Task 5: Malware Types & Behavior Analysis (Basic)

1. Different Types of Malware:

Virus

- Attaches itself to legitimate files or programs
- Spreads when the infected file is executed
- Needs **user action** to spread
  Example: Infected .exe file

Worm

- Self-replicating malware
- Spreads automatically over networks without user interaction
- Exploits vulnerabilities
  Example: Conficker worm

Trojan

- Disguised as a legitimate application
- Does not self-replicate
- Often opens a backdoor for attackers
  Example: Fake cracked software

Ransomware

- Encrypts victim's files
- Demands ransom for decryption key
- Causes financial and data loss
  Example: WannaCry, LockBit

2. Using VirusTotal (Safe Method):

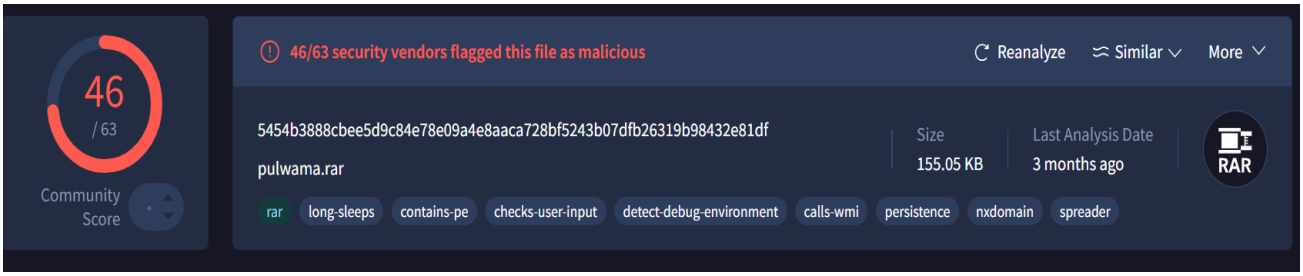
Important:

Do **NOT** upload live malware files.
Instead, upload **known malware hashes** (safe and legal).

Steps:

1. Go to **VirusTotal**
2. Select **Search**
3. Paste a known malware **hash (MD5/SHA256)**
4. View the analysis report

Example hash MD5 (Took from GitHUB): **f211694aaf443b12b2eca9f5e7f25407**



3. Analyzing Detection Reports:

Key things to observe in VirusTotal:

Detection Ratio

- Example: 60 / 72 engines detected
- Higher ratio = more dangerous malware

Malware Labels

- Trojan.Diona

File Information

- File type: EXE
- File size: 155.05 KB

4. Behavior Indicators (Very Important):

Look under **Behavior / Relations** tab:

Common Indicators:

- Creates or modifies system files
- Connects to suspicious IP addresses
- Downloads additional payloads

- Modify registry keys

Example:

- Creates file in AppData
- Communicates with C2 server
- Adds startup registry entry

5. Malware Lifecycle:

1. Delivery

- Email attachment
- Malicious website
- USB drive

2. Execution

- User opens file
- Exploit triggers malware

3. Persistence

- Registry changes
- Scheduled tasks

4. Command & Control (C2)

- Malware contacts attacker server

5. Action on Objectives

- Data theft
- Encryption
- Lateral movement

6. How Malware Spreads:

- Phishing emails
- Fake software updates
- Infected websites

- Exploiting unpatched systems
- Network shares & weak passwords

7. Prevention Methods:

Technical Controls:

- Updated antivirus / EDR
- OS and software patching
- Firewall & IDS/IPS
- Disable macros

User Awareness:

- Do not open unknown attachments
- Avoid cracked/pirated software
- Verify links before clicking

Best Practices:

- Regular backups
- Least privilege access
- Application whitelisting

8. Summary of Findings:

- Malware comes in many forms such as viruses, worms, trojans, and ransomware, each with different behavi0or and impact.
- Using VirusTotal, malware can be safely analysed by searching known hashes and reviewing detection ratios, behaviour indicators, and network activity.
- Understanding the malware lifecycle and spread methods helps in designing effective prevention strategies.
- Strong security controls, regular updates, and user awareness are essential to reduce malware infections.