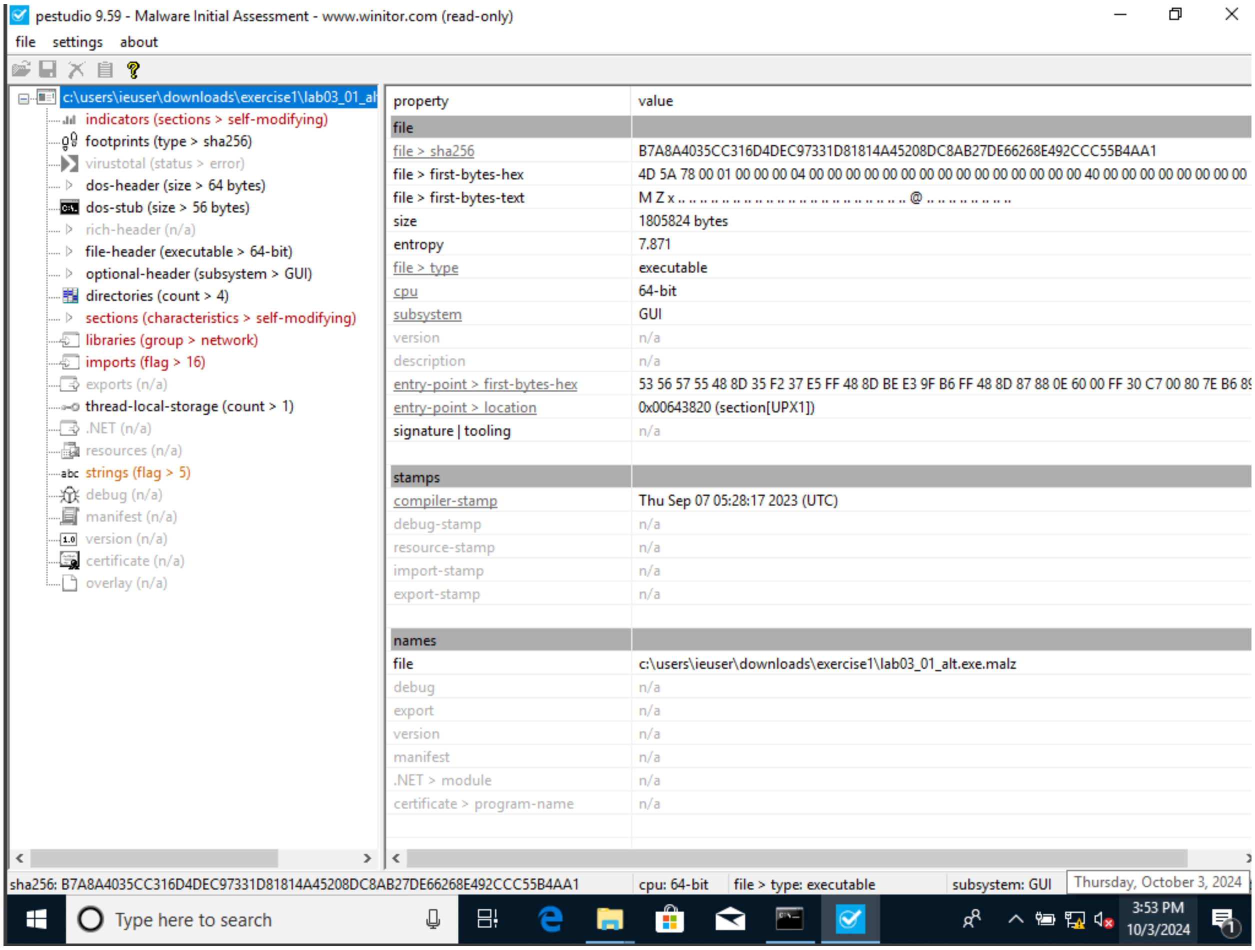
CPSC 458-01 Lab 3-1

Wayne Muse

Question 1: What are this malware's imports and strings?

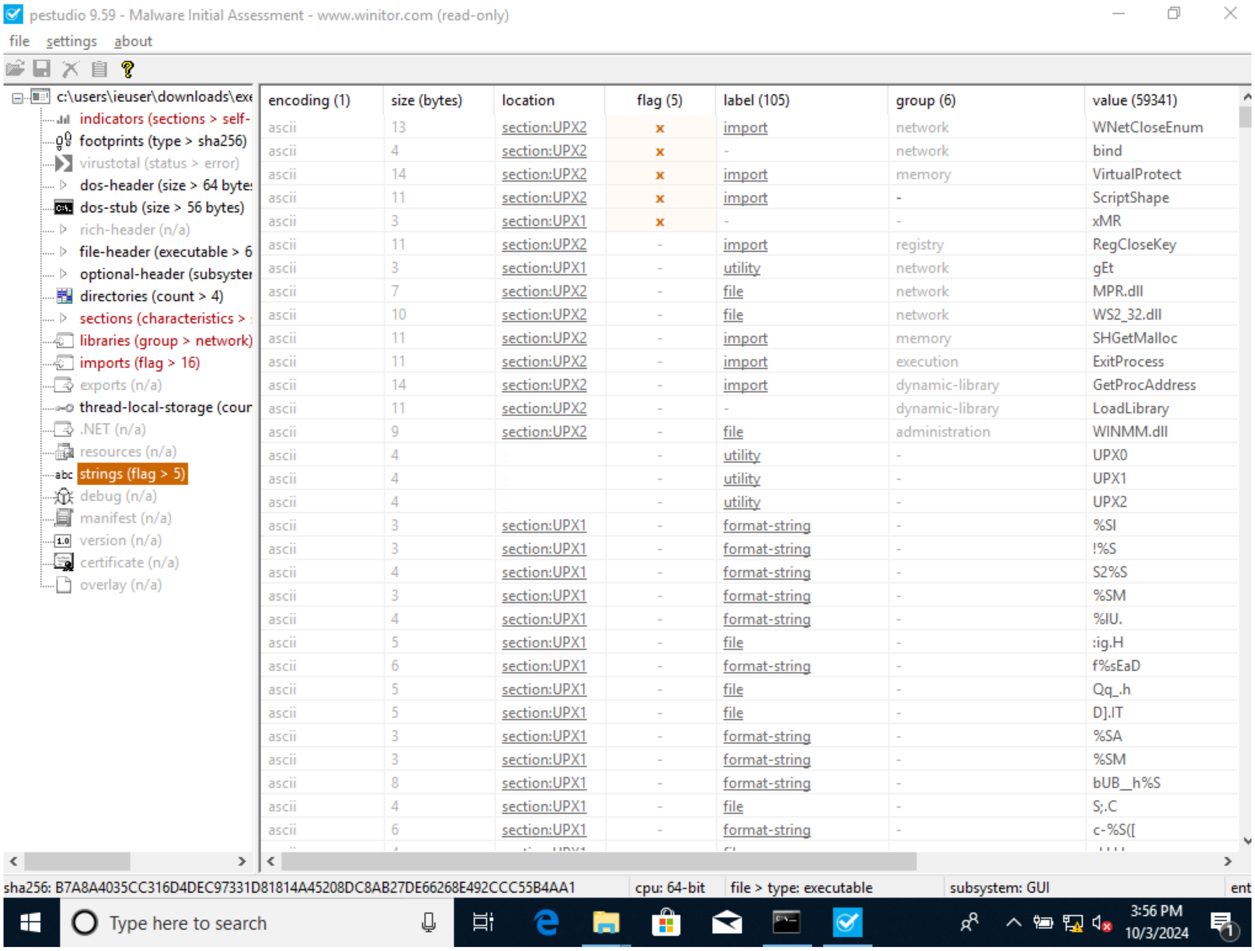


pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

- c:\users\ieuser\downloads\exercise1\lab03_01_al
  - indicators (sections > self-modifying)
  - footprints (type > sha256)
  - virustotal (status > error)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 56 bytes)
  - rich-header (n/a)
  - file-header (executable > 64-bit)
  - optional-header (subsystem > GUI)
  - directories (count > 4)
  - sections (characteristics > self-modifying)
  - libraries (group > network)
  - imports (flag > 16)
  - exports (n/a)
  - thread-local-storage (count > 1)
  - .NET (n/a)
  - resources (n/a)
  - strings (flag > 5)
  - debug (n/a)
  - manifest (n/a)
  - version (n/a)
  - certificate (n/a)
  - overlay (n/a)

property	value
file	
file > sha256	B7A8A4035CC316D4DEC97331D81814A45208DC8AB27DE66268E492CCC55B4AA1
file > first-bytes-hex	4D 5A 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file > first-bytes-text	M Z x .. .. @ .. ..
size	1805824 bytes
entropy	7.871
file > type	executable
cpu	64-bit
subsystem	GUI
version	n/a
description	n/a
entry-point > first-bytes-hex	53 56 57 55 48 8D 35 F2 37 E5 FF 48 8D BE E3 9F B6 FF 48 8D 87 88 0E 60 00 FF 30 C7 00 80 7E B6 8
entry-point > location	0x00643820 (section[UPX1])
signature | tooling	n/a
stamps	
compiler-stamp	Thu Sep 07 05:28:17 2023 (UTC)
debug-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a
names	
file	c:\users\ieuser\downloads\exercise1\lab03_01_alt.exe.malz
debug	n/a
export	n/a
version	n/a
manifest	n/a
.NET > module	n/a
certificate > program-name	n/a

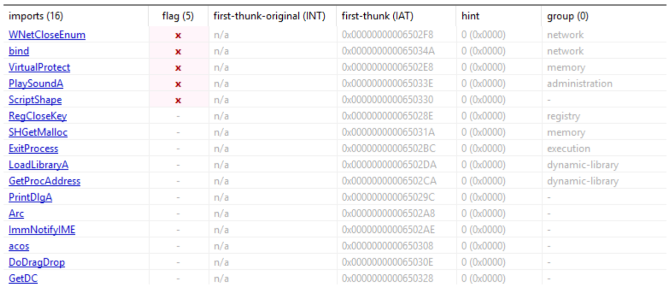
sha256: B7A8A4035CC316D4DEC97331D81814A45208DC8AB27DE66268E492CCC55B4AA1 cpu: 64-bit file > type: executable subsystem: GUI Thursday, October 3, 2024


pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)
file settings about

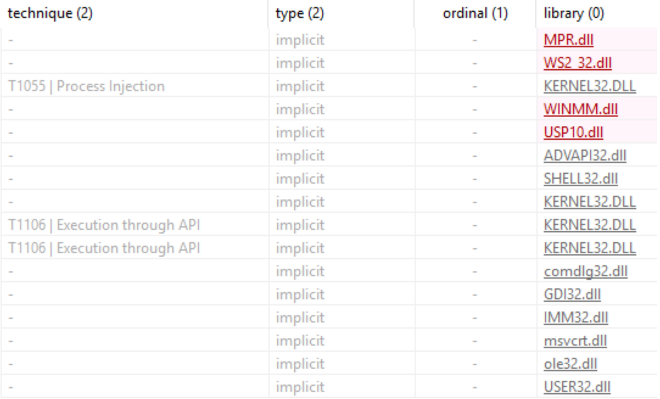
```
c:\users\ieuser\downloads\exe
  indicators (sections > self-
  footprints (type > sha256)
  virustotal (status > error)
  dos-header (size > 64 bytes
  dos-stub (size > 56 bytes)
  rich-header (n/a)
  file-header (executable > 6
  optional-header (subsyster
  directories (count > 4)
  sections (characteristics > 
  libraries (group > network)
  imports (flag > 16)
  exports (n/a)
  thread-local-storage (cour
  .NET (n/a)
  resources (n/a)
  strings (flag > 5)
  debug (n/a)
  manifest (n/a)
  version (n/a)
  certificate (n/a)
  overlay (n/a)
```

encoding (1)	size (bytes)	location	flag (5)	label (105)	group (6)	value (59341)
ascii	13	section:UPX2	×	import	network	WNetCloseEnum
ascii	4	section:UPX2	×	-	network	bind
ascii	14	section:UPX2	×	import	memory	VirtualProtect
ascii	11	section:UPX2	×	import	-	ScriptShape
ascii	3	section:UPX1	×	-	-	xMR
ascii	11	section:UPX2	-	import	registry	RegCloseKey
ascii	3	section:UPX1	-	utility	network	gEt
ascii	7	section:UPX2	-	file	network	MPR.dll
ascii	10	section:UPX2	-	file	network	WS2_32.dll
ascii	11	section:UPX2	-	import	memory	SHGetMalloc
ascii	11	section:UPX2	-	import	execution	ExitProcess
ascii	14	section:UPX2	-	import	dynamic-library	GetProcAddress
ascii	11	section:UPX2	-	-	dynamic-library	LoadLibrary
ascii	9	section:UPX2	-	file	administration	WINMM.dll
ascii	4		-	utility	-	UPX0
ascii	4		-	utility	-	UPX1
ascii	4		-	utility	-	UPX2
ascii	3	section:UPX1	-	format-string	-	%SI
ascii	3	section:UPX1	-	format-string	-	!%S
ascii	4	section:UPX1	-	format-string	-	S2%S
ascii	3	section:UPX1	-	format-string	-	%SM
ascii	4	section:UPX1	-	format-string	-	%IU.
ascii	5	section:UPX1	-	file	-	:ig.H
ascii	6	section:UPX1	-	format-string	-	f%sEaD
ascii	5	section:UPX1	-	file	-	Qq_.h
ascii	5	section:UPX1	-	file	-	D].IT
ascii	3	section:UPX1	-	format-string	-	%SA
ascii	3	section:UPX1	-	format-string	-	%SM
ascii	8	section:UPX1	-	format-string	-	bUB_h%S
ascii	4	section:UPX1	-	file	-	S;.C
ascii	6	section:UPX1	-	format-string	-	c-%S([

sha256: B7A8A4035CC316D4DEC97331D81814A45208DC8AB27DE66268E492CCC55B4AA1 | cpu: 64-bit | file > type: executable | subsystem: GUI | ent



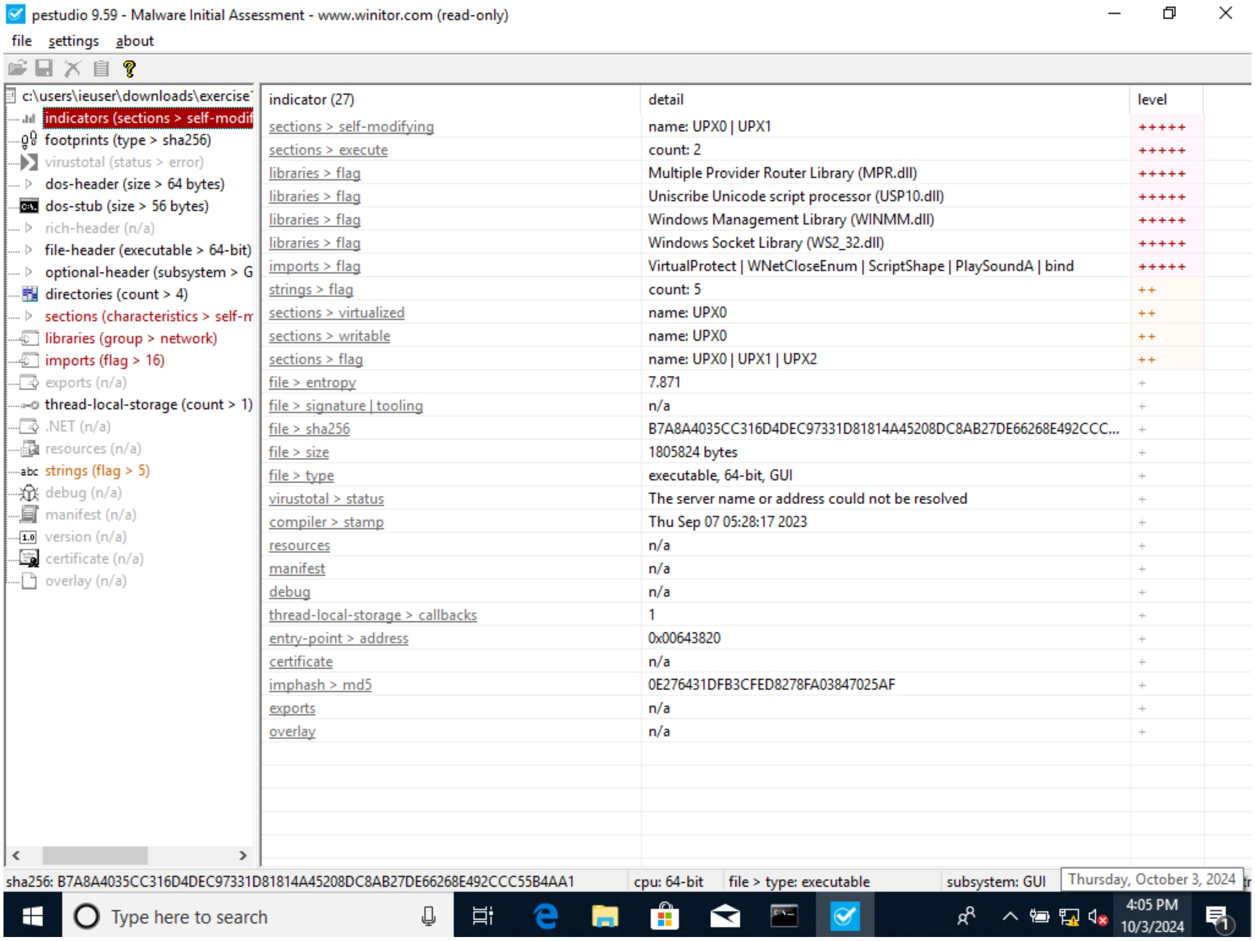
imports (16)	flag (5)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (0)
WNetCloseEnum	×	n/a	0x00000000006502F8	0 (0x0000)	network
bind	×	n/a	0x000000000065034A	0 (0x0000)	network
VirtualProtect	×	n/a	0x00000000006502E8	0 (0x0000)	memory
PlaySoundA	×	n/a	0x000000000065033E	0 (0x0000)	administration
ScriptShape	×	n/a	0x0000000000650330	0 (0x0000)	-
RegCloseKey	-	n/a	0x000000000065028E	0 (0x0000)	registry
SHGetMalloc	-	n/a	0x000000000065031A	0 (0x0000)	memory
ExitProcess	-	n/a	0x00000000006502BC	0 (0x0000)	execution
LoadLibraryA	-	n/a	0x00000000006502DA	0 (0x0000)	dynamic-library
GetProcAddress	-	n/a	0x00000000006502CA	0 (0x0000)	dynamic-library
PrintDlgA	-	n/a	0x000000000065029C	0 (0x0000)	-
Arc	-	n/a	0x00000000006502A8	0 (0x0000)	-
ImmNotifyIME	-	n/a	0x00000000006502AE	0 (0x0000)	-
acos	-	n/a	0x0000000000650308	0 (0x0000)	-
DoDragDrop	-	n/a	0x000000000065030E	0 (0x0000)	-
GetDC	-	n/a	0x0000000000650328	0 (0x0000)	-



technique (2)	type (2)	ordinal (1)	library (0)
-	implicit	-	MPR.dll
-	implicit	-	WS2_32.dll
T1055 | Process Injection	implicit	-	KERNEL32.DLL
-	implicit	-	WINMM.dll
-	implicit	-	USP10.dll
-	implicit	-	ADVAPI32.dll
-	implicit	-	SHELL32.dll
-	implicit	-	KERNEL32.DLL
T1106 | Execution through API	implicit	-	KERNEL32.DLL
T1106 | Execution through API	implicit	-	KERNEL32.DLL
-	implicit	-	comdlg32.dll
-	implicit	-	GDI32.dll
-	implicit	-	IMM32.dll
-	implicit	-	msvcrt.dll
-	implicit	-	ole32.dll
-	implicit	-	USER32.dll

PEStudio has flagged 5 of the 16 imports. From the imports, it appears that the malware is attempting to access and write to the machine’s memory. Additionally, it appears to affect network connections by importing WnetCloseEnum. This import is responsible for closing network connections implying that this malware sample establishes or hijacks some network connection.

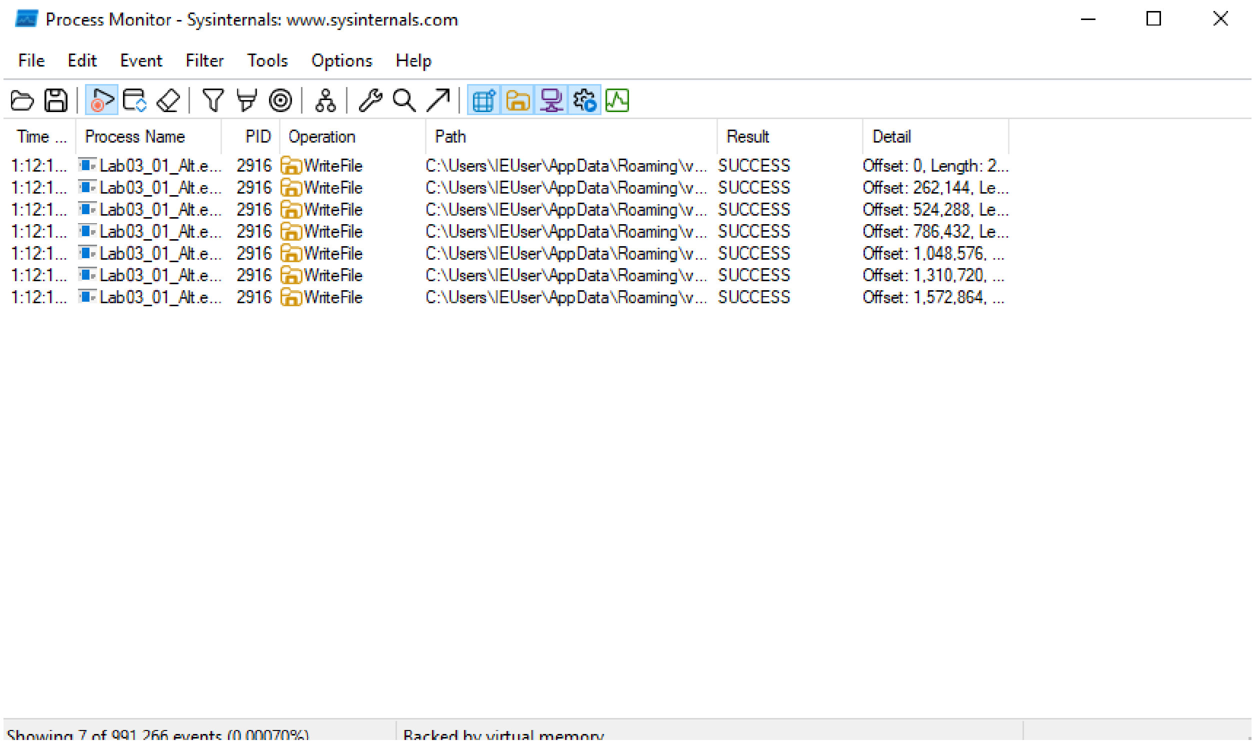
Question 2: What are the malware's host-based indicators?


pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)
file settings about
c:\users\ieuser\downloads\exercise
indicators (sections > self-modif
footprints (type > sha256)
virustotal (status > error)
dos-header (size > 64 bytes)
dos-stub (size > 56 bytes)
rich-header (n/a)
file-header (executable > 64-bit)
optional-header (subsystem > G
directories (count > 4)
sections (characteristics > self-m
libraries (group > network)
imports (flag > 16)
exports (n/a)
thread-local-storage (count > 1)
.NET (n/a)
resources (n/a)
strings (flag > 5)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (n/a)
Type here to search
4:05 PM
10/3/2024

indicator (27)	detail	level
sections > self-modifying	name: UPX0 | UPX1	+++++
sections > execute	count: 2	+++++
libraries > flag	Multiple Provider Router Library (MPR.dll)	+++++
libraries > flag	Uniscribe Unicode script processor (USP10.dll)	+++++
libraries > flag	Windows Management Library (WINMM.dll)	+++++
libraries > flag	Windows Socket Library (WS2_32.dll)	+++++
imports > flag	VirtualProtect | WNetCloseEnum | ScriptShape | PlaySoundA | bind	+++++
strings > flag	count: 5	++
sections > virtualized	name: UPX0	++
sections > writable	name: UPX0	++
sections > flag	name: UPX0 | UPX1 | UPX2	++
file > entropy	7.871	+
file > signature | tooling	n/a	+
file > sha256	B7A8A4035CC316D4DEC97331D81814A45208DC8AB27DE66268E492CCC...	+
file > size	1805824 bytes	+
file > type	executable, 64-bit, GUI	+
virustotal > status	The server name or address could not be resolved	+
compiler > stamp	Thu Sep 07 05:28:17 2023	+
resources	n/a	+
manifest	n/a	+
debug	n/a	+
thread-local-storage > callbacks	1	+
entry-point > address	0x00643820	+
certificate	n/a	+
imphash > md5	0E276431DFB3CFED8278FA03847025AF	+
exports	n/a	+
overlay	n/a	+

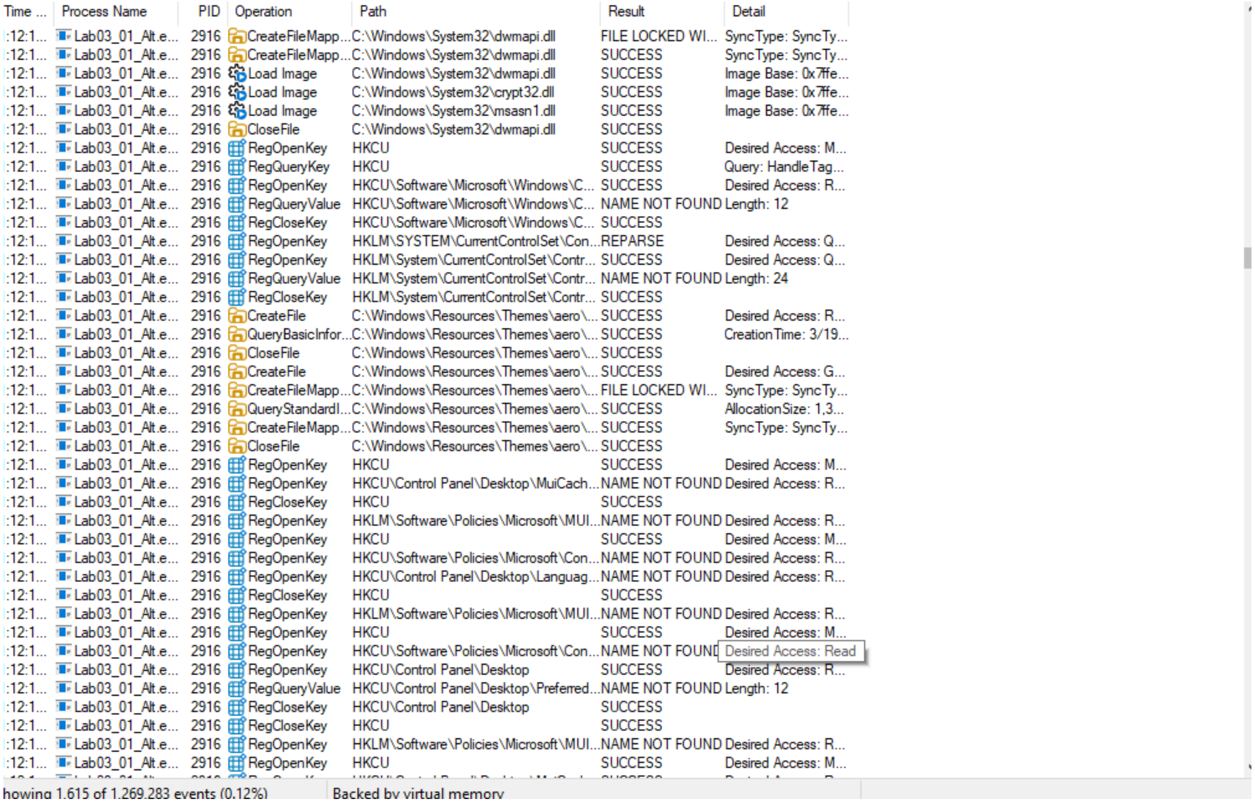
sha256: B7A8A4035CC316D4DEC97331D81814A45208DC8AB27DE66268E492CCC55B4AA1 cpu: 64-bit file > type: executable subsystem: GUI Thursday, October 3, 2024

Using PEStudio again to find the malware's host-based indicators there are 7 highly suspicious indicators and 4 mildly suspicious. From the indicators it seems that this code is self-modifying and accesses various networking processes such a WS2_32.dll which creates a socket and MPR.dll which handles computer communication between the OS and multiple network providers. We see in screenshots below that under a Dynamic Analysis, the malware writes to C\Users\IEUser\AppData\Roaming\vmx32to64.exe which allows it run on start up and establish a network connection.



Time ...	Process Name	PID	Operation	Path	Result	Detail
1:12:1...	Lab03_01_Alt.e...	2916	WriteFile	C:\Users\IEUser\AppData\Roaming\v...	SUCCESS	Offset: 0, Length: 2...
1:12:1...	Lab03_01_Alt.e...	2916	WriteFile	C:\Users\IEUser\AppData\Roaming\v...	SUCCESS	Offset: 262,144, Le...
1:12:1...	Lab03_01_Alt.e...	2916	WriteFile	C:\Users\IEUser\AppData\Roaming\v...	SUCCESS	Offset: 524,288, Le...
1:12:1...	Lab03_01_Alt.e...	2916	WriteFile	C:\Users\IEUser\AppData\Roaming\v...	SUCCESS	Offset: 786,432, Le...
1:12:1...	Lab03_01_Alt.e...	2916	WriteFile	C:\Users\IEUser\AppData\Roaming\v...	SUCCESS	Offset: 1,048,576, ...
1:12:1...	Lab03_01_Alt.e...	2916	WriteFile	C:\Users\IEUser\AppData\Roaming\v...	SUCCESS	Offset: 1,310,720, ...
1:12:1...	Lab03_01_Alt.e...	2916	WriteFile	C:\Users\IEUser\AppData\Roaming\v...	SUCCESS	Offset: 1,572,864, ...

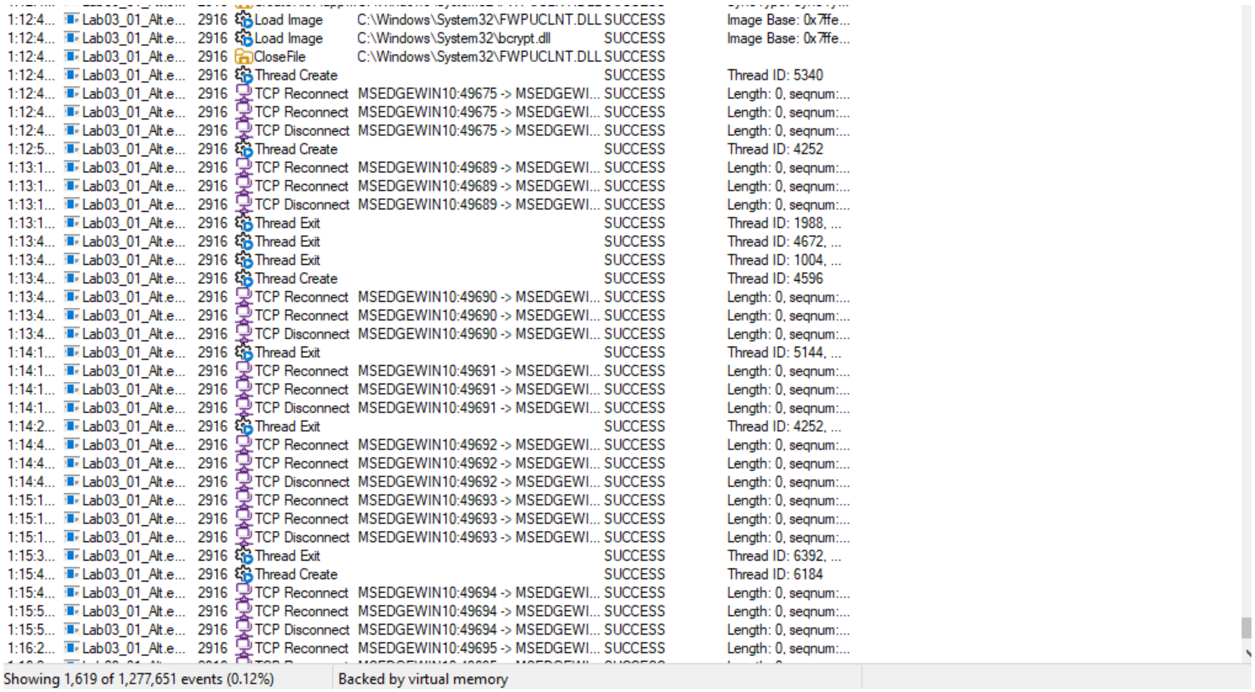
Showing 7 of 991,266 events (0.00070%) Backed by virtual memory



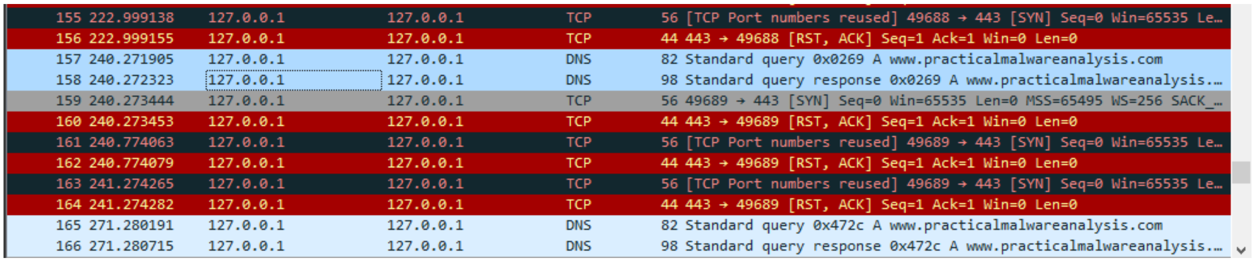
Time ...	Process Name	PID	Operation	Path	Result	Detail
:12:1...	Lab03_01_Alt.e...	2916	CreateFileMapp...	C:\Windows\System32\dwmapi.dll	FILE LOCKED WI...	SyncType: SyncTy...
:12:1...	Lab03_01_Alt.e...	2916	CreateFileMapp...	C:\Windows\System32\dwmapi.dll	SUCCESS	SyncType: SyncTy...
:12:1...	Lab03_01_Alt.e...	2916	Load Image	C:\Windows\System32\dwmapi.dll	SUCCESS	Image Base: 0x7ffe...
:12:1...	Lab03_01_Alt.e...	2916	Load Image	C:\Windows\System32\crypt32.dll	SUCCESS	Image Base: 0x7ffe...
:12:1...	Lab03_01_Alt.e...	2916	Load Image	C:\Windows\System32\msasn1.dll	SUCCESS	Image Base: 0x7ffe...
:12:1...	Lab03_01_Alt.e...	2916	CloseFile	C:\Windows\System32\dwmapi.dll	SUCCESS	
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
:12:1...	Lab03_01_Alt.e...	2916	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
:12:1...	Lab03_01_Alt.e...	2916	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	Length: 12
:12:1...	Lab03_01_Alt.e...	2916	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
:12:1...	Lab03_01_Alt.e...	2916	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
:12:1...	Lab03_01_Alt.e...	2916	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
:12:1...	Lab03_01_Alt.e...	2916	CreateFile	C:\Windows\Resources\Themes\aero\...	SUCCESS	Desired Access: R...
:12:1...	Lab03_01_Alt.e...	2916	QueryBasicInfor...	C:\Windows\Resources\Themes\aero\...	SUCCESS	CreationTime: 3/19...
:12:1...	Lab03_01_Alt.e...	2916	CloseFile	C:\Windows\Resources\Themes\aero\...	SUCCESS	
:12:1...	Lab03_01_Alt.e...	2916	CreateFile	C:\Windows\Resources\Themes\aero\...	SUCCESS	Desired Access: G...
:12:1...	Lab03_01_Alt.e...	2916	CreateFileMapp...	C:\Windows\Resources\Themes\aero\...	FILE LOCKED WI...	SyncType: SyncTy...
:12:1...	Lab03_01_Alt.e...	2916	QueryStandardI...	C:\Windows\Resources\Themes\aero\...	SUCCESS	AllocationSize: 1,3...
:12:1...	Lab03_01_Alt.e...	2916	CreateFileMapp...	C:\Windows\Resources\Themes\aero\...	SUCCESS	SyncType: SyncTy...
:12:1...	Lab03_01_Alt.e...	2916	CloseFile	C:\Windows\Resources\Themes\aero\...	SUCCESS	
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU\Control Panel\Desktop\MuiCach...	NAME NOT FOUND	Desired Access: R...
:12:1...	Lab03_01_Alt.e...	2916	RegCloseKey	HKCU	SUCCESS	
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Desired Access: R...
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU\Software\Policies\Microsoft\Con...	NAME NOT FOUND	Desired Access: R...
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU\Control Panel\Desktop\Languag...	NAME NOT FOUND	Desired Access: R...
:12:1...	Lab03_01_Alt.e...	2916	RegCloseKey	HKCU	SUCCESS	
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Desired Access: R...
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU\Software\Policies\Microsoft\Con...	NAME NOT FOUND	Desired Access: Read
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: R...
:12:1...	Lab03_01_Alt.e...	2916	RegQueryValue	HKCU\Control Panel\Desktop\Preferred...	NAME NOT FOUND	Length: 12
:12:1...	Lab03_01_Alt.e...	2916	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
:12:1...	Lab03_01_Alt.e...	2916	RegCloseKey	HKCU	SUCCESS	
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Desired Access: R...
:12:1...	Lab03_01_Alt.e...	2916	RegOpenKey	HKCU	SUCCESS	Desired Access: M...

howing 1,615 of 1,269,283 events (0.12%) Backed by virtual memory

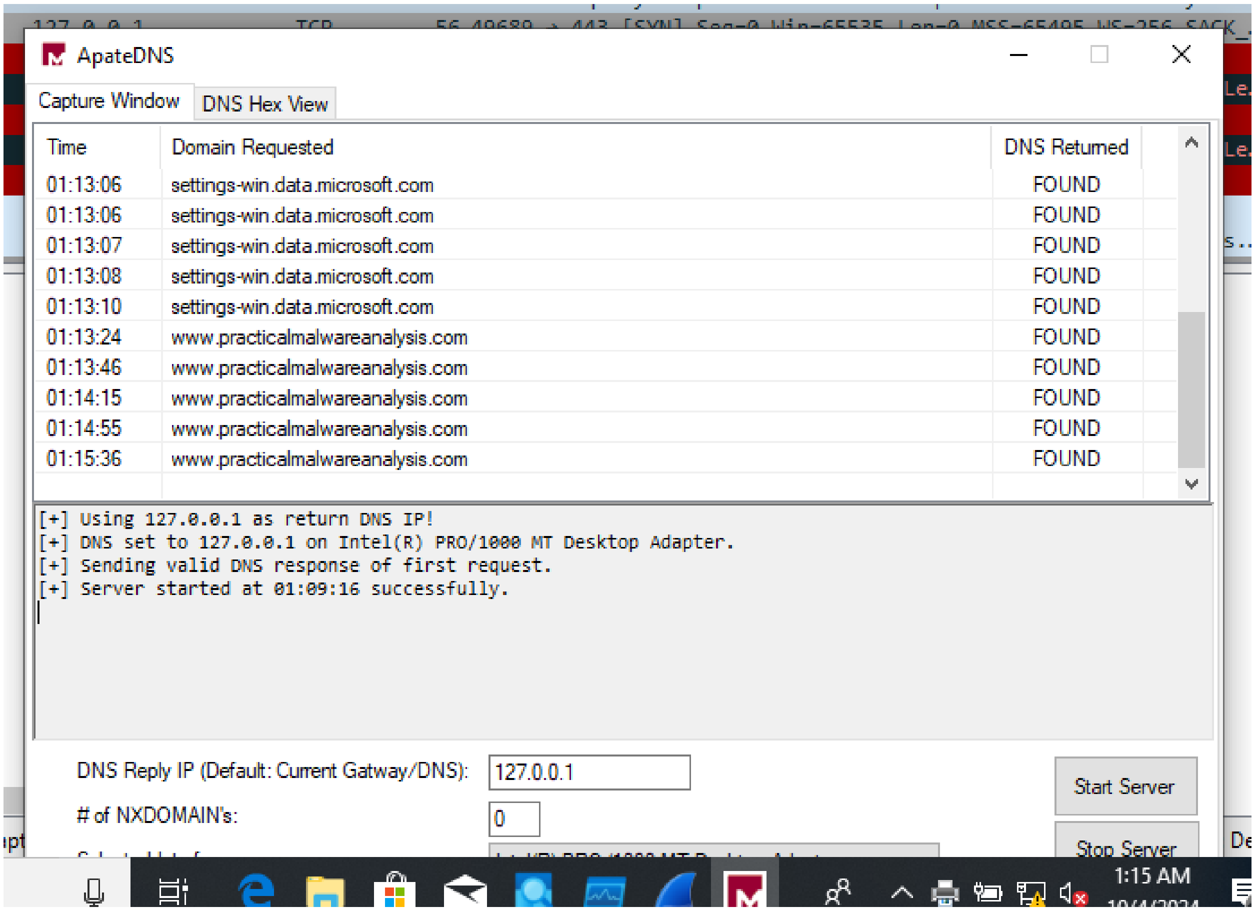
Question 3: Are there any useful network-based signatures for this malware? If so, what are they?



```
1:12:4... Lab03_01_Alt.e... 2916 Load Image      C:\Windows\System32\FWPUCLNT.DLL SUCCESS   Image Base: 0x7ffe...
1:12:4... Lab03_01_Alt.e... 2916 Load Image      C:\Windows\System32\bcrypt.dll   SUCCESS   Image Base: 0x7ffe...
1:12:4... Lab03_01_Alt.e... 2916 CloseFile       C:\Windows\System32\FWPUCLNT.DLL SUCCESS
1:12:4... Lab03_01_Alt.e... 2916 Thread Create                                    SUCCESS   Thread ID: 5340
1:12:4... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49675 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:12:4... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49675 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:12:4... Lab03_01_Alt.e... 2916 TCP Disconnect  MSEDGEWIN10:49675 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:12:5... Lab03_01_Alt.e... 2916 Thread Create                                    SUCCESS   Thread ID: 4252
1:13:1... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49689 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:13:1... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49689 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:13:1... Lab03_01_Alt.e... 2916 TCP Disconnect  MSEDGEWIN10:49689 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:13:1... Lab03_01_Alt.e... 2916 Thread Exit                                      SUCCESS   Thread ID: 1988, ...
1:13:4... Lab03_01_Alt.e... 2916 Thread Exit                                      SUCCESS   Thread ID: 4672, ...
1:13:4... Lab03_01_Alt.e... 2916 Thread Exit                                      SUCCESS   Thread ID: 1004, ...
1:13:4... Lab03_01_Alt.e... 2916 Thread Create                                    SUCCESS   Thread ID: 4596
1:13:4... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49690 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:13:4... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49690 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:13:4... Lab03_01_Alt.e... 2916 TCP Disconnect  MSEDGEWIN10:49690 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:14:1... Lab03_01_Alt.e... 2916 Thread Exit                                      SUCCESS   Thread ID: 5144, ...
1:14:1... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49691 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:14:1... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49691 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:14:1... Lab03_01_Alt.e... 2916 TCP Disconnect  MSEDGEWIN10:49691 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:14:2... Lab03_01_Alt.e... 2916 Thread Exit                                      SUCCESS   Thread ID: 4252, ...
1:14:4... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49692 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:14:4... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49692 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:14:4... Lab03_01_Alt.e... 2916 TCP Disconnect  MSEDGEWIN10:49692 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:15:1... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49693 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:15:1... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49693 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:15:1... Lab03_01_Alt.e... 2916 TCP Disconnect  MSEDGEWIN10:49693 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:15:3... Lab03_01_Alt.e... 2916 Thread Exit                                      SUCCESS   Thread ID: 6392, ...
1:15:4... Lab03_01_Alt.e... 2916 Thread Create                                    SUCCESS   Thread ID: 6184
1:15:4... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49694 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:15:5... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49694 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:15:5... Lab03_01_Alt.e... 2916 TCP Disconnect  MSEDGEWIN10:49694 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
1:16:2... Lab03_01_Alt.e... 2916 TCP Reconnect   MSEDGEWIN10:49695 -> MSEDGEWI... SUCCESS   Length: 0, seqnum:...
Showing 1,619 of 1,277,651 events (0.12%)   Backed by virtual memory
```



```
155 222.999138  127.0.0.1  127.0.0.1  TCP  56 [TCP Port numbers reused] 49688 → 443 [SYN] Seq=0 Win=65535 Le…
156 222.999155  127.0.0.1  127.0.0.1  TCP  44 443 → 49688 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
157 240.271905  127.0.0.1  127.0.0.1  DNS  82 Standard query 0x0269 A www.practicalmalwareanalysis.com
158 240.272323  127.0.0.1  127.0.0.1  DNS  98 Standard query response 0x0269 A www.practicalmalwareanalysis.…
159 240.273444  127.0.0.1  127.0.0.1  TCP  56 49689 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_…
160 240.273453  127.0.0.1  127.0.0.1  TCP  44 443 → 49689 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 240.774063  127.0.0.1  127.0.0.1  TCP  56 [TCP Port numbers reused] 49689 → 443 [SYN] Seq=0 Win=65535 Le…
162 240.774079  127.0.0.1  127.0.0.1  TCP  44 443 → 49689 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
163 241.274265  127.0.0.1  127.0.0.1  TCP  56 [TCP Port numbers reused] 49689 → 443 [SYN] Seq=0 Win=65535 Le…
164 241.274282  127.0.0.1  127.0.0.1  TCP  44 443 → 49689 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
165 271.280191  127.0.0.1  127.0.0.1  DNS  82 Standard query 0x472c A www.practicalmalwareanalysis.com
166 271.280715  127.0.0.1  127.0.0.1  DNS  98 Standard query response 0x472c A www.practicalmalwareanalysis.…
```



Time	Domain Requested	DNS Returned
01:13:06	settings-win.data.microsoft.com	FOUND
01:13:06	settings-win.data.microsoft.com	FOUND
01:13:07	settings-win.data.microsoft.com	FOUND
01:13:08	settings-win.data.microsoft.com	FOUND
01:13:10	settings-win.data.microsoft.com	FOUND
01:13:24	www.practicalmalwareanalysis.com	FOUND
01:13:46	www.practicalmalwareanalysis.com	FOUND
01:14:15	www.practicalmalwareanalysis.com	FOUND
01:14:55	www.practicalmalwareanalysis.com	FOUND
01:15:36	www.practicalmalwareanalysis.com	FOUND

```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending valid DNS response of first request.
[+] Server started at 01:09:16 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1

# of NXDOMAIN's: 0

This malware is similar to the sample from the book because both attempts to request the www.practicalmalwareanalysis.com domain. I opened ApateDNS and created a fake DNS server, I opened wireshark to capture any packets and used process monitor and filtered for malware. The malware attempts to establish a TCP connection likely trying to download something from practicalmalwareanalysis website.