

CSE 434S – Reverse Engineering and Malware Analysis

HW1 - Basic Static Analysis

Download the archive file for this assignment from Canvas and extract the archive to a virtual machine (the archive password is "infected"). The archive contains Sample1 and Sample2, which are malware samples. **Do NOT run them!**

The lecture slides and Chapter 1 and Appendix A in the textbook, as well as the slides on Windows API calls and the Resource Hacker program posted to the assignment Canvas page, will be helpful for completing the assignment.

Important instructions for your writeup:

- Use this document to answer the questions.
- Explain your answers and add repeatable notes as you did in the similar lab exercise.
- Take screenshots when needed, but note that screenshots cannot replace your words.
- A good explanation doesn't necessarily mean a lengthy one. Be concise!
- Assume that the reader doesn't have the book or our slides. It doesn't mean that you need to explain the theory, but it means that you cannot answer a question by saying "I followed instructions on page 3 and slide 15".
- Whenever possible, describe your steps in first person.

CSE434S

Part 1: Sample1

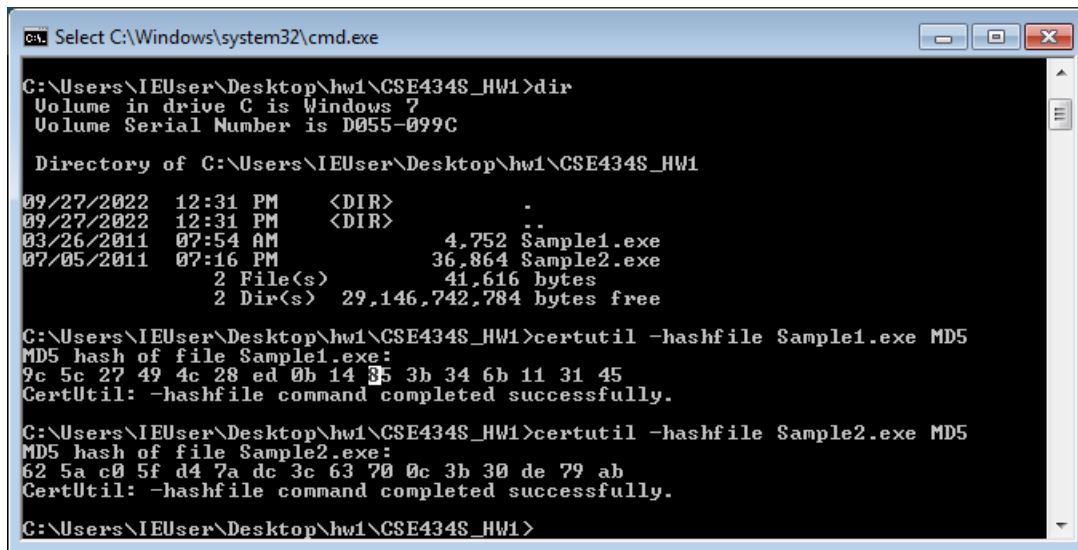
1) What is the MD5 of Sample1? (2 pts)

C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>certutil -hashfile Sample1.exe MD5

MD5 hash of file Sample1.exe:

9c 5c 27 49 4c 28 ed 0b 14 85 3b 34 6b 11 31 45

CertUtil: -hashfile command completed successfully.



```
C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>dir
Volume in drive C is Windows 7
Volume Serial Number is D055-099C

Directory of C:\Users\IEUser\Desktop\hw1\CSE434S_HW1

09/27/2022  12:31 PM    <DIR>          .
09/27/2022  12:31 PM    <DIR>          ..
03/26/2011  07:54 AM             4,752 Sample1.exe
07/05/2011  07:16 PM            36,864 Sample2.exe
               2 File(s)             41,616 bytes
               2 Dir(s)  29,146,742,784 bytes free

C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>certutil -hashfile Sample1.exe MD5
MD5 hash of file Sample1.exe:
9c 5c 27 49 4c 28 ed 0b 14 85 3b 34 6b 11 31 45
CertUtil: -hashfile command completed successfully.

C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>certutil -hashfile Sample2.exe MD5
MD5 hash of file Sample2.exe:
62 5a c0 5f d4 7a dc 3c 63 70 0c 3b 30 de 79 ab
CertUtil: -hashfile command completed successfully.

C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>
```

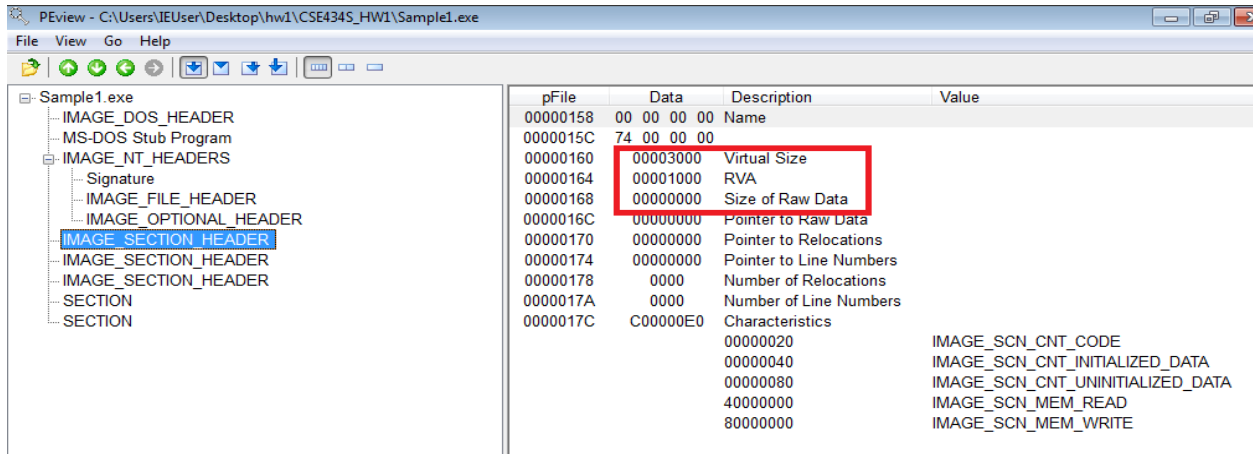
CSE434S

2) Is Sample1 packed? List three indicators to justify your answer. If packed, what packer was used to pack Sample2? (5 pts)

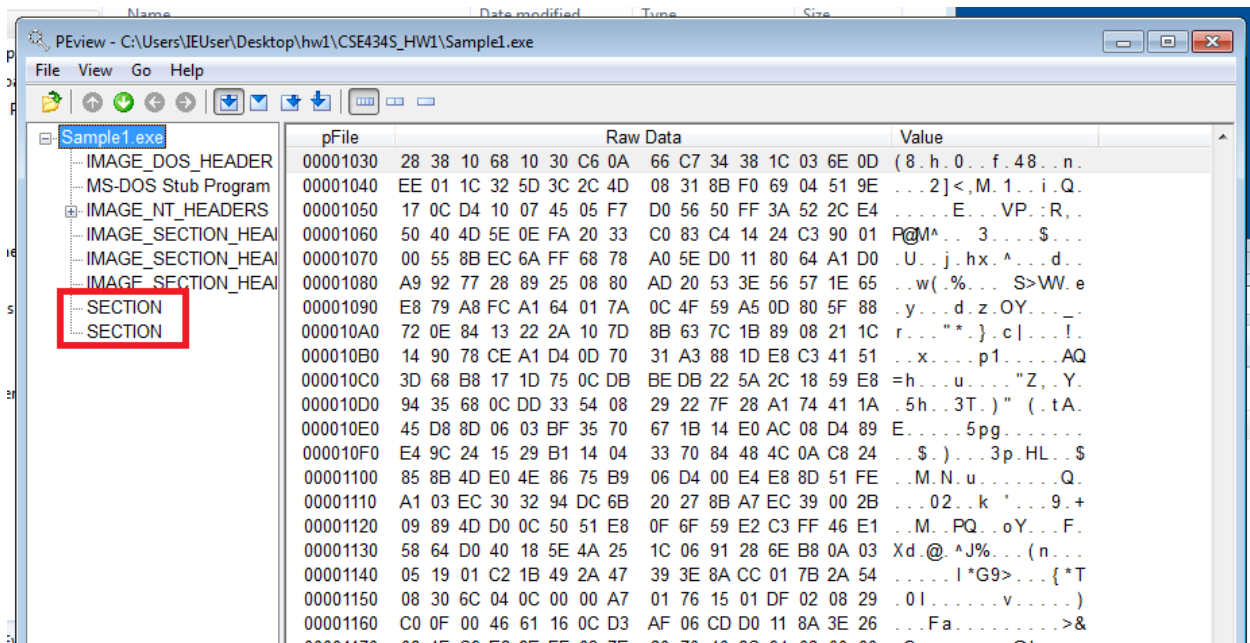
Yes, it is packed! And the packer is FSG 1.0 -> dulek/xt.

I found 3 indicators by using PeiD and Pevview.

The first indicator is that Virtual Size is much larger than Size of Raw data. In fact Size of Raw data is zero!

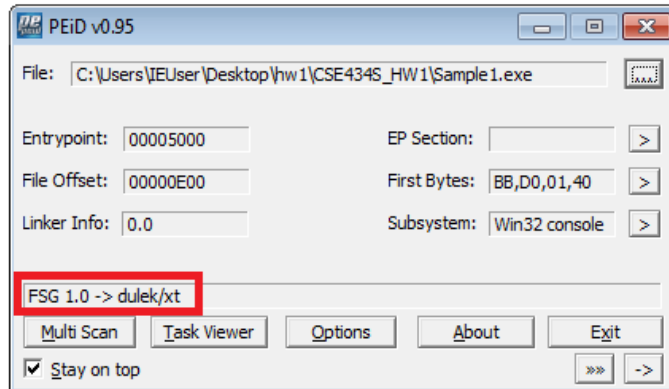


Second indicator is that there was no common PE sections for .text, .rdata, .data, .rsrc.



CSE434S

And finally, I can see the packer's name when I opened the file with PeiD. The packer is FSG 1.0 -> dulek/xt.




3) If needed, unpack Sample1 and describe how you unpacked it. What is the md5 of the unpacked file? (3 pts)

The file is packed using FSG 1.0 -> dulek/xt and I haven't learn how to unpack it. Of course, I don't know the md5 checksum of the file.

4) What is the exact date and time (to the second) that Sample1 was compiled? (2 pts)

I cannot find out the compile time because the file is packed. And I also analyze the file using Virus total, but there was no compilation time.



7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec

1a016-02.exe

2392_3@2392

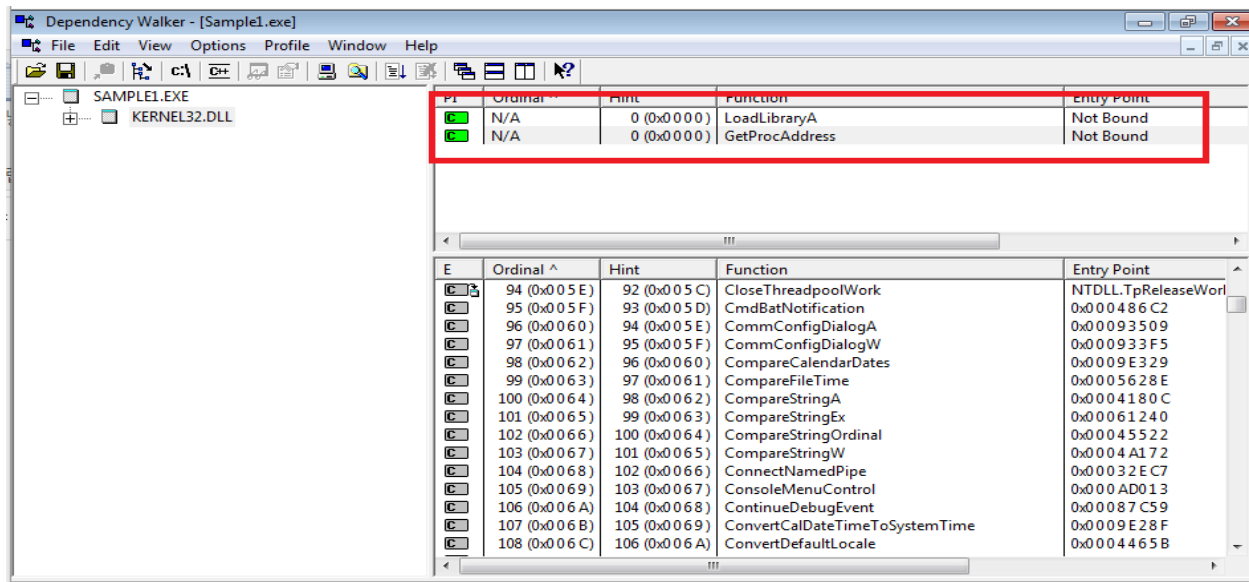
▼

Portable Executable Info ⓘ				
Sections				
Name	Virtual Address	Virtual Size	MD5	Chi2
t	4096	12288	d41d8cd98f00b204e9800998ecf8427e	-1
ta	16384	4096	dcbb3117347a183b93cc9e50e09abd92	580.1
a	20480	4096	83d2bc9613dfc4bc5c714214023f386f	27890

CSE434S

5) Investigate the Windows API functions that Sample1 imports. List two functions that suggest that Sample1 can check whether it is being debugged. How can a malware Sample use each of these functions to check whether it is being debugged? (5 pts)

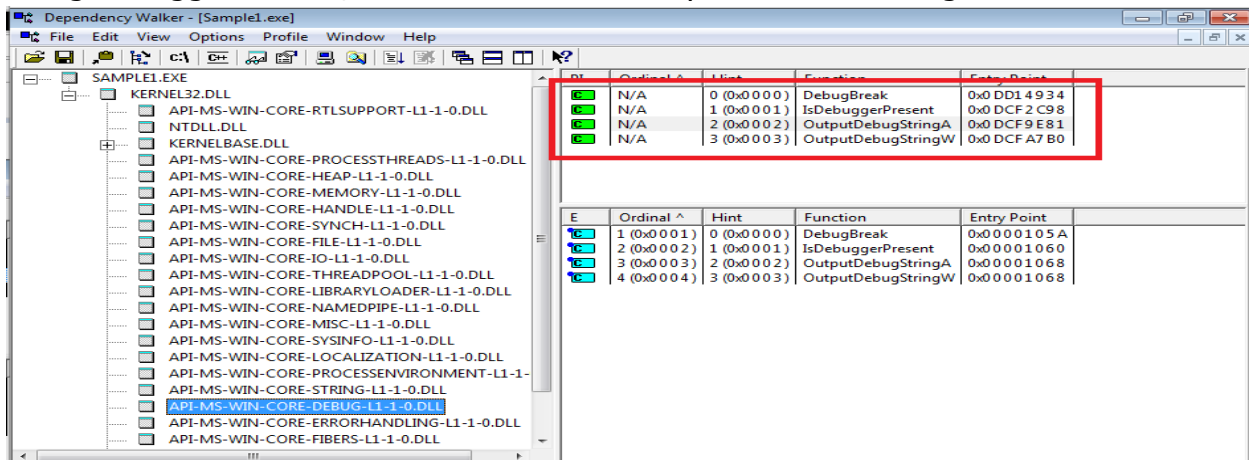
First, Sample1 imports two functions. 'LoadLibraryA' 'GetProcAddress'. With these two imports, I can tell that Sample1 uses Runtime Linking which is common in malware.



And it imports several functions about debugging. I can see the list when I looked it up using Dependency walker.

IsDebuggerPresent, OutputDebugString

Lastly, I think IsDebuggerPresent is a function which can tell whether the program is being debugged or not. Maybe, Sample1 calls this function to check the status of being debugged or not, so it can act differently if it is in a debug situation.



CSE434S

6) Which section in Sample1 contains executable code? What is the virtual size of this section? (5 pts)

Usually, the executable code's location is in Common PE Sections but the file is packed. Unless unpacking the file, it is hard to find out which section is.

7) Do any of Sample1's imports suggest that it is able to connect to the internet? Do any of the strings in Sample1 suggest that it is able to connect to the internet? Why is this suspicious? (10 pts)

Unless unpacking the file, it is hard to find out Sample1 uses internet connection or not. And I cannot find strings look like an IP address as well. Since it is packed, I looked through the whole strings in a file, I couldn't find anything suspicious because all of those strings looked meaningless.

8) Can you say what this malware does? You will be graded for providing educated conclusions based on your findings, and not necessarily for the correctness of your conclusions. (3 points)

Since it is packed and I don't know how to unpack this file at the moment, I have to say the I'm not sure about what it does. And also, I can see only two functions imported, LoadLibraryA, GetProcAddress. It is a sign of Runtime Linking and is common in malware program. I only assume the program will call libraries runtime basis.

CSE434S

Part 2: Sample2

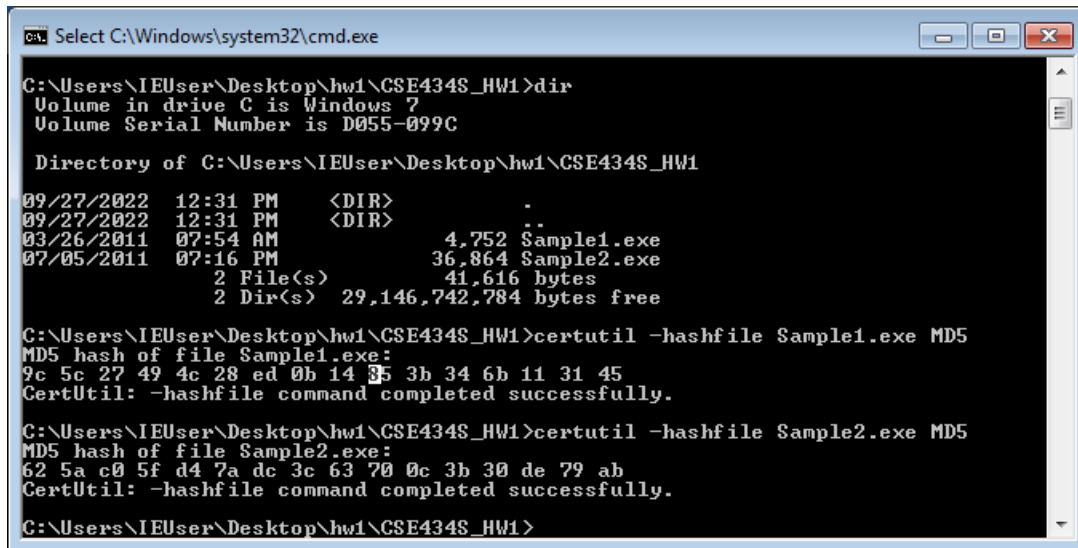
1) What is the MD5 of Sample2? (2 pts)

C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>certutil -hashfile Sample2.exe MD5

MD5 hash of file Sample2.exe:

62 5a c0 5f d4 7a dc 3c 63 70 0c 3b 30 de 79 ab

CertUtil: -hashfile command completed successfully.



```

C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>dir
Volume in drive C is Windows 7
Volume Serial Number is D055-099C

Directory of C:\Users\IEUser\Desktop\hw1\CSE434S_HW1

09/27/2022  12:31 PM    <DIR>          .
09/27/2022  12:31 PM    <DIR>          ..
03/26/2011  07:54 AM             4,752 Sample1.exe
07/05/2011  07:16 PM             36,864 Sample2.exe
               2 File(s)              41,616 bytes
               2 Dir(s)  29,146,742,784 bytes free

C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>certutil -hashfile Sample1.exe MD5
MD5 hash of file Sample1.exe:
9c 5c 27 49 4c 28 ed 0b 14 35 3b 34 6b 11 31 45
CertUtil: -hashfile command completed successfully.

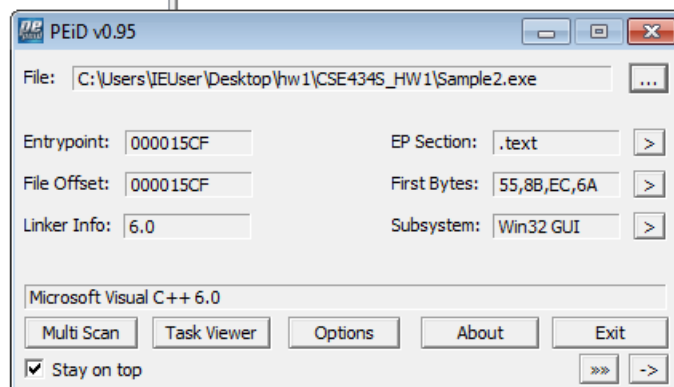
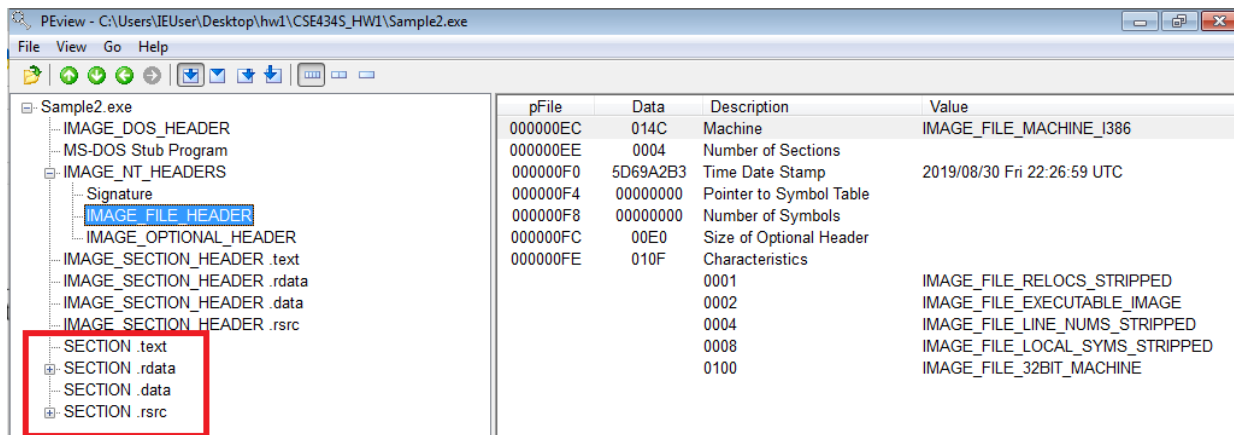
C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>certutil -hashfile Sample2.exe MD5
MD5 hash of file Sample2.exe:
62 5a c0 5f d4 7a dc 3c 63 70 0c 3b 30 de 79 ab
CertUtil: -hashfile command completed successfully.

C:\Users\IEUser\Desktop\hw1\CSE434S_HW1>
```

CSE434S

2) Is Sample 2 packed? List three indicators to justify your answer. If packed, what packer was used to pack Sample2? (5 pts)

I don't think it's packed. I can see the SECTION HEADER clearly using PView and there was no packing information with PEiD.



3) If needed, unpack Sample2 and describe how you unpacked it. What is the md5 of the unpacked file? (3 pts)

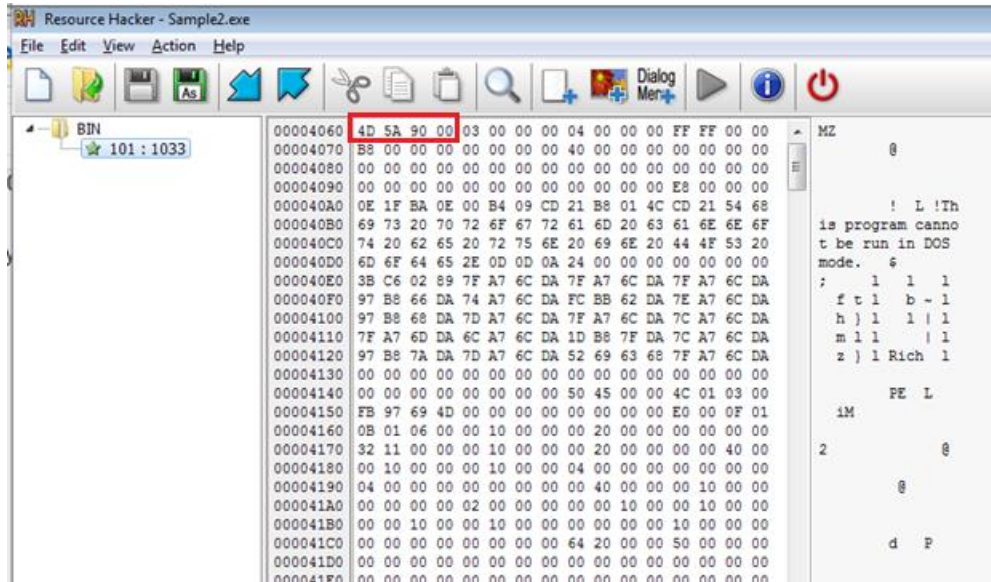
I think the file is not packed with packing tools. Therefore, the md5 is the same with original file's md5.

62 5a c0 5f d4 7a dc 3c 63 70 0c 3b 30 de 79 ab

CSE434S

4) Use Resource Hacker to investigate the first resource in the unpacked file. What are the first 4 bytes of the resource (take a screenshot)? Based on these bytes, what is the type of this file? (10 pts)

The first 4 bytes of the resource: 4D 5A 90 00



And I found out that it is a DOS executable file.

A screenshot of a web browser displaying the Wikipedia page "List of file signatures". The browser's address bar shows "en.wikipedia.org/wiki/List_of_file_signatures". The page content is a table with columns for file signatures. The entry for "4D 5A" (MZ) is highlighted with a red rectangle. The table lists various file signatures, including LZIP, cpio, DOS MZ executable, DOS ZM executable, zip, aar, and apk. The highlighted entry is for the DOS MZ executable file, which is described as "DOS MZ executable and its descendants (including NE and PE)".

			iff	
4C 5A 49 50	LZIP	0	lz	lzip compressed file ^[17]
30 37 30 37 30 37	070707	0	cpio	cpio archive file ^[18]
4D 5A	MZ	0	exe scr sys dll fon cpl iec ime rs tsp mz	DOS MZ executable and its descendants (including NE and PE)
5A 4D	ZM	0	exe	DOS ZM executable and its descendants (rare)
			zip aar apk	

CSE434S

5) Perform additional analysis on the resource file from the previous question. What do you think this file does and why is it malicious? (10 pts)



When I checked the strings in Sample2, I found several suspicious strings.

GetWindowsDirectoryA, WinExec, URLDownloadToFileA

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

From the strings I found, it will download some files from internet and try to execute it. This is typical behavior of a malicious program.

BIN	00006130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	!	!	!	!
★ 101:1033	00006140	C0 21 00 00 CC 21 00 00 E0 21 00 00 F0 21 00 00	!	!	!	!
	00006150	00 22 00 00 0E 22 00 00 20 22 00 00 00 00 00 00	!	!	!	!
	00006160	48 21 00 00 00 00 00 00 7D 01 47 65 74 57 69 6E	!	!	!	!
	00006170	64 6F 77 73 44 69 72 65 63 74 6F 72 79 41 00 00	!	!	!	!
	00006180	D3 02 57 69 6E 45 78 65 63 00 65 01 47 65 74 54	!	!	!	!
	00006190	65 6D 70 50 61 74 68 41 00 00 4B 45 52 4E 45 4C	!	!	!	!
	000061A0	33 32 2E 64 6C 6C 00 00 3E 00 55 52 4C 46 6F 77	!	!	!	!
	000061B0	6E 6C 6F 61 64 54 6F 46 69 6C 65 41 00 00 75 72	!	!	!	!
	000061C0	6C 6D 6F 6E 2E 64 6C 6C 00 00 AE 01 5F 73 6E 70	!	!	!	!
	000061D0	72 69 6E 74 66 00 4D 53 56 43 52 54 2E 64 6C 6C	!	!	!	!
	000061E0	00 00 D3 00 5F 65 78 69 74 00 48 00 5F 58 63 70	!	!	!	!
	000061F0	74 46 69 6C 74 65 72 00 49 02 65 78 69 74 00 00	!	!	!	!
	00006200	64 00 5F 5F 70 5F 5F 5F 69 6E 69 74 65 6E 76 00	!	!	!	!
	00006210	58 00 5F 5F 67 65 74 6D 61 69 6E 61 72 67 73 00	!	!	!	!
	00006220	0F 01 5F 69 6E 69 74 74 65 72 6D 00 83 00 5F 5F	!	!	!	!
	00006230	73 65 74 75 73 65 72 6D 61 74 68 65 72 72 00 00	!	!	!	!
	00006240	9D 00 5F 61 64 6A 75 73 74 5F 66 64 69 76 00 00	!	!	!	!
	00006250	6A 00 5F 5F 70 5F 5F 63 6F 6D 6D 6F 64 65 00 00	!	!	!	!
	00006260	6F 00 5F 5F 70 5F 5F 66 6D 6F 64 65 00 00 81 00	!	!	!	!
	00006270	5F 5F 73 65 74 5F 61 70 70 5F 74 79 70 65 00 00	!	!	!	!
	00006280	CA 00 5F 65 78 63 65 70 74 5F 68 61 6E 64 6C 65	!	!	!	!
	00006290	72 33 00 00 B7 00 5F 63 6F 6E 74 72 6F 6C 66 70	!	!	!	!
	000062A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	!	!	!	!

 BIN  101 : 1033	<pre> 00007010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00007020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00007030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00007040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00007050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00007060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00007070 5C 77 69 6E 75 70 2E 65 78 65 00 00 25 73 25 73 00007080 00 00 00 00 5C 73 79 73 74 65 6D 33 32 5C 77 75 00007090 70 64 6D 67 72 64 2E 65 78 65 00 00 25 73 25 73 000070A0 00 00 00 00 68 74 74 70 3A 2F 77 77 77 2E 70 000070B0 72 61 63 74 69 63 61 6C 6D 61 6C 77 61 72 65 61 000070C0 6E 61 6C 79 73 69 73 2E 63 6F 6D 2F 75 70 64 61 000070D0 74 65 72 2E 65 78 65 00 01 00 00 00 00 00 00 00 000070E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 </pre>	<pre> \winup.exe \$\$\$ \system32\wu pdmgrd.exe \$\$\$ http://www.p racticalmalwarea nalysis.com/upda ter.exe </pre>
---	---	--

CSE434S

6) Can you say what this malware does? You will be graded for providing an educated conclusion based on your findings, and not necessarily for the correctness of your conclusions. (2 points)

The file starts with '4D 5A 90 00' which is a sign of an executable file. And from the functions it uses, Sample2 will download a program from the URL 'http://www.practicalmalwareanalysis.com/updater.exe' and executes the file for malicious purpose.
