

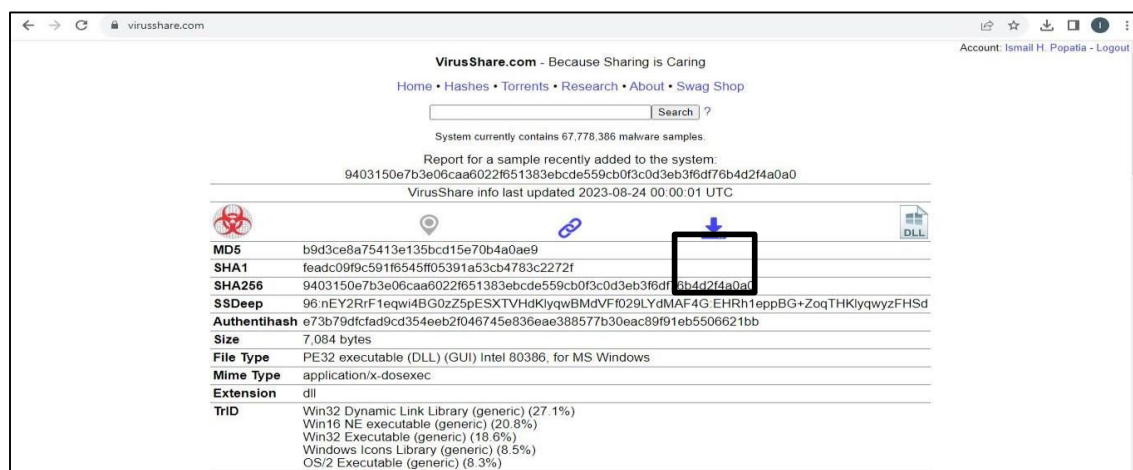
## Practical No.7

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

#### 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

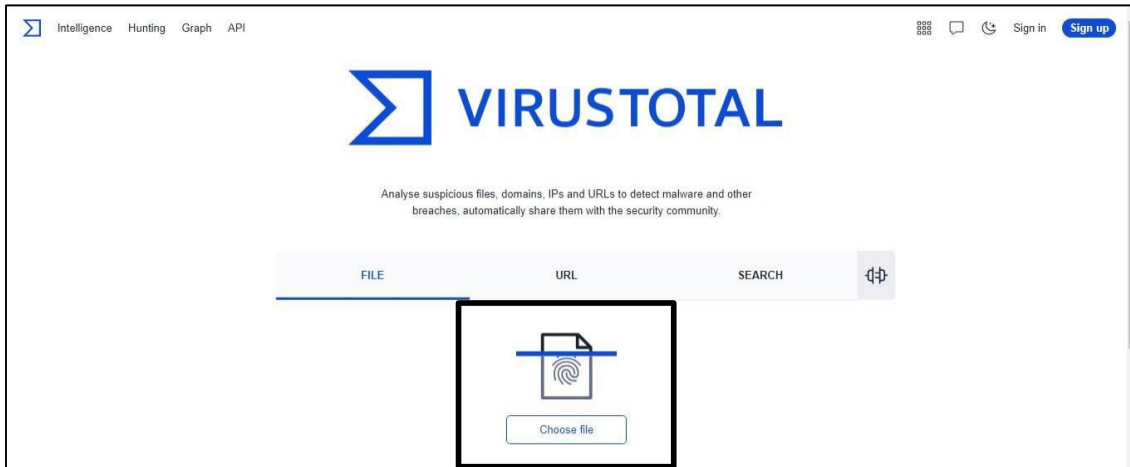
- 1) We select the website [www.virusshare.com](http://www.virusshare.com) for downloading the clean sample of Malware (an account needs to be created for the same). Any other source can be selected to download the Malware (clean sample and authorised site)



- 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](http://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

The screenshot shows the VirusTotal analysis results for a file. The file's SHA-256 hash is `afa04b5abdf338e46c682d6b09fa295c6259c0f1b2e8df35238a7f195b946949`. The file size is 34.40 KB, and it was last analyzed 2 days ago. The file type is identified as EXE. A summary at the top indicates that 2 out of 73 security vendors flagged this file as malicious. The 'DETECTION' tab is active, showing a table of security vendors' analysis results.

Security vendors' analysis		Do you want to automate checks?	
Cynet	Malicious (score: 100)	Trapmine	Suspicious.low.ml.score
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected

We are interpret the following findings

- a) 2 security vendors out of 72 flagged this file as malicious
- b) The detection tab shows the threats-type which were flagged by the vendors for e.g

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to <a href="#">automate checks</a> .				
Security vendors' analysis ⓘ				Do you want to automate checks?
Cynet	❗ Malicious (score: 100)		Trapmine	❗ Suspicious low ml.score
Acronis (Static ML)	✅ Undetected		AhnLab-V3	✅ Undetected
Alibaba	✅ Undetected		AliCloud	✅ Undetected
ALYac	✅ Undetected		Antiy-AVL	✅ Undetected
Arcabit	✅ Undetected		Avast	✅ Undetected
AVG	✅ Undetected		Avira (no cloud)	✅ Undetected
Baidu	✅ Undetected		BitDefender	✅ Undetected
Bkav Pro	✅ Undetected		ClamAV	✅ Undetected
CMC	✅ Undetected		CrowdStrike Falcon	✅ Undetected
CTX	✅ Undetected		Cylance	✅ Undetected
DeepInstinct	✅ Undetected		DrWeb	✅ Undetected

c) The details tab gives the following information

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join our Community

 and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic properties

MD5

0fee95585e001f49aa5fb2e6fe015ccb

SHA-1

20e53cb58f94a987eddded0f04981339d26319c53

SHA-256

afa04b5abdf338e46c682d6b09fa295c6259cf1b2e8df35238a7f195b946949

Vhash

0340466d0505z

Authentihash

01ac20afa3953ec4a91c5bc83798c06e664706d6905ffa61d1d2c854bc2401ba

SSDEEP

768:dlBvbCGbikI4YQGa7FTfzmULWPDWv9dlGQSLl9kTfHwlaGR+OfZMZDs0wM+GzLobiZiOF+UrvTgs+VLBh

TLSH

T1AFF2C62AB01589BEDE106DF82C6DF1DA502F8D2736A0FB717718C5C349E04AEE0A395

File type

Win32 EXE 

executable

windows

win32

pe

peexe

Magic

PE32 executable (GUI) Intel 80386, for MS Windows

TrID

Win32 Executable (generic) (34%) | Win32 Executable Watcom C++ (generic) (20.1%) | OS/2 Executable (generic) (15.3%) | Generic Win/DOS Executable (15.1%) | DOS ...

DetectItEasy

PE32 | Compiler: Borland C++ | Linker: Turbo Linker (5.0) [GUI32]

Magika

PEBIN

File size

34.40 KB (35224 bytes)

History

Creation Time

2008-06-01 11:58:16 UTC

First Submission

2024-09-18 06:21:29 UTC

Last Submission

2024-10-03 07:14:51 UTC

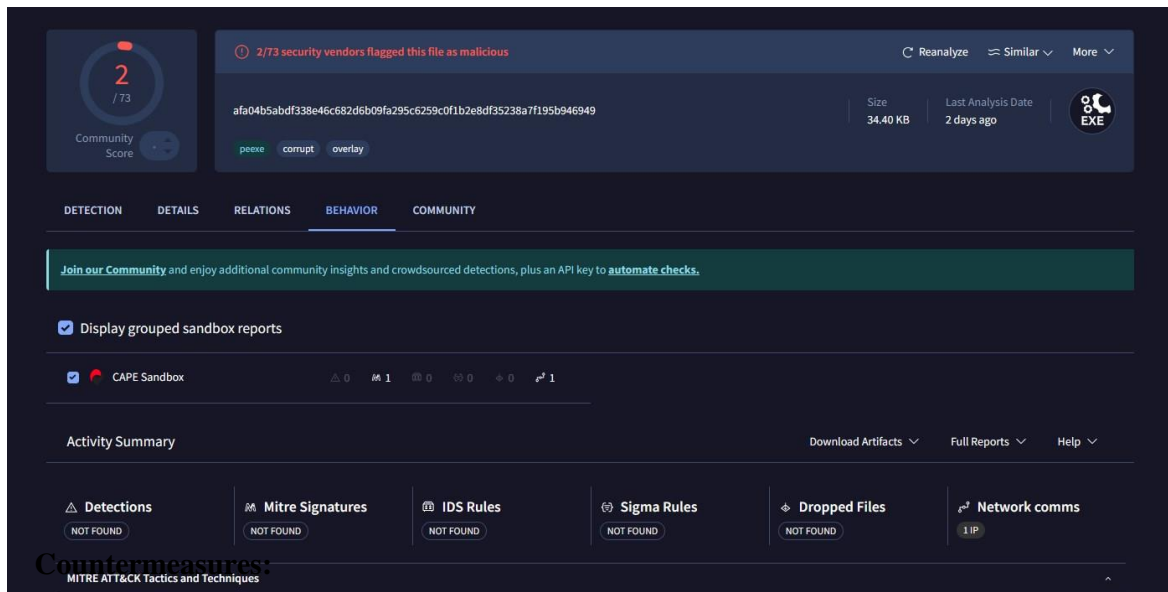
Last Analysis

2024-10-01 06:52:22 UTC

Portable Executable Info

Header

- 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



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.
8. **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.
9. **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.

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

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

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

13. **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.

14. **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.