Assignment 1

Adam Livingston

University Of Arizona

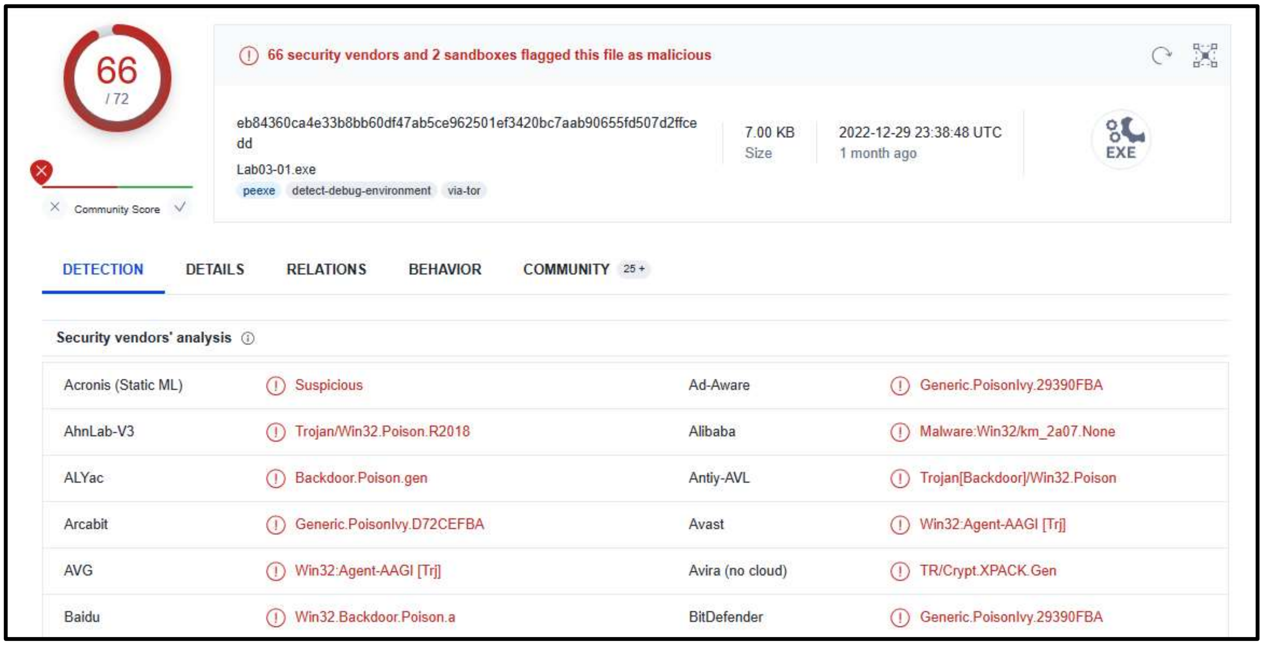
CYBV 454 MALWARE THREATS & ANALYSIS

Professor Galde

31 Jan 2023

LAB 3-1

- LAB03-01.exe : d537acb8f56a1ce206bc35cf8ff959c0



66 security vendors and 2 sandboxes flagged this file as malicious

eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffce
dd

Lab03-01.exe

peexe detect-debug-environment via-tor

7.00 KB
Size

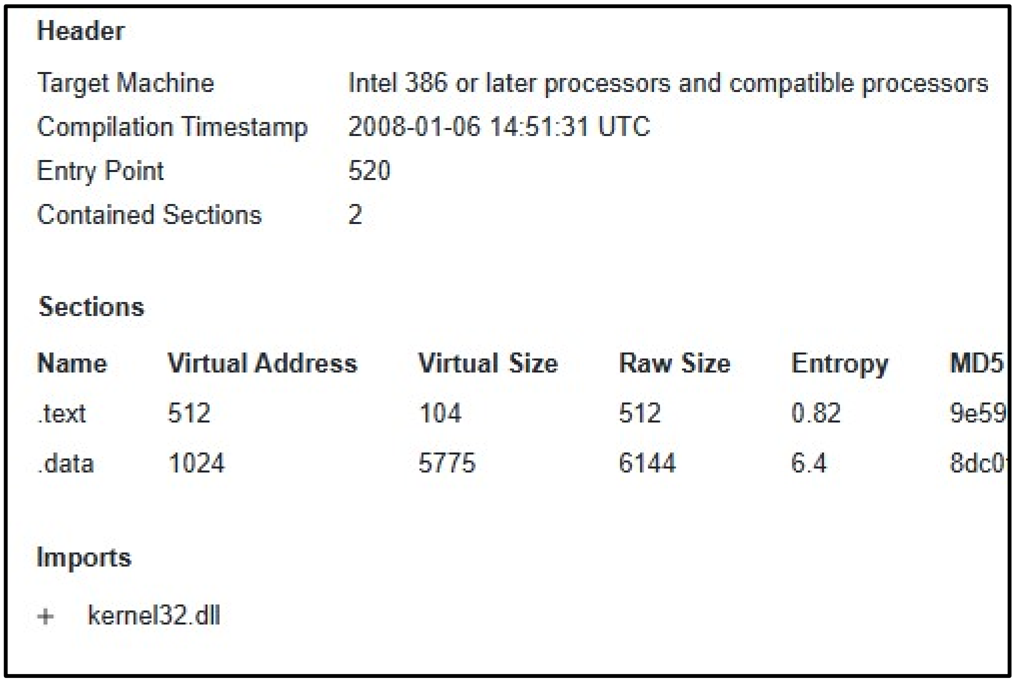
2022-12-29 23:38:48 UTC
1 month ago

Security vendors' analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Generic.PoisonIvy.29390FBA
AhnLab-V3	Trojan/Win32.Poison.R2018	Alibaba	Malware:Win32/km_2a07.None
ALYac	Backdoor.Poison.gen	Antiy-AVL	Trojan[Backdoor]/Win32.Poison
Arcabit	Generic.PoisonIvy.D72CEFBA	Avast	Win32:Agent-AAGI [Trj]
AVG	Win32:Agent-AAGI [Trj]	Avira (no cloud)	TR/Crypt.XPACK.Gen
Baidu	Win32.Backdoor.Poison.a	BitDefender	Generic.PoisonIvy.29390FBA

Figure 1: Virus Total Findings for file Lab03-01.exe.

Virus Total found 66 matching signatures for Trojan (possibly backdoor) malware for the file Lab03-01.exe (Figure1). It has a compilation timestamp of 06 Jan 2008 at 14:51:31 UTC (Figure 2). It appears to only import Kernel32.dll, suggesting it manipulates memory, files, and other hardware (Figure 2). Under the "Behavior" tab, the malware reportedly has indicators of privilege escalation and defense evasion (Figure 3). It is also reported that it has the capability to perform DNS (Figure 4). Based on the fact that this malware had the name of "backdoor" in the initial findings along with its network connection capabilities, it is reasonable to assume that this malware is in fact a back door.



Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2008-01-06 14:51:31 UTC
Entry Point	520
Contained Sections	2

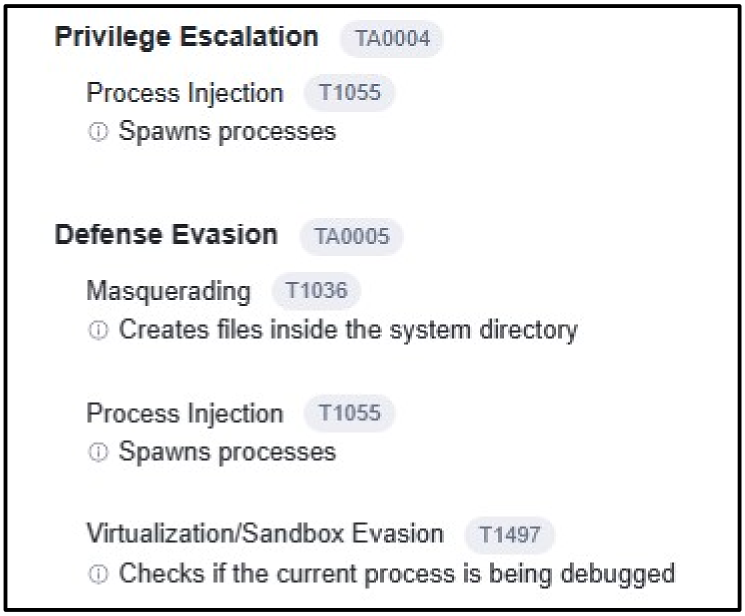
Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	512	104	512	0.82	9e59
.data	1024	5775	6144	6.4	8dc0

Imports

+ kernel32.dll

Figure 2: Virus Total Compilation Timestamp and .dll imports for Lab03-01.exe



Privilege Escalation TA0004

Process Injection T1055

ⓘ Spawns processes

Defense Evasion TA0005

Masquerading T1036

ⓘ Creates files inside the system directory

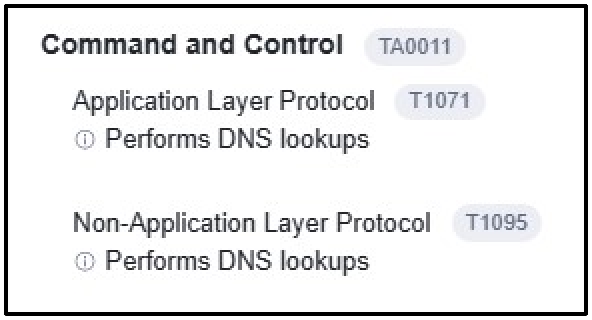
Process Injection T1055

ⓘ Spawns processes

Virtualization/Sandbox Evasion T1497

ⓘ Checks if the current process is being debugged

Figure 3: Virus Total behavior for Lab03-01.exe



Command and Control TA0011

Application Layer Protocol T1071

ⓘ Performs DNS lookups

Non-Application Layer Protocol T1095

ⓘ Performs DNS lookups

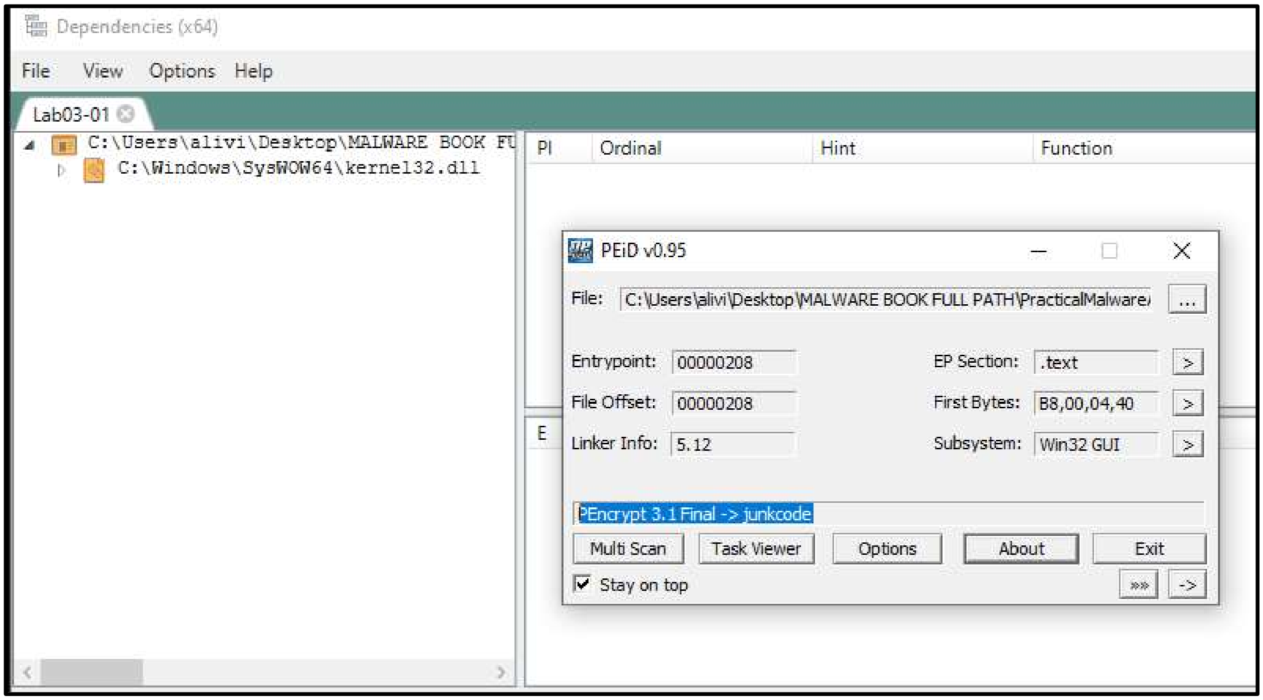
Figure 4: Virus Total network behavior for Lab03-01.exe

LAB 3-1

LAB 3-1 Question 1

What are this malware's imports and strings?

After analysis with Dependencies and PEiD, the malware appears to be packed. Figure 5 shows that there is an output from PEiD of "PEEncrypt 3.1 Final -> Junkcode and the only import is kernel32.dll. Using PEview, we see that the only imports within the address table are ExitProcess and kernel32.dll (Figure 6). Without any additional imports, it is difficult to predict the purpose of this malware. A strings analysis with BinText showed some interesting imports. There are calls to modify the registry key, "SOFTWARE\Classes\http\shell\open\commandV", which, according to Microsoft, is where one would add an http subkey to the registry (Figure 7). We even see the string, "CONNECT %s:%iHTTP/1.0". Based on the initial analysis on VirusTotal, this malware most likely uses this registry key to create a shell. This shell would then then be used over port 80 by the malicious actor to create a TCP connection and access the user's system.



```
C:\Users\alivi\Desktop\MALWARE BOOK FU
    C:\Windows\SysWOW64\kernel32.dll
```

File: C:\Users\alivi\Desktop\MALWARE BOOK FULL PATH\PracticalMalware/

Entrypoint: 00000208 EP Section: .text

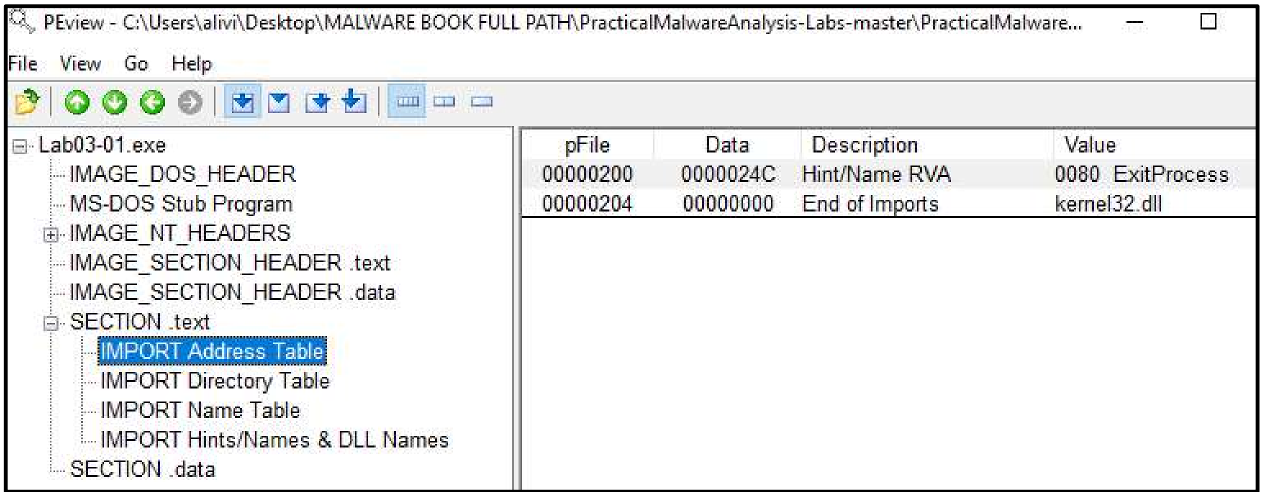
File Offset: 00000208 First Bytes: B8,00,04,40

Linker Info: 5.12 Subsystem: Win32 GUI

PEncrypt 3.1 Final -> junkcode

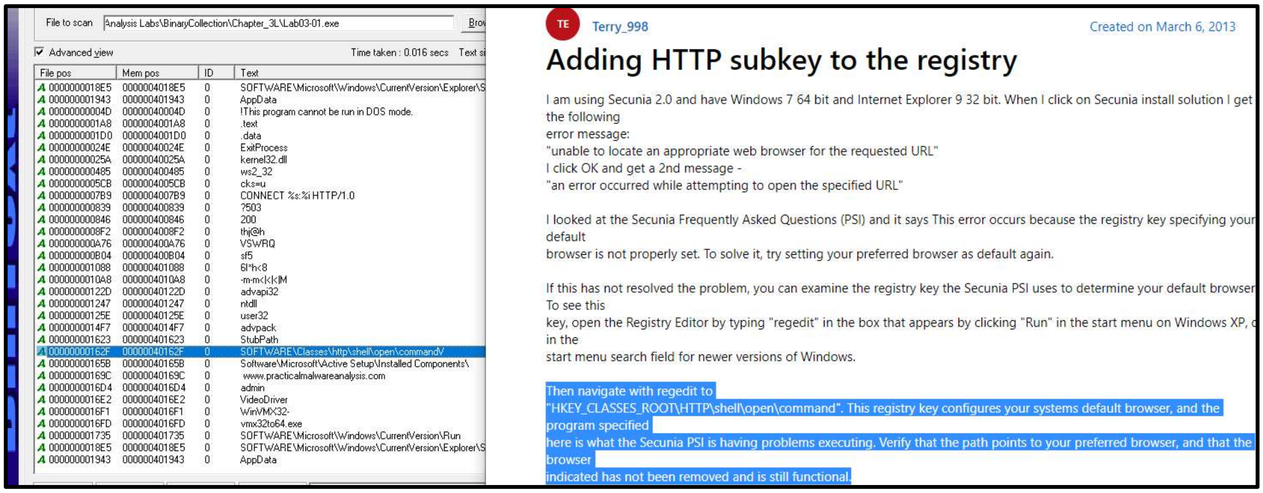
☑ Stay on top

Figure 5: Evidence of packing for Lab03-01.exe


PEview - C:\Users\alivi\Desktop\MALWARE BOOK FULL PATH\PracticalMalwareAnalysis-Labs-master\PracticalMalware...
File View Go Help
Lab03-01.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
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

pFile	Data	Description	Value
00000200	0000024C	Hint/Name RVA	0080 ExitProcess
00000204	00000000	End of Imports	kernel32.dll

Figure 6: More evidence of packing for Lab03-01.exe



```
File pos          Mem pos          ID  Text
A 0000000018E5    0000004018E5     0   SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\S
A 000000001943    000000401943     0   AppData
A 00000000004D    00000040004D     0   !This program cannot be run in DOS mode.
A 0000000001A8    0000004001A8     0   .text
A 0000000001D0    0000004001D0     0   .data
A 00000000024E    00000040024E     0   ExitProcess
A 00000000025A    00000040025A     0   kernel32.dll
A 000000000485    000000400485     0   ws2_32
A 0000000005CB    0000004005CB     0   cks=u
A 0000000007B9    0000004007B9     0   CONNECT %s:%i HTTP/1.0
A 000000000839    000000400839     0   ?503
A 000000000846    000000400846     0   200
A 0000000008F2    0000004008F2     0   thj@h
A 000000000A76    000000400A76     0   VSWRQ
A 000000000B04    000000400B04     0   sf5
A 000000001088    000000401088     0   6I*h<8
A 0000000010A8    0000004010A8     0   -m-m<|<|<|M
A 00000000122D    00000040122D     0   advapi32
A 000000001247    000000401247     0   ntdll
A 00000000125E    00000040125E     0   user32
A 0000000014F7    0000004014F7     0   advpack
A 000000001623    000000401623     0   StubPath
A 00000000162F    00000040162F     0   SOFTWARE\Classes\http\shell\open\commandV
A 00000000165B    00000040165B     0   Software\Microsoft\Active Setup\Installed Components\
A 00000000169C    00000040169C     0    www.practicalmalwareanalysis.com
A 0000000016D4    0000004016D4     0   admin
A 0000000016E2    0000004016E2     0   VideoDriver
A 0000000016F1    0000004016F1     0   WinVMX32-
A 0000000016FD    0000004016FD     0   vmx32to64.exe
A 000000001735    000000401735     0   SOFTWARE\Microsoft\Windows\CurrentVersion\Run
A 0000000018E5    0000004018E5     0   SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\S
A 000000001943    000000401943     0   AppData
```

TE Terry_998 Created on March 6, 2013

Adding HTTP subkey to the registry

I am using Secunia 2.0 and have Windows 7 64 bit and Internet Explorer 9 32 bit. When I click on Secunia install solution I get
the following
error message:
"unable to locate an appropriate web browser for the requested URL"
I click OK and get a 2nd message -
"an error occurred while attempting to open the specified URL"

I looked at the Secunia Frequently Asked Questions (PSI) and it says This error occurs because the registry key specifying your
default
browser is not properly set. To solve it, try setting your preferred browser as default again.

If this has not resolved the problem, you can examine the registry key the Secunia PSI uses to determine your default browser
To see this
key, open the Registry Editor by typing "regedit" in the box that appears by clicking "Run" in the start menu on Windows XP, c
in the
start menu search field for newer versions of Windows.

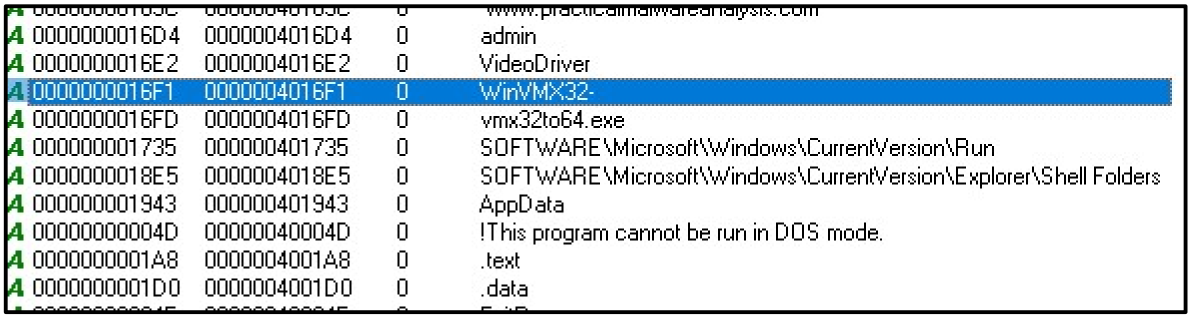
Then navigate with regedit to
"HKEY_CLASSES_ROOT\HTTP\shell\open\command". This registry key configures your systems default browser, and the
program specified
here is what the Secunia PSI is having problems executing. Verify that the path points to your preferred browser, and that the
browser
indicated has not been removed and is still functional.

Figure 7: More evidence of packing for Lab03-01.exe

LAB 3-1 Question 2

What are the malware's host-based indicators?

One host-based indicator to look for would be the creation of the object, "WinVMX32" which would be located in the registry within "SOFTWARE\Microsoft\Windows\CurrentVersion\Run" (Figure 8). This object would be a good indicator that a machine has been infected with malware and there would be a good probability that this object is located in the Windows\sytem32 folder as many malware that imports kernel32.dll make modifications to that folder or attempt to access it.



```
                                       www.practicalmalwareanalysis.com
A 0000000016D4   0000004016D4   0      admin
A 0000000016E2   0000004016E2   0      VideoDriver
A 0000000016F1   0000004016F1   0      WinVMX32-
A 0000000016FD   0000004016FD   0      vmx32to64.exe
A 000000001735   000000401735   0      SOFTWARE\Microsoft\Windows\CurrentVersion\Run
A 0000000018E5   0000004018E5   0      SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
A 000000001943   000000401943   0      AppData
A 00000000004D   00000040004D   0      !This program cannot be run in DOS mode.
A 0000000001A8   0000004001A8   0      .text
A 0000000001D0   0000004001D0   0      .data
```

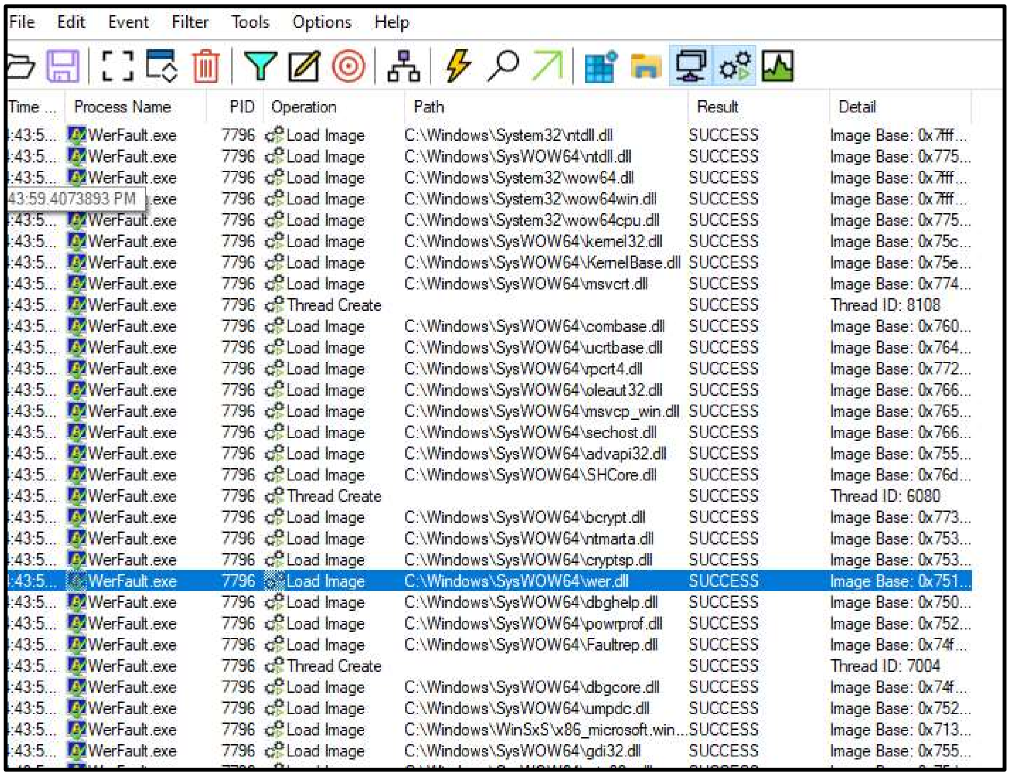
Figure 8: WinVMX32 registry creation by Lab03-01.exe

LAB 3-1 Question 3

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

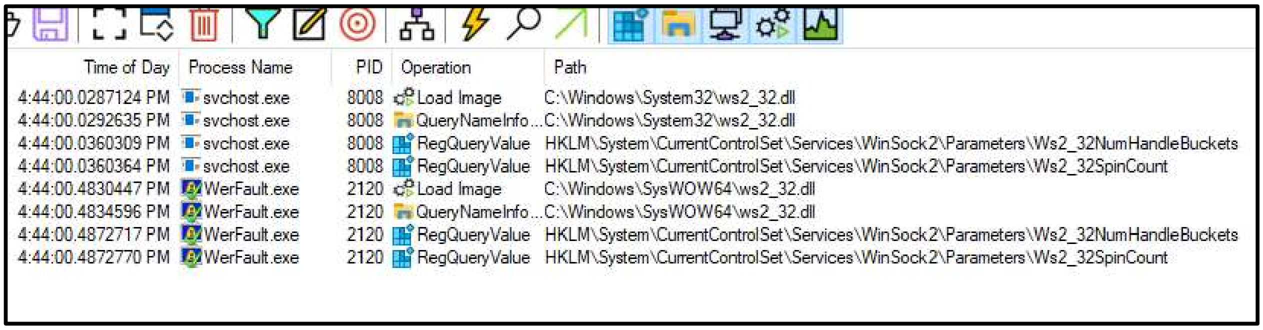
Because we identified in VirusTotal and our strings analysis that this malware most likely connects over http and makes DNS calls, a netcat listener was established on port 80 and port 53. This was done in conjunction with active monitoring on ApdateDNS, procmon, and Wireshark. When Lab03-01.exe was ran, Process Explorer briefly showed the process and then showed "WerFault.exe" (the Windows Problem Reporting Application) which was confirmed in abundance in the Process Monitor Capture (Figure 9). This happened despite the fact that no GUI-based error reporting message was created and therefore can most likely be attributed to Lab03-01.exe. This also happened when the malware was ran without the use of ApdateDNS and on both occasions, Netcat did not pick up any traffic on ports 80 and 53. There some specific instances of WerFault.exe occurring on network-based .dlls showed failed attempts at using Ws2_32.dll (Figure 10). Procmon did not show any events that coincided with setting registry values or writing to files (Figure 11).

Beginning the suspect that the malware and/or the host the malware intends to connect to may be defunct, the malware was uploaded to app.any,run to test it in a different OS environment. It showed that the malware did not run. (Figure 12). The online sandbox did not show any network callouts or file modifications.



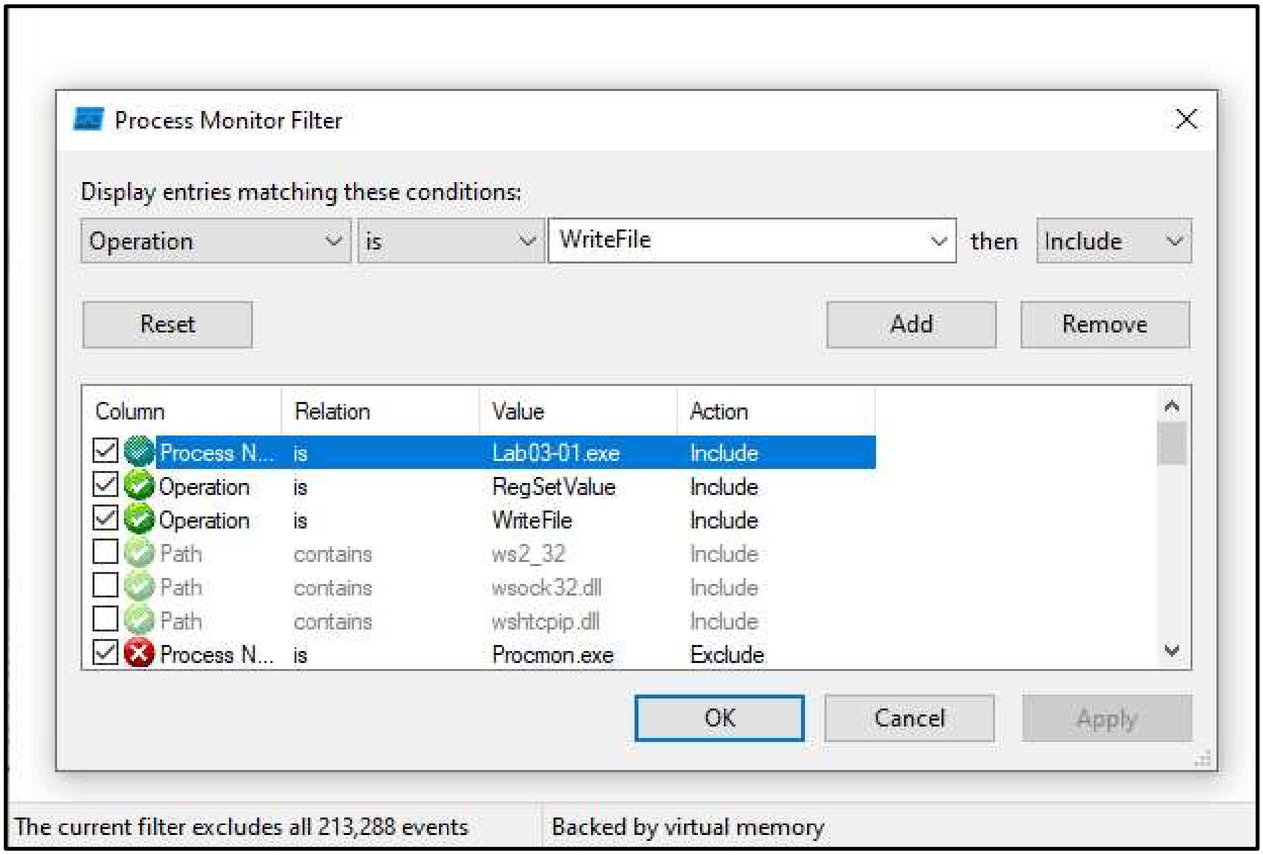
Time ...	Process Name	PID	Operation	Path	Result	Detail
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fff...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x775...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7fff...
43:59.4073893 PM	.exe	7796	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fff...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x775...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75c...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x75e...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x774...
:43:5...	WerFault.exe	7796	Thread Create		SUCCESS	Thread ID: 8108
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\combase.dll	SUCCESS	Image Base: 0x760...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\ucrtbase.dll	SUCCESS	Image Base: 0x764...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Image Base: 0x772...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x766...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\msvcp_win.dll	SUCCESS	Image Base: 0x765...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x766...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x755...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\SHCore.dll	SUCCESS	Image Base: 0x76d...
:43:5...	WerFault.exe	7796	Thread Create		SUCCESS	Thread ID: 6080
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS	Image Base: 0x773...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS	Image Base: 0x753...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\cryptsp.dll	SUCCESS	Image Base: 0x753...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\wer.dll	SUCCESS	Image Base: 0x751...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Image Base: 0x750...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\powrprof.dll	SUCCESS	Image Base: 0x752...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\Faultrep.dll	SUCCESS	Image Base: 0x74f...
:43:5...	WerFault.exe	7796	Thread Create		SUCCESS	Thread ID: 7004
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\dbgcore.dll	SUCCESS	Image Base: 0x74f...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\umpdc.dll	SUCCESS	Image Base: 0x752...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\WinSxS\x86_microsoft.win...	SUCCESS	Image Base: 0x713...
:43:5...	WerFault.exe	7796	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x755...

Figure 9: Lots of error messages generated after running Lab03-01.exe



Time of Day	Process Name	PID	Operation	Path
4:44:00.0287124 PM	svchost.exe	8008	Load Image	C:\Windows\System32\ws2_32.dll
4:44:00.0292635 PM	svchost.exe	8008	QueryNameInfo...	C:\Windows\System32\ws2_32.dll
4:44:00.0360309 PM	svchost.exe	8008	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Ws2_32NumHandleBuckets
4:44:00.0360364 PM	svchost.exe	8008	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Ws2_32SpinCount
4:44:00.4830447 PM	WerFault.exe	2120	Load Image	C:\Windows\SysWOW64\ws2_32.dll
4:44:00.4834596 PM	WerFault.exe	2120	QueryNameInfo...	C:\Windows\SysWOW64\ws2_32.dll
4:44:00.4872717 PM	WerFault.exe	2120	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Ws2_32NumHandleBuckets
4:44:00.4872770 PM	WerFault.exe	2120	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Ws2_32SpinCount

Figure 10: ws2_32.dll failures after running Lab03-01.exe



Process Monitor Filter

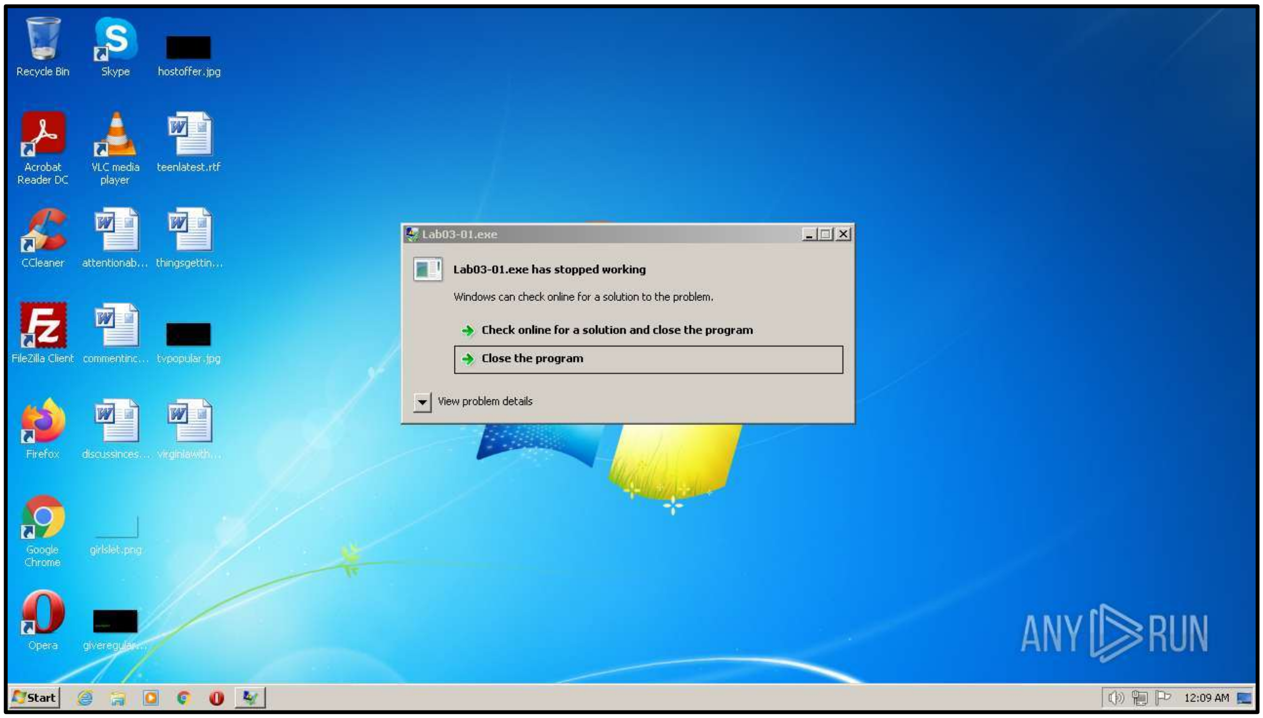
Display entries matching these conditions:

Operation | is | WriteFile | then | Include

	Column	Relation	Value	Action
☑	Process N...	is	Lab03-01.exe	Include
☑	Operation	is	RegSetValue	Include
☑	Operation	is	WriteFile	Include
☐	Path	contains	ws2_32	Include
☐	Path	contains	wsock32.dll	Include
☐	Path	contains	wshtcpip.dll	Include
☑	Process N...	is	Procmon.exe	Exclude

The current filter excludes all 213,288 events | Backed by virtual memory

Figure 11: RegSetValue and WriteFile operations by Lab03-01.exe exclude all events.



Lab03-01.exe

Lab03-01.exe has stopped working

Windows can check online for a solution to the problem.

→ Check online for a solution and close the program

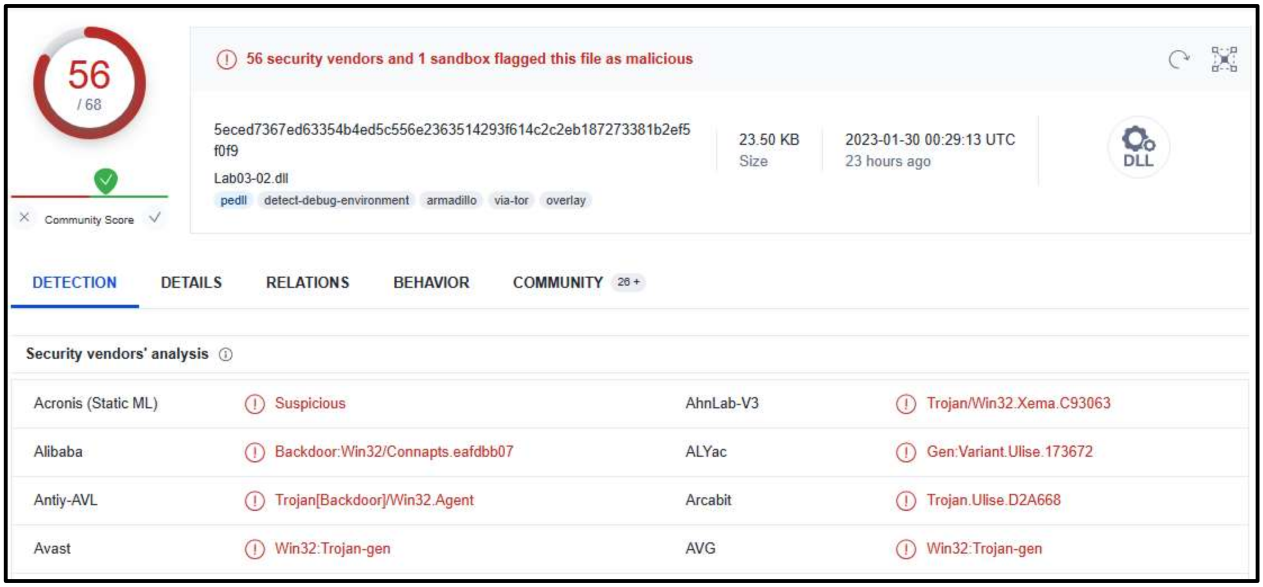
→ Close the program

View problem details

Figure 12: app.any.run screenshot for Lab03-01.exe not responding.

LAB 3-2

- LAB03-02.dll : 84882c9d43e23d63b82004fae74ebb61



56 / 68

Community Score

56 security vendors and 1 sandbox flagged this file as malicious

5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9

Lab03-02.dll

pedll detect-debug-environment armadillo via-tor overlay

23.50 KB Size

2023-01-30 00:29:13 UTC 23 hours ago

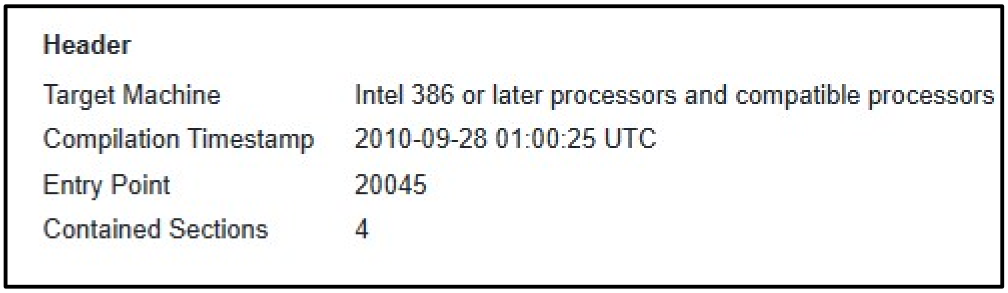
DLL

Security vendors' analysis

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.Xema.C93063
Alibaba	Backdoor:Win32/Connapts.eafdbb07	ALYac	Gen:Variant.Ulise.173672
Antiy-AVL	Trojan[Backdoor]/Win32.Agent	Arcabit	Trojan.Ulise.D2A668
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen

Figure 13: Virus Total Findings for file Lab03-02.dll.

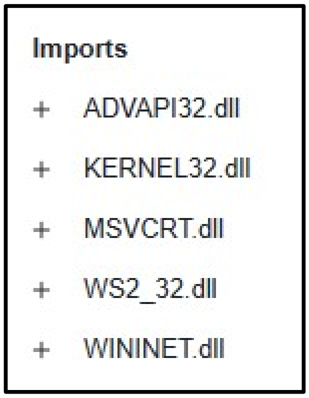
Virus Total found 56 matching signatures for Trojan malware for the file Lab03-02.dll with indications that it could be a backdoor (Figure 13). It has a compilation timestamp of 28 Sep 2010 at 01:00:25 UTC (Figure 14). It appears to import Kernel32.dll and advapi32.dll suggesting it manipulates memory, files, and other hardware. The additional import of wininet.dll suggests that it has the ability to configure ports and protocols in conjunction with Ws2_32.dll. (Figure 15). Under the “Behavior” tab, it is noted that the malware schedules a task and found a very long command line which indicates that the file may be encrypted or packed. It also executes commands using a shell (Figure 16). It has other indicators of persistence, privilege escalation, and defense evasion (Figure 17). It is also reported that the file has network calls, performing DNS lookups, using HTTPS, and potentially downloading/writing to files (Figure 18). VirusTotal also notes that the malware may be obfuscated (Figure 19).



Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2010-09-28 01:00:25 UTC
Entry Point	20045
Contained Sections	4

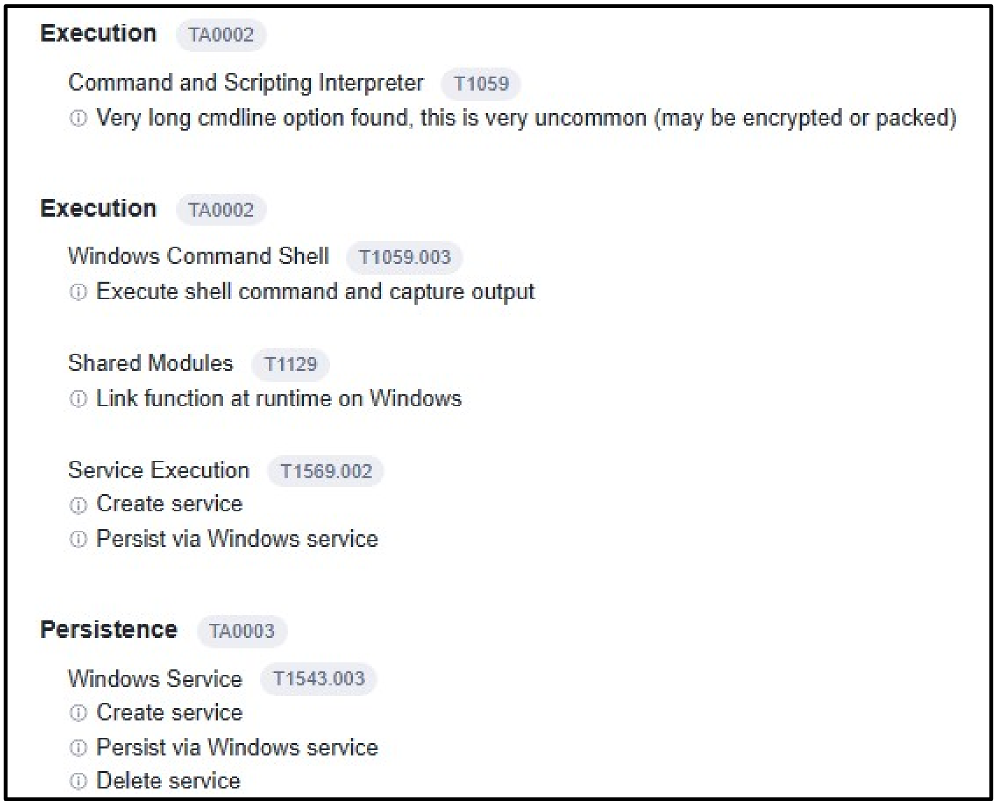
Figure 14: Virus Total Timestamp for file Lab03-02.dll.



Imports

- + ADVAPI32.dll
- + KERNEL32.dll
- + MSVCRT.dll
- + WS2_32.dll
- + WININET.dll

Figure 15: Virus Total Imports for Lab03-02.dll.



Execution TA0002

Command and Scripting Interpreter T1059
ⓘ Very long cmdline option found, this is very uncommon (may be encrypted or packed)

Execution TA0002

Windows Command Shell T1059.003
ⓘ Execute shell command and capture output

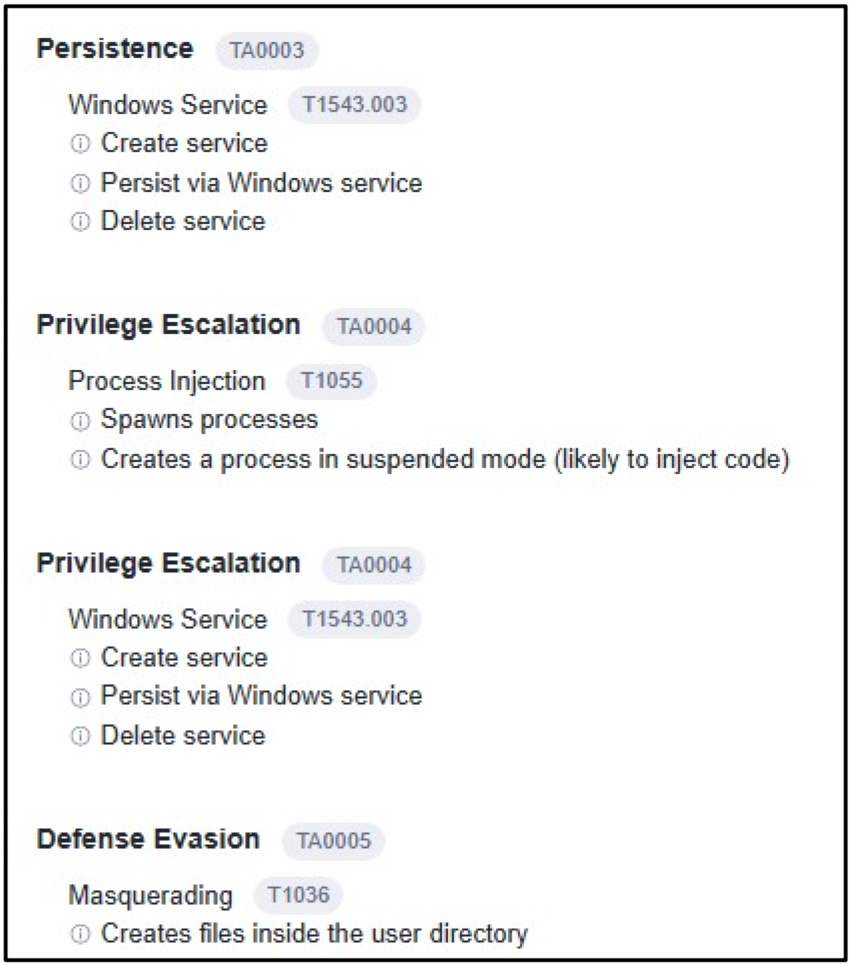
Shared Modules T1129
ⓘ Link function at runtime on Windows

Service Execution T1569.002
ⓘ Create service
ⓘ Persist via Windows service

Persistence TA0003

Windows Service T1543.003
ⓘ Create service
ⓘ Persist via Windows service
ⓘ Delete service

Figure 16: Virus Total Behavior for file Lab03-02.dll.



Persistence TA0003

Windows Service T1543.003
ⓘ Create service
ⓘ Persist via Windows service
ⓘ Delete service

Privilege Escalation TA0004

Process Injection T1055
ⓘ Spawns processes
ⓘ Creates a process in suspended mode (likely to inject code)

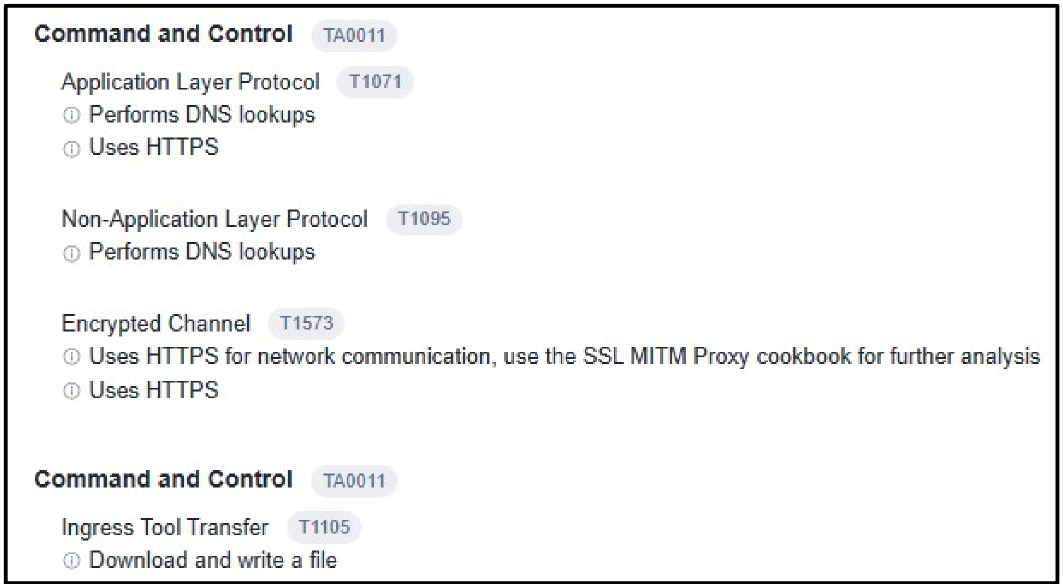
Privilege Escalation TA0004

Windows Service T1543.003
ⓘ Create service
ⓘ Persist via Windows service
ⓘ Delete service

Defense Evasion TA0005

Masquerading T1036
ⓘ Creates files inside the user directory

Figure 17: Virus Total Behavior for file Lab03-02.dll.



Command and Control TA0011

Application Layer Protocol T1071
ⓘ Performs DNS lookups
ⓘ Uses HTTPS

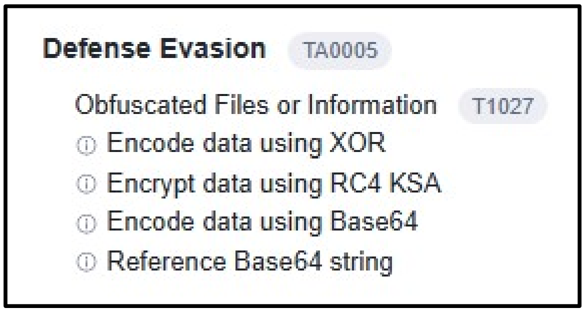
Non-Application Layer Protocol T1095
ⓘ Performs DNS lookups

Encrypted Channel T1573
ⓘ Uses HTTPS for network communication, use the SSL MITM Proxy cookbook for further analysis
ⓘ Uses HTTPS

Command and Control TA0011

Ingress Tool Transfer T1105
ⓘ Download and write a file

Figure 18: Virus Total C&C for file Lab03-02.dll.



Defense Evasion TA0005

Obfuscated Files or Information T1027

ⓘ Encode data using XOR

ⓘ Encrypt data using RC4 KSA

ⓘ Encode data using Base64

ⓘ Reference Base64 string

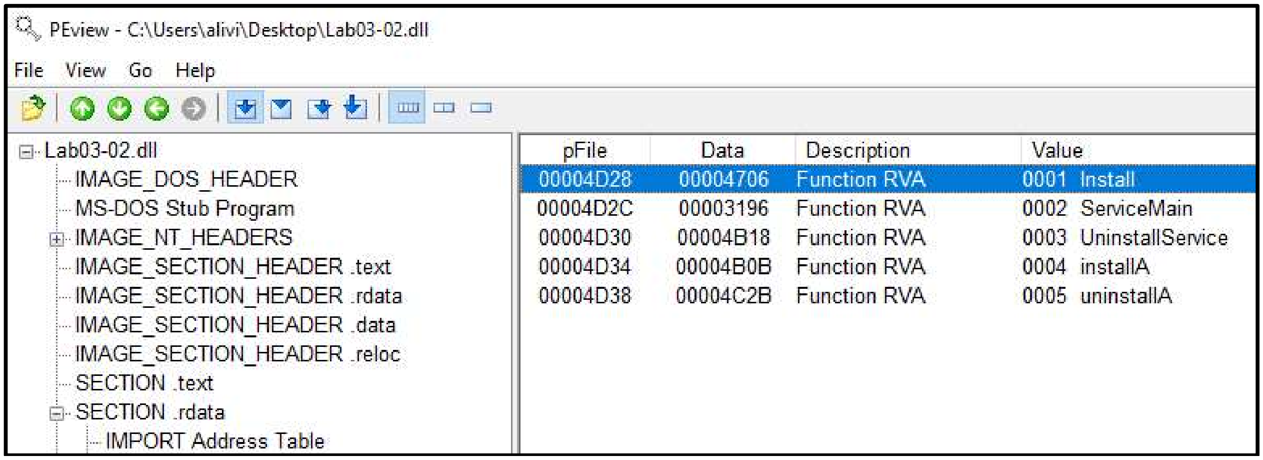
Figure 19: Virus Total indications of obfuscation for Lab03-02.dll.

LAB 3-2

LAB 3-2 Question 1

How can you get this malware to install itself?

The native program in Windows environments, “rundll32.exe” provides user a method to manually run .dll files using the syntax, “C:\>rundll32.exe <dllName>.dll, Export arguments” on the command line. To get it to install, the rundll32.exe is also used but with the syntax “C:\>rundll32.exe <dllName>.dll, Install”. This syntax is used to install a dll if the dll file has an “install” export, which Lab03-02.dll was confirmed as having after viewing it in PEview under the “EXPORT Address Table” (Figure 20). We also notice in Figure 20 that the export of “installA” was included in this table. This argument was also passed in rundll32.exe when installing the malware on a virtual machine in addition to the “install”


PEview - C:\Users\alivi\Desktop\Lab03-02.dll
File View Go Help
Lab03-02.dll
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table

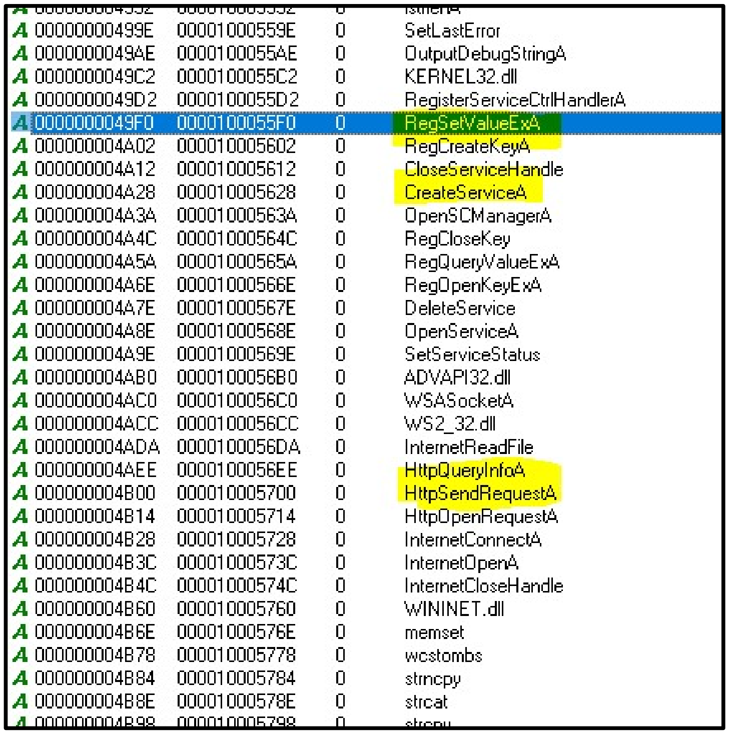
pFile	Data	Description	Value
00004D28	00004706	Function RVA	0001 Install
00004D2C	00003196	Function RVA	0002 ServiceMain
00004D30	00004B18	Function RVA	0003 UninstallService
00004D34	00004B0B	Function RVA	0004 installA
00004D38	00004C2B	Function RVA	0005 uninstallA

Figure 20: “Install” and “installA” exports included in Lab03-02.dll.

LAB 3-2 Question 2

How would you get this malware to run after installation?

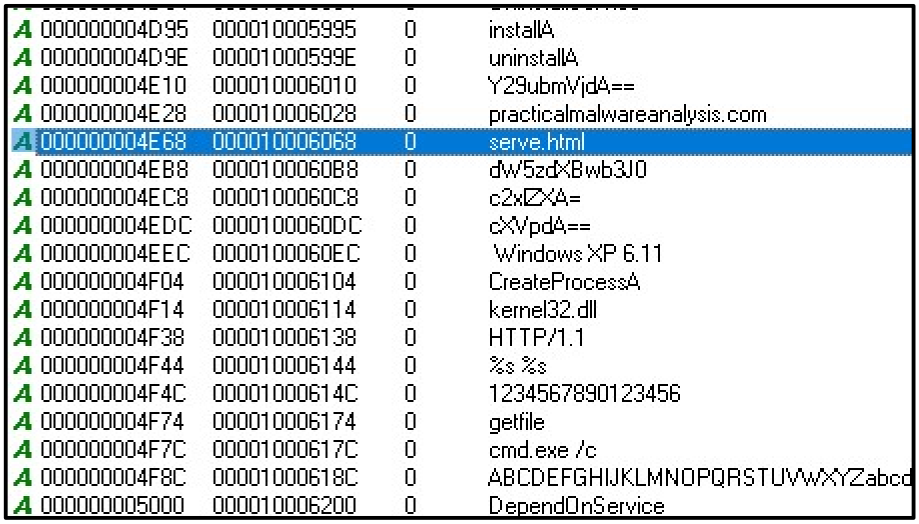
After installing the malware by finding the proper export argument in PEview, a string analysis was conducted in order to find any clues of what the proper commands are to get it to run. There are numerous functions that the malware imports that suggest manipulation of services. From these services, it can be deduced that registry values will be altered, services will be created, and some networking functions over HTTP will be used.



```
A 00000000499E   00001000559E   0   SetLastError
A 0000000049AE   0000100055AE   0   OutputDebugStringA
A 0000000049C2   0000100055C2   0   KERNEL32.dll
A 0000000049D2   0000100055D2   0   RegisterServiceCtrlHandlerA
A 0000000049F0   0000100055F0   0   RegSetValueExA
A 000000004A02   000010005602   0   RegCreateKeyA
A 000000004A12   000010005612   0   CloseServiceHandle
A 000000004A28   000010005628   0   CreateServiceA
A 000000004A3A   00001000563A   0   OpenSCManagerA
A 000000004A4C   00001000564C   0   RegCloseKey
A 000000004A5A   00001000565A   0   RegQueryValueExA
A 000000004A6E   00001000566E   0   RegOpenKeyExA
A 000000004A7E   00001000567E   0   DeleteService
A 000000004A8E   00001000568E   0   OpenServiceA
A 000000004A9E   00001000569E   0   SetServiceStatus
A 000000004AB0   0000100056B0   0   ADVAPI32.dll
A 000000004AC0   0000100056C0   0   WSASocketA
A 000000004ACC   0000100056CC   0   WS2_32.dll
A 000000004ADA   0000100056DA   0   InternetReadFile
A 000000004AEE   0000100056EE   0   HttpQueryInfoA
A 000000004B00   000010005700   0   HttpSendRequestA
A 000000004B14   000010005714   0   HttpOpenRequestA
A 000000004B28   000010005728   0   InternetConnectA
A 000000004B3C   00001000573C   0   InternetOpenA
A 000000004B4C   00001000574C   0   InternetCloseHandle
A 000000004B60   000010005760   0   WININET.dll
A 000000004B6E   00001000576E   0   memset
A 000000004B78   000010005778   0   wcstombs
A 000000004B84   000010005784   0   strncpy
A 000000004B8E   00001000578E   0   strcat
A 000000004B98   000010005798   0   strcpy
```

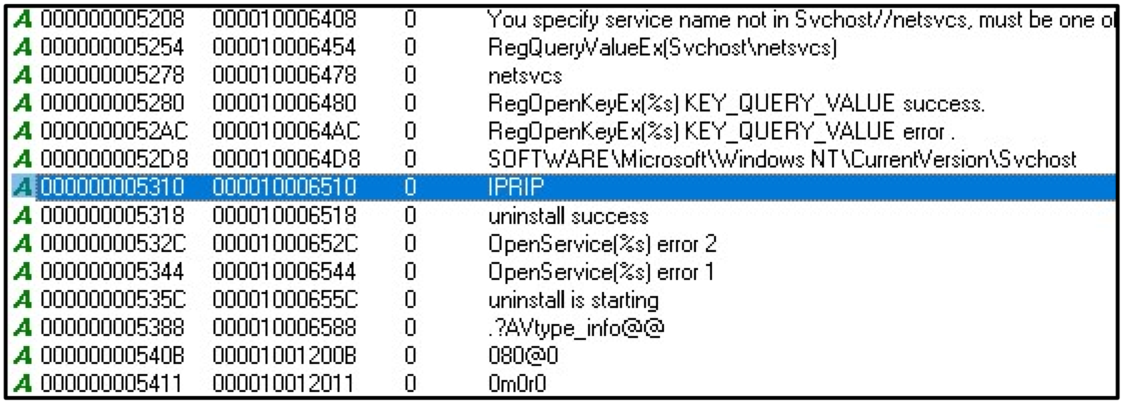
Figure 21: Lab03-02.dll imported functions.

Some more notable features on the string analysis are “serve.html”, “IPRIP”, and calls to edit registry keys (Figures 22 and 23). To figure out how to run this malware, RegShot and Process Monitor will be used to verify the changes the malware makes during installation.



```
A 000000004D95   000010005995   0   installA
A 000000004D9E   00001000599E   0   uninstallA
A 000000004E10   000010006010   0   Y29ubmVjdA==
A 000000004E28   000010006028   0   practicalmalwareanalysis.com
A 000000004E68   000010006068   0   serve.html
A 000000004EB8   0000100060B8   0   dW5zdXBwb3J0
A 000000004EC8   0000100060C8   0   c2xlZXA=
A 000000004EDC   0000100060DC   0   cXVpdA==
A 000000004EEC   0000100060EC   0    Windows XP 6.11
A 000000004F04   000010006104   0   CreateProcessA
A 000000004F14   000010006114   0   kernel32.dll
A 000000004F38   000010006138   0   HTTP/1.1
A 000000004F44   000010006144   0   %s %s
A 000000004F4C   00001000614C   0   1234567890123456
A 000000004F74   000010006174   0   getfile
A 000000004F7C   00001000617C   0   cmd.exe /c
A 000000004F8C   00001000618C   0   ABCDEFGHIJKLMNOPQRSTUVWXYZabcd
A 000000005000   000010006200   0   DependOnService
```

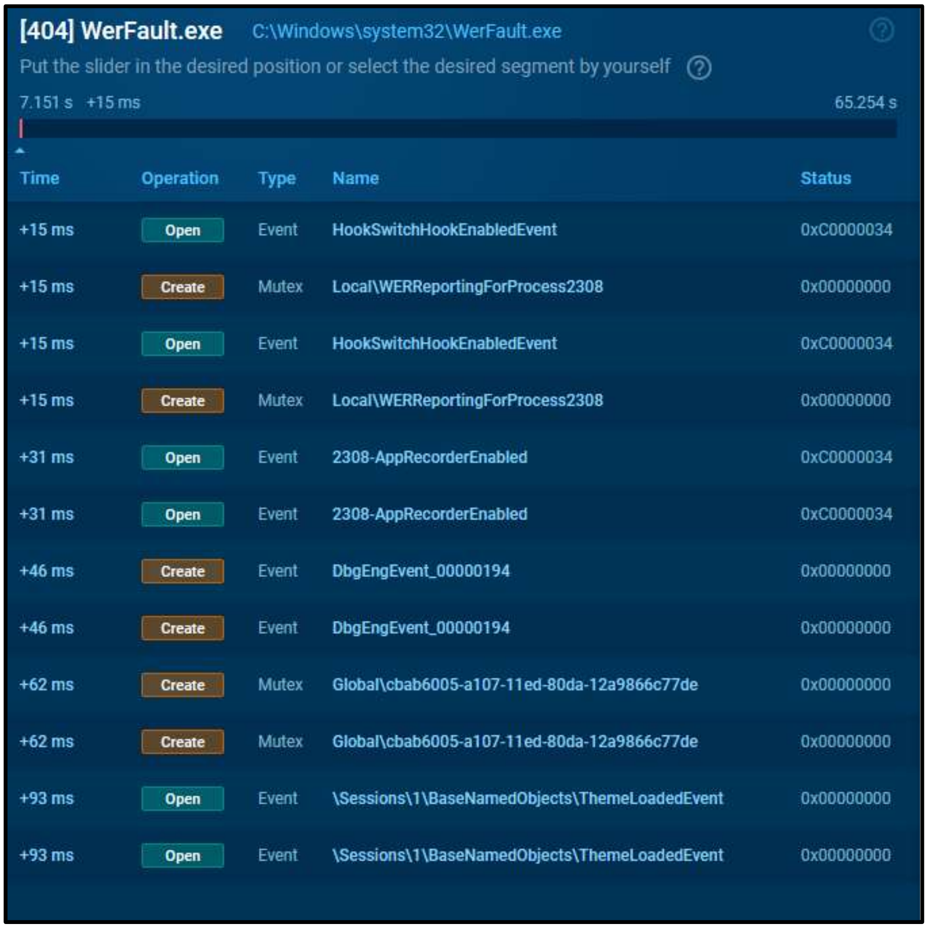
Figure 22: Lab03-02.dll serve.html.



```
A 000000005208   000010006408   0   You specify service name not in Svchost//netsvcs, must be one o
A 000000005254   000010006454   0   RegQueryValueEx(Svchost\netsvcs)
A 000000005278   000010006478   0   netsvcs
A 000000005280   000010006480   0   RegOpenKeyEx(%s) KEY_QUERY_VALUE success.
A 0000000052AC   0000100064AC   0   RegOpenKeyEx(%s) KEY_QUERY_VALUE error .
A 0000000052D8   0000100064D8   0   SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost
A 000000005310   000010006510   0   IPRIP
A 000000005318   000010006518   0   uninstall success
A 00000000532C   00001000652C   0   OpenService(%s) error 2
A 000000005344   000010006544   0   OpenService(%s) error 1
A 00000000535C   00001000655C   0   uninstall is starting
A 000000005388   000010006588   0   .?AVtype_info@@
A 00000000540B   00001001200B   0   080@0
A 000000005411   000010012011   0   0m0r0
```

Figure 23: Lab03-02.dll IPRIP.

Within a Windows 10 VM Windows, installing Lab03-02.dll did not produce any viable results. Regshot showed failed registry edits and, like Lab03-01.exe, Process Monitor noted multiple instances of WerFault.exe. A Windows 7 VM (app.any.run) also produced the same output as Lab03-01.exe with an error message stating that the file stopped working but did note that malicious activity was detected by WerFault.exe due to the creation of mutexes (Figure 24). This necessitated an attempt to install the .dll on a WindowsXP machine.



[404] WerFault.exe C:\Windows\system32\WerFault.exe

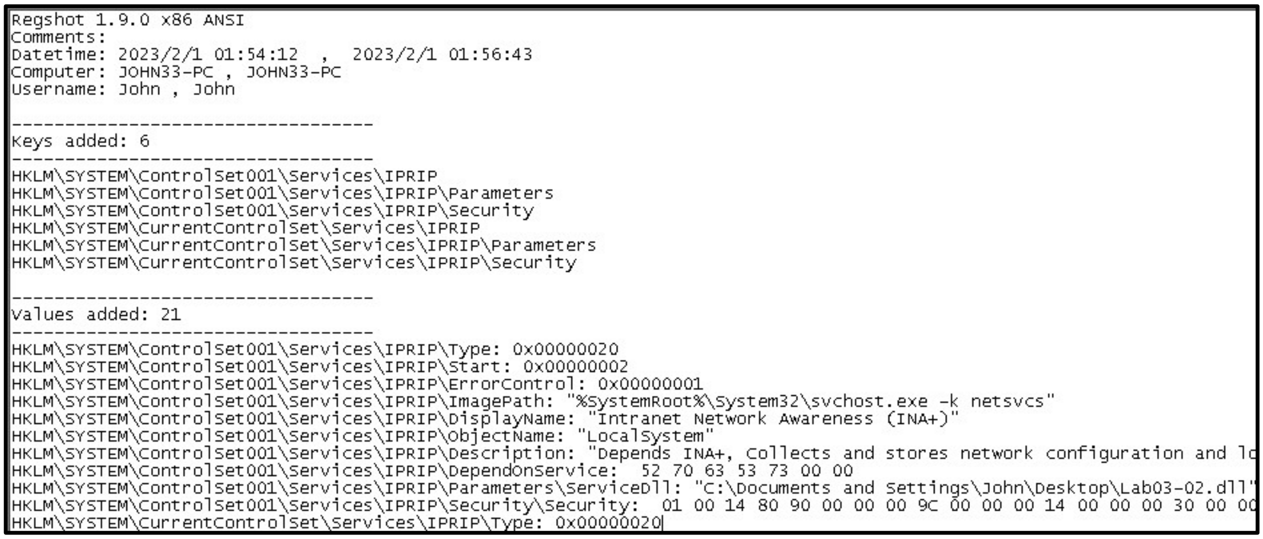
Put the slider in the desired position or select the desired segment by yourself

7.151 s +15 ms 65.254 s

Time	Operation	Type	Name	Status
+15 ms	Open	Event	HookSwitchHookEnabledEvent	0xC0000034
+15 ms	Create	Mutex	Local\WERReportingForProcess2308	0x00000000
+15 ms	Open	Event	HookSwitchHookEnabledEvent	0xC0000034
+15 ms	Create	Mutex	Local\WERReportingForProcess2308	0x00000000
+31 ms	Open	Event	2308-AppRecorderEnabled	0xC0000034
+31 ms	Open	Event	2308-AppRecorderEnabled	0xC0000034
+46 ms	Create	Event	DbgEngEvent_00000194	0x00000000
+46 ms	Create	Event	DbgEngEvent_00000194	0x00000000
+62 ms	Create	Mutex	Global\cbab6005-a107-11ed-80da-12a9866c77de	0x00000000
+62 ms	Create	Mutex	Global\cbab6005-a107-11ed-80da-12a9866c77de	0x00000000
+93 ms	Open	Event	\Sessions\1\BaseNamedObjects\ThemeLoadedEvent	0x00000000
+93 ms	Open	Event	\Sessions\1\BaseNamedObjects\ThemeLoadedEvent	0x00000000

Figure 24: app.any.run report of Lab03-02.dll.

After installing the malware on a Windows XP VM, the results provided more indications of the changes it made. Regshot captured key and value additions to the registry with they keyword of IPRIP which was identified in the strings analysis (Figure 25). Additionally, Process Monitor identified similar activity in the registry (Figure 26). Paying close attention to the Regshot capture in Figure 25, there is a path set to the "svchost.exe" application which can be reasonably deduced that svchost.exe is the application used by the malware to perform its function. This would require installing the malware as a service by using the command, "rundll32.exe Lab03-02.dll, installA IPRIP" since IPRIP is an executable .dll file. It can then be run with the command "net start IPRIP".

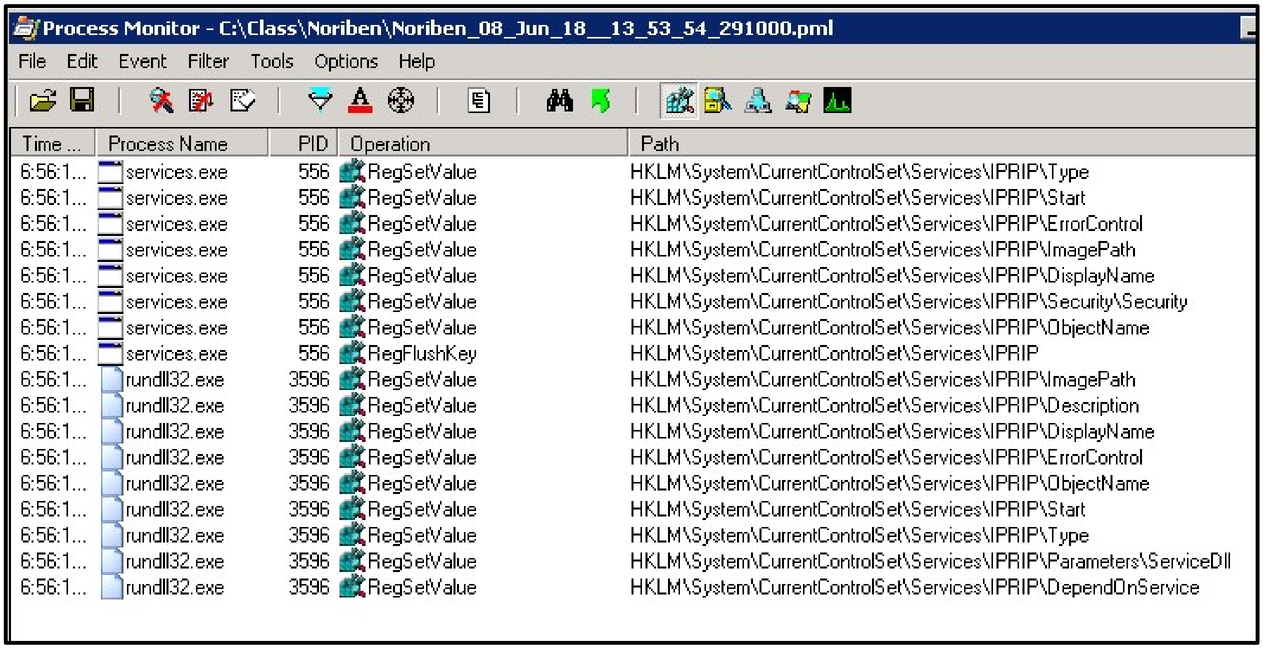


```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2023/2/1 01:54:12  ,  2023/2/1 01:56:43
Computer: JOHN33-PC , JOHN33-PC
Username: John , John

----------------------------------
Keys added: 6
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security

----------------------------------
Values added: 21
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and lo
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService:  52 70 63 53 73 00 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\John\Desktop\Lab03-02.dll"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Type: 0x00000020
```

Figure 25: Regshot results after installing Lab03-02.dll.



Process Monitor - C:\Class\Noriben\Noriben_08_Jun_18__13_53_54_291000.pml
File
Edit
Event
Filter
Tools
Options
Help

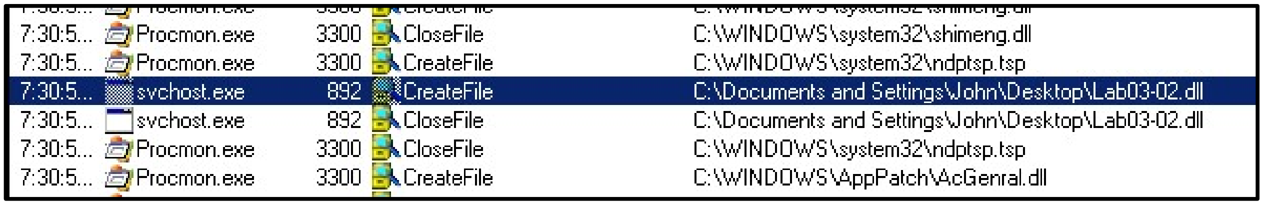
Time ...	Process Name	PID	Operation	Path
6:56:1...	services.exe	556	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\Type
6:56:1...	services.exe	556	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\Start
6:56:1...	services.exe	556	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\ErrorControl
6:56:1...	services.exe	556	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\ImagePath
6:56:1...	services.exe	556	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\DisplayName
6:56:1...	services.exe	556	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\Security\Security
6:56:1...	services.exe	556	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\ObjectName
6:56:1...	services.exe	556	RegFlushKey	HKLM\System\CurrentControlSet\Services\IPRIP
6:56:1...	rundll32.exe	3596	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\ImagePath
6:56:1...	rundll32.exe	3596	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\Description
6:56:1...	rundll32.exe	3596	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\DisplayName
6:56:1...	rundll32.exe	3596	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\ErrorControl
6:56:1...	rundll32.exe	3596	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\ObjectName
6:56:1...	rundll32.exe	3596	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\Start
6:56:1...	rundll32.exe	3596	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\Type
6:56:1...	rundll32.exe	3596	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll
6:56:1...	rundll32.exe	3596	RegSetValue	HKLM\System\CurrentControlSet\Services\IPRIP\DependOnService

Figure 26: Process Monitor results after installing Lab03-02.dll.

LAB 3-2 Question 3

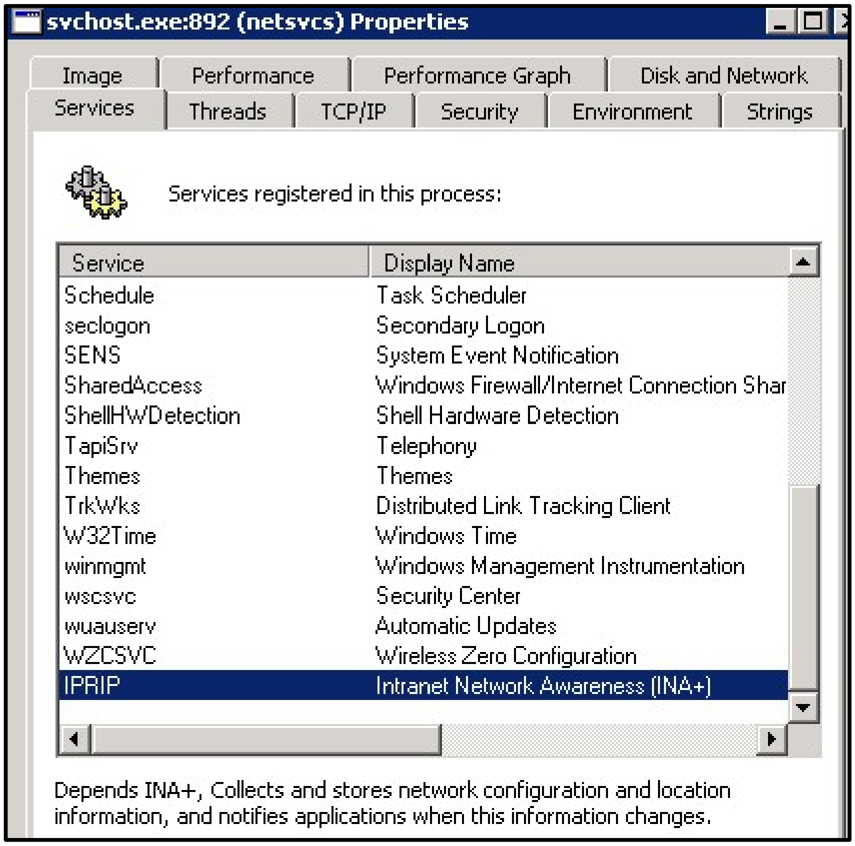
How can you find the process under which this malware is running?

After installing the malware with run32dll.exe and running the command "net start IPRIP," Process Monitor and Wireshark captures were made. Process Monitor captured that Lab03-02.dll used the process svchost.exe (Figure 27). A brief check in Process Explorer revealed that IPRIP was indeed running under this process (Figure 28).



```
7:30:5...  Procmon.exe   3300  CloseFile    C:\WINDOWS\system32\shimeng.dll
7:30:5...  Procmon.exe   3300  CreateFile   C:\WINDOWS\system32\ndptsp.tsp
7:30:5...  svchost.exe    892  CreateFile   C:\Documents and Settings\John\Desktop\Lab03-02.dll
7:30:5...  svchost.exe    892  CloseFile    C:\Documents and Settings\John\Desktop\Lab03-02.dll
7:30:5...  Procmon.exe   3300  CloseFile    C:\WINDOWS\system32\ndptsp.tsp
7:30:5...  Procmon.exe   3300  CreateFile   C:\WINDOWS\AppPatch\AcGenral.dll
```

Figure 27: Lab03-02.dll uses svchost.exe.



svchost.exe:892 (netsvcs) Properties

Services registered in this process:

Service	Display Name
Schedule	Task Scheduler
seclogon	Secondary Logon
SENS	System Event Notification
SharedAccess	Windows Firewall/Internet Connection Shar
ShellHWDetection	Shell Hardware Detection
TapiSrv	Telephony
Themes	Themes
TrkWks	Distributed Link Tracking Client
W32Time	Windows Time
winmgmt	Windows Management Instrumentation
wscsvc	Security Center
wuauserv	Automatic Updates
WZCSVC	Wireless Zero Configuration
IPRIP	Intranet Network Awareness (INA+)

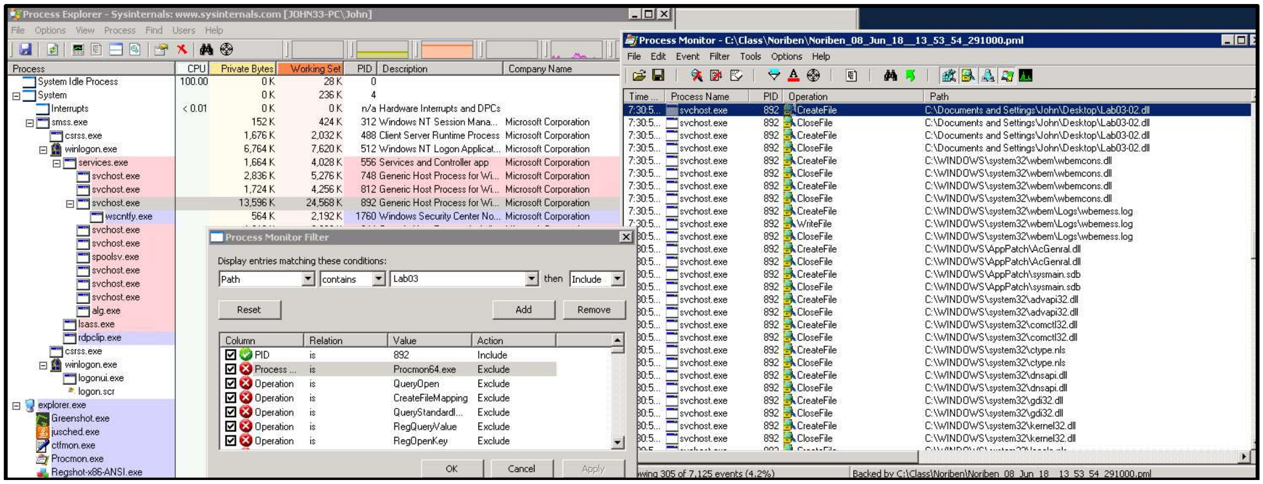
Depends INA+, Collects and stores network configuration and location information, and notifies applications when this information changes.

Figure 28: IPRIP being used under svhost.exe.

LAB 3-2 Question 4

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

Because the malware runs under the process svchost.exe, Process Explorer gives us the PID of svchost.exe that IPRIP is being used under as 892. That filter can be applied to procmon as well as any other useful information to narrow down the breadth of services that svchost.exe runs, such as the path containing “Lab03-02” (Figure 29).


Process Explorer - Sysinternals: www.sysinternals.com [JOHN33-PC\John]
File Options View Process Find Users Help
Process Monitor - C:\Class\Noriben\Noriben_08_Jun_18__13_53_54_291000.pml
File Edit Event Filter Tools Options Help
Process Monitor Filter
Reset
Add
Remove
OK
Cancel
Apply

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	100.00	0 K	28 K	0		
System		0 K	236 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		152 K	424 K	312	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,676 K	2,032 K	488	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,764 K	7,620 K	512	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,664 K	4,028 K	556	Services and Controller app	Microsoft Corporation
svchost.exe		2,836 K	5,276 K	748	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,724 K	4,256 K	812	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13,596 K	24,568 K	892	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		564 K	2,192 K	1760	Windows Security Center No...	Microsoft Corporation
svchost.exe						
svchost.exe						
spoolsv.exe						
svchost.exe						
svchost.exe						
svchost.exe						
alg.exe						
lsass.exe						
rdpclip.exe						
csrss.exe						
winlogon.exe						
logonui.exe						
logon.scr						
explorer.exe						
Greenshot.exe						
jusched.exe						
ctfmon.exe						
Procmon.exe						
Regshot-x86-ANSI.exe						

Display entries matching these conditions:

Path ▼ contains ▼ Lab03 ▼ then Include ▼

Column	Relation	Value	Action
☑ ✓ PID	is	892	Include
☑ ☒ Process ...	is	Procmon64.exe	Exclude
☑ ☒ Operation	is	QueryOpen	Exclude
☑ ☒ Operation	is	CreateFileMapping	Exclude
☑ ☒ Operation	is	QueryStandardI...	Exclude
☑ ☒ Operation	is	RegQueryValue	Exclude
☑ ☒ Operation	is	RegOpenKey	Exclude

Time ...	Process Name	PID	Operation	Path
7:30:5...	svchost.exe	892	CreateFile	C:\Documents and Settings\John\Desktop\Lab03-02.dll
7:30:5...	svchost.exe	892	CloseFile	C:\Documents and Settings\John\Desktop\Lab03-02.dll
7:30:5...	svchost.exe	892	CreateFile	C:\Documents and Settings\John\Desktop\Lab03-02.dll
7:30:5...	svchost.exe	892	CloseFile	C:\Documents and Settings\John\Desktop\Lab03-02.dll
7:30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\system32\wbem\wbemcons.dll
7:30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\system32\wbem\wbemcons.dll
7:30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\system32\wbem\wbemcons.dll
7:30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\system32\wbem\wbemcons.dll
7:30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\system32\wbem\Logs\wbemess.log
7:30:5...	svchost.exe	892	WriteFile	C:\WINDOWS\system32\wbem\Logs\wbemess.log
30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\system32\wbem\Logs\wbemess.log
30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\AppPatch\AcGenral.dll
30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\AppPatch\AcGenral.dll
30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb
30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\AppPatch\sysmain.sdb
30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\system32\advapi32.dll
30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\system32\advapi32.dll
30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\system32\comctl32.dll
30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\system32\comctl32.dll
30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\system32\ctype.nls
30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\system32\ctype.nls
30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\system32\dnsapi.dll
30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\system32\dnsapi.dll
30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\system32\gdi32.dll
30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\system32\gdi32.dll
30:5...	svchost.exe	892	CreateFile	C:\WINDOWS\system32\kernel32.dll
30:5...	svchost.exe	892	CloseFile	C:\WINDOWS\system32\kernel32.dll

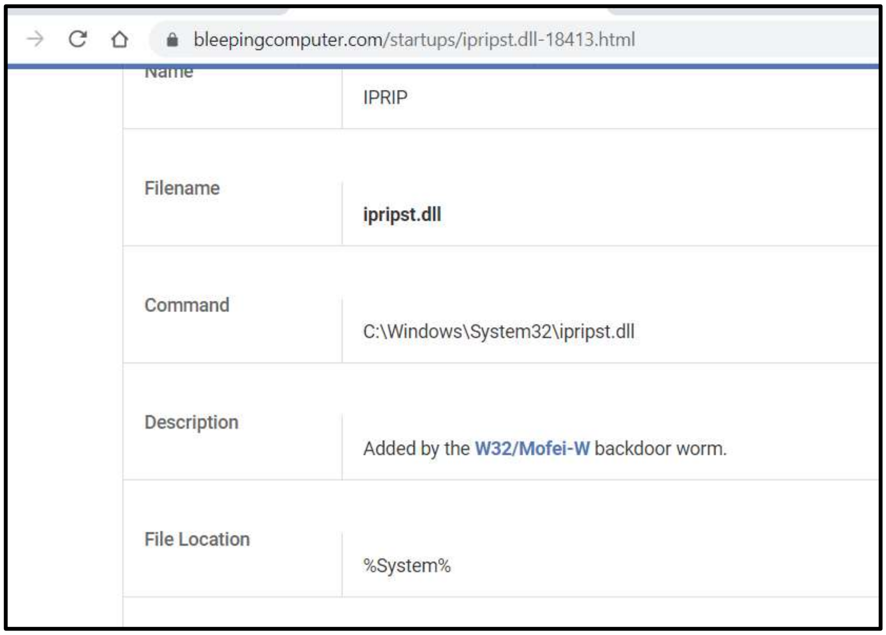
owing 305 of 7,125 events (4.2%) | Backed by C:\Class\Noriben\Noriben_08_Jun_18__13_53_54_291000.pml

Figure 29: Process Monitor Filters.

LAB 3-2 Question 5

What are the malware’s host-based indicators?

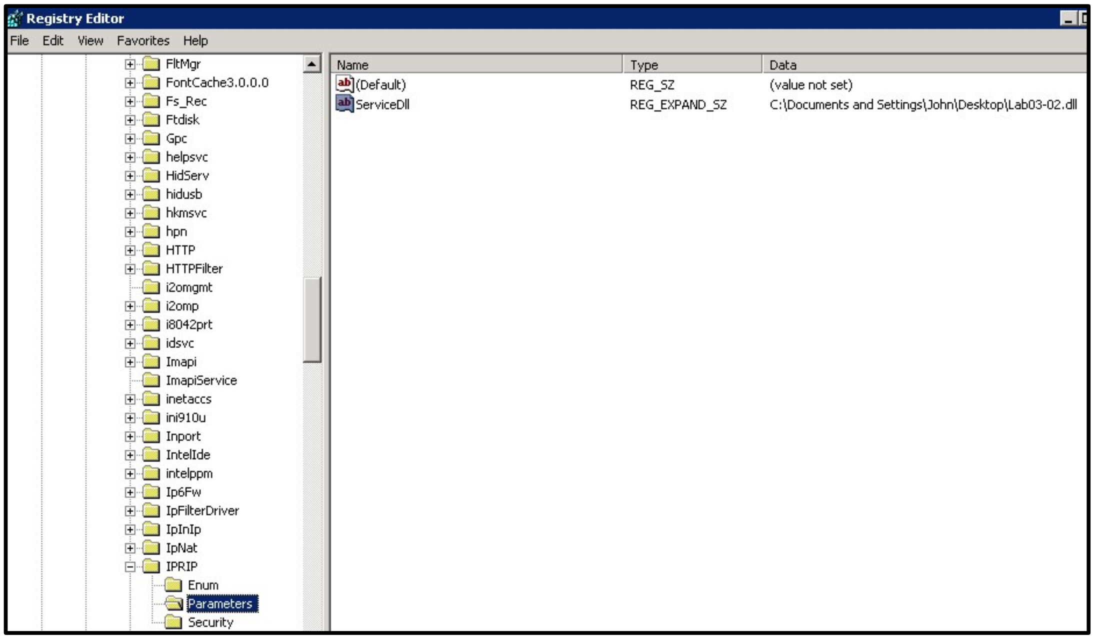
It would be very suspicious to have svchost running the IPRIP service as it has been used, according to bleepingcomputer.com, as a backdoor by other malware in the past (Figure 30). The malware embeds itself in the windows registry under: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPRIP\ Parameters\ServiceDll. The data in ServiceDll shows the name of the file and having ServiceDll data values set is a good host-based indicator of infection (Figre 31). Additionally, when the same path was inspected on an uninfected Windows 10 machine, the IPRIP service did not exist under that path (Figure 32). The mere existence of IPRIP would be a good host-based indicator of infection.



bleepingcomputer.com/startups/ipripst.dll-18413.html

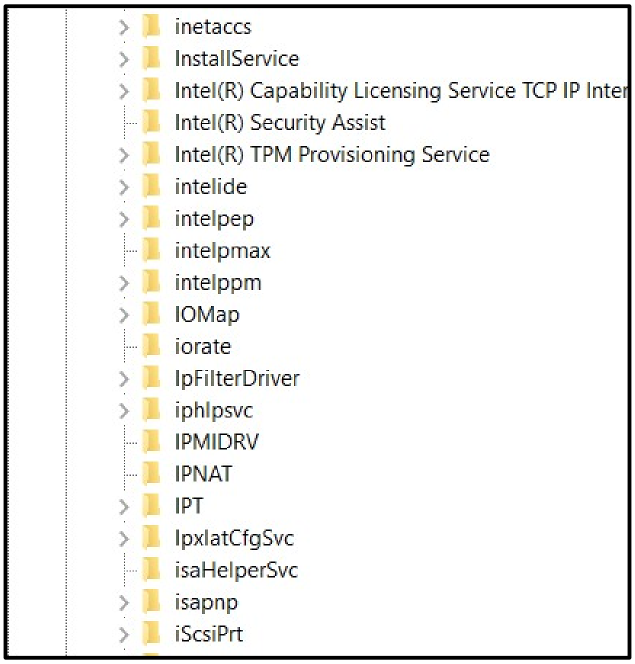
Name	IPRIP
Filename	**ipripst.dll**
Command	C:\Windows\System32\ipripst.dll
Description	Added by the W32/Mofei-W backdoor worm.
File Location	%System%

Figure 31: IPRIP has been used by malware.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ServiceDll	REG_EXPAND_SZ	C:\Documents and Settings\John\Desktop\Lab03-02.dll

Figure 31: Lab03-02.dll located in the registry.



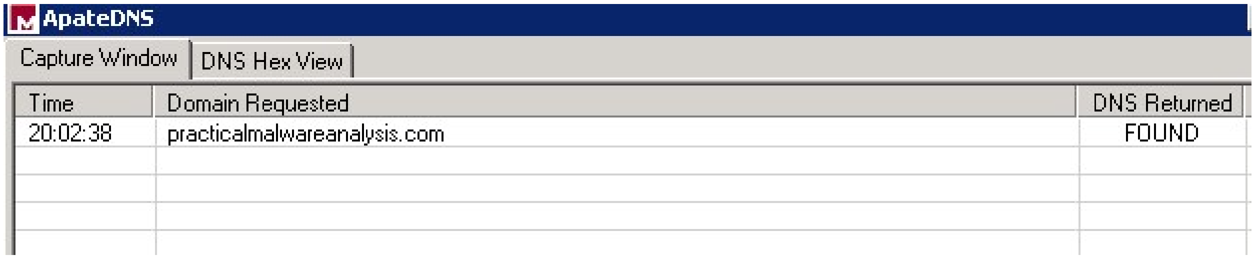
inetaccs
InstallService
Intel(R) Capability Licensing Service TCP IP Inter
Intel(R) Security Assist
Intel(R) TPM Provisioning Service
intelide
intelpep
intelpmax
intelppm
IOMap
iorate
IpFilterDriver
iphlpsvc
IPMIDRV
IPNAT
IPT
IpxlatCfgSvc
isaHelperSvc
isapnp
iScsiPrt

Figure 31: Path to IPRIP service does not exist in an uninfected machine's registry.

LAB 3-2 Question 6

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

The only useful network-based signature that this malware provided was that, every so often, the malware makes a DNS callout to the website, "practicalmalwareanalysis.com" (Figure 32). The network administrator for an enterprise should add this domain to the block list.

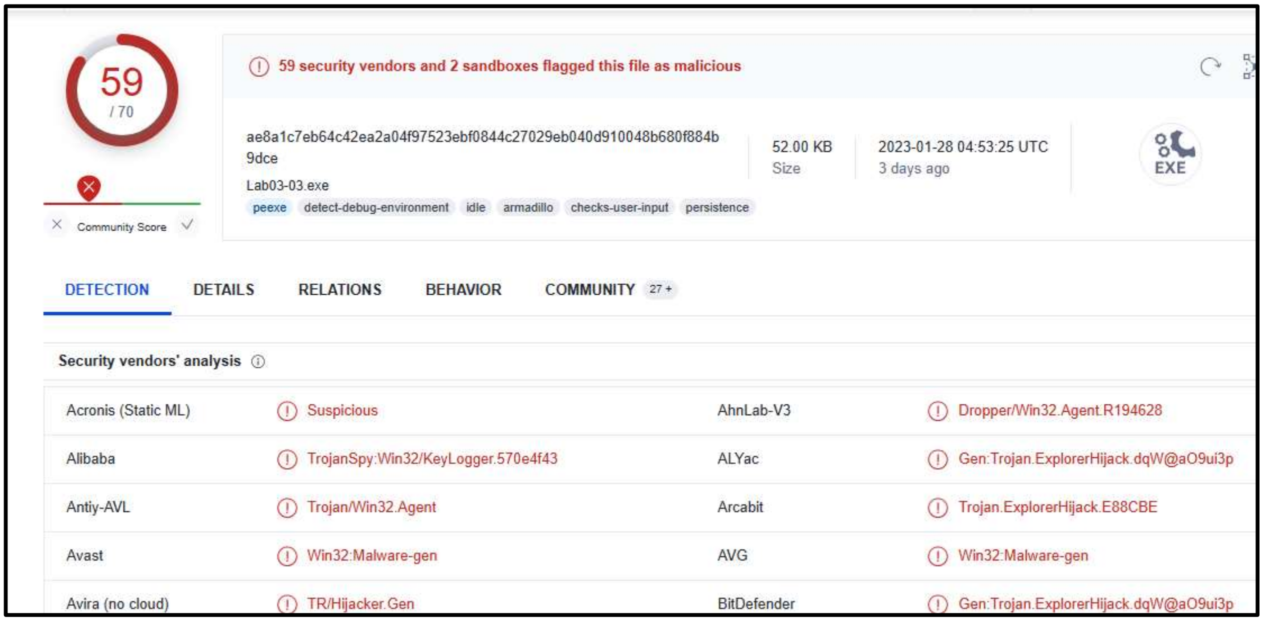


Time	Domain Requested	DNS Returned
20:02:38	practicalmalwareanalysis.com	FOUND

Figure 32: Callout to practicalmalwareanalysis.com.

LAB 3-3

- LAB03-03.exe : e2bf42217a67e46433da8b6f4507219e



59 / 70

Community Score

59 security vendors and 2 sandboxes flagged this file as malicious

ae8a1c7eb64c42ea2a04f97523ebf0844c27029eb040d910048b680f884b9dce

Lab03-03.exe

peexe detect-debug-environment idle armadillo checks-user-input persistence

52.00 KB
Size

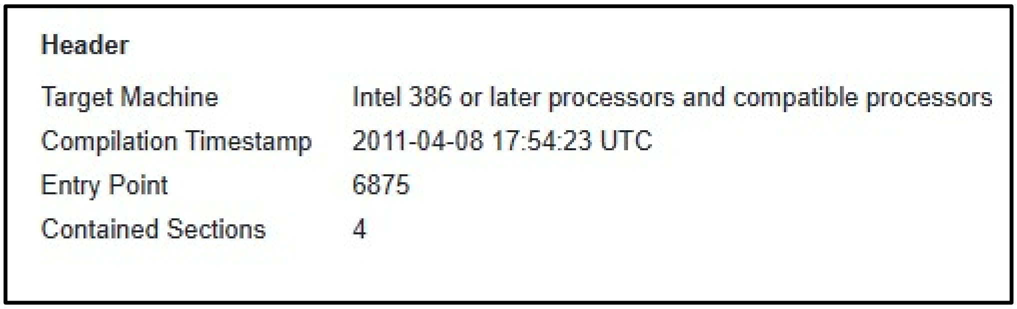
2023-01-28 04:53:25 UTC
3 days ago

Security vendors' analysis

Acronis (Static ML)	Suspicious	AhnLab-V3	Dropper/Win32.Agent.R194628
Alibaba	TrojanSpy:Win32/KeyLogger.570e4f43	ALYac	Gen:Trojan.ExplorerHijack.dqW@aO9ui3p
Antiy-AVL	Trojan/Win32.Agent	Arcabit	Trojan.ExplorerHijack.E88CBE
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Hijacker.Gen	BitDefender	Gen:Trojan.ExplorerHijack.dqW@aO9ui3p

Figure 33: Virus Total Findings for file Lab03-03.exe.

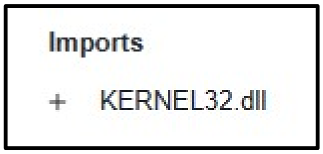
Virus Total found 59 matching signatures for Trojan malware with potential explorer hijack functionality for the file Lab03-03.exe (Figure 33). It has a compilation timestamp of 08 Apr 2011 at 17:54:23 UTC (Figure 34). It appears to only import Kernel32.dll suggesting it manipulates memory, files, and other hardware (Figure 35). Under the "Behavior" tab, it is noted that the malware executes by using process hollowing and attempting to dynamically load functions (Figure 36). It has indicators of privilege escalation and defense evasion (Figures 36 and 37). Noting that it has input capture characteristics, it is possible that this malware is a keylogger, sending the inputs back to a Command and Control host since it performs DNS lookups (Figure 38).



Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2011-04-08 17:54:23 UTC
Entry Point	6875
Contained Sections	4

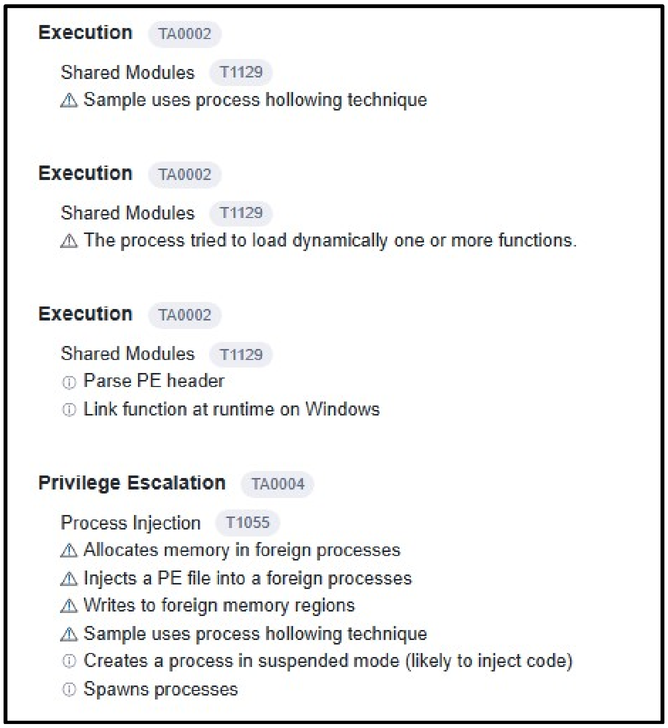
Figure 34: Virus Total Compilation Timestamp for file Lab03-03.exe.



Imports

+ KERNEL32.dll

Figure 35: Virus Total Import for file Lab03-03.exe



Execution TA0002

Shared Modules T1129
⚠ Sample uses process hollowing technique

Execution TA0002

Shared Modules T1129
⚠ The process tried to load dynamically one or more functions.

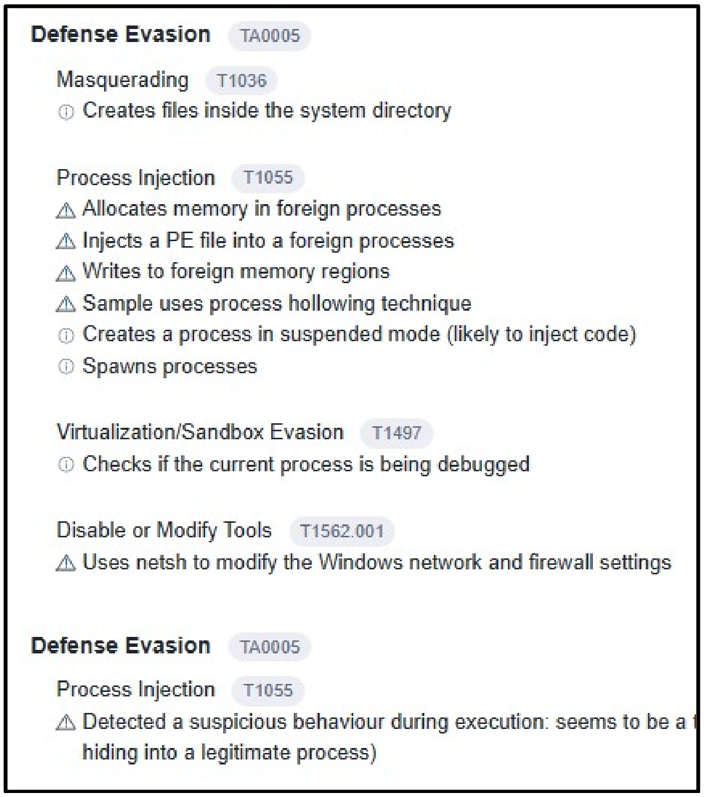
Execution TA0002

Shared Modules T1129
ⓘ Parse PE header
ⓘ Link function at runtime on Windows

Privilege Escalation TA0004

Process Injection T1055
⚠ Allocates memory in foreign processes
⚠ Injects a PE file into a foreign processes
⚠ Writes to foreign memory regions
⚠ Sample uses process hollowing technique
ⓘ Creates a process in suspended mode (likely to inject code)
ⓘ Spawns processes

Figure 36: Virus Total behavior for file Lab03-03.exe.



Defense Evasion TA0005

Masquerading T1036

ⓘ Creates files inside the system directory

Process Injection T1055

⚠ Allocates memory in foreign processes

⚠ Injects a PE file into a foreign processes

⚠ Writes to foreign memory regions

⚠ Sample uses process hollowing technique

ⓘ Creates a process in suspended mode (likely to inject code)

ⓘ Spawns processes

Virtualization/Sandbox Evasion T1497

ⓘ Checks if the current process is being debugged

Disable or Modify Tools T1562.001

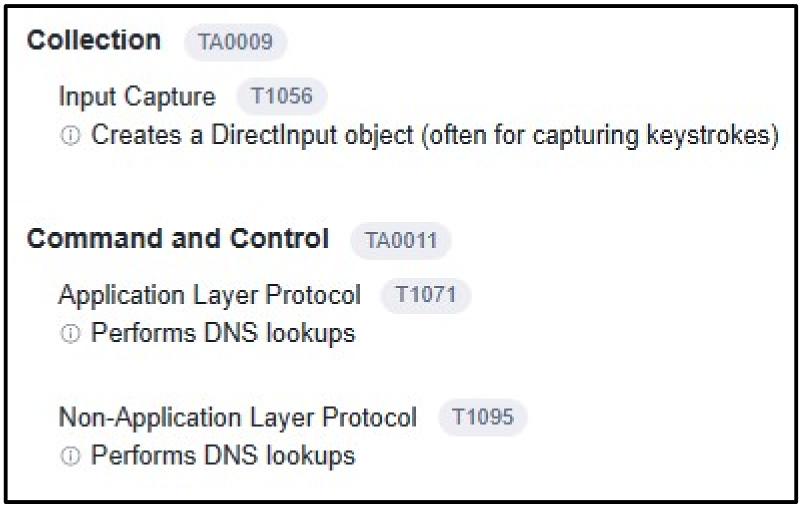
⚠ Uses netsh to modify the Windows network and firewall settings

Defense Evasion TA0005

Process Injection T1055

⚠ Detected a suspicious behaviour during execution: seems to be a hiding into a legitimate process)

Figure 37: Virus Total behavior for file Lab03-03.exe.



Collection TA0009

Input Capture T1056

ⓘ Creates a DirectInput object (often for capturing keystrokes)

Command and Control TA0011

Application Layer Protocol T1071

ⓘ Performs DNS lookups

Non-Application Layer Protocol T1095

ⓘ Performs DNS lookups

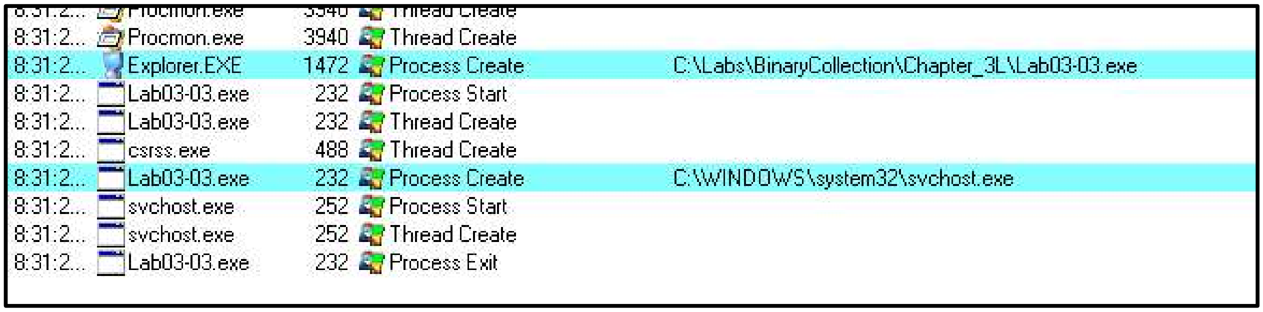
Figure 38: Virus Total C&C for file Lab03-03.exe.

LAB 3-3

LAB 3-3 Question 1

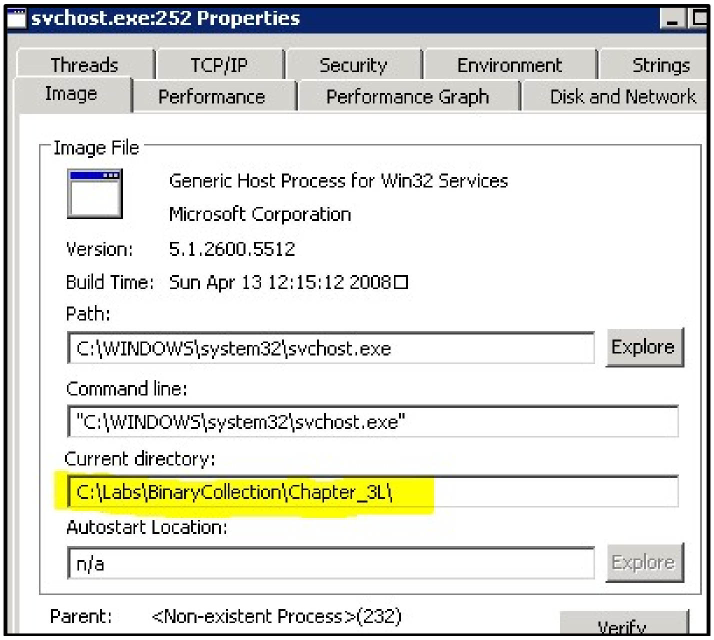
What do you notice when monitoring this malware with Process Explorer?

To first get an indication of what the malware would look like in process explorer, Process Monitor was used to create a capture first. From the capture, the process that would be used by the malware, and therefore the process to look for in Process Explorer, would be svchost.exe (Figure 39). This is confirmed by examining a svchost.exe instance in Process Explorer and that it is accessing the current directory where the malware is stored (Figure 40).



```
8:31:2...  Procmon.exe   3940  Thread Create
8:31:2...  Procmon.exe   3940  Thread Create
8:31:2...  Explorer.EXE  1472  Process Create   C:\Labs\BinaryCollection\Chapter_3L\Lab03-03.exe
8:31:2...  Lab03-03.exe   232  Process Start
8:31:2...  Lab03-03.exe   232  Thread Create
8:31:2...  csrss.exe      488  Thread Create
8:31:2...  Lab03-03.exe   232  Process Create   C:\WINDOWS\system32\svchost.exe
8:31:2...  svchost.exe    252  Process Start
8:31:2...  svchost.exe    252  Thread Create
8:31:2...  Lab03-03.exe   232  Process Exit
```

Figure 39: Lab03-03.exe uses svchost.exe to run.



svchost.exe:252 Properties

Generic Host Process for Win32 Services

Microsoft Corporation

Version: 5.1.2600.5512

Build Time: Sun Apr 13 12:15:12 2008□

Path: C:\WINDOWS\system32\svchost.exe

Command line: "C:\WINDOWS\system32\svchost.exe"

Current directory: C:\Labs\BinaryCollection\Chapter_3L\

Autostart Location: n/a

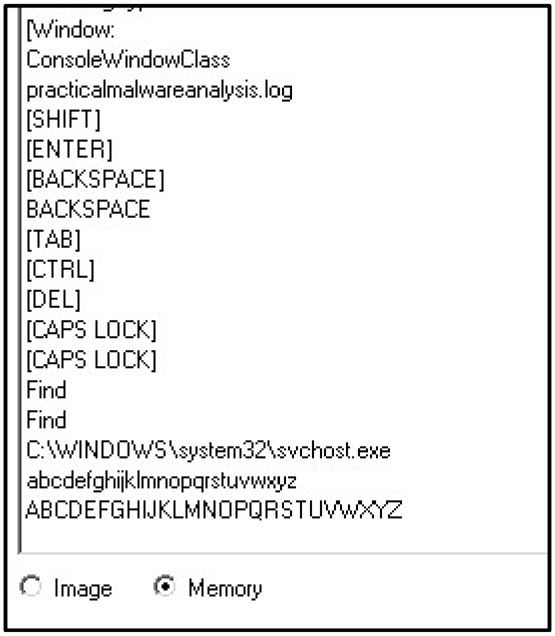
Parent: <Non-existent Process>(232)

Figure 40: svchost.exe running in the malware's directory.

LAB 3-3 Question 2

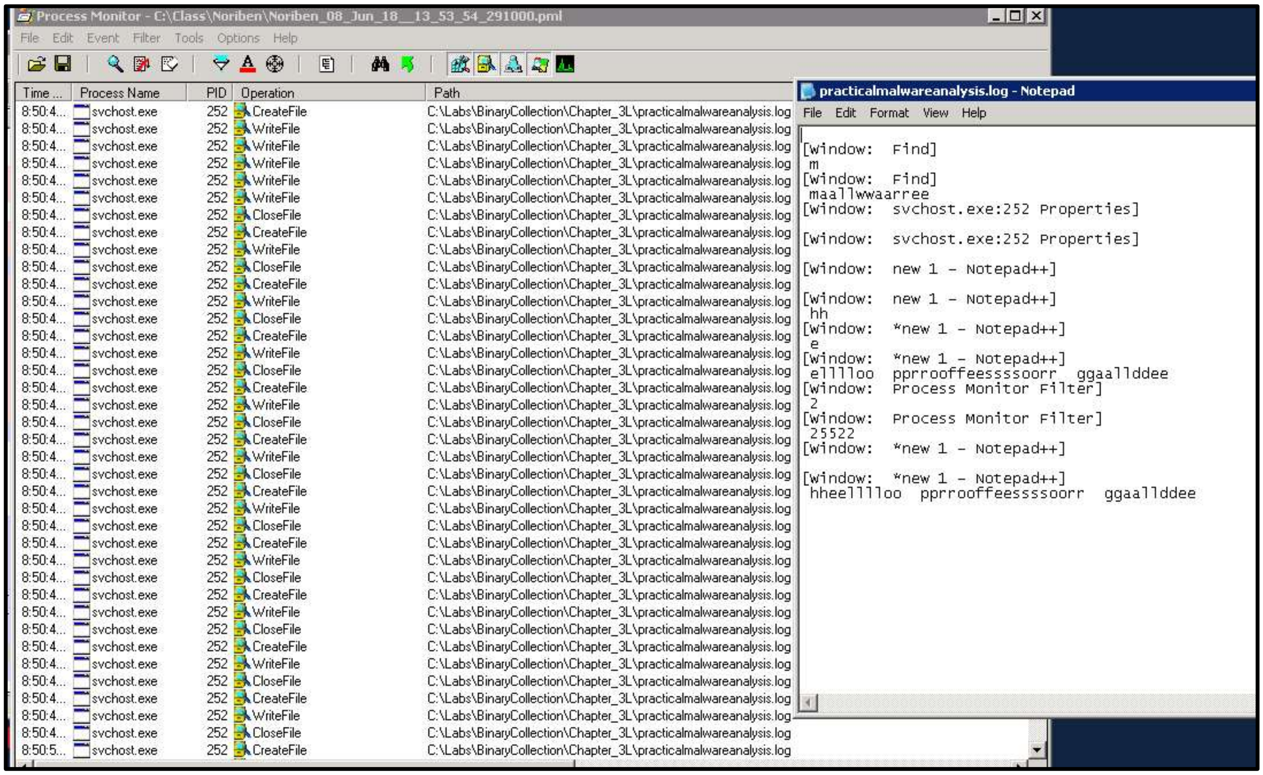
Can you identify any live memory modifications?

In the “Properties” window of svchost.exe running the malware, the “Strings” tab offers an option to view not only the image of the running process, but also the memory. The process has multiple printable strings that are suspicious in the memory. There is a reference to a suspicious URL of practicalmalwareanalysis.log as well as what appears to be keyboard inputs of “[SHIFT]”, “[BACKSPACE]”, etc. (Figure 41). This string pattern is highly suggestive of the malware being a keylogger, a potential behavior characteristic identified by Virus Total. To test this, the svchost.exe PID of 252 was added as a filter into procmon and some text was typed into a notepad document. The PID captured every keystroke and stored it in the directory from which the malware was running (Figure 42).



```
[Window:
ConsoleWindowClass
practicalmalwareanalysis.log
[SHIFT]
[ENTER]
[BACKSPACE]
BACKSPACE
[TAB]
[CTRL]
[DEL]
[CAPS LOCK]
[CAPS LOCK]
Find
Find
C:\WINDOWS\system32\svchost.exe
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Figure 41: Lab03-03.exe memory strings.


Process Monitor - C:\Class\Noriben\Noriben_08_Jun_18__13_53_54_291000.pml
File Edit Event Filter Tools Options Help
practicalmalwareanalysis.log - Notepad
File Edit Format View Help

```
Time ...  Process Name  PID  Operation   Path
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  WriteFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:4... svchost.exe   252  CloseFile   C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
8:50:5... svchost.exe   252  CreateFile  C:\Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
```

```

[Window:  Find]
 m
[Window:  Find]
 maallwwaarree
[Window:  svchost.exe:252 Properties]

[Window:  svchost.exe:252 Properties]

[Window:  new 1 - Notepad++]

[Window:  new 1 - Notepad++]
 hh
[Window:  *new 1 - Notepad++]
 e
[Window:  *new 1 - Notepad++]
 ellllоо  pprrooffeessssoorr  ggaallddee
[Window:  Process Monitor Filter]
 2
[Window:  Process Monitor Filter]
 25522
[Window:  *new 1 - Notepad++]

[Window:  *new 1 - Notepad++]
 hheellllоо  pprrooffeessssoorr  ggaallddee
```

Figure 42: Lab03-03.exe stores keystrokes in a .txt file in its directory.

LAB 3-3 Question 3

What are the malware's host-based indicators?

For this particular malware, the most noticeable host-based indicator was the generation of a .txt file titled, "practicalmalwareanalysis.log." The presence of a file of this extension and name on a host system would not only be indicative of infection, but also help point to the directory in which the malware is installed (Figure 43). If the malware was modified in any way to change the name or location of which the directory is stored, then using procmon to monitor svchost.exe PIDs while simultaneously pressing buttons on the keyboard to live-capture memory. The malware was tested by entering strings in a .txt file and randomly on the screen, both of which were captured by the malware.

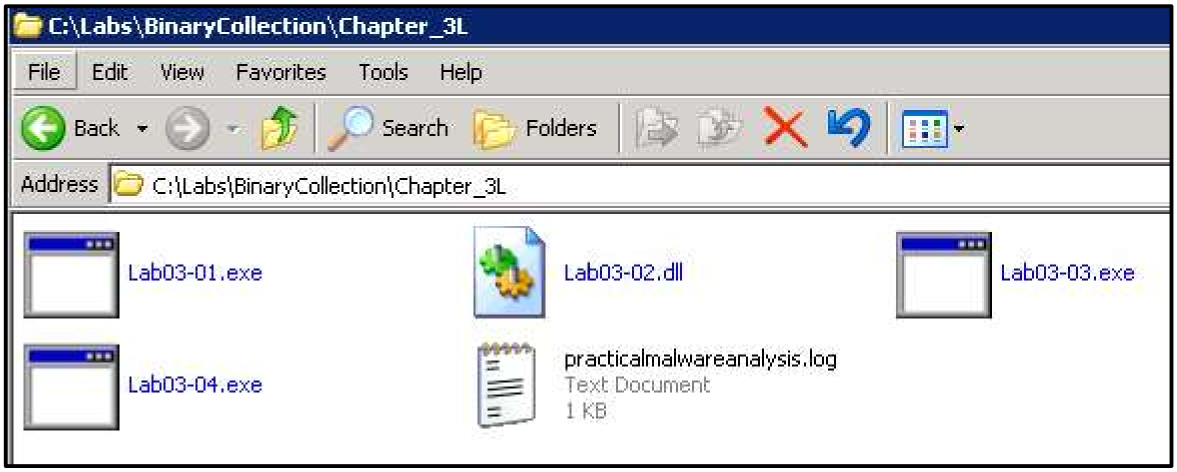


Figure 43: practicalmalwareanalysis.log is stored in the directory of the malware.

LAB 3-3 Question 4

What is the purpose of this program?

It is extraordinarily clear that this malware is a keylogger. However, procmon did not detect any attempts to send that information to a remote host (Figure 44). This would lead to the reasonable assumption that someone with malicious intent on capturing the keystrokes of a user would have access to the machine of that user. This would then mean that those two individuals likely live in close proximity, if not cohabitate with each other. Likely, a keylogger of this type would be used by a jealous, malicious, or otherwise ill-intended person trying to spy on their significant other.

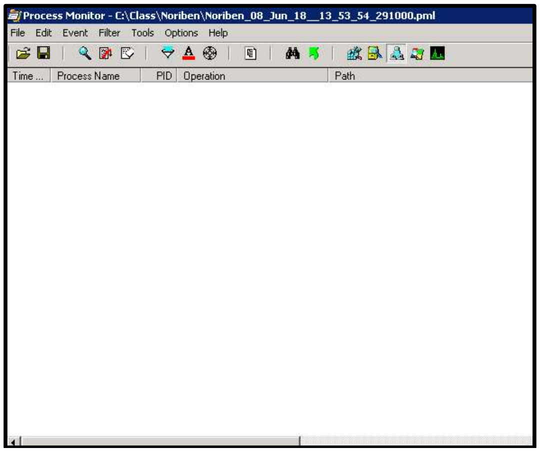
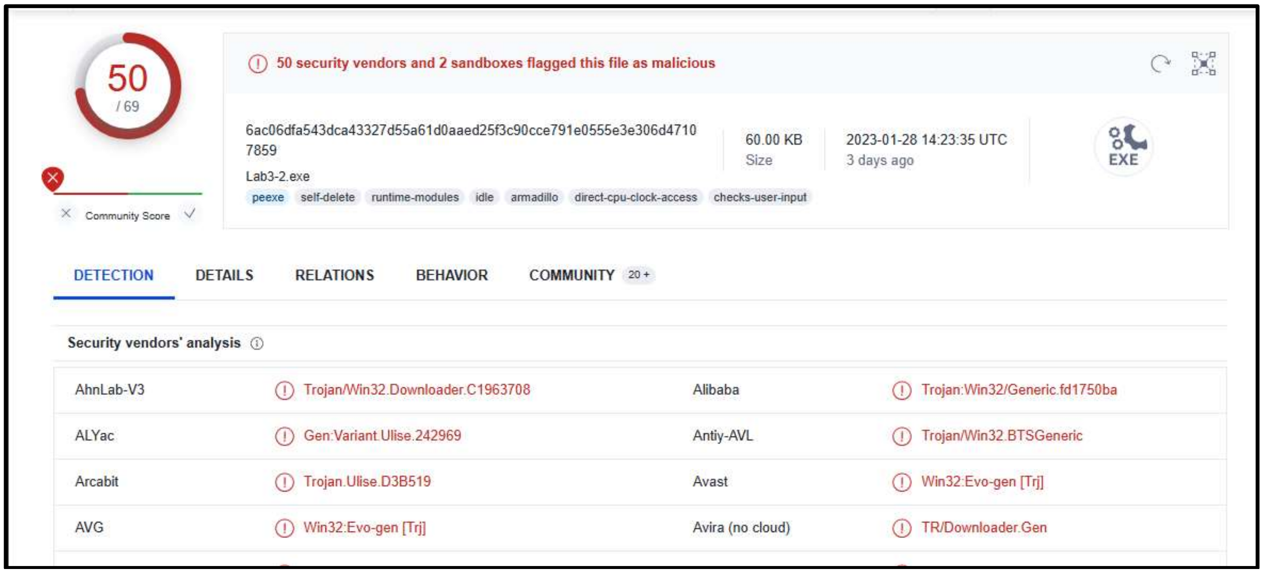

Process Monitor - C:\Class\Noriben\Noriben_08_Jun_18__13_53_54_291000.pml
File
Edit
Event
Filter
Tools
Options
Help
Time ...
Process Name
PID
Operation
Path

Figure 44: Lab03-03.exe did not have any network traffic.

LAB 3-4

- LAB03-04.exe : b94af4a4d4af6eac81fc135abda1c40c



50 / 69

Community Score

50 security vendors and 2 sandboxes flagged this file as malicious

6ac06dfa543dca43327d55a61d0aaed25f3c90cce791e0555e3e306d4710 7859

Lab3-2.exe

peexe self-delete runtime-modules idle armadillo direct-cpu-clock-access checks-user-input

60.00 KB Size

2023-01-28 14:23:35 UTC 3 days ago

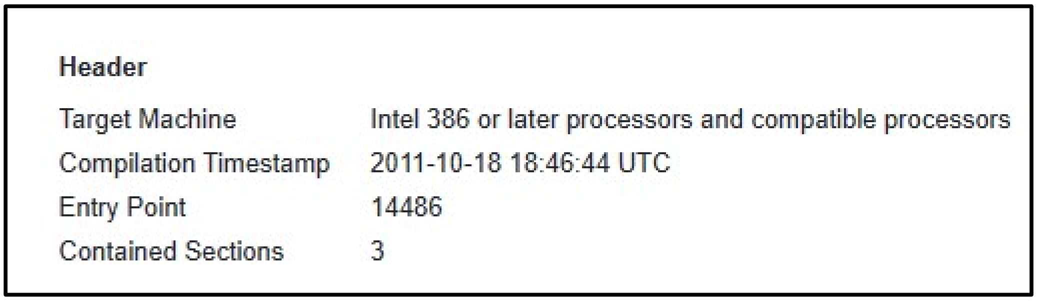
EXE

Security vendors' analysis

AhnLab-V3	Trojan/Win32.Downloader.C1963708	Alibaba	Trojan:Win32/Generic.fd1750ba
ALYac	Gen:Variant.Ulise.242969	Antiy-AVL	Trojan/Win32.BTSGeneric
Arcabit	Trojan.Ulise.D3B519	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	TR/Downloader.Gen

Figure 45: Virus Total Findings for file Lab03-04.exe.

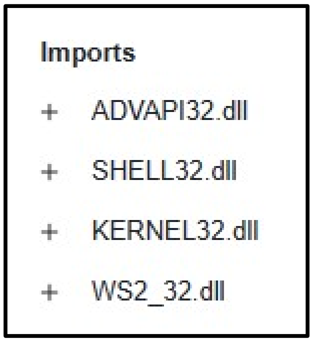
Virus Total found 50 matching signatures for Trojan malware for the file Lab03-04.exe (Figure 45). It has a compilation timestamp of 18 Oct 2011 at 18:46:44UTC (Figure 46). It appears to import Kernel32.dll and advapi32.dll, suggesting it manipulates memory, files, and other hardware as well as the potential to edit the registry. The additional imports of shell32.dll and ws2_32.dll suggest that it possibly opens a shell and connects to the internet, allowing for a remote domain or host to upload or even remotely connect to the infected machine (Figure 47). Under the "Behavior" tab, it is noted that the malware has other indicators of persistence and privilege escalation, as well as creating a process that is likely to inject code (Figure 48). Noting that it has input capture characteristics, it is possible that this malware has characteristics of a keylogger and has some functionality to perform downloads and file writing (Figure 49).



Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2011-10-18 18:46:44 UTC
Entry Point	14486
Contained Sections	3

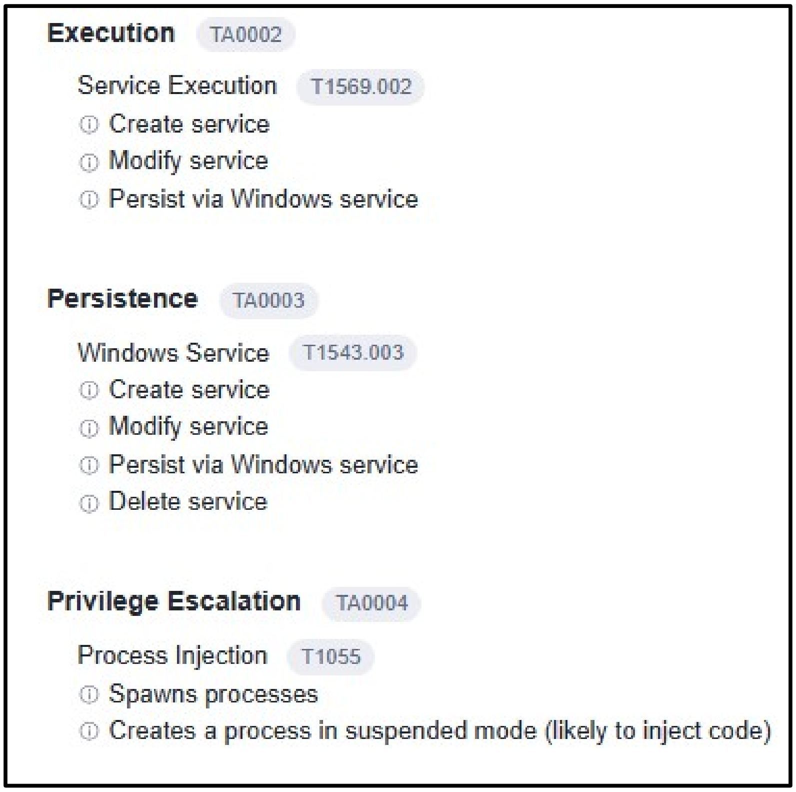
Figure 46: Virus Total compilation timestamp for file Lab03-04.exe.



Imports

- + ADVAPI32.dll
- + SHELL32.dll
- + KERNEL32.dll
- + WS2_32.dll

Figure 47: Virus Total imports for file Lab03-04.exe.



Execution TA0002

Service Execution T1569.002

ⓘ Create service

ⓘ Modify service

ⓘ Persist via Windows service

Persistence TA0003

Windows Service T1543.003

ⓘ Create service

ⓘ Modify service

ⓘ Persist via Windows service

ⓘ Delete service

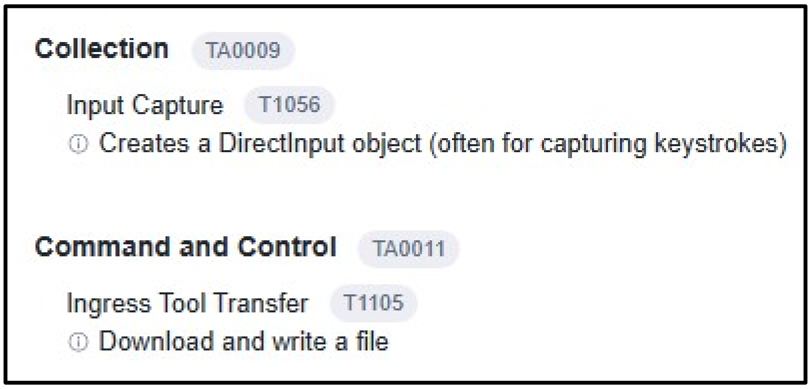
Privilege Escalation TA0004

Process Injection T1055

ⓘ Spawns processes

ⓘ Creates a process in suspended mode (likely to inject code)

Figure 48: Virus Total behavior for file Lab03-04.exe.



Collection TA0009

Input Capture T1056

ⓘ Creates a DirectInput object (often for capturing keystrokes)

Command and Control TA0011

Ingress Tool Transfer T1105

ⓘ Download and write a file

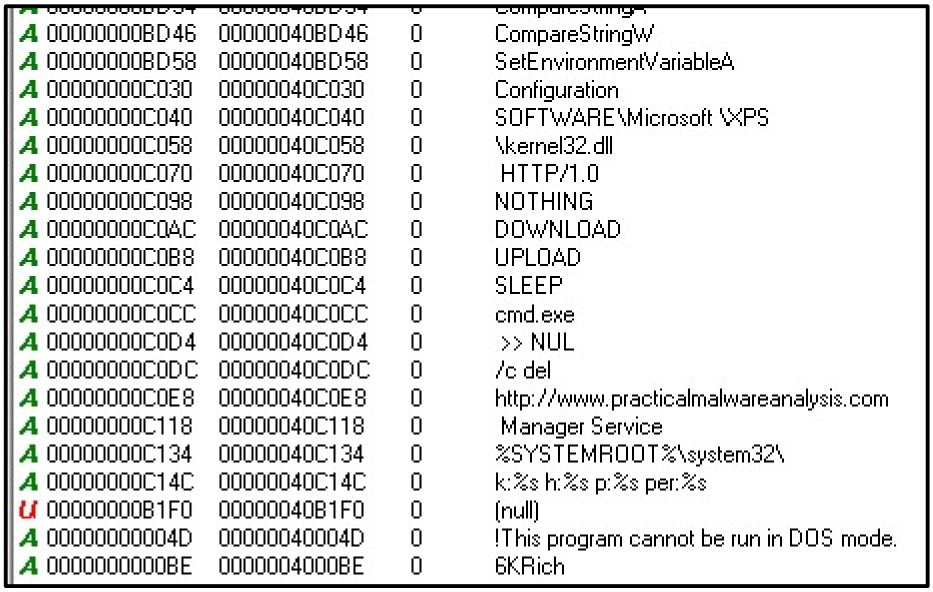
Figure 49: Virus Total input capture and C&C for file Lab03-04.exe.

LAB 3-4

LAB 3-4 Question 1

What happens when you run this file?

While conducting a static analysis, some strings contained within the file suggested that this malware potentially has the ability to download and upload files with a potential domain of www.practicalmalwareanalysis.com. Combined with the string of "HTTP/1.0", it is likely that this malware is a backdoor (Figure 50).



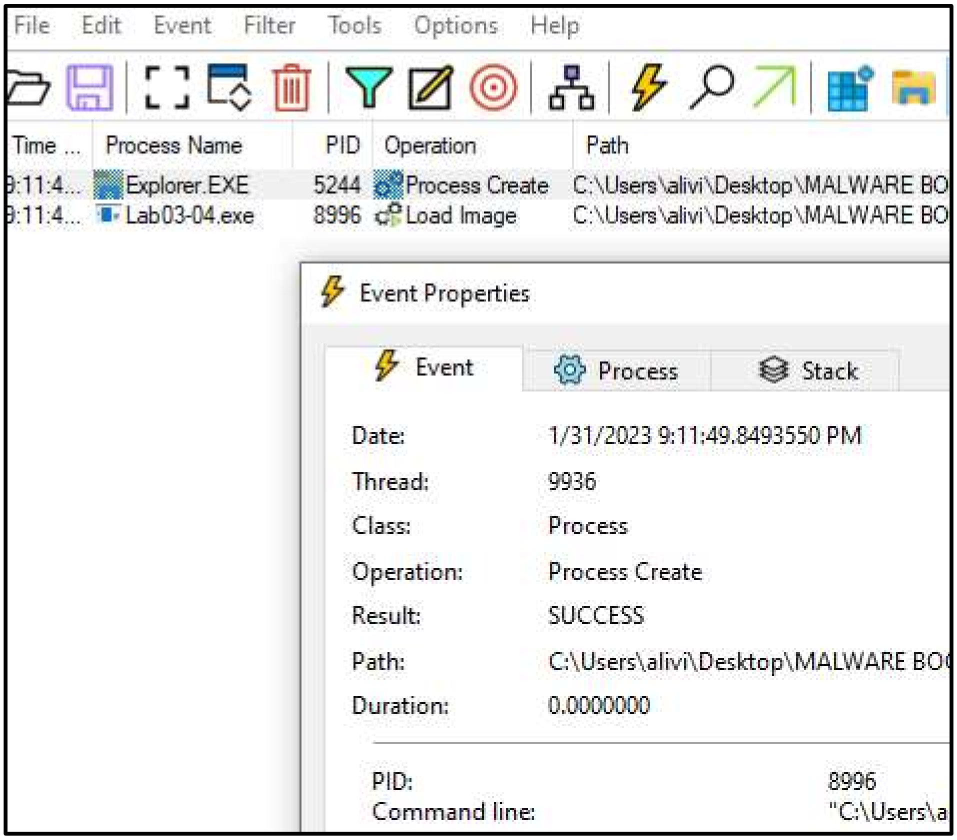
```
A 00000000BD46   00000040BD46   0    CompareStringW
A 00000000BD58   00000040BD58   0    SetEnvironmentVariableA
A 00000000C030   00000040C030   0    Configuration
A 00000000C040   00000040C040   0    SOFTWARE\Microsoft \XPS
A 00000000C058   00000040C058   0    \kernel32.dll
A 00000000C070   00000040C070   0     HTTP/1.0
A 00000000C098   00000040C098   0    NOTHING
A 00000000C0AC   00000040C0AC   0    DOWNLOAD
A 00000000C0B8   00000040C0B8   0    UPLOAD
A 00000000C0C4   00000040C0C4   0    SLEEP
A 00000000C0CC   00000040C0CC   0    cmd.exe
A 00000000C0D4   00000040C0D4   0     >> NUL
A 00000000C0DC   00000040C0DC   0    /c del
A 00000000C0E8   00000040C0E8   0    http://www.practicalmalwareanalysis.com
A 00000000C118   00000040C118   0     Manager Service
A 00000000C134   00000040C134   0    %SYSTEMROOT%\system32\
A 00000000C14C   00000040C14C   0    k:%s h:%s p:%s per:%s
U 00000000B1F0   00000040B1F0   0    (null)
A 00000000004D   00000040004D   0    !This program cannot be run in DOS mode.
A 0000000000BE   0000004000BE   0    6KRich
```

Figure 50: BinText strings for Lab03-04.exe.

To dynamically analyze the malware when it is run, instances of both procmon and Process Explorer were set up in order to capture any output that would provide clues that would lead to the purpose of this malware. Additionally, because of the potential for this malware to act as a backdoor, ApdateDNS was set up in order to capture any outbound traffic.

When the malware was run, Lab03-04.exe deleted itself from the directory it was in and did not end up in the Recycle Bin. In procmon, a process was created by Lab03-04.exe with a PID of

8996 (Figure 51). Filtering procmon by that PID, a cmd.exe process was created that shows how the file deleted itself (Figure 52).



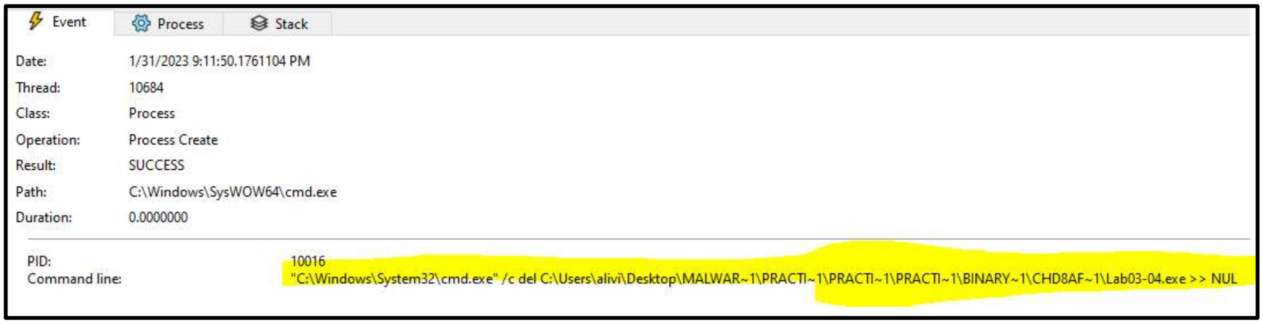
Time ...	Process Name	PID	Operation	Path
9:11:4...	Explorer.EXE	5244	Process Create	C:\Users\alivi\Desktop\MALWARE BO
9:11:4...	Lab03-04.exe	8996	Load Image	C:\Users\alivi\Desktop\MALWARE BO

Event Properties

```
Date:          1/31/2023 9:11:49.8493550 PM
Thread:        9936
Class:         Process
Operation:     Process Create
Result:        SUCCESS
Path:          C:\Users\alivi\Desktop\MALWARE BO
Duration:      0.0000000

PID:                               8996
Command line:                      "C:\Users\a
```

Figure 51: Created PID of 8996 by Lab03-04.exe.



```
Date:          1/31/2023 9:11:50.1761104 PM
Thread:        10684
Class:         Process
Operation:     Process Create
Result:        SUCCESS
Path:          C:\Windows\SysWOW64\cmd.exe
Duration:      0.0000000

PID:                  10016
Command line:         "C:\Windows\System32\cmd.exe" /c del C:\Users\alivi\Desktop\MALWAR~1\PRACTI~1\PRACTI~1\PRACTI~1\BINARY~1\CHD8AF~1\Lab03-04.exe >> NUL
```

Figure 52: How Lab03-04.exe deleted itself.

LAB 3-4 Question 2

What is causing the roadblock in dynamic analysis?

When a search of PID 8996 is conducted in Process Explorer, no results come back which indicate that the malware is not actively running on the machine (Figure 53). Furthermore, there aren't any network-based indicators that this malware is attempting to conduct. The fact that the malware deleted itself presents a roadblock that the VM needs to be reset to the previous snapshot if further dynamic or static analyses are conducted. However, the malware does not delete duplicates of itself and only deletes the .exe file that was run by the user. Without more advanced knowledge on how to analyze malware, especially with increasing complexity, the roadblocks are not the tools nor the malware. The roadblock is the skill of the analyst.

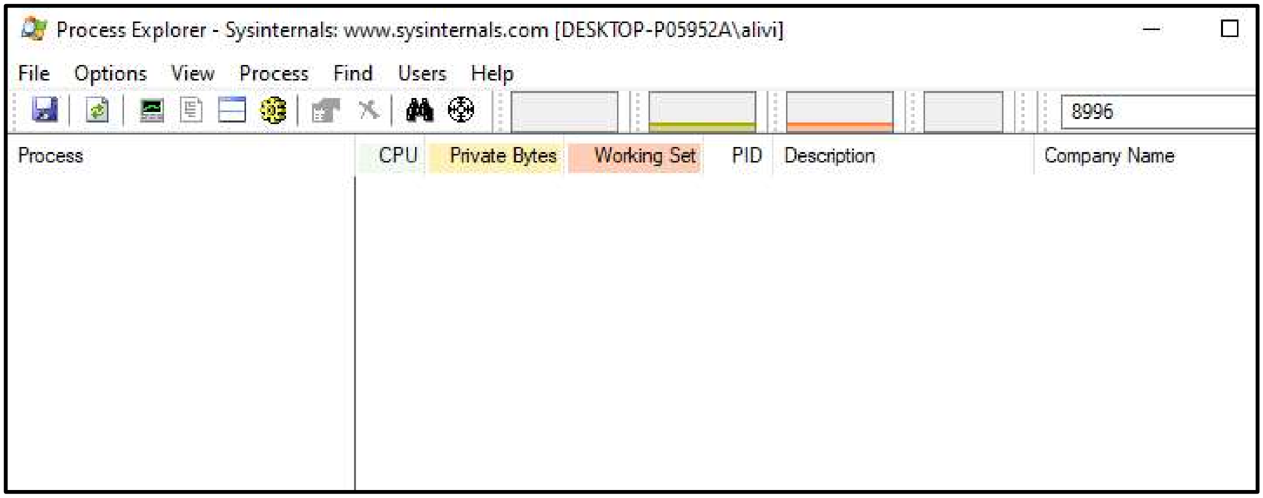

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-P05952A\alivi]
File Options View Process Find Users Help
8996
Process
CPU
Private Bytes
Working Set
PID
Description
Company Name

Figure 53: Lab03-04.exe is not actively running.

LAB 3-4 Question 3

Are there other ways to run this program?

Without further knowledge of how to run a self-deleting piece of malware in order to view its effects on a sandbox environment, I cannot think of anything. I am excited to learn more on how to overcome this type of challenge and perform an even more thorough analysis. The book teases more advanced dynamic analysis techniques in the future and infers solutions to the self-deleting-malware problem.