Task 5: Malware Types & Behavior Analysis (Basic)

Tools Used

Primary Tool: VirusTotal web

Objective

The objective of this task is to analyze malware using VirusTotal, understand different malware types, observe detection reports and behavior indicators, study the malware lifecycle, and identify malware spread and prevention methods.

Malware Definition

Malware is malicious software designed to harm systems, steal data, disrupt operations, or gain unauthorized access to computers and networks.

Types of Malware

Virus

A virus attaches itself to legitimate files and requires user action to execute. It spreads through infected files and removable media.

Worm

A worm is a standalone malware that spreads automatically without user interaction, mainly through network vulnerabilities.

Trojan

A trojan disguises itself as legitimate software to trick users into installing it and often creates backdoors.

Ransomware

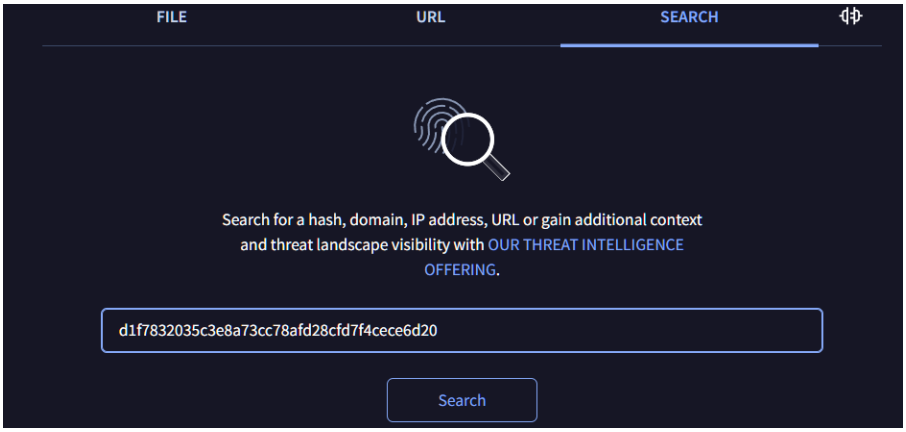
Ransomware encrypts files on a system and demands payment to restore access.

Malware Analysis Using VirusTotal

Malware Sample Used

A known safe test malware hash was analyzed.
vulnerable hash

d1f7832035c3e8a73cc78afd28cfd7f4cece6d20

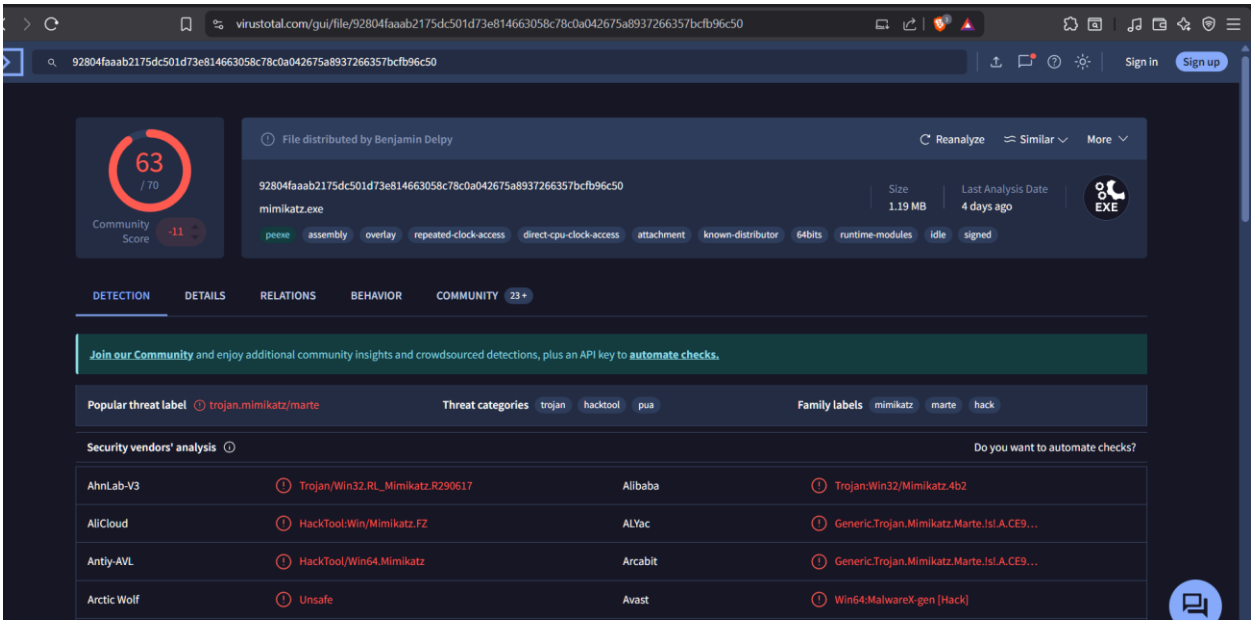


Malware Hash Search on VirusTotal

Detection Report Analysis

The detection report showed that multiple antivirus engines identified the file as malicious. The file was labeled as a known test malware signature used for validating security detection.

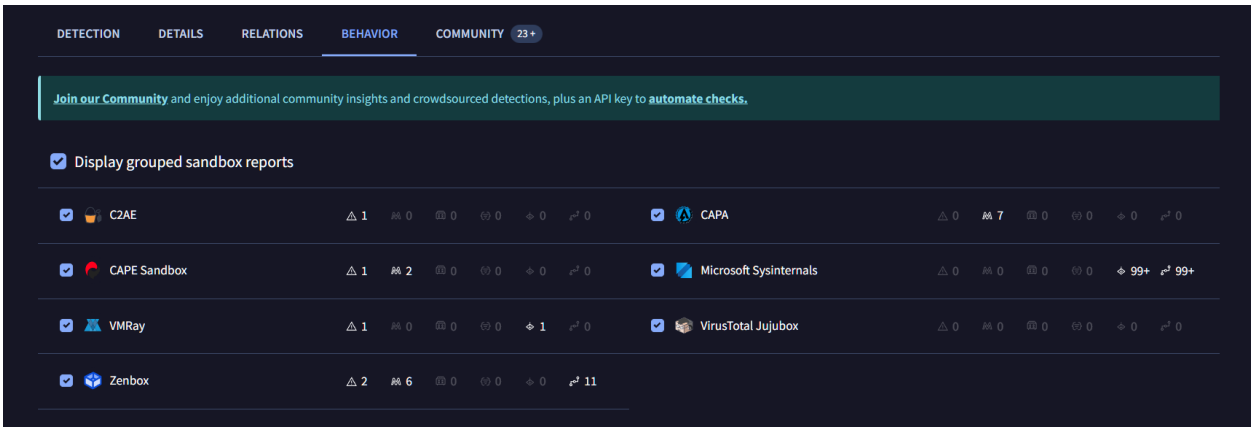
Screenshot 2: Detection Ratio and Antivirus Results



Behavior Indicators Observed

- Malicious signature detection
- Antivirus alert triggering
- Known test malware behavior
- No destructive payload

Screenshot 3: Behavior / Details Tab on VirusTotal



Malware Lifecycle

Delivery occurs through malicious emails, downloads, or websites.
Execution happens when the malware runs on the system.

Persistence is achieved through registry or startup modifications.
Propagation allows the malware to spread to other systems.
Payload execution includes data theft or encryption.
Command and control enables communication with attacker servers.

Malware Spread Methods

- Phishing emails
- Malicious attachments or links
- Infected USB devices
- Unpatched system vulnerabilities
- Pirated or cracked software

Malware Prevention Methods

Technical Controls

- Antivirus and endpoint protection
- Firewalls and intrusion detection systems
- Regular system updates and patching
- Email and web security filtering

User Awareness

- Avoid suspicious links and downloads
- Verify email senders
- Do not install unknown software
- Disable macros in documents

Backup and Recovery

- Maintain regular offline backups
- Test backup restoration periodically

Summary

This task demonstrated practical malware analysis using VirusTotal. Detection reports and behavior indicators were reviewed to understand malware classification, lifecycle, spread methods, and prevention strategies.