CYBER SECURITY INTERNSHIP – TASK 5

Malware Types & Behavior Analysis (Basic)

---

1. Malware Overview

Malware refers to malicious software designed to harm computer systems, steal sensitive information, or disrupt normal operations. Malware can infect systems through various methods such as email attachments, malicious websites, and infected software downloads. Understanding malware types and their behavior is important for improving cyber security awareness and prevention.

---

2. Types of Malware

Virus

A virus is a type of malware that attaches itself to legitimate files or programs. It spreads when the infected file is executed by the user. Viruses usually require human interaction to propagate.

Worm

A worm is a self-replicating malware that spreads automatically across networks without user interaction. Worms exploit system vulnerabilities and can spread rapidly.

Trojan

A trojan disguises itself as legitimate software to trick users into installing it. Once installed, it performs malicious activities such as data theft or system backdoor creation.

Ransomware

Ransomware encrypts user files and demands payment (ransom) in exchange for the decryption key. It is one of the most dangerous malware types due to data loss risks.

---

3. Malware Analysis Using VirusTotal

VirusTotal is an online malware scanning service that analyzes files and hashes using multiple antivirus engines. In this task, a known malware hash was analyzed using VirusTotal. The report showed that the sample was detected as malicious by multiple antivirus engines, confirming its harmful nature.

This method allows safe malware analysis without downloading or executing malicious files.

---

4. Behavior Indicators Observed

The VirusTotal report indicated the following behavior indicators:

- File modification activity
- Network communication with external servers
- Detection by multiple antivirus engines

These behaviors are commonly associated with malicious software attempting to compromise systems or communicate with command-and-control servers.

---

5. Malware Lifecycle

The typical malware lifecycle consists of the following stages:

1. **Creation** – Malware is developed by attackers
2. **Distribution** – Spread through emails, websites, or downloads
3. **Execution** – Malware is executed on the victim system
4. **Infection** – System resources or data are compromised
5. **Persistence** – Malware maintains long-term access

---

6. Malware Spread Methods

Malware commonly spreads through:

- Email attachments and phishing emails
- Malicious websites and links
- Infected or pirated software downloads
- Removable media such as USB drives

---

7. Malware Prevention Methods

Effective malware prevention includes:

- Using updated antivirus software
- Avoiding unknown email attachments and links
- Keeping operating systems and applications updated
- Avoiding pirated or untrusted software
- Enabling firewalls and security settings

---

8. Conclusion

This task provided a basic understanding of malware types, their behavior, and detection methods using Virus Total. By learning how malware spreads and how to prevent infections, users can improve their overall cyber security awareness and protect systems from threats.