

Practical Malware Analysis Chapter 1

Lab 1-1

Lap 1 : lab01-01.exe , lab01-01.dll

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

Lab01-01.dll :

5f0e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

45 / 70

45 security vendors and no sandboxes flagged this file as malicious

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Lab01-01.dll
Size: 160.00 KB
2023-04-27 11:42:37 UTC
3 days ago

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.ulise/skeeyah Threat categories: trojan Family labels: ulise skeeyah r002c0phf20

Security vendors' analysis

Alibaba	Trojan.Win32/Skeeyah.7fb0ebff	ALYac	Trojan.Agent.Waski
Antiy-AVL	Trojan/Win32.BTSGeneric	Arcabit	Trojan.Ulise.D19D44
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
BitDefender	Gen:Variant.Ulise.105796	BitDefenderTheta	Gen:NN.ZedlaF.36164.kq4@aGkQVtp
ClamAV	Win.Malware.Agent-6369668-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Skeeyah.AK.gen!Eldorado	DeepInstinct	MALICIOUS
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Ulise.105796 (B)
eScan	Gen:Variant.Ulise.105796	ESET-NOD32	A Variant Of Generik.TGEWDD

Lab01-01.exe :

58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47

55 / 71

55 security vendors and 1 sandbox flagged this file as malicious

58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Lab01-01.exe
Size: 16.00 KB
2023-04-30 20:39:17 UTC
24 minutes ago

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.ulise/aenjaris Threat categories: trojan Family labels: ulise aenjaris r002c0dcd20

AhnLab-V3	❗ Trojan:Win32.Agent.C957604	Alibaba	❗ Trojan:Win32/Aenjaris.2be749b4
ALYac	❗ Trojan.Agent.16384SS	Antiy-AVL	❗ Trojan:Win32.TSGeneric
Arcabit	❗ Trojan.Ulise.D1BC1E	Avast	❗ Win32:Malware-gen
AVG	❗ Win32:Malware-gen	Avira (no cloud)	❗ HEUR/AGEN.1344261
BitDefender	❗ Gen:Variant.Ulise.113694	ClamAV	❗ Win.Malware.Agent-6342616-0
CrowdStrike Falcon	❗ Win/malicious_confidence_100% (W)	Cybreason	❗ Malicious.82141a
Cylance	❗ Unsafe	Cynet	❗ Malicious (score: 100)
Cyren	❗ W32/Ulise.CK.genEldorado	DeepInstinct	❗ MALICIOUS
Elastic	❗ Malicious (high Confidence)	Emsisoft	❗ Gen:Variant.Ulise.113694 (B)

Similar antivirus programs are :

AVG – Avast – Bitdefender are and many of them.

-> When were these files compiled ?

Lab01-01.dll : Sun Dec 19 / 16:16:38 / 2010

pestudio 9.45 - Malware Initial Assessment - www.winitor.com [c:\users\anubis\desktop\practical malware analysis labs\binarycollection\chapter_1\lab01-01.dll]

file settings about

c:\users\anubis\desktop\practical malware analysis

- indicators (34)
- virustotal (45/70)
- dos-header (64 bytes)
- dos-stub (160 bytes)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (3)
- sections (4)
- libraries (flag)
- imports (flag)
- exports (n/a)
- tls-callback (n/a)
- .NET (n/a)
- resources (n/a)
- strings (count) *
- debug (n/a)
- manifest (n/a)
- version (n/a)
- overlay (n/a)

property	value	detail
characteristics	0x210E	
dynamic-link-library	0x2000	true
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0000	false
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
general		
compiler-stamp	0x4D0E2FE6	Sun Dec 19 16:16:38 2010 UTC
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	Intel-386
sections	0x0004	4
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000

Lab01-01.exe : Sun Dec 19 / 16:16:19 / 2010

pestudio 9.45 - Malware Initial Assessment - www.winitor.com [c:\users\anubis\desktop\practical malware analysis labs\binarycollection\chapter_1\lab01-01.exe]

file settings about

c:\users\anubis\desktop\practical malware analysis

- indicators (27)
 - virustotal (error)
 - dos-header (64 bytes)
 - dos-stub (168 bytes)
 - rich-header (Visual Studio)
 - file-header (Intel-386)
 - optional-header (console)
- directories (2)
- sections (3)
- libraries (2)
- imports (flag)
- exports (n/a)
- tls-callback (n/a)
- .NET (n/a)
- resources (n/a)
- strings (151) *
- debug (n/a)
- manifest (n/a)
- version (n/a)
- overlay (n/a)

property	value	detail
characteristics	0x010F	
dynamic-link-library	0x0000	false
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
general		
compiler-stamp	0x4D0E2FD3	Sun Dec 19 16:16:19 2010 UTC
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	Intel-386
sections	0x0003	3
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000

-> Do any imports indicate what this malware does? If so, what are the imports?

Lab01-01.exe : libraries → Kernel32.dll , MSVcrtdll

c:\users\anubis\desktop\practical malware analysis

imports (25)

flag (4)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (2)	type (1)	ordinal (0)	library (2)
-	0x00002144	0x00002144	437 (0x01B5)	memory	implicit	-	KERNEL32
-	0x000021D0	0x000021D0	657 (0x0291)	memory	implicit	-	MSVCRT
x	0x00002132	0x00002132	688 (0x02B0)	file	implicit	-	KERNEL32
x	0x00002154	0x00002154	470 (0x01D6)	file	implicit	-	KERNEL32
-	0x00002164	0x00002164	53 (0x0035)	file	implicit	-	KERNEL32
-	0x0000217A	0x0000217A	52 (0x0034)	file	implicit	-	KERNEL32
-	0x00002188	0x00002188	144 (0x0090)	file	implicit	-	KERNEL32
x	0x00002194	0x00002194	157 (0x009D)	file	implicit	-	KERNEL32
x	0x000021A4	0x000021A4	148 (0x0094)	file	implicit	-	KERNEL32
-	0x000021B6	0x000021B6	40 (0x0028)	file	implicit	-	KERNEL32
-	0x00002124	0x00002124	27 (0x001B)	-	implicit	-	KERNEL32
-	0x000021DA	0x000021DA	585 (0x0249)	-	implicit	-	MSVCRT
-	0x000021EE	0x000021EE	211 (0x00D3)	-	implicit	-	MSVCRT
-	0x000021F6	0x000021F6	72 (0x0048)	-	implicit	-	MSVCRT
-	0x00002204	0x00002204	100 (0x0064)	-	implicit	-	MSVCRT

Lab01-01.dll : libraries → KERNEL.dll , MSVCRT.dll , WS2 32.dll

c:\users\anubis\desktop\practical malware analysis

imports (20)

flag (11)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (4)	type (1)	ordinal (10)	library (3)
-	0x00002130	0x00002130	63 (0x003F)	synchronization	implicit	-	KERNEL32
-	0x00002140	0x00002140	493 (0x01ED)	synchronization	implicit	-	KERNEL32
x	0x00000017	0x00000017	0 (0x0000)	network	implicit	x	WS2 32.dll
x	0x00000073	0x00000073	0 (0x0000)	network	implicit	x	WS2 32.dll
x	0x00000008	0x00000008	0 (0x0000)	network	implicit	x	WS2 32.dll
x	0x00000004	0x00000004	0 (0x0000)	network	implicit	x	WS2 32.dll
x	0x00000013	0x00000013	0 (0x0000)	network	implicit	x	WS2 32.dll
x	0x00000016	0x00000016	0 (0x0000)	network	implicit	x	WS2 32.dll
x	0x00000010	0x00000010	0 (0x0000)	network	implicit	x	WS2 32.dll
x	0x00000003	0x00000003	0 (0x0000)	network	implicit	x	WS2 32.dll
x	0x00000074	0x00000074	0 (0x0000)	network	implicit	x	WS2 32.dll
x	0x00000009	0x00000009	0 (0x0000)	network	implicit	x	WS2 32.dll
-	0x00002192	0x00002192	657 (0x0291)	memory	implicit	-	MSVCRT
-	0x00002116	0x00002116	662 (0x0296)	execution	implicit	-	KERNEL32
x	0x0000211E	0x0000211E	68 (0x0044)	execution	implicit	-	KERNEL32
-	0x00002108	0x00002108	27 (0x001B)	-	implicit	-	KERNEL32
-	0x0000219C	0x0000219C	157 (0x009D)	-	implicit	-	MSVCRT
-	0x00002186	0x00002186	271 (0x010F)	-	implicit	-	MSVCRT
-	0x0000217E	0x0000217E	606 (0x025E)	-	implicit	-	MSVCRT
-	0x00002168	0x00002168	704 (0x02C0)	-	implicit	-	MSVCRT

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

Lab01-01.dll : not found

Lab01-01.exe : →C:\windows\system32\kerne132.dll

→C:\Windows\System\Kernel32.dll

c:\users\anubis\desktop\practical malware analy	encoding (2)	size (bytes)	location	flag (4)	label (31)	group (2)	value (151)
indicators (27)	ascii	12	0x00003020	-	library	-	kernel32.dll
virustotal (error)	ascii	11	0x00002126	-	import	-	CloseHandle
dos-header (64 bytes)	ascii	11	0x000021F8	-	import	-	XcptFilter
dos-stub (168 bytes)	ascii	13	0x00002206	-	import	-	p_initenv
rich-header (Visual Studio)	ascii	13	0x00002216	-	import	-	getmainargs
file-header (Intel-386)	ascii	9	0x00002226	-	import	-	initterm
optional-header (console)	ascii	16	0x00002232	-	import	-	setusermatherr
directories (2)	ascii	12	0x00002246	-	import	-	adjust_fdiv
sections (3)	ascii	12	0x00002256	-	import	-	p_commode
libraries (2)	ascii	10	0x00002266	-	import	-	p_fmcode
imports (flag)	ascii	14	0x00002274	-	import	-	set_app_type
exports (n/a)	ascii	16	0x00002286	-	import	-	except_handler2
tls-callback (n/a)	ascii	10	0x0000229A	-	import	-	controlfp
.NET (n/a)	ascii	8	0x000022A8	-	import	-	stricmp
resources (n/a)	ascii	12	0x00003010	-	file	-	kernel32.dll
strings (151)	ascii	4	0x00003030	-	file	-	exe
debug (n/a)	ascii	32	0x0000304C	-	file	-	C:\windows\system32\kernel32.dll
manifest (n/a)	ascii	12	0x0000307C	-	file	-	Lab01-01.dll
version (n/a)	ascii	32	0x0000308C	-	file	-	C:\Windows\System32\Kernel32.dll
overlay (n/a)	ascii	40	0x0000004D	-	dos-message	-	This program cannot be run in DOS mode.
	ascii	5	0x000000C8	-	-	-	Richm
	ascii	5	0x000001E0	-	-	-	.text
	ascii	7	0x00000207	-	-	-	.rdata
	ascii	6	0x0000022F	-	-	-	@.data

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

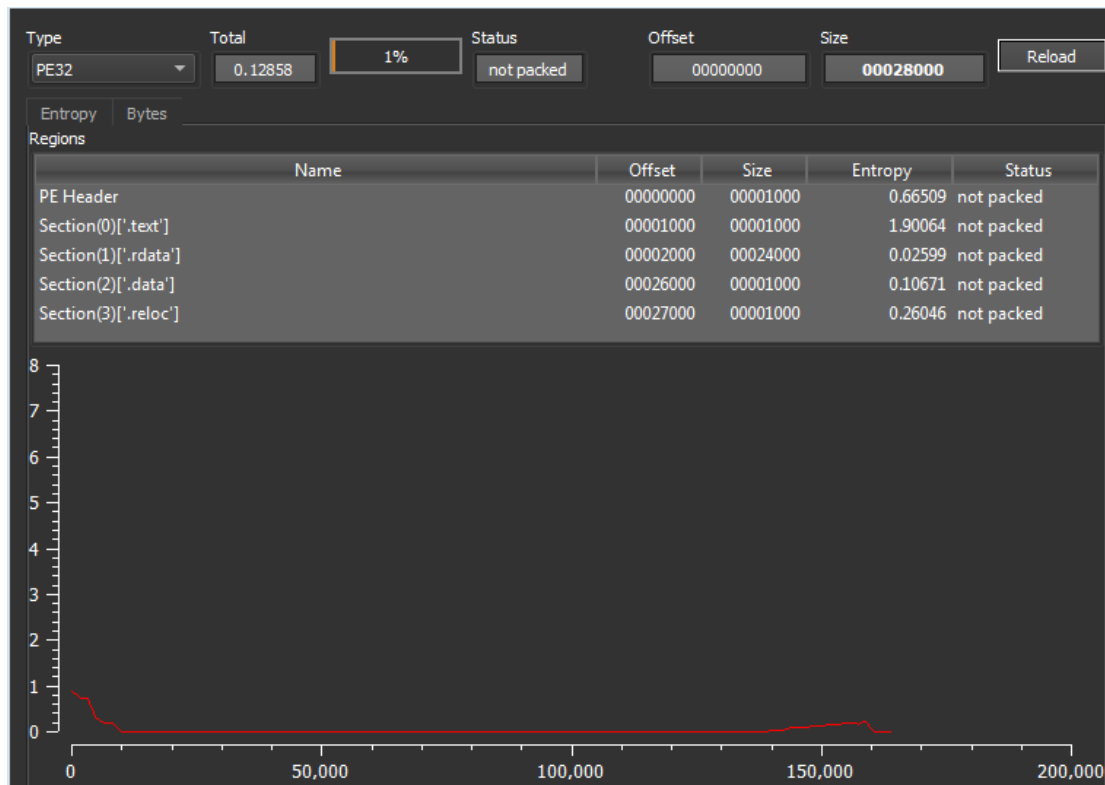
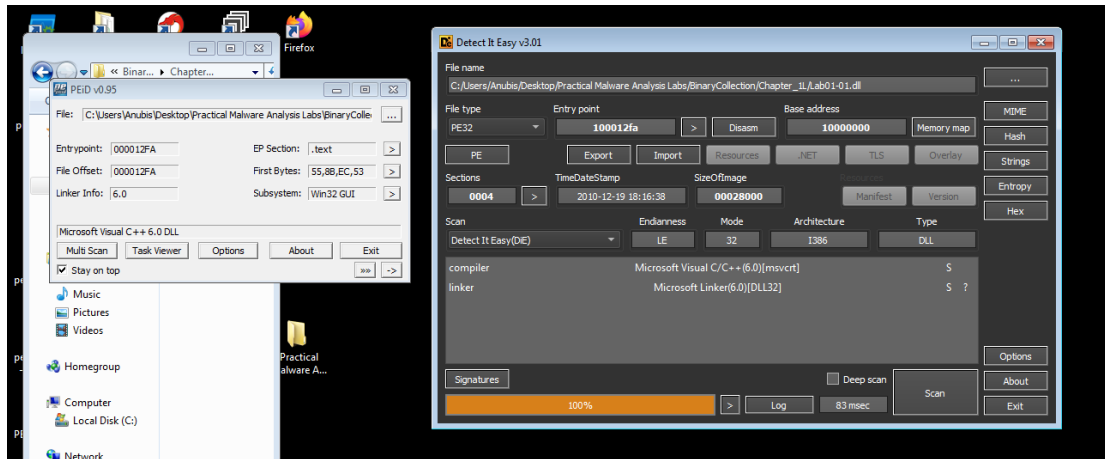
lab01-01.exe : not found.

Lab01-01.dll : 127.26.152.13

c:\users\anubis\desktop\practical malware analy	encoding (2)	size (bytes)	location	flag (1)	label (12)	group (4)	value (55)
indicators (34)	ascii	11	0x00002132	-	import	synchronization	CreateMutex
virustotal (error)	ascii	9	0x00002142	-	import	synchronization	OpenMutex
dos-header (64 bytes)	ascii	10	0x0000215C	-	library	network	WS2_32.dll
dos-stub (160 bytes)	ascii	6	0x00002194	-	-	memory	malloc
rich-header (Visual Studio)	ascii	13	0x00002120	✖	import	execution	CreateProcess
file-header (Intel-386)	ascii	5	0x00002118	-	-	execution	Sleep
optional-header (GUI)	ascii	4	0x00026010	-	utility	-	evex
directories (3)	ascii	13	0x00026028	-	url-pattern	-	127.26.152.13
sections (4)	ascii	12	0x0000214E	-	library	-	kernel32.dll
libraries (flag)	ascii	10	0x00002172	-	library	-	MSVCRT.dll
imports (flag)	ascii	11	0x0000210A	-	import	-	CloseHandle
exports (n/a)	ascii	9	0x00002188	-	import	-	initterm
tls-callback (n/a)	ascii	12	0x0000219E	-	import	-	adjust_fdiv
.NET (n/a)	ascii	40	0x0000004D	-	dos-message	-	This program cannot be run in DOS mode.
resources (n/a)	ascii	4	0x000000C0	-	-	-	Rich
strings (count)	ascii	5	0x000001D8	-	-	-	.text
debug (n/a)	ascii	7	0x000001FF	-	-	-	.rdata
manifest (n/a)	ascii						

-> Are there any indications that either of these files is packed or obfuscated?

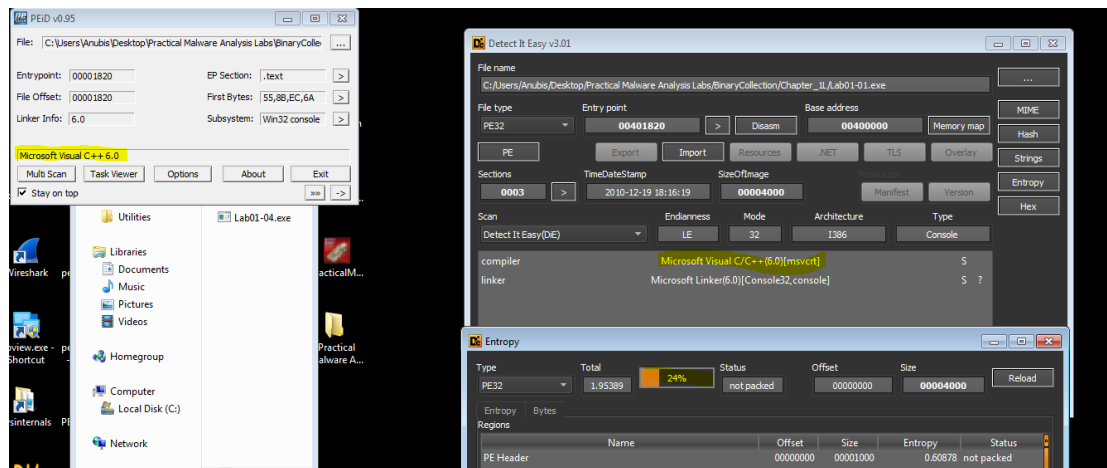
Lab01-01.dll : using PEID , DIE



Entropy = 1%

Not Packed.

Lab01-01.exe : using PEID , DIE



Entropy = 24%

Not Packed.

->What would you guess is the purpose of these files?

Lab01-01.dll :

From my readings of functions it looks like Backdoor.

Lab01-01.exe :

The **CreateFileMappingA** function creates a memory-mapped file and allocates an area in system memory to store the allocated file. The file is stored in system memory and is represented as a temporary memory file, allowing for easy access and control.

The **MapViewOfFile** function maps a memory-mapped file created by the **CreateFileMappingA** function to an area in the working memory of a given application process. In other words, the function assigns part of the temporary file stored in memory to the application process that is making the binding.

When finished working with the custom region, the program should use the **UnmapViewOfFile** function to release the custom region and return the used resources to the system.

Lab 1-2

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

- 54 security vendors and 1 sandbox flagged this as file malicious

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

Popular threat label	trojan.ulise/trojanclicker	Threat categories	image, downloader	Family labels	ulise, trojanclicker, startpage
----------------------	----------------------------	-------------------	-------------------	---------------	---------------------------------

Security vendors' analysis ⓘ Do you want to automate checks?

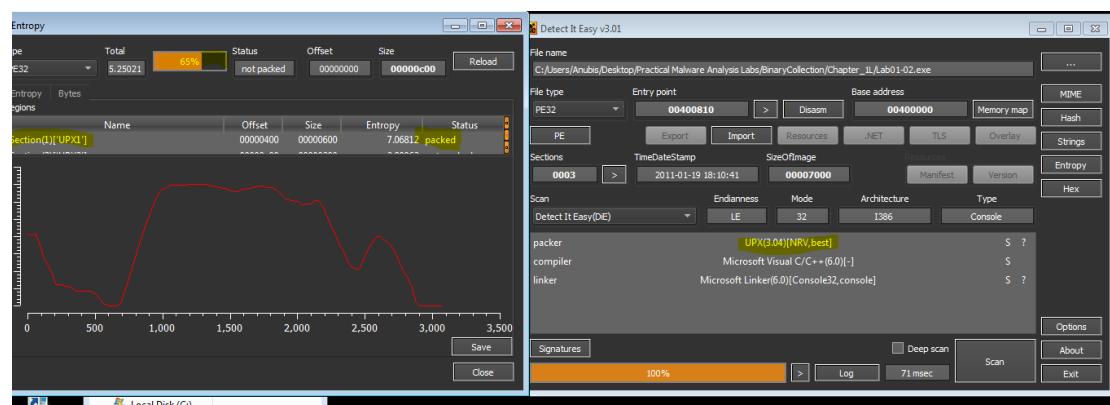
AhnLab-V3	Trojan.Win32.StartPage.C26214	Alibaba	TrojanClicker.Win32/Generic.1ba1980f
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan.Win32.SGeneric
Arcabit	Trojan.Ser.Ulise.216	Avast	Win32.Malware-gen
AVG	Win32.Malware-gen	Avira (no cloud)	TR/Downloader.Gen
Baidu	Win32.Trojan-Clicker.Agent.ad	BitDefender	Gen.Variant.Ser.Ulise.216
BitDefenderTheta	Gen:NN.ZexaF.36164.amGfaWi867f	ClamAV	Win.Malware.Agent-6350563-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cyren	Malicious (score: 100)	Cyren	W32/Agent.DJC.gen/Eldorado
DeepInstinct	MALICIOUS	DrWeb	Trojan.Click3.12740

-> 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

Using PEID , DIE.

PEID : not detected

DIE :



Type of packed UPX

```

C:\Users\Anubis\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>upx -d unpacked-lab01-02.exe
Ultimate Packer for executables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020
-----
File size      Ratio      Format      Name
-----
16384 <-      3072      18.75%      win32/pe      unpacked-lab01-02.exe
Unpacked 1 file.

```

We will notice a difference in space between the compressed file lab01-02.exe and the unpacked-lab01-02 file.exe

Lab01-01.dll	12/19/2010 11:16 ...	Application extens...	160 KB
Lab01-01.exe	1/8/2012 2:19 AM	Application	16 KB
Lab01-02.exe	1/19/2011 11:10 AM	Application	3 KB
Lab01-03.exe	3/26/2011 7:54 AM	Application	5 KB
Lab01-04.exe	7/5/2011 7:16 PM	Application	36 KB
unpacked-lab01-02.exe	1/19/2011 11:10 AM	Application	16 KB

We will also notice the difference in the number of imports

Packed :

Offset	Name	Func. Count	Bound?	OriginalFirstThunk	TimeDateStamp	Forwarder	NameRVA	FirstThunk
A00	KERNEL32.DLL	6	FALSE	0	0	0	6098	6064
A14	ADVAPI32.dll	1	FALSE	0	0	0	60A5	6080
A28	MSVCRT.dll	1	FALSE	0	0	0	60B2	6088
A3C	WININET.dll	1	FALSE	0	0	0	60BD	6090

Unpacked :

Offset	Name	Func. Count	Bound?	OriginalFirstThunk	TimeDateStamp	Forwarder	NameRVA	FirstThunk
208C	KERNEL32.DLL	9	FALSE	0	0	0	216C	2010
20A0	ADVAPI32.dll	3	FALSE	0	0	0	2179	2000
20B4	MSVCRT.dll	13	FALSE	0	0	0	2186	2038
20C8	WININET.dll	2	FALSE	0	0	0	2191	2070

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

imports (9)	flag (3)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (5)	type (1)	ordinal (0)	library (4)
CreateServiceA	x	n/a	0:00000120	0 (0x0000)	services	implicit	-	ADVAPI32
InternetOpenA	x	n/a	0:00000136	0 (0x0000)	network	implicit	-	WININET
VirtualProtect	x	n/a	0:000000E6	0 (0x0000)	memory	implicit	-	KERNEL32
VirtualAlloc	-	n/a	0:000000F6	0 (0x0000)	memory	implicit	-	KERNEL32
VirtualFree	-	n/a	0:00000104	0 (0x0000)	memory	implicit	-	KERNEL32
ExitProcess	-	n/a	0:00000112	0 (0x0000)	execution	implicit	-	KERNEL32
LoadLibraryA	-	n/a	0:000000C8	0 (0x0000)	dynamic-library	implicit	-	KERNEL32
GetProcAddress	-	n/a	0:000000D6	0 (0x0000)	dynamic-library	implicit	-	KERNEL32
exit	-	n/a	0:00000130	0 (0x0000)	-	implicit	-	MSVCRT

CreateServiceA – InternetOpenA – GetProcAddress – LoadLibraryA – ExitProcess – exit .

He runs the Internet and creates a service for him and loads the library and uses functions and operations in a malicious way and then closes the processes and functions and then closes the malicious file.

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

Host : not Detected.

Network : <http://www.malwareanalysisbook.com> → is opened by function InternetOpenUrl

encoding (2)	size (bytes)	location	flag (4)	label (31)	group (6)	value (79)
ascii	19	0x000021CA	-	import	synchronization	CreateWaitableTimer
ascii	9	0x000021EE	-	import	synchronization	OpenMutex
ascii	16	0x000021FA	-	import	synchronization	SetWaitableTimer
ascii	19	0x0000220C	-	import	synchronization	WaitForSingleObject
ascii	11	0x00002222	-	import	synchronization	CreateMutex
ascii	13	0x0000223E	×	import	services	CreateService
ascii	26	0x0000224E	×	import	services	StartServiceCtrlDispatcher
ascii	13	0x0000225C	-	import	services	OpenSCManager
ascii	11	0x00002191	-	library	network	WININET.dll
ascii	15	0x0000232C	×	import	network	InternetOpenUrl
ascii	12	0x0000233E	×	import	network	InternetOpen
ascii	20	0x000021A0	-	import	file	SystemTimeToFileTime
ascii	11	0x000021E0	-	import	execution	ExitProcess
ascii	12	0x00002230	-	import	execution	CreateThread
ascii	17	0x00002186	-	import	dynamic-library	GetModuleFileName
ascii	34	0x00003030	-	url-pattern	-	http://www.malwareanalysisbook.com
ascii	12	0x0000216C	-	library	-	KERNEL32.dll
ascii	12	0x00002179	-	library	-	ADVAPI32.dll
ascii	10	0x00002186	-	library	-	MSVCRT.dll
ascii	11	0x00002284	-	import	-	_XcptFilter
ascii	13	0x00002298	-	import	-	_p_initenv
ascii	13	0x000022A8	-	import	-	_getmainargs
ascii	9	0x000022B8	-	import	-	_initterm
ascii	16	0x000022C4	-	import	-	_setusermatherr
ascii	12	0x000022D6	-	import	-	_adjust_fdiv

Lab 1-3

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

- 60 security vendors and no sandboxes flagged this file as malicious.

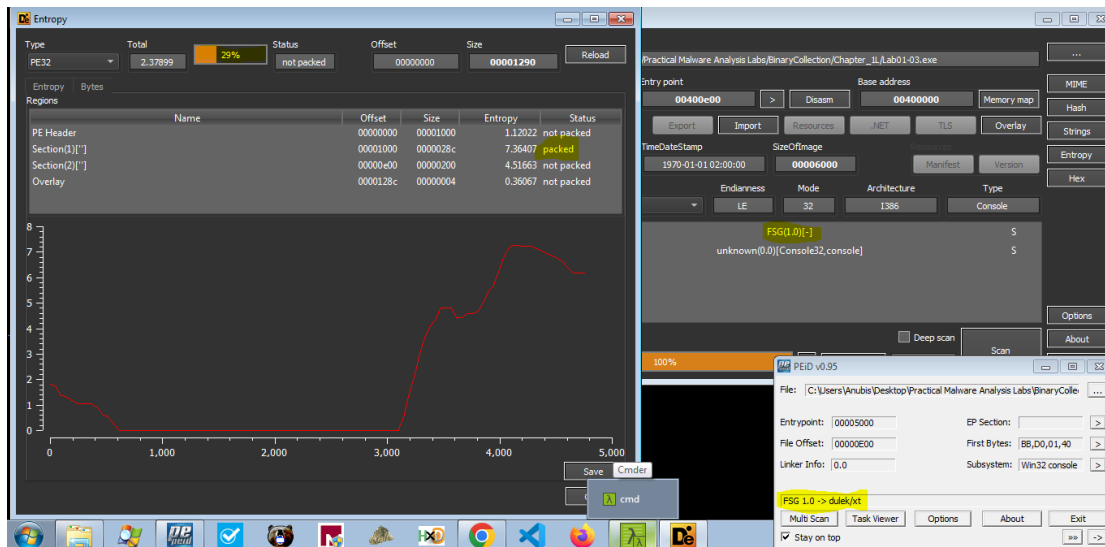
- type of malware : spyware

- rate of file 60/70

AhnLab-V3	⚠ Trojan/Win.Generic.R427327	Alibaba	⚠ TrojanClicker.Win32/Tnega.3bb840a6
ALYac	⚠ Gen:Variant.Graftor.968808	Antiy-AVL	⚠ Trojan/Win32.SGeneric
Arcabit	⚠ Trojan.Graftor.DEC868	Ayast	⚠ Win32.Malware-gen
AVG	⚠ Win32.Malware-gen	Baidu	⚠ Win32.Trojan-Clicker.Agent.z
BitDefender	⚠ Gen:Variant.Graftor.968808	BitDefenderTheta	⚠ Gen:NN.ZexaF.36132.ambdaODILcf
Bkav Pro	⚠ W32.AIDetectNet.01	ClamAV	⚠ Win.Malware.Emoney.9937593-0
CrowdStrike Falcon	⚠ Win/malicious_confidence_100% (W)	Cylance	⚠ Unsafe
Cynet	⚠ Malicious (score: 100)	Cyren	⚠ W32/SuspPack.DH.genEldorado
DeepInStinct	⚠ MALICIOUS	DrWeb	⚠ Trojan.Click2.16518
Elastic	⚠ Malicious (high Confidence)	Emmisoft	⚠ Gen:Variant.Graftor.968808 (B)
eScan	⚠ Gen:Variant.Graftor.968808	ESET-NOD32	⚠ Win32/TrojanClicker.Agent.NVN
Fortinet	⚠ W32/WebDown.E76Atr	GData	⚠ Gen:Variant.Graftor.968808

-> 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.

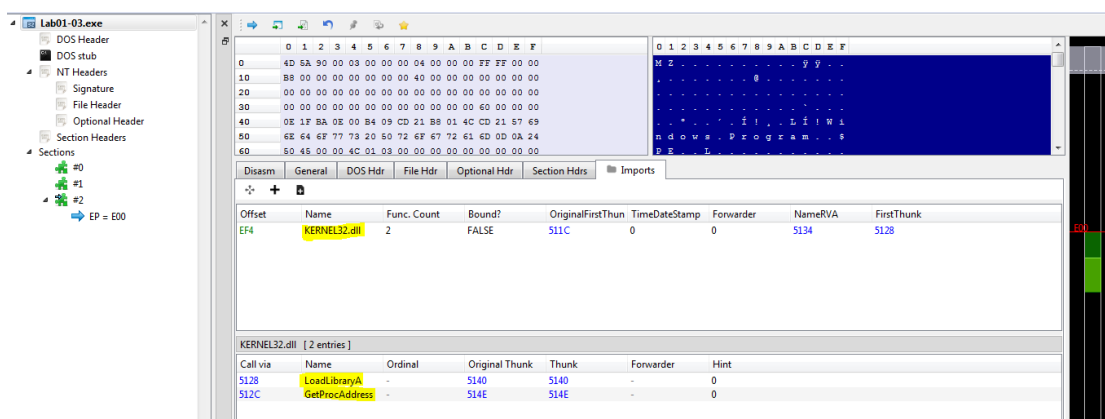
- using by PEID , DIE



- Entropy = 26 % .
- The part of file is packed .
- Type of packed = FSG 1.0
- PEID , DIE is detected .
- I have not studied unpack FSG wait for chapter 8.

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

Using : PE-bear



Imports → LoadLibraryA , GetProcAddress

Libraries → KERNEL32.dll

The file is packed

Creates a process and loads a library.

I can't answer more than this because I don't have the file unpack.

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

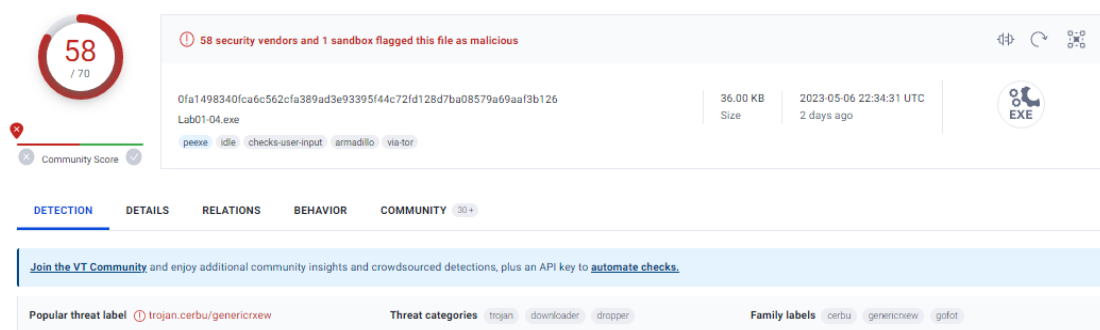
I can't find this information because I don't have the unpack file.

Lab 1-4

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

- The rate in VirusTotal : 58 / 70

- Type of threat : Downloader , dropper

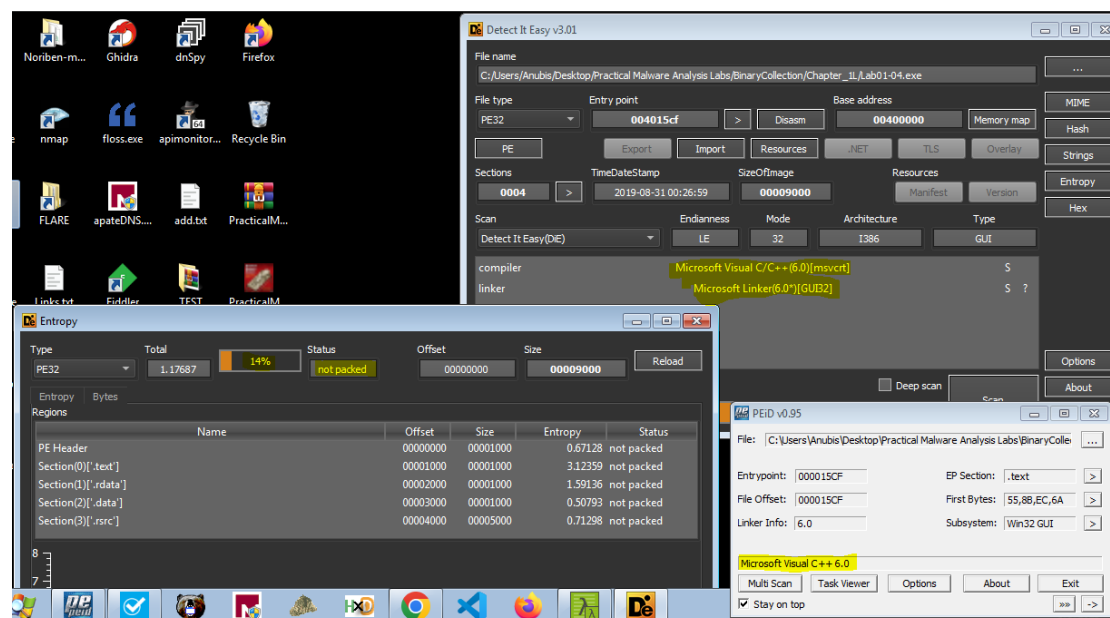


- AntiVirus detected :

Alibaba	🚫 TrojanDownloader.Win32/DownLdr.080f6...	ALYac	🚫 Gen:Variant.Cerbu.64782
Antiy-AVL	🚫 Trojan[Downloader]/Win32.AGeneric	Arcabit	🚫 Trojan.Cerbu.DFD0E
Avast	🚫 Win32:DropperX-gen [Drp]	AVG	🚫 Win32:DropperX-gen [Drp]
Avira (no cloud)	🚫 TR/Dldr.Small.romlh	BitDefender	🚫 Gen:Variant.Cerbu.64782
BitDefenderTheta	🚫 AtPacker.6911D1B71F	Bkav Pro	🚫 W32.AIDetectMalware
ClamAV	🚫 Win.Trojan.Agent-375080	CrowdStrike Falcon	🚫 Win/malicious_confidence_100% (W)
Cybereason	🚫 Malicious.f447ad	Cylance	🚫 Unsafe
Cynet	🚫 Malicious (score: 100)	Cyren	🚫 W32/Heuristic-217/Eldorado
DeepInSight	🚫 MALICIOUS	DrWeb	🚫 Trojan.DownLoader5.60705
Elastic	🚫 Malicious (high Confidence)	Emsisoft	🚫 Gen:Variant.Cerbu.64782 (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.

- using PEID , DIE :



- Status : Not Packed

- signature : Microsoft Visual C/C++[5.0]

- Entropy in DIE : 14%

-> When was this program compiled?

- using pestudio : Fri Aug 22:26:59 | UTC

- de -> virustotal (error) -> dos-stub (64 bytes) -> rich-header (168 bytes) -> file-header (PE0000) -> optional-header (GUI) -> directories (3) -> sections (file) -> libraries (3) -> imports (flag) -> exports (n/a) -> tls-callback (n/a) -> .NET (n/a) -> resources (executable) -> strings (167) * -> debug (n/a) -> manifest (n/a) -> version (n/a) -> overlay (n/a)	characteristics		0x010F	
	dynamic-link-library	0x0000	false	
	32-bit words support	0x0100	true	
	file-can-be-executed	0x0002	true	
	system-image	0x0000	false	
	large-address-aware	0x0000	false	
	debug-stripped	0x0000	false	
	line-stripped-from-file	0x0004	true	
	local-symbols-stripped-from-file	0x0008	true	
	relocation-stripped	0x0001	true	
	uniprocessor	0x0000	false	
	bytes-of-machine-words-reversed-Low	0x0000	false	
	bytes-of-machine-words-reversed-Hi	0x0000	false	
	media-run-from-swap	0x0000	false	
	network-run-from-swap	0x0000	false	
	general			
	compiler-stamp	0x5D69A283	Fri Aug 30 22:26:59 2019 UTC	
	size-of-optional-header	0x00E0	224 bytes	
	signature	0x00004550	PE00	
	machine	0x014C	Intel-386	
	sections	0x0004	4	
	pointer-symbol-table	0x00000000	0x00000000	
	number-of-symbols	0x00000000	0x00000000	

- open pestudio go to file-header found here.

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

- open pestudio go to imports.

imports (34)	flag (8)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (6)	type (1)	ordinal (0)	library
OpenProcessToken	x	0x000022CC	0x000022CC	322 (0x0142)	security	implicit	-	ADVA
LookupPrivilegeValueA	x	0x000022B4	0x000022B4	245 (0x00F5)	security	implicit	-	ADVA
AdjustTokenPrivileges	x	0x0000229C	0x0000229C	23 (0x0017)	security	implicit	-	ADVA
SizeofResource	-	0x00002214	0x00002214	661 (0x0295)	resource	implicit	-	KERN
FindResourceA	-	0x00002236	0x00002236	163 (0x00A3)	resource	implicit	-	KERN
LoadResource	-	0x00002226	0x00002226	455 (0x01C7)	resource	implicit	-	KERN
GetWindowsDirectoryA	-	0x0000225A	0x0000225A	381 (0x017D)	reckoning	implicit	-	KERN
WriteFile	x	0x000021FA	0x000021FA	735 (0x02DF)	file	implicit	-	KERN
CreateFileA	-	0x00002206	0x00002206	52 (0x0034)	file	implicit	-	KERN
MoveFileA	x	0x00002272	0x00002272	477 (0x01DD)	file	implicit	-	KERN
GetTempPathA	-	0x0000227E	0x0000227E	357 (0x0165)	file	implicit	-	KERN
WinExec	x	0x000021F0	0x000021F0	723 (0x02D3)	execution	implicit	-	KERN
CreateRemoteThread	x	0x000021B8	0x000021B8	70 (0x0046)	execution	implicit	-	KERN
GetCurrentProcess	-	0x000021A4	0x000021A4	247 (0x00F7)	execution	implicit	-	KERN
OpenProcess	x	0x00002196	0x00002196	495 (0x01EF)	execution	implicit	-	KERN
GetProcAddress	-	0x000021CE	0x000021CE	318 (0x013E)	dynamic-library	implicit	-	KERN
LoadLibraryA	-	0x000021E0	0x000021E0	450 (0x01C2)	dynamic-library	implicit	-	KERN
GetModuleHandleA	-	0x00002246	0x00002246	294 (0x0126)	dynamic-library	implicit	-	KERN
CloseHandle	-	0x00002188	0x00002188	27 (0x001B)	-	implicit	-	KERN
_snprintf	-	0x000022EE	0x000022EE	430 (0x01AE)	-	implicit	-	MSVC
_exit	-	0x00002306	0x00002306	211 (0x00D3)	-	implicit	-	MSVC
_XcptFilter	-	0x0000230E	0x0000230E	72 (0x0048)	-	implicit	-	MSVC
exit	-	0x0000231C	0x0000231C	585 (0x0249)	-	implicit	-	MSVC
_p_initenv	-	0x00002324	0x00002324	100 (0x0064)	-	implicit	-	MSVC
_getmainargs	-	0x00002334	0x00002334	88 (0x0058)	-	implicit	-	MSVC
_initterm	-	0x00002344	0x00002344	271 (0x010F)	-	implicit	-	MSVC
_returnaddress	-	0x00002350	0x00002350	131 (0x0083)	-	implicit	-	MSVC

- he used libraries : ADVAPI32.dll , KERNEL32.dll , MSVCRT.dll

- It creates a process through the **OpenProcessToken** method, loads other libraries through the **LoadLibraryA** function, creates a file, writes it, moves it to hide it through the **WriteFile**, **CreateFileA**, **MoveFileA** function, and does many other harmful things.

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

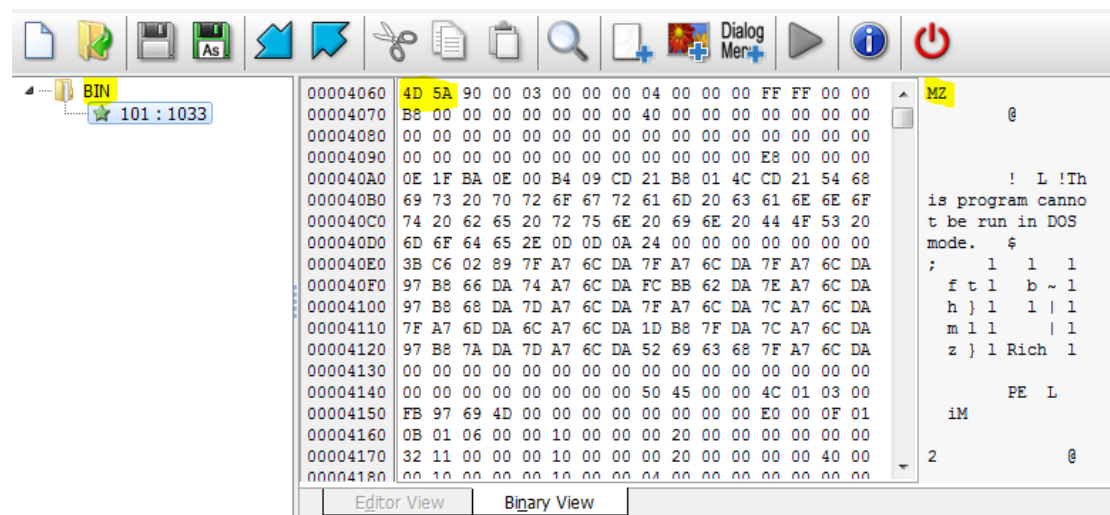
- open pestudio go to strings found here.

Resource	Offset	Value	Type	Import	Export	String
resources (executable)	11	0x000021E2	import	dynamic-library		LoadLibrary
strings (167)	15	0x00002248	import	dynamic-library		GetModuleHandle
debug (n/a)	12	0x00003010	utility			winlogon.exe
manifest (n/a)	51	0x000070A4	url-pattern			http://www.practicalmalwareanalysis.com/updater.exe
version (n/a)	12	0x0000228E	library			KERNEL32.dll
overlay (n/a)	4	0x00000000				

- URL : <http://www.practicalmalwareanalysis.com/updater.exe>

-> 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?

- open Resource Hacker go to the folder Inside him file (source).



- using pestudio there the information about this file :

property	value
md5	A4C93CA41DC5E38EA92D6BB10DED4CD6
sha1	F60493D3311351F51A6D397908462618829C6548
sha256	BD9C56DE7C72E14A1A93B38F096B0766DA49A154B08D3756F99B9F9AA8F42944
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z @
file-size	36864 bytes
entropy	1.178
imphash	AADE0EA6FBDCD9B8E96FE999CAE6F603
signature	Microsoft Visual C++ v6.0
tooling	Visual Studio 6.0
entry-point	55 8B EC 6A FF 68 98 20 40 00 68 10 17 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 20 53
file-version	n/a
description	n/a
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	Fri Aug 30 22:26:59 2019 UTC
debugger-stamp	n/a
resources-stamp	0x00000000
import-stamp	0x00000000
exports-stamp	n/a

Finally Chapter 1