

# Practical Malware Analysis Chapter 3

Lab 3-1 :

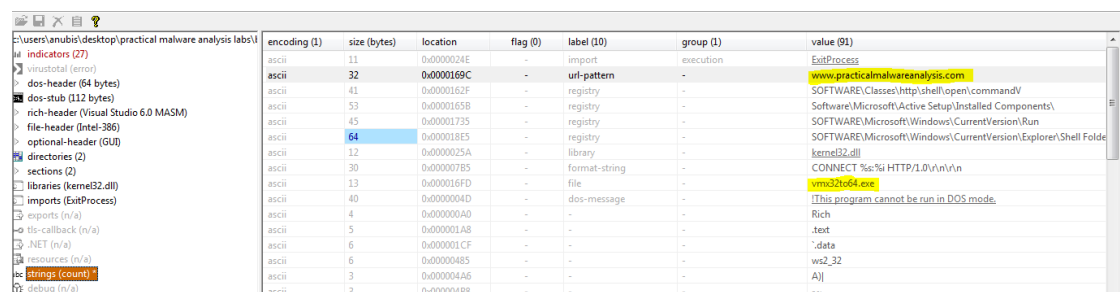
->What are this malware's imports and strings?

The number of imports is very small, this shows that the malware is compressed and opfused



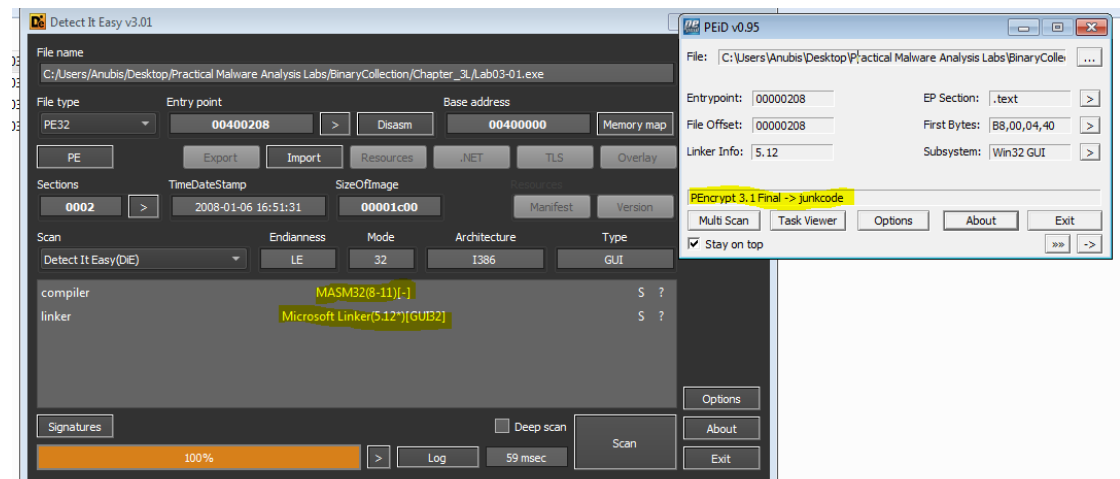
imports (1)	flag (0)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (1)	type (1)	ordinal (0)	library (1)
ExitProcess	-	0x0000024C	0x0000024C	128 (0x0080)	execution	implicit	-	kernel32.dll

Through strings we found this IOC: [www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com) and I also found this [vmx32to64.exe](#) is an executable file um, I think it authorizes something from 32 to 64, but as we progress, we'll find out what it is.



encoding (1)	size (bytes)	location	flag (0)	label (10)	group (1)	value (91)
ascii	11	0x0000024E	-	import	execution	ExitProcess
ascii	32	0x0000169C	-	url-pattern	-	www.practicalmalwareanalysis.com
ascii	41	0x0000162F	-	registry	-	SOFTWARE\Classes\http\shell\open\commandV
ascii	53	0x00001658	-	registry	-	Software\Microsoft\Active Setup\Installed Components\
ascii	45	0x00001735	-	registry	-	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
ascii	64	0x000018E5	-	registry	-	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
ascii	12	0x0000025A	-	library	-	kernel32.dll
ascii	30	0x000007B5	-	format-string	-	CONNECT %s: %s HTTP/1.0\n\n
ascii	13	0x000016FD	-	file	-	vmx32to64.exe
ascii	40	0x0000004D	-	dos-message	-	[This program cannot be run in DOS mode.
ascii	4	0x00000040	-	-	-	Rich
ascii	5	0x000001A8	-	-	-	.text
ascii	6	0x000001CF	-	-	-	.data
ascii	6	0x00000485	-	-	-	ws2_32
ascii	3	0x000004A6	-	-	-	A
ascii	3	0x000004B8	-	-	-	~_

PEID discovered that the file was compressed but DIE did not detect that it was compressed, hmm.



-> What are the malware's host-based indicators?

Not detected.

-> Are there any useful network-based signatures for this malware? If so, what are they?

Yes .

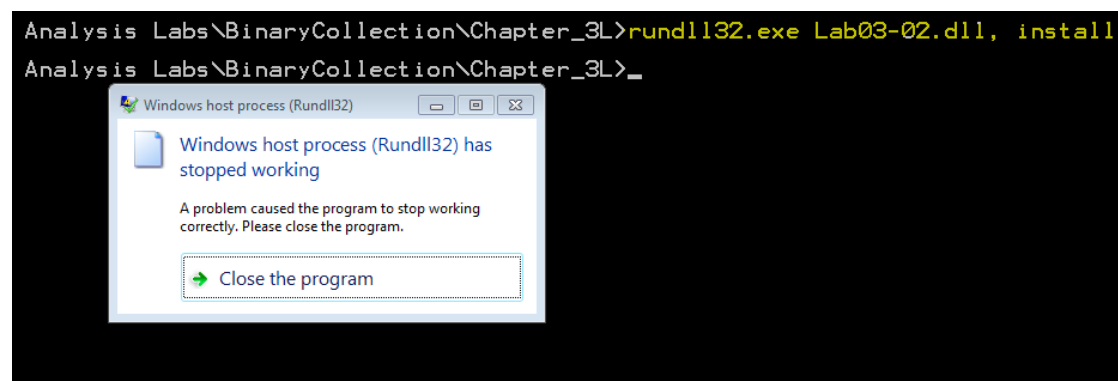
IOCs : [www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com)

Lab 3-2 :

**Note :** I can not run this file because it works on Windows XP and I am using Windows 7 but I try to extract any information.

-> How can you get this malware to install itself ?

Using this command, I can install the malware, but as we mentioned, the malware does not respond due to the version of Windows.



Ordinal	Function RVA	Name Ordinal	Name RVA	Name
N/A	00004D38	00004D58	00004D4C	00004D9E
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	00004706	0000	00005969	Install
00000002	00003196	0001	00005978	ServiceMain
00000003	00004B18	0002	00005984	UninstallService
00000004	00004B0B	0003	00005995	installA
00000005	00004C2B	0004	0000599E	uninstallA

-> How would you get this malware to run after installation ?

To run the dll file by typing this command in the cmd window:

**rundll32.exe lab3-2.exe, NameOfExports**

but as we mentioned, the malware does not respond due to the version of Windows.

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
N/A	00004D38	00004D58	00004D4C	00004D9E
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	00004706	0000	00005969	Install
00000002	00003196	0001	00005978	ServiceMain
00000003	00004B18	0002	00005984	UninstallService
00000004	00004B0B	0003	00005995	installA
00000005	00004C2B	0004	0000599E	uninstallA

-> How can you find the process under which this malware is running?

Sorry, I cannot solve it because of the incompatibility of the Windows version.

-> Which filters could you set in order to use procmon to glean information?

Sorry, and I cannot solve it because of the incompatibility of the Windows version.

-> What are the malware's host-based indicators ?

Intranet Network Awareness (INA+)  
Depends INA+, Collects and stores network configuration and location information, and notifies applications when this information changes.

-> Are there any useful network-based signatures for this malware ?

I am find this Possible IOCs :

serve.html

practicalmalwareanalysis.com

This is my analysis of this lab, but that's not all. There may be more, but I couldn't run this file because my version of Windows was released.

Lab 3-3 :

**Note :** I can not run this file because it works on Windows XP and I am using Windows 7.

Lab 3-4 :

-> What happens when you run this file?

Ooooooh, he's hide.

I think he is deleted by itself

-> What is causing the roadblock in dynamic analysis ?

Because it does not work on virtual machine (sandboxes) and therefore will remove itself.

-> Are there other ways to run this program ?

I think there are no ways but to run it on your device and therefore the device will be damaged and this is not recommended.