

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	3
II. LAB01-02	6
III. LAB01-03	9
IV. LAB01-04	9

I. LAB01-01

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

The screenshot shows the VirusTotal analysis interface for a specific file. At the top, there's a navigation bar with tabs like 'Popular', 'threat label', 'trojan.doina/skeeyah', 'Threat categories', 'trojan', and 'Family labels' (doina, skeeyah). Below this is a search bar and a 'Do you want to automate checks?' button.

The main area displays a table of security vendor analysis results:

Vendor	Detection
Alibaba	Trojan:Win32/Skeeyah.7fb0ebff
AliCloud	Backdoor:Win/Agent!LW.BOM
ALYac	Trojan.Agent.Waski
Antiy-AVL	Trojan/Win32.BTSGeneric
Arcabit	Trojan.Doina.D12B4A
Avast	Win32:Malware-gen
AVG	Win32:Malware-gen
BitDefender	Gen:Variant.Doina.76618
Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Malware.Agent-6369668-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Dll.trojan.skeeyah
Cylance	Unsafe
Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS
Elastic	Malicious (high Confidence)

Threat Label: trojan.doina/skeeyah

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!LW.BOM
- Various other detections related to malware.

- B. When were these files compiled?

PEView - C:\Users\hp464\OneDrive\Documents\lab\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter...

File View Go Help					
		pFile	Data	Description	Value
Lab01-01.exe		000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
IMAGE_DOS_HEADER		000000EE	0003	Number of Sections	
MS-DOS Stub Program		000000F0	4D0E2FD3	Time Date Stamp	2010/12/19 Sun 16:16:19 UTC
IMAGE_NT_HEADERS		000000F4	00000000	Pointer to Symbol Table	
Signature		000000F8	00000000	Number of Symbols	
IMAGE_FILE_HEADER		000000FC	00E0	Size of Optional Header	
IMAGE_OPTIONAL_HEADER		000000FE	010F	Characteristics	
0001					IMAGE_FILE_RELOCS_STRIPPED
0002					IMAGE_FILE_EXECUTABLE_IMAGE
0004					IMAGE_FILE_LINE_NUMS_STRIPPED
0008					IMAGE_FILE_LOCAL_SYMS_STRIPPED
0100					IMAGE_FILE_32BIT_MACHINE
IMAGE_SECTION_HEADER.tex					
IMAGE_SECTION_HEADER.rda					
IMAGE_SECTION_HEADER.dat					
SECTION .text					
SECTION .rdata					
SECTION .data					

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?

PEView - C:\Users\hp464\OneDrive\Documents\lab\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter...

File View Go Help					
		pFile	Data	Description	Value
Lab01-01.exe		000001E0	2E 74 65 78	Name	.text
IMAGE_DOS_HEADER		000001E4	74 00 00 00		
MS-DOS Stub Program		000001E8	00000970	Virtual Size	
IMAGE_NT_HEADERS		000001EC	00001000	RVA	
Signature		000001F0	00001000	Size of Raw Data	
IMAGE_FILE_HEADER		000001F4	00001000	Pointer to Raw Data	
IMAGE_OPTIONAL_HEADER		000001F8	00000000	Pointer to Relocations	
IMAGE_SECTION_HEADER.tex		000001FC	00000000	Pointer to Line Numbers	
IMAGE_SECTION_HEADER.rda		00000200	0000	Number of Relocations	
IMAGE_SECTION_HEADER.dat		00000202	0000	Number of Line Numbers	
SECTION .text		00000204	60000020	Characteristics	
00000020					IMAGE_SCN_CNT_CODE
20000000					IMAGE_SCN_MEM_EXECUTE
40000000					IMAGE_SCN_MEM_READ
IMAGE_SECTION_HEADER.tex					
IMAGE_SECTION_HEADER.rda					
IMAGE_SECTION_HEADER.dat					
SECTION .text					
SECTION .rdata					
SECTION .data					

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

A	0000000002196	000000402196	0	FindNextFileA
A	00000000021A6	0000004021A6	0	FindFirstFileA
A	00000000021B8	0000004021B8	0	CopyFileA

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?

pFile	Raw Data	Value
00003000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00003010	6B 65 72 6E 65 31 33 32 2E 64 6C 6C 00 00 00 00	kerne132.dll....
00003020	6B 65 72 6E 65 6C 33 32 2E 64 6C 6C 00 00 00 00	kernel32.dll....
00003030	2E 65 78 65 00 00 00 00 5C 2A 00 00 2E 2E 00 00	.exe....*....
00003040	2E 00 00 00 43 3A 5C 2A 00 00 00 43 3A 5C 77	...C:*....C:\w
00003050	69 6E 64 6F 77 73 5C 73 79 73 74 65 6D 33 32 5C	indows\System32\
00003060	6B 65 72 6E 65 31 33 32 2E 64 6C 6C 00 00 00 00	kerne132.dll....
00003070	4B 65 72 6E 65 6C 33 32 2E 00 00 00 4C 61 62 30	Kernel32....Lab0
00003080	31 2D 30 31 2E 64 6C 6C 00 00 00 43 3A 5C 57	1-01.dll....C:\W
00003090	69 6E 64 6F 77 73 5C 53 79 73 74 65 6D 33 32 5C	indows\System32\
000030A0	4B 65 72 6E 65 6C 33 32 2E 64 6C 6C 00 00 00 00	Kernel32.dll....
000030B0	57 41 52 4E 49 4E 47 5F 54 48 49 53 5F 57 49 4C	WARNING_THIS_WIL
000030C0	4C 5F 44 45 53 54 52 4F 59 5F 59 4F 55 52 5F 4D	L_DESTROY_YOUR_M
000030D0	41 43 48 49 4E 45 00 00 01 00 00 00 00 00 00 00	ACHINE.....
000030E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000030F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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?

File pos	Mem pos	ID	Text
A 000000000214E	00001000214E	0	KERNEL32.dll
A 000000000215C	00001000215C	0	WS2_32.dll
A 000000000216A	00001000216A	0	strcmp
A 0000000002172	000010002172	0	MSVCRT.dll
A 0000000002188	000010002188	0	_interim
A 0000000002194	000010002194	0	malloc
A 000000000219E	00001000219E	0	_adjust_fdiv
A 000000026018	000010026018	0	sleep
A 000000026020	000010026020	0	hello
A 000000026028	000010026028	0	127.26.152.13
A 000000026038	000010026038	0	SADFHUHF
A 000000027008	000010027008	0	/010[0h0p0
A 000000027029	000010027029	0	141G1[1I1
A 000000027039	000010027039	0	1Y2a2g2r2

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?

The screenshot shows the VirusTotal analysis interface for the file `c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b5... Lab01-02.exe`. The main summary indicates that 57 out of 71 security vendors flagged the file as malicious. Below this, detailed information includes the file size (3.00 KB) and the last analysis date (1 day ago). The file type is identified as EXE. A list of threat labels includes `peexe`, `detect-debug-environment`, `checks-user-input`, `long-sleeps`, `checks-disk-space`, `via-tor`, `idle`, and `upx`. Below the summary, tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY are visible, with the DETECTION tab selected. A call-to-action button encourages users to join the community. The SECURITY VENDORS' ANALYSIS section lists detections from AhnLab-V3, Alibaba, and AliCloud, along with their respective threat labels. A blue speech bubble icon is located in the bottom right corner.

- 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.

```
C:\Users\hp464\OneDrive\Documents\upx391w\upx391w>upx.exe -d "C:\Users\hp464\OneDrive\Documents\lab\alwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-02.exe"
    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
      -----        -----       -----
      16384 <-      3072     18.75%     win32/pe     Lab01-02.exe

Unpacked 1 file.

C:\Users\hp464\OneDrive\Documents\upx391w\upx391w>
```

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?

Search Filter Help			
File to scan C:\Users\hp464\OneDrive\Documents\lab\PracticalMal			
<input checked="" type="checkbox"/> Advanced view Time taken : 0.000 secs Text size: 551 bytes (0.54K)			
File pos	Mem pos	ID	Text
A 00000000021E0	0000004021E0	0	ExitProcess
A 00000000021EE	0000004021EE	0	OpenMutexA
A 00000000021FA	0000004021FA	0	SetWaitableTimer
A 000000000220C	00000040220C	0	WaitForSingleObject
A 0000000002222	000000402222	0	CreateMutexA
A 0000000002230	000000402230	0	CreateThread
A 000000000223E	00000040223E	0	CreateServiceA
A 000000000224E	00000040224E	0	StartServiceCtrlDispatcherA
A 000000000226C	00000040226C	0	OpenSCManagerA
A 000000000227C	00000040227C	0	_exit
A 0000000002284	000000402284	0	_XcptFilter
A 0000000002298	000000402298	0	_p__interv
A 00000000022A8	0000004022A8	0	_getmainargs
A 00000000022B8	0000004022B8	0	_initerm
Ready AN: 40 UN: 0 RS: 0 Find Save			

Search | Filter | Help |

File to scan C:\Users\hp464\OneDrive\Documents\lab\PracticalMalv

Advanced view Time taken : 0.000 secs Text size: 551 bytes (0.54K)

File pos	Mem pos	ID	Text
A 00000000022C4	0000004022C4	0	_setusermatherr
A 00000000022D6	0000004022D6	0	_adjust_fdiv
A 00000000022E4	0000004022E4	0	_p_commode
A 00000000022F2	0000004022F2	0	_p_fmode
A 00000000022FE	0000004022FE	0	_set_app_type
A 000000000230E	00000040230E	0	_except_handler3
A 0000000002320	000000402320	0	_controlfp
A 000000000232C	00000040232C	0	InternetOpenUrlA
A 000000000233E	00000040233E	0	InternetOpenA
A 0000000003010	000000403010	0	MalService
A 000000000301C	00000040301C	0	Malservice
A 0000000003028	000000403028	0	HGL345
A 0000000003030	000000403030	0	http://www.malwareanalysisbook.com
A 0000000003054	000000403054	0	Internet Explorer 8.0

Ready AN: 40 UN: 0 RS: 0

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?

BinText 3.0.3

Search | Filter | Help |

File to scan C:\Users\hp464\OneDrive\Documents\lab\PracticalMalv

Advanced view Time taken : 0.000 secs Text size: 551 bytes (0.54K)

File pos	Mem pos	ID	Text
A 00000000022C4	0000004022C4	0	_setusermatherr
A 00000000022D6	0000004022D6	0	_adjust_fdiv
A 00000000022E4	0000004022E4	0	_p_commode
A 00000000022F2	0000004022F2	0	_p_fmode
A 00000000022FE	0000004022FE	0	_set_app_type
A 000000000230E	00000040230E	0	_except_handler3
A 0000000002320	000000402320	0	_controlfp
A 000000000232C	00000040232C	0	InternetOpenUrlA
A 000000000233E	00000040233E	0	InternetOpenA
A 0000000003010	000000403010	0	MalService
A 000000000301C	00000040301C	0	Malservice
A 0000000003028	000000403028	0	HGL345
A 0000000003030	000000403030	0	http://www.malwareanalysisbook.com
A 0000000003054	000000403054	0	Internet Explorer 8.0

Ready AN: 40 UN: 0 RS: 0

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\mrدام\Downloads\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab01-03.exe: IOException: C:\Users\mrدام\OneDrive\M&Y t&n\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?

The screenshot shows the VirusTotal analysis interface for the file *Lab01-04.exe*. The main summary indicates 62 out of 72 security vendors flagged the file as malicious. Below this, the file's metadata is shown: SHA-256 hash (0fa1498340fca6c562cfa389ad3e93395f44c72fd128d...), size (36.00 KB), and last analysis date (1 day ago). The file is categorized as an EXE file. Threat labels listed include *peexe*, *armadillo*, *idle*, *checks-user-input*, and *via-tor*. A navigation bar at the bottom includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (30+). A call-to-action button encourages users to join the community and automate checks. Below this, a section titled "Security vendors' analysis" lists vendor findings. For AhnLab-V3, it found a Trojan/Win.Downloader. For AliCloud, it found a Trojan[downloader]:Win/Gofot.gyf. For Antiy-AVL, it found a Trojan[Downloader]/Win32.AGeneric. To the right, there is a link to "Activate Windows" with a "Go to Settings to activate Windows" button.

- 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.

pFile	Data	Description	Value
000001E0	2E 74 65 78	Name	.text
000001E4	74 00 00 00		
000001E8	00000720	Virtual Size	
000001EC	00001000	RVA	
000001F0	00001000	Size of Raw Data	
000001F4	00001000	Pointer to Raw Data	
000001F8	00000000	Pointer to Relocations	
000001FC	00000000	Pointer to Line Numbers	
00000200	0000	Number of Relocations	
00000202	0000	Number of Line Numbers	
00000204	60000020	Characteristics	
	00000020	IMAGE_SCN_CNT_CODE	
	20000000	IMAGE_SCN_MEM_EXECUTE	
	40000000	IMAGE_SCN_MEM_READ	

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

- C. When was this program compiled?

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0004	Number of Sections	
000000F0	5D69A2B3	Time Date Stamp	2019/08/30 Fri 22:26:59 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	
	0001	IMAGE_FILE_RELOCS_STRIPPED	
	0002	IMAGE_FILE_EXECUTABLE_IMAGE	
	0004	IMAGE_FILE_LINE_NUMS_STRIPPED	
	0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED	
	0100	IMAGE_FILE_32BIT_MACHINE	

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?

A 00000000021F2	0000004021F2	0	WinExec
A 00000000021FC	0000004021FC	0	WriteFile
A 0000000002208	000000402208	0	CreateFileA

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?

00000007084	000000407084	0	\system32\wupdmgd.exe
000000070A4	0000004070A4	0	http://www.practicalmalwareanalysis.com/updater.exe

The path \system32\wupdmgd.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 screenshot shows the Resource Hacker interface with two panes. The left pane displays the file structure of 'Lab01-04.exe' with various sections like IMAGE_DOS_HEADER, IMAGE_NT_HEADERS, and sections for text, rdata, rsrc, and rsrc. The right pane shows the raw data and value for each entry. A specific entry in the rsrc section is highlighted with a blue border, showing its raw data and value.

pFile	Raw Data	Value
00004060	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....
00004070	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....
00004080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004090	00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00 00
000040A0	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68L..!Th
000040B0	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
000040C0	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
000040D0	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode...\$.....
000040E0	3B C6 02 89 7F A7 6C DA 7F A7 6C DA 7F A7 6C DAI..I..I..
000040F0	97 B8 66 DA 74 A7 6C DA FC BB 62 DA 7E A7 6C DA	..f.t.l..b~I..
00004100	97 B8 68 DA 7D A7 6C DA 7F A7 6C DA 7C A7 6C DA	..h].l..l..I..I..
00004110	7F A7 6D DA 6C A7 6C DA 1D B8 7F DA 7C A7 6C DA	.m..l..l..I..I..I..
00004120	97 B8 7A DA 7D A7 6C DA 52 69 63 68 7F A7 6C DA	..z}.l.Rich..I..
00004130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004140	00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00PE..L..
00004150	FB 97 69 4D 00 00 00 00 00 00 00 E0 0F 01 ..iM.....	
00004160	0B 01 06 00 00 10 00 00 00 20 00 00 00 00 00 00
00004170	32 11 00 00 00 10 00 00 00 20 00 00 00 00 40 00	2.....@.....
00004180	00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00
00004190	04 00 00 00 00 00 00 00 00 40 00 00 00 10 00 00@.....
000041A0	00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00
000041B0	00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00
000041C0	00 00 00 00 00 00 00 00 64 20 00 00 50 00 00 00d..P..
000041D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000041E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000041F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004210	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004220	00 20 00 00 54 00 00 00 00 00 00 00 00 00 00 00	..T.....
00004230	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004240	2E 74 65 78 74 00 00 00 7C 02 00 00 00 10 00 00	text.....
00004250	00 10 00 00 00 10 00 00 00 00 00 00 00 00 00 00Windows.....
00004260	00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00	Settings to 'actdata\windows.
00004270	x2 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00R.....

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.