

Assignment 1

Adam Livingston

University Of Arizona

CYBV 454 MALWARE THREATS & ANALYSIS

Professor Galde

24 Jan 2023

LAB 1-1

- LAB01-01.exe : bb7425b82141a1c0f7d60e5106676bb1
- LAB01-01.dll : 290934c61de9176ad682ffdd65f0a669

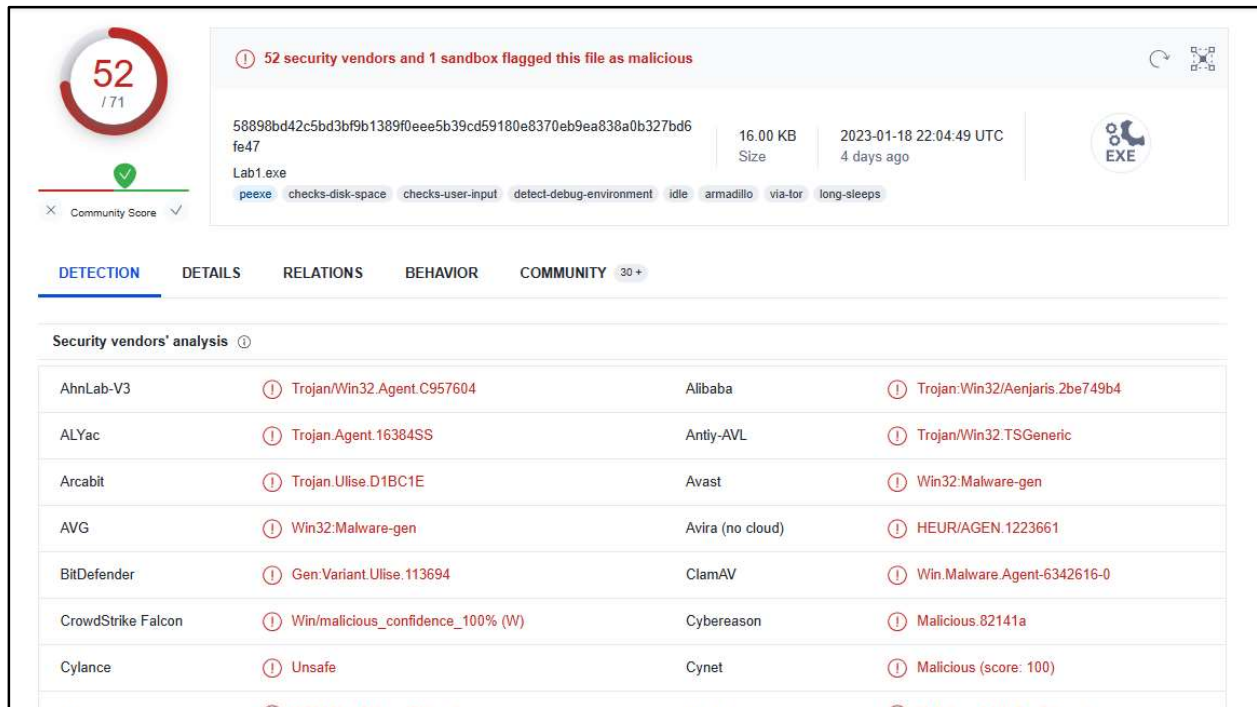


Figure 1: Virus Total Findings for file Lab01-01.exe.

Virus Total found 52 matching signatures for Trojan malware for the file Lab01-01.exe (Figure 1). It has a compilation timestamp of 19 Dec 2010 at 16:16:19 UTC (Figure 2). It appears to import Kernel32.dll, suggesting it manipulates memory, files, and other hardware (Figure 3). 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 4). It has other indicators of persistence, privilege escalation, and defense evasion (Figures 4 and 5). 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 and uses HTTPS (Figure 6).

Header	
Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2010-12-19 16:16:19 UTC
Entry Point	6176
Contained Sections	3
Sections	

Figure 2: Virus Total Compilation Timestamp for file Lab01-01.exe.

Sections					
Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	2416	4096	4.45	7e39ebe7cdeda4c636d513a0fe140ff4
.rdata	8192	690	4096	1.13	2de0f3a50219cb3d0dc891c4fbf6f02a
.data	12288	252	4096	0.44	f5e2ba1465f131f57b0629e96bbe107e
Imports					
+ KERNEL32.dll					
+ MSVCRT.dll					

Figure 3: Virus Total Imports for file Lab01-01.exe.

Execution TA0002	
Scheduled Task/Job T1053	① Creates COM task schedule object (often to register a task for autostart)
Command and Scripting Interpreter T1059	⚠ Very long command line found ① Very long cmdline option found, this is very uncommon (may be encrypted or packed) ① Executes the "sed" command used to modify input streams (typically from files or pipes)
Scripting T1064	① Executes commands using a shell command-line interpreter
Persistence TA0003	
Scheduled Task/Job T1053	① Creates COM task schedule object (often to register a task for autostart)
Systemd Service T1543.002	① Executes the "systemctl" command used for controlling the systemd system and service manager
Windows Service T1543.003	① Modifies existing windows services ① Creates or modifies windows services

Figure 4: Virus Total Behavior1 for file Lab01-01.exe.



Figure 5: Virus Total Behavior2 for file Lab01-01.exe.

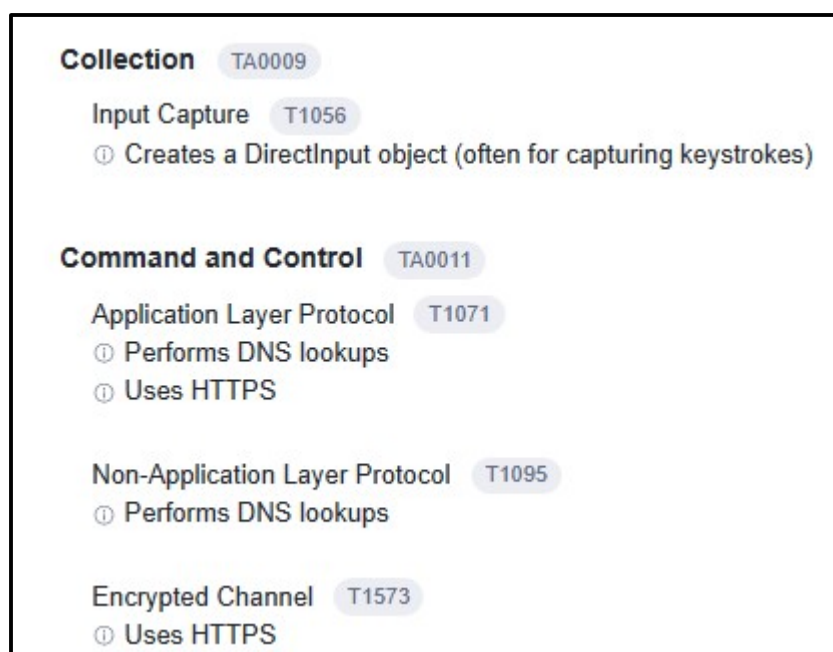


Figure 6: Virus Total Input Capture and C&C for file Lab01-01.exe.

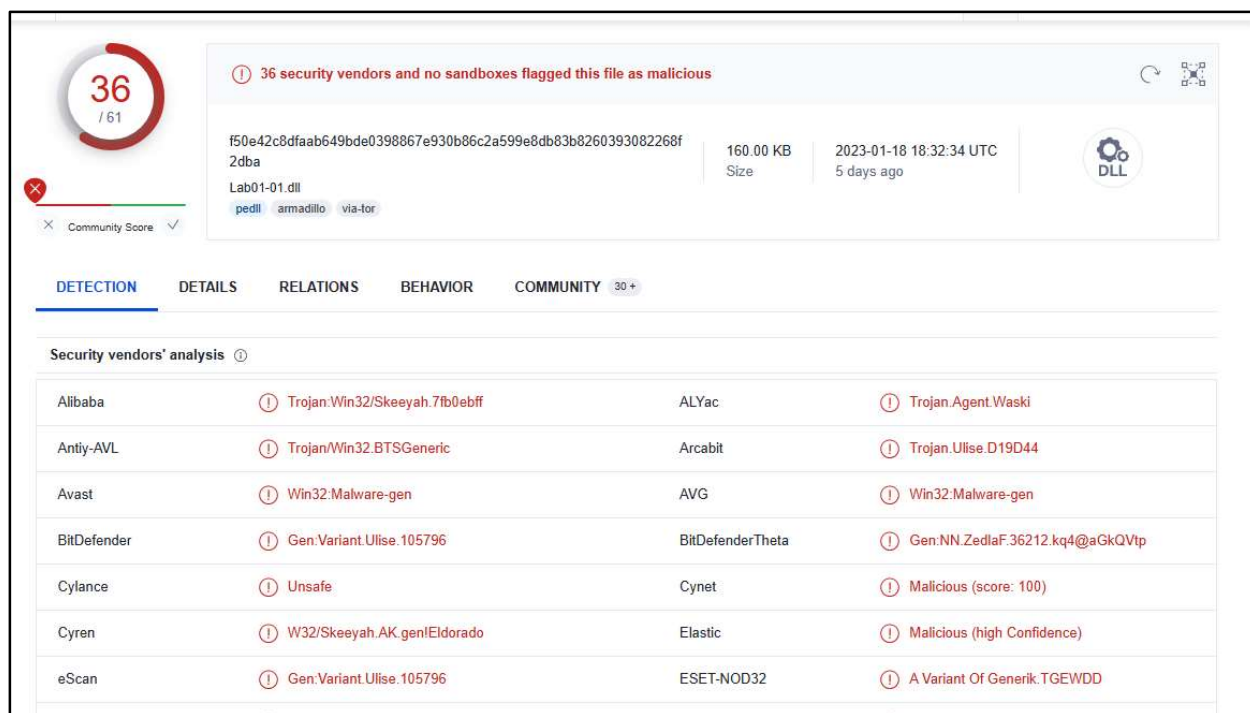


Figure 7: Virus Total Findings for file Lab01-01.dll.

Virus Total found 36 matching signatures for Trojan malware for the file Lab01-01.dll (Figure 7). It has a compilation timestamp of 19 Dec 2010 at 16:16:38 UTC (Figure 8). It appears to import Kernel32.dll, suggesting it manipulates memory, files, and other hardware (Figure 9). There are no behavioral indicators on Virus Total for this dll, but has a similar name to the .exe. Most likely, this dll is a companion piece that allows the .exe to run.

Header	
Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2010-12-19 16:16:38 UTC
Entry Point	4858
Contained Sections	4

Figure 8: Virus Total Compilation Timestamp for file Lab01-01.dll.

.data	155648	108
.reloc	159744	516
Imports		
+ KERNEL32.dll		
+ MSVCRT.dll		
+ WS2_32.dll		

Figure 9: Virus Total Imports for file Lab 01-01.dll.

LAB 1-1

LAB 1-1 Question 1

Upload the files to <http://www.VirusTotal.com/> and view the reports. Does the file match any existing antivirus signatures?

Yes, Figure 1 shows Lab01-01.exe matching 52 existing antivirus signatures and Lab01-01.dll matching 36 existing antivirus signatures.

LAB 1-1 Question 2

When were these files compiled?

Lab01-01.exe has a compilation timestamp of 19 Dec 2010 at 16:16:19 UTC (Figure 2). Lab01-01.dll has a compilation timestamp of 19 Dec 2010 at 16:16:38 UTC (Figure 8). Both files were compiled within 19 seconds of each other, suggesting they most likely have a codependent relationship. The executable most likely relies on the dll to run.

LAB 1-1 Question 3

Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?

Virus Total noted that Lab01-01.exe found a very long command line which indicates that the file may be encrypted or packed (Figure 4). PEiD also shows an indication of packing by way of “Microsoft Visual C++ 6.0” (Figure 10). Similarly, PEiD shows packing for Lab01-01.dll using “Microsoft Visual C++ 6.0 DLL” (Figure 11). This leads me to believe that both files were written in the C++ programming language, but **not** packed. Using PEBview, the program does not have obfuscate its intentions of what it does. There is a warning that states,

“THIS_WILL_DESTROY_YOUR_MACHINE” (Figure 12). A string analysis using BinText yielded no useful results other than the same warning found in Figure 12.

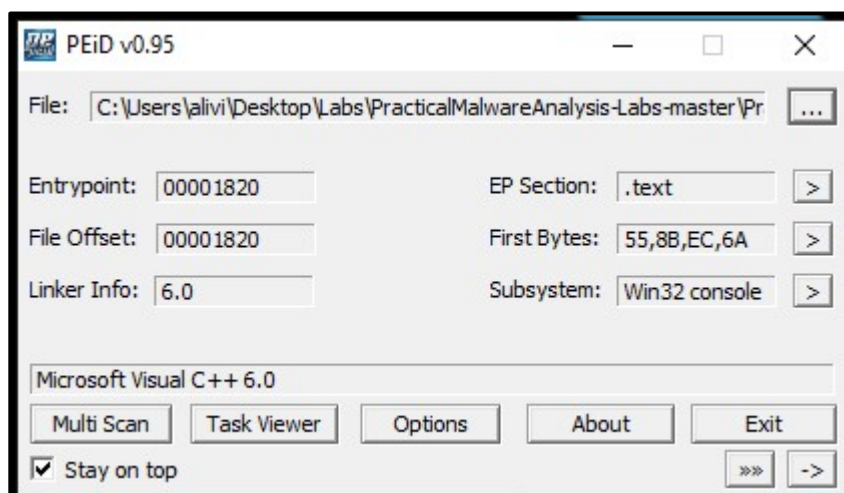


Figure 10: PEiD shows packing for file Lab 01-01.exe.

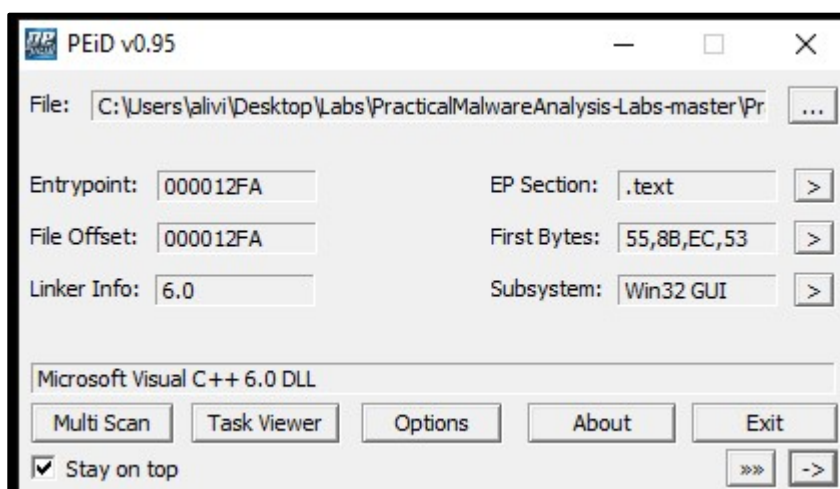


Figure 11: PEiD shows packing for file Lab 01-01.dll.

```
6D 33 32 5C  indows\System32\  
00 00 00 00  Kernel32.dll....  
5F 57 49 4C  WARNING_THIS_WIL  
55 52 5F 4D  L_DESTROY_YOUR_M  
00 00 00 00  ACHINE.....  
00 00 00 00  .....  
00 00 00 00  .....  
00 00 00 00  .....
```

Figure 12: PView string found for file Lab 01-01.exe.

LAB 1-1 Question 4

Do any imports hint at what this malware does? If so, which imports are they?

According to Virus Total, Lab01-01.exe appears to import Kernel32.dll, suggesting it manipulates memory, files, and other hardware (Figure 3). This was verified using the program, Dependencies. In addition to kernel32, it shows imports ntdll.dll which will give the malware access to the kernel and potentially use it for manipulating processes and hiding. Advapi32.dll was also found which allows the program to manipulate the service manager and registry (Figure 13). There was also a user32.dll import that can be used to control user interface components (Figure 14).

Additionally, Dependencies found the kernel32.dll import for Lab01-01.dll as well as Ws2_32.dll (Figure 15). The Ws2_32.dll indicates that the malware will perform some network-related tasks which was indicated by Virus Total, but for the .exe. This solidifies my suspicion that the malicious .dll is a companion piece to the .exe.

Lab01-01.exe has commands that indicate that it finds and copies files (Figure 16) whereas Lab01-01.dll shows commands to create a process then sleeps (Figure 17).

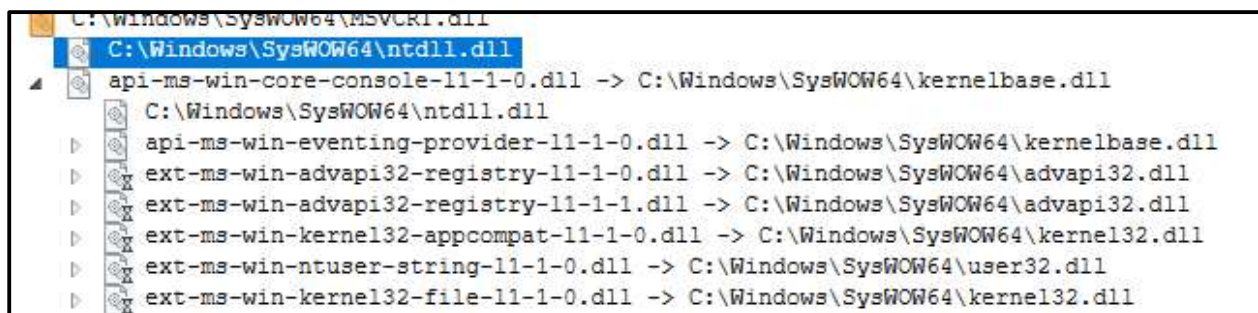


Figure 13: kernel32.dll, ntdll.dll, and advapi32.dll import found for file Lab 01-01.exe.

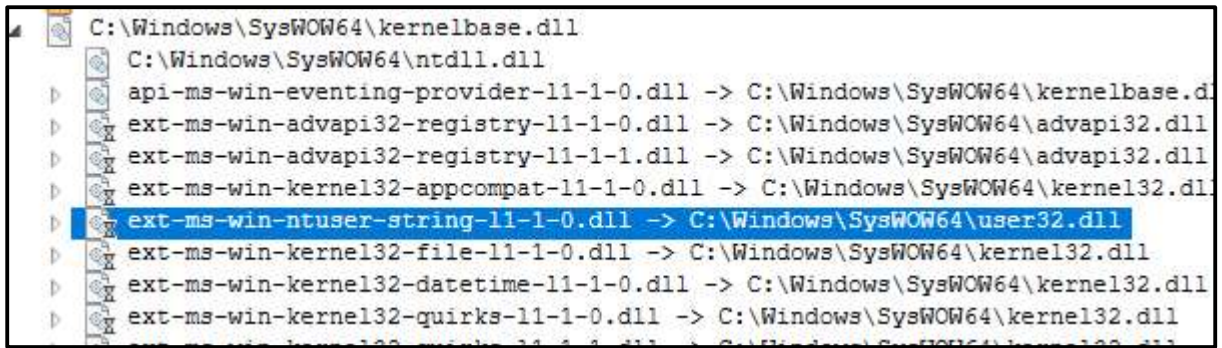


Figure 14: user32.dll import found for file Lab 01-01.exe.

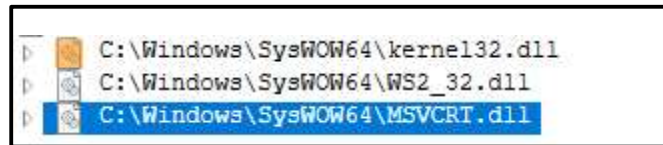


Figure 15: kernel32.dll and Ws2_32.dll imports found for file Lab 01-01.dll.

A 000000002146	000000402146	0	IsBadReadPtr
A 000000002156	000000402156	0	MapViewOfFile
A 000000002166	000000402166	0	CreateFileMappingA
A 00000000217C	00000040217C	0	CreateFileA
A 00000000218A	00000040218A	0	FindClose
A 000000002196	000000402196	0	FindNextFileA
A 0000000021A6	0000004021A6	0	FindFirstFileA
A 0000000021B8	0000004021B8	0	CopyFileA
A 0000000021C2	0000004021C2	0	KERNEL32.dll
A 0000000021D2	0000004021D2	0	malloc
A 0000000021E2	0000004021E2	0	MSVCRT.dll
A 0000000021F0	0000004021F0	0	exit

Figure 16: Lab 01-01.exe finding files and copying them.

A 000000002104	000010002104	0	CloseHandle
A 000000002118	000010002118	0	Sleep
A 000000002120	000010002120	0	CreateProcessA
A 000000002132	000010002132	0	CreateMutexA
A 000000002142	000010002142	0	OpenMutexA
A 00000000214E	00001000214E	0	KERNEL32.dll
A 00000000215C	00001000215C	0	WS2_32.dll
A 00000000216A	00001000216A	0	strcmp
A 000000002172	000010002172	0	MSVCRT.dll
A 000000002188	000010002188	0	_initterm
A 000000002194	000010002194	0	malloc
A 00000000219E	00001000219E	0	_adjust_fdiv
A 0000000026018	000010026018	0	sleep
A 0000000026020	000010026020	0	hello

Figure 17: Lab 01-01.dll creating a process then sleeping.

LAB 1-1 Question 5

Are there any other files or host-based indicators that you could look for on infected systems?

Yes. Indicators of compromise or infection from malware can be either overt or covert. A more covert way of hiding malware would be in memory (through the use of a rootkit or other fileless virus) or through alteration of the registry. A more overt way would be the use of ransomware, locking the user's machine unless a ransom is paid and explicitly demanding the user to do so. Other overt indicators would be alteration of the GUI and rendering the machine useless. Files could also be manipulated, created, deleted, or otherwise rendered useless. Some other indicators could be a noticeable decrease in performance which can be measured based on the CPU and memory usage through task manager, process monitor, or other performance-measuring tools. A user can also determine if is a malware infection due to random movement of the mouse cursor, unwanted ad popups, or frequent, spontaneous command-prompt popups (for Windows OS).

Throughout the static analysis both of these malicious files, they did not show any promise to have file-based indicators of compromise/infection. Running the malware on both Windows 10 and Windows XP machines did not produce the kerne132.dll file that the textbook indicates.

After the .exe was run, the Process Monitor program noticed an immediate access by the program to Conhost.exe (the command prompt) and accessed the .dll imports that were identified in the static analysis (Figure 18). However, no noticeable changes were made to the machine.

Time of Day	Process Name	PID	Operation	Path	Result
4:17:52.0765247	Lab01-01.exe	5568	Thread Create		SUCCESS
4:17:52.0790156	svchost.exe	9112	Thread Create		SUCCESS
4:17:52.0851923	Lab01-01.exe	5568	Load Image	C:\Users\alivi\Desktop\Labs\Practical...	SUCCESS
4:17:52.0860659	Lab01-01.exe	5568	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS
4:17:52.0866825	Lab01-01.exe	5568	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS
4:17:52.0878862	Lab01-01.exe	5568	Load Image	C:\Windows\System32\wow64.dll	SUCCESS
4:17:52.0879540	Lab01-01.exe	5568	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS
4:17:52.0888216	Lab01-01.exe	5568	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS
4:17:52.0893467	Lab01-01.exe	5568	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS
4:17:52.0894513	Lab01-01.exe	5568	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS
4:17:52.0909790	Lab01-01.exe	5568	Process Create	C:\Windows\System32\Conhost.exe	SUCCESS
4:17:52.0909841	Conhost.exe	3160	Process Start		SUCCESS
4:17:52.0909892	Conhost.exe	3160	Thread Create		SUCCESS
4:17:52.0914256	Conhost.exe	3160	Load Image	C:\Windows\System32\conhost.exe	SUCCESS
4:17:52.0914449	Conhost.exe	3160	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS
4:17:52.0920359	Conhost.exe	3160	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS
4:17:52.0935235	Conhost.exe	3160	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS

Figure 18: Lab 01-01.exe executed with subsequent Conhost.exe calls.

LAB 1-1 Question 6

What network-based indicators could be used to find this malware on infected machines?

I did not find any network-based indicators for this malware when I ran it using FakeNetNG, contrary to what Virus Total stated with its reported attempts to call out through port 443 or port 53. This was confirmed using Process Monitor and Netcat listening on those ports and did not find any network activity around the time that Lab01-01.exe was run at 4:17:52 (Figure 19). However, a BinText analysis of Lab01-01.dll refers to an IP address of 127.26.152.13 which could be used as a network-based indicator of malware execution (Figure 20).

Time of Day	Process Name	PID	Operation	Path	Result	Detail
4:19:20.8800936	msedge.exe	1732	UDP Send	DESKTOP-P05952A.localdomain:50529...	SUCCESS	Length: 36, sequ...
4:19:20.8815914	fakenet.exe	7448	UDP Receive	DESKTOP-P05952A.localdomain:domai...	SUCCESS	Length: 36, sequ...
4:19:20.8817150	msedge.exe	1732	UDP Send	DESKTOP-P05952A.localdomain:50529...	SUCCESS	Length: 36, sequ...
4:19:20.8822962	fakenet.exe	7448	UDP Receive			
4:19:20.8862666	svchost.exe	2244	UDP Send			
4:19:20.8879719	fakenet.exe	7448	UDP Receive			
4:19:20.8894019	msedge.exe	1732	UDP Receive			
4:19:20.8910845	msedge.exe	1732	UDP Receive			
4:19:20.8915356	fakenet.exe	7448	UDP Send			
4:19:20.8922578	svchost.exe	2244	UDP Receive			
4:19:20.8930699	msedge.exe	1732	UDP Send			
4:19:20.8934062	msedge.exe	1732	UDP Send			


```

Command Prompt - ncat -l -p 53
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\alivi>ncat
Ncat: You must specify a host to connect to. QUITTING.

C:\Users\alivi>ncat -l -p 443
C:\Users\alivi>ncat -l -p 54
C:\Users\alivi>ncat -l -p 53
  
```

Figure 19: Lab 01-01.exe network activity not aligned with time it ran.

A	000000002188	000010002188	0	_initterm
A	000000002194	000010002194	0	malloc
A	00000000219E	00001000219E	0	_adjust_fdiv
A	0000000026018	000010026018	0	sleep
A	0000000026020	000010026020	0	hello
A	0000000026028	000010026028	0	127.26.152.13
A	0000000026038	000010026038	0	SADFHUHF
A	0000000027008	000010027008	0	/0l0{0h0p0
A	0000000027029	000010027029	0	141G1[1l1
A	0000000027039	000010027039	0	1Y2a2g2r2
A	000000002705B	00001002705B	0	3!3}3
A	000000000004D	00001000004D	0	!This program cannot be run in DOS mo
A	00000000001D8	0000100001D8	0	.text

Figure 20: Lab 01-01.dll suspicious IP address.

LAB 1-1 Question 7

What would you guess is the purpose of these files?

Because of the suspicious IP address in the .dll file and that it creates a process followed by sleeping, I suspect that the .exe runs the .dll to create a backdoor at IP address 127.26.152.13 which would allow it to be routed back to the malicious actor. Since the .exe also searches for and copies files, I also suspect that this backdoor is used for data exfiltration/theft.

LAB 1-2

- LAB01-02.exe : 8363436878404da0ae3e46991e355b83

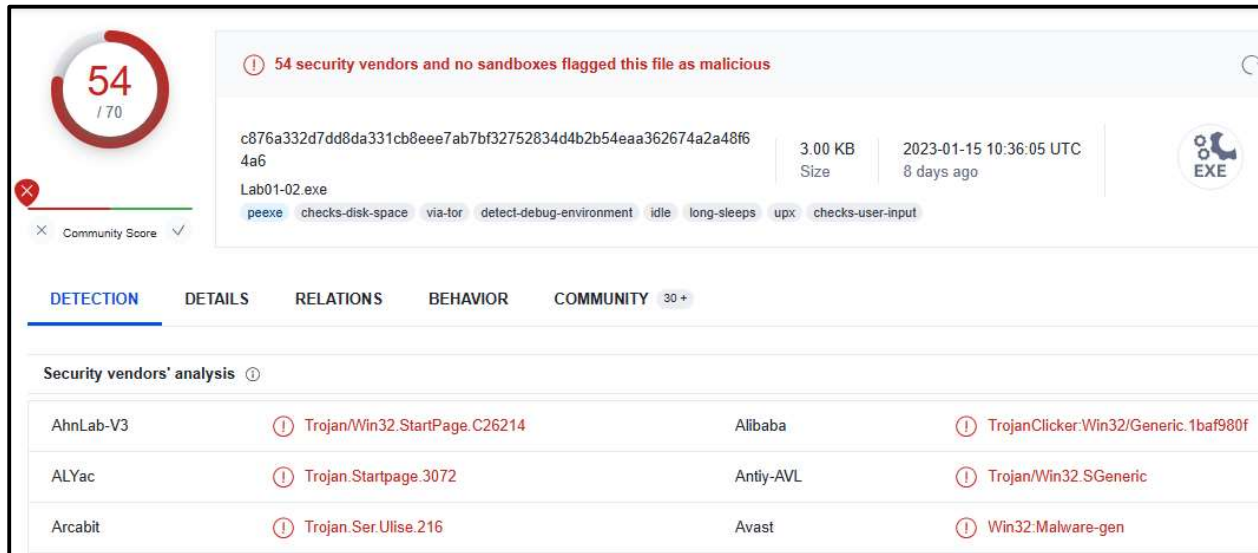


Figure 21: Virus Total Findings for file Lab01-02.exe.

Virus Total found 54 matching signatures for Trojan malware for the file Lab01-02.exe (Figure 21). It has a compilation timestamp of 19 Jan 2011 at 16:10:41 UTC (Figure 22). 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. (Figure 23). 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. It has other indicators of persistence, privilege escalation, and defense evasion (Figures 24 and 25). 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 and uses HTTPS (Figure 26).

Header	
Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2011-01-19 16:10:41 UTC
Entry Point	21520
Contained Sections	3

Figure 22: Virus Total Timestamp for file Lab01-02.exe.

Imports	
+	ADVAPI32.dll
+	KERNEL32.DLL
+	MSVCRT.dll
+	WININET.dll

Figure 23: Virus Total Imports for file Lab01-02.exe.

Execution TA0002	
Command and Scripting Interpreter T1059	
① Very long cmdline option found, this is very uncommon (may be encrypted or packed)	
Service Execution T1569.002	
① Uses sc.exe to modify the status of services	
Persistence TA0003	
Windows Service T1543.003	
① Modifies existing windows services	
① Uses sc.exe to modify the status of services	
① Creates or modifies windows services	
LSASS Driver T1547.008	
① Spawns drivers	
DLL Side-Loading T1574.002	
① Tries to load missing DLLs	
Privilege Escalation TA0004	
Process Injection T1055	
① Spawns processes	
① Creates a process in suspended mode (likely to inject code)	
Windows Service T1543.003	

Figure 24: Virus Total Behavior for file Lab01-02.exe.

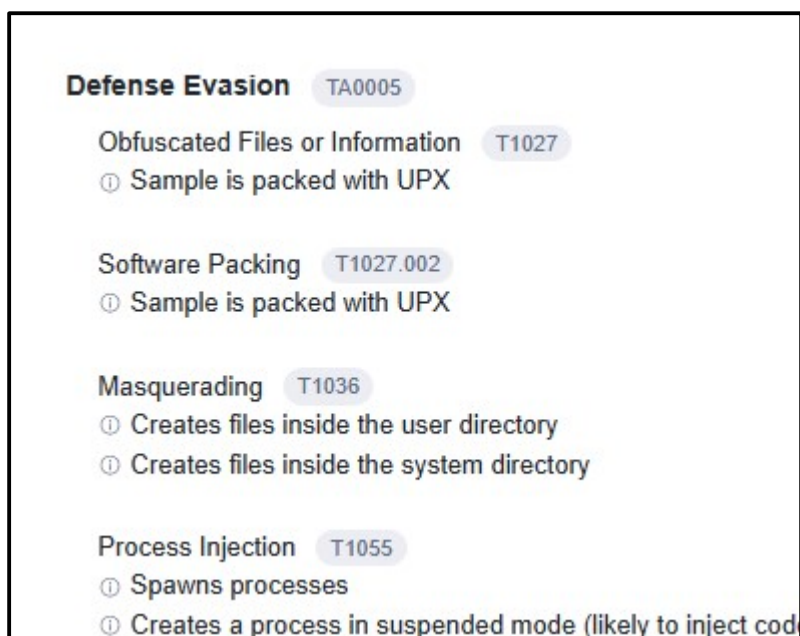


Figure 25: Virus Total Behavior for file Lab01-02.exe.

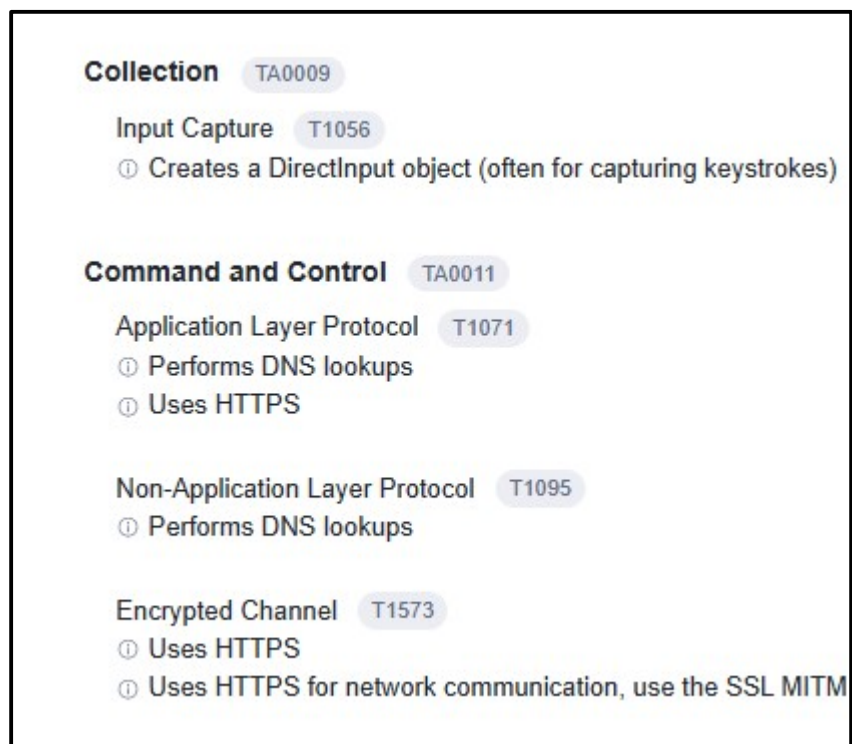


Figure 26: Virus Total C&C for file Lab01-02.exe.

LAB 1-2

LAB 1-2 Question 1

Upload the *Lab01-02.exe* file to <http://www.VirusTotal.com/>. Does it match any existing antivirus definitions?

Yes, Figure 21 shows Lab01-02.exe matching 54 existing antivirus signatures.

LAB 1-2 Question 2

Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

Virus Total noted that Lab01-02.exe found a very long command line which indicates that the file may be encrypted or packed (Figure 24). PEiD also shows an indication of packing by way of “UPX -> www.upx.sourceforge.net *” (Figure 27). The file was successfully unpacked which showed the size increased from 3kb to 16kb (Figure 28)

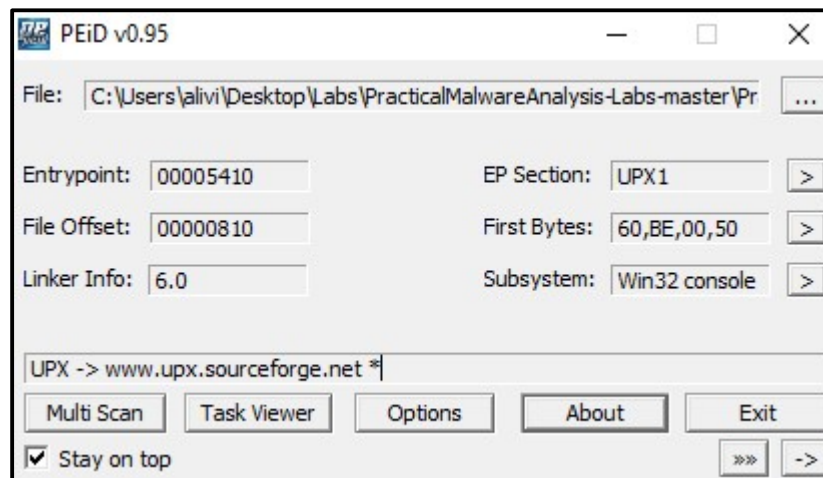


Figure 27: PEiD shows packing for file Lab01-02.exe.

COPYING	1/24/2023 1:58 PM	File	18 KB
Lab01-02.exe	1/19/2011 11:10 AM	Application	3 KB
Lab1-2	1/19/2011 11:10 AM	File	16 KB
LICENSE	1/24/2023 1:58 PM	File	6 KB
NEWS	1/24/2023 1:58 PM	File	24 KB

Figure 28: Unpacked difference in size for Lab01-02.exe.

A thorough static analysis of the file using Dependencies, PEview, and PEiD showed no indication of the file's intention (aside from some .dll imports). This is an indicator of obfuscation.

LAB 1-2 Question 3

Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?

The imports of Kernel32.dll and advapi32.dll suggests the file manipulates memory, files, and other hardware. The additional import of wininet.dll suggests that it has the ability to configure ports and protocols. (Figure 23). The Dependencies tool showed the same .dll imports for the file (Figure 29). Although the .dll imports let us know what the program has the capability to do, it doesn't tell us exactly what it does.

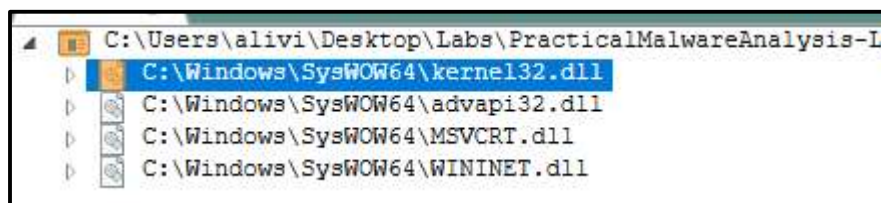


Figure 29: .dll imports with Dependencies program for Lab01-02.exe.

LAB 1-2 Question 4

What host- or network-based indicators could be used to identify this malware on infected machines?

The program was initially ran on app.any.run to see what it did to a Windows 7 machine. The website did not detect any file manipulation or network traffic and eventually cleared it with “no threats detected” (Figure 30).

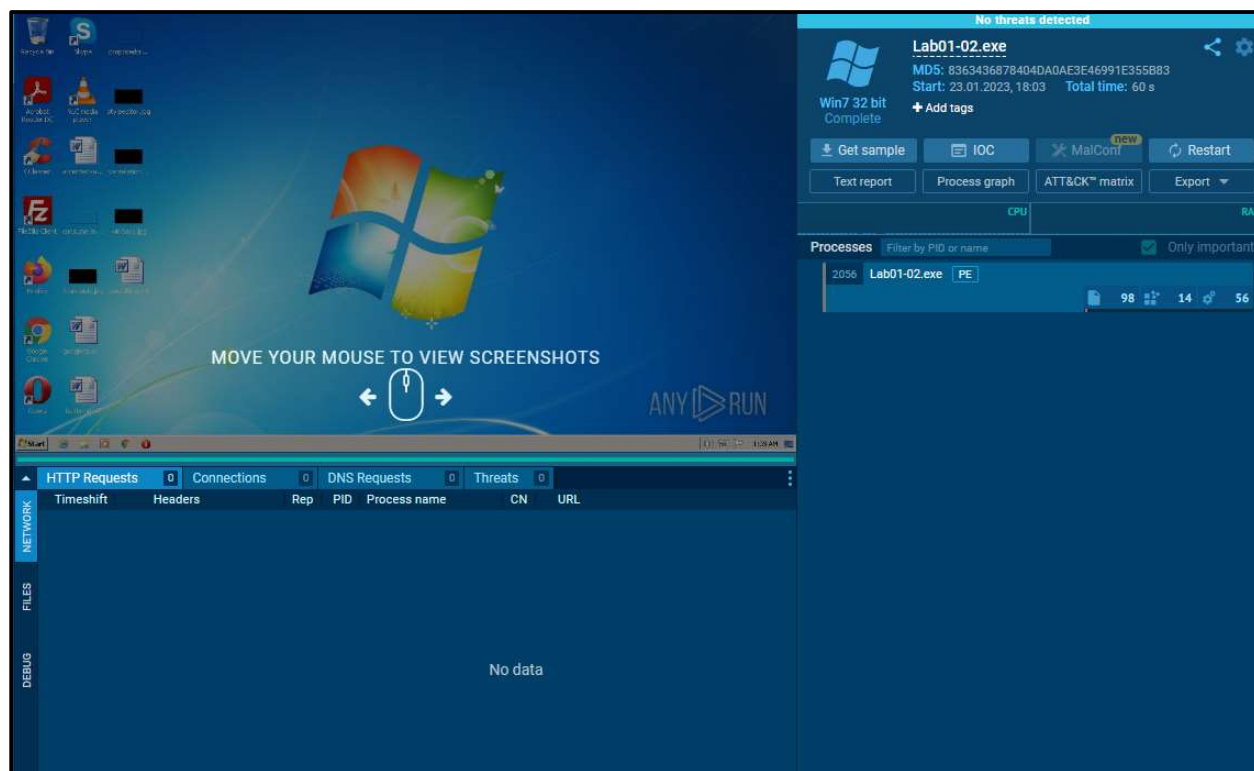


Figure 30: app.any.run report Lab01-02.exe.

Knowing that this file is malicious and yet did not yield malicious results with this initial analysis leads me to believe that it is possibly dependent on the Lab01-01.dll file in order to run. This is due to the Lab01-01.dll's import for Ws2_32.dll due to the networking capability and the fact that Lab01-01.dll was not included in this app.any.run sandbox.

However, when the malware was ran on the Windows XP VM, a command prompt popup was seen briefly (Figure 31). Additionally, Fakenet detected TCP connections over port 80 to getgreenshot.org (Figure 32). This is a tool to get screenshots on a Windows system and it was noticed that the tool, when it was attempted to be opened, displayed an error saying that it was

already running (Figure 33). Fakenet also detected a new connection to Microsoft-CryptoAPI which suggests a malicious actor is attempting to encrypt Windows-based applications or files to be inaccessible to the user (Figure 34).

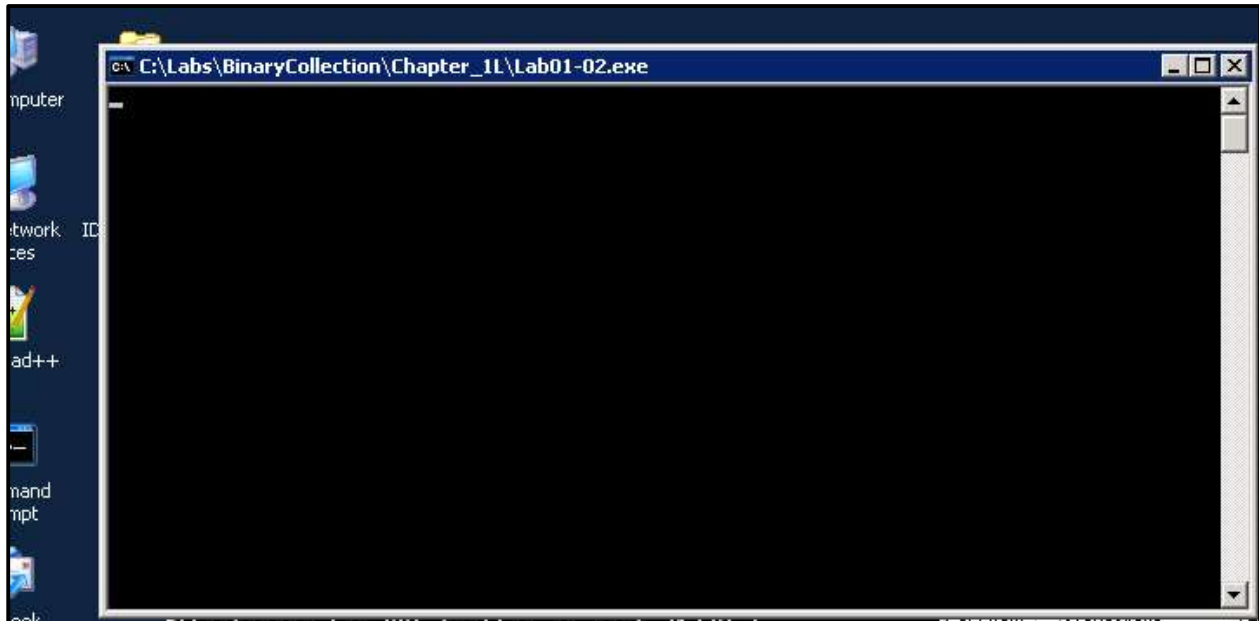


Figure 31: Command prompt popup after running Lab01-02.exe.

```
[Received new connection on port: 80.]
[New request on port 80.]
[Received unsupported HTTP request.]
HEAD /project-feed/ HTTP/1.1
Host: getgreenshot.org
Connection: Keep-Alive

[Received new connection on port: 80.]
[New request on port 80.]
GET /project-feed/ HTTP/1.1
Host: getgreenshot.org
Connection: Keep-Alive
```

Figure 32: Fakenet Report after running Lab01-02.exe.

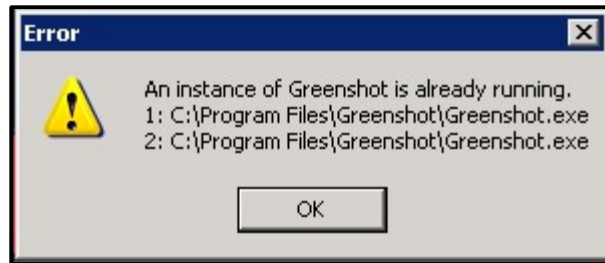


Figure 33: Error window after attempting to run Greenshot.exe.

```
[Received new connection on port: 80.]
[New request on port 80.]
GET /ctnca.crl HTTP/1.1
Accept: */*
User-Agent: Microsoft-CryptoAPI/5.131.2600.5512
Host: crl.certum.pl
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache

[Failed to open file C:\Class\Fakenet1.0c-OLD\Fakenet1.0b\default1 to respond to HTTP request.]

[Received new connection on port: 80.]
[New request on port 80.]
GET /cscasha2.crl HTTP/1.1
Accept: */*
User-Agent: Microsoft-CryptoAPI/5.131.2600.5512
Host: crl.certum.pl
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

Figure 34: Fakenet report for request for CryptoAPI.

Indicators that a machine might be infected with this malware are unauthorized network connections on port 80 to Microsoft-CryptoAPI as well as open connections to greenshot.org. Host-based indicators include the inability to use the program Greenshot as well as encrypted files that were not authorized by the user. The latter instance did not happen during testing, but the connection to Microsoft-CryptoAPI is extremely suspicious.

LAB 1-3

- LAB01-03.exe : 9c5c27494c28ed0b14853b346b113145

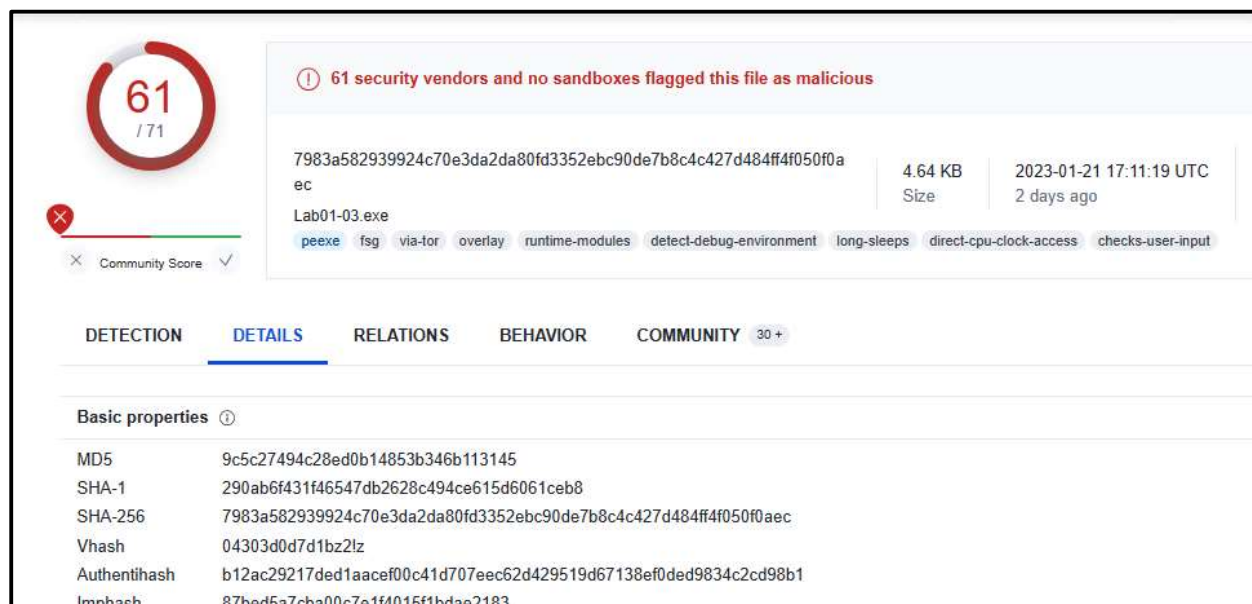


Figure 35: Virus Total Findings for file Lab01-03.exe.

Virus Total found 61 matching signatures for Trojan malware for the file Lab01-03.exe (Figure 35). Virus Total did not detect a compilation timestamp. It appears to only import Kernel32.dll suggesting it manipulates memory, files, and other hardware (Figure 36). 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. It has other indicators of persistence, privilege escalation, and defense evasion (Figures 37 and 38). 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, uses HTTPS, and HTTP (Figure 39).



Figure 36: Virus Total imports for file Lab01-03.exe.

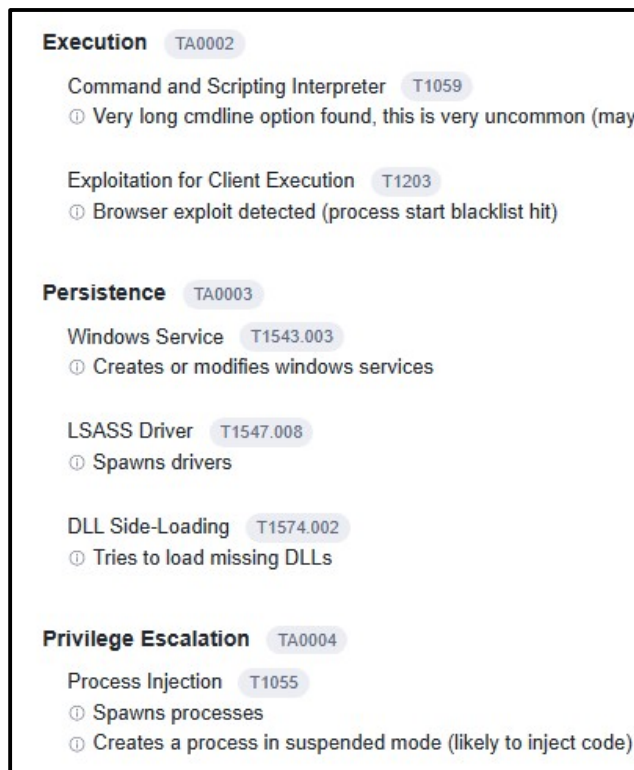


Figure 37: Virus Total behavior for file Lab01-03.exe.

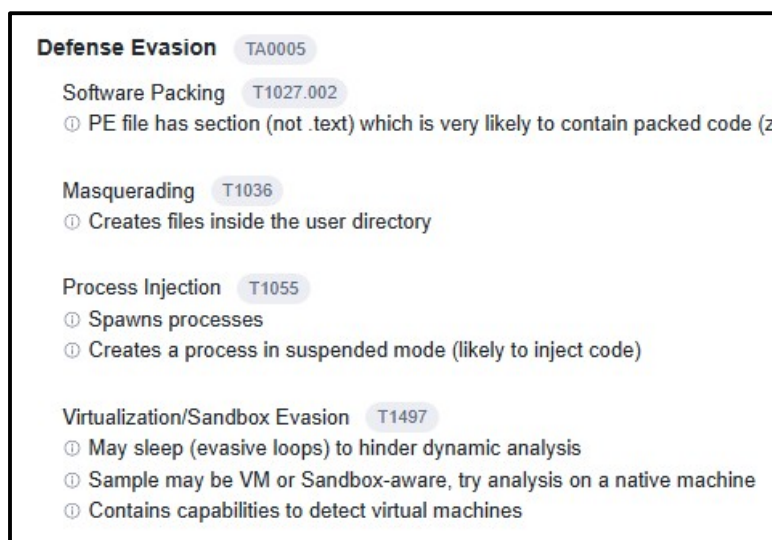


Figure 38: Virus Total behavior for file Lab01-03.exe.

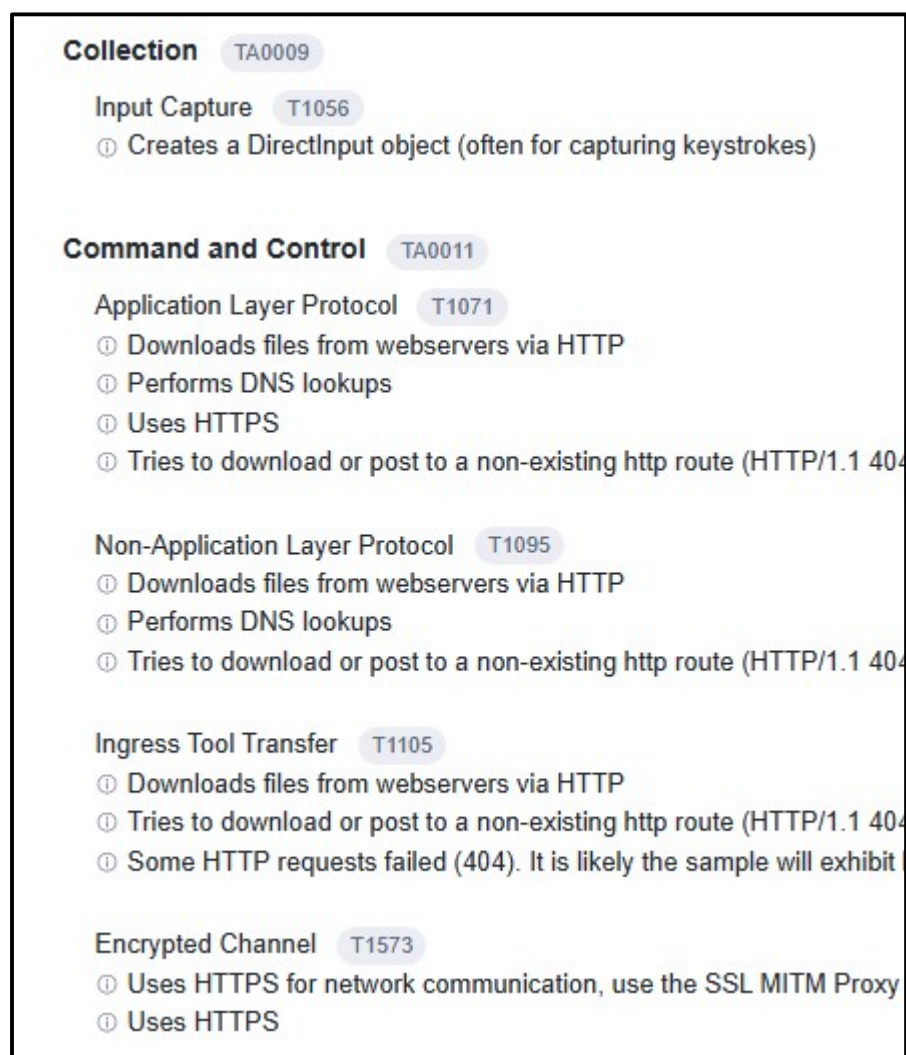


Figure 39: Virus Total C&C for file Lab01-03.exe

LAB 1-3

LAB 1-3 Question 1

Upload the files to <http://www.VirusTotal.com/> and view the reports. Does the file match any existing antivirus signatures?

Yes, Figure 35 shows Lab01-03.exe matching 61 existing antivirus signatures.

LAB 1-3 Question 2

Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

Virus Total noted that Lab01-02.exe found a very long command line which indicates that the file may be encrypted or packed (Figure 37). PEiD also shows an indication of packing by way of “FSG 1.0 -> dulek/xt” (Figure 40). Uniextract could not unpack the file. A static analysis with PEsview, BinText, and dependencies did not reveal any indications of the file’s intentions and therefore is obfuscated.

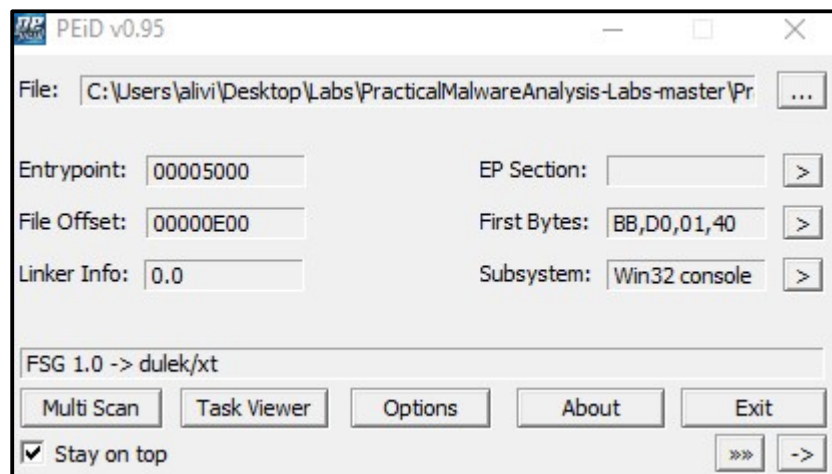


Figure 40: PEiD packing for file Lab01-03.exe

LAB 1-3 Question 3

Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?

According to the Dependencies program, the only import this malware imports is kernel32.dll, matching the Virus Total report, which suggests the file has the ability to manipulate memory, files, and other hardware (Figure 41).

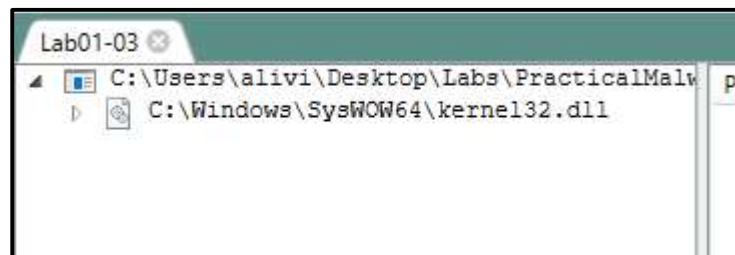


Figure 41: Dependencies finding kernel32.dll import for file Lab01-03.exe

LAB 1-3 Question 4

What host- or network-based indicators could be used to identify this malware on infected machines?

When the program was run on app.any.run, it showed the spontaneous running of internet explorer to five different http websites, suggesting this program makes callouts over port 80. Additionally, two of those webpage calls were to the domains containing the online certificate status protocol (OCSP) based in the UK. (Figure 42). It also calls out to two websites that begin with ctldl.windowsupdate.com that appear to download some files. This domain was confirmed by Microsoft to be blocked due to a malicious IP address (Figure 43). It can be interpreted from these two facts that the possibility of the digital certificate associated with the machine that executes this software might be stolen and/or additional malicious software will be downloaded from an identified malicious domain.

CYBV 454 Assignment 1 LIVINGSTON

An app.any.run identified a malicious IP address of 67.27.158.126 to which the host machine running the malware sent a GET TCP segment over HTTP to download “Disallowedcertstl.cab” (Figure 44). The download contains the Certificate Trust List (CTL) of Disallowed Certificates. According to Microsoft, this file is used in conjunction with certificate management on network computers, leading me to assume that computers connected to the machine running the malware may have their digital certificates revoked and are unable to be trusted entities on the internet. IP address 8.241.122.254 performed the same function as 67.27.158.126. IP address 3.33.152.147 was identified as malicious, but it (the destination IP) did not complete the TCP handshake from the host when ran in app.any.run.



The screenshot shows a network traffic analysis tool interface. It has tabs for HTTP Requests (5), Connections (13), DNS Requests (9), and Threats (0). A sidebar on the left has categories: NETWORK, FILES, and BUG. The main table lists network requests with columns: Timeshift, Headers, Rep, PID, Process name, CN, and URL. The first row shows a 404 Not Found response for a GET request to a URL from malwareanalysisbook.com. Subsequent rows show successful 200 OK responses for GET requests to windowsupdate.com and ocs.digicert.com.

Timeshift	Headers	Rep	PID	Process name	CN	URL
1569 ms	GET 404: Not Found	✓	3512	iexplore.exe	🇺🇸	http://www.malwareanalysisbook.com/ad...
17870 ms	GET 200: OK	✓	3144	iexplore.exe	🇺🇸	http://ctldl.windowsupdate.com/msdownlo...
21958 ms	GET 200: OK	✓	3144	iexplore.exe	🇬🇧	http://ocsp.digicert.com/MFEwTzBNMEsw...
39379 ms	GET 200: OK	✓	3144	iexplore.exe	🇺🇸	http://ctldl.windowsupdate.com/msdownlo...
41378 ms	GET 200: OK	✓	3144	iexplore.exe	🇬🇧	http://ocsp.digicert.com/MFEwTzBNMEsw...

Figure 42: app.any.run report for file Lab01-03.exe



The screenshot shows a Microsoft Q&A page. The header includes the Microsoft logo and navigation links: Learn, Documentation, Training, Certifications, Q&A (selected), Code Samples, Assessments, Shows, and Events. Below the header, there are tabs for Q&A, Questions, Tags, and FAQ & Help. The main content area features a large heading: "CTLDDL.windowsupdate.com being blocked due to mailicious IP (IP address is being blocked)". Below this, it says "asked Jun 7, 2022, 7:28 AM by" followed by a user profile for Kevin wagner.

Microsoft | Learn | Documentation | Training | Certifications | Q&A | Code Samples | Assessments | Shows | Events

Q&A | Questions | Tags | FAQ & Help

CTLDDL.windowsupdate.com being blocked due to mailicious IP (IP address is being blocked)

asked Jun 7, 2022, 7:28 AM by


 Kevin wagner

Figure 43: Domain that file Lab01-03.exe calls to is malicious.

CYBV 454 Assignment 1 LIVINGSTON

The image shows a Wireshark packet capture interface. On the left, the 'Main object - Lab01-03.exe' pane lists several hashes: SHA256 (7983a582939924c...), SHA1 (290ab6f431f46547...), and MD5 (9c5c27494c28ed0...). Below this, the 'Connections (4)' pane shows four IP addresses: 3.33.152.147, 67.27.158.126, 8.241.122.254, and 15.197.142.173. The main packet list pane shows a series of packets. Packet 247 is a SYN packet from 192.168.100.116 to 67.27.158.126. Packet 248 is a SYN, ACK packet from 67.27.158.126 to 192.168.100.116. Packet 249 is an ACK packet from 192.168.100.116 to 67.27.158.126. Packet 250 is a GET request from 192.168.100.116 to 67.27.158.126. The packet details pane shows the GET request for the URL `/msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?...`. The packet bytes pane shows the raw data of the GET request.

No.	Time	Source	Destination	Protocol	Length	Info
247	39.484589	192.168.100.116	67.27.158.126	TCP	66	57677 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
248	39.520100	67.27.158.126	192.168.100.116	TCP	66	80 → 57677 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1206 SACK_PERM
249	39.520236	192.168.100.116	67.27.158.126	TCP	54	57677 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
250	39.520401	192.168.100.116	67.27.158.126	HTTP	340	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?...
251	39.556340	67.27.158.126	192.168.100.116	TCP	54	80 → 57677 [ACK] Seq=1 Ack=287 Win=64256 Len=0
252	39.626662	67.27.158.126	192.168.100.116	TCP	1260	80 → 57677 [ACK] Seq=1 Ack=287 Win=64256 Len=1206 [TCP segment of a
253	39.626722	67.27.158.126	192.168.100.116	TCP	1260	80 → 57677 [PSH, ACK] Seq=1207 Ack=287 Win=64256 Len=1206 [TCP segme
254	39.626756	67.27.158.126	192.168.100.116	TCP	1260	80 → 57677 [ACK] Seq=2413 Ack=287 Win=64256 Len=1206 [TCP segment of
255	39.626951	192.168.100.116	67.27.158.126	TCP	54	57677 → 80 [ACK] Seq=287 Ack=2413 Win=66304 Len=0
256	39.627513	67.27.158.126	192.168.100.116	TCP	780	80 → 57677 [PSH, ACK] Seq=3619 Ack=287 Win=64256 Len=726 [TCP segmen
257	39.627687	192.168.100.116	67.27.158.126	TCP	54	57677 → 80 [ACK] Seq=287 Ack=4345 Win=66304 Len=0
258	39.627982	67.27.158.126	192.168.100.116	HTTP	946	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
259	39.828439	192.168.100.116	67.27.158.126	TCP	54	57677 → 80 [ACK] Seq=287 Ack=5237 Win=65280 Len=0

Figure 44: GET request from host to malicious IP.

When ran on both a Windows 10 and Windows XP VM, an instance of internet explorer was executed. Both of the tabs for internet explorer had a URL of <http://www.malwareanalysisbook.com/ad.html>, which confirms the findings of app.any.run with the exception of the ctldl.windowsupdate URL. A Java plugin notification was at the bottom of the IE window (Figure 45). Enabling this plugin did not produce any effects. Since the IP addresses flagged by app.any.run were flagged as malicious as well as the Microsoft download site, those IP addresses can be monitored for suspicious activity and the Microsoft website should be blacklisted on host-based firewalls and Access Control Lists in an enterprise network. It is unclear as to what this malware does.

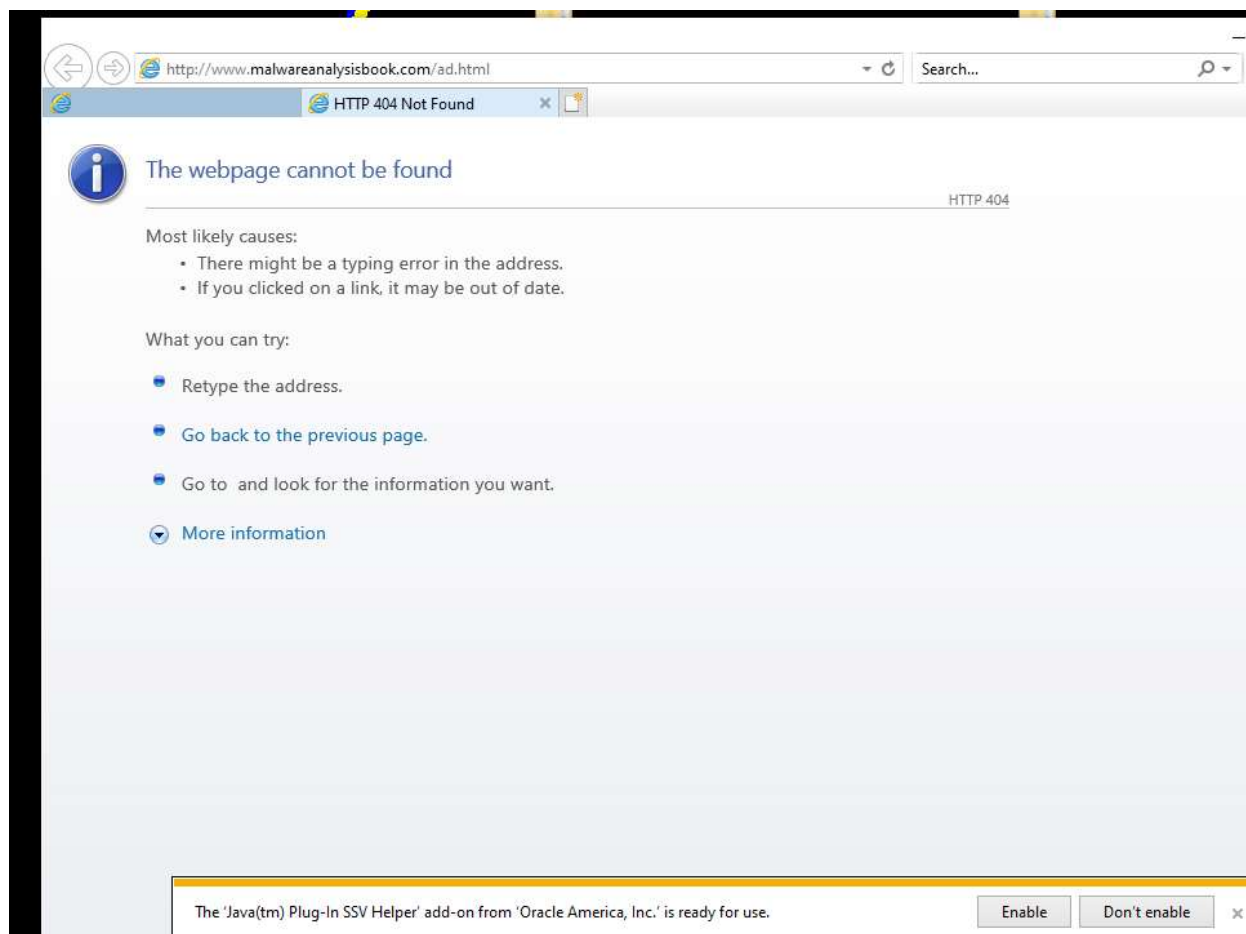


Figure 45: IE tabs opened by Lab01-03.exe.

LAB 1-4

- LAB01-04.exe : 625ac05fd47adc3c63700c3b30de79ab

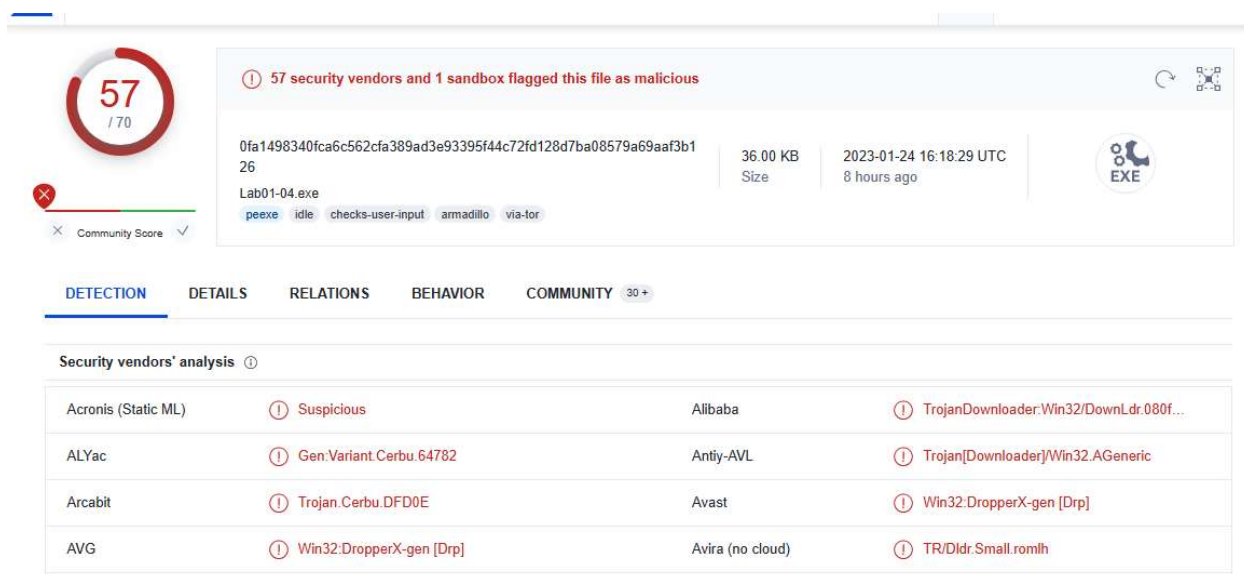


Figure 46: Virus Total Findings for file Lab01-04.exe.

Virus Total found 57 matching signatures for Trojan malware for the file Lab01-04.exe (Figure 46). It has a compilation timestamp of 30 Aug 2019 at 22:26:59 UTC (Figure 47). 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 (Figure 48). Under the “Behavior” tab, it is noted that the malware has other indicators of persistence, privilege escalation, and defense evasion (Figure 49). Noting that it has input capture characteristics, it is possible that this malware has characteristics of a keylogger, and has some functionality to perform DNS lookups (Figure 50).

Header	
Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2019-08-30 22:26:59 UTC
Entry Point	5583
Contained Sections	4

Figure 47: Virus Total compilation timestamp for file Lab01-04.exe.

Imports	
+	ADVAPI32.dll
+	KERNEL32.dll
+	MSVCRT.dll

Figure 48: Virus Total imports for file Lab01-04.exe.

Persistence	
Windows Service	T1543.003
① Creates or modifies windows services	
LSASS Driver	T1547.008
① Spawns drivers	
Privilege Escalation	
Process Injection	T1055
① Spawns processes	
① Creates a process in suspended mode (likely to inject code)	
Windows Service	T1543.003
① Creates or modifies windows services	
LSASS Driver	T1547.008
① Spawns drivers	
Privilege Escalation	
Access Token Manipulation	T1134
① Acquire debug privileges	
① Modify access privileges	
Defense Evasion	
Process Injection	T1055
① Spawns processes	
① Creates a process in suspended mode (likely to inject code)	

Figure 49: Virus Total behavior for file Lab01-04.exe.

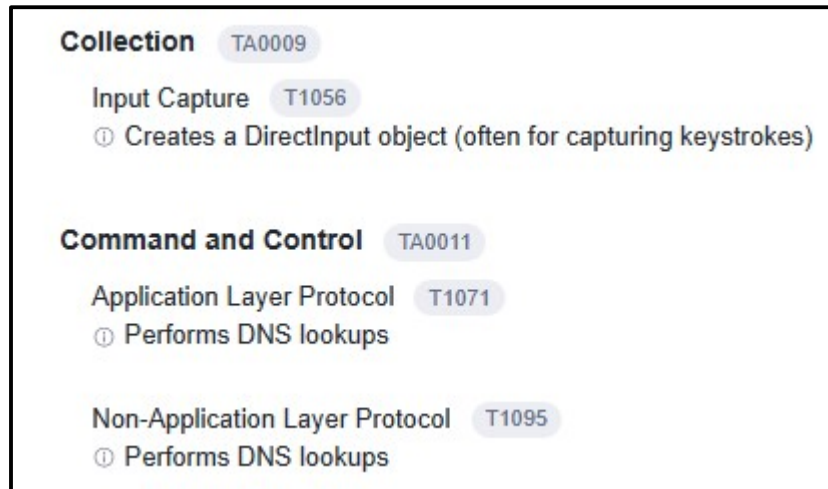


Figure 50: Virus Total input capture and C&C for file Lab01-04.exe.

LAB 1-4 Question 1

Upload the *Lab01-04.exe* file to <http://www.VirusTotal.com/>. Does it match any existing antivirus definitions?

Virus Total found 57 matching signatures for Trojan malware for the file Lab01-04.exe (Figure 46).

LAB 1-4 Question 2

Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

PEiD did not find any indication that the file is packed, but was written in C++ (Figure 51).

There are no indications of obfuscation. We see that a suspicious URL to

www.malwareanalysisbok.com/updater.exe is called which will potentially download malicious software (Figure 52). Additionally, the string `\system32\wupdmgr.exe` in combination with `GetWindowsDirectory` indicate that a file might be created or edited by the malware (Figure 53).

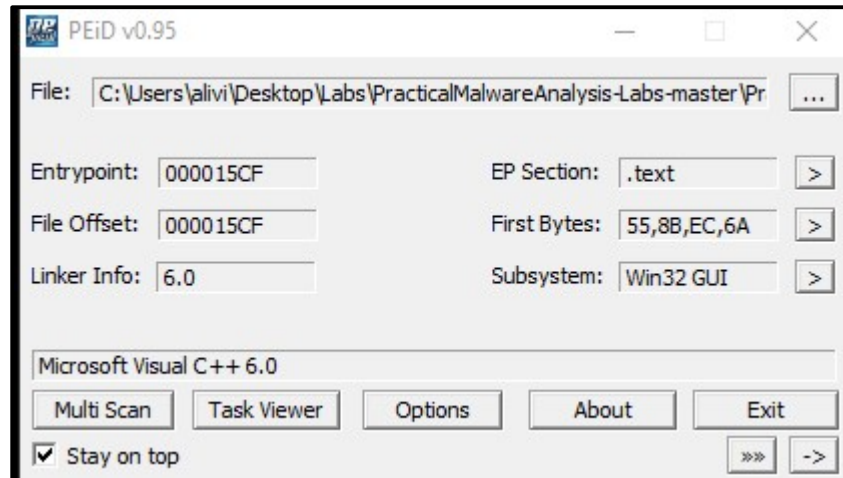


Figure 51: PEiD – no packing for file Lab01-04.exe.

000000406296	0	_controlfp
000000407070	0	\winup.exe
000000407084	0	\system32\wupdmgrd.exe
0000004070A4	0	http://www.practicalmalwareanalysis.com/updater.exe
00000040004D	0	!This program cannot be run in DOS mode.
0000004001E0	0	.text

Figure 52: Lab01-04.exe suspicious callout to website.

00000030B8	0000004030B8	0	EnumProcesses
00000030C8	0000004030C8	0	psapi.dll
00000030D4	0000004030D4	0	\system32\wupdmgr.exe
00000030F4	0000004030F4	0	\winup.exe
00000040AD	0000004040AD	0	!This program cannot be run in DOS mode.
0000004240	000000404240	0	.text
0000004268	000000404268	0	.rdata
000000428F	00000040428F	0	@.data
0000005134	000000405134	0	Rh<0@
0000005159	000000405159	0	QhD0@
000000616A	00000040616A	0	GetWindowsDirectoryA
0000006182	000000406182	0	WinExec

Figure 53 Lab01-04.exe call to GetWindowsDirectory

LAB 1-4 Question 3

When was this program compiled?

It has a compilation timestamp of 30 Aug 2019 at 22:26:59 UTC (Figure 47).

LAB 1-4 Question 4

Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?

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 (Figure 48). Because of the callout to an unknown URL that appears to have a .exe file attached (Figure 52), it is reasonable to assume that the malware will install this file or make an edit to an existing file in C:\Windows\System32\wupdmgr.exe directory (Figure 53).

LAB 1-4 Question 5

What host- or network-based indicators could be used to identify this malware on infected machines?

Although there is a potential to call to a suspicious website to possibly download a .exe file, there aren't any .dll imports that suggest it utilizes an internet connection to do so (Figure 54). FakenetNG and app.any.run did not report any internet queries made by the malware (Figure 55).

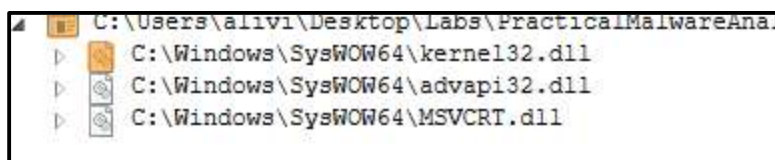


Figure 53: PEiD report for Lab01-04.exe.

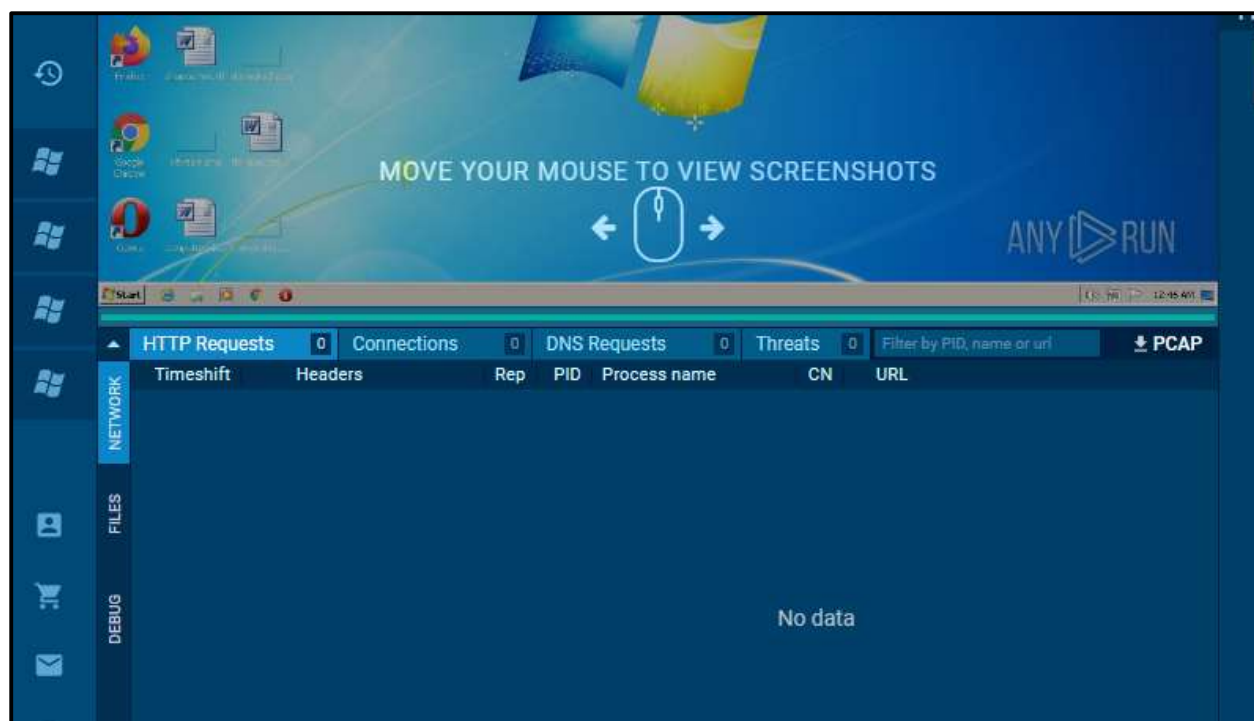


Figure 54: PEiD report for Lab01-04.exe.

LAB 1-4 Question 6

This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?

The .bin file extracted from Lab01-04.exe using ResourceHacker shows an interesting import when viewed in PEvent: “URLDownloadToFileA”. It also calls the command “WinExec” (Figure 55). This suggests that the malicious file has an embedded file with access to network functions because URLDownloadToFile is commonly used by malicious downloaders. The WinExec most likely executes the file which was downloaded. However, when the malware was ran on a Windows 10 VM, there were no suspicious callouts for downloading files when Process Monitor or AupdateDNS were running.

pFile	Data	Description	Value
00002000	00002120	Hint/Name RVA	02D3 WinExec
00002004	0000212A	Hint/Name RVA	0165 GetTempPathA
00002008	00002108	Hint/Name RVA	017D GetWindowsDirectoryA
0000200C	00000000	End of Imports	KERNEL32.dll
00002010	00002234	Hint/Name RVA	00B7 _controlfp
00002014	0000216A	Hint/Name RVA	01AE _snprintf
00002018	00002182	Hint/Name RVA	00D3 _exit
0000201C	0000218A	Hint/Name RVA	0048 _XcptFilter
00002020	00002198	Hint/Name RVA	0249 exit
00002024	000021A0	Hint/Name RVA	0064 __p__initenv
00002028	000021B0	Hint/Name RVA	0058 __getmainargs
0000202C	000021C0	Hint/Name RVA	010F _initterm
00002030	000021CC	Hint/Name RVA	0083 __setusermatherr
00002034	000021E0	Hint/Name RVA	009D _adjust_fdiv
00002038	000021F0	Hint/Name RVA	006A __p__commode
0000203C	00002200	Hint/Name RVA	006F __p__fmode
00002040	0000220E	Hint/Name RVA	0081 __set_app_type
00002044	00002220	Hint/Name RVA	00CA _except_handler3
00002048	00000000	End of Imports	MSVCRT.dll
0000204C	00002148	Hint/Name RVA	003E URLDownloadToFileA
00002050	00000000	End of Imports	urlmon.dll

Figure 55: Binary extraction from Lab01-04.exe.