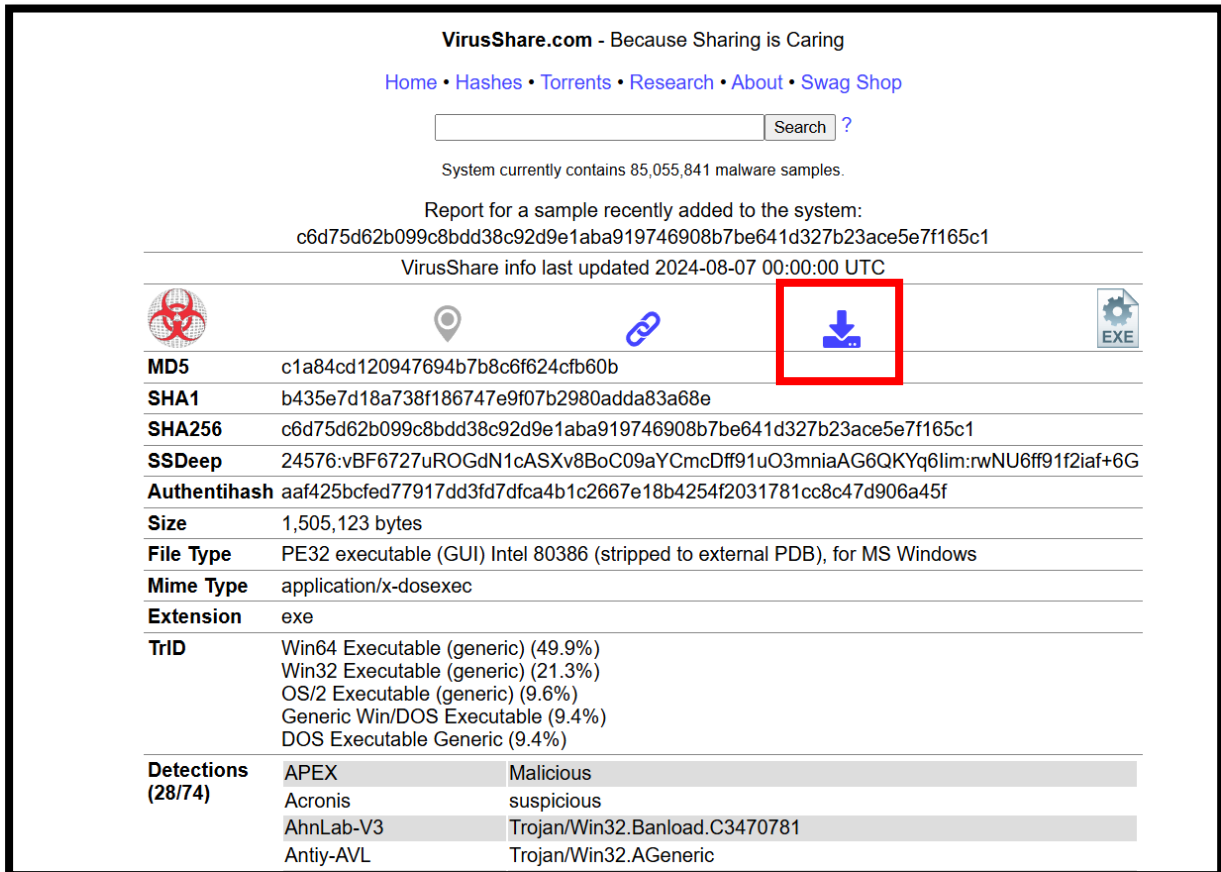


Practical No 9

AIM: Malware Analysis and Detection: Analyze and identify malware samples using antivirus tools, analyze their behavior, and develop countermeasures to mitigate their impact.

Step 1: Visit the website VirusShare.com for downloading the virus samples.

Step 2: Click on Download.








VirusShare.com - Because Sharing is Caring

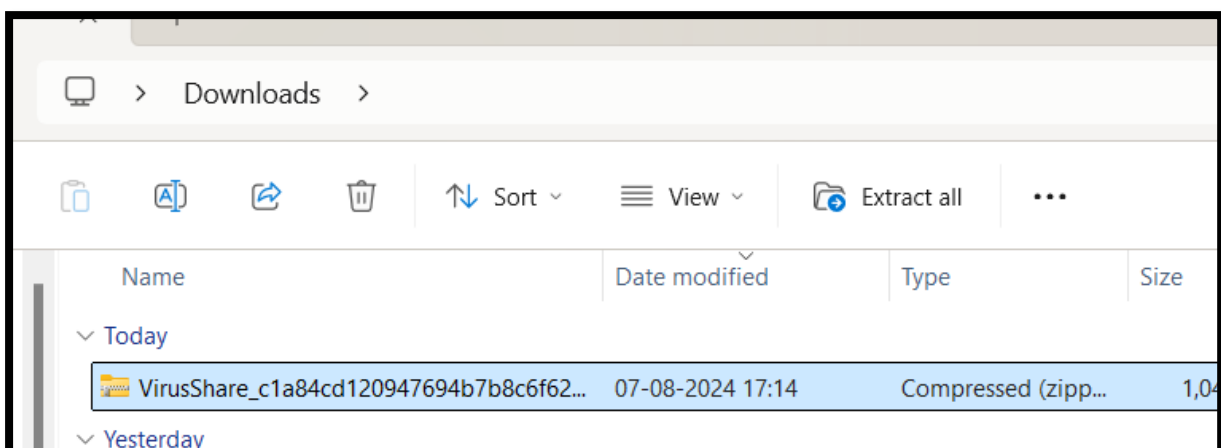
[Home](#) • [Hashes](#) • [Torrents](#) • [Research](#) • [About](#) • [Swag Shop](#)

System currently contains 85,055,841 malware samples.

Report for a sample recently added to the system:
c6d75d62b099c8bdd38c92d9e1aba919746908b7be641d327b23ace5e7f165c1

VirusShare info last updated 2024-08-07 00:00:00 UTC

												
MD5	c1a84cd120947694b7b8c6f624cfb60b											
SHA1	b435e7d18a738f186747e9f07b2980adda83a68e											
SHA256	c6d75d62b099c8bdd38c92d9e1aba919746908b7be641d327b23ace5e7f165c1											
SSDeep	24576:vBF6727uROGdN1cASXv8BoC09aYCMcDff91uO3mniaAG6QKYq6lim:rwNU6ff91f2iaf+6G											
Authentihash	aaf425bcfed77917dd3fd7dfca4b1c2667e18b4254f2031781cc8c47d906a45f											
Size	1,505,123 bytes											
File Type	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows											
Mime Type	application/x-dosexec											
Extension	exe											
TrID	Win64 Executable (generic) (49.9%) Win32 Executable (generic) (21.3%) OS/2 Executable (generic) (9.6%) Generic Win/DOS Executable (9.4%) DOS Executable Generic (9.4%)											
Detections (28/74)	<table border="1"><tr><td>APEX</td><td>Malicious</td></tr><tr><td>Acronis</td><td>suspicious</td></tr><tr><td>AhnLab-V3</td><td>Trojan/Win32.Banload.C3470781</td></tr><tr><td>Antiy-AVL</td><td>Trojan/Win32.AGeneric</td></tr></table>				APEX	Malicious	Acronis	suspicious	AhnLab-V3	Trojan/Win32.Banload.C3470781	Antiy-AVL	Trojan/Win32.AGeneric
APEX	Malicious											
Acronis	suspicious											
AhnLab-V3	Trojan/Win32.Banload.C3470781											
Antiy-AVL	Trojan/Win32.AGeneric											

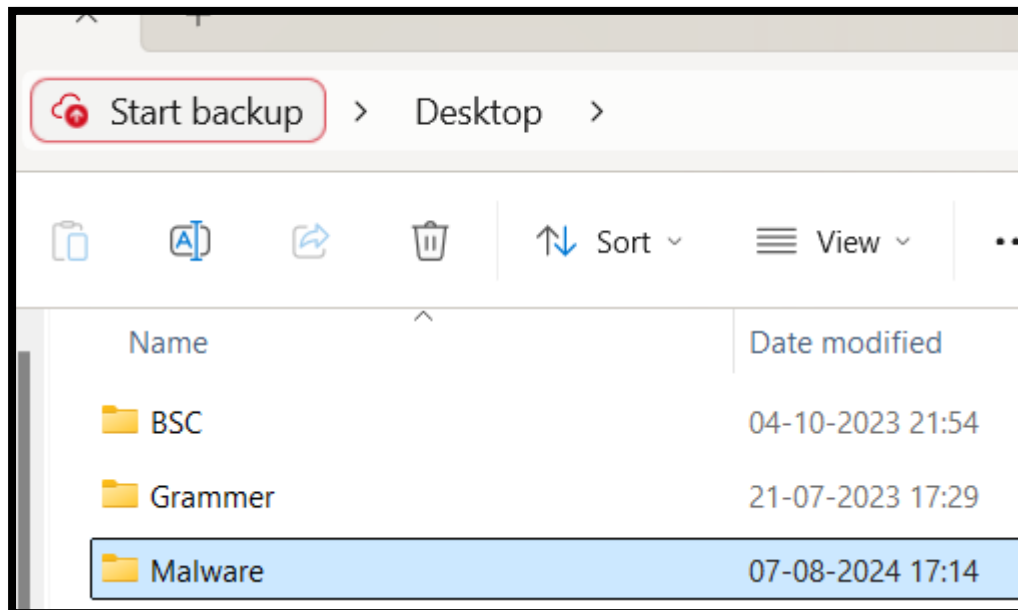


Downloads

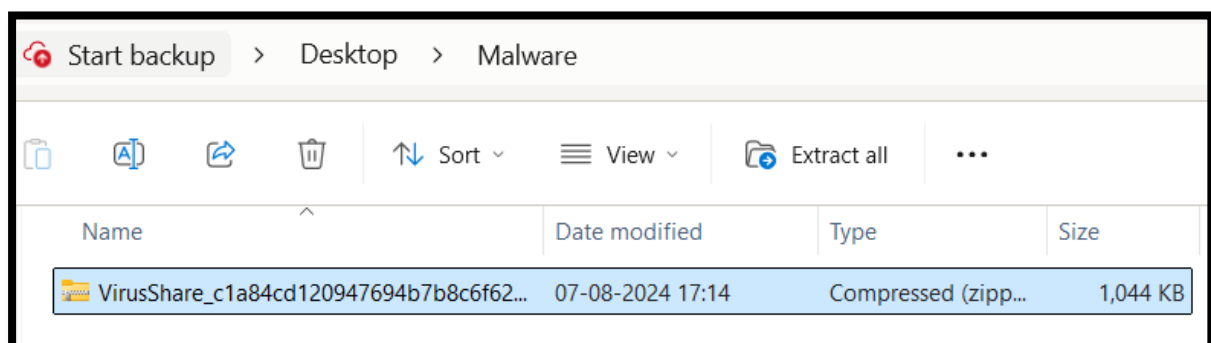
Sort View Extract all

Name	Date modified	Type	Size
Today			
VirusShare_c1a84cd120947694b7b8c6f62...	07-08-2024 17:14	Compressed (zipp...	1,04
Yesterday			

Step 3: Create a folder on the desktop name as Malware.



Step 4: Paste the zip file in that folder.



Step 5: Now scan the zip file on the website www.virustotal.com. Choose a file and scan it.



VirusShare.com - Because Sharing is Caring

[Home](#) • [Hashes](#) • [Torrents](#) • [Research](#) • [About](#) • [Swag Shop](#)

VirusShare.com is a repository of malware samples to provide security researchers, incident responders, forensic analysts, and the morbidly curious access to samples of live malicious code.

For safety reasons, access to the site is granted by invitation only. To request to be added to the list, please email Melissa at Melissa97@virusshare.com with 'access' in the subject. She will review your request and hopefully send you an invitation link. Access to the site may be revoked at any time.

The use of bots, scripts, or other methods to scrape data from the site, download samples at an excessive rate, or otherwise affecting the performance of the site, backend systems, or user experience will not be tolerated.

This site provides access to live malware. VirusShare is not responsible for any damage, infection, breach or other incident that may result from accessing this website and displaying or downloading information. Access is granted at your risk.

All samples are delivered in password-protected zip-files for safety. **The password for all zip-compressed malware samples is "infected".**

You can follow VirusShare via Mastodon at [@VXShare@infosec.exchange](https://infosec.exchange/@VXShare).

If you need to contact the administrator, he can be emailed at admin@virusshare.com

VirusShare is a service hosted and maintained by [Corvus Forensics](#).

If you would like to support the project, please purchase some items from our [swag shop](#)!

Regarding cookies: This site uses cookies. If you do not agree to allow the session cookie, you will not find this site particularly useful since you will not be able to authenticate. You can read our privacy policy [here](#).



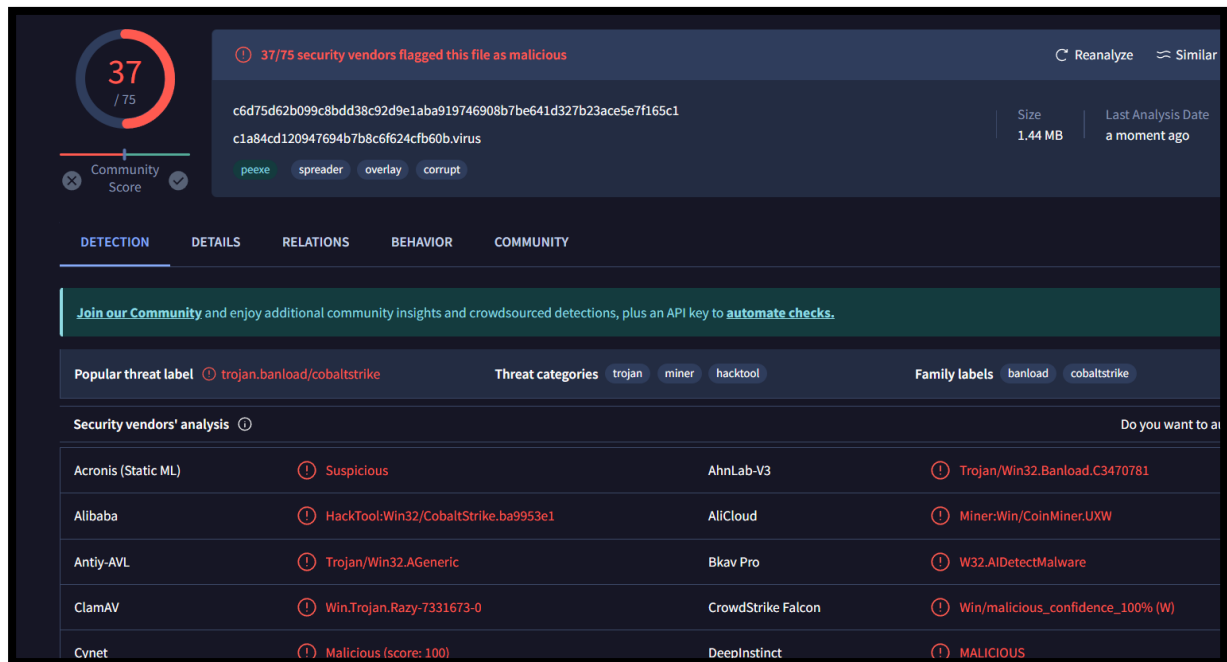
VirusShare_c1a84cd120947694b7b8c6f624cfb60b.zip ×

You are trying to upload a file with password. If you want us to scan the file inside it add the password. We can only scan it if there is exactly one file inside the zip.

The file can be uploaded even if you do not know the password. Just leave the field empty.



Confirm upload



Step 6: FIND THE SUITABLE REMEDIATION.

- 1. Disconnect from the Internet:** Disconnect your computer from the internet to prevent the virus from spreading and to minimize further damage.
- 2. Use Antivirus Software:** Run a full system scan using reputable antivirus software. Make sure your antivirus definitions are up to date before initiating the scan.
- 3. Quarantine Infected Files:** If your antivirus software identifies infected files, quarantine or delete them as per the recommendations of the antivirus program.
- 4. Update Your Operating System:** Ensure that your operating system is up to date with the latest security patches and updates. This helps in closing vulnerabilities that malware may exploit.
- 5. Enable Firewall:** Make sure your computer's firewall is enabled to prevent unauthorized access.
- 6. Change Passwords:** Change passwords for your important accounts, especially if you suspect that sensitive information may have been compromised.
- 7. Restore from Backup:** If you have a recent and clean backup of your files, restore your system to that backup. This can help eliminate the virus from your system.