Cyber Security Internship Report

Cyber Security Internship – Task 5

Malware Types & Behavior Analysis Report

Submitted by: Hetal Antala

Date : 22 / 01 / 2026

1. Introduction

Malware refers to malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Malware poses a serious threat to individuals, organizations, and governments by compromising confidentiality, integrity, and availability of systems and data.

This report focuses on understanding different types of malware, their behavior, lifecycle, and prevention techniques. The analysis is performed using **VirusTotal**, an online malware scanning and analysis platform that aggregates results from multiple antivirus engines.

---

2. Types of Malware

2.1 Virus

A virus attaches itself to legitimate files or programs and spreads when the infected file is executed by the user. Viruses often require user interaction to propagate and can damage files or slow system performance.

2.2 Worm

A worm is a self-replicating malware that spreads automatically across networks without requiring user interaction. Worms exploit network vulnerabilities and can cause widespread damage very quickly.

2.3 Trojan

A trojan disguises itself as legitimate software to trick users into installing it. Once executed, it can create backdoors, steal sensitive data, or give attackers unauthorized access to the system.

2.4 Ransomware

Ransomware encrypts files on the victim's system and demands a ransom payment in exchange for the decryption key. It is one of the most financially damaging types of malware.

3. Malware Sample Analysis Using VirusTotal

A known malware hash was analyzed using VirusTotal to understand detection results and observed behavior without executing the malware.

3.1 Malware Name

WannaCry Ransomware

3.2 Detection Summary

- Detected by multiple antivirus engines
- Classified as ransomware
- High threat score indicating severe risk

3.3 Behavior Observed

- Encrypts user files
- Modifies system registry keys
- Establishes persistence to survive reboots
- Communicates with external command-and-control servers

4. Malware Lifecycle

The typical lifecycle of malware includes the following stages:

1. **Initial Delivery** – Through phishing emails, malicious links, or exploited vulnerabilities

2. **Execution** – Malware runs on the victim's system

3. **Persistence** – Ensures it remains active after system restarts

4. **Command and Control (C2)** – Communicates with attacker-controlled servers

5. **Payload Execution** – Performs malicious actions such as data theft or encryption

5. Malware Propagation Methods

Malware commonly spreads using the following methods:

- Email attachments and phishing campaigns
- Exploit kits targeting software vulnerabilities
- Infected or pirated software downloads
- Network vulnerabilities and unsecured systems

6.Prevention Techniques

Effective malware prevention includes:

- Installing and updating antivirus software
- Applying operating system and software updates
- Enabling firewalls
- Maintaining regular data backups
- Educating users about cybersecurity awareness and phishing attacks

7.Conclusion

Malware analysis using VirusTotal provides valuable insights into threat detection and behavior without risking system execution. Understanding malware types, lifecycle, and propagation methods is essential for building strong cybersecurity defenses.

Implementing preventive measures such as regular updates, antivirus tools, and user awareness significantly reduces the risk of malware infections. This task helped develop foundational knowledge in malware analysis and threat identification.