Malware Types & Behavior Analysis Report

By : NROUPSINH GOHIL

1. Introduction

Malware, short for malicious software, refers to any program designed to harm computer systems, steal data, disrupt operations, or gain unauthorized access. Malware is one of the most common cyber threats faced by individuals and organizations today.

---

2. Types of Malware

The common types of malware studied in this task are:

- **Virus:** A malicious program that attaches itself to legitimate files and spreads when the infected file is executed.
- **Worm:** A self-replicating malware that spreads automatically over networks without user interaction.
- **Trojan:** A malicious program disguised as legitimate software to trick users into installing it.
- **Ransomware:** Malware that encrypts user files and demands payment to restore access.

---

3. Malware Analysis Using VirusTotal

A known malware hash was analyzed using VirusTotal. VirusTotal scans files and hashes using multiple antivirus engines to identify malicious content.

Observations:

- The malware hash was detected by multiple security vendors.
- The file was classified as malicious by most antivirus engines.
- The malware was identified as a test malware used to verify antivirus detection.

This confirms that VirusTotal is an effective tool for identifying and analyzing malware threats.

---

4. Malware Behavior Indicators

Malware commonly exhibits the following behaviors:

- Creation of unauthorized files
- Modification of system settings or registry
- High CPU or memory usage
- Communication with suspicious external servers

These indicators help security tools detect malicious activity.

---

5. Malware Lifecycle

The malware lifecycle consists of the following stages:

1. Development of malware by the attacker
2. Distribution through emails, downloads, or removable media
3. Infection when the user executes the malware
4. Execution of malicious code
5. Persistence to remain active on the system
6. Payload execution such as data theft or file encryption
7. Propagation to other systems (optional)

---

6. Malware Spread Methods

Malware spreads using multiple techniques:

- Email attachments and phishing links
- Malicious or compromised websites
- Pirated or cracked software
- Infected USB or external devices
- Network vulnerabilities and exploits
- Fake software update prompts

---

7. Malware Prevention Methods

Malware infections can be prevented by:

- Installing and updating antivirus software
- Avoiding suspicious emails and links
- Downloading software only from trusted sources
- Keeping operating systems and applications updated
- Enabling firewalls
- Using strong passwords and multi-factor authentication
- Disabling auto-run for external devices

---

8. Conclusion

In this task, different malware types such as viruses, worms, trojans, and ransomware were studied. A known malware hash was analyzed using VirusTotal to understand malware detection and behavior. The task provided insights into malware lifecycle, spreading techniques, and prevention methods, building a strong foundation in malware awareness and basic threat analysis.