ELEVATE LABS
TASK 5
Malware Types & Behavior Analysis

Student Name: Chalumuri Sri Venkata Srinivas

University: Aditya University

Domain: Cybersecurity

Duration: 1st January 2026 to 30th April 2026

1. Learn different malware types

Malware :- Malware, short for malicious software, refers to any program or code intentionally created to disrupt, damage, or gain unauthorized access to computer systems and networks.

Malware is designed to violate the security principles of confidentiality, integrity, and availability of information.

Types of Malware :-

1. VirusA computer virus is a type of malware that attaches itself to a legitimate program or file and spreads when the infected file is executed by the user.

- Viruses cannot function independently and require a host file to activate.
- Once executed, the virus replicates by inserting its malicious code into other files or programs on the same system.
- Viruses often spread through email attachments, removable storage devices like USB drives, pirated software, and malicious downloads.

2. Worm

- ❖ A worm is a standalone malicious program that is capable of self-replication and automatic propagation across computer networks.
- ❖ Unlike viruses, worms do not require a host file or user interaction to spread.
- ❖ They exploit vulnerabilities in operating systems, network services, or applications to infect new systems.
- ❖ Worms are particularly dangerous because they can spread extremely fast, consuming network bandwidth and system resources.

3. Trojan Horse

- ❖ A Trojan horse is malware that disguises itself as legitimate or useful software in order to trick users into installing it.
- ❖ Unlike viruses and worms, Trojans do not replicate themselves.
- ❖ They rely on social engineering techniques such as fake emails, cracked software, or malicious websites.
- ❖ Once installed, a Trojan can perform various malicious activities, including opening backdoors, stealing sensitive information, monitoring user activity, or downloading additional malware.nthena

4. Ransomware

- ❖ Ransomware is a type of malware that restricts access to data or systems by encrypting files or locking the operating system and then demands a ransom payment from the victim to restore access.
- ❖ It typically spreads through phishing emails, malicious attachments, compromised websites, or exploitation of software vulnerabilities.
- ❖ Modern ransomware uses strong cryptographic algorithms, making it extremely difficult to recover data without the decryption key.
- ❖ Ransomware attacks can cause severe financial losses, operational downtime, and reputational damage, especially for organizations such as hospitals, banks, and government agencies. Even after payment, there is no guarantee that attackers will restore the data.

2. Known malware samples to VirusTotal.

- **Malware Samples :-**

  Malware samples are actual copies or instances of malicious software collected for the purpose of study, analysis, detection, and investigation.

- **Virus Total :-**

  VirusTotal is a free online malware analysis service that allows users to upload files, URLs, IP addresses, domains, and file hashes to check whether they are malicious.

  It analyzes the submitted item using multiple antivirus engines and security tools simultaneously and provides a detailed report of the results.

✓ **Steps Involved:-**

Step 1: Obtain the Malware Hash

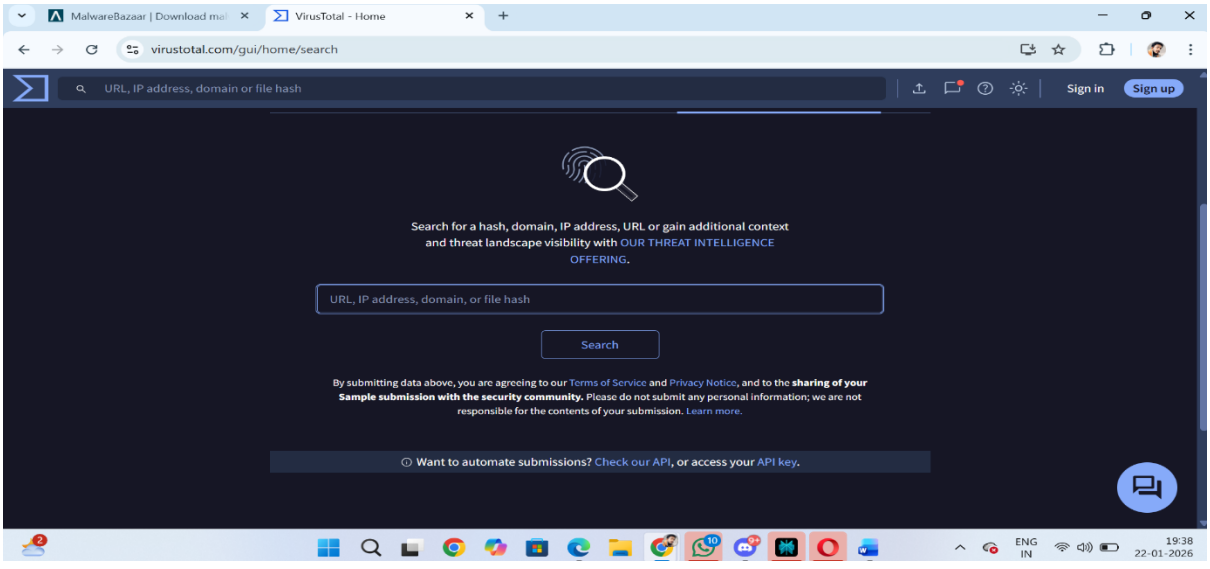
The hash value of a suspicious or known malware file can be obtained using:

Any database sample hash like malware bazar

Step 2: Open VirusTotal

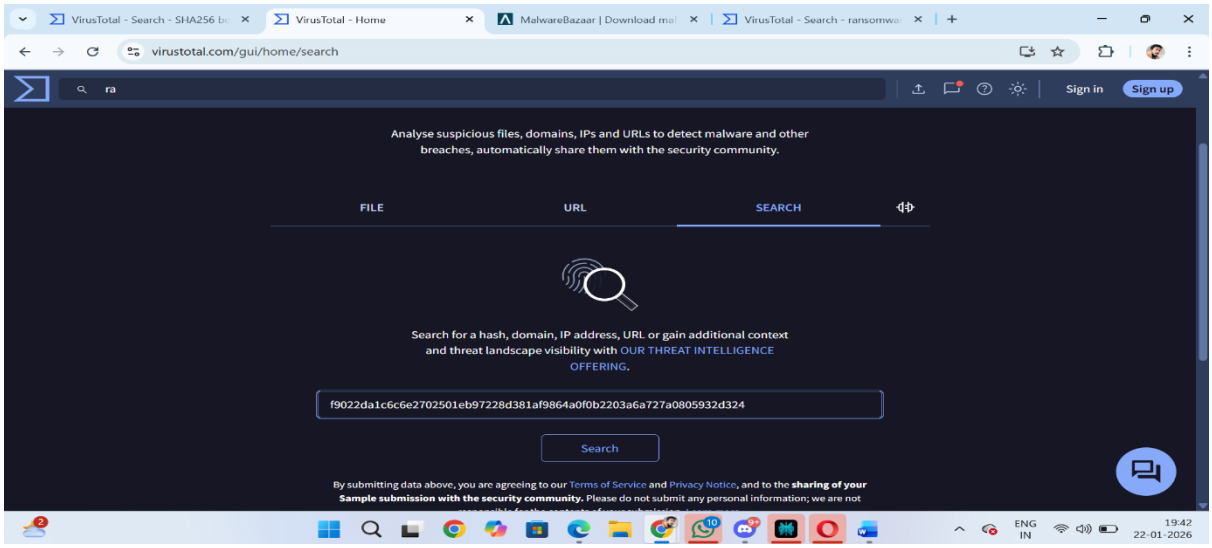
Open a web browser

Go to the VirusTotal website



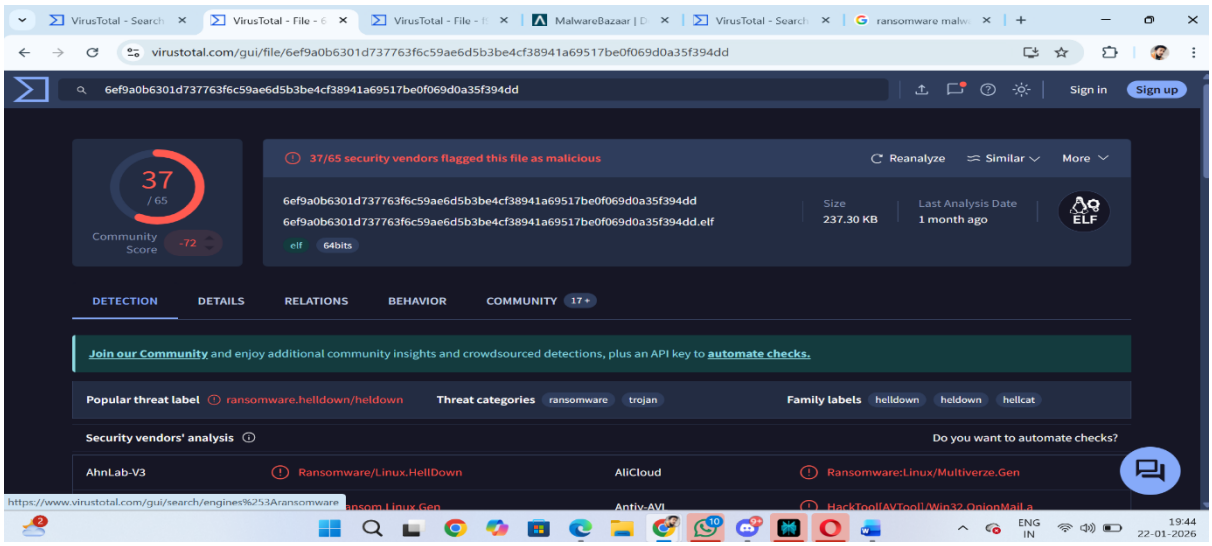
3: Submit the Hash

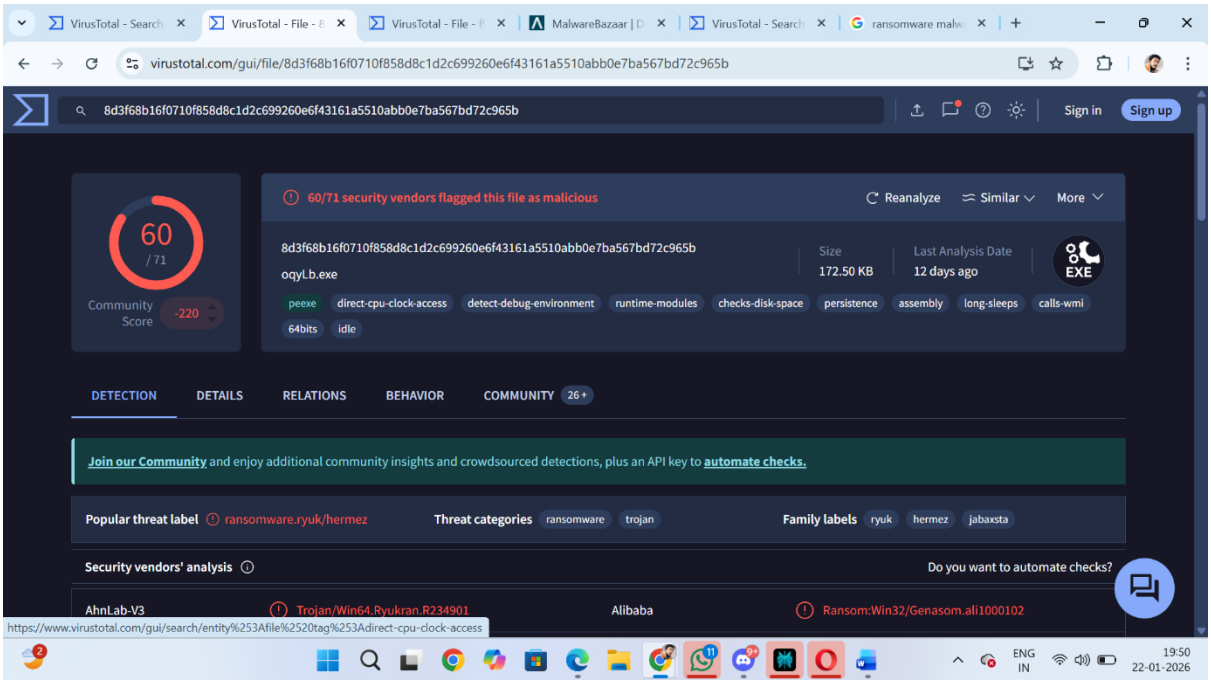
Copy the malware hash value
Paste the hash into the search bar on VirusTotal
Press Enter or click the search icon



Step 4: View the Analysis Report

If the hash exists in VirusTotal's database, a detailed report is displayed containing:
Detection ratio (e.g., 45/70 engines detected malware)
Malware family name





3. Analysis of Detection Reports

- Detection reports are the analytical outputs generated by malware scanning platforms such as VirusTotal after a suspicious file, URL, or hash is submitted for examination.
- These reports provide a consolidated view of how multiple antivirus engines and security tools classify and interpret the submitted artifact.
- he primary purpose of a detection report is to determine whether a file is malicious, suspicious, or benign by correlating results from various independent security vendors.
- A key component of a detection report is the detection ratio, which indicates how many security engines have flagged the file as malicious out of the total number of engines used.
- Detection reports also include malware type classifications, such as virus, worm, Trojan, or ransomware

For the above examples

Basic properties

MD5	c0202cf6aeab8437c638533d14563d35
SHA-1	5767653494d05b3f3f38f1662a63335d09ae6489
SHA-256	8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b
Vhash	015076655d155515555088z54hz3lz
Authentihash	dbec4905fbe2d9be19d9bf6d518dec29345bb2266377b501846ae87f4ca13c18
Imphash	3d84250cdbe08a9921b4fb008881914b
Rich PE header hash	0419af1e713584cc28b658beec622601
SSDEEP	3072:tEyekjv8/eFJ59W2+yV3XgDJ/nptkIV77pJd7RQy+P/:qMo/eF7EDyVgFfn7QyK
TLSH	T1CF048D4772A532F8F173CA3585528452F7B6BC7507609B6F03A4827A1F176929F3AF20
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32+ executable (GUI) x86-64, for MS Windows
TrID	Win64 Executable (generic) (48.7%) | Win16 NE executable (generic) (23.3%) | OS/2 Executable (generic) (9.3%) | Gene
DetectItEasy	PE64 | Compiler: Microsoft Visual C/C++ (19.00.23918) [LTCG/C++] | Linker: Microsoft Linker (14.00.23918) | Tool: Visua
Magika	PEBIN
File size	172.50 KB (176640 bytes)

History

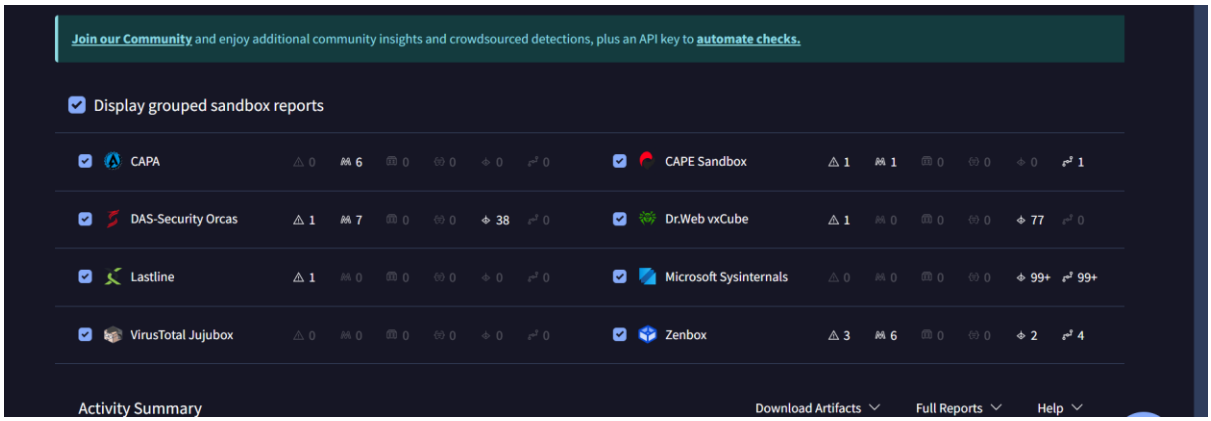
4.Observation of Behavior Indicators

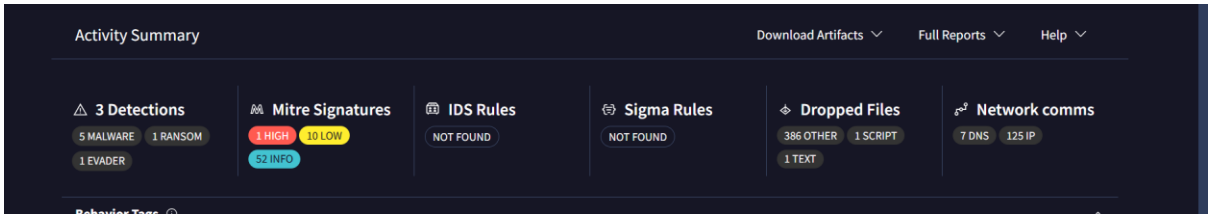
Behavior indicators refer to the observable actions and activities performed by a file or program when it is executed within a system or analyzed in a controlled environment.

In malware analysis, observing behavior indicators is a crucial step used to understand how malware operates beyond signature-based detection.

These indicators reveal the runtime behavior of malicious software and help analysts identify malicious intent even when the malware is new or obfuscated.

Behavior indicators commonly include actions such as file system modifications, registry changes, process creation or injection, and unauthorized network communications.





5. Understand malware lifecycle

- The malware lifecycle describes the complete sequence of stages through which malicious software is created, delivered, executed, and maintained on a victim system.
- Understanding the malware lifecycle helps security analysts and forensic investigators identify attack patterns, detect threats early, and implement effective countermeasures.
- The lifecycle begins with development, where attackers design and code the malware to perform specific malicious functions such as data theft, system control, or ransomware encryption.
- This stage may include obfuscation and packing techniques to evade detection.
- The next stage is delivery, in which the malware is transmitted to the target system using methods such as phishing emails, malicious attachments, compromised websites, removable media, or network exploitation.
- Following delivery is the exploitation and installation stage, where the malware takes advantage of system vulnerabilities or user actions to execute its code and install itself on the system.
- Once installed, the malware enters the execution phase during which it begins performing its intended malicious activities, such as modifying files, stealing credentials, or spreading to other systems.
- The next stage is command and control (C2), where the malware communicates with attacker-controlled servers to receive instructions, send stolen data, or download additional payload

6. Learn how malware spreads.

- Malware spreads through various infection vectors that exploit technical vulnerabilities and human behavior. These methods enable attackers to deliver malicious code to target systems and ensure widespread infection. Understanding malware propagation techniques is essential for cybersecurity defense and digital forensic investigations.

- One of the most common methods of malware spread is phishing emails, where attackers send malicious attachments or links disguised as legitimate messages. When users open the attachment or click the link, the malware is downloaded and executed. Another major propagation method is malicious websites and drive-by downloads, where malware is automatically downloaded when a user visits a compromised or fake website, often exploiting browser or plugin vulnerabilities.

- Malware also spreads through removable media, such as USB drives and external hard disks. Infected media can automatically execute malware when connected to a system or trick users into running malicious files. Network-based spreading is commonly used by worms, which exploit open ports and unpatched vulnerabilities to move laterally across systems without user interaction.

- Another important spread mechanism is software bundling and pirated applications, where malware is hidden inside cracked or free software. Users unknowingly install malware along with the desired program. Malware can also propagate through file-sharing networks and cloud storage, where infected files are shared among multiple users.

- Advanced malware uses exploitation of system vulnerabilities, targeting outdated operating systems, weak passwords,

7. Identify prevention methods

User Awareness & Training

- Educate users to avoid suspicious links, emails, and attachments.
- Teach recognition of phishing and social engineering attacks.
- Encourage safe browsing habits.

Anti-Malware / Antivirus Software

- Install reputable antivirus / anti-malware programs.
- Keep definitions updated.
- Run regular system scans.

Regular Software Updates / Patch Management

- Keep OS, applications, and software **up-to-date**.
- Patch vulnerabilities that malware can exploit.

Firewalls & Network Security

- Use firewalls to block unauthorized access.
- Segment networks to limit malware spread.
- Monitor network traffic for anomalies.

8. Summarize findings.

Malware is malicious software designed to damage, steal, or disrupt systems. Common types include viruses, worms, trojans, and ransomware. Known malware can be analyzed safely using hashes on platforms like VirusTotal, which provide detection reports and behavior indicators. Understanding the malware lifecycle and its methods of spread helps in implementing effective prevention measures, such as antivirus software, firewalls, user awareness, patching, access control, and backups.