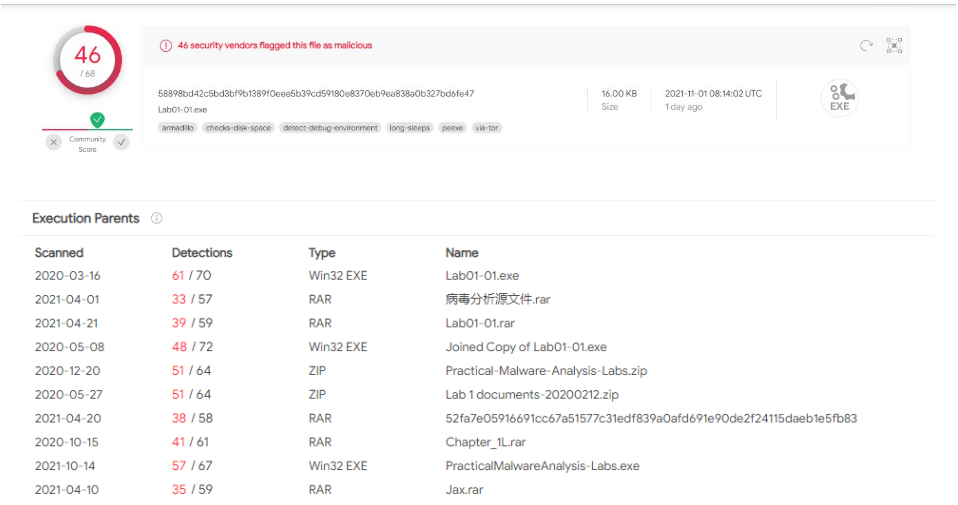
Muhammad Izham Bin Norhamadi
B032020039

Lab 4 Basic Static Malware Analysis

Task 1

1) Yes, it has similarities with other sandbox test virus.

Lab01-01.exe



46 / 68

Community Score

46 security vendors flagged this file as malicious

58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Lab01-01.exe
armadillo checks-disk-space detect-debug-environment long-sleeps peexe via-tor

16.00 KB Size

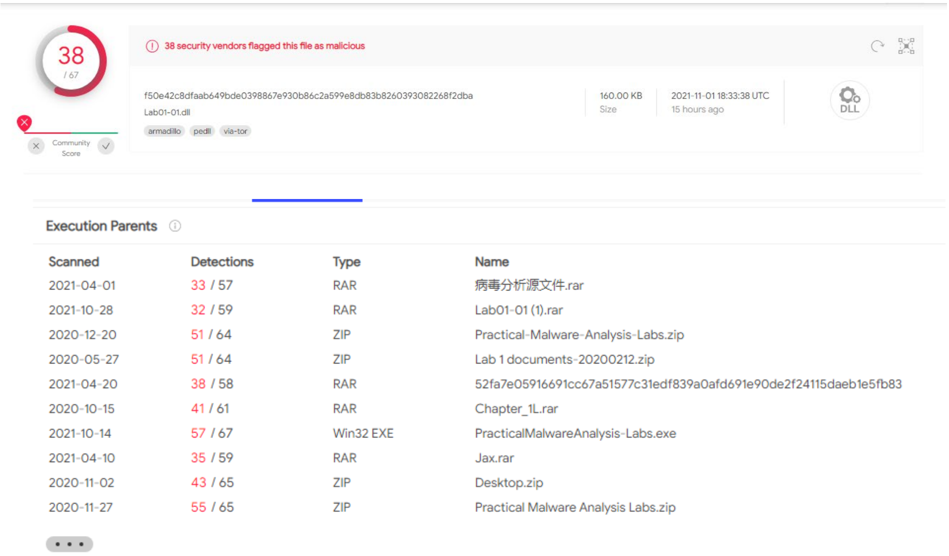
2021-11-01 08:14:02 UTC
1 day ago

EXE

Execution Parents

Scanned	Detections	Type	Name
2020-03-16	61 / 70	Win32 EXE	Lab01-01.exe
2021-04-01	33 / 57	RAR	病毒分析源文件.rar
2021-04-21	39 / 59	RAR	Lab01-01.rar
2020-05-08	48 / 72	Win32 EXE	Joined Copy of Lab01-01.exe
2020-12-20	51 / 64	ZIP	Practical-Malware-Analysis-Labs.zip
2020-05-27	51 / 64	ZIP	Lab 1 documents-20200212.zip
2021-04-20	38 / 58	RAR	52fa7e05916691cc67a51577c31edf839a0afd691e90de2f24115daeb1e5fb83
2020-10-15	41 / 61	RAR	Chapter_1L.rar
2021-10-14	57 / 67	Win32 EXE	PracticalMalwareAnalysis-Labs.exe
2021-04-10	35 / 59	RAR	Jax.rar

Lab01-01.dll



38 / 67

Community Score

38 security vendors flagged this file as malicious

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Lab01-01.dll
armadillo pedll via-tor

160.00 KB Size

2021-11-01 18:33:38 UTC
15 hours ago

DLL

Execution Parents

Scanned	Detections	Type	Name
2021-04-01	33 / 57	RAR	病毒分析源文件.rar
2021-10-28	32 / 59	RAR	Lab01-01 (1).rar
2020-12-20	51 / 64	ZIP	Practical-Malware-Analysis-Labs.zip
2020-05-27	51 / 64	ZIP	Lab 1 documents-20200212.zip
2021-04-20	38 / 58	RAR	52fa7e05916691cc67a51577c31edf839a0afd691e90de2f24115daeb1e5fb83
2020-10-15	41 / 61	RAR	Chapter_1L.rar
2021-10-14	57 / 67	Win32 EXE	PracticalMalwareAnalysis-Labs.exe
2021-04-10	35 / 59	RAR	Jax.rar
2020-11-02	43 / 65	ZIP	Desktop.zip
2020-11-27	55 / 65	ZIP	Practical Malware Analysis Labs.zip

• • •

2)

Lab01-01.exe

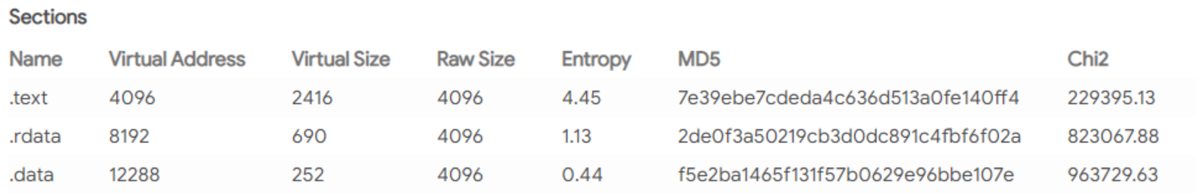
2010-12-19 16:16:19

Lab01-01.dll

2010-12-19 16:16:38

3) None of the files is packed or obfuscated, since all the PE sections have much larger raw sizes than virtual sizes.

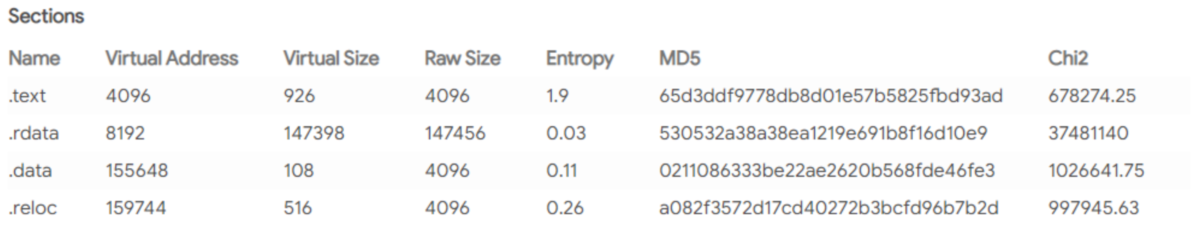
Lab01-01.exe



Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	2416	4096	4.45	7e39ebe7cdeda4c636d513a0fe140ff4	229395.13
.rdata	8192	690	4096	1.13	2de0f3a50219cb3d0dc891c4fbf6f02a	823067.88
.data	12288	252	4096	0.44	f5e2ba1465f131f57b0629e96bbe107e	963729.63

Lab01-01.dll



Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	926	4096	1.9	65d3ddf9778db8d01e57b5825fbd93ad	678274.25
.rdata	8192	147398	147456	0.03	530532a38a38ea1219e691b8f16d10e9	37481140
.data	155648	108	4096	0.11	0211086333be22ae2620b568fde46fe3	1026641.75
.reloc	159744	516	4096	0.26	a082f3572d17cd40272b3bcfd96b7b2d	997945.63

4) Imports:

Kernel32.dll

- Is a Windows kernel module
- Runs as a background process and carries out important functions like memory management, input/output operations and interrupts
- The malware will search through file system

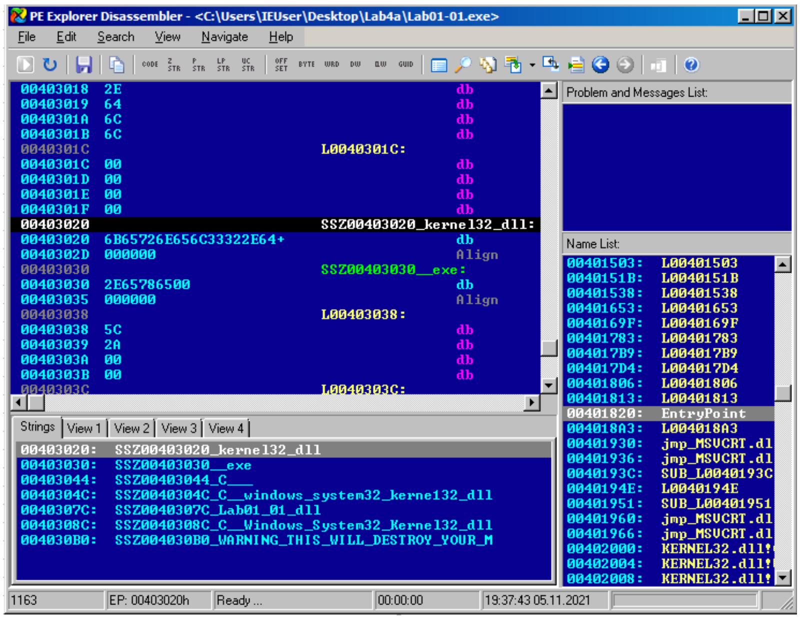
MSVCRT.dll

- is the C standard library for the Visual C++
- provides programs with standart C functions such as string manipulation, memory allocation, C-style input/output calls, and others

WS2_32.dll

- establish and handle network connections
- contains the Windows Sockets API
- used to run most network and internet applications

5)



```
00403018  2E                                        db
00403019  64                                        db
0040301A  6C                                        db
0040301B  6C                                        db
0040301C                            L0040301C:
0040301C  00                                        db
0040301D  00                                        db
0040301E  00                                        db
0040301F  00                                        db
00403020                            SSZ00403020_kernel32_dll:
00403020  6B65726E656C33322E64+                     db
0040302D  000000                                    Align
00403030                            SSZ00403030__exe:
00403030  2E65786500                                db
00403035  000000                                    Align
00403038                            L00403038:
00403038  5C                                        db
00403039  2A                                        db
0040303A  00                                        db
0040303B  00                                        db
0040303C                            L0040303C:
```

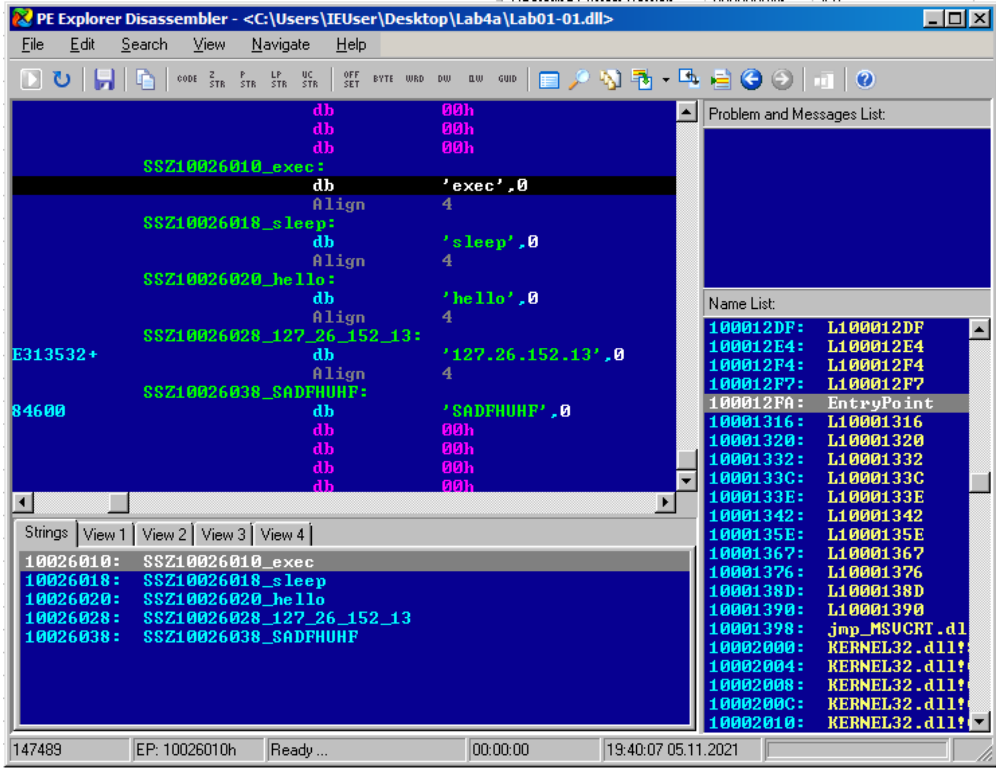
```
00403020:  SSZ00403020_kernel32_dll
00403030:  SSZ00403030__exe
00403044:  SSZ00403044_C___
0040304C:  SSZ0040304C_C__windows_system32_kerne132_dll
0040307C:  SSZ0040307C_Lab01_01_dll
0040308C:  SSZ0040308C_C__Windows_System32_Kernel32_dll
004030B0:  SSZ004030B0_WARNING_THIS_WILL_DESTROY_YOUR_M
```

```
00401503:  L00401503
0040151B:  L0040151B
00401538:  L00401538
00401653:  L00401653
0040169F:  L0040169F
00401783:  L00401783
004017B9:  L004017B9
004017D4:  L004017D4
00401806:  L00401806
00401813:  L00401813
00401820:  EntryPoint
004018A3:  L004018A3
00401930:  jmp_MSVCRT.dl
00401936:  jmp_MSVCRT.dl
0040193C:  SUB_L0040193C
0040194E:  L0040194E
00401951:  SUB_L00401951
00401960:  jmp_MSVCRT.dl
00401966:  jmp_MSVCRT.dl
00402000:  KERNEL32.dll!
00402004:  KERNEL32.dll!
00402008:  KERNEL32.dll!
```

```
1163 | EP: 00403020h | Ready ... | 00:00:00 | 19:37:43 05.11.2021
```

Dissambling lab01-01.exe will find strings around kernel32.dll

6)



```
                         db          00h
                         db          00h
                         db          00h
          SSZ10026010_exec:
                         db          'exec',0
                         Align       4
          SSZ10026018_sleep:
                         db          'sleep',0
                         Align       4
          SSZ10026020_hello:
                         db          'hello',0
                         Align       4
          SSZ10026028_127_26_152_13:
E313532+                 db          '127.26.152.13',0
                         Align       4
          SSZ10026038_SADFHUHF:
84600                    db          'SADFHUHF',0
                         db          00h
                         db          00h
                         db          00h
                         db          00h
```

```
10026010:  SSZ10026010_exec
10026018:  SSZ10026018_sleep
10026020:  SSZ10026020_hello
10026028:  SSZ10026028_127_26_152_13
10026038:  SSZ10026038_SADFHUHF
```

```
100012DF:  L100012DF
100012E4:  L100012E4
100012F4:  L100012F4
100012F7:  L100012F7
100012FA:  EntryPoint
10001316:  L10001316
10001320:  L10001320
10001332:  L10001332
1000133C:  L1000133C
1000133E:  L1000133E
10001342:  L10001342
1000135E:  L1000135E
10001367:  L10001367
10001376:  L10001376
1000138D:  L1000138D
10001390:  L10001390
10001398:  jmp_MSVCRT.dl
10002000:  KERNEL32.dll!
10002004:  KERNEL32.dll!
10002008:  KERNEL32.dll!
1000200C:  KERNEL32.dll!
10002010:  KERNEL32.dll!
```

```
147489    EP: 10026010h    Ready ...    00:00:00    19:40:07 05.11.2021
```

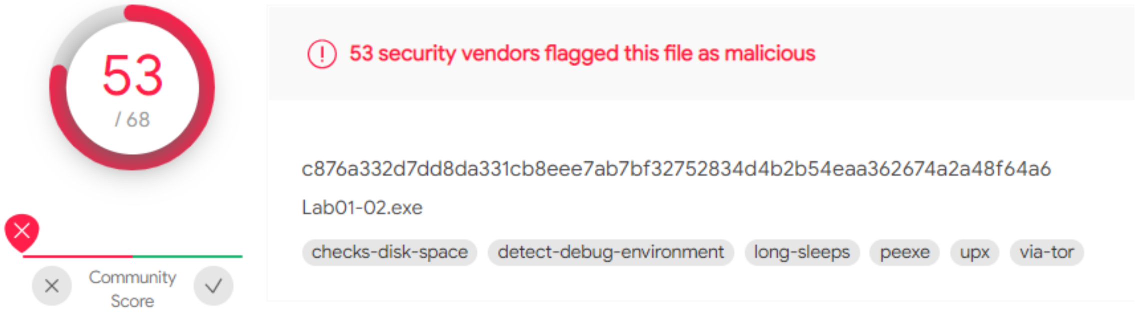
An IP 127.26.152.13 was found with other strings after disassembling Lab01-01.dll

7)

Lab01-01.exe and Lab01-01.dll are likely related and functions together to search through directories on the infected system. The presence of IP address and network based imports can be used to send information.

Task 2

1)



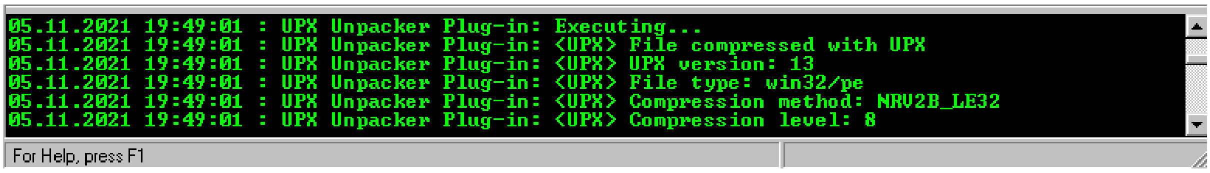
53 security vendors flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Lab01-02.exe

53 out of 68 antivirus detected this exe as malicious with most of them detect it as a Trojan.

2) Yes, the file is packed. The virtual size of the sections are much bigger than the raw size. The packer that was used is UPX packer. Unpacked using PE explorer

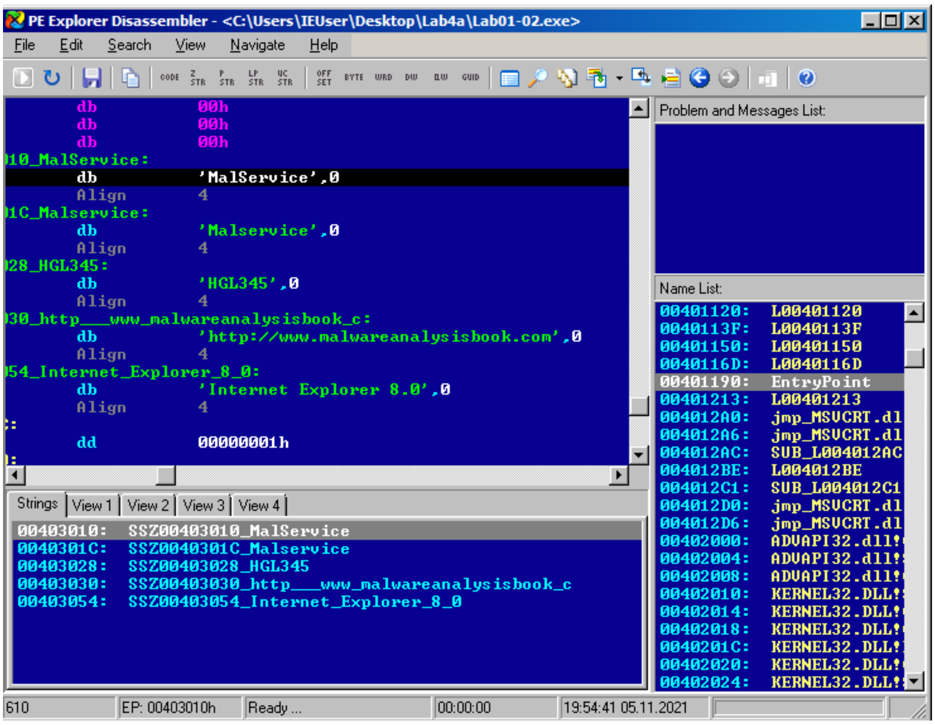


```
05.11.2021 19:49:01 : UPX Unpacker Plug-in: Executing...
05.11.2021 19:49:01 : UPX Unpacker Plug-in: <UPX> File compressed with UPX
05.11.2021 19:49:01 : UPX Unpacker Plug-in: <UPX> UPX version: 13
05.11.2021 19:49:01 : UPX Unpacker Plug-in: <UPX> File type: win32/pe
05.11.2021 19:49:01 : UPX Unpacker Plug-in: <UPX> Compression method: NRV2B_LE32
05.11.2021 19:49:01 : UPX Unpacker Plug-in: <UPX> Compression level: 8
```

UPX Unpacker plugin unpacked the exe

3) The imports are ADVAPI32.dll, KERNEL32.DLL, MSVCRT.dll, WININET.dll. Noteable services are CreateServiceA and InternetOpenA

4)



```
        db            00h
        db            00h
        db            00h
)10_MalService:
        db            'MalService',0
        Align         4
)1C_Malservice:
        db            'Malservice',0
        Align         4
)28_HGL345:
        db            'HGL345',0
        Align         4
)30_http___www_malwareanalysisbook_c:
        db            'http://www.malwareanalysisbook.com',0
        Align         4
)54_Internet_Explorer_8_0:
        db            'Internet Explorer 8.0',0
        Align         4
::
        dd            00000001h
):
```

```
00403010:  SSZ00403010_MalService
0040301C:  SSZ0040301C_Malservice
00403028:  SSZ00403028_HGL345
00403030:  SSZ00403030_http___www_malwareanalysisbook_c
00403054:  SSZ00403054_Internet_Explorer_8_0
```

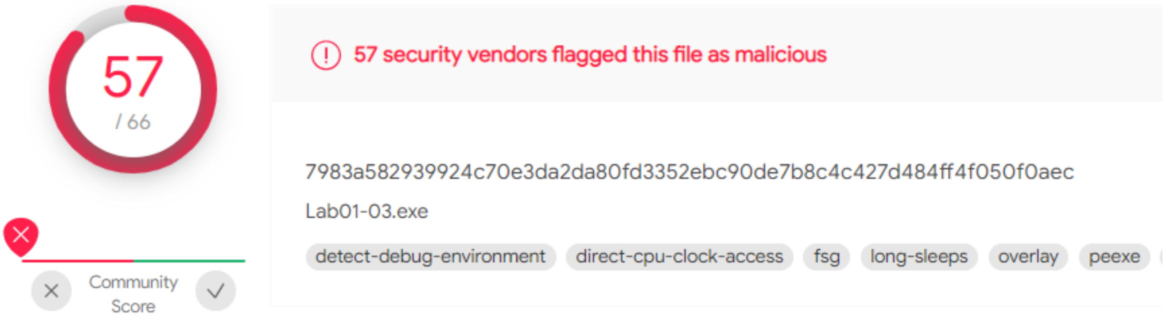
```
00401120:  L00401120
0040113F:  L0040113F
00401150:  L00401150
0040116D:  L0040116D
00401190:  EntryPoint
00401213:  L00401213
004012A0:  jmp_MSVCRT.dl
004012A6:  jmp_MSVCRT.dl
004012AC:  SUB_L004012AC
004012BE:  L004012BE
004012C1:  SUB_L004012C1
004012D0:  jmp_MSVCRT.dl
004012D6:  jmp_MSVCRT.dl
00402000:  ADVAPI32.dll!
00402004:  ADVAPI32.dll!
00402008:  ADVAPI32.dll!
00402010:  KERNEL32.DLL!
00402014:  KERNEL32.DLL!
00402018:  KERNEL32.DLL!
0040201C:  KERNEL32.DLL!
00402020:  KERNEL32.DLL!
00402024:  KERNEL32.DLL!
```

```
610   EP: 00403010h   Ready ...   00:00:00   19:54:41 05.11.2021
```

After disassembling the exe, in the strings of the file contains the link to malwareanalysisbook.com and Internet Explorer 8.0 that potentionally act as a host or network based indicators of malicious activity, through the service to run, URL to connect to and preferred browser.

Task 3

1)



57
/ 66

Community Score

57 security vendors flagged this file as malicious

7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec

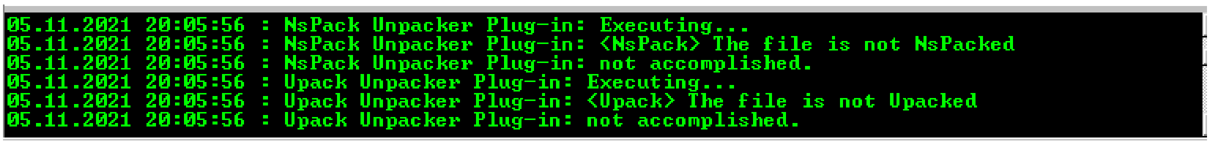
Lab01-03.exe

detect-debug-environment direct-cpu-clock-access fsg long-sleeps overlay peexe

57 out of 66 antivirus detected this exe as malicious with most of them detect the exe as Trojan or Spyware.

2)

Yes, the file is packed with the packer FSG v1.00 (Eng) -> dulek/xt. Unable to unpack the file with PE Explorer plugins

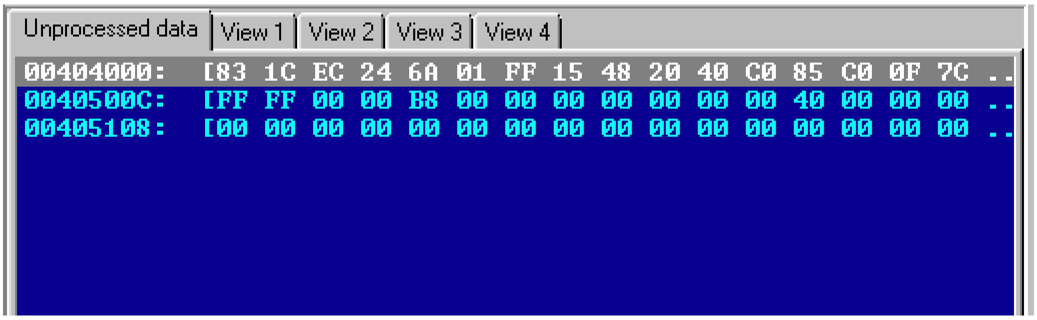


```
05.11.2021 20:05:56 : NsPack Unpacker Plug-in: Executing...
05.11.2021 20:05:56 : NsPack Unpacker Plug-in: <NsPack> The file is not NsPacked
05.11.2021 20:05:56 : NsPack Unpacker Plug-in: not accomplished.
05.11.2021 20:05:56 : Upack Unpacker Plug-in: Executing...
05.11.2021 20:05:56 : Upack Unpacker Plug-in: <Upack> The file is not Upacked
05.11.2021 20:05:56 : Upack Unpacker Plug-in: not accomplished.
```

3)

The import doesn’t tell much, just KERNEL32.dll which is imported by most programs for creating process.

4)



```
00404000:  [83 1C EC 24 6A 01 FF 15 48 20 40 C0 85 C0 0F 7C ..
0040500C:  [FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 ..
00405108:  [00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..
```

Unprocessed data doesn’t give much hint on the malware.