

**Name: Shrey Ratna**

**Registration number: 11915128**

**Roll number: 14**

**Subject: INT301**

**1.INTRODUCTION**

**1.1 Objective of the project**

In today's world, cyberattacks have become increasingly sophisticated, and malicious actors are using advanced techniques to evade detection and compromise systems. One of the primary challenges in detecting and responding to such attacks is the ability to accurately identify and analyze the malware used in these attacks. Malware analysis involves studying the behavior of malicious software to understand how it works, what it does, and how to defend against it.

The Redline tool is a powerful and versatile tool that can help in malware analysis by providing detailed insights into the behavior of a system during a cyberattack. This project aims to leverage the capabilities of Redline to perform a thorough analysis of malware samples and extract valuable information such as indicators of compromise (IOCs), command and control (C2) infrastructure, and other TTPs used by the malware.

The analysis will involve running malware samples in a controlled environment, monitoring the system activity, and using Redline to extract and analyze relevant data. The results of the analysis will be used to create actionable intelligence reports that can help enhance cybersecurity defenses, improve incident response capabilities, and better protect organizations from cyber threats.

Overall, the objective of this project is to demonstrate the value of using the Redline tool in malware analysis and to provide a comprehensive understanding of the techniques used by malicious actors to evade detection and compromise systems. The insights gained from this analysis can help organizations better prepare for and respond to cyber threats, ultimately improving their overall security posture.

**1.2 Description of the project**

The project for malware analysis using Redline tool is aimed at providing a comprehensive and detailed analysis of malware-infected systems. Redline is a free, standalone host investigation tool developed by FireEye that provides detailed analysis of Windows operating systems. The tool enables the collection of a wide range of system data and generates reports that can be used to identify and investigate potential malware infections.

The project will involve using the Redline tool to perform a thorough investigation of a potentially infected system. The tool will be used to collect system data such as running processes, network connections, and registry settings, which will then be analysed to determine whether the system is infected with malware.

The project will involve the following steps:

1. Installation and configuration of Redline tool on a system to be analysed.
2. Collection of system data using Redline tool
3. Analysis of collected data to identify potential malware infections.
4. Creation of detailed reports that document the findings of the analysis.
5. Presentation of the findings to stakeholders and recommendations for remediation

The project will require expertise in malware analysis and knowledge of Redline tool. The analysis will involve analyzing large amounts of data, and therefore, the analyst must possess the ability to recognize patterns, identify anomalies, and use deductive reasoning to draw conclusions.

The output of the project will be detailed reports that provide an accurate and comprehensive analysis of the infected system, enabling stakeholders to make informed decisions on how to remediate the malware infection. The project is highly relevant to organizations that require a proactive approach to malware detection and prevention, and it can be used to improve security measures, such as intrusion detection systems and firewalls.

**1.3 Scope of the project**

Objective: To analyze malware using the Redline tool.

Tasks:

1. Research and provide an overview of Redline's capabilities for malware analysis.
2. Install and configure Redline on a Windows system.
3. Collect malware samples for analysis.
4. Use Redline to analyze the malware samples and document the results.
5. Identify the malware's behavior, including its communication channels, persistence mechanisms, and other techniques used by the malware.
6. Develop recommendations for the effective use of Redline for malware analysis.

Deliverables:

1. Report outlining Redline's capabilities for malware analysis.
2. Documentation outlining Redline's installation and configuration for malware analysis.
3. Summary document of malware samples analyzed and results of the analysis.
4. Report identifying the malware's behavior.
5. Recommendations for the effective use of Redline.

Constraints:

1. Project limited to analyzing Windows-based malware.
2. Redline will be the sole tool used for malware analysis.
3. No actual malware infections on the system.

Conclusion: This project will contribute to the knowledge of malware analysis techniques and the use of Redline as a tool for malware analysis.

**2. System Description**

**2.1 Target system description**

Target system description.


**2.4 Dataset used in support of the project**

[**https://github.com/mandiant/iocs**](https://github.com/mandiant/iocs)

**3.Analysis Report**

**3.1 System snapshot and report**

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated

**References**

[**www.google.com**](http://www.google.com)

[**www.github.com**](http://www.github.com)

[**www.fireeye.dev**](http://www.fireeye.dev)