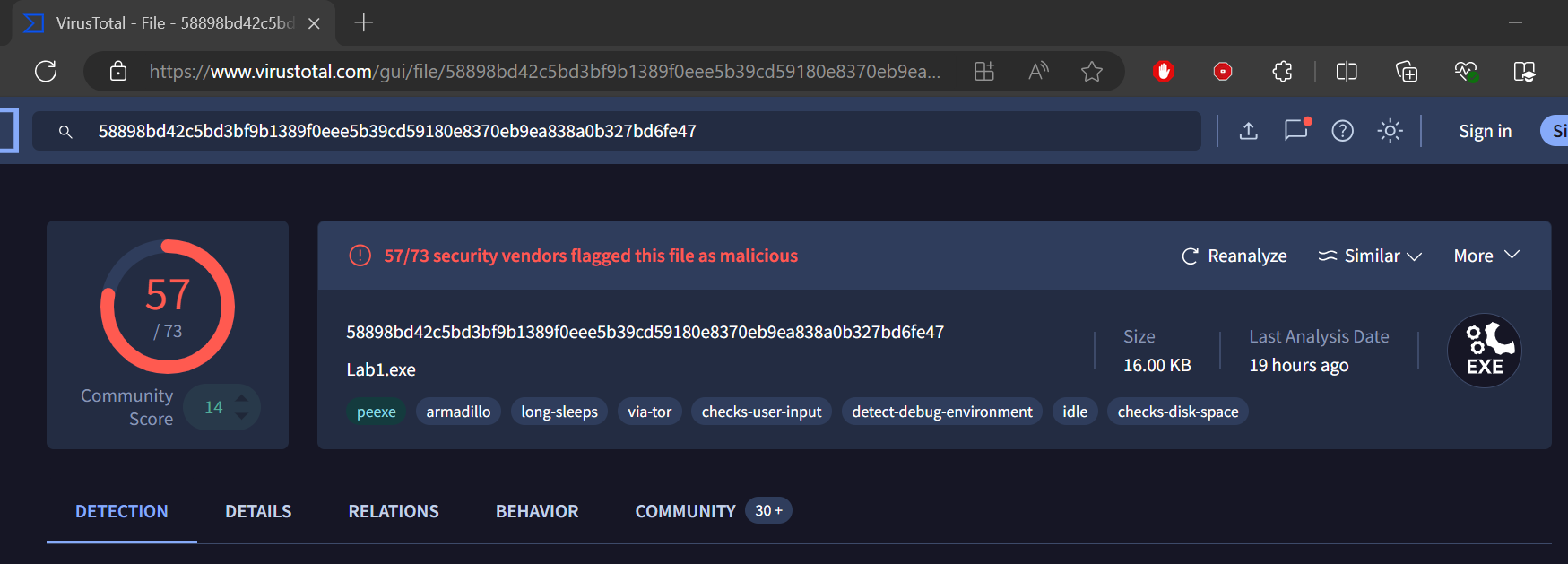
**150182 Kipruto Isaac**

**Practical Malware Analysis - Chapter 1 Lab**

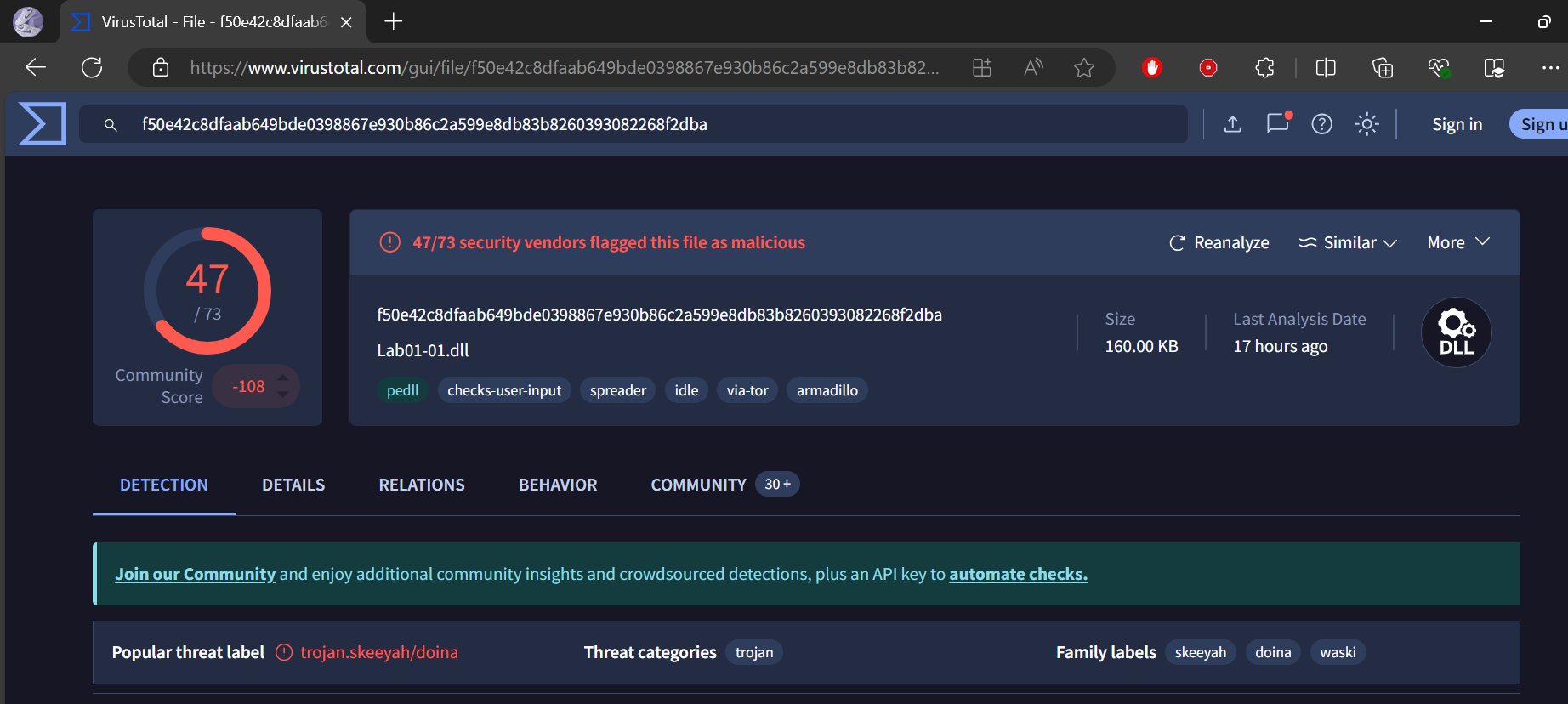
**Question 1**

Upload the files to http://www.VirusTotal.com/ and view the reports. Does file match any existing antivirus signatures?

Lab01-01.exe



Lab01-01.dll



**Question 2**

When were these files compiled?

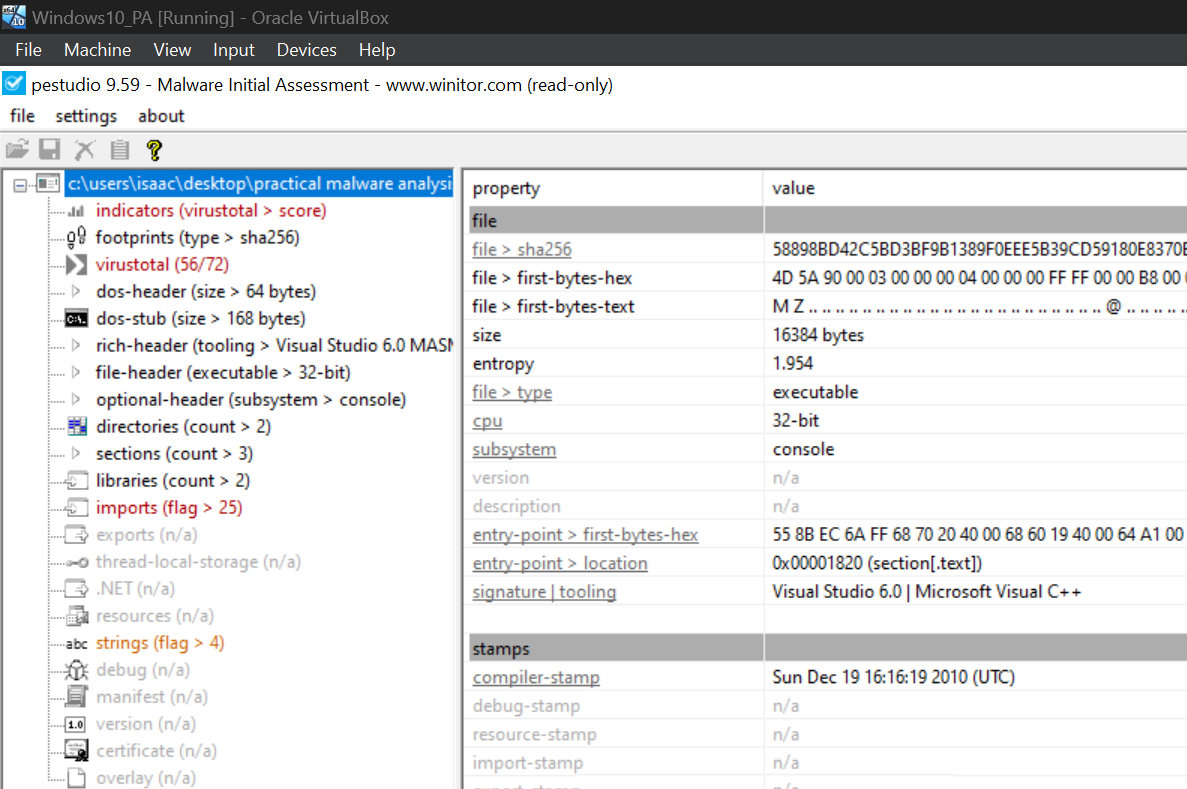
Lab01-01.dll

**A screenshot of a computer

Description automatically generated**



**Lab01-01.exe**





**Question 3**

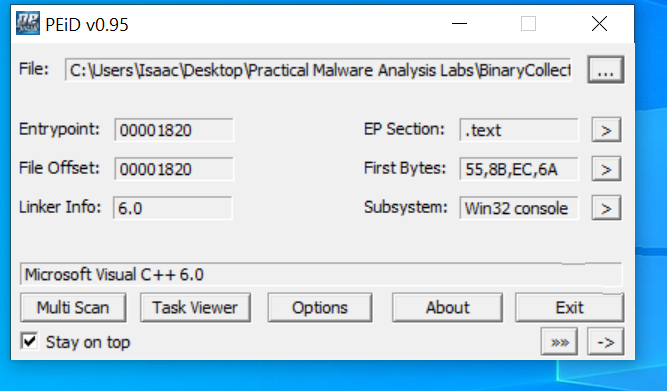
Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?

No, there’s no indicators these files are packed or obfuscated

**Lab01-01.dll**

****

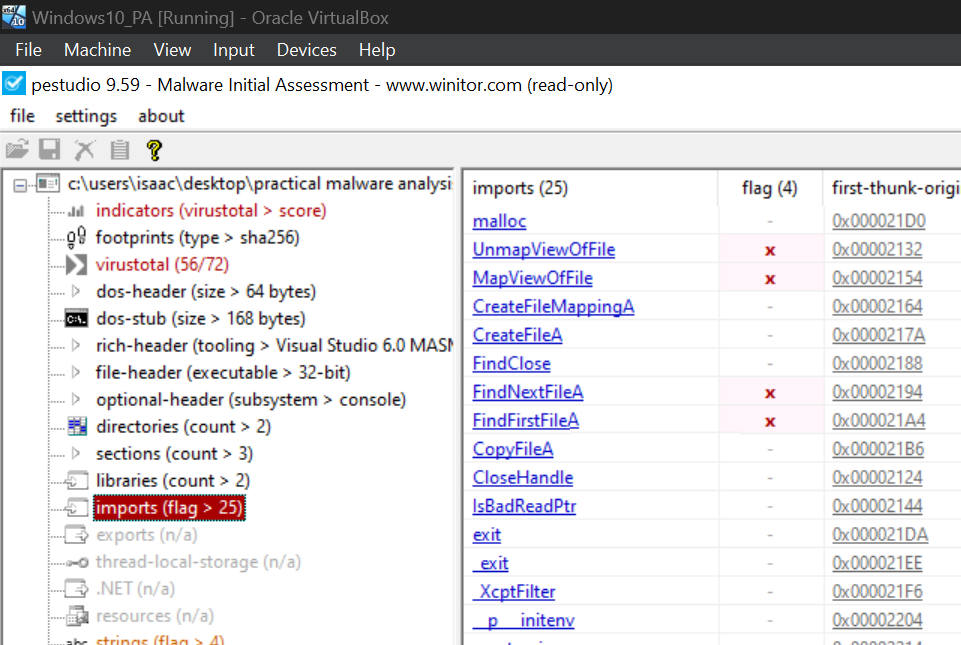
**Lab01-01.exe**

****

**Question 4**

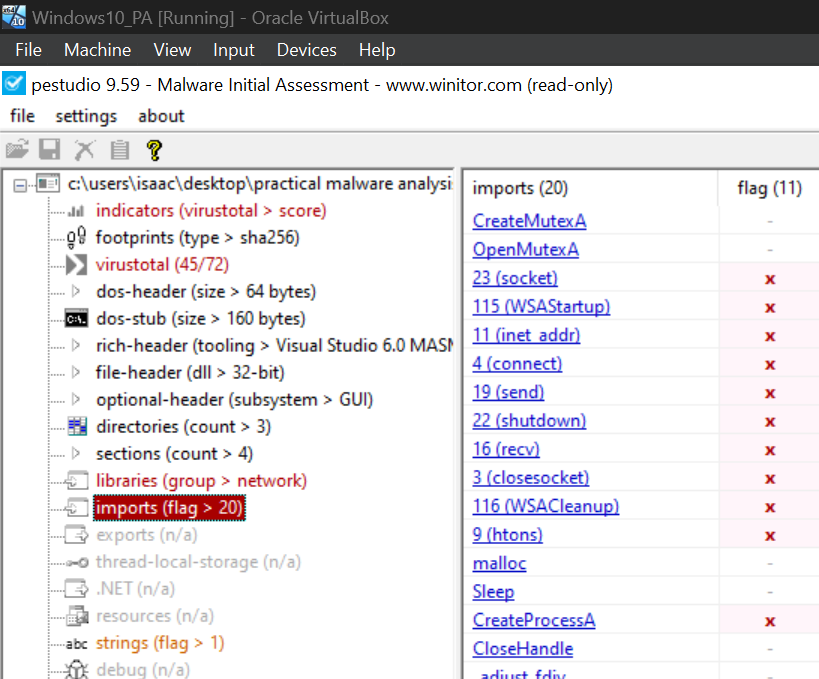
Do any imports hint at what this malware does? If so, which imports are they?

**Lab01-01.exe**

Based on this we can infer that the dll would likely spawn a new process and sleep (pause execution) at some stage. 

**Lab01-01.dll**

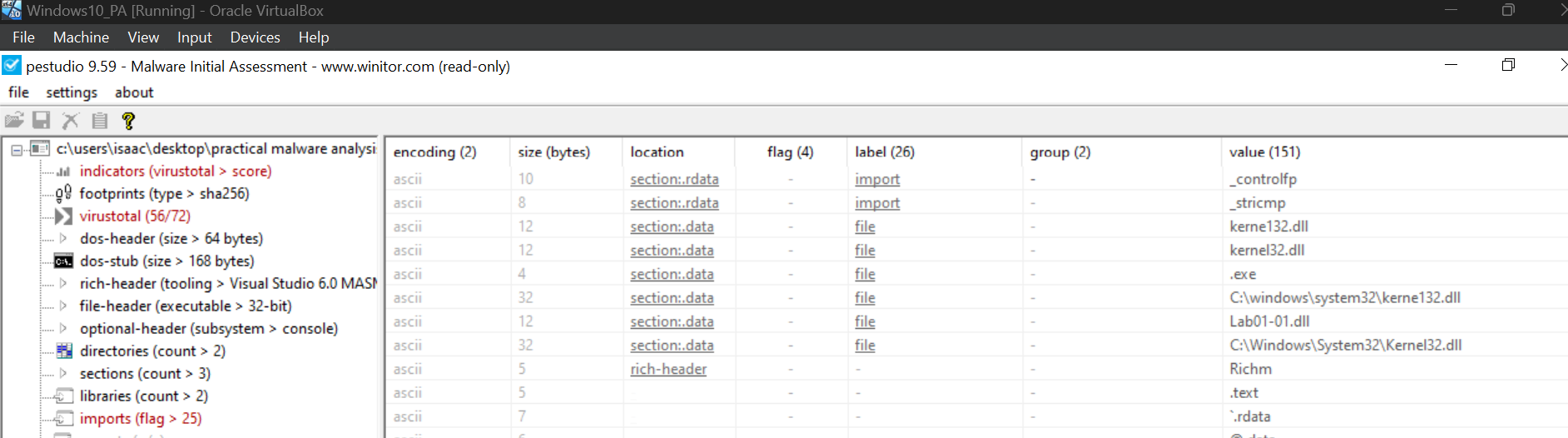
Based on this we can infer that the program has connects to a network or IP of some kind and opens a socket to send and receive packets.



**Question 5**

Are there any other files or host-based indicators that you could look for on infected systems?

Examining the strings contained within Lab01-01.exe more closely reveals that it is referencing a file called C:\windows\system32\kerne132.dll.

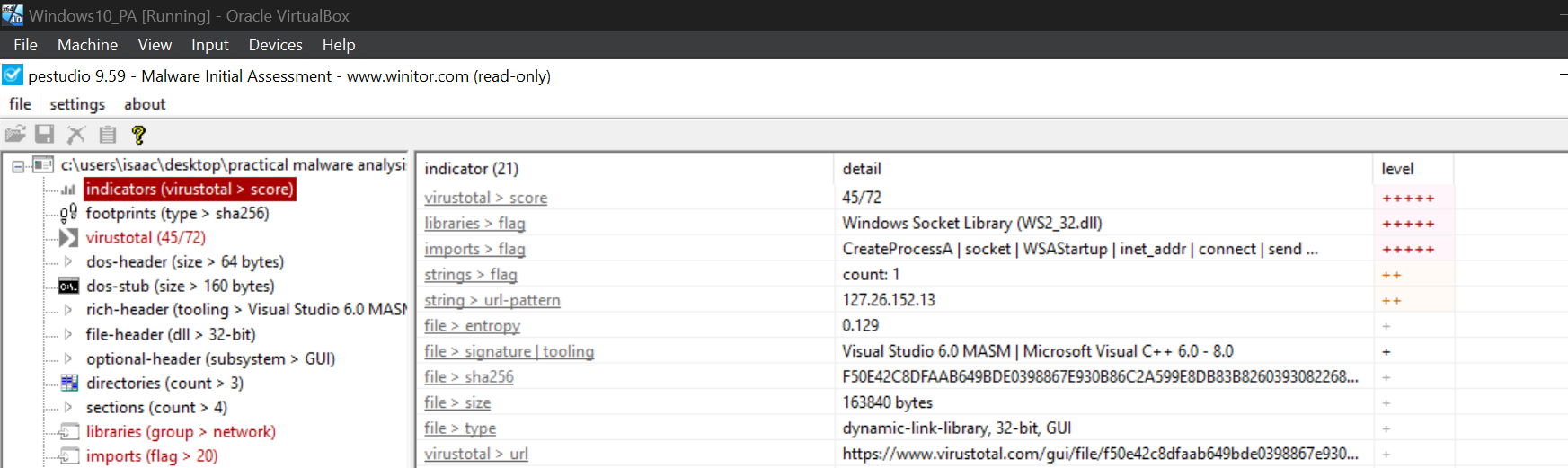




**Question 6**

What network-based indicators could be used to find this malware on infected machines?

Examining the strings contained within Lab01-01.dll more closely reveals that there is what appears to be an IP address. Because of this and the network imports, it is highly likely that this DLL contacts this IP address, and as such we are able to use this to find infected systems which have contacted 127.26.152.13.





**Question 7**

What would you guess is the purpose of these files?

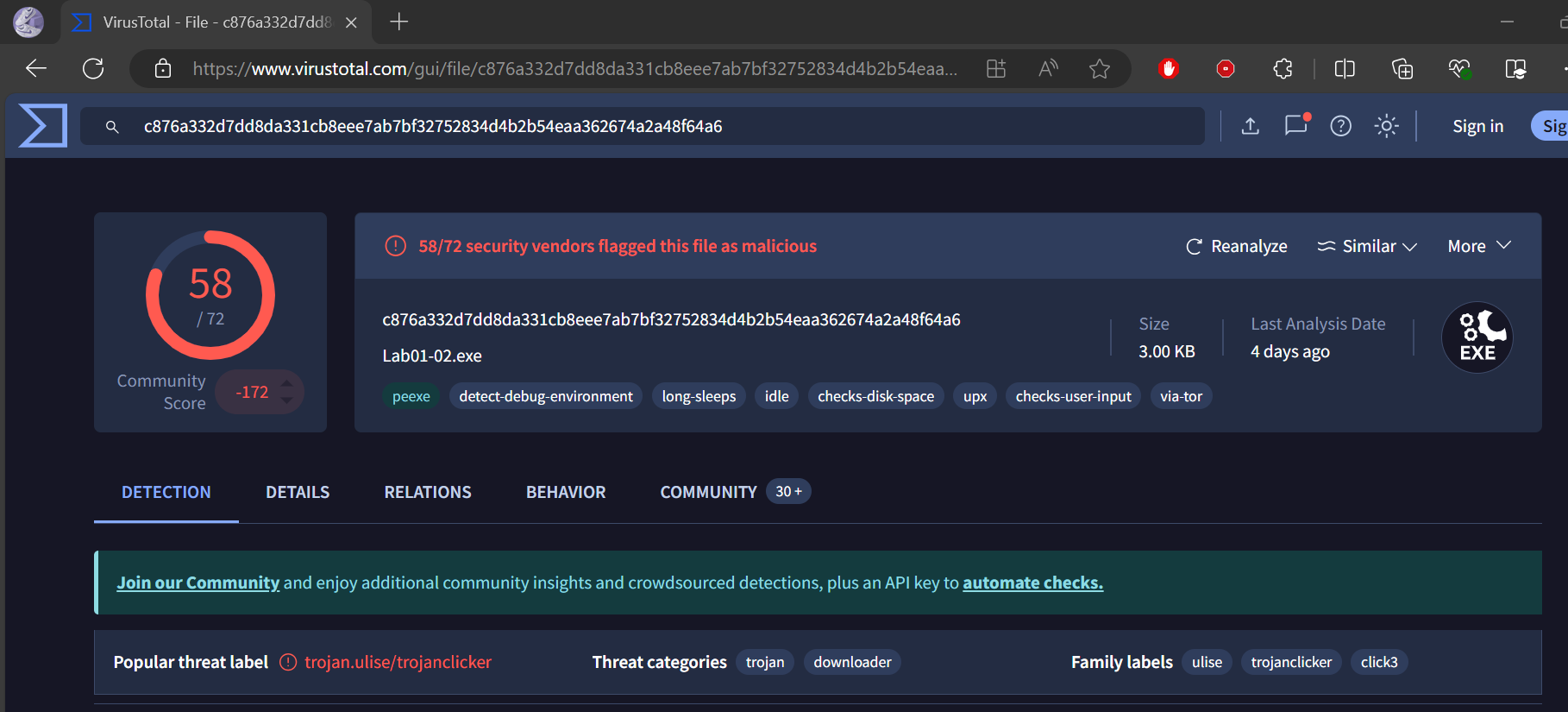
Based on everything we’ve enumerated above, we would guess that the executable is used to run the DLL which acts as a backdoor or remote access trojan (RAT). Based on the imports it’s possible the executable searches to see if C:\windows\system32\kerne132.dll exists, and if it doesn’t it may attempt to copy the malicious DLL to C:\windows\system32\kerne132.dll which is used for persistence. Upon executing the DLL, it likely contacts a C2 server at 127.26.152.13.

**Lab 1-2**

This lab uses the file Lab01-02.exe. Analyse the file Lab01-02.exe.

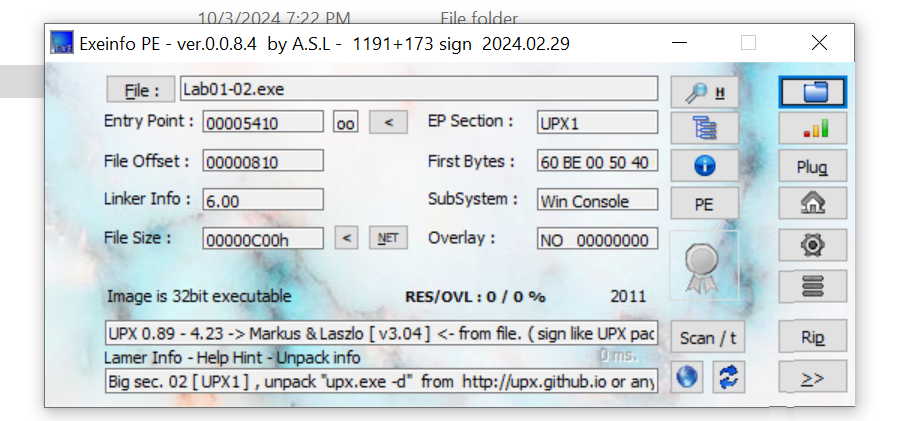
**Question 1**

Upload the Lab01-02.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?



**Question 2**

Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible. Diving in with a different tool called Exeinfo PE

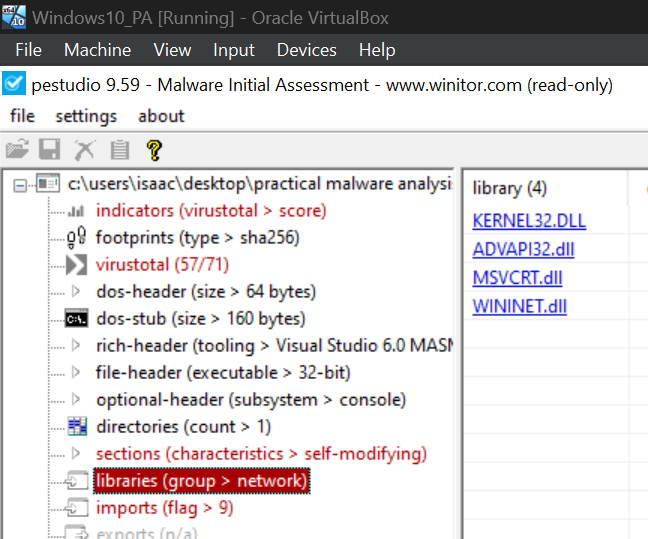


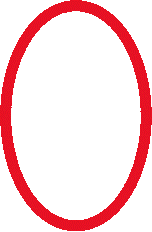


**Question 3**

Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?

Analysing Lab01-02.exe through Dependency Walker highlighted the below interesting functions:





**Question 4**

What host- or network-based indicators could be used to identify this malware on infected machines?

A screenshot of a computer

Description automatically generated

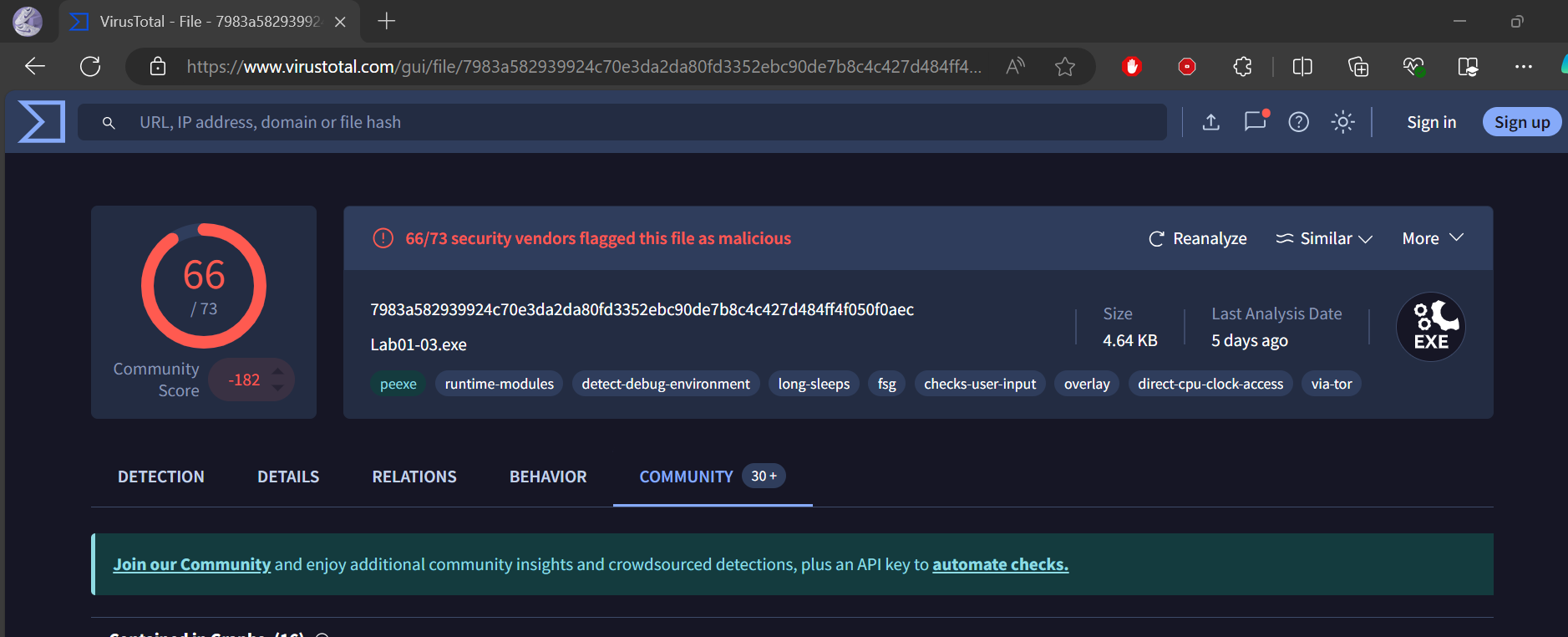


**Lab 1-3**

This lab uses the file Lab01-03.exe. Analyze the file Lab01-03.exe.

**Question 1**

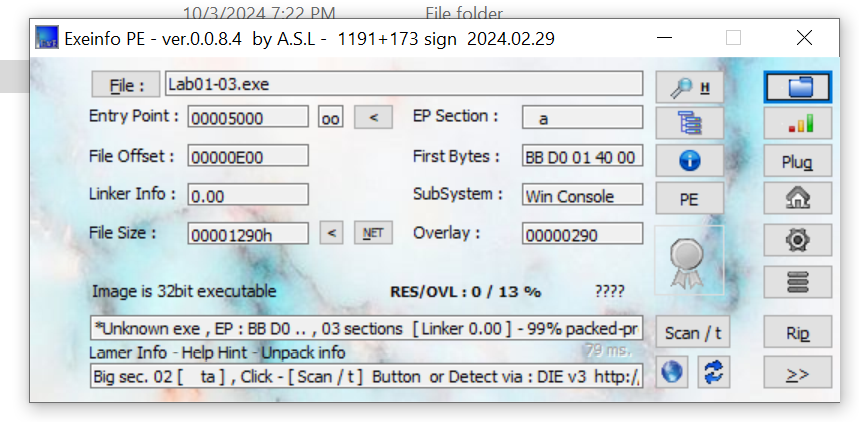
Upload the Lab01-03.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?



**Question 2**

Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

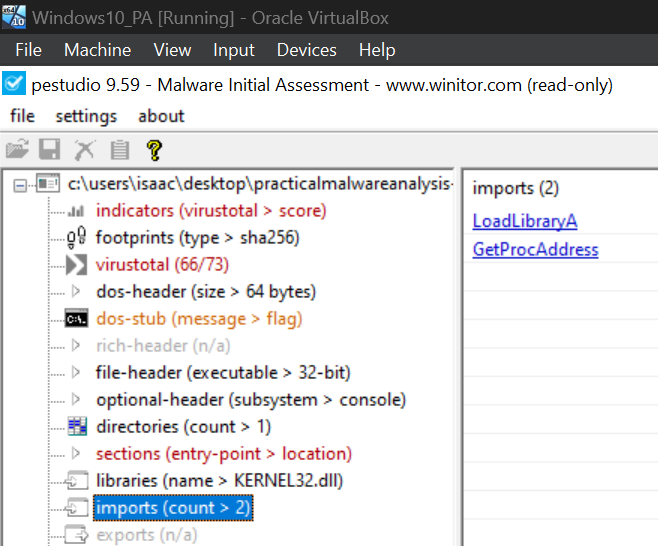
PE Detective revealed that this file was packed this time using FSG.

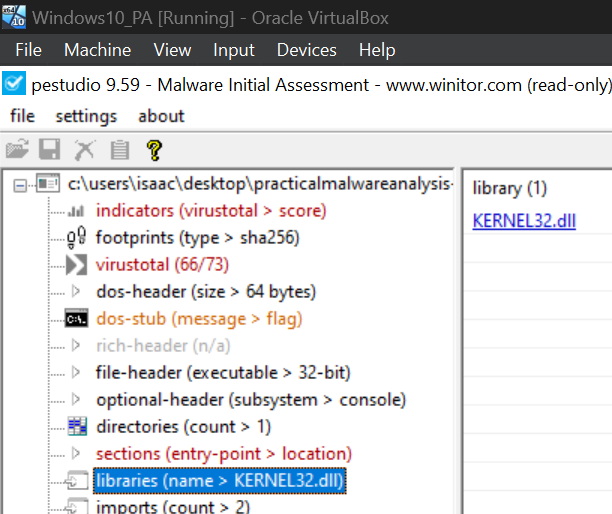


**Question 3**

Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?

At present the file is packed with FSG, and we are unable to unpack this with the techniques learnt so far.





**Question 4**

What host- or network-based indicators could be used to identify this malware on infected machines?

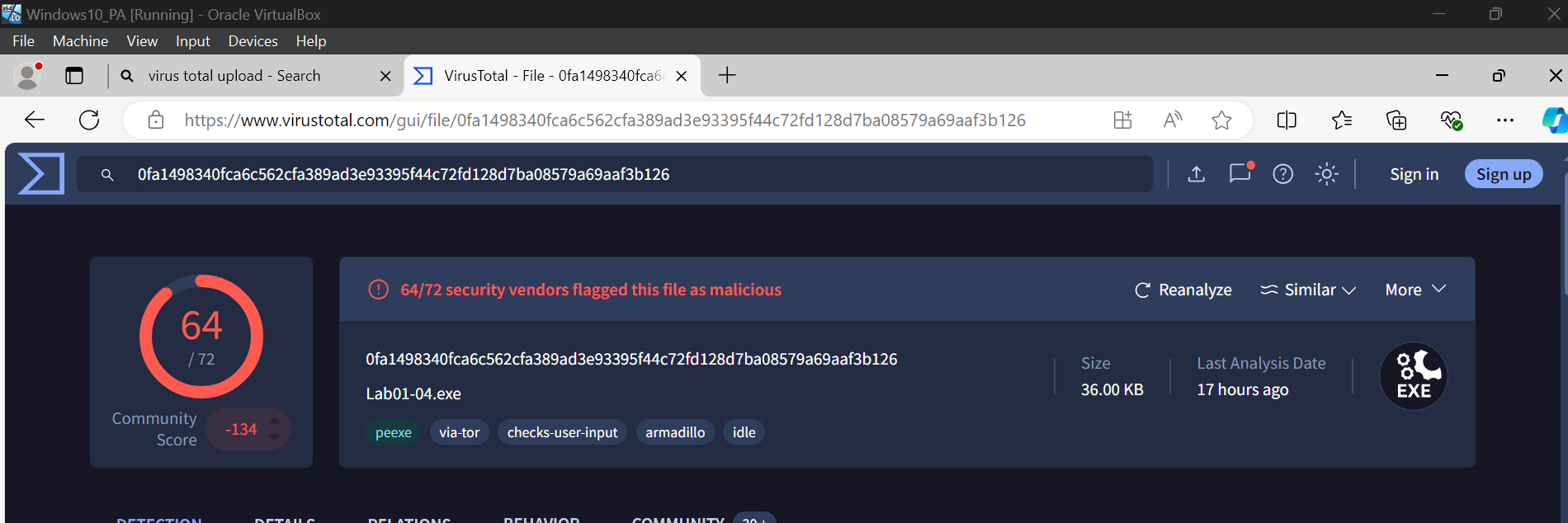
At present the file is packed with FSG, and we are unable to unpack this with the techniques learnt so far.

**Lab 1-4**

This lab uses the file Lab01-04.exe. Analyse the file Lab01-04.exe.

**Question 1**

Upload the Lab01-04.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?



**Question 2**

Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

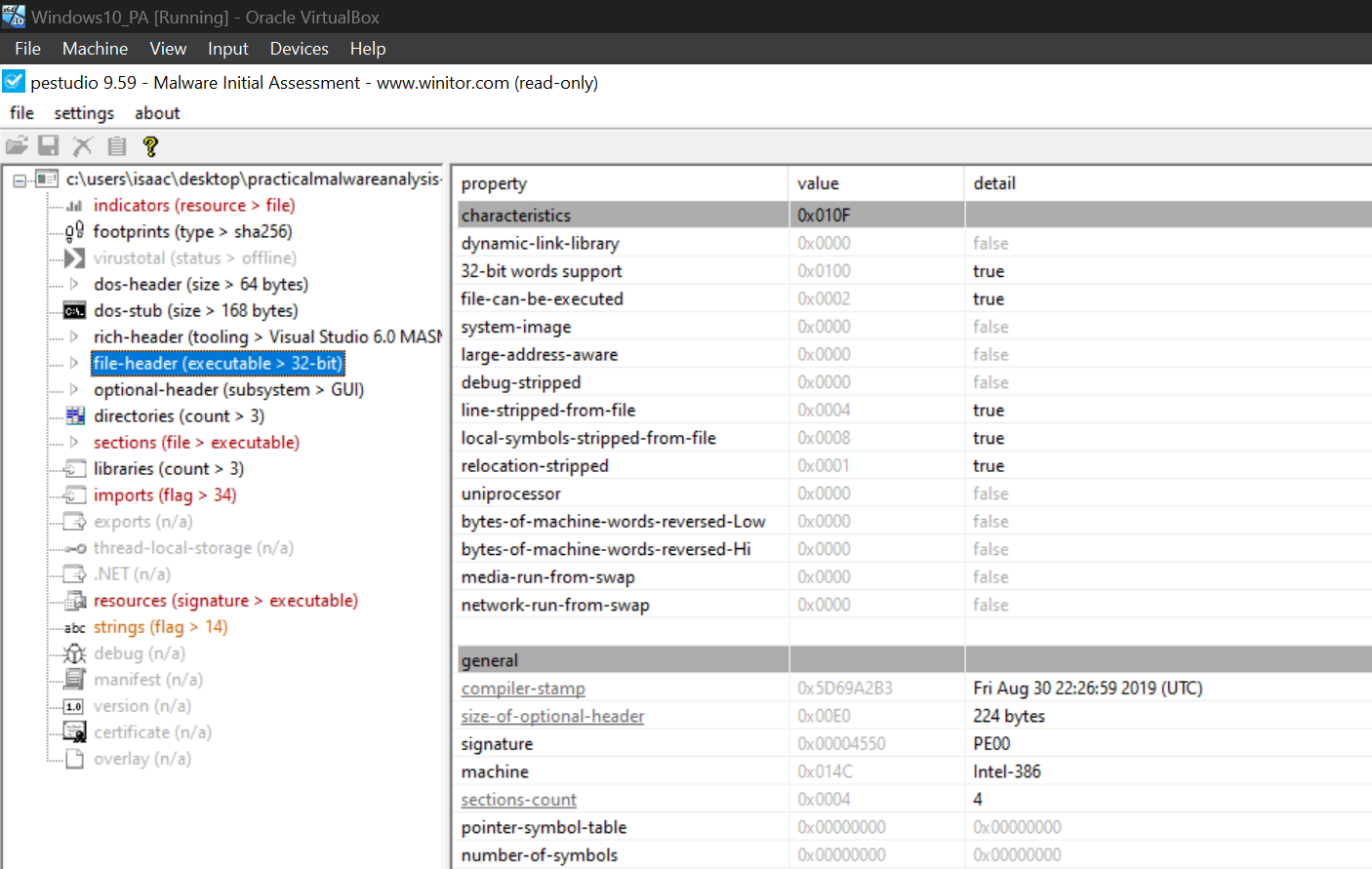
There are no indications this file is packed or obfuscated, PEiD identifies it was created with Microsoft Visual C++ 6.0, PEview shows similar virtual and raw data size, and dependency walker shows a number of imports.



**Question 3**

When was this program compiled?

we can see this program says it was compiled on the 30th of August 2019.

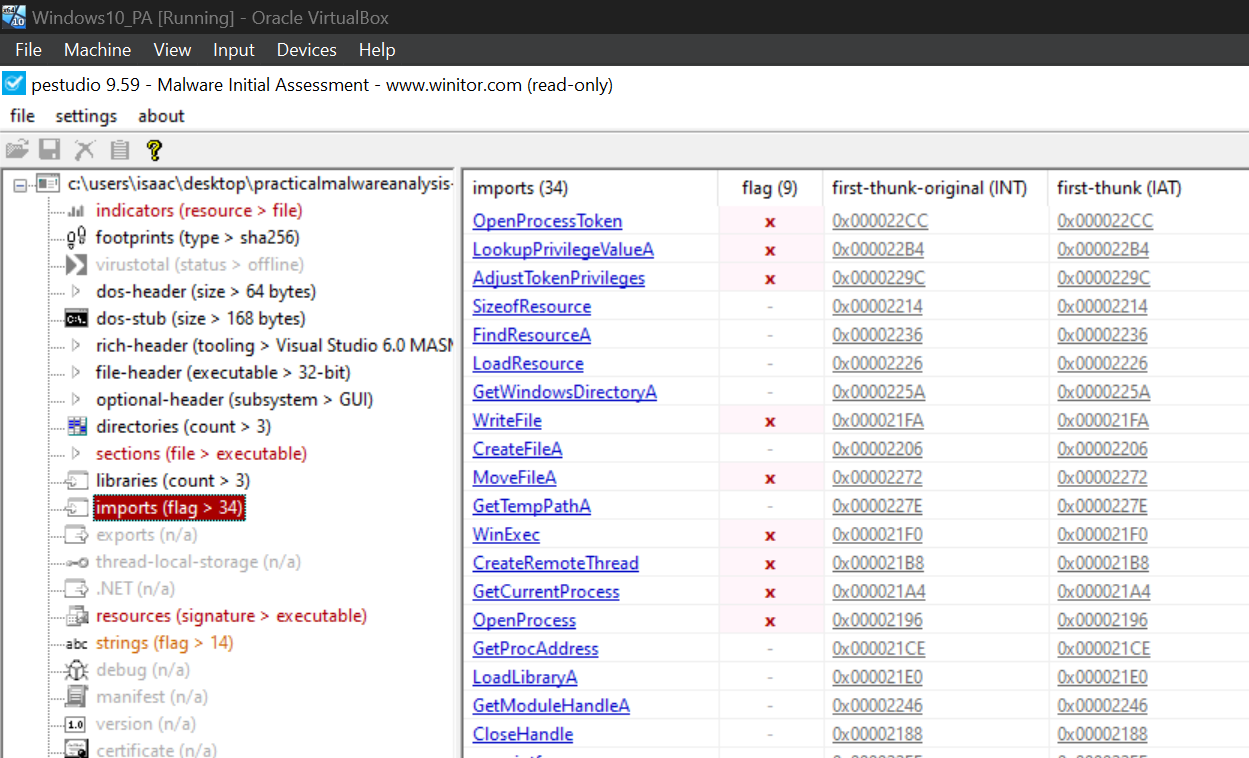


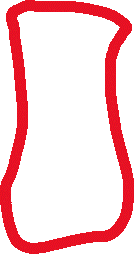


**Question 4**

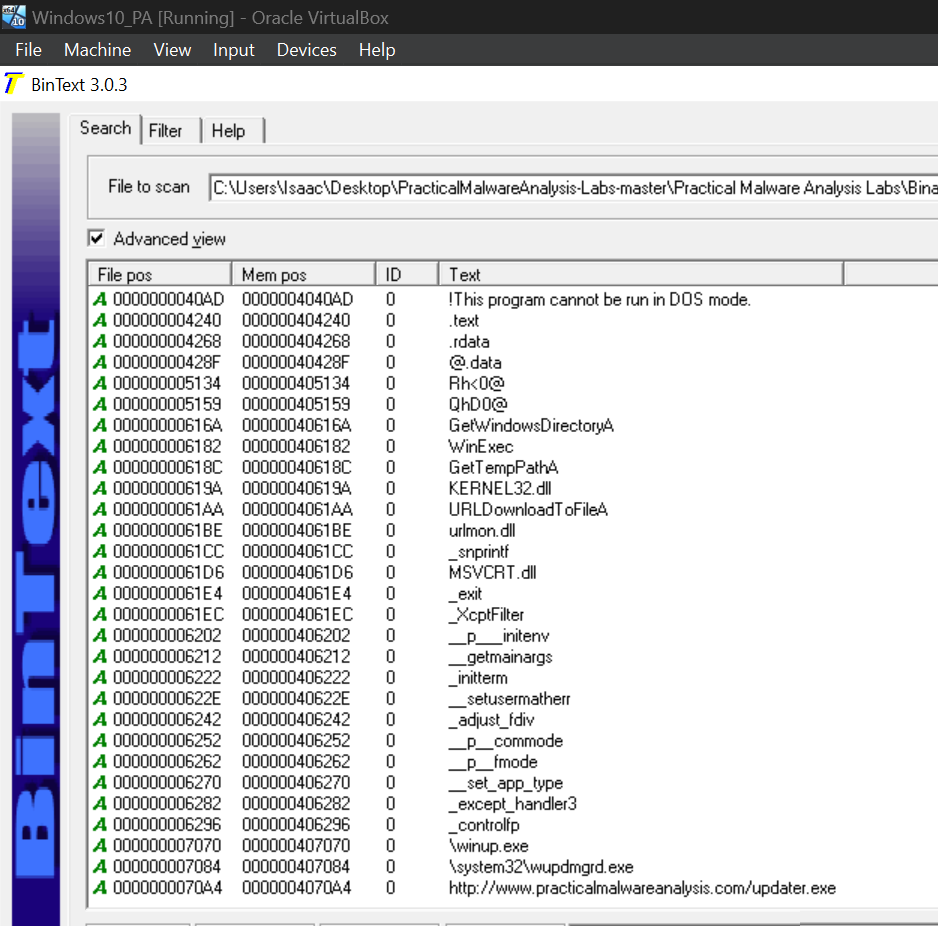
Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?

Based on the imports from Kernel32 we can see that this will load resources from the file’s resource section and write files to disk.





**Question 5**

What host-based or network-based indicators could be used to identify this malware on infected machines? 

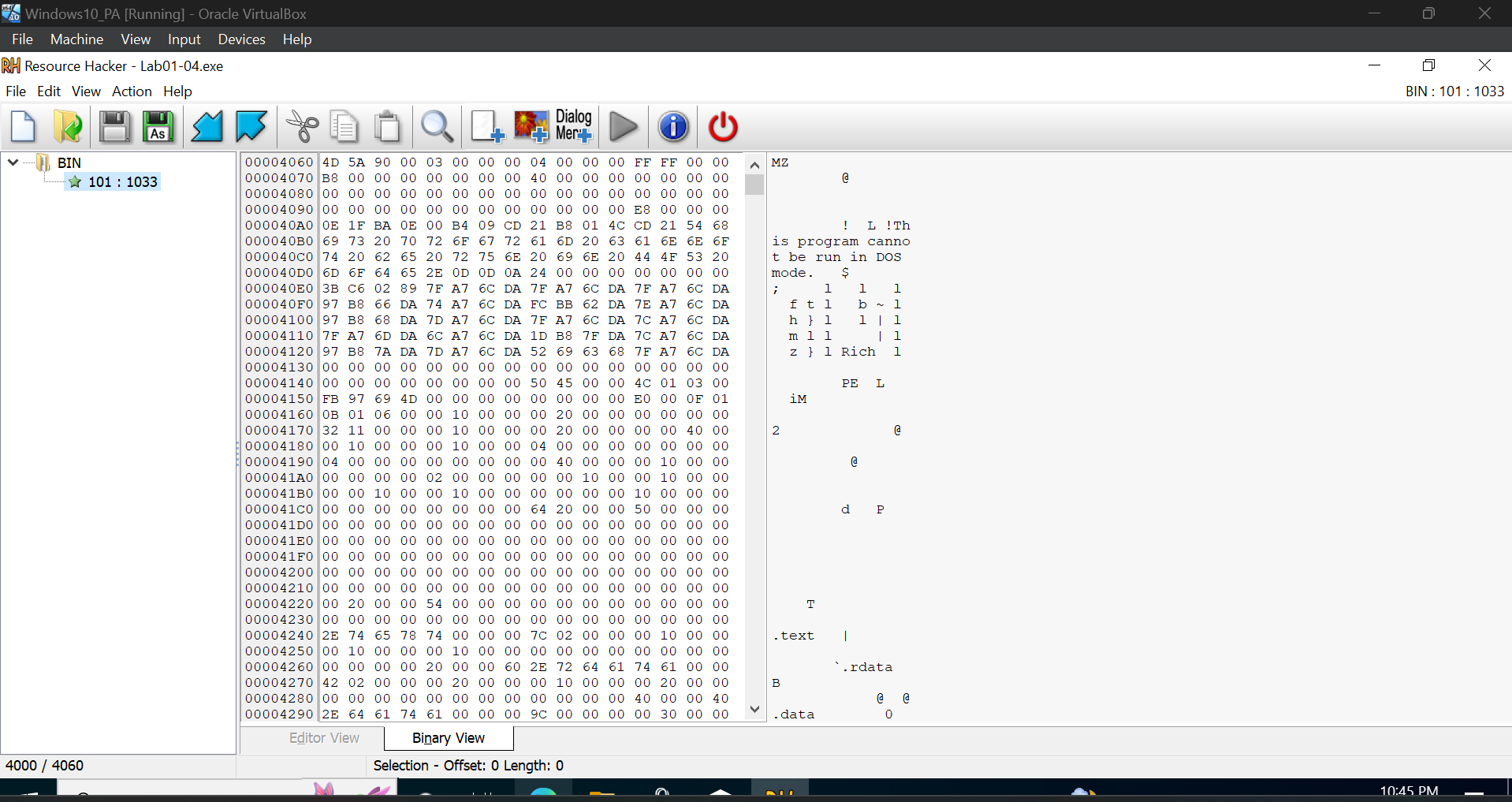


we go to BinText to view the strings, and we see a lot in there, a function called URLDownloadToFile.

**Question 6**

This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?

Looking at this resource through Resource Hacker, we can see that it has a header which indicates it is an embedded executable.



the binary file we get more information about the file, and we can see more imports and the original compile time.

