

Practical Malware Analysis Lab 1-4

Questions

1. Upload the Lab01-04.exe file to <https://www.VirusTotal.com/>. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indications? If the file is packed, unpack it if possible.
3. When was this program compiled?
4. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
5. What host- or network-based indicators could be used to identify this malware on infected machines?
6. 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?

Question 1

[Result for Lab01-04.exe](#)

MD5: 625ac05fd47adc3c63700c3b30de79ab

This EXE definitely seems malicious. The file was detected by 52/66 engines.

Question 2

This file does not seem to be packed. The virtual size is smaller than the RAW size.

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	1824	4096	3.12	77df9f7ebc4a2bc4bdf2b454d7635aee	419793.88
.rdata	8192	978	4096	1.59	d630e1eb49ed821e38202aefef911a39	729061.13
.data	12288	332	4096	0.51	d9a3822a7733a76776d8b6e64e364b9d	946649.25
.rsrc	16384	16480	20480	0.71	398569177d4d82090d3e1747be560f9a	4618603

Question 3

Compilation Timestamp: 2019-08-30 22:26:59 (incorrect)

Question 4

This file imports 3 DLLs kernel32.dll, advapi32.dll and MSVCRT.dll

Kernel32.dll

[GetProcAddress](#)

[LoadLibraryA](#)

[WinExec](#)

[WriteFile](#)
[CreateFileA](#)
[SizeofResource](#)
[CreateRemoteThread](#)
[FindResourceA](#)
[GetModuleHandleA](#)
[GetWindowsDirectory](#)
[MoveFileA](#)
[GetTempPathA](#)
[GetCurrentProcess](#)
[CloseHandle](#)
[LoadResource](#)

advapi32.dll

[OpenProcessToken](#)
[LookupPrivilegeValue](#)
[AdjustTokenPrivileges](#)

MSVCRT.dll

Nothing super important

Strings Lab01-04.exe results in

BIN

#101

URLDownloadToFileA

urlmon.dll

\winup.exe

\system32\wupdmgrd.exe

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

This exe definitely works with files it references multiple file handling functions. The program also loads some type of resource. Functions such as [LookupPrivilegeValue](#) and [AdjustTokenPrivileges](#) suggest that maybe it modifies some type of privilege value. The malware also downloads a file using URLDownloadToFileA possibly <http://www.practicalmalwareanalysis.com/updater.exe> maybe some type of updater for the malware. **WinExec** is used to start applications so maybe it starts [\system32\wupdmgrd.exe](#) and [\winup.exe](#). Winup is associated with malware and modifies processes.

Question 5

I would look for any extra files in your tmp directory because the malware seems to request for the specific directory [GetTempPathA](#). If the file Winup is in your C drive this could also mean

you are infected. I would also watch web traffic to the website
<http://www.practicalmalwareanalysis.com/updater.exe>.

Question 6

When loading the malware into Resource Hacker I saw one resource: BIN 101 : 1033.
Extracting it gave me the file BIN101. When using the strings command it displayed.
URLDownloadToFileA

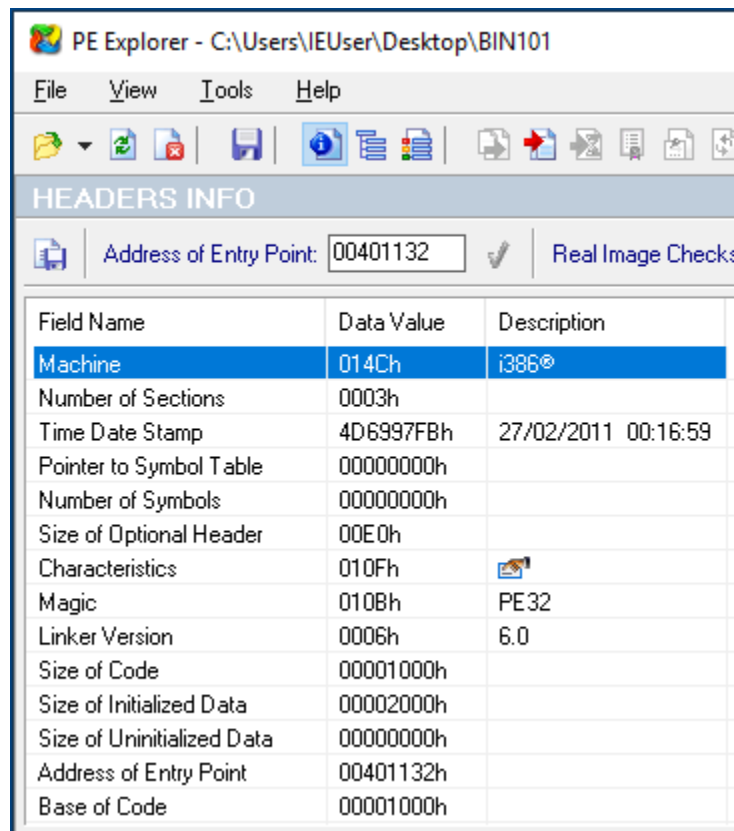
\\winup.exe


\\system32\\wupdmgrd.exe

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

It looks like a smaller copy of the malware maybe this is for just updating it?

When analysing the BIN in PE Explorer we can see the compilation timestamp is now
27/02/2011.



Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0003h	
Time Date Stamp	4D6997FBh	27/02/2011 00:16:59
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	010Fh	
Magic	010Bh	PE32
Linker Version	0006h	6.0
Size of Code	00001000h	
Size of Initialized Data	00002000h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	00401132h	
Base of Code	00001000h	