September 17, 2022

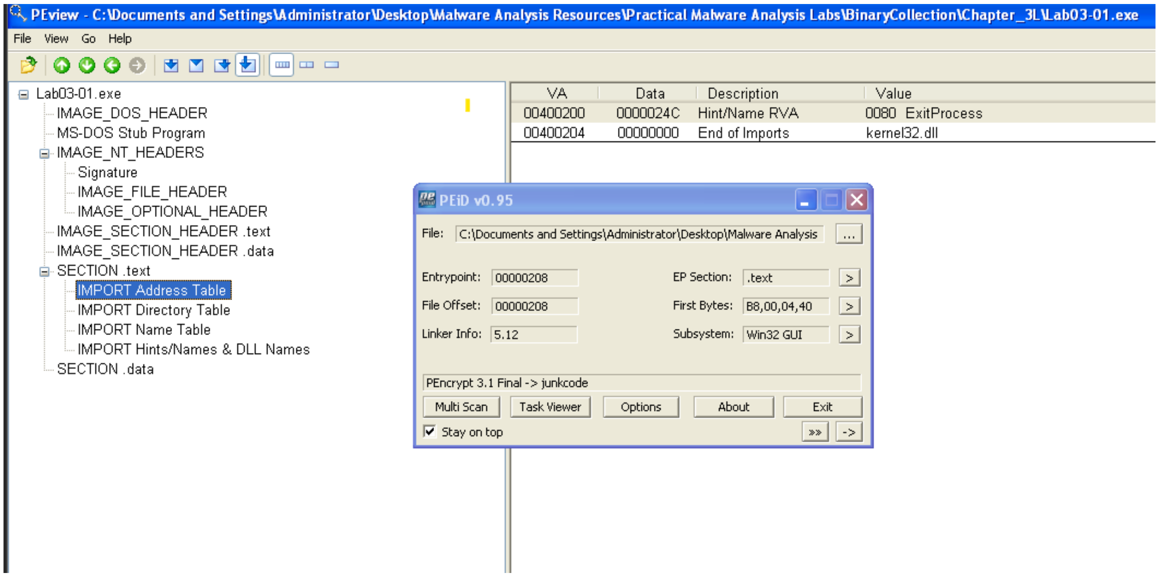
ASSIGNMENT 2

LAB 3-1

Analyze the malware found in the file *Lab03-01.exe* using basic dynamic analysis tools.

Questions

i. What are this malware's imports and strings?



PEview - C:\Documents and Settings\Administrator\Desktop\Malware Analysis Resources\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\Lab03-01.exe

```
Lab03-01.exe
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
    IMAGE_NT_HEADERS
        Signature
        IMAGE_FILE_HEADER
        IMAGE_OPTIONAL_HEADER
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .data
    SECTION .text
        IMPORT Address Table
        IMPORT Directory Table
        IMPORT Name Table
        IMPORT Hints/Names & DLL Names
    SECTION .data
```

VA	Data	Description	Value
00400200	0000024C	Hint/Name RVA	0080 ExitProcess
00400204	00000000	End of Imports	kernel32.dll

PEiD v0.95

File: C:\Documents and Settings\Administrator\Desktop\Malware Analysis

Entrypoint: 00000208 EP Section: .text

File Offset: 00000208 First Bytes: B8,00,04,40

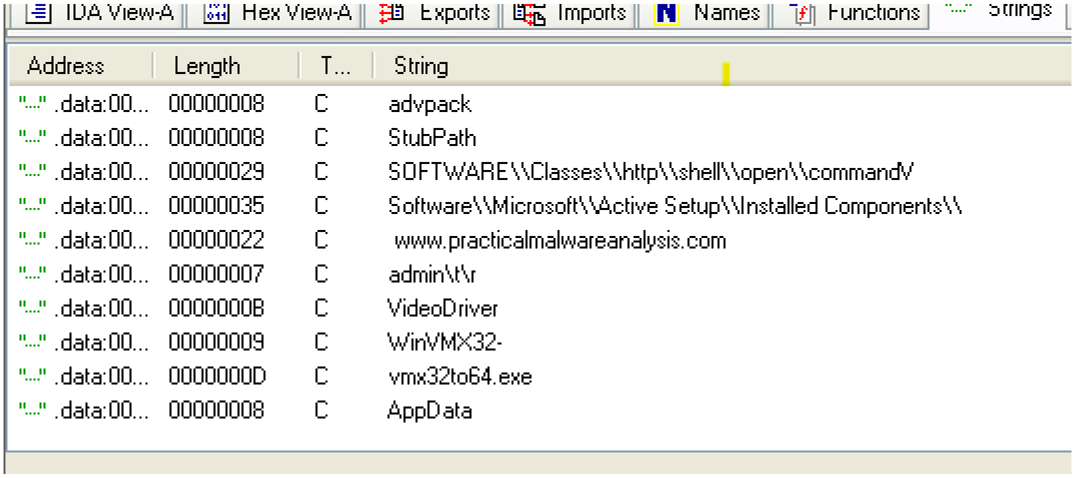
Linker Info: 5.12 Subsystem: Win32 GUI

PEncrypt 3.1 Final -> junkcode

-After analyzing the .exe lab file given in *PEiD* and *PEview*, I was able to find the information needed to view the imports and strings. After my analysis, I was able to conclude that the file is packed, and the only import that could be found was *ExitProcess*, though I was not able to find any clear observation of the strings of the given file since the file is packed.

ii. What are the malware's host-based indicators?
-The malicious software makes a mutex called *WinVMX32*, copies itself to *C:WindowsSystem32vmx32to64.exe*, and sets up the registry value *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver* to run on system startup.

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



Address	Length	T...	String
"..." .data:00...	00000008	C	advpack
"..." .data:00...	00000008	C	StubPath
"..." .data:00...	00000029	C	SOFTWARE\\Classes\\http\\shell\\open\\commandV
"..." .data:00...	00000035	C	Software\\Microsoft\\Active Setup\\Installed Components\\
"..." .data:00...	00000022	C	www.practicalmalwareanalysis.com
"..." .data:00...	00000007	C	admin\t\r
"..." .data:00...	0000000B	C	VideoDriver
"..." .data:00...	00000009	C	WinVMX32-
"..." .data:00...	0000000D	C	vmx32to64.exe
"..." .data:00...	00000008	C	AppData

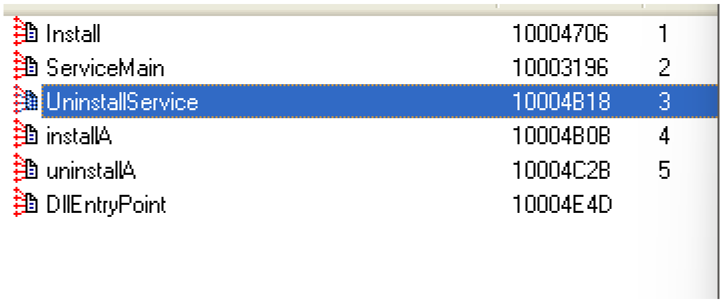
-After analyzing the file in IdaPro I was able to conclude that a network-based signature would be *www.practicalmalwareanalysis.com*.

LAB 3-2

Analyze the malware found in the file *Lab03-02.dll* using basic dynamic analysis tools.

Questions

i. How can you get this malware to install itself?

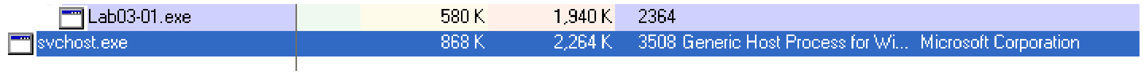


Install	10004706	1
ServiceMain	10003196	2
UninstallService	10004B18	3
installA	10004B0B	4
uninstallA	10004C2B	5
DllEntryPoint	10004E4D	

-Run the malware's exported installA function via ServiceMain with this function Lab03-02.dll,installA to install it as a service.

ii. How would you get this malware to run after installation?
-Analyzing the screenshot given in question one, we would get the service to run with the function *ServiceMain.* After starting the service, it will install using the net command of *IPRIP*.

iii. How can you find the process under which this malware is running?

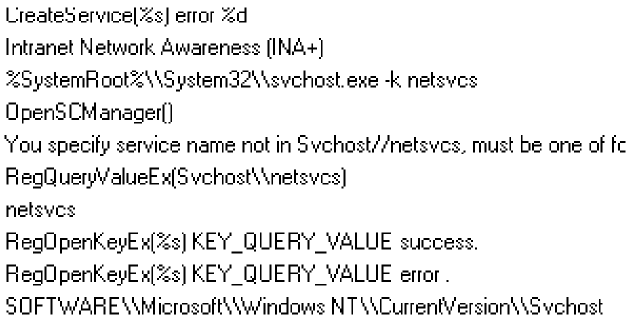


Lab03-01.exe	580 K	1,940 K	2364		
svchost.exe	868 K	2,264 K	3508	Generic Host Process for Wi...	Microsoft Corporation

-When opening the .dll file given into ProcessExplorer instead of being labeled Lab03-02.dll it is labeled under the process it is running under, svchost.exe. I was also able to find the path of the extension file by exploring ProcessExplorer, the path is C:\\WINDOWS\system32\svchost.exe.

iv. Which filters could you set in order to use procmon to glean information?
- When I inspected ProcMon with PID 1148 filtering, I was able to find many registry RegOpenKey and ReadFiles, but they all seem to be tied to svchost.exe and nothing stands out as malicious.

v. What are the malware's host-based indicators?



```
CreateService(%s) error %d
Intranet Network Awareness (INA+)
%SystemRoot%\\System32\\svchost.exe -k netsvcs
OpenSCManager()
You specify service name not in Svchost//netsvcs, must be one of fc
RegQueryValueEx(Svchost\\netsvcs)
netsvcs
RegOpenKeyEx(%s) KEY_QUERY_VALUE success.
RegOpenKeyEx(%s) KEY_QUERY_VALUE error .
SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Svchost
```

- After analyzing the file in Idapro I was able to find both host based indicators which are INA+ and the network activity of *practicalmalwareanalysis.com/serve.html.* Although I could not get a lot of information using the tools that were given because this file is a *.dll* file. I as well analyzed the file in *ApateDNS*, and *Wireshark*, though I did not gain any information.

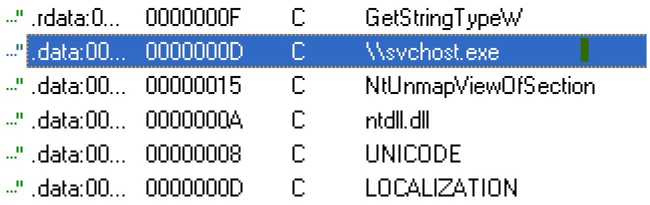
vi. Are there any useful network-based signatures for this malware?
- The network activity of *practicalmalwareanalysis.com/serve.html.* I was able to find this information by using the tool *IdaPro*. Once analyzing this in *IdaPro* I was able to also analyze how the process functions under *installA*.

LAB 3-3

Execute the malware found in the file *Lab03-03.exe* while monitoring it using basic dynamic analysis tools in a safe environment.

Questions

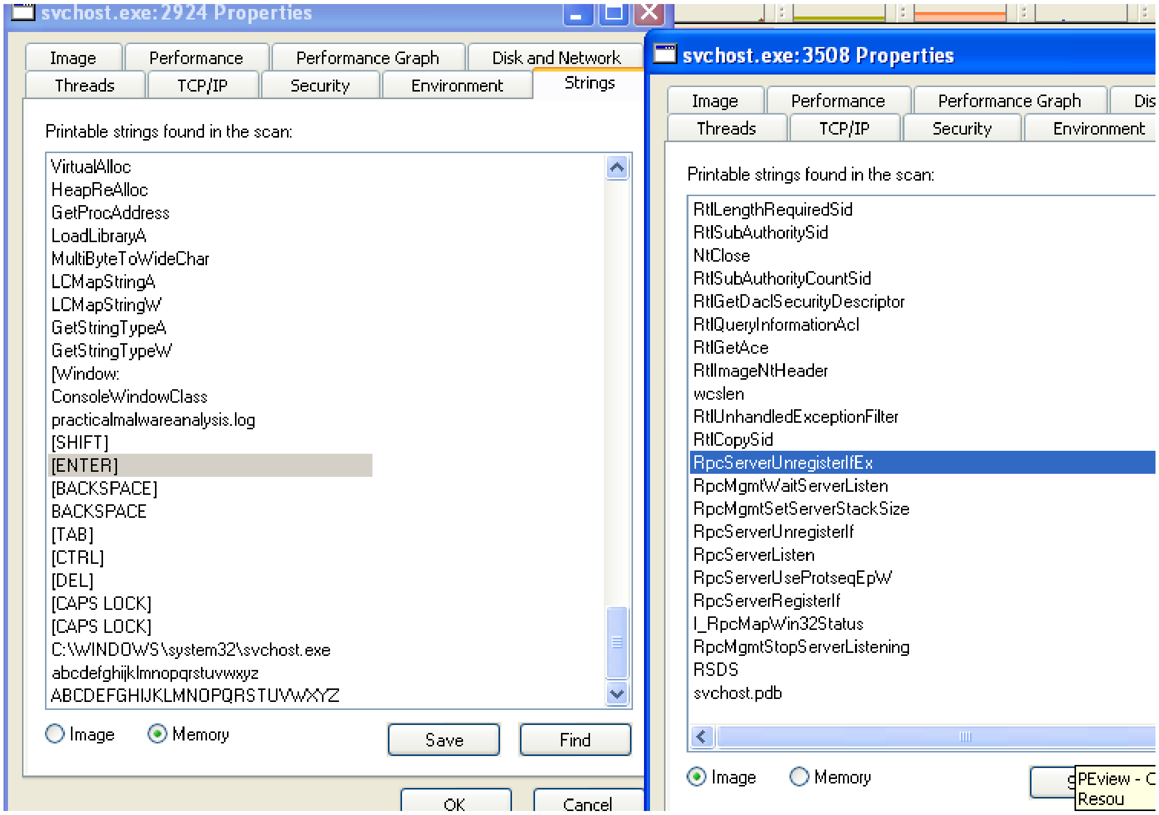
i. What do you notice when monitoring this malware with Process Explorer?



```
..." .rdata:0...   0000000F   C   GetStringTypeW
..." .data:00...   0000000D   C   \\svchost.exe
..." .data:00...   00000015   C   NtUnmapViewOfSection
..." .data:00...   0000000A   C   ntdll.dll
..." .data:00...   00000008   C   UNICODE
..." .data:00...   0000000D   C   LOCALIZATION
```

- When analyzing the file in IdaPro and understanding the processes running under strings, I was able to analyze that the extension file, *svchost.exe* process is replaced with the virus. I also ran this file under ProcessExplorer and when running the file, it runs under *svchost.exe* as well.

ii. Can you identify any live memory modifications?

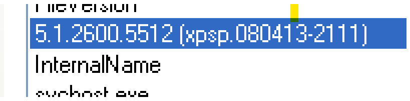


```
VirtualAlloc
HeapReAlloc
GetProcAddress
LoadLibraryA
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
[Window:
ConsoleWindowClass
practicalmalwareanalysis.log
[SHIFT]
[ENTER]
[BACKSPACE]
BACKSPACE
[TAB]
[CTRL]
[DEL]
[CAPS LOCK]
[CAPS LOCK]
C:\WINDOWS\system32\svchost.exe
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

```
RtlLengthRequiredSid
RtlSubAuthoritySid
NtClose
RtlSubAuthorityCountSid
RtlGetDaclSecurityDescriptor
RtlQueryInformationAcl
RtlGetAce
RtlImageNtHeader
wcslen
RtlUnhandledExceptionFilter
RtlCopySid
RpcServerUnregisterIfEx
RpcMgmtWaitServerListen
RpcMgmtSetServerStackSize
RpcServerUnregisterIf
RpcServerListen
RpcServerUseProtseqEpW
RpcServerRegisterIf
I_RpcMapWin32Status
RpcMgmtStopServerListening
RSDS
svchost.pdb
```

-*Svchost.exe* memory image and disk image cannot be compared since they are different. *Practicalmalwareanalysis.log* and *[ENTER]* are strings found in the memory image but not in the disk image. I was able to find and compare these images from the tool *ProcessExplorerer*.

iii. What are the malware's host-based indicators?



```
FileVersion
5.1.2600.5512 (xpsp.080413-2111)
InternalName
svchost.exe
```

-After analyzing the file using ProcessExplorerer I was able to find a host-based indicator of a driver address of *5.1.2600.5512*. I was also able to analyze that the file also has a terminate process function in the extension file of the malware. As well as the file has many *.dll* string files in the strings of the program itself.

iv. What is the purpose of this program?

- After re-analyzing my notes from the previous tasks of this lab I was able to conclude the purpose of the program. The purpose of this program is to perform process replacements on *svchost.exe* to launch a keylogger.

LAB 3-4

Analyze the malware found in the file *Lab03-04.exe* using basic dynamic analysis tools.

Questions

i. What happens when you run this file?
- When executing the file, the CMD is opened by a process that then deletes the original executable after it has run and hidden elsewhere.

ii. What is causing the roadblock in dynamic analysis?
- The program tries to hide by determining whether the system is a virtual machine (VM). A.V. detection, etc. There is no doubt that this will make it challenging to examine the file using dynamic analysis.

iii. Are there other ways to run in this program?
- Other options include opening this executable with Ollydbg or IdaPro so we can analyze it more effectively.