

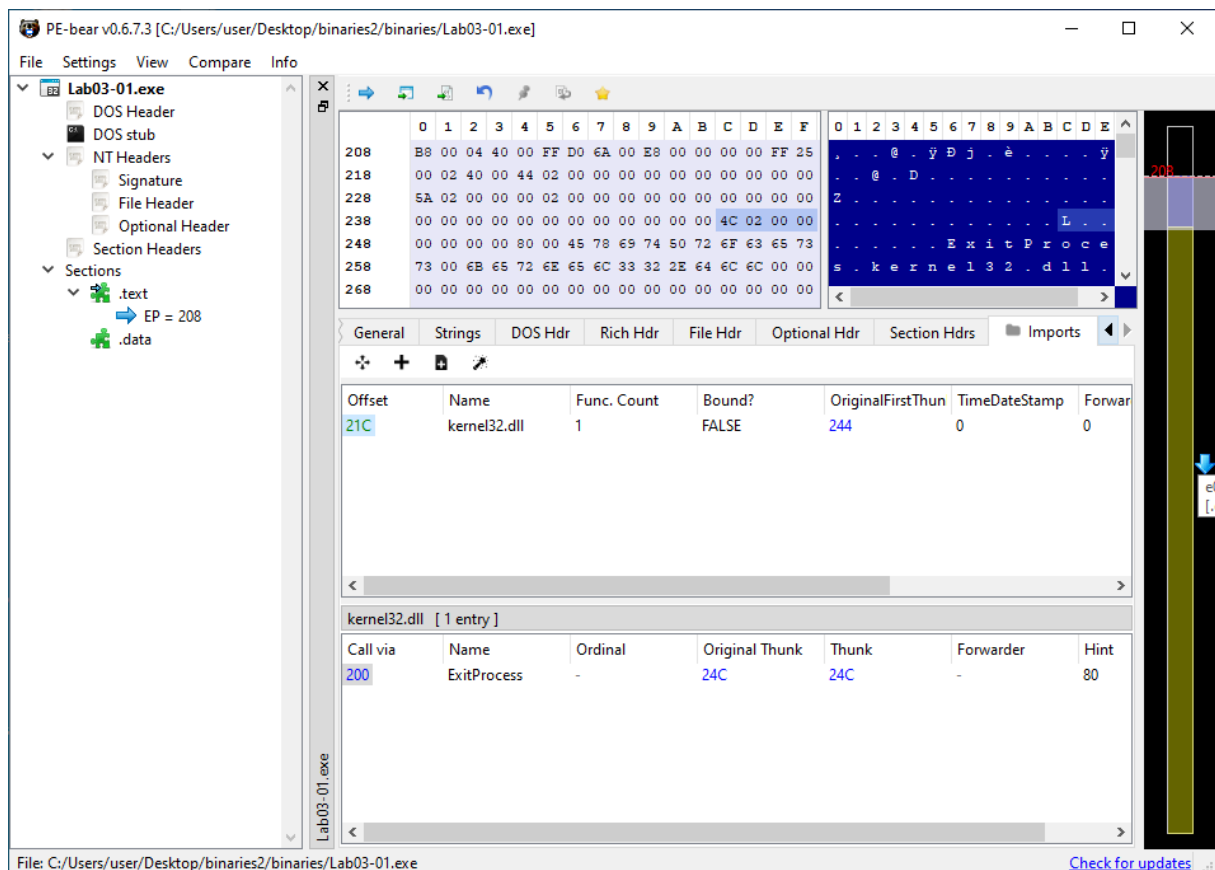
Analiza Malware Laboratorium nr 3

Raport – Nikodem Jakubowski

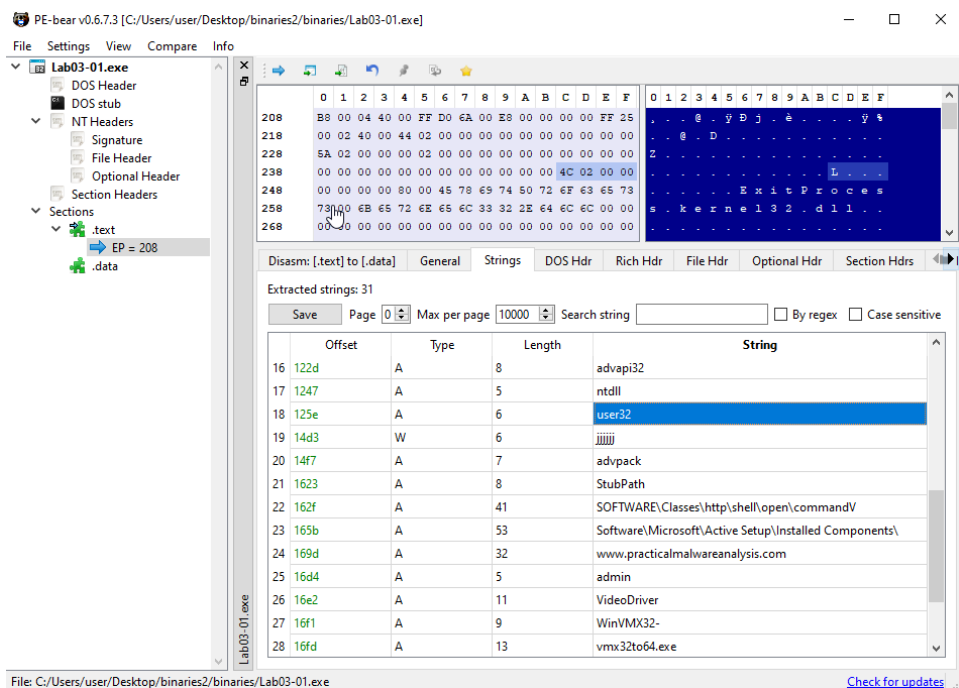
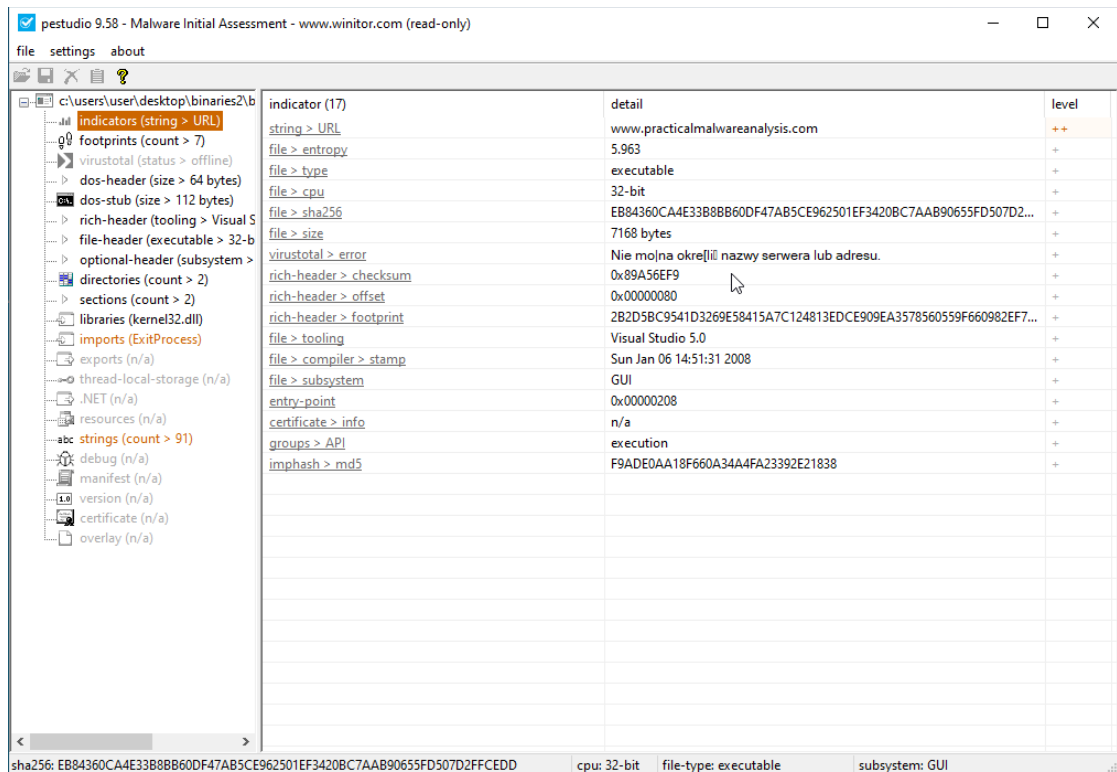
Laboratorium 3.1

Przeprowadź analizę złośliwego oprogramowania znajdującego się w pliku Lab03-01.exe. Wykorzystaj do tego celu podstawowe narzędzia do analizy dynamicznej. Odpowiedz na poniższe pytania:

1. Jakie importy i łańcuchy jesteśmy w stanie odszukać w tym pliku?
Znalezione importy dotyczą kernel32.dll. Sprawdziłem również, że plik jest zobfuskowany, więc prawdopodobnie nie widać wszystkiego.

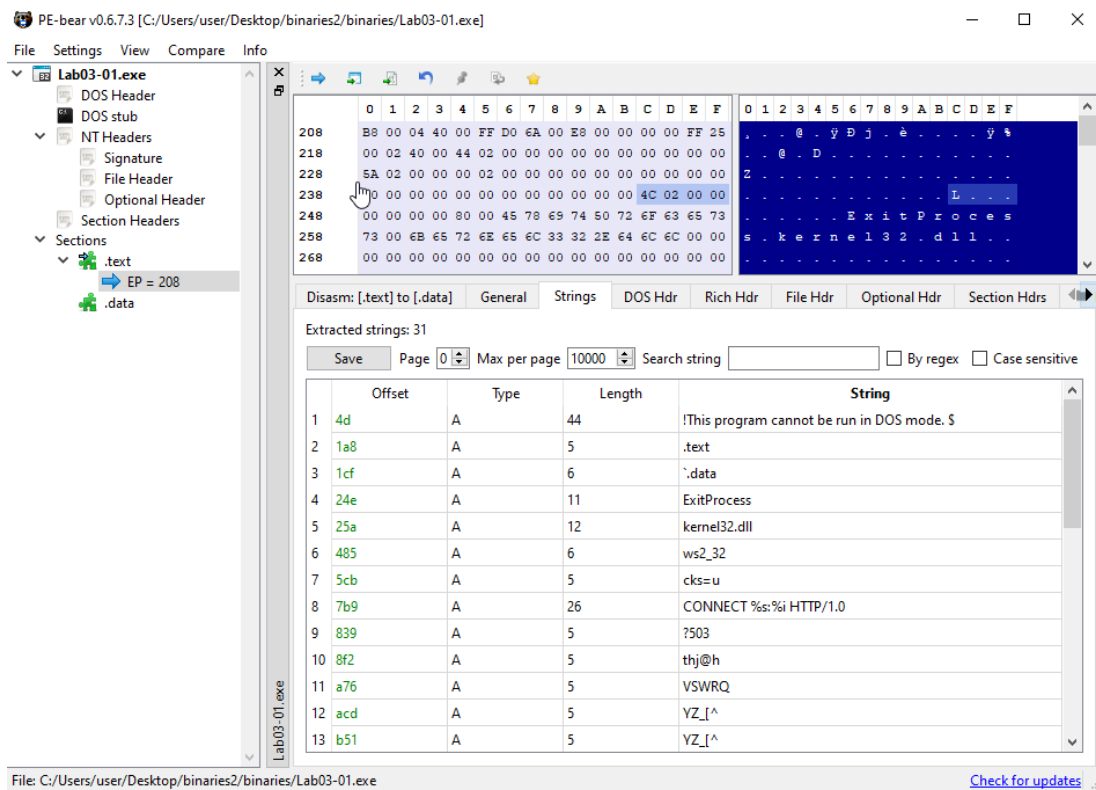


- Podaj wszystkie indykatory hostowe związane z tym programem.
Poniżej widzimy wszystkie indykatory hostowe znalezione w programie pestudio.



3. Czy wśród zebranych informacji znajdują się jakieś pomocne indykatory sieciowe mogące opisać analizowane złośliwe oprogramowanie?

Najciekawszy z nich jest w linii 8-ej dotyczący requestu http.



Laboratorium 3.2

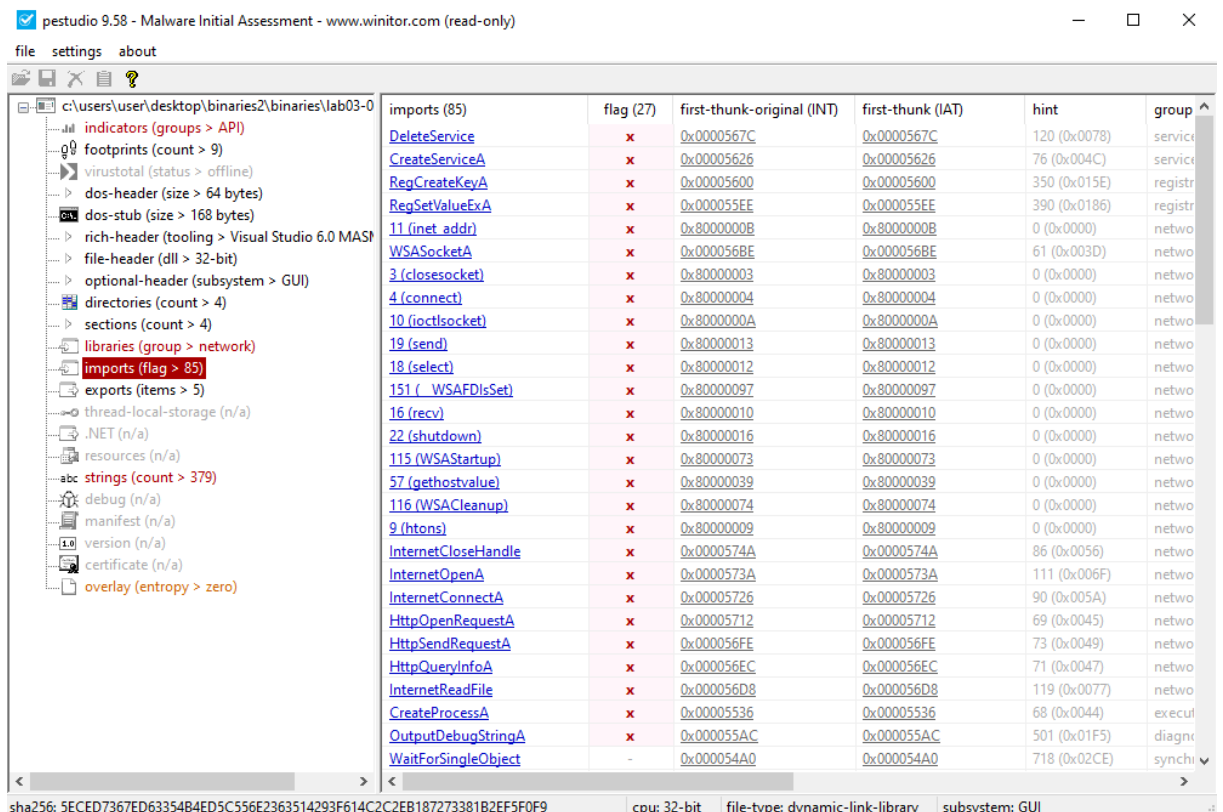
Przeprowadź analizę złośliwego oprogramowania znajdującego się w pliku Lab03-02.dll. Wykorzystaj w tym celu podstawowe narzędzia do analizy dynamicznej. Odpowiedz na poniższe pytania:

1. Wypisz najistotniejsze funkcje analizowanego pliku. Które z nich znajdują się na czarnej liście i dlaczego?

Najistotniejsze funkcje:

- a) DeleteService/CreateService,
- b) RegCreateKeyA – modyfikacja zawartości rejestru,
- c) connect/send/select,
- d) HttpOpenRequest/SendRequest.

Są na czarnej liście, ponieważ stanowią typowe sygnatury plików niebezpiecznych, np. jedna z nich wskazuje na potencjalne wykorzystanie współdzielonej biblioteki do wysłania podejrzanego requestu http.



2. W jaki sposób można zmusić program malware do instalacji?

Biblioteki automatycznie się nie instalują, dlatego trzeba im w tym „pomóc”. Poniżej zdjęcie komendy użytej w cmd.

```
C:\Documents and Settings\user\Desktop\binaries2\binaries>
C:\Documents and Settings\user\Desktop\binaries2\binaries>
C:\Documents and Settings\user\Desktop\binaries2\binaries>
C:\Documents and Settings\user\Desktop\binaries2\binaries>rundll32.exe Lab03-02.dll, Install
C:\Documents and Settings\user\Desktop\binaries2\binaries>_
```

3. W jaki sposób po zainstalowaniu złośliwego oprogramowania można go uruchomić?

Wystarczy włączyć usługi sieciowe w obrębie sieci host-only.

```
C:\Documents and Settings\user\Desktop\binaries2\binaries>net start IPRIP
The Intranet Network Awareness (INA+) service is starting.
The Intranet Network Awareness (INA+) service was started successfully.
```

4. Jak można odszukać proces działający jako złośliwe oprogramowanie?

5. W celu zbierania informacji dotyczących złośliwego oprogramowania możemy wykorzystać program procmon. Jakich filtrów należy użyć, aby zebrać jak najwięcej istotnych informacji?

Odpowiem od razu na oba pytania, bo są one powiązane.

Zanim włączy się malware, warto zresetować przechwytywanie w procmon i włączyć przechwytywanie tuż przed włączeniem próbki. Później jako filtr najprościej jest podać ścieżkę do folderu, w którym znajduje się analizowana biblioteka.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
2:57:20...	cmd.exe	1704	CreateFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: R...
2:57:20...	cmd.exe	1704	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	
2:57:20...	cmd.exe	1704	CreateFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: R...
2:57:20...	cmd.exe	1704	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	
2:57:20...	cmd.exe	1704	QueryOpen	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	CreationTime: 4/13...
2:57:21...	net.exe	268	CreateFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: E...
2:57:21...	net.exe	268	FileSystemControl	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Control: FSCTL_IS...
2:57:21...	net1.exe	280	FileSystemControl	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Control: FSCTL_IS...
2:57:21...	net1.exe	280	FileSystemControl	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Control: FSCTL_IS...
2:57:24...	net.exe	268	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	
3:06:40...	cmd.exe	1704	CreateFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: R...
3:06:40...	cmd.exe	1704	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: R...
3:06:40...	cmd.exe	1704	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	
3:07:39...	Explorer.EXE	1472	QueryOpen	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	CreationTime: 4/13...
3:07:39...	Explorer.EXE	1472	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Filter: binaries, 1: bi...
3:07:39...	Explorer.EXE	1472	CreateFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: G...
3:07:39...	Explorer.EXE	1472	ReadFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	INVALID DEVICE ...	Offset: 0, Length: 24
3:07:39...	Explorer.EXE	1472	QueryInformati...	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	VolumeCreationTim...
3:07:39...	Explorer.EXE	1472	QueryAllInforma...	C:\Documents and Settings\user\Desktop\binaries2\binaries	BUFFER OVERFL...	CreationTime: 4/13...
3:07:39...	Explorer.EXE	1472	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	
3:07:39...	Explorer.EXE	1472	CreateFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: R...
3:07:39...	Explorer.EXE	1472	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	O: ... 1: Lab03-01.e...
3:07:39...	Explorer.EXE	1472	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2\binaries	NO MORE FILES	
3:07:39...	Explorer.EXE	1472	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	
3:07:39...	Explorer.EXE	1472	QueryOpen	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	CreationTime: 4/13...
3:07:39...	Explorer.EXE	1472	CreateFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: R...
3:07:39...	Explorer.EXE	1472	NotifyChangeDi...	C:\Documents and Settings\user\Desktop\binaries2\binaries	NOTIFY CLEANUP	Filter: FILE_NOTIF...
3:07:39...	Explorer.EXE	1472	QueryOpen	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	CreationTime: 4/13...
3:07:39...	Explorer.EXE	1472	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Filter: binaries, 1: bi...
3:07:39...	Explorer.EXE	1472	QueryOpen	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	CreationTime: 4/13...
3:07:39...	Explorer.EXE	1472	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Filter: binaries, 1: bi...
3:07:39...	Explorer.EXE	1472	QueryOpen	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	CreationTime: 4/13...
3:07:39...	Explorer.EXE	1472	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Filter: binaries, 1: bi...
3:07:39...	Explorer.EXE	1472	CreateFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: G...
3:07:39...	Explorer.EXE	1472	ReadFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	INVALID DEVICE ...	Offset: 0, Length: 24
3:07:39...	Explorer.EXE	1472	QueryInformati...	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	VolumeCreationTim...
3:07:39...	Explorer.EXE	1472	QueryAllInforma...	C:\Documents and Settings\user\Desktop\binaries2\binaries	BUFFER OVERFL...	CreationTime: 4/13...
3:07:39...	Explorer.EXE	1472	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	
3:07:43...	Explorer.EXE	1472	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	

Showing 40 of 101,005 events (0.039%) Backed by virtual memory

6. Odszukaj przydatne indykatory sieciowe dla analizowanego pliku.

W wiresharku widać podejrzane requesty korzystające z protokołu SSDP, ponownie widać to, co wcześniej w pestudio: HTTP /1.1.

Capturing from Local Area Connection [Wireshark 1.10.14 (v1.10.14-0-g825f971 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

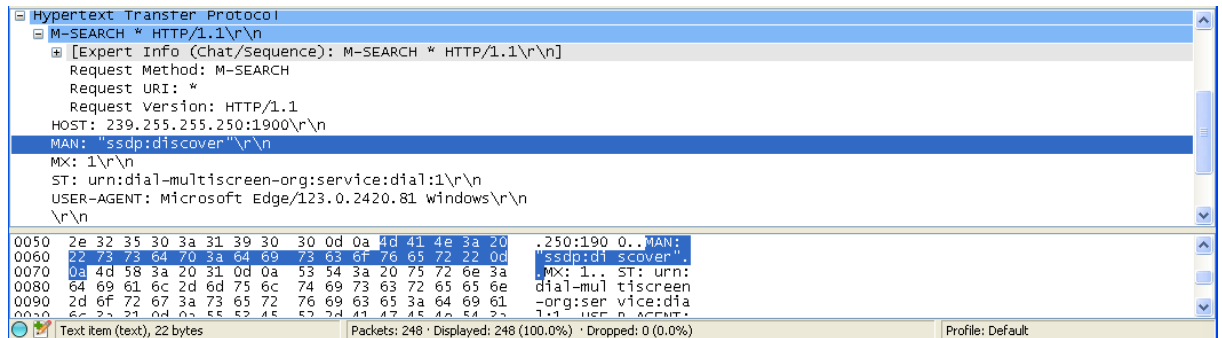
Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2	0.99943200	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3	2.00156500	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4	3.00118000	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5	25.6634530	192.168.56.103	192.168.56.255	BROWSEF	216	Get Backup List Request
6	25.6654910	192.168.56.103	192.168.56.255	NBNS	92	Name query NB WORKGROUP<1b>
7	26.4136220	192.168.56.103	192.168.56.255	NBNS	92	Name query NB WORKGROUP<1b>
8	27.1656390	192.168.56.103	192.168.56.255	NBNS	92	Name query NB WORKGROUP<1b>
9	35.7246070	192.168.56.1	224.0.0.251	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc_tcp.local, "QU" q
10	35.7246270	fe80::d91a:d5d7:267ff02::fb	224.0.0.251	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc_tcp.local, "QU" q
11	36.7253120	192.168.56.1	224.0.0.251	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc_tcp.local, "QM" q
12	36.7253310	fe80::d91a:d5d7:267ff02::fb	224.0.0.251	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc_tcp.local, "QM" q
13	43.7508050	192.168.56.103	192.168.56.255	BROWSEF	258	Domain/workgroup Announcement WORKGROUP, NT Workstation, Dom
14	47.8746790	192.168.56.103	192.168.56.255	BROWSEF	243	Local Master Announcement AGH-5B8E6BDA456, workstation, Serv
15	50.9219710	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16	51.9237010	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
17	52.9246850	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
18	53.9258000	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
19	119.992494	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20	121.002380	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
21	122.003632	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
22	123.004306	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
23	166.375512	192.168.56.103	192.168.56.255	BROWSEF	243	Local Master Announcement AGH-5B8E6BDA456, workstation, Serv
24	170.922656	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

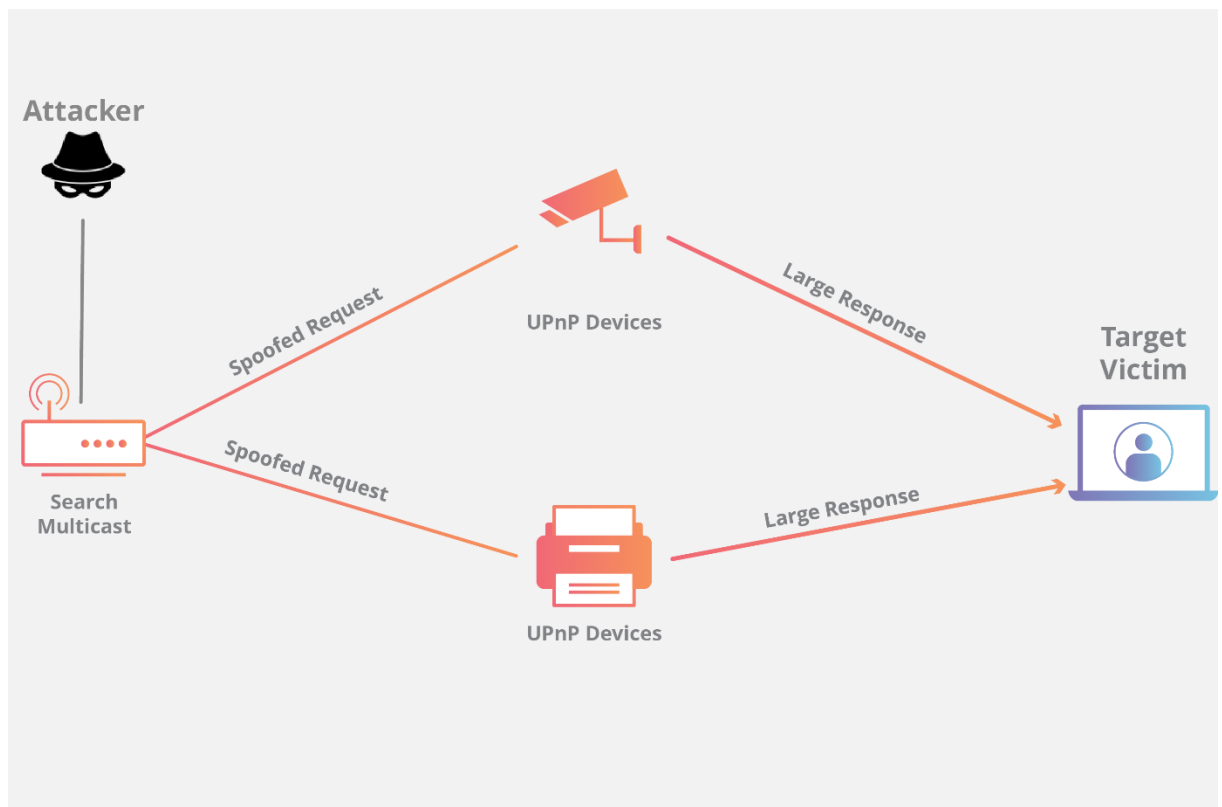
Doczytałem, że atak DDOS wykorzystujący protokół SSDP polega na wysłaniu wielu pakietów „ssdp:discover” z urządzenia ofiary. Później urządzenie ofiary otrzymuje masę odpowiedzi od urządzeń (np. kamery,

drukarki), które konfiguruje się przy pomocy tego protokołu. Duży narzut powoduje oczywiście spowolnienie sieci.

Poniżej pakiet zawierający akcję „ssdp:discover”



Grafika ułatwiająca zrozumienie ataku.



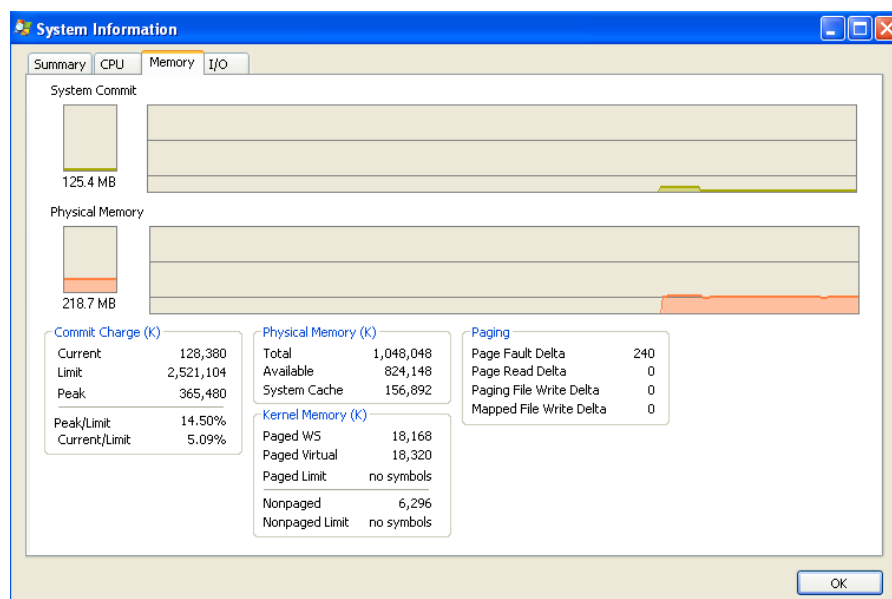
¹ Źródło: <https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack/> [dostęp 13.04.2024r.].

Laboratorium 3.3

Przeprowadź analizę złośliwego oprogramowania znajdującego się w pliku Lab03-03.exe. Wykorzystaj do tego celu podstawowe narzędzia do analizy dynamicznej. Odpowiedz na poniższe pytania:

1. Jakie informacje jesteś w stanie odszukać w trakcie analizy pliku Lab03-03.exe przy pomocy programu Process Explorer?

Program od razu otwiera cmd i wykonuje skrypt. Jest widoczny tylko przez chwilę w procesie eksplorera i znika. Można obserwować ciągłe zapisywanie do pamięci w trakcie działania programu.



2. Odszukaj zachodzące modyfikacje pamięci.

Zacząłem od przetestowania programu regshot, ale tam nie było nic ciekawego.

```

- res -x86 -Notepad
File Edit Format View Help

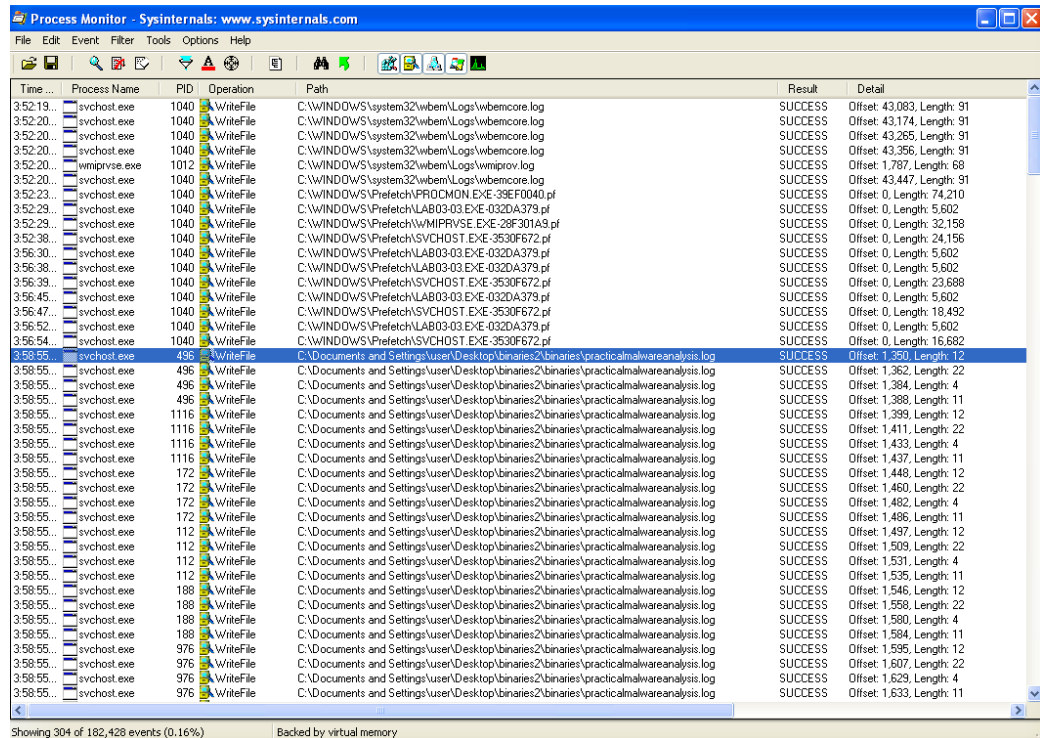
regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2024/4/13 13:44:35 , 2024/4/13 13:45:37
Computer: AGH-SB8E6D4A56 , AGH-SB8E6D4A56
Username: user , user


values modified: 6
-----
HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed: 37 6C 62 56 CB C7 11 03 C1 E2 E7 7A 72 D1 C1 C9 0E 71 6F CB 64 36 E3 2E 1C A0 07
HKU\S-1-5-21-343818398-152049171-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11I
HKU\S-1-5-21-343818398-152049171-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11I
HKU\S-1-5-21-343818398-152049171-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11I
HKU\S-1-5-21-343818398-152049171-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11I
HKU\S-1-5-21-343818398-152049171-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11I
HKU\S-1-5-21-343818398-152049171-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11I
HKU\S-1-5-21-343818398-152049171-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\33\shell\colinfo: 00 00 00 00 00 00
HKU\S-1-5-21-343818398-152049171-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\33\shell\colinfo: 00 00 00 00 00 00
HKU\S-1-5-21-343818398-152049171-1343024091-1003\SessionInformationProgramCount: 0x00000005
HKU\S-1-5-21-343818398-152049171-1343024091-1003\SessionInformationProgramCount: 0x00000004


total changes: 6
-----

```

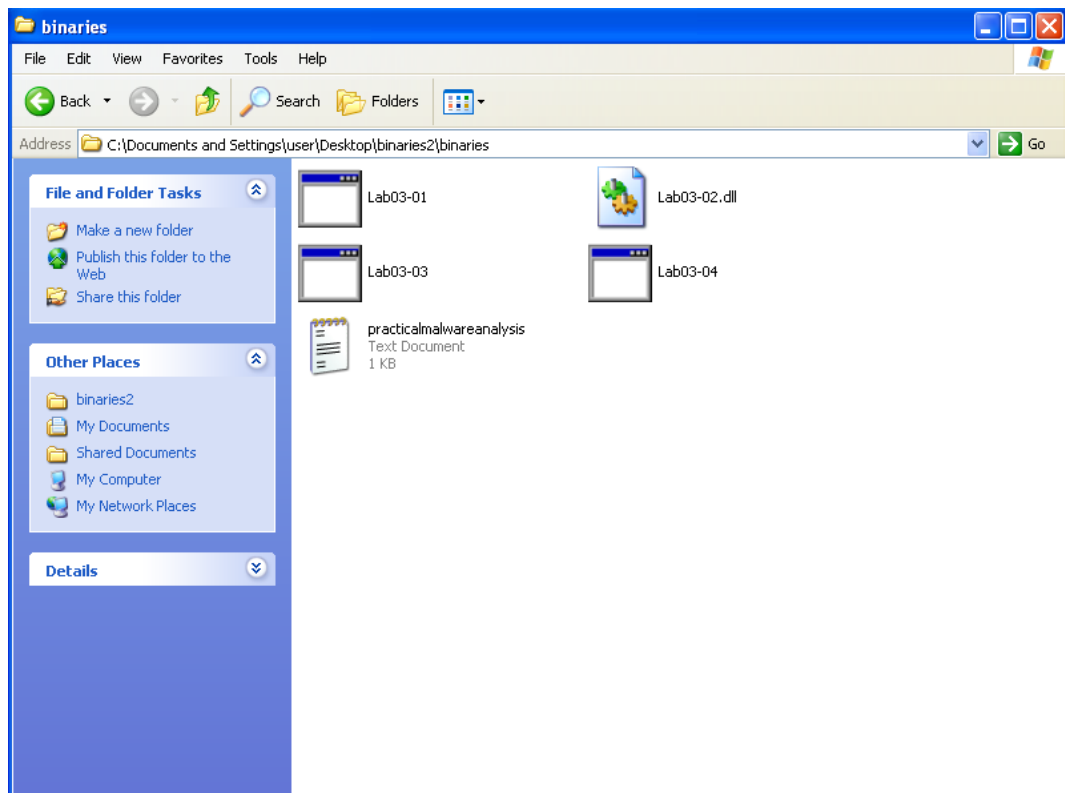

W proces monitor w oczy rzucił mi się plik z logami.



Time ...	Process Name	PID	Operation	Path	Result	Detail
3:52:19...	svchost.exe	1040	WriteFile	C:\WINDOWS\system32\wbem\Logs\wbemcore.log	SUCCESS	Offset: 43,083, Length: 91
3:52:20...	svchost.exe	1040	WriteFile	C:\WINDOWS\system32\wbem\Logs\wbemcore.log	SUCCESS	Offset: 43,174, Length: 91
3:52:20...	svchost.exe	1040	WriteFile	C:\WINDOWS\system32\wbem\Logs\wbemcore.log	SUCCESS	Offset: 43,265, Length: 91
3:52:20...	svchost.exe	1040	WriteFile	C:\WINDOWS\system32\wbem\Logs\wbemcore.log	SUCCESS	Offset: 43,356, Length: 91
3:52:20...	wmiiprse.exe	1012	WriteFile	C:\WINDOWS\system32\wbem\Logs\wmiiprse.log	SUCCESS	Offset: 1,787, Length: 68
3:52:20...	svchost.exe	1040	WriteFile	C:\WINDOWS\system32\wbem\Logs\wbemcore.log	SUCCESS	Offset: 43,447, Length: 91
3:52:23...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\PROCDMON.EXE-39EF0040.pf	SUCCESS	Offset: 0, Length: 74,210
3:52:23...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\LAB03-03.EXE-032DA379.pf	SUCCESS	Offset: 0, Length: 5,602
3:52:23...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\WMIIPRSE.EXE-28F301A3.pf	SUCCESS	Offset: 0, Length: 32,158
3:52:38...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf	SUCCESS	Offset: 0, Length: 24,156
3:56:30...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\LAB03-03.EXE-032DA379.pf	SUCCESS	Offset: 0, Length: 5,602
3:56:38...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\LAB03-03.EXE-032DA379.pf	SUCCESS	Offset: 0, Length: 5,602
3:56:39...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf	SUCCESS	Offset: 0, Length: 23,688
3:56:45...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\LAB03-03.EXE-032DA379.pf	SUCCESS	Offset: 0, Length: 5,602
3:56:47...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf	SUCCESS	Offset: 0, Length: 18,492
3:56:52...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\LAB03-03.EXE-032DA379.pf	SUCCESS	Offset: 0, Length: 5,602
3:56:54...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf	SUCCESS	Offset: 0, Length: 16,682
3:58:55...	svchost.exe	496	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,350, Length: 12
3:58:55...	svchost.exe	496	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,362, Length: 22
3:58:55...	svchost.exe	496	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,384, Length: 4
3:58:55...	svchost.exe	496	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,388, Length: 11
3:58:55...	svchost.exe	1116	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,399, Length: 12
3:58:55...	svchost.exe	1116	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,411, Length: 22
3:58:55...	svchost.exe	1116	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,433, Length: 4
3:58:55...	svchost.exe	1116	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,437, Length: 11
3:58:55...	svchost.exe	172	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,448, Length: 12
3:58:55...	svchost.exe	172	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,460, Length: 22
3:58:55...	svchost.exe	172	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,482, Length: 4
3:58:55...	svchost.exe	172	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,486, Length: 11
3:58:55...	svchost.exe	112	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,497, Length: 12
3:58:55...	svchost.exe	112	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,509, Length: 22
3:58:55...	svchost.exe	112	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,531, Length: 4
3:58:55...	svchost.exe	112	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,535, Length: 11
3:58:55...	svchost.exe	188	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,546, Length: 12
3:58:55...	svchost.exe	188	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,558, Length: 22
3:58:55...	svchost.exe	188	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,580, Length: 4
3:58:55...	svchost.exe	188	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,584, Length: 11
3:58:55...	svchost.exe	976	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,595, Length: 12
3:58:55...	svchost.exe	976	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,607, Length: 22
3:58:55...	svchost.exe	976	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,629, Length: 4
3:58:55...	svchost.exe	976	WriteFile	C:\Documents and Settings\user\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 1,633, Length: 11

Showing 304 of 182,428 events (0.16%) Backed by virtual memory

Od razu podążyłem za jego lokalizacją i zbadałem zawartość.



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
3:38:17...	Lab03-03.exe	1724	Process Start		SUCCESS	Parent PID: 1472, Command line: "C:\Documents and Settings\user\...
3:38:17...	Lab03-03.exe	1724	Thread Create		SUCCESS	Thread ID: 1108
3:38:17...	Lab03-03.exe	1724	QueryNameInfo...	C:\Documents and Settings\user\Desktop\binaries2\binaries\Lab0...	SUCCESS	Name: \Documents and Settings\user\Desktop\binaries2\binaries\...
3:38:17...	Lab03-03.exe	1724	Load Image	C:\Documents and Settings\user\Desktop\binaries2\binaries\Lab0...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
3:38:17...	Lab03-03.exe	1724	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xdaf000
3:38:17...	Lab03-03.exe	1724	QueryNameInfo...	C:\Documents and Settings\user\Desktop\binaries2\binaries\Lab0...	SUCCESS	Name: \Documents and Settings\user\Desktop\binaries2\binaries\...
3:38:17...	Lab03-03.exe	1724	CreateFile	C:\WINDOWS\Prefetch\LAB03-03.EXE-032DA379.pl	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchron...
3:38:17...	Lab03-03.exe	1724	QueryStandard...	C:\WINDOWS\Prefetch\LAB03-03.EXE-032DA379.pl	SUCCESS	AllocationSize: 8,192, EndOfFile: 5,602, NumberOfLinks: 1, Delet...
3:38:17...	Lab03-03.exe	1724	ReadFile	C:\WINDOWS\Prefetch\LAB03-03.EXE-032DA379.pl	SUCCESS	Offset: 0, Length: 5,602
3:38:17...	Lab03-03.exe	1724	CloseFile	C:\WINDOWS\Prefetch\LAB03-03.EXE-032DA379.pl	SUCCESS	
3:38:17...	Lab03-03.exe	1724	CreateFile	C:\	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Dis...
3:38:17...	Lab03-03.exe	1724	QueryInfo...	C:\	SUCCESS	VolumeCreationTime: 3/6/2024 7:52:36 PM, VolumeSerialNumber: ...
3:38:17...	Lab03-03.exe	1724	FileSystemControl...	C:\	SUCCESS	Control: FSCTL_FILE_PREFETCH
3:38:17...	Lab03-03.exe	1724	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\	SUCCESS	0: AUTOEXEC.BAT, 1: boot.ini, 2: CONFIG.SYS, 3: Documents an...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\	NO MORE FILES	
3:38:17...	Lab03-03.exe	1724	CloseFile	C:\	SUCCESS	
3:38:17...	Lab03-03.exe	1724	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: ..., 2: All Users, 3: Default User, 4: LocalService, 5: Networ...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
3:38:17...	Lab03-03.exe	1724	CloseFile	C:\Documents and Settings	SUCCESS	
3:38:17...	Lab03-03.exe	1724	CreateFile	C:\Documents and Settings\user	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings\user	SUCCESS	0: ., 1: ..., 2: Application Data, 3: Cookies, 4: Desktop, 5: Favorites...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings\user	NO MORE FILES	
3:38:17...	Lab03-03.exe	1724	CloseFile	C:\Documents and Settings\user	SUCCESS	
3:38:17...	Lab03-03.exe	1724	CreateFile	C:\Documents and Settings\user\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings\user\Desktop	SUCCESS	0: ., 1: ..., 2: apateDNS.exe, 3: binaries2, 4: binaries2.zip, 5: odbg11...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings\user\Desktop	NO MORE FILES	
3:38:17...	Lab03-03.exe	1724	CloseFile	C:\Documents and Settings\user\Desktop	SUCCESS	
3:38:17...	Lab03-03.exe	1724	CreateFile	C:\Documents and Settings\user\Desktop\BINARIES2	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2	SUCCESS	0: ., 1: ..., 2: binaries
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2	NO MORE FILES	
3:38:17...	Lab03-03.exe	1724	CloseFile	C:\Documents and Settings\user\Desktop\binaries2	SUCCESS	
3:38:17...	Lab03-03.exe	1724	CreateFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	0: ., 1: ..., 2: Lab03-01.exe, 3: Lab03-02.dll, 4: Lab03-03.exe, 5: Lab...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\Documents and Settings\user\Desktop\binaries2\binaries	NO MORE FILES	
3:38:17...	Lab03-03.exe	1724	CloseFile	C:\Documents and Settings\user\Desktop\binaries2\binaries	SUCCESS	
3:38:17...	Lab03-03.exe	1724	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1: ..., 2: 0log, 3: addons, 4: AppPatch, 5: assembly, 6: Blue Lac...
3:38:17...	Lab03-03.exe	1724	QueryDirectory	C:\WINDOWS	NO MORE FILES	
3:38:17...	Lab03-03.exe	1724	CloseFile	C:\WINDOWS	SUCCESS	

Showing 412 of 48,529 events (0.84%)

Backed by virtual memory.

Time	Process	PID	Operation	Path	Result	Offset	Length
4:00:51	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\NOTEPAD.EXE-336351A9.pf	SUCCESS	Offset: 0	Length: 14,960
4:01:57...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\EXPLORER.EXE-082F38A3.pf	SUCCESS	Offset: 0	Length: 15,780
4:02:17...	svchost.exe	1040	WriteFile	C:\WINDOWS\Prefetch\FIREFOX.EXE-28641590.pf	SUCCESS	Offset: 0	Length: 60,728
4:02:19...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Local Settings\Application Data\Mozilla\Firefox\Profiles\afgduu2a.d...	SUCCESS	Offset: 8	Length: 4
4:02:19...	svchost.exe	1040	WriteFile	C:\WINDOWS\system32\wbem\Logs\wbemcore.log	SUCCESS	Offset: 43,538	Length: 91
4:02:19...	wmpiprse.exe	1012	WriteFile	C:\WINDOWS\system32\wbem\Logs\wmpiprov.log	SUCCESS	Offset: 1,930	Length: 68
4:02:20...	svchost.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\cookies...	SUCCESS	Offset: 0	Length: 32
4:02:20...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\cookies...	SUCCESS	Offset: 32	Length: 24
4:02:20...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\cookies...	SUCCESS	Offset: 56	Length: 32,768
4:02:21...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\sessionC...	SUCCESS	Offset: 0	Length: 53
4:02:21...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\sessionC...	SUCCESS	Offset: 0	Length: 90
4:02:21...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\storage...	SUCCESS	Offset: 0	Length: 32
4:02:21...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\storage...	SUCCESS	Offset: 0	Length: 4,096
4:02:21...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\storage...	SUCCESS	Offset: 32	Length: 24
4:02:21...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\storage...	SUCCESS	Offset: 56	Length: 4,096
4:02:21...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\storage...	SUCCESS	Offset: 4,152	Length: 24
4:02:21...	firefox.exe	428	WriteFile	C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Profiles\afgduu2a.default\storage...	SUCCESS	Offset: 4,176	Length: 4,096
4:02:21...	svchost.exe	1040	WriteFile	C:\WINDOWS\system32\wbem\Logs\wbemcore.log	SUCCESS	Offset: 43,629	Length: 91
4:02:22...	svchost.exe	1040	WriteFile	C:\WINDOWS\system32\wbem\Logs\wbemcore.log	SUCCESS	Offset: 43,720	Length: 91
4:02:22...	svchost.exe	496	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,662	Length: 12
4:02:22...	svchost.exe	496	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,674	Length: 44
4:02:22...	svchost.exe	496	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,718	Length: 4
4:02:22...	svchost.exe	1116	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,722	Length: 12
4:02:22...	svchost.exe	1116	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,734	Length: 44
4:02:22...	svchost.exe	1116	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,778	Length: 4
4:02:22...	svchost.exe	1172	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,782	Length: 12
4:02:22...	svchost.exe	172	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,794	Length: 44
4:02:22...	svchost.exe	172	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,838	Length: 44
4:02:22...	svchost.exe	112	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,842	Length: 12
4:02:22...	svchost.exe	112	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,854	Length: 44
4:02:22...	svchost.exe	112	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,898	Length: 4
4:02:22...	svchost.exe	188	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,902	Length: 12
4:02:22...	svchost.exe	188	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,914	Length: 44
4:02:22...	svchost.exe	188	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,958	Length: 4
4:02:22...	svchost.exe	976	WriteFile	C:\Documents and Settings\User\Desktop\binaries2\binaries\practicalmalwareanalysis.log	SUCCESS	Offset: 2,962	Length: 12

Showing 610 of 231,926 events (0.26%)
Backed by virtual memory

```
[window: Search Results]
assssssdddddadaaaaaawwwwwwdoddoddaaaaasssssssdoddoddaaaaasssssssdoddodo [ENTER] o [ENTER] o [ENTER] o [ENTER] o [ENTER]
[window: Mozilla Firefox Start Page - Mozilla Firefox]

[window: Mozilla Firefox Start Page - Mozilla Firefox]

[window: Mozilla Firefox Start Page - Mozilla Firefox]

[window: Mozilla Firefox Start Page - Mozilla Firefox]

[window: Mozilla Firefox Start Page - Mozilla Firefox]

[window: Mozilla Firefox Start Page - Mozilla Firefox]

[window: Mozilla Firefox Start Page - Mozilla Firefox]

[window: Mozilla Firefox Start Page - Mozilla Firefox]
[TAB] [TAB] [TAB] [TAB] [TAB] [TAB] [CAPS LOCK] [CAPS LOCK] [CAPS LOCK] [CAPS LOCK] [CAPS LOCK] [CAPS LOCK]
```

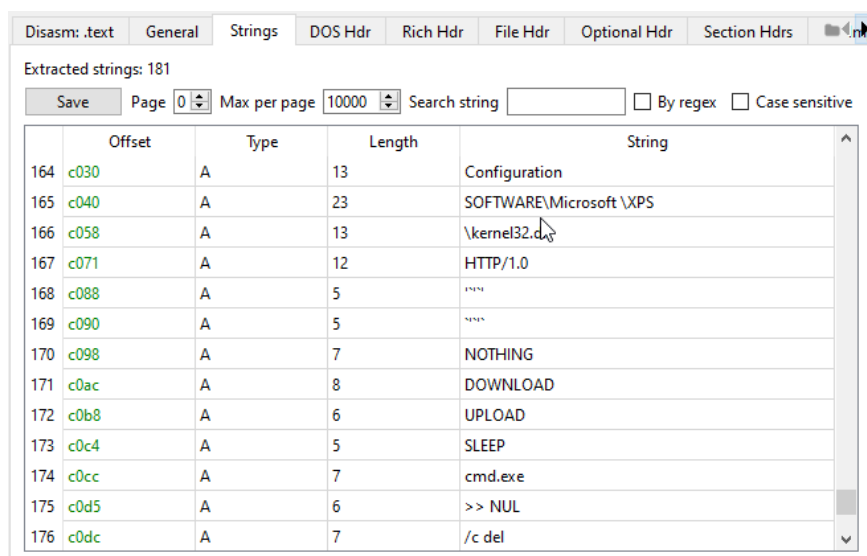
```
[window: Mozilla Firefox Start Page - Mozilla Firefox]
[TAB][TAB][TAB][TAB][TAB][TAB][TAB][CAPS LOCK][CAPS LOCK][CAPS LOCK][CAPS LOCK][CAPS LOCK][CAPS LOCK][CAPS LOCK][CAPS LOCK]
BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE
[window: Problem loading page - Mozilla Firefox]
f
[window: Problem loading page - Mozilla Firefox]
f
[window: Problem loading page - Mozilla Firefox]
f
[window: Problem loading page - Mozilla Firefox]
f
[window: Problem loading page - Mozilla Firefox]
f
[window: Problem loading page - Mozilla Firefox]
f
[window: Problem loading page - Mozilla Firefox]
faaaaaaaaaccccccceeeeeeeebbbbbbbooooooooooooooookkkkkkkccccccccooooooooommmmmmmmm[ENTER] [ENTER] [ENTER] [ENTER] [ENTER] [ENTER]
```

Laboratorium 3.4

Przeprowadź analizę złośliwego oprogramowania znajdującego się w pliku Lab03-04.exe. Wykorzystaj do tego celu podstawowe narzędzia do analizy dynamicznej. Odpowiedz na poniższe pytania:

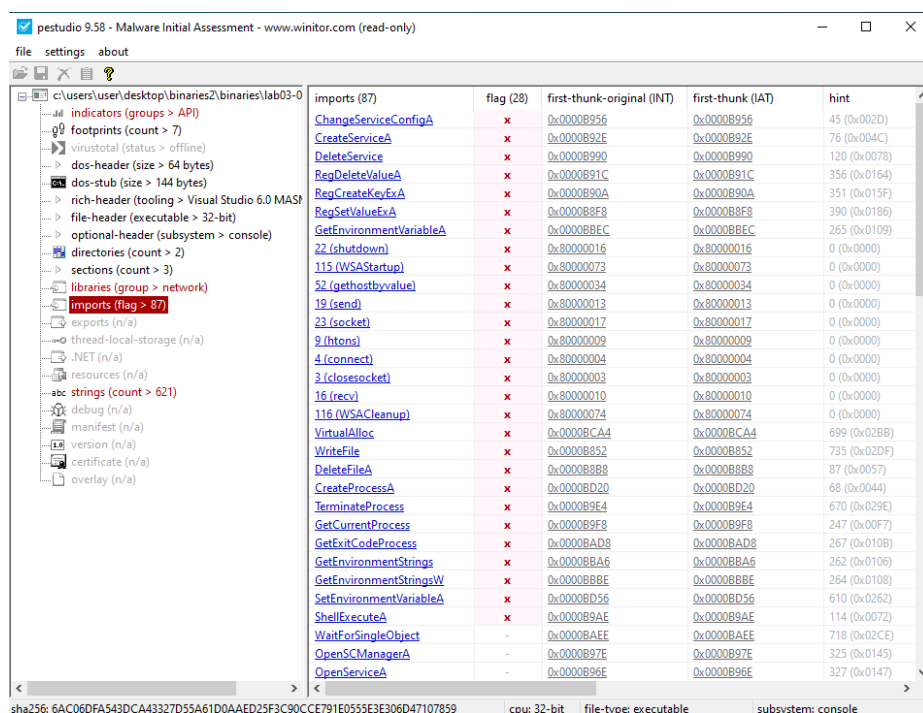
1. Zbadaj strukturę PE oraz łańcuchy pliku Lab03-04.exe. Czy plik zawiera „ciekawe” informacje?

Zanotowałem najdziwniejsze na pierwszy rzut oka łańcuchy i sygnatury.



	Offset	Type	Length	String
164	c030	A	13	Configuration
165	c040	A	23	SOFTWARE\Microsoft \XPS
166	c058	A	13	\kernel32.d
167	c071	A	12	HTTP/1.0
168	c088	A	5	
169	c090	A	5	
170	c098	A	7	NOTHING
171	c0ac	A	8	DOWNLOAD
172	c0b8	A	6	UPLOAD
173	c0c4	A	5	SLEEP
174	c0cc	A	7	cmd.exe
175	c0d5	A	6	>> NUL
176	c0dc	A	7	/c del

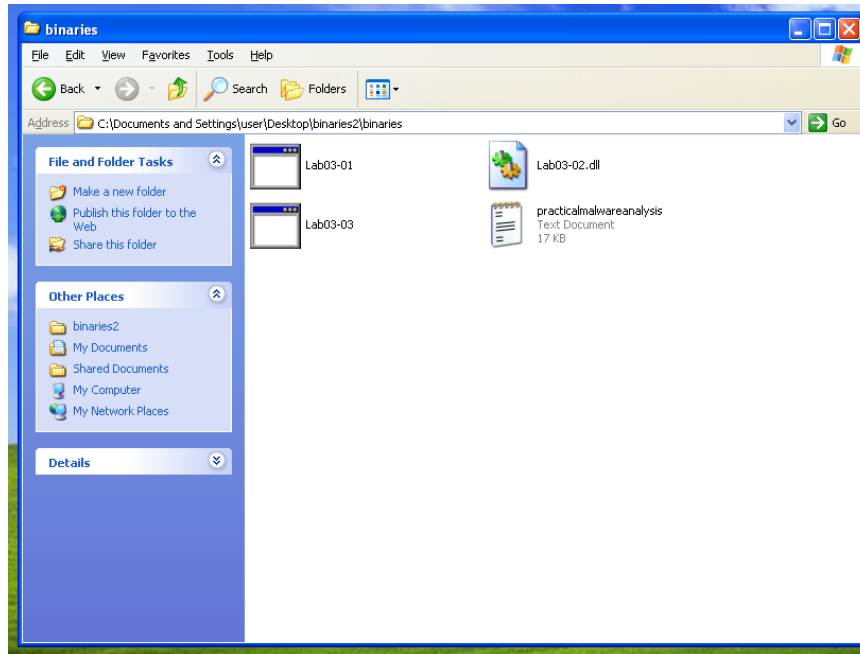
Przejrzałem również importy.



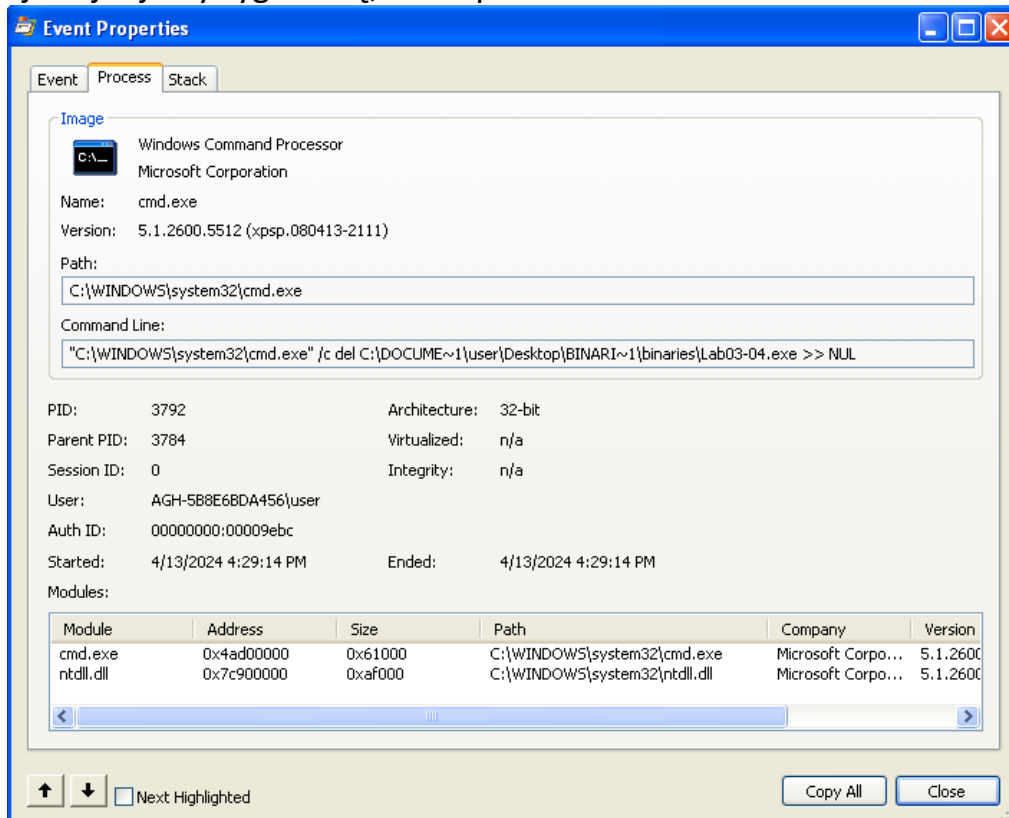
imports (87)	flag (28)	first-thunk-original (INT)	first-thunk (IAT)	hint
ChangeServiceConfigA	x	0x0000B956	0x0000B956	45 (0x002D)
CreateServiceA	x	0x0000B92E	0x0000B92E	76 (0x004C)
DeleteService	x	0x0000B990	0x0000B990	120 (0x0078)
RegDeleteValueA	x	0x0000B91C	0x0000B91C	356 (0x0164)
RegCreateKeyExA	x	0x0000B90A	0x0000B90A	351 (0x015F)
RegSetValueExA	x	0x0000B8F8	0x0000B8F8	390 (0x0186)
GetEnvironmentVariableA	x	0x0000B8EC	0x0000B8EC	265 (0x0109)
22 (shutdown)	x	0x80000016	0x80000016	0 (0x0000)
115 (WSAStartup)	x	0x80000073	0x80000073	0 (0x0000)
52 (gethostbyname)	x	0x80000034	0x80000034	0 (0x0000)
19 (send)	x	0x80000013	0x80000013	0 (0x0000)
23 (socket)	x	0x80000017	0x80000017	0 (0x0000)
9 (htons)	x	0x80000009	0x80000009	0 (0x0000)
4 (connect)	x	0x80000004	0x80000004	0 (0x0000)
3 (closesocket)	x	0x80000003	0x80000003	0 (0x0000)
16 (recv)	x	0x80000010	0x80000010	0 (0x0000)
116 (WSACleanup)	x	0x80000074	0x80000074	0 (0x0000)
VirtualAlloc	x	0x0000BCA4	0x0000BCA4	699 (0x02BB)
WriteFile	x	0x0000B852	0x0000B852	735 (0x02DF)
DeleteFileA	x	0x0000B8B8	0x0000B8B8	87 (0x0057)
CreateProcessA	x	0x0000BD20	0x0000BD20	68 (0x0044)
TerminateProcess	x	0x0000B9E4	0x0000B9E4	670 (0x029E)
GetCurrentProcess	x	0x0000B9F8	0x0000B9F8	247 (0x00F7)
GetExitCodeProcess	x	0x0000BAD8	0x0000BAD8	267 (0x010B)
GetEnvironmentStrings	x	0x0000BBA6	0x0000BBA6	262 (0x0106)
GetEnvironmentStringsW	x	0x0000BBBE	0x0000BBBE	264 (0x0108)
SetEnvironmentVariableA	x	0x0000BD56	0x0000BD56	610 (0x0262)
ShellExecuteA	x	0x0000B9AE	0x0000B9AE	114 (0x0072)
WaitForSingleObject	-	0x0000BAEE	0x0000BAEE	718 (0x02CE)
OpenSCManagerA	-	0x0000B97E	0x0000B97E	325 (0x0145)
OpenServiceA	-	0x0000B96E	0x0000B96E	327 (0x0147)

2. Opisz zdarzenia towarzyszące uruchomieniu tego pliku.

Po uruchomieniu pliku tworzy się proces, otwiera się cmd i szybko zamyka. Co ciekawe z oryginalnej lokalizacji znika plik wykonywalny. Na pierwszy rzut oka dziwne, ale to prawdopodobnie mechanizm utrudniający analizę.



Tutaj znajdujemy sygnaturę, która potwierdza to zachowanie.



3. Co powoduje blokadę analizy dynamicznej?

Prawdopodobnie jakiś mechanizm ochronny. Być może oparty na strefie czasowej, lokalizacji, a może na wykrywaniu środowiska systemowego (wykrywanie maszyn wirtualnych).

4. W jaki sposób można uruchomić ten program?

Trzeba skorzystać z techniki lub programu, który nie doprowadzi do zamknięcia próbki. Dobrym rozwiązaniem mogłyby być programy do deasemblacji. Może tam dałoby się znaleźć odpowiedź na pytanie, jaki mechanizm powoduje problemy i jak ewentualnie można je obejść.