# Domain 02 Demo 02

# Analyzing Malware Reports Using VirusTotal

**Objective:** To perform a comprehensive malware analysis using VirusTotal, hash, IP information, and graph visualization to understand the malware's behavior and network relationships

**Tools required:** None

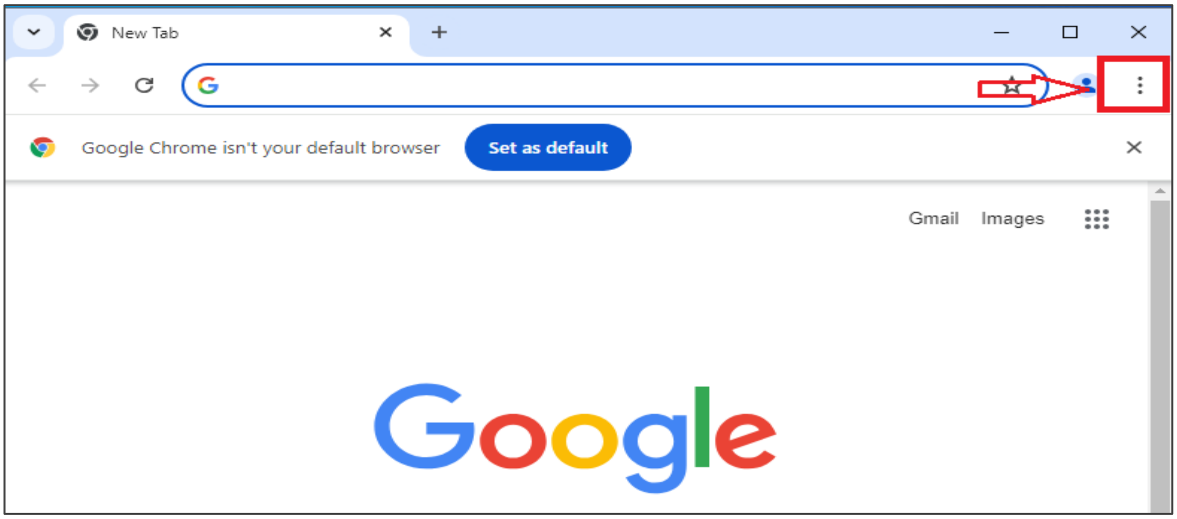
**Prerequisites:** None

Steps to be followed:

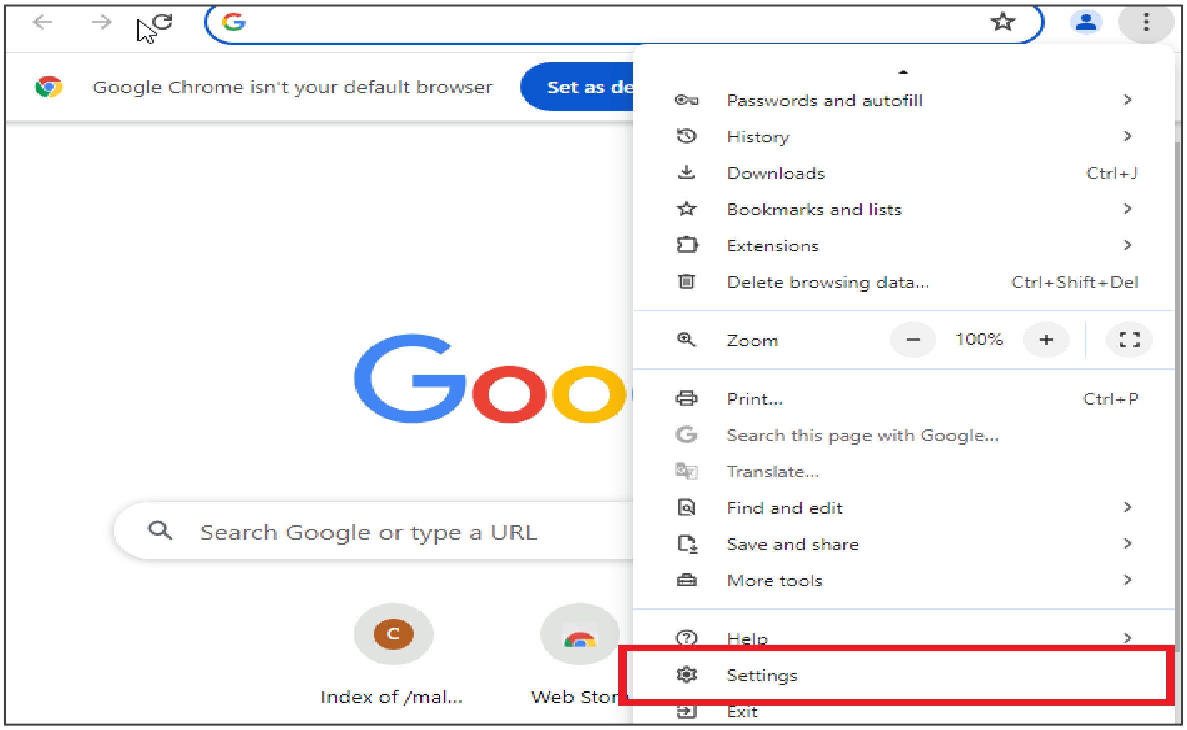
1. Disable the Google Chrome security settings
2. Disable the Windows Defender
3. Download the malware
4. Download 7-zip
5. Perform VirusTotal analysis
6. Perform hash, IP information, and graph analysis

## Step 1: Disable the Google Chrome security settings

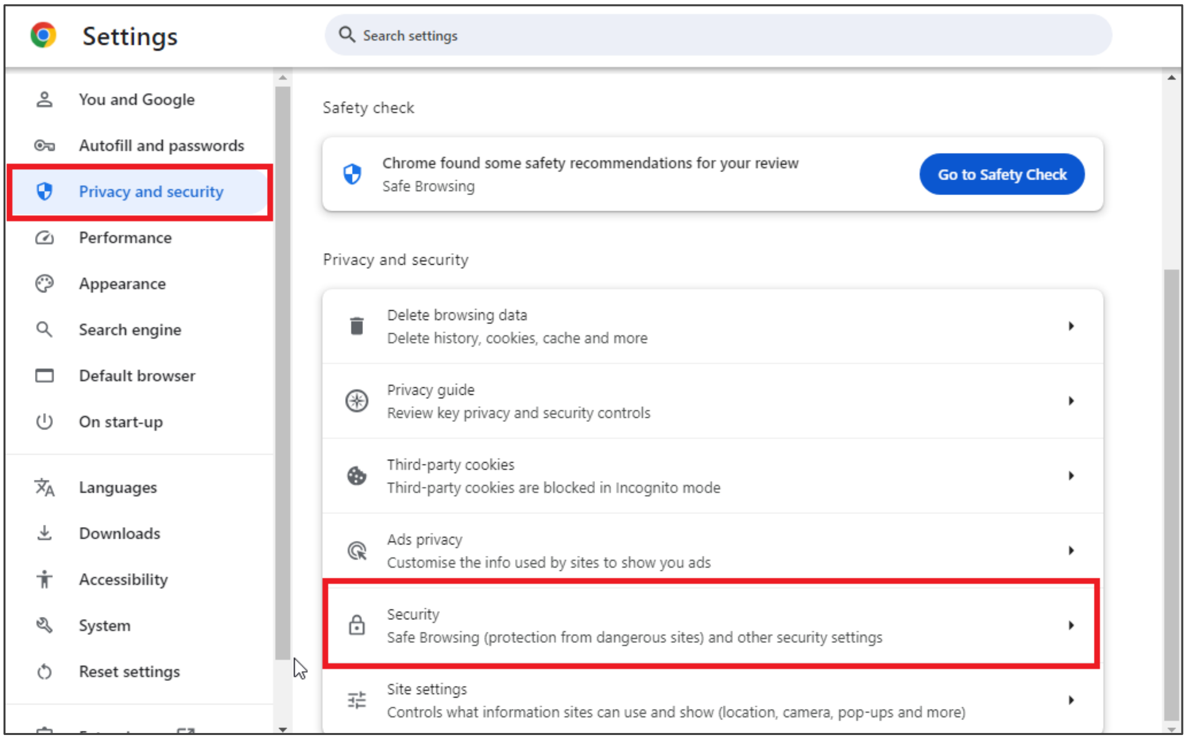
1.1 Open the **Google Chrome** browser, go to the **3 dots** in the right corner, and **click** on it



1.2 Click on the **Settings** option



1.3 Select **Privacy and security** and click on **Security**



Safety check

Chrome found some safety recommendations for your review
Safe Browsing

Privacy and security

Delete browsing data
Delete history, cookies, cache and more

Privacy guide
Review key privacy and security controls

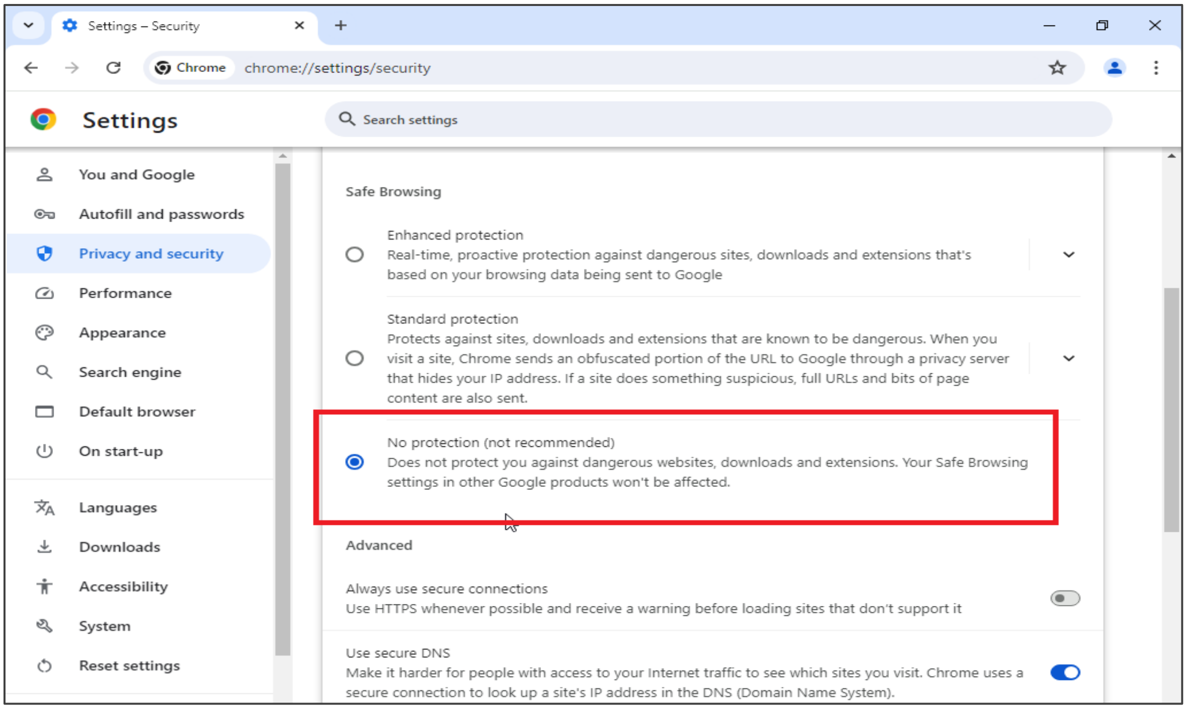
Third-party cookies
Third-party cookies are blocked in Incognito mode

Ads privacy
Customise the info used by sites to show you ads

Security
Safe Browsing (protection from dangerous sites) and other security settings

Site settings
Controls what information sites can use and show (location, camera, pop-ups and more)

1.4 Select the **No protection (not recommended)** option



Safe Browsing

○ Enhanced protection
Real-time, proactive protection against dangerous sites, downloads and extensions that's based on your browsing data being sent to Google

○ Standard protection
Protects against sites, downloads and extensions that are known to be dangerous. When you visit a site, Chrome sends an obfuscated portion of the URL to Google through a privacy server that hides your IP address. If a site does something suspicious, full URLs and bits of page content are also sent.

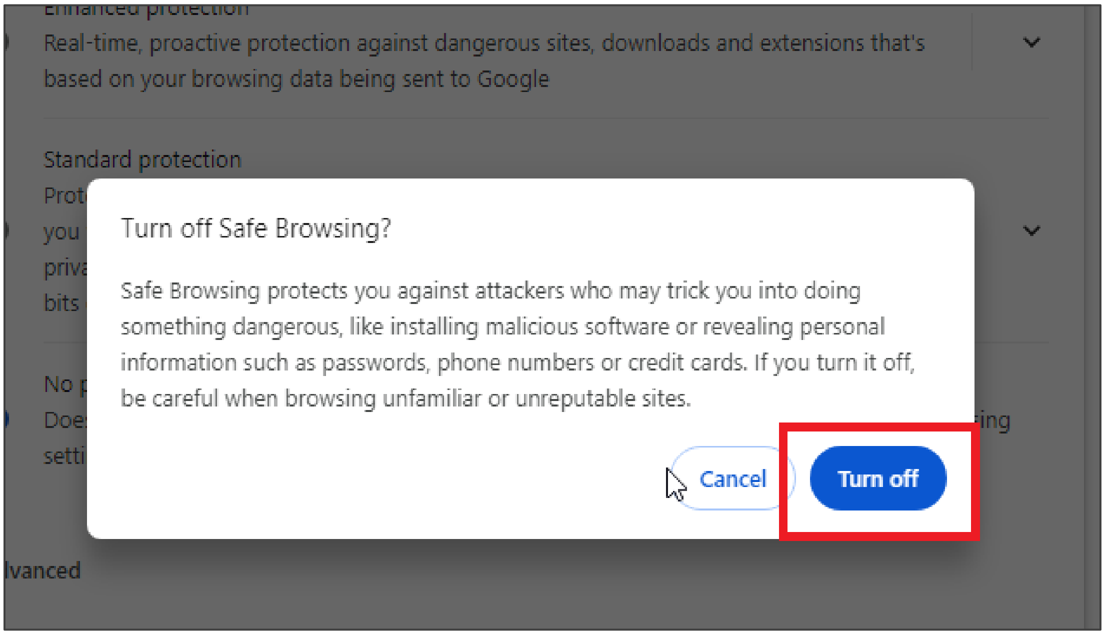
● No protection (not recommended)
Does not protect you against dangerous websites, downloads and extensions. Your Safe Browsing settings in other Google products won't be affected.

Advanced

Always use secure connections
Use HTTPS whenever possible and receive a warning before loading sites that don't support it

Use secure DNS
Make it harder for people with access to your Internet traffic to see which sites you visit. Chrome uses a secure connection to look up a site's IP address in the DNS (Domain Name System).

1.5 Click on the **Turn off** button when prompted



Enhanced protection

Real-time, proactive protection against dangerous sites, downloads and extensions that's based on your browsing data being sent to Google

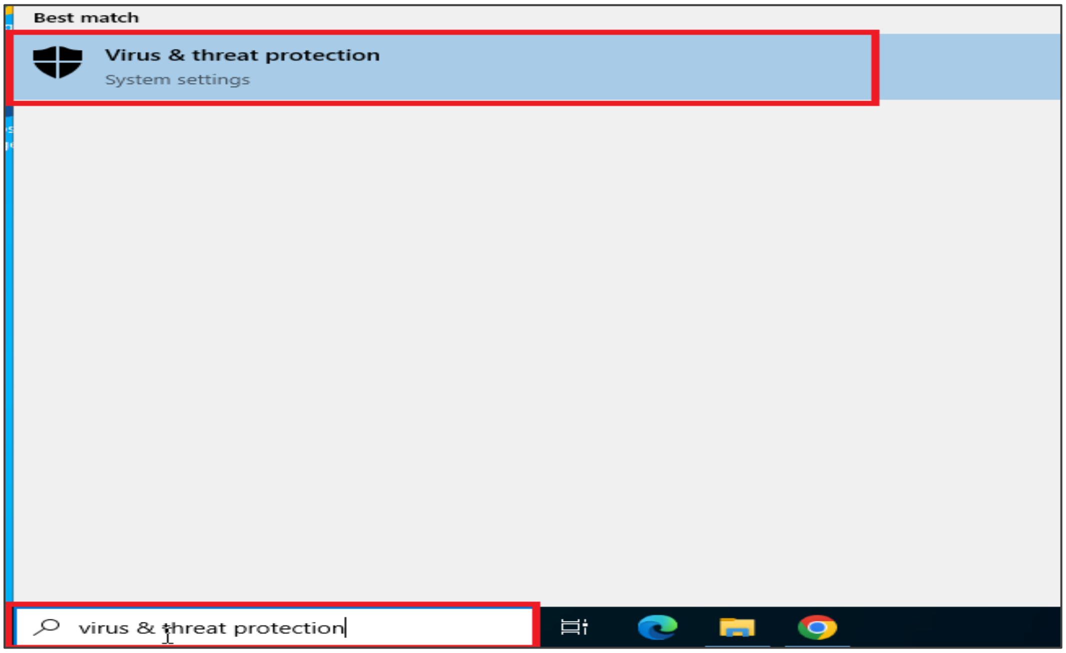
Standard protection

Turn off Safe Browsing?

Safe Browsing protects you against attackers who may trick you into doing something dangerous, like installing malicious software or revealing personal information such as passwords, phone numbers or credit cards. If you turn it off, be careful when browsing unfamiliar or unreputable sites.

## Step 2: Disable the Windows Defender

2.1 Search for **Virus & threat protection** in the Windows search box and open it

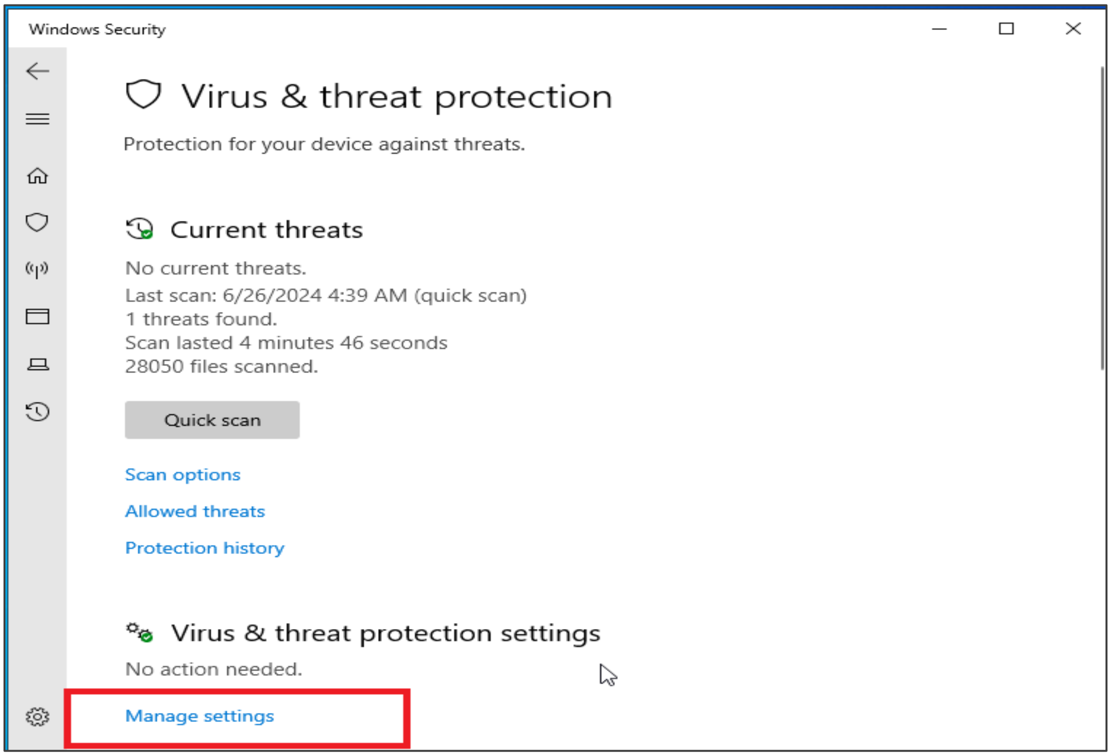


Best match

Virus & threat protection
System settings

virus & threat protection

2.2 Go to the **Manage settings** option in the **Virus & threat protection** window



Windows Security

Virus & threat protection

Protection for your device against threats.

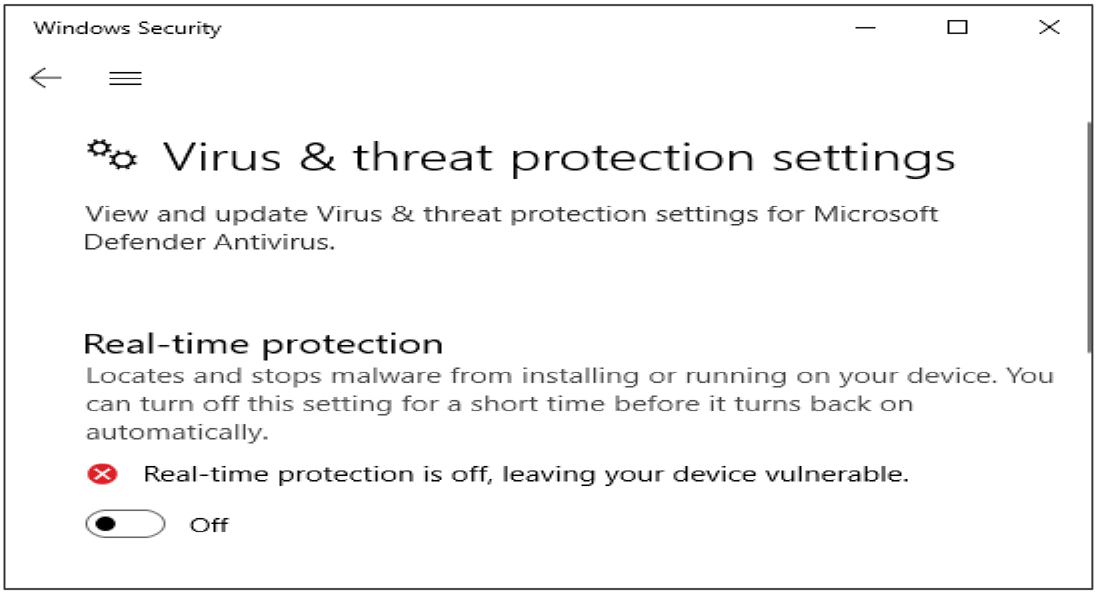
Current threats

No current threats.
Last scan: 6/26/2024 4:39 AM (quick scan)
1 threats found.
Scan lasted 4 minutes 46 seconds
28050 files scanned.

Virus & threat protection settings

No action needed.

2.3 Turn off **Real-time protection** and other relevant settings



Windows Security

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

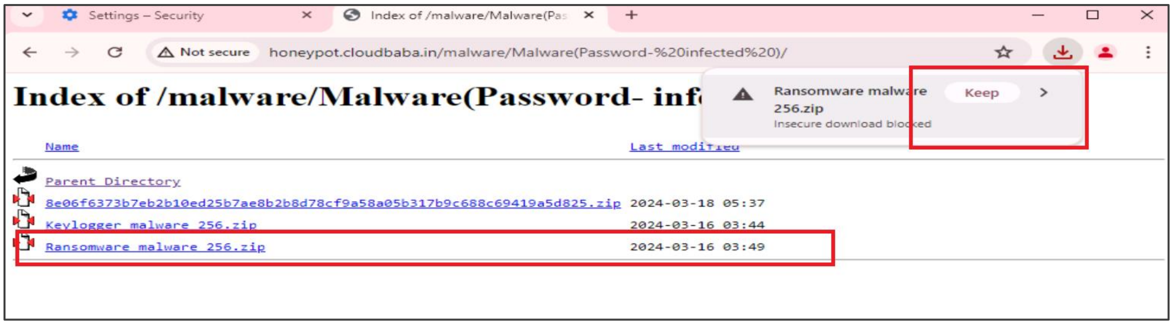
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

## Step 3: Download the malware

3.1 Visit **http://honeypot.cloudbaba.in/malware**, click on any malware link to download it, and then click **Keep** to confirm the download

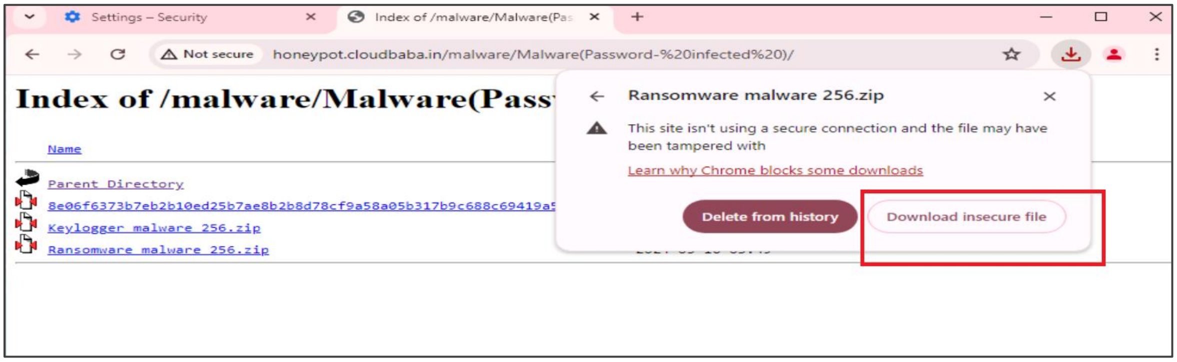

Settings – Security
Index of /malware/Malware(Pas
Not secure
honeypot.cloudbaba.in/malware/Malware(Password-%20infected%20)/
Keep

# Index of /malware/Malware(Password- inf

Ransomware malware 256.zip
Insecure download blocked

```
Name                                                                        Last modified
Parent Directory
8e06f6373b7eb2b10ed25b7ae8b2b8d78cf9a58a05b317b9c688c69419a5d825.zip 2024-03-18 05:37
Keylogger malware 256.zip                                            2024-03-16 03:44
Ransomware malware 256.zip                                           2024-03-16 03:49
```

3.2 Click on **Download insecure file**


Settings – Security
Index of /malware/Malware(Pas
Not secure
honeypot.cloudbaba.in/malware/Malware(Password-%20infected%20)/
Delete from history
Download insecure file

# Index of /malware/Malware(Pass

```
Name
Parent Directory
8e06f6373b7eb2b10ed25b7ae8b2b8d78cf9a58a05b317b9c688c69419a5
Keylogger malware 256.zip
Ransomware malware 256.zip
```

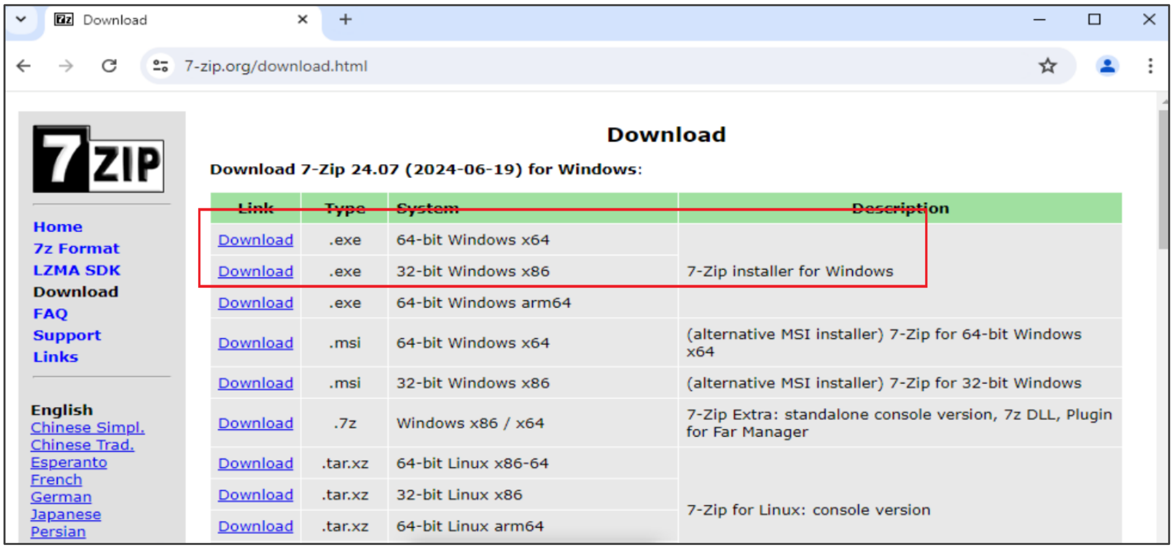
Ransomware malware 256.zip

This site isn't using a secure connection and the file may have been tampered with

Learn why Chrome blocks some downloads

## Step 4: Download 7-zip

4.1 Download **7-zip** using the link given below to extract the downloaded malware sample: **https://www.7-zip.org/download.html**

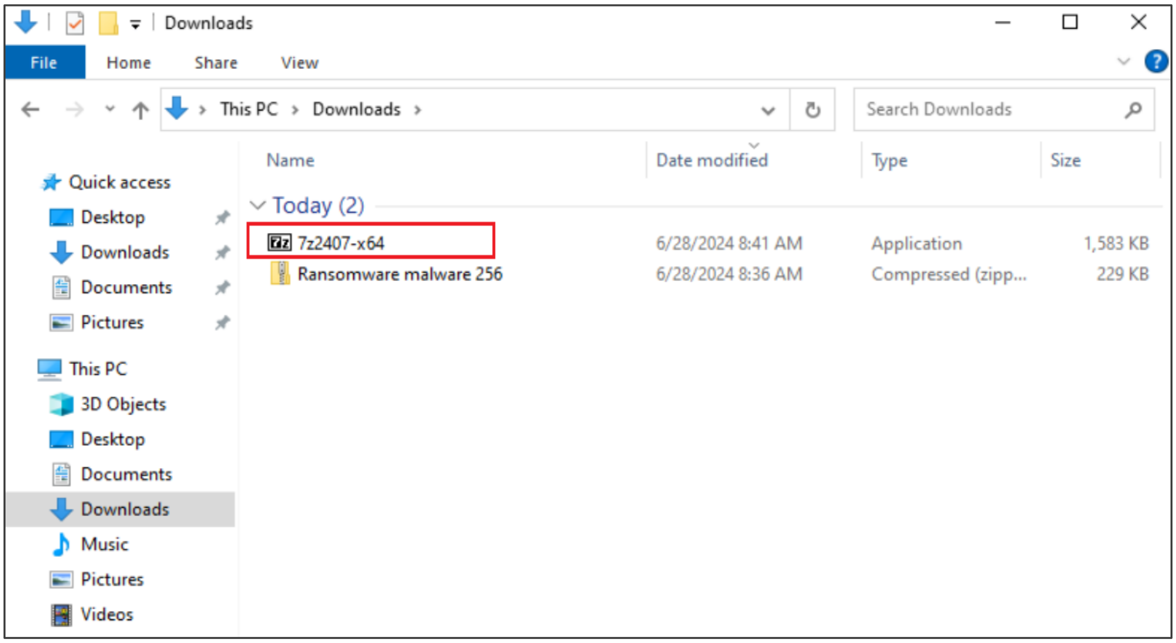


Download

Download 7-Zip 24.07 (2024-06-19) for Windows:

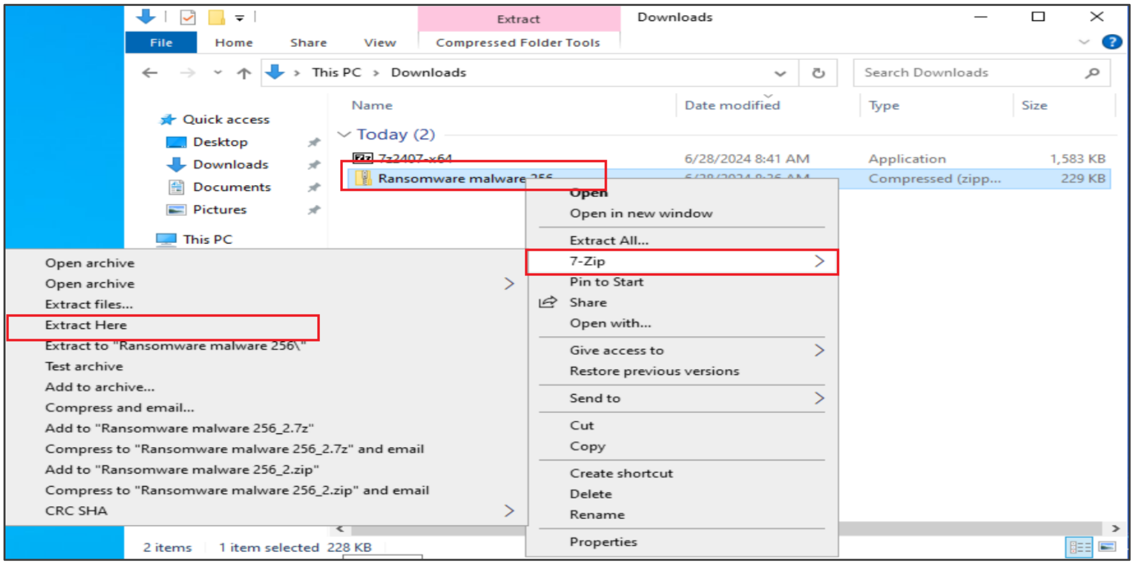
| Link | Type | System | Description |
|---|---|---|---|
| Download | .exe | 64-bit Windows x64 | 7-Zip installer for Windows |
| Download | .exe | 32-bit Windows x86 | |
| Download | .exe | 64-bit Windows arm64 | |
| Download | .msi | 64-bit Windows x64 | (alternative MSI installer) 7-Zip for 64-bit Windows x64 |
| Download | .msi | 32-bit Windows x86 | (alternative MSI installer) 7-Zip for 32-bit Windows |
| Download | .7z | Windows x86 / x64 | 7-Zip Extra: standalone console version, 7z DLL, Plugin for Far Manager |
| Download | .tar.xz | 64-bit Linux x86-64 | 7-Zip for Linux: console version |
| Download | .tar.xz | 32-bit Linux x86 | |
| Download | .tar.xz | 64-bit Linux arm64 | |

4.2 Go to the **Downloads** folder and double-click on the **7-zip exe file** to install it

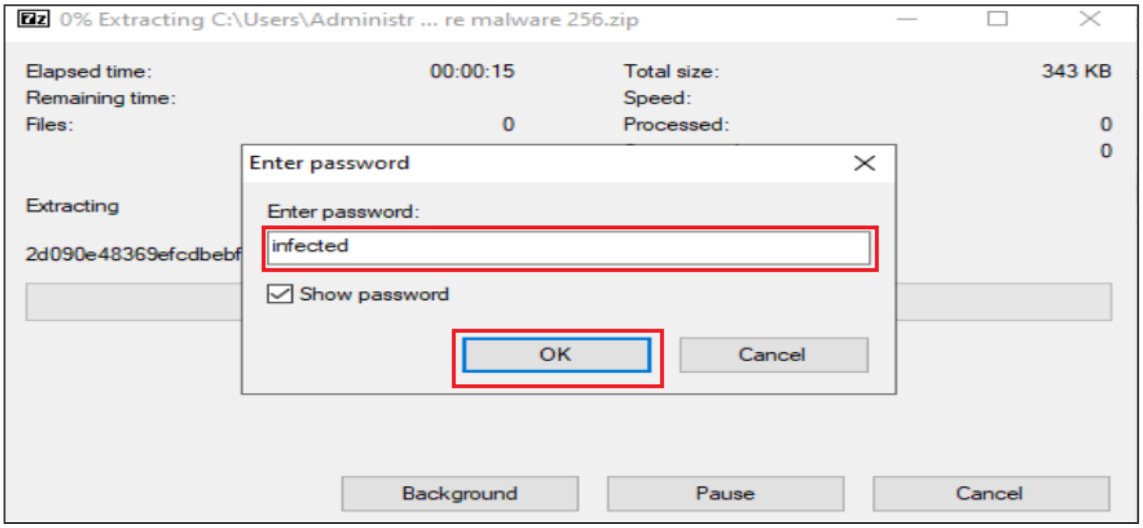


| Name | Date modified | Type | Size |
|---|---|---|---|
| 7z2407-x64 | 6/28/2024 8:41 AM | Application | 1,583 KB |
| Ransomware malware 256 | 6/28/2024 8:36 AM | Compressed (zipp... | 229 KB |

4.3 Right-click on the downloaded malware sample, select **7-zip,** and click **Extract Here**



4.4 Enter the password as **infected** and click on **OK** to extract the file



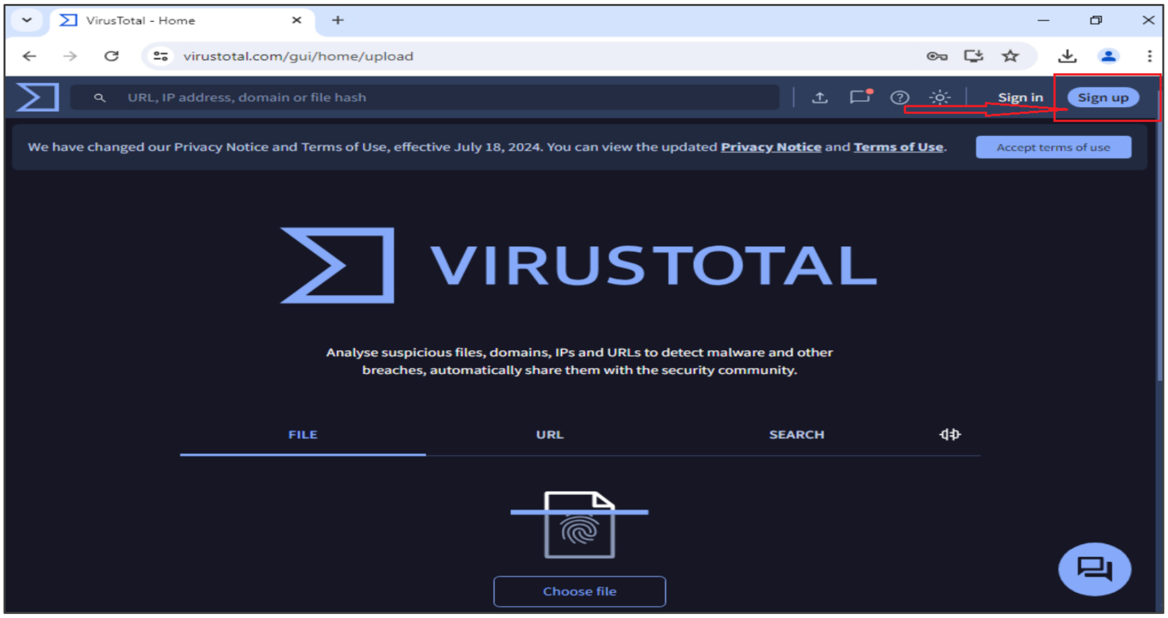
Elapsed time: 00:00:15
Remaining time:
Files: 0
Total size: 343 KB
Speed:
Processed: 0
0

Enter password: infected

☑ Show password

## Step 5: Perform VirusTotal analysis

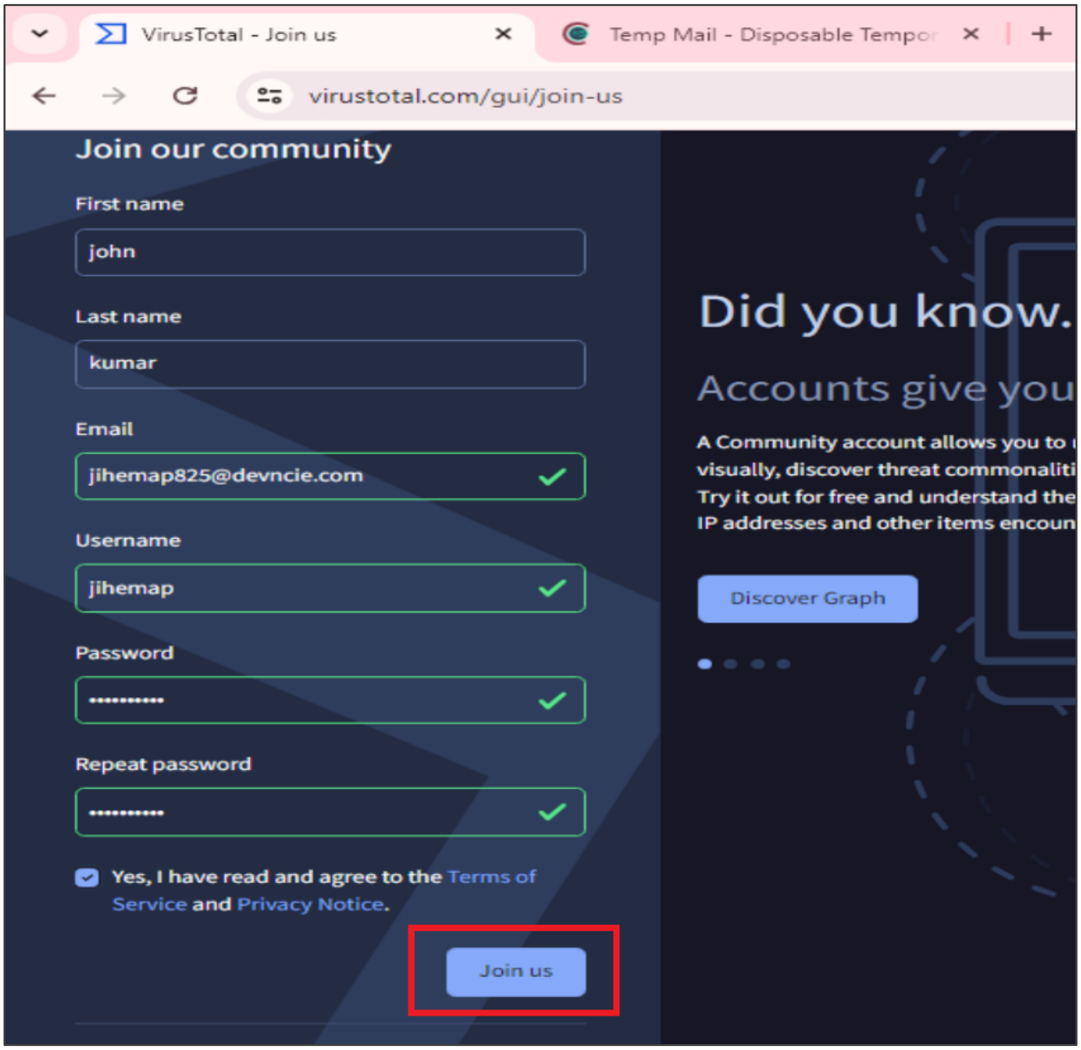
5.1 Visit the link given below to open the **VirusTotal** application and click on the **Sign up** button:
**https://www.virustotal.com/gui/home/upload**



We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated **Privacy Notice** and **Terms of Use**.

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

5.2 Fill in the details and click on **Join us**



VirusTotal - Join us
Temp Mail - Disposable Tempor
virustotal.com/gui/join-us

Join our community

First name: john

Last name: kumar

Email: jihemap825@devncie.com ✓

Username: jihemap ✓

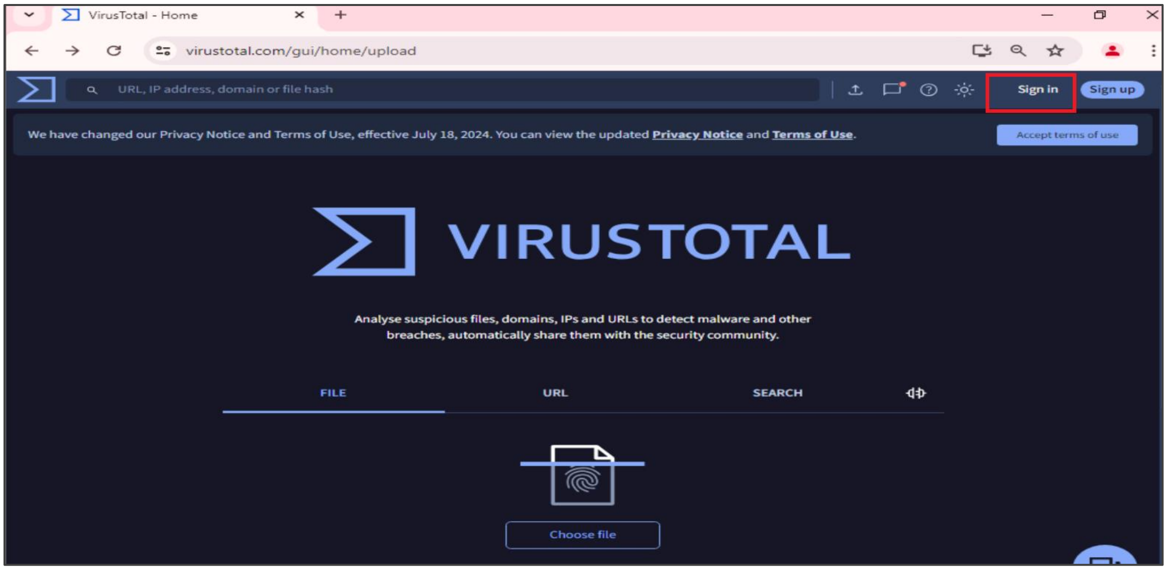
Password: ••••••••••• ✓

Repeat password: ••••••••••• ✓

☑ Yes, I have read and agree to the Terms of Service and Privacy Notice.

Join us
Did you know.
Accounts give you
A Community account allows you to
visually, discover threat commonaliti
Try it out for free and understand the
IP addresses and other items encoun
Discover Graph

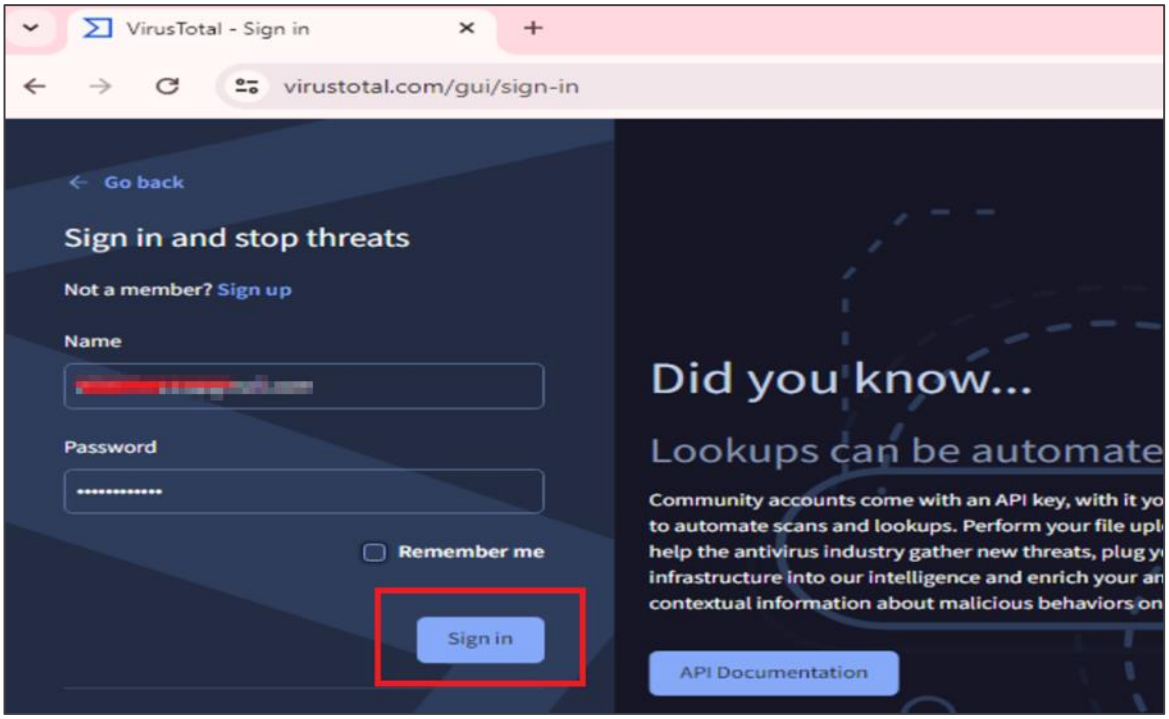
5.3 Click on **Sign in** after verifying your email ID



We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated Privacy Notice and Terms of Use.

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

5.4 Enter the email address and password and click on **Sign in**



Sign in and stop threats

Not a member? Sign up

Name

[redacted]

Password

•••••••••••••

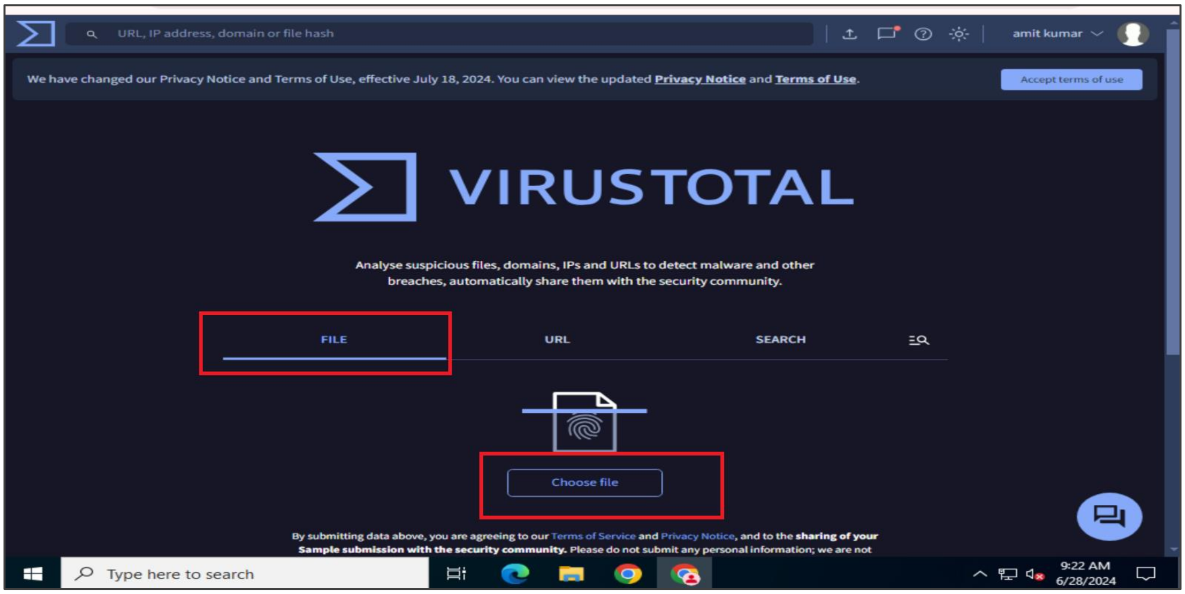
□ Remember me

Did you know...

Lookups can be automate

Community accounts come with an API key, with it yo
to automate scans and lookups. Perform your file upl
help the antivirus industry gather new threats, plug y
infrastructure into our intelligence and enrich your an
contextual information about malicious behaviors on

5.5 Under the **FILE** option, click on **Choose File** to upload the extracted file for malware analysis

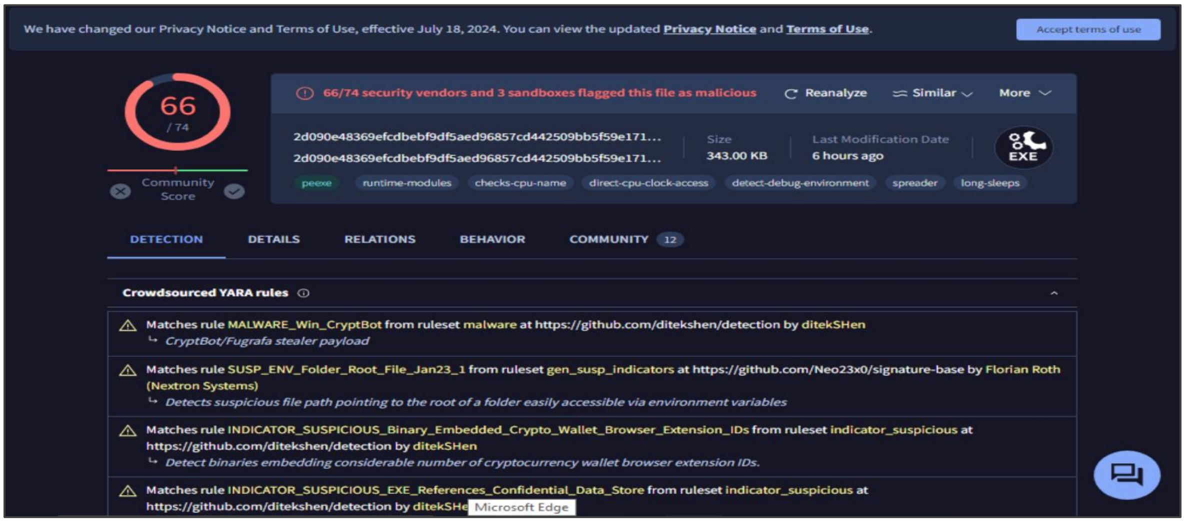


We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated **Privacy Notice** and **Terms of Use**.

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not

It can be observed that the malware sample was scanned by 74 antivirus engines, with 66 detecting it as malicious. This number is expected to increase over time.



We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated **Privacy Notice** and **Terms of Use**.

66/74 security vendors and 3 sandboxes flagged this file as malicious

2d090e48369efcdbebf9df5aed96857cd442509bb5f59e171...
2d090e48369efcdbebf9df5aed96857cd442509bb5f59e171...

Size
343.00 KB

Last Modification Date
6 hours ago

peexe runtime-modules checks-cpu-name direct-cpu-clock-access detect-debug-environment spreader long-sleeps

**Crowdsourced YARA rules**

⚠ Matches rule MALWARE_Win_CryptBot from ruleset malware at https://github.com/ditekshen/detection by ditekSHen
↳ *CryptBot/Fugrafa stealer payload*

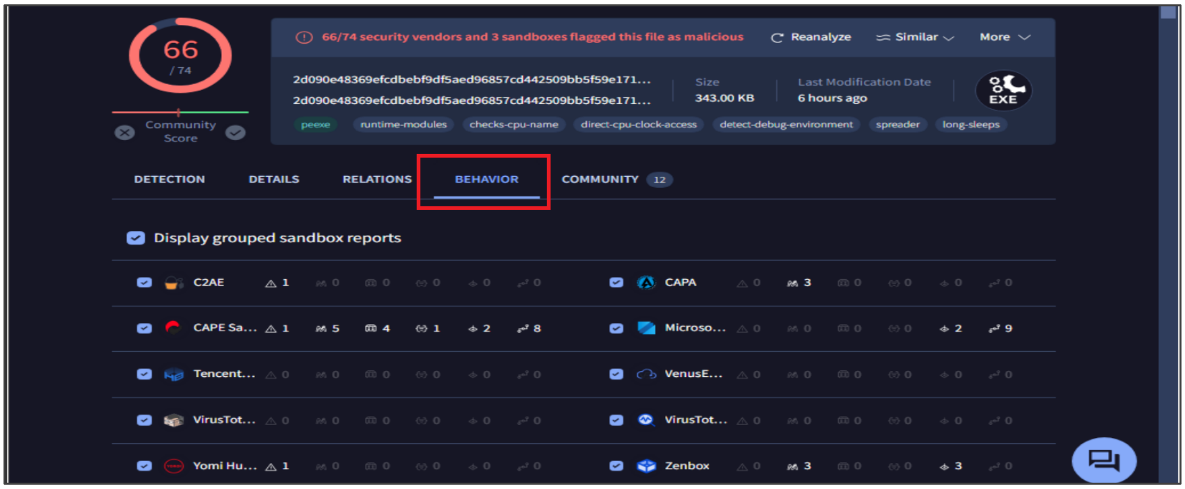
⚠ Matches rule SUSP_ENV_Folder_Root_File_Jan23_1 from ruleset gen_susp_indicators at https://github.com/Neo23x0/signature-base by Florian Roth (Nextron Systems)
↳ *Detects suspicious file path pointing to the root of a folder easily accessible via environment variables*

⚠ Matches rule INDICATOR_SUSPICIOUS_Binary_Embedded_Crypto_Wallet_Browser_Extension_IDs from ruleset indicator_suspicious at https://github.com/ditekshen/detection by ditekSHen
↳ *Detect binaries embedding considerable number of cryptocurrency wallet browser extension IDs.*

⚠ Matches rule INDICATOR_SUSPICIOUS_EXE_References_Confidential_Data_Store from ruleset indicator_suspicious at https://github.com/ditekshen/detection by ditekSHe

## Step 6: Perform hash, IP information, and graph analysis

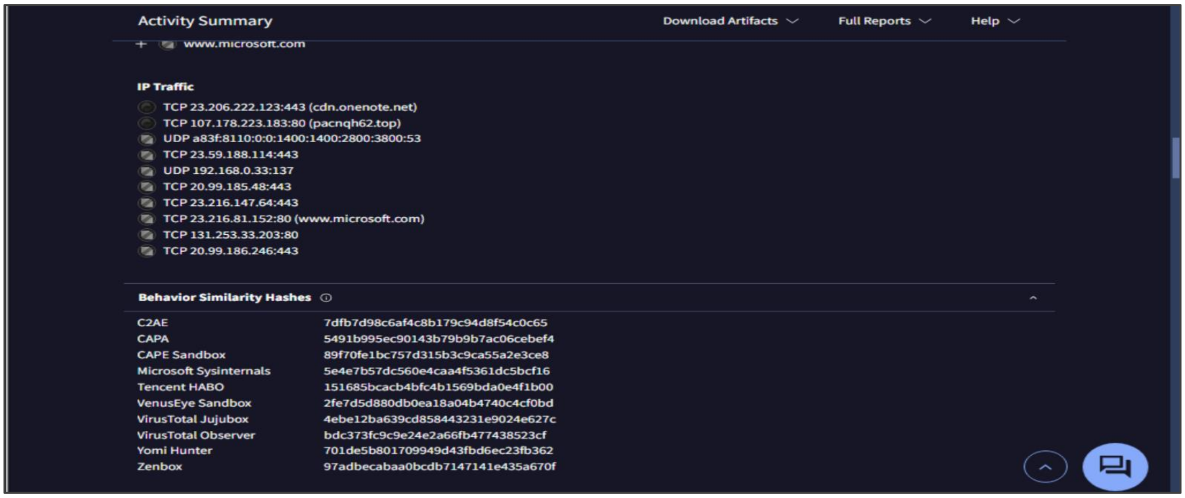
6.1 Click on the **BEHAVIOR** tab and scroll down to view the details about the IP traffic and hashes



66/74 security vendors and 3 sandboxes flagged this file as malicious

2d090e48369efcdbebf9df5aed96857cd442509bb5f59e171...
2d090e48369efcdbebf9df5aed96857cd442509bb5f59e171...

☑ Display grouped sandbox reports



+ www.microsoft.com

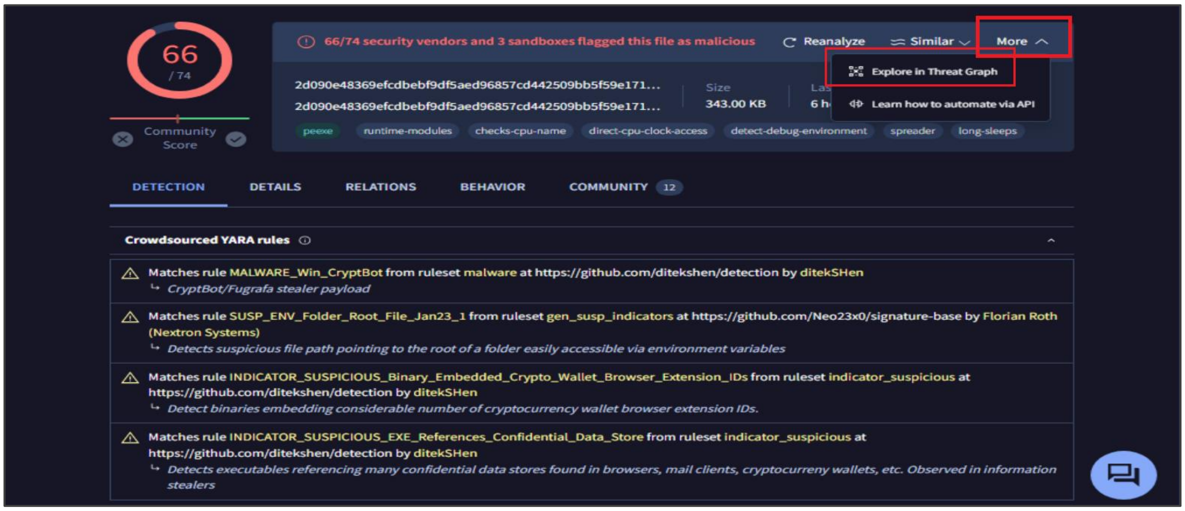
**IP Traffic**

```
TCP 23.206.222.123:443 (cdn.onenote.net)
TCP 107.178.223.183:80 (pacnqh62.top)
UDP a83f:8110:0:0:1400:1400:2800:3800:53
TCP 23.59.188.114:443
UDP 192.168.0.33:137
TCP 20.99.185.48:443
TCP 23.216.147.64:443
TCP 23.216.81.152:80 (www.microsoft.com)
TCP 131.253.33.203:80
TCP 20.99.186.246:443
```

**Behavior Similarity Hashes**

| | |
|---|---|
| C2AE | 7dfb7d98c6af4c8b179c94d8f54c0c65 |
| CAPA | 5491b995ec90143b79b9b7ac06cebef4 |
| CAPE Sandbox | 89f70fe1bc757d315b3c9ca55a2e3ce8 |
| Microsoft Sysinternals | 5e4e7b57dc560e4caa4f5361dc5bcf16 |
| Tencent HABO | 151685bcacb4bfc4b1569bda0e4f1b00 |
| VenusEye Sandbox | 2fe7d5d880db0ea18a04b4740c4cf0bd |
| VirusTotal Jujubox | 4ebe12ba639cd858443231e9024e627c |
| VirusTotal Observer | bdc373fc9c9e24e2a66fb477438523cf |
| Yomi Hunter | 701de5b801709949d43fbd6ec23fb362 |
| Zenbox | 97adbecabaa0bcdb7147141e435a670f |

6.2 Select the **More** option and choose **Explore in Threat Graph**



66/74 security vendors and 3 sandboxes flagged this file as malicious

2d090e48369efcdbebf9df5aed96857cd442509bb5f59e171...
2d090e48369efcdbebf9df5aed96857cd442509bb5f59e171...

**Crowdsourced YARA rules**

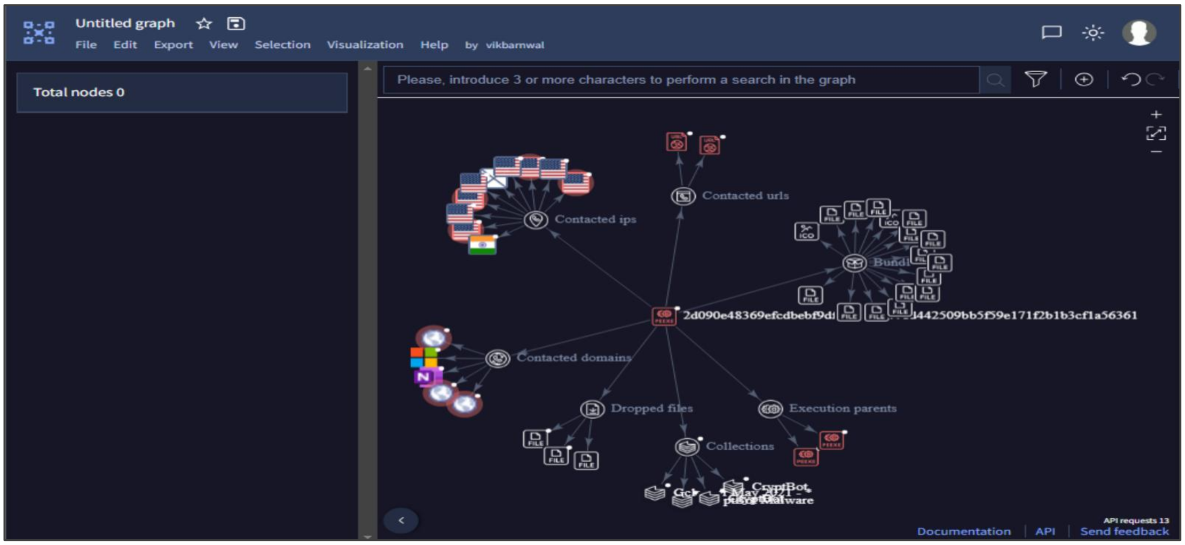
⚠ Matches rule MALWARE_Win_CryptBot from ruleset malware at https://github.com/ditekshen/detection by ditekSHen
↳ *CryptBot/Fugrafa stealer payload*

⚠ Matches rule SUSP_ENV_Folder_Root_File_Jan23_1 from ruleset gen_susp_indicators at https://github.com/Neo23x0/signature-base by Florian Roth (Nextron Systems)
↳ *Detects suspicious file path pointing to the root of a folder easily accessible via environment variables*

⚠ Matches rule INDICATOR_SUSPICIOUS_Binary_Embedded_Crypto_Wallet_Browser_Extension_IDs from ruleset indicator_suspicious at https://github.com/ditekshen/detection by ditekSHen
↳ *Detect binaries embedding considerable number of cryptocurrency wallet browser extension IDs.*

⚠ Matches rule INDICATOR_SUSPICIOUS_EXE_References_Confidential_Data_Store from ruleset indicator_suspicious at https://github.com/ditekshen/detection by ditekSHen
↳ *Detects executables referencing many confidential data stores found in browsers, mail clients, cryptocurreny wallets, etc. Observed in information stealers*

The graph is available for analysis.

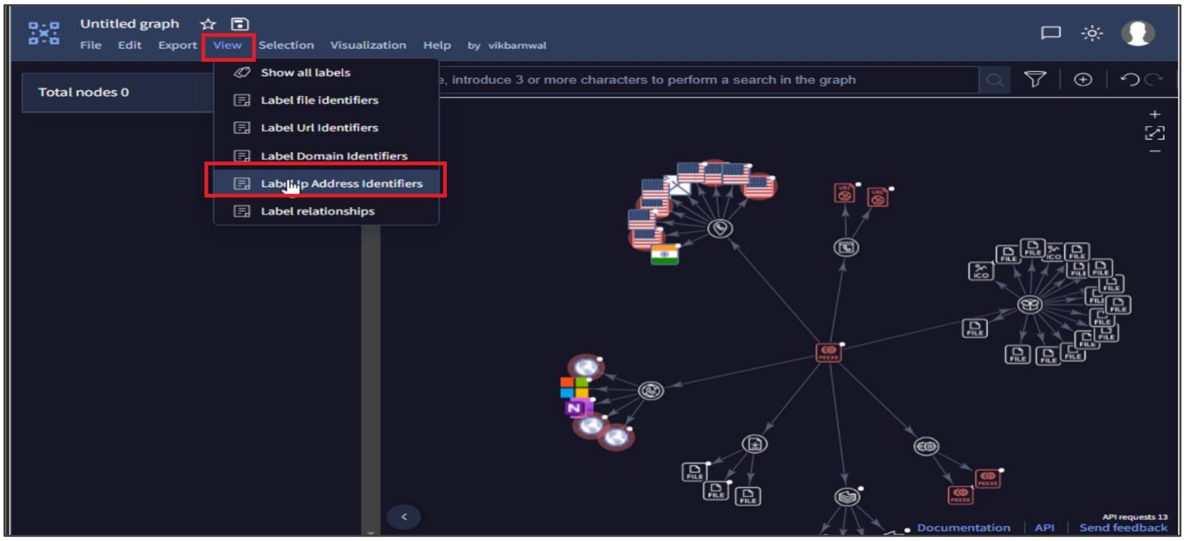


Total nodes 0

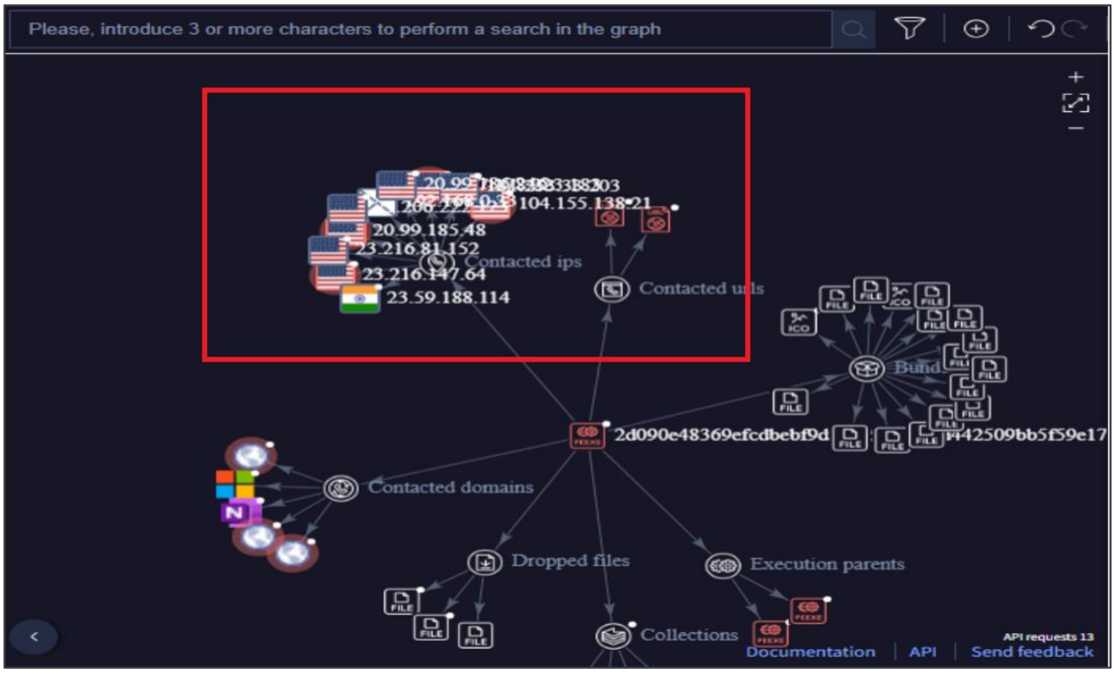
Please, introduce 3 or more characters to perform a search in the graph

2d090e48369efcdbebf9d... 442509bb5f59e171f2b1b3cf1a56361

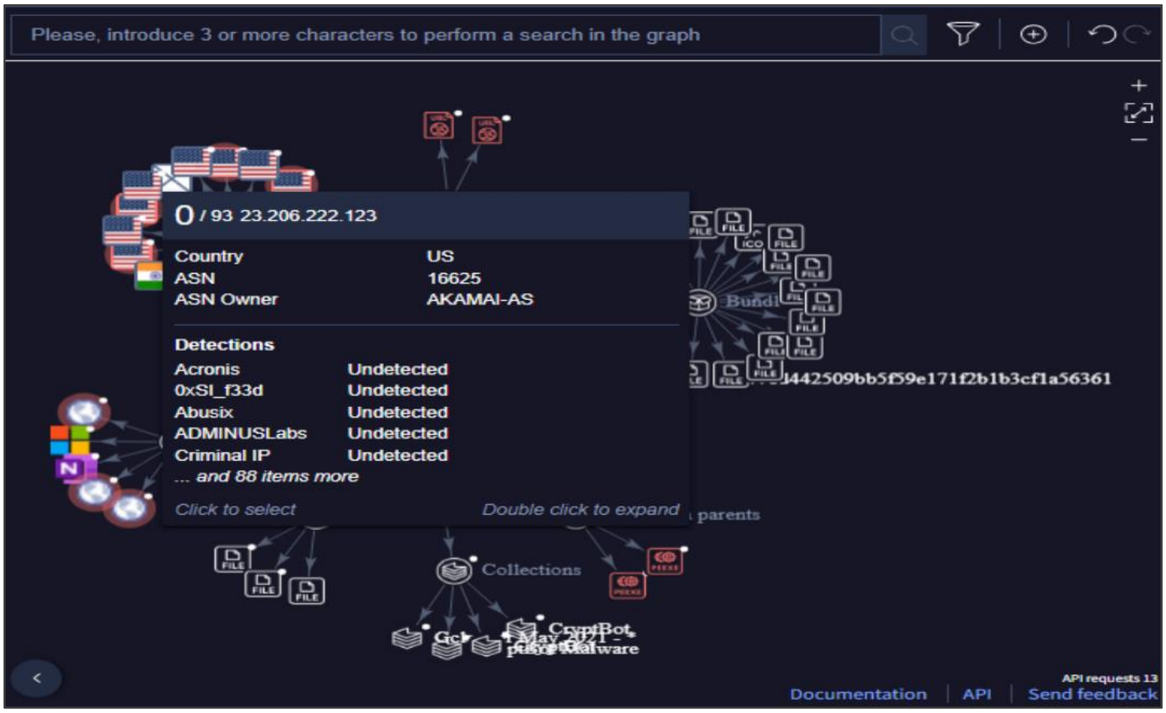
6.3 Select **View** and then select **Label Ip Address Identifiers** to see the IP address of the given country



You can also see the individual IP address.



Individual information about each IP address can be found by hovering the cursor over it.



Please, introduce 3 or more characters to perform a search in the graph

0 / 93 23.206.222.123

| | |
|---|---|
| Country | US |
| ASN | 16625 |
| ASN Owner | AKAMAI-AS |

**Detections**

| | |
|---|---|
| Acronis | Undetected |
| 0xSI_f33d | Undetected |
| Abusix | Undetected |
| ADMINUSLabs | Undetected |
| Criminal IP | Undetected |

*... and 88 items more*

*Click to select* *Double click to expand*

Following the above steps, you have successfully performed a comprehensive malware analysis using VirusTotal, hash, IP information, and graph visualization to understand the malware's behavior and network relationships.