection and Prevention using Artificial Intelligence Techniques*

[5] Slavisa Z. Ilic, Milan J. Gnjatovic, Brankica M. Popovic, Nemanja D. Macek (2022) *A Pilot Comparative Analysis of the Cuckoo and Drakvuf Sandboxes: An End-User Perspective*; Military Technical Courier

[6] Naveen Kumar C.G and Dr.Sanjay Pande M.B (2017) *A Study on Ransomware and its Effect on India and Rest of the World*; International Journal of Engineering Research and Technology (IJERT), 2278-0181

[7] Joshua Tommy Juwono, Charles Lim, Alva Erwin(2015) *A Comparative Study of Behavior Analysis Sandboxes in Malware Detection*

[8] Dr. Todd Emma, Dr. Brian Bennett, Dr. Megan Quinn(2016) *An Analysis of Faculty and Staff's Identification of Malware Threats*

[9] Lena Yuryna Connolly, David S. Wall, Michael Lang, Bruce Oddson (2020) *An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability*; Journal of Cybersecurity

[10] Anusmita Ray and Dr. Asoke Nath(2016) *Introduction to Malware and Malware Analysis: A brief overview* International Journal of Advance Research in Computer Science and Management, 2321-7782

[11] Faitouri A. Aboaoja, Anazida Zainal, Fuad A. Ghaleb, Bander Ali Saleh Al-rimy, Taiseer Abdalla Elfadil Eisa and Asma Abbas Hassan Elnour(2022) *Malware Detection Issues, Challenges, and Future Directions: A Survey*; Applied Sciences, 2076- 3417

[12] Monnappa K A *Automating Linux Malware Analysis Using Limon Sandbox*;

[13] Maria Thomas ;International Journal of Engineering Research and Technology (IJERT); *Computer Viruses*; 2278-0181, 2015

[14] Xiyue Deng and Jelena Mirkovic; *Malware Analysis Through High-level Behavio*

[15] Takahiro KASAMA (2014); *A Study on Malware Analysis Leveraging Sandbox Evasive Behaviors*

[16] NOR ZAKIAH GORMENT, ALI SELAMAT, LIM KOK CHENG AND ONDREJ KREJCAR ;IEEE, 2023; *Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges, and Future Directions*

[17] Namratha Suraneni, 2022; *Malware Detection and Analysis*

[18] Zoltan Balazs (2015)THE JOURNAL ON CYBER CRIME and DIGITAL INVESTIGATIONS; *Malware Analysis Sandbox Testing Methodology*

[19] Cesar Augusto Borges de Andrade, Claudio Gomes de Mello, Julio Cesar Duarte; *Malware Automatic Analysis*

[20] Dennis Distler (2007);*Malware Anal- ysis: An Intro- duction*

[21] Ekta Gandotra, Divya Bansal, Sanjeev Sofat;Journal of Information Security (2014); *Malware Anal- ysis and Classification: A Survey*

[22] Aini Khalida Muslim, Dzunnur Zaily Mohd Dzulkifli, Mohammed Hay- der Nadhim, Roy Haizal Abdellah (2019); *A Study of Ransomware Attacks: Evolution and Prevention*; JOURNAL OF SOCIAL TRANS- FORMATION AND REGIONAL DEVELOPMENT

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Rahul .
Assignment title:	No Repository 7
Submission title:	Review_Paper_Malware_Analysis_Using_Sandbox.pdf
File name:	Review_Paper_Malware_Analysis_Using_Sandbox.pdf
File size:	267.89K
Page count:	9
Word count:	3,684
Character count:	22,553
Submission date:	09-May-2024 01:18AM (UTC-0400)
Submission ID:	2374874587

Malware Analysis Using Sandbox

Prof. Reshma Kanse, Pranav Taskar, Aditi Thakur, Nargis Shah, Shubham Jha

Abstract

As the threat landscape of cyberattacks continues to evolve, the need for robust malware analysis tools becomes imperative. This project introduces an innovative Malware Sandbox, designed to enhance cybersecurity through dynamic analysis of malicious software. The sandbox employs cutting-edge technologies to dissect and scrutinize suspicious files in a controlled environment, providing a deeper understanding of their behavior and potential threats.

Keywords: cybersecurity, dynamic analysis, malware, sandbox, security professionals, threat intelligence, threat landscape.

1 Introduction

The ubiquity of the Internet in contemporary society has transformed the landscape of communication and knowledge dissemination, ushering in an era of unparalleled connectivity and technological innovation [1]. However, this digital evolution has also given rise to significant cybersecurity challenges, particularly in the realm of malware detection and categorization [1][2]. Malicious software, or malware, poses a persistent threat to computer systems and network infrastructures, capable of causing extensive damage and compromising sensitive information [3].

The proliferation of Internet of Things (IoT) devices has further exacerbated the cybersecurity landscape, providing a vast attack surface for malicious actors to exploit vulnerabilities and propagate advanced malware strains [3]. In response to this escalating threat, researchers have increasingly turned to innovative approaches such as machine learning (ML) and artificial intelligence (AI) to bolster malware detection and classification capabilities [1, 4]. However, despite advancements in deep learning models and ML techniques, challenges persist in achieving robust and accurate malware analysis [1].

One promising avenue for mitigating the impact of malware is the utilization of sandbox environments for dynamic analysis [5][7]. Sandboxing offers a controlled and isolated environment for analyzing the behavior of suspicious files and software, enabling researchers to uncover malicious intent and potential threats [5][7]. Recent studies have highlighted the effectiveness of sandboxing in detecting and analyzing malware, leveraging machine learning algorithms and behavior analysis to enhance accuracy and efficiency [5][7].

This project aims to contribute to the field of malware analysis by leveraging sandboxing techniques to investigate malware behavior and classification. Drawing inspiration from recent research on malware detection methodologies and sandbox comparison studies [1][5][7], this project seeks to explore the efficacy of sandbox environments in identifying and mitigating malware threats. By leveraging insights from existing literature and leveraging modern ML approaches such as Random Forest and Support Vector Machine, this project endeavors to enhance our understanding of malware behavior and inform proactive cybersecurity strategies.

1

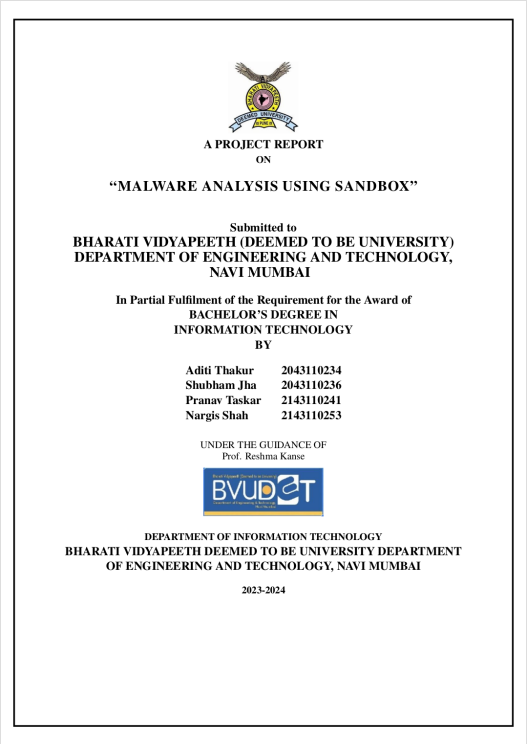
Copyright 2024 Turnitin. All rights reserved.

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Rahul .
Assignment title:	No Repository 8
Submission title:	report_Malware_Analysis_using_Sandbox.pdf
File name:	report_Malware_Analysis_using_Sandbox.pdf
File size:	5.15M
Page count:	45
Word count:	7,166
Character count:	45,419
Submission date:	09-May-2024 01:19AM (UTC-0400)
Submission ID:	2374875111



A PROJECT REPORT
ON

"MALWARE ANALYSIS USING SANDBOX"

Submitted to
BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)
DEPARTMENT OF ENGINEERING AND TECHNOLOGY,
NAVI MUMBAI

In Partial Fulfilment of the Requirement for the Award of
BACHELOR'S DEGREE IN
INFORMATION TECHNOLOGY
BY

Aditi Thakur 2043110234
Shubham Jha 2043110236
Pranav Taskar 2143110241
Nargis Shah 2143110253

UNDER THE GUIDANCE OF
Prof. Reshma Kanse

DEPARTMENT OF INFORMATION TECHNOLOGY
BHARATI VIDYAPEETH DEEMED TO BE UNIVERSITY DEPARTMENT
OF ENGINEERING AND TECHNOLOGY, NAVI MUMBAI

2023-2024

Copyright 2024 Turnitin. All rights reserved.

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Rahul .
Assignment title:	No Repository 3
Submission title:	Implementation_Paper_Malware_Analysis_Using_Sandbox.pdf
File name:	Implementation_Paper_Malware_Analysis_Using_Sandbox.pdf
File size:	1.75M
Page count:	12
Word count:	3,541
Character count:	21,041
Submission date:	09-May-2024 12:44AM (UTC-0400)
Submission ID:	2373136466

Malware Analysis Using Sandbox

Prof. Reshma Kanse, Pranav Taskar, Aditi Thakur, Nargis Shah, Shubham Jha

Abstract

As the threat landscape of cyberattacks continues to evolve, the need for robust malware analysis tools becomes imperative. This project introduces an innovative Malware Sandbox, designed to enhance cybersecurity through dynamic analysis of malicious software. The sandbox employs cutting-edge technologies to dissect and scrutinize suspicious files in a controlled environment, providing a deeper understanding of their behavior and potential threats.

Keywords: cybersecurity, dynamic analysis, malware, sandbox, security professionals, threat intelligence, threat landscape.

1 Introduction

The ubiquity of the Internet in contemporary society has transformed the landscape of communication and knowledge dissemination, ushering in an era of unparalleled connectivity and technological innovation [1]. However, this digital evolution has also given rise to significant cybersecurity challenges, particularly in the realm of malware detection and categorization [1][2]. Malicious software, or malware, poses a persistent threat to computer systems and network infrastructures, capable of causing extensive damage and compromising sensitive information [3].

The proliferation of Internet of Things (IoT) devices has further exacerbated the cybersecurity landscape, providing a vast attack surface for malicious actors to exploit vulnerabilities and propagate advanced malware strains [3]. In response to this escalating threat, researchers have increasingly turned to innovative approaches such as machine learning (ML) and artificial intelligence (AI) to bolster malware detection and classification capabilities [1, 4]. However, despite advancements in deep learning models and ML techniques, challenges persist in achieving robust and accurate malware analysis [1].

One promising avenue for mitigating the impact of malware is the utilization of sandbox environments for dynamic analysis [5][7]. Sandboxing offers a controlled and isolated environment for analyzing the behavior of suspicious files and software, enabling researchers to uncover malicious intent and potential threats [5][7]. Recent studies have highlighted the effectiveness of sandboxing in detecting and analyzing malware, leveraging machine learning algorithms and behavior analysis to enhance accuracy and efficiency [5][7].

This project aims to contribute to the field of malware analysis by leveraging sandboxing techniques to investigate malware behavior and classification. Drawing inspiration from recent research on malware detection methodologies and sandbox comparison studies [1][5][7], this project seeks to explore the efficacy of sandbox environments in identifying and mitigating malware threats. By leveraging insights from existing literature and leveraging modern ML approaches such as Random Forest and Support Vector Machine, this project endeavors to enhance our understanding of malware behavior and inform proactive cybersecurity strategies.

1

Copyright 2024 Turnitin. All rights reserved.

From: Microsoft CMT <email@msr-cmt.org>
Sent: Tuesday, April 30, 2024 8:25:41 PM
To: Aditi Kumari Thakur <akthakurdet20-it@bvucoep.edu.in>
Subject: International Conference on Intelligent Computing and Communication Techniques : Submission (383) has been created.

Hello,

The following submission has been created.

Track Name: Cyber Security

Paper ID: 383

Paper Title: Malware Analysis using Sandbox

Abstract:
As the threat landscape of cyberattacks continues to evolve, the need for robust malware analysis tools becomes imperative. This project introduces an innovative Malware Sandbox, designed to enhance cybersecurity through dynamic analysis of malicious software. The sandbox employs cutting-edge technologies to dissect and scrutinize suspicious files in a controlled environment, providing a deeper understanding of their behavior and potential threats.

Created on: Tue, 30 Apr 2024 14:55:34 GMT

Last Modified: Tue, 30 Apr 2024 14:55:34 GMT

Authors:
- akthakurdet20-it@bvucoep.edu.in (Primary)

Secondary Subject Areas: Not Entered
Submission Files: Malware_Analysis_Using_Sandbox_Implementation_Paper.pdf (1 Mb, Tue, 30 Apr 2024 14:55:13 GMT)

Submission Questions Response: Not Entered

Thanks,
CMT team.