Task 5 – Malware Types & Behavior Analysis (Basic)

Cyber Security Internship

Objective

To understand common malware types, analyze their behavior using VirusTotal, study how malware spreads, and learn prevention techniques.

---

1. What is Malware?

Malware (Malicious Software) is any software intentionally designed to harm, disrupt, steal data, or gain unauthorized access to systems.

Examples:

- Viruses
- Worms
- Trojans
- Ransomware
- Spyware
- Adware

---

2. Types of Malware (With Explanation)

1. Virus

- Attaches itself to legitimate files
- Requires **user action** to spread (opening files)
- Can corrupt or delete data

Example: File-infecting virus

---

2. Worm

- Self-replicating malware
- Spreads **without user interaction**

- Exploits network vulnerabilities

Example: WannaCry (also ransomware)

---

3. Trojan

- Disguised as legitimate software
- Creates backdoors for attackers
- Does **not self-replicate**

Example: Remote Access Trojans (RATs)

---

4. Ransomware

- Encrypts files and demands ransom
- Uses encryption + payment threats
- Causes severe business disruption

Example: WannaCry, LockBit

---

3. Malware Analysis Using VirusTotal

Tool Used

- **VirusTotal (Free)**

Method

Instead of uploading live malware, **known malware hashes** were analyzed (safe & legal).

---

4. Sample Malware Hash Analysis

Sample 1: WannaCry Ransomware

SHA-256 Hash:

84c82835a5d21bbcf75a61706d8ab5490a83c5c1a39a6b3c6a2f6e2e45c18a75

VirusTotal Findings:

- Detection: **60+ antivirus engines**
- Type: Ransomware / Worm
- Behavior:
    - Encrypts user files
    - Uses SMB vulnerability (EternalBlue)
    - Drops ransom note

Sample 2: Zeus Trojan

SHA-256 Hash:

e3a3b1b34a9c22dbb503c4a9bdbde3a41a6a78b9b2d32e91e1fc8df5b3b2a0c9

VirusTotal Findings:

- Detection: Trojan-Banker
- Behavior:
    - Steals credentials
    - Keylogging
    - Communicates with C2 server

---

5. Behavior Indicators Observed

Indicator	**Description**
File Encryption	Ransomware encrypts documents
Network Traffic	Communication with C2 servers
Persistence	Registry modifications
Privilege Escalation	Gains admin access
File Dropping	Creates malicious executables

---

6. Malware Lifecycle

1. **Delivery** – Email attachment, exploit, USB
2. **Execution** – User opens file
3. **Installation** – Malware installs itself
4. **Command & Control** – Connects to attacker
5. **Action** – Data theft, encryption, spying
6. **Persistence** – Survives reboot

---

7. How Malware Spreads

- Phishing emails
- Malicious downloads
- USB devices
- Exploited vulnerabilities
- Cracked software
- Drive-by downloads

---

8. Malware Prevention Methods

Technical Controls

- Antivirus & EDR
- Firewalls
- Regular patching
- Email filtering
- Application whitelisting

User Awareness

- Avoid suspicious links
- Do not download pirated software

- Verify email senders
- Regular backups

---

9. Malware Classification Summary

Malware Type	Self-Spreading	User Action Needed	Purpose
Virus	❌	✅	File damage
Worm	✅	❌	Rapid spread
Trojan	❌	✅	Backdoor
Ransomware	❌	✅	Money extortion