

TASK 5

1. Introduction

This report details the classification and behavioral analysis of various malware types. The goal is to understand how malware functions, how it is detected, and how organizations can prevent infection.

2. Malware Classification

Malware Type	Characteristics
Virus	Attaches to legitimate files and requires human action to spread.
Worm	Self-replicating and spreads across networks without human intervention.
Trojan	Disguises itself as useful software to trick users.
Ransomware	Encrypts user files and demands payment for the decryption key.

3. Behavioural Analysis

Using **VirusTotal** as the primary analysis tool , I analyzed known malware hashes to observe the following indicators:

- **Detection Reports:** Multiple AV engines flagged the samples as malicious based on signature-based detection.
- **File Activity:** Observed the creation of temporary files and modification of system files.
- **Registry Modification:** Identified changes to startup keys (Persistence).
- **Network Behavior:** Observed communication with Command and Control (C2) servers via suspicious IP addresses.

4. Malware Lifecycle and Spreading

The lifecycle generally follows these stages:

Delivery: Spreads via phishing, infected downloads, or network vulnerabilities.

Infection/Execution: The payload is triggered on the victim's machine.

Persistence: The malware ensures it stays active after system reboots.

Propagation: (For worms) Seeking new targets on the network.

5. Prevention Methods

To mitigate these threats, the following methods are recommended:

- Maintain updated antivirus and anti-malware software.
- Regularly patch operating systems and applications.
- Perform frequent data backups to defend against ransomware.
- Implement network firewalls and email filtering.

