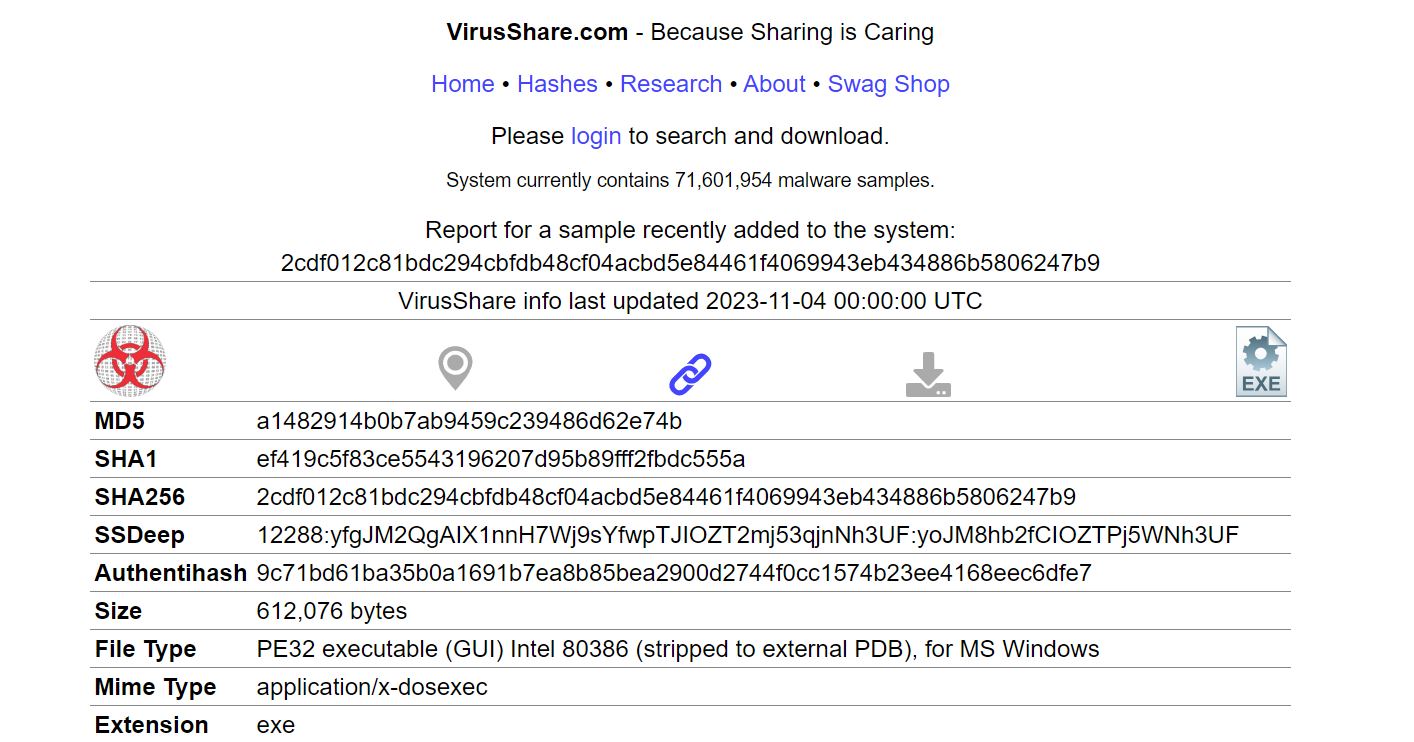
**Practical – 9**

**Aim: To do Detect and Analyse Malware**

**Steps:**

Open the website [www.virusshare.com](http://www.virusshare.com/)  to download the clean sample of Malware.

Create account by sending a mail to Melissa at [melissa97@virusshare.com](mailto:melissa97@virusshare.com) with 'access' in the subject. She will review your request and hopefully send you an invitation link.

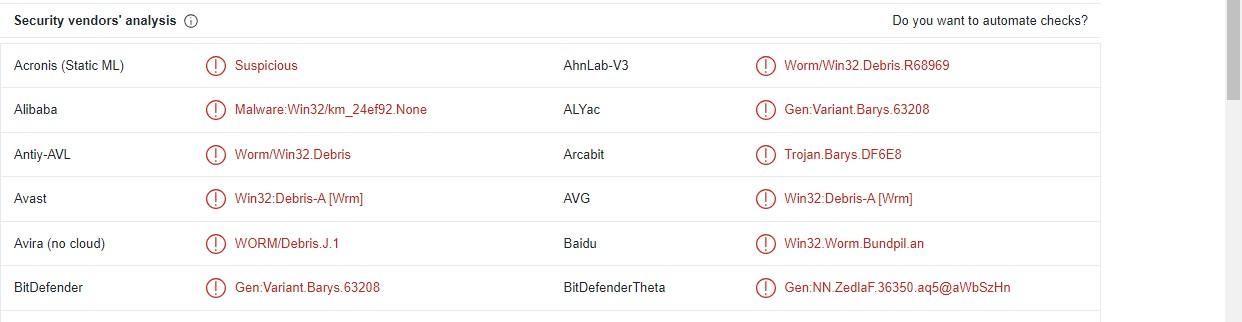
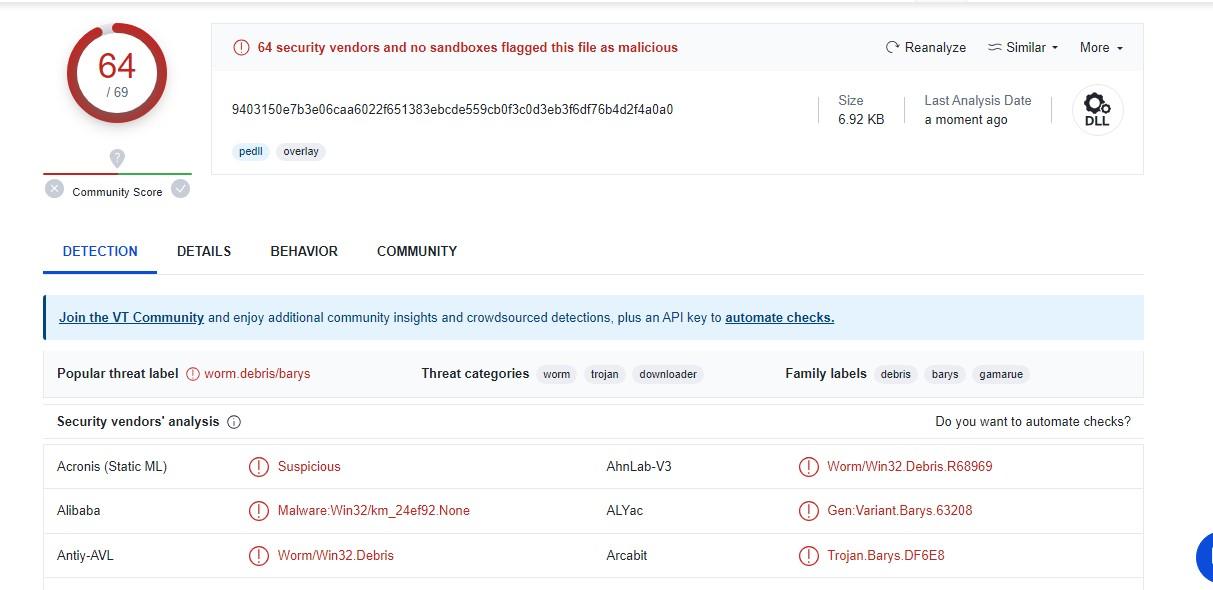


By clicking the above download icon the Malware gets downloaded in ZIP format. 

Do not unzip the file, we create a folder “Malware” on desktop and save the file in the folder. In order to analyse the Malware, we select the website [www.virustotal.com](http://www.virustotal.com/)



Click on “Choose File” and select the file from the location (ZIP file will do, if asks for

password enter infected). We get the following after the upload is complete

We interpret the following findings

* + 1. 64 security vendors out of 69 flagged this file as malicious
    2. The detection tab shows the threats-type which were flagged by the vendors for e.g
    3. The details tab gives the following information
       1. Basic properties
       2. History
       3. Compiler products
       4. Header
       5. Sections
       6. Imports
       7. Exports
       8. Overlays
    4. The Behavior tab gives the following information
       1. Activity summary
       2. MITRE ATT&CK Tactics and Techniques
       3. Behavior Similarity Hashes
       4. Process and service actions