Malware Analysis and Detection

Aim: To do Detect and Analyse Malware (Clean Samples)

Theory:

Malware, short for "malicious software," refers to a broad category of software programs or code specifically designed to infiltrate, damage, disrupt, or gain unauthorized access to computer systems, networks, and digital devices. Malware is created with malicious intent, often to steal sensitive information, gain control over systems, extort money, or cause harm to users or organizations. There are various types of malware, each with distinct characteristics and purposes. Some common types of malware include:

1. Viruses: Viruses are malicious programs that attach themselves to legitimate files or programs and spread by infecting other files. When infected files are executed, the virus replicates and spreads further, potentially causing damage to data and systems.

2. Worms: Worms are standalone programs that replicate and spread across computer networks without needing to attach themselves to other files. They often exploit security vulnerabilities to self-propagate and can cause network congestion and data loss.

3. Trojans: Trojans are deceptive programs that disguise themselves as legitimate software, tricking users into installing them. Once installed, Trojans can perform a variety of malicious activities, such as stealing sensitive information, opening backdoors, or launching attacks.

4. Ransomware: Ransomware encrypts a user's files or entire system and demands a ransom payment in exchange for providing the decryption key. It can lead to data loss and significant disruption if not properly managed.

5. Spyware: Spyware is designed to secretly gather information from a user's device, such as browsing habits, passwords, and personal data. This information is then sent to a remote attacker or entity.

6. Adware: Adware is software that displays unwanted advertisements, often in the form of pop-ups or banners, on a user's device. While not as malicious as other types of malware, it can be disruptive and invasive.

7. Keyloggers: Keyloggers record a user's keystrokes, allowing attackers to capture sensitive information like passwords, credit card numbers, and other confidential data.

8. Botnets: Botnets are networks of compromised computers or devices, known as "bots" or "zombies," controlled by a central attacker. Botnets are often used to launch coordinated attacks, distribute spam, or carry out other malicious activities.

9. Rootkits: Rootkits are designed to hide malicious activities from the user and security software. They can modify or replace core system files to gain unauthorized access and control over a system.

10. Backdoors: Backdoors provide unauthorized access to a compromised system. They can be used by attackers to maintain control over a system, often allowing them to return even after the initial breach is resolved.

Malware can enter systems through various vectors, including malicious email attachments, compromised websites, infected software downloads, and even through physical devices like infected USB drives. To protect against malware, it's essential to maintain strong cybersecurity practices, including using reputable antivirus and anti-malware software, keeping software up-to-date, avoiding suspicious links and downloads, and practicing safe browsing habits.
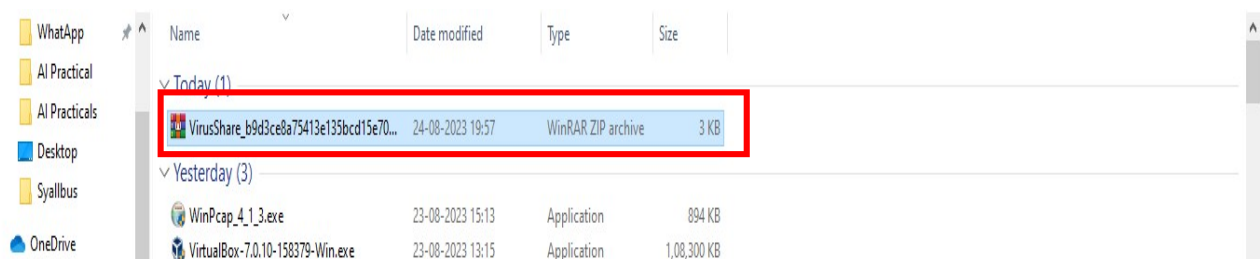
Analysis:

For analysing the Malware, we need one. A clean sample of the Malware needs to be downloaded from a trusted website, the downloading and analysis is demonstrated by the following steps

1) We select the website www.virusshare.com for downloading the clean sample of Malware (an account needs to be created for the same). Any other source can be selected to download the Malware (clean sample and authorised site)
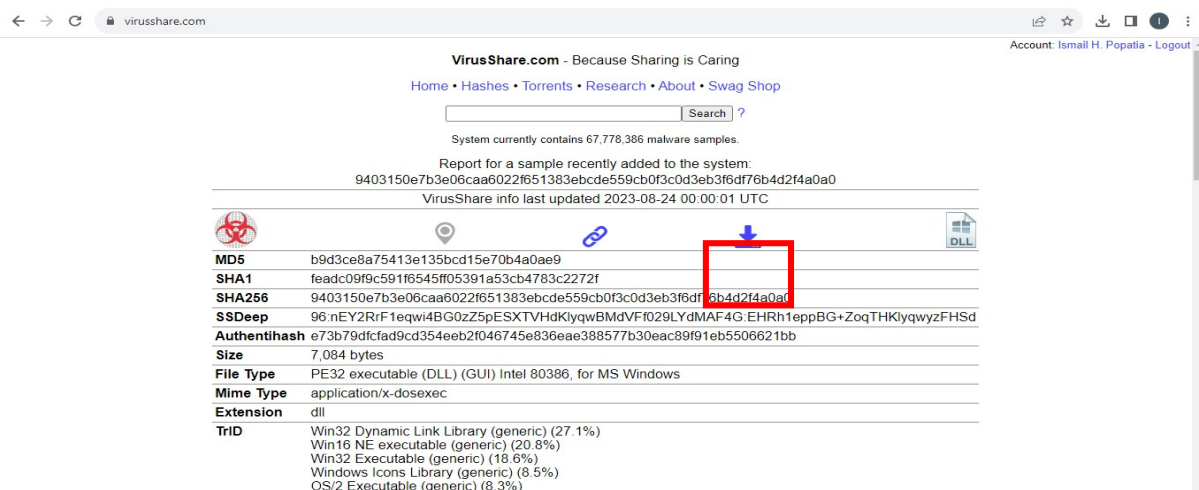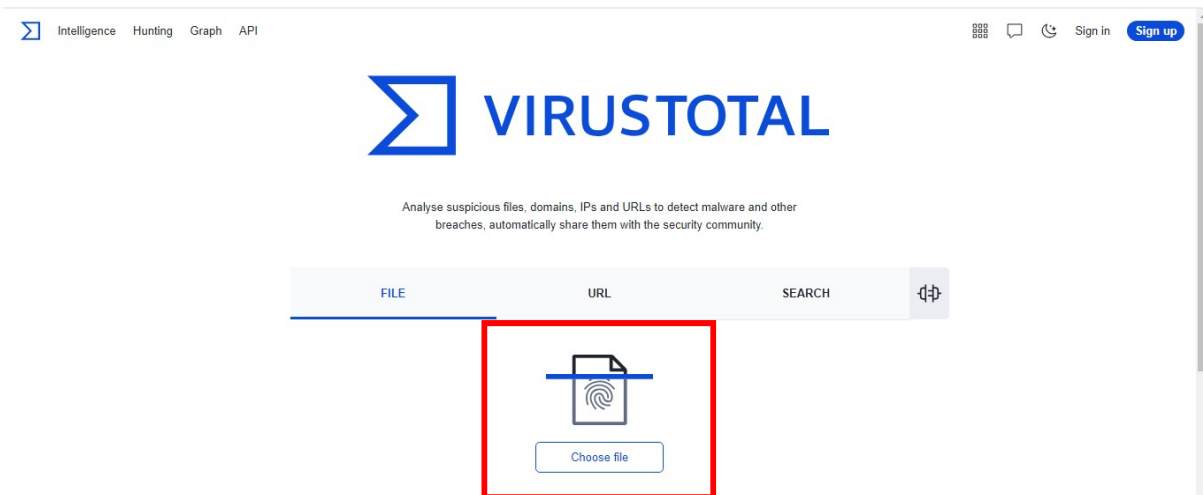

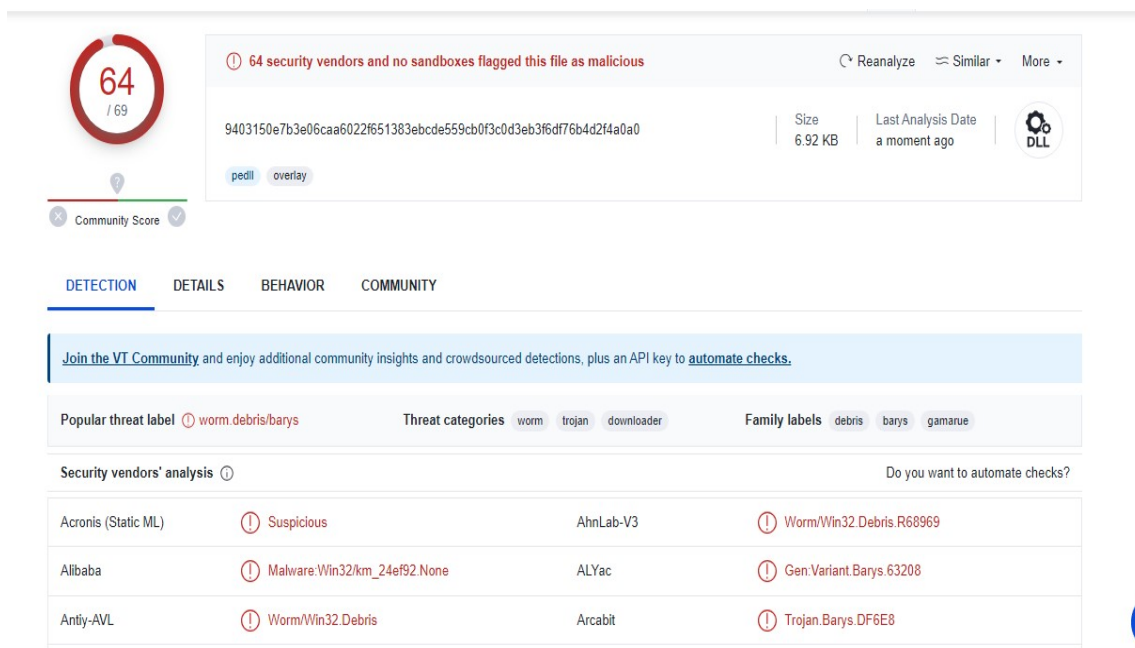2) By clicking the above download icon the Malware gets downloaded in ZIP format.

3) For unzip the password is "infected", there is no need to unzip the file, we create a folder "Malware" on desktop and save the file in the folder

4) In order to analyse the Malware, we select the website www.virustotal.com

5) Click on "Choose File" and select the file from the location (ZIP file will do, if asks for password enter infected)

6) We get the following after the upload is complete

We interpret the following findings

a) 64 security vendors out of 69 flagged this file as malicious
b) The detection tab shows the threats-type which were flagged by the vendors for e.g

c) The details tab gives the following information
   i.   Basic properties
   ii. History
   iii. Compiler products
   iv. Header
   v.   Sections
   vi. Imports
   vii. Exports
   viii. Overlays
d) The Behavior tab gives the following information
   i.   Activity summary
   ii. MITRE ATT&CK Tactics and Techniques
   iii. Behavior Similarity Hashes
   iv. Process and service actions

Countermeasures:

Countermeasures are strategies, actions, or precautions taken to prevent or mitigate various risks, threats, or undesirable events. In the context of cyber-security and dealing with potential malware, viruses, and other online threats, here are some common countermeasures you can take:

1. Use Antivirus and Anti-Malware Software: Install reputable antivirus and anti-malware software on your devices. Keep the software updated to ensure you have the latest protection against known threats.

2. Keep Operating Systems and Software Updated: Regularly update your operating system, web browsers, plugins, and other software. Updates often include security patches that address vulnerabilities.

3. Use Strong and Unique Passwords: Use complex passwords that combine upper and lower case letters, numbers, and symbols. Avoid using common or easily guessable passwords. Consider using a password manager to securely store your passwords.

4. Enable Two-Factor Authentication (2FA): Whenever possible, enable two-factor authentication for your online accounts. This adds an extra layer of security by requiring a second form of verification in addition to your password.

5. Be Cautious with Email and Attachments: Be wary of unsolicited emails, especially those with attachments or links. Don't open attachments or click on links from unknown or suspicious sources. Verify the sender's authenticity before taking any action.

6. Use a Firewall: Enable firewalls on your devices and network. Firewalls help block unauthorized access and protect your system from external threats.

7. Regular Backups: Regularly back up your important data to an external source or a cloud storage service. In case of a malware attack or data loss, you'll have a copy of your important files.

9. Secure Wi-Fi Networks: Secure your home or office Wi-Fi network with a strong password and encryption. Avoid using public Wi-Fi networks for sensitive activities.

10. Use Ad-Blockers and Script Blockers: Install browser extensions that block ads and potentially malicious scripts. This can help prevent drive-by downloads and malvertising.

11. Disable Macros: Disable macros in office documents unless you're certain they are safe. Malicious macros are often used to deliver malware.

12. Download Software from Official Sources: Only download software from reputable and official sources. Be cautious of downloading software from unfamiliar websites.

13. Regularly Scan for Malware: Perform regular scans of your devices using reputable antivirus and anti-malware tools.

14. Use Virtual Private Networks (VPNs): When connecting to the internet, especially on public networks, use a VPN to encrypt your internet connection and enhance your privacy.

15. Implement Security Policies: If you're managing a network or a business, establish and enforce security policies for employees, including guidelines for safe browsing, email practices, and device usage.

For the video demonstration of the practical click on the link below or scan the QR-code

https://youtu.be/H2agWcwaqvM