

Alanna Richerson

01168621

Download the zip file from Canvas that contains hw\_1\_in.exe and hw\_1\_in.dll (or Lab01-02.exe in "Chapter\_1L" if you are having trouble of downloading the file). Unzip them to a location on your VM. Please address the following queries (attach screenshots to support your answers):

1. Upload the files to VirusTotal and evaluate the generated reports. Does the consensus suggest that they are malicious? If so, can you pinpoint the type of malware indicated?

51 / 64

51 security vendors and no sandboxes flagged this file as malicious

a2d33fbd4a37fc01082e1a21c813ee308c06acbd1240a07908de1f7b8e6f00b

hw\_1\_in(4).zip

Size: 4.26 KB | Last Analysis Date: 2 months ago

zip contains-pe

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label: Trojan:Win32/Agent.C957604

Threat categories: trojan

Family labels: ulisse, aenjaris, kkbv

Security vendors' analysis

Vendor	Detection
AhnLab-V3	Trojan:Win32/Agent.C957604
ALYac	Trojan.Agent.Waski
Arcabit	Trojan.Ulisse.DIBCIE [many]
AVG	Win32/Malware-gen
BitDefender	Gen:Variant.Ulisse.113694
ClamAV	Win.Malware.Agent-6342616-0
Alibaba	Trojan:Win32/Aenjaris.7f3a4542
Antiy-AVL	Trojan:Win32/BTSGeneric
Avast	Win32/Malware-gen
Avira (no cloud)	TR/Agent.kkbv
BitDefenderTheta	Gen:NN.Zedlbf.36722.kq4@aGkQVtp
Cynet	Malicious (score: 99)

2. Identify the compilation dates of the files.

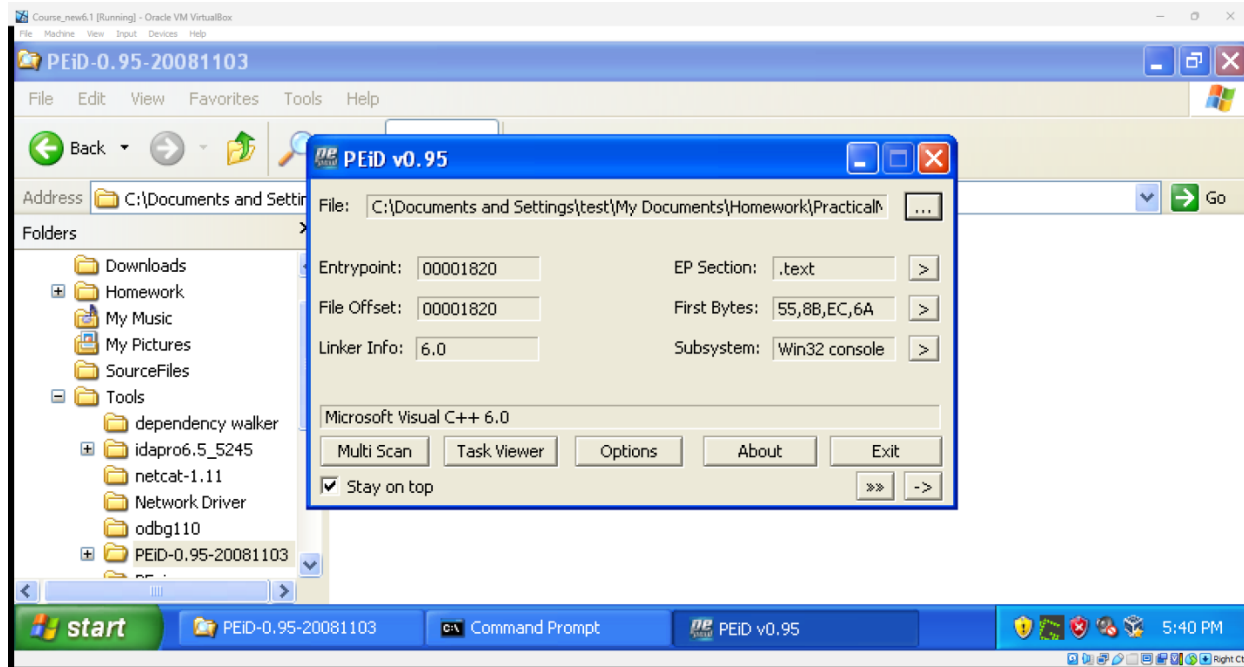
PEView - C:\Documents and Settings\test\My Documents\Homework\Practical\MalwareAnal...

File View Go Help

Lab01-01.exe

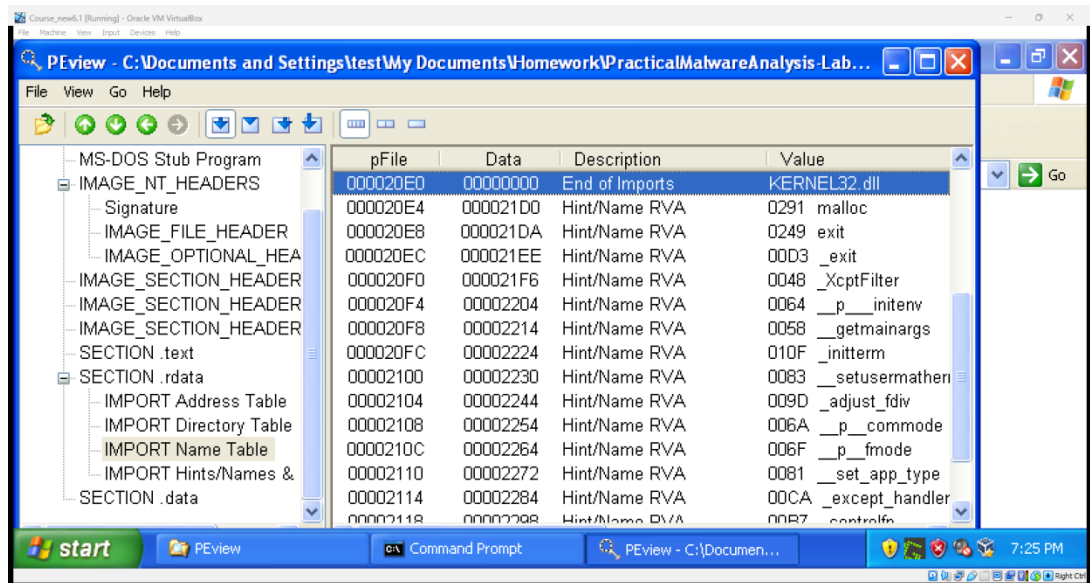
pFile	Data	Description	Value
IMAGE_DOS_HEAD	000000EC	Machine	IMAGE_FILE_MACHINE_I386
MS-DOS Stub Prog	000000EE	Number of Sections	0003
IMAGE_NT_HEADERS	000000F0	Time Date Stamp	2010/12/19 Sun 16:16:19
Signature	000000F4	Pointer to Symbol Table	4D0E2FD3
IMAGE_FILE_HEADER	000000F8	Number of Symbols	00000000
IMAGE_OPTIONAL_HEADER	000000FC	Size of Optional Header	00E0
IMAGE_SECTION_HEADER	000000FE	Characteristics	010F
IMAGE_SECTION_HEADER			0001
IMAGE_SECTION_HEADER			0002
IMAGE_SECTION_HEADER			0004
SECTION .text			0008
SECTION .rdata			0100
SECTION .data			

- Examine whether the program is packed. Could you describe the method you utilized to find this out? Support your answer with screenshots.

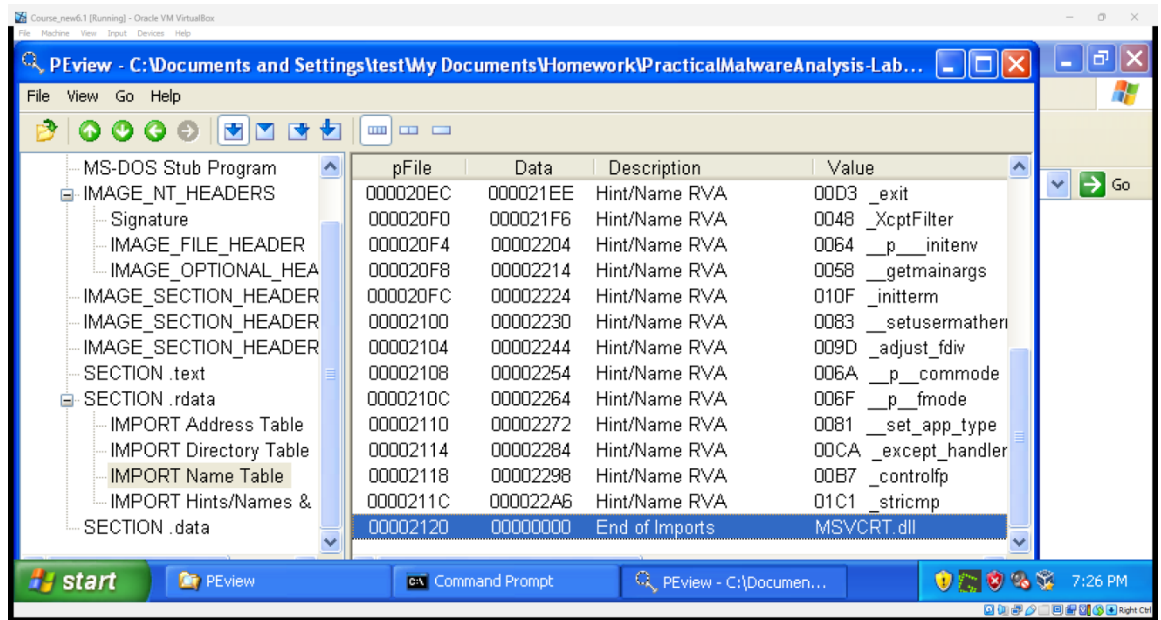


1.

- List down the imports. Are there any that raise suspicion? Can you deduce the malware's functionalities from the imports?



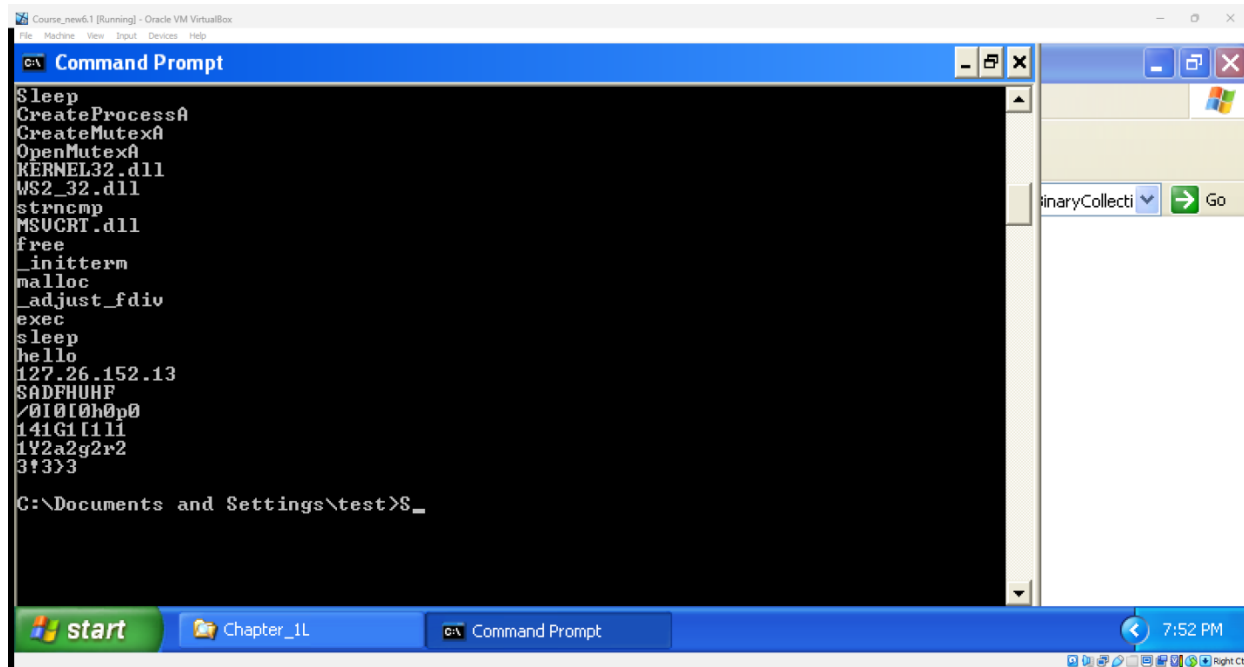
1.



2.

3. This malware allows for a network-enabled back door

5. Are there any signs of network-based indicators? If an IP address is evident, what is it, and what insights can be gained from it?



1.

6. Based on your analysis, can you speculate on the malware's objective?

1. The malware's speculated objective is to create a backdoor. The exec string will probably be transmitted to the IP address for initializing the backdoor via CreateProcess, employing sleep to avoid detection.

Remember to attach screenshots wherever possible to substantiate your findings.

