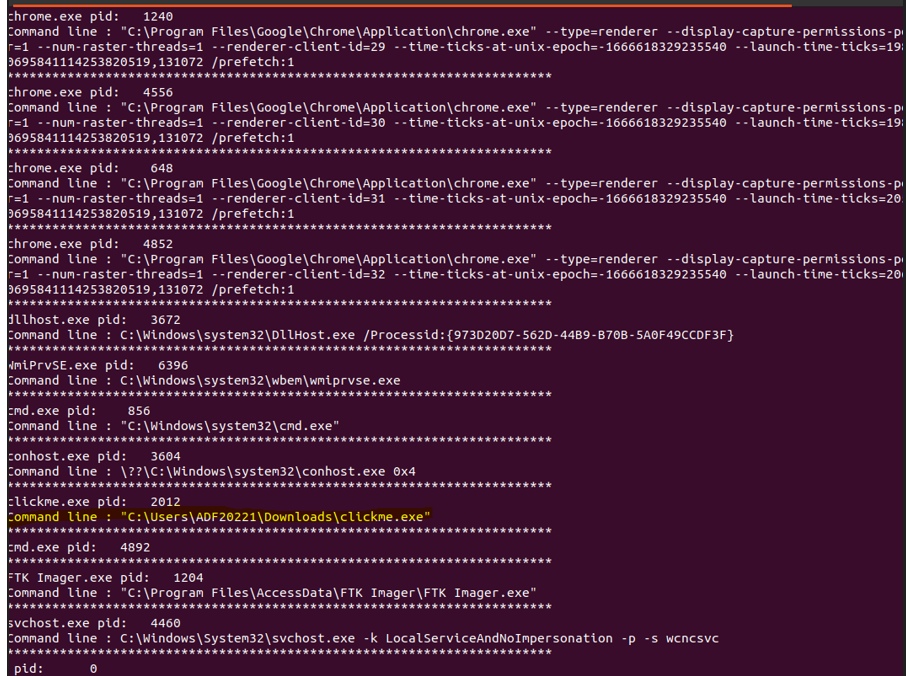
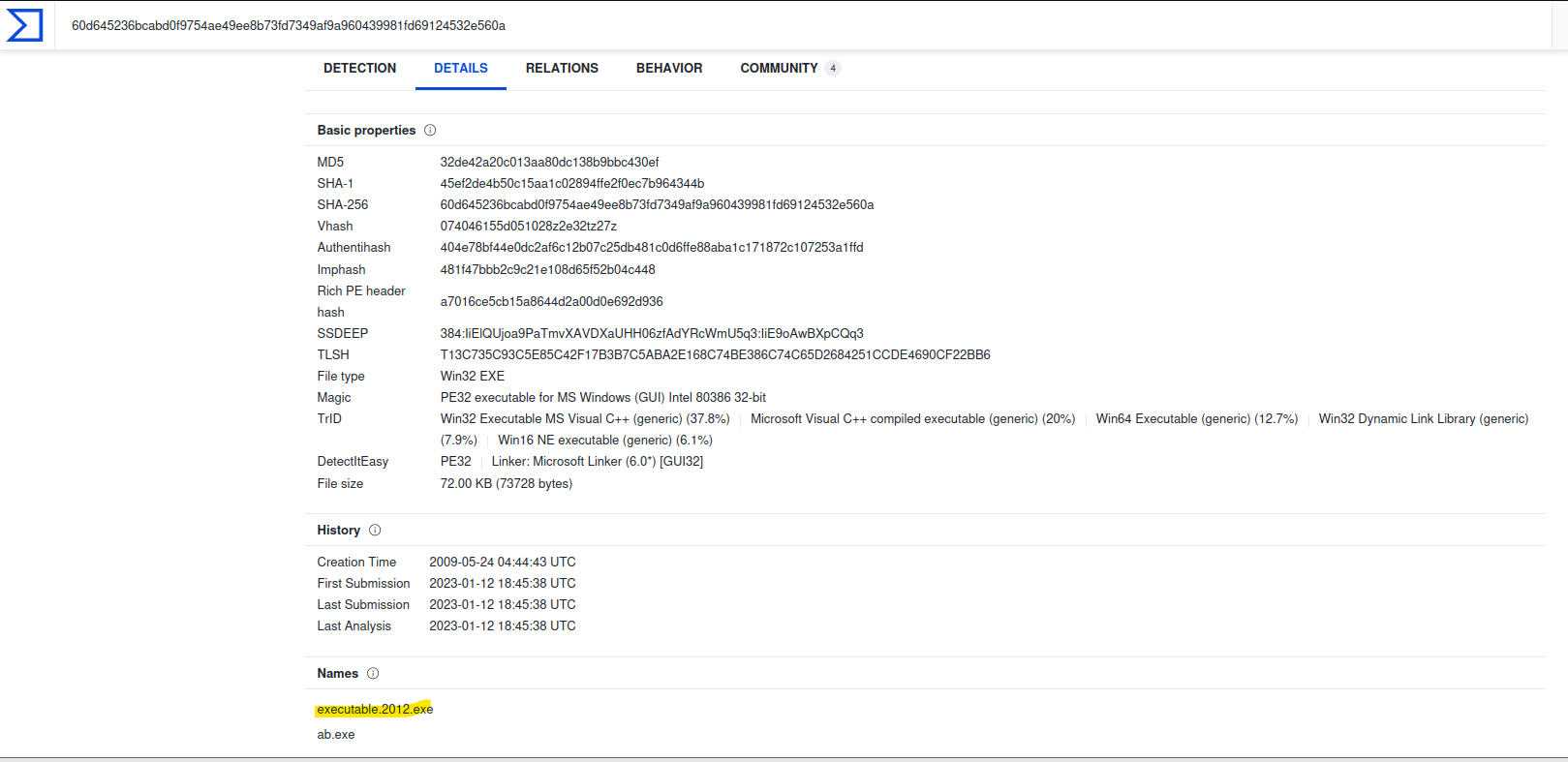
**Memory Analysis**

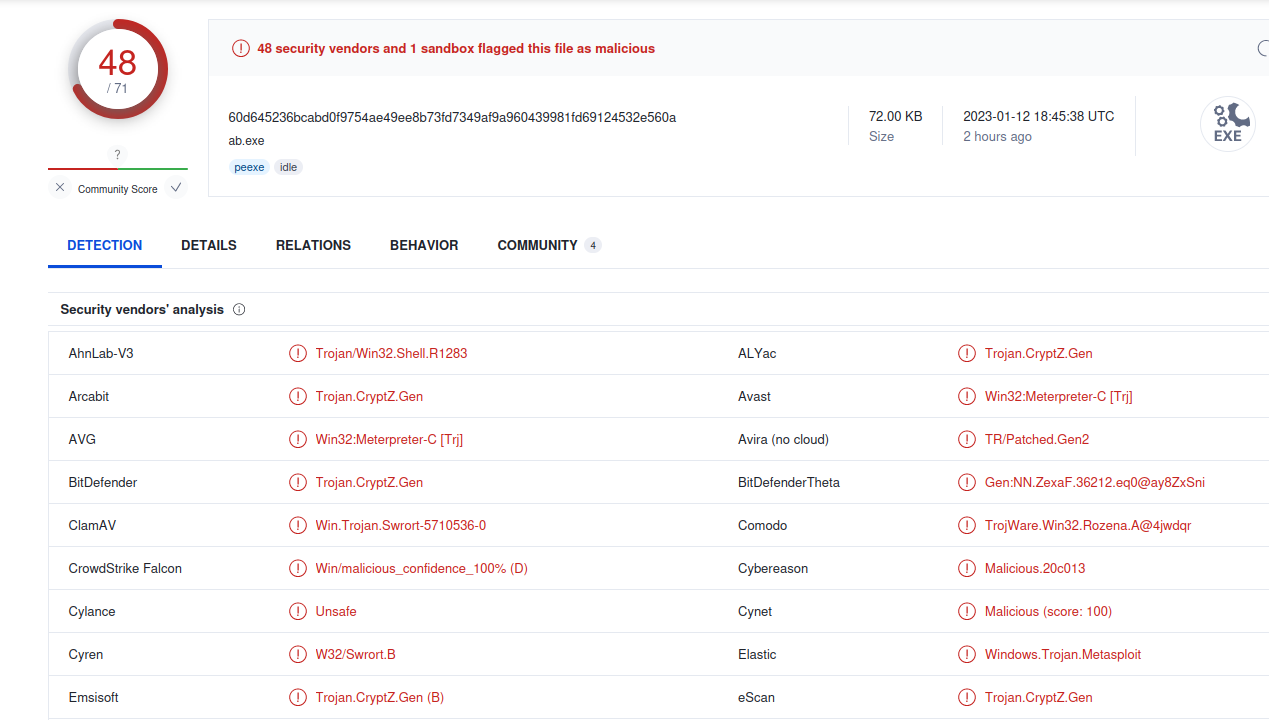
With the analysis of volatility tools, I find a malicious executing file which is named “clickme.exe” on “C:\Users\ADF20221\Downloads\” location. And the file process ID or PID is 2012.



We can see here that the file was executed by the ADF20221 user. We dump the file from the memory file on my local PC by the volatility tools. The file is downloaded with “executable.2012.exe” name. We can see here the PID 2012 is added.

And I make scans by virustotal online tools.

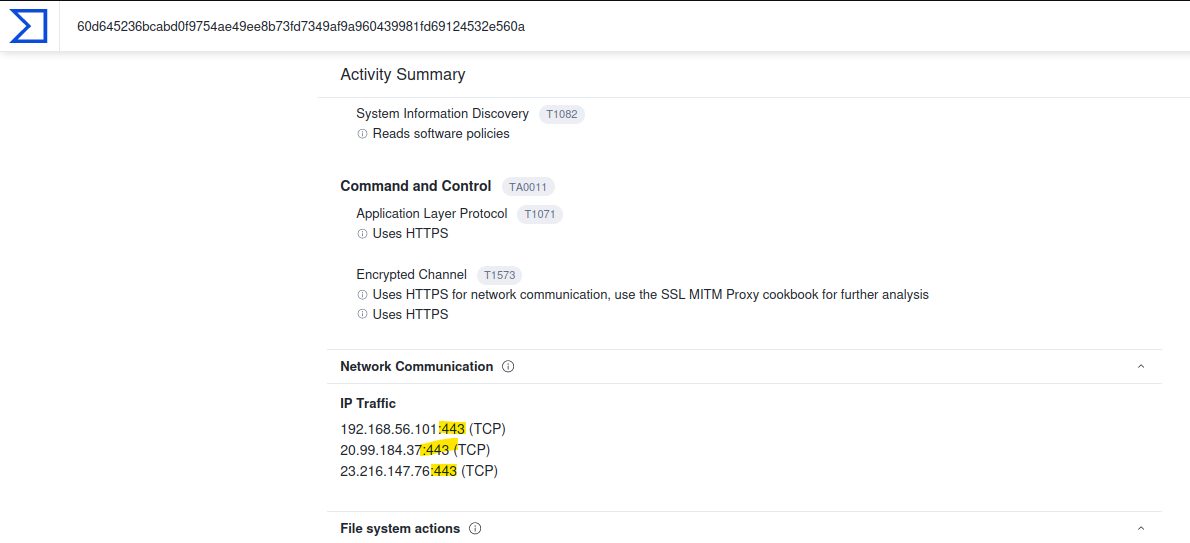




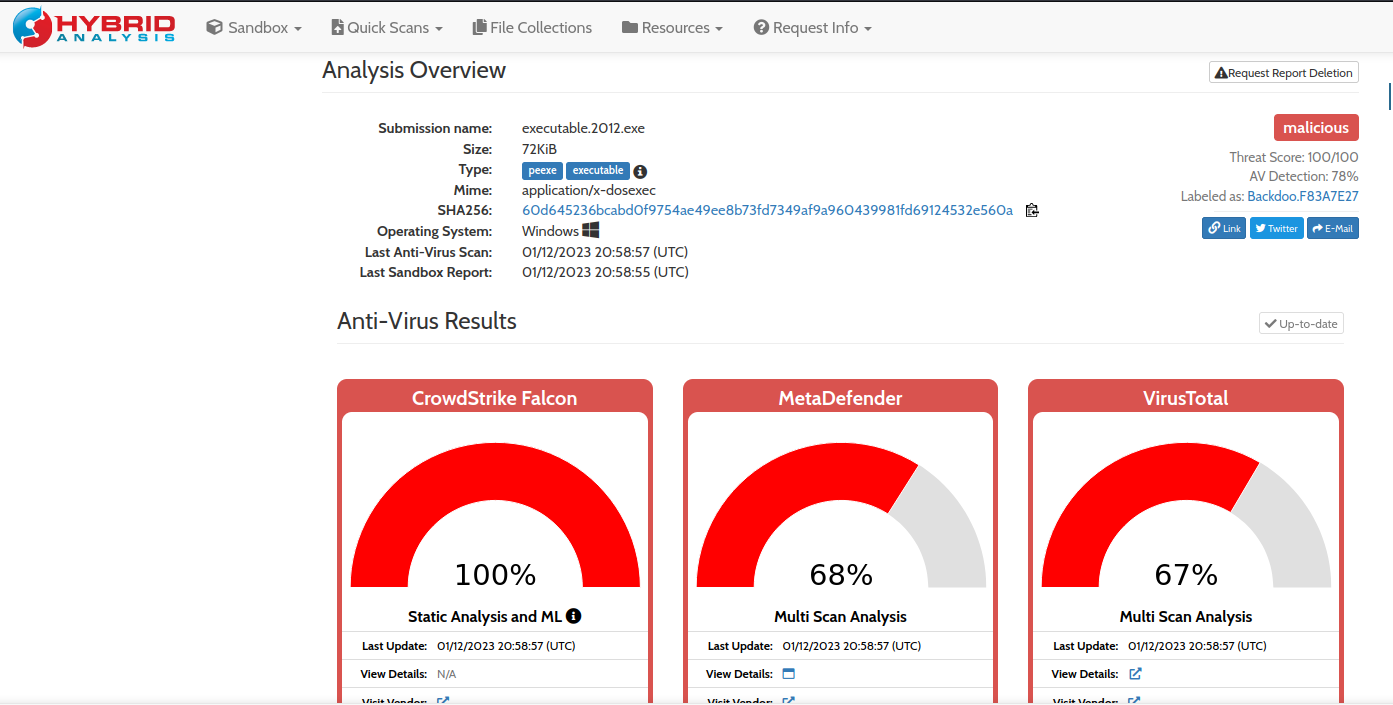


So, Now we know that the clickme.exe or PID 2012 is a malicious file and it is a trojan.

By checking the behavior section of virustotal of this trojan, I noticed that the attacker attacked by the 443 port or HTTPS.

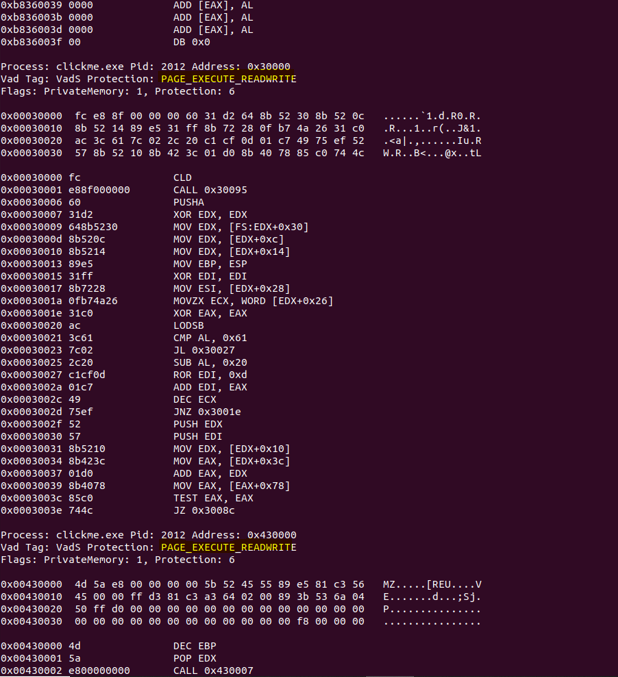


I also scan the file with Hybrid-analysis online tools. Where the file also scans as malicious. And the name of this malware is “Trojan.Swrort” or “Trojan Win32”. And this is a backdoor trojan. Which makes a remote connection to the attacker.

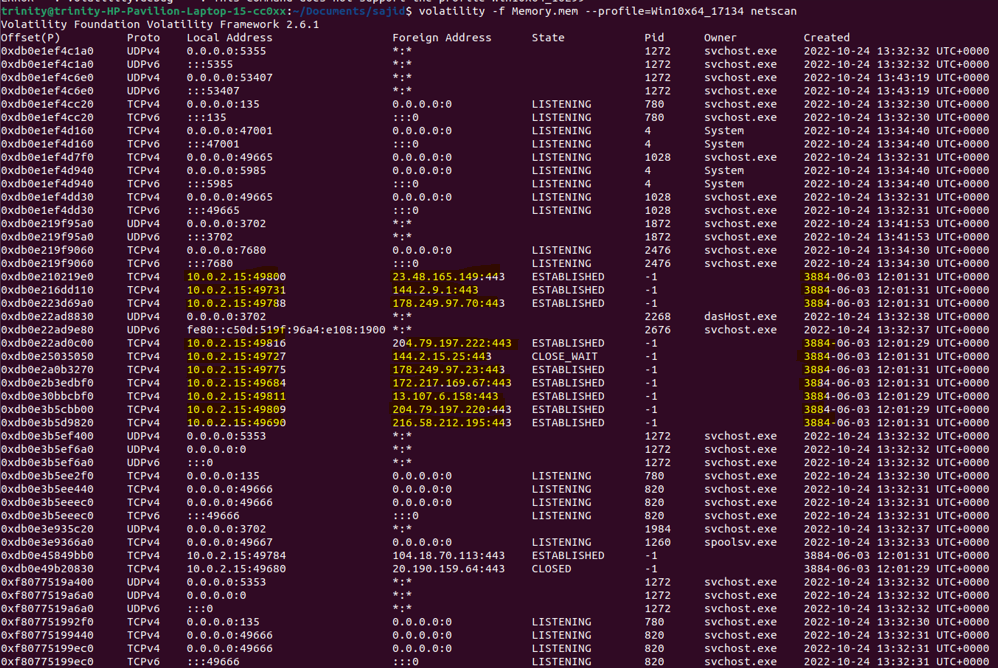




After checking the scripts of clickme.exe file by volatility, I can see that the file has read and write permission.



And I also find that a malicious connection was established which was happening for the execution of the trojan.



Here I can also notice that the foreign IP establishes a connection with the local machine.

So the attacker attacked the victim's machine with “clickme.exe” or PID 2012 and which is a trojan.

We know that Trojan.Swrort or Trojan Win32 is a very harmful Trojan. For stopping this trojan, there have a lot of ways. Such as:

* Go to PowerShell and kill Process 2012.
* Remove the clickme.exe from the registry.
* Install Malwarebytes for permanent protection from Trojans.