UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI

Information and Communication Technology Department

REPORT

Labwork 1

Malware Analyst

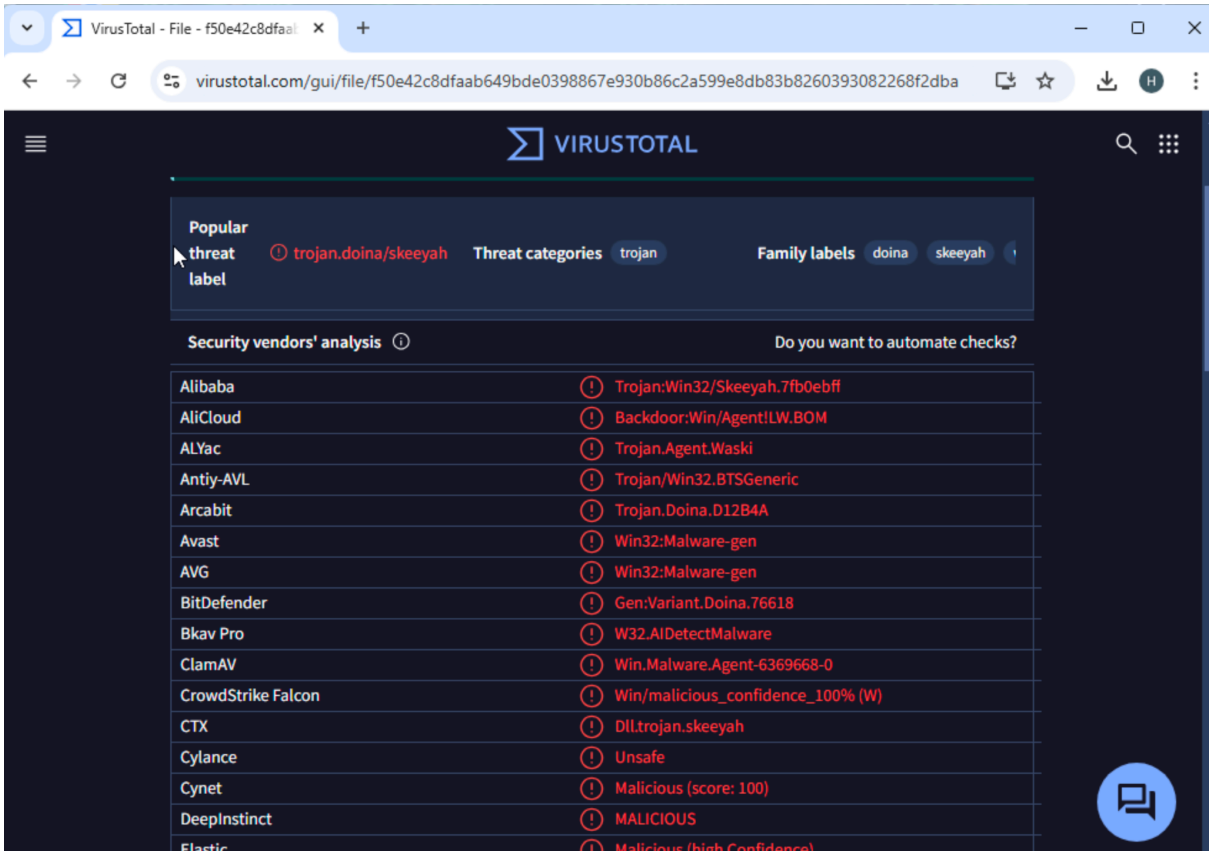
Student name : Phạm Phú Hưng

Student ID : BA12-081

Table Contents

I. LAB01-01

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



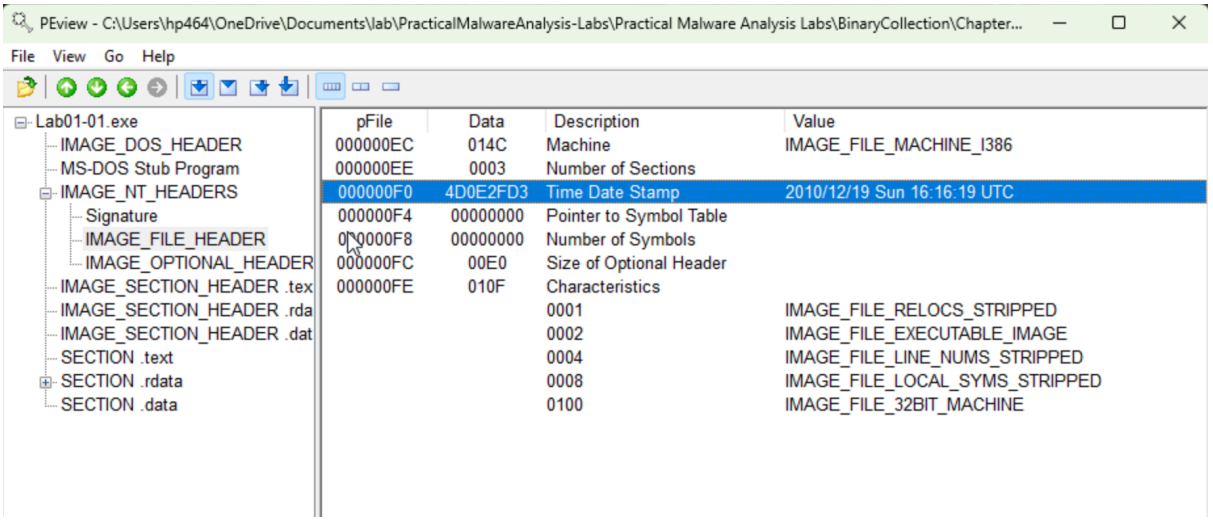
Threat Label: trojan.doina/skeyyah

Threat Categories: Trojan

Security Vendors' Analysis: Various antivirus vendors have reported this file, with many identifying it as a Trojan or similar malware. For example:

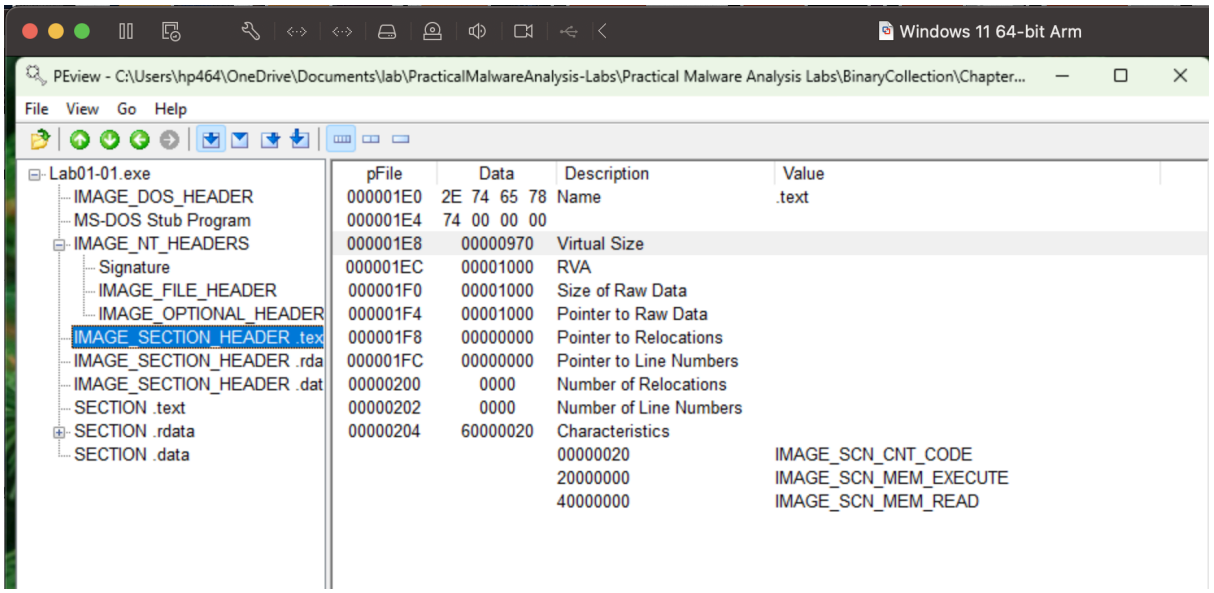
- Trojan /Skeeyah.7fb0ebf
- Backdoor /Agent!IW.BOM
- Various other detections related to malware.

B. When were these files compiled?



The **Time Date Stamp** indicates that the file was compiled on **December 19, 2010, at 16:16:19 UTC**.

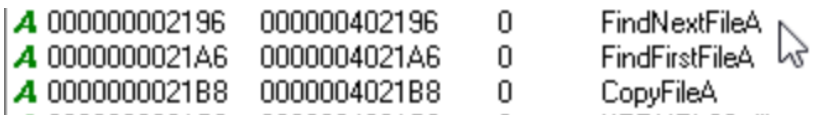
C. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?



There are no indications that either file is packed or obfuscated.

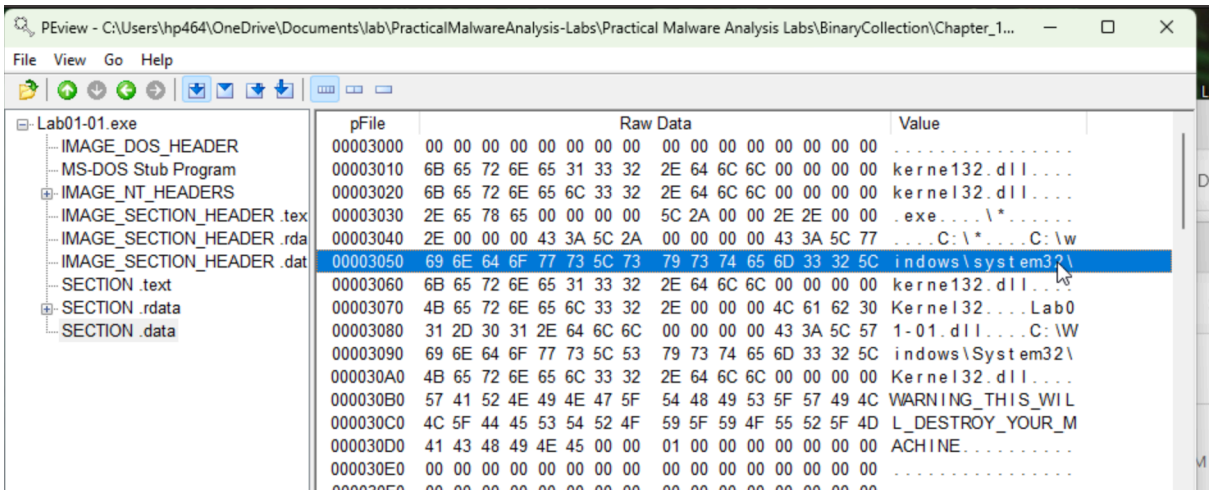
Because Virtual Size at tells us how much space is allocated for a section during the loading process. The Size of Raw Data at shows how big the section is on disk. These two values should usually be equal, because data should take up just as much space on the disk as it does in memory. Small differences are normal, and are due to differences between alignment in memory and on disk.

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



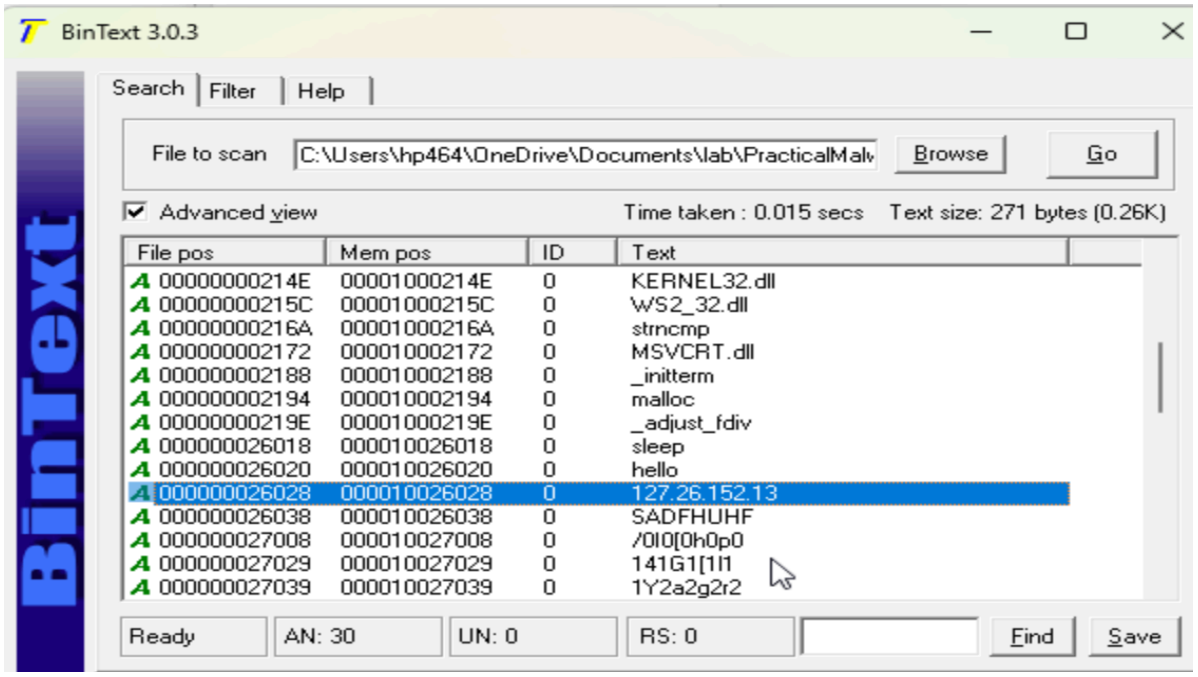
The imports from Lab01-01.exe are FindFirstFile, FindNextFile, and CopyFile

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



In this case: C:\Windows\System32\kerne132.dll for additional malicious activity. Note that the file kerne132.dll, with the number 1 instead of the letter l, is meant to look like the system file kernel32.dll. This file can be used as a host indicator to search for the malware.

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



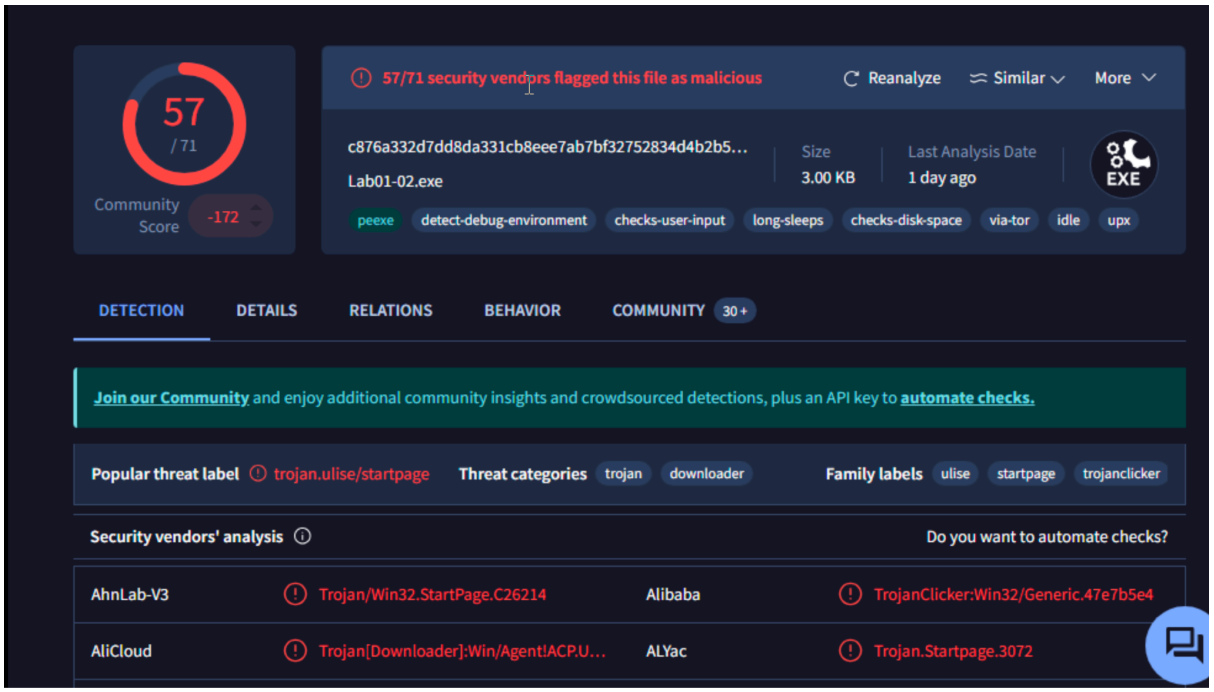
The .dll file contains a reference to local IP address 127.26.152.13. This address is an artifact of this program having been created for educational and not malicious purposes. If this was real malware, the IP address should be routable, and it would be a good network-based indicator for use in identifying this malware.

G. What would you guess is the purpose of these files?

The .dll file is probably a backdoor. The .exe file is used to install or run the DLL.

II. LAB01-02

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



- Popular Threat Label: The file is labeled as `trojan.ulise/startpage`.
- Security Vendors' Analysis:

- Most vendors have categorized this file under various Trojan families, with specific detections like `Trojan.Win32.StartPage.C26214`, `Trojan[Downloader]:Win/Agent!ACP.U...`, and more.

- Notable mentions include detections from AhnLab-V3, AliCloud, and BitDefender, among others.

- File Properties:

- The file is identified as a PE32 executable, specifically for Windows, and it's packed using UPX compression.

- The size of the file is 3.00 KB, which is relatively small and typical for malicious payloads designed to download additional malware or payloads.

- Indicators of Malicious Behavior:

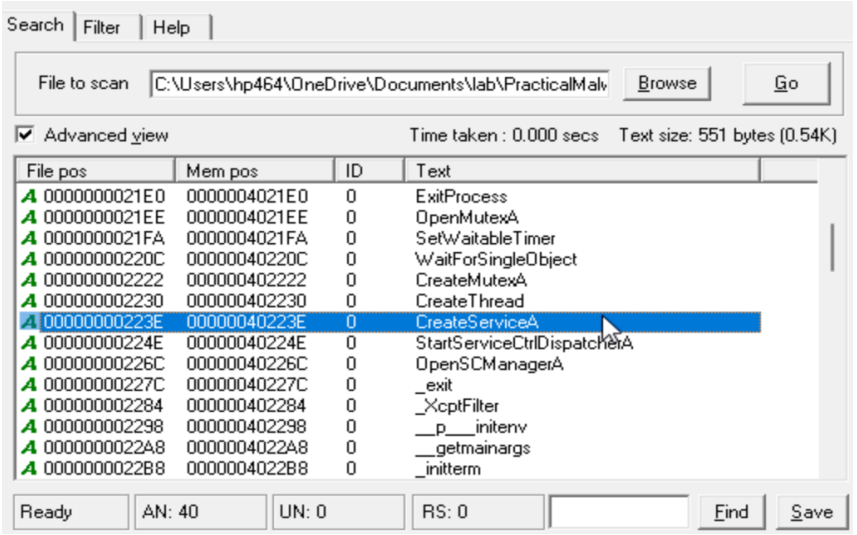
- The detections imply that the file likely has behavior associated with Trojans, such as downloading other malware or redirecting users to potentially harmful websites.

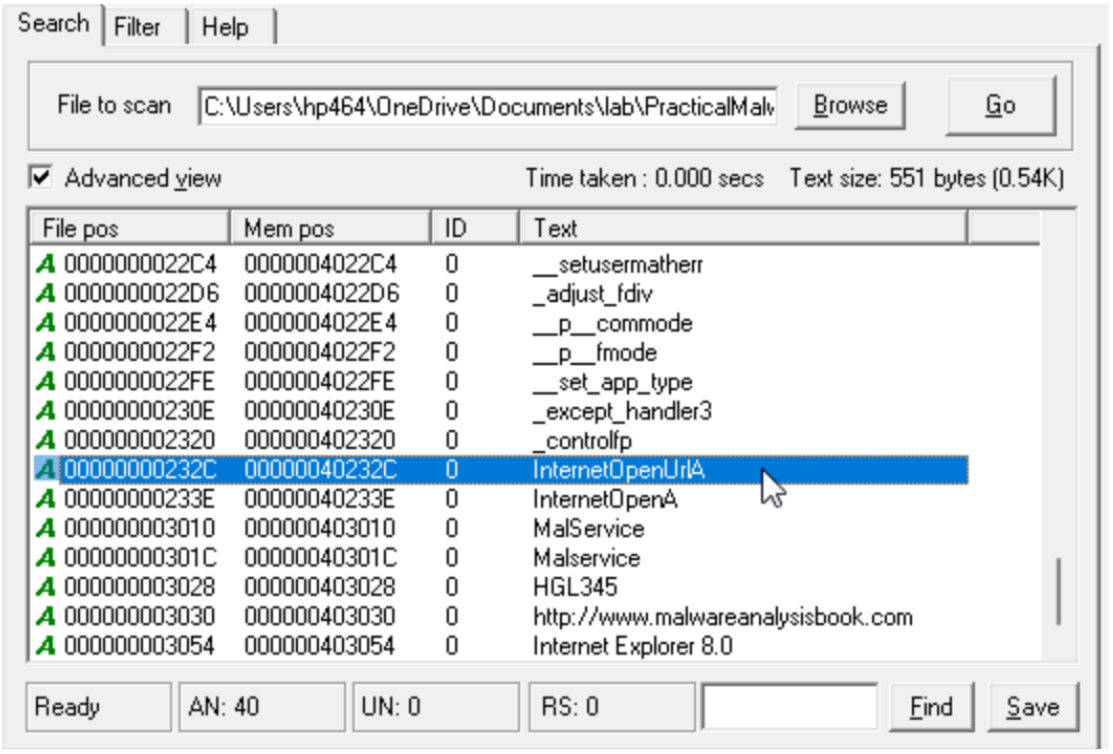
B. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

use command:

upx.exe -d <path Lab01-02.exe>

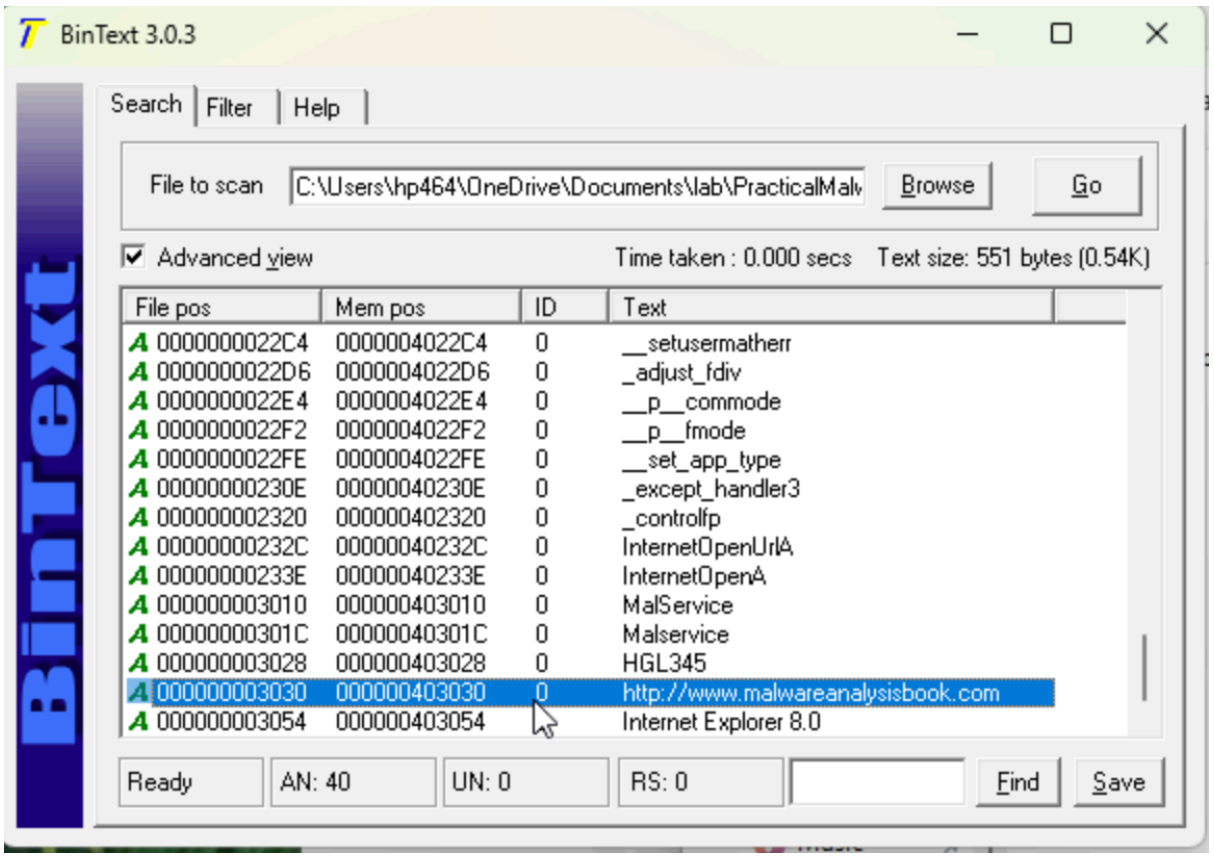
C. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?





After unpacking the file, the most interesting imports are CreateService, InternetOpen, and InternetOpenURL

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



Checking infected machines for a service called Malservice and for network traffic to http://www.malwareanalysisbook.com/

III. LAB01-03

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

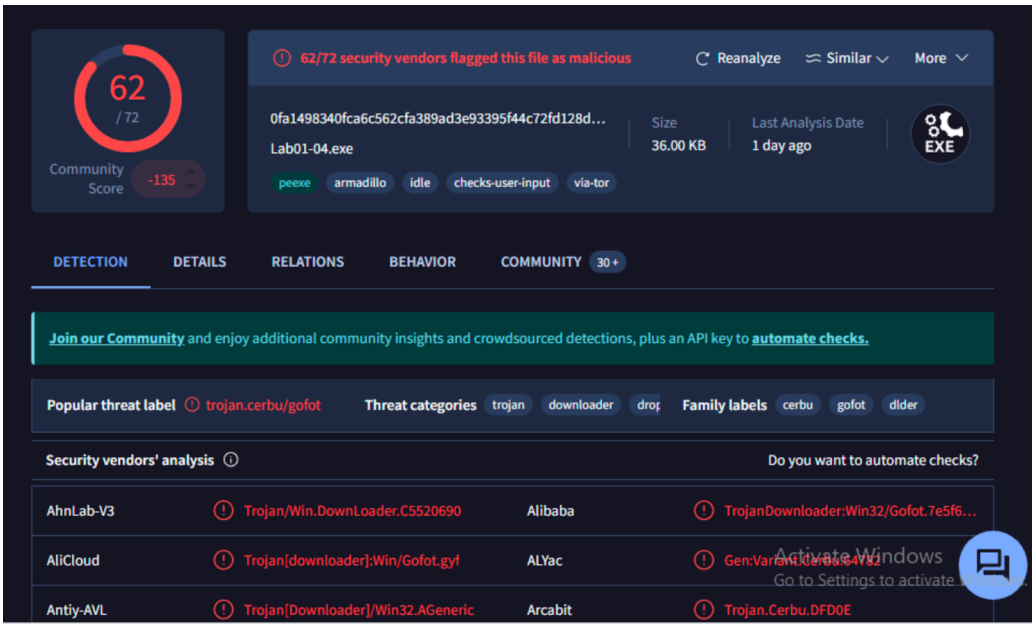
```
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2013
UPX 3.91w       Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 2013

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: C:\Users\mrdam\Downloads\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-03.exe: IOExce
ption: C:\Users\mrdam\OneDrive\Mßy tφnh\test: Permission denied

Unpacked 0 files.
```

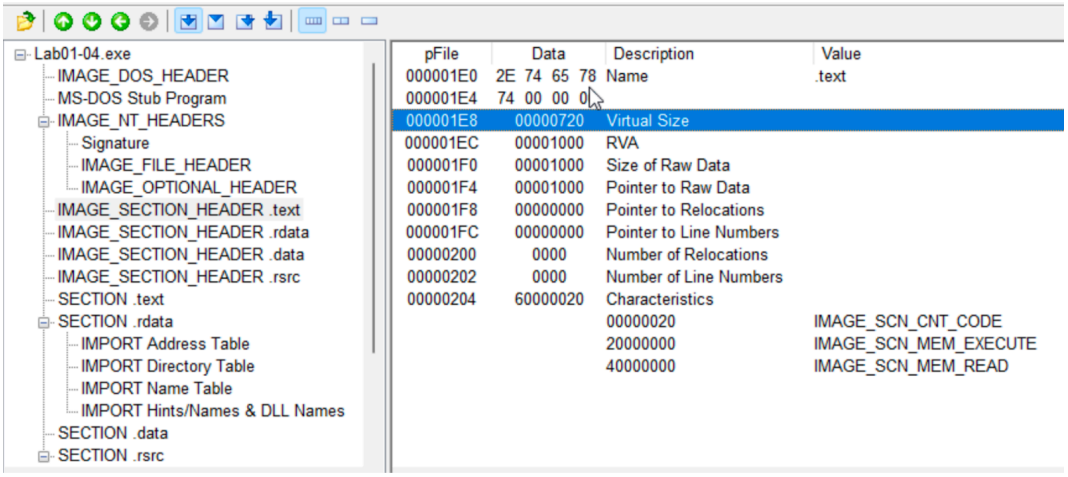
IV. LAB01-04

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



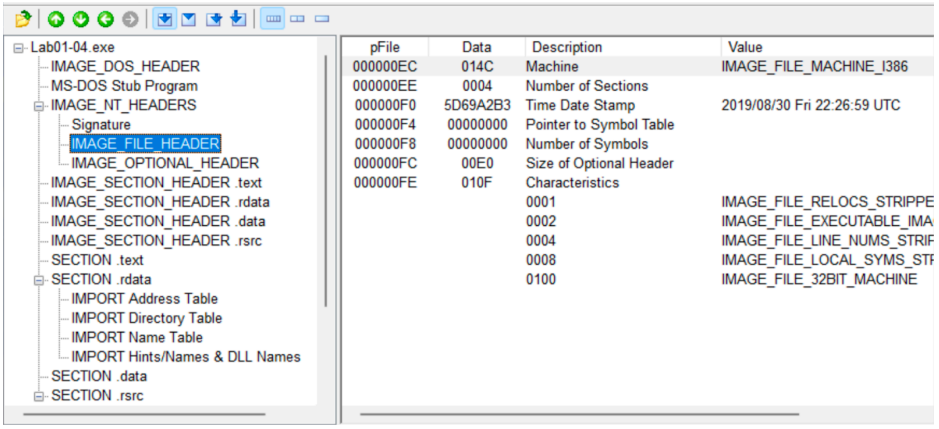
- Malicious Flags: 62 vendors have flagged this file as malicious.
- Threat Labels: The file is categorized under multiple threat labels, including:
  - Trojan
  - Downloader
  - Dropper

B. 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.



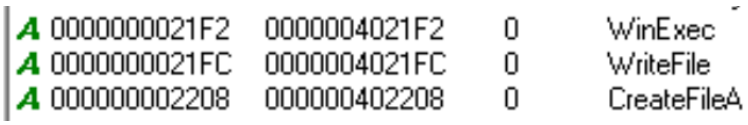
There are no indications that the file is packed or obfuscated.

C. When was this program compiled?



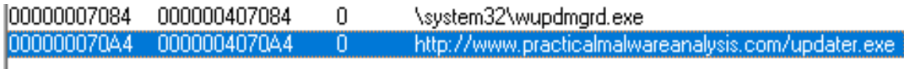
The file compiled in August 2019

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



The imports from WinExec and WriteFile, along with the results from VirusTotal.com,

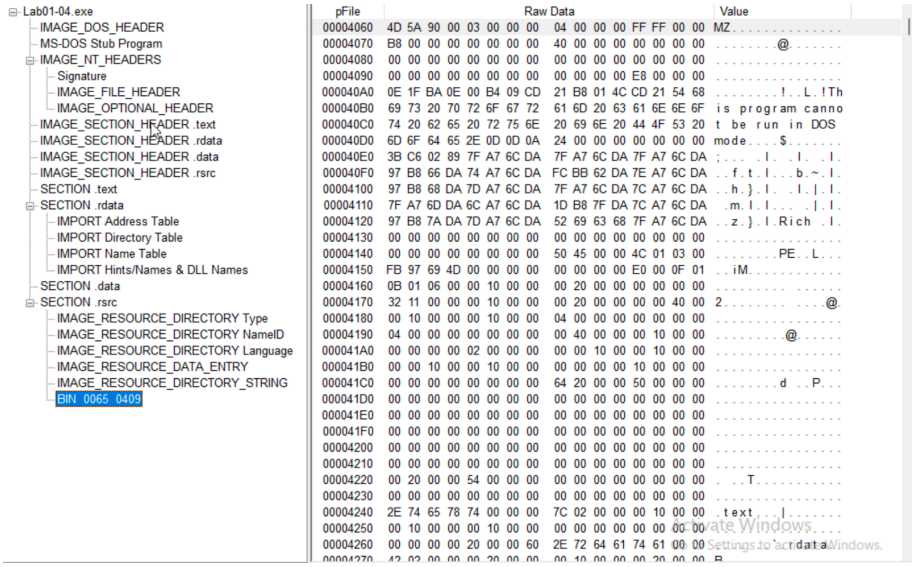
E. What host- or network-based indicators could be used to identify this malware on infected machines?



The path \system32\wupdmgr.exe suggests that this program may be capable of creating or altering a

file in that directory. Additionally, the URL www.malwareanalysisbook.com/updater.exe likely points to a location where further malware is kept and prepared for download.

F. 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?



The resource section includes another PE executable. Utilize Resource Hacker to extract this resource as binary data, then analyze the binary file just like you would with any executable. The executable found in the resource section functions as a downloader that retrieves additional malware.