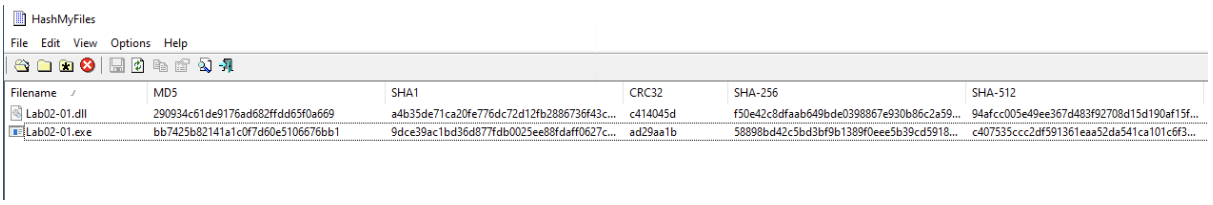
Podstawy Analizy Statycznej

Analiza Malware - Sebastian Knap

Zadanie 1.1 Lab02-01.exe i Lab02-01.dll

1. Analiza sum kontrolnych, sygnatur plików



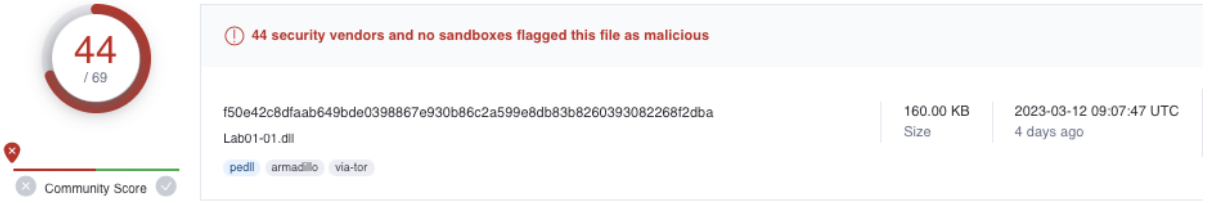
Filename	MD5	SHA1	CRC32	SHA-256	SHA-512
Lab02-01.dll	290934c61de9176ad682ffdd65f0a669	a4b35de71ca20fe776dc72d12fb2886736f43c...	c414045d	f50e42c8dfaab649bde0398867e930b86c2a59...	94afcc005e49ee367d483f92708d15d190af15f...
Lab02-01.exe	bb7425b82141a1c0f7d60e5106676bb1	9dce39ac1bd36d877fdb0025ee88fdaff0627c...	ad29aa1b	58898bd42c5bd3bf9b1389f0eee5b39cd5918...	c407535ccc2df591361eaa52da541ca101c6f3...

Plik: Lab02-01.dll

MD5: 290934c61de9176ad682ffdd65f0a669

SHA1: a4b35de71ca20fe776dc72d12fb2886736f43c22

SHA256: f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

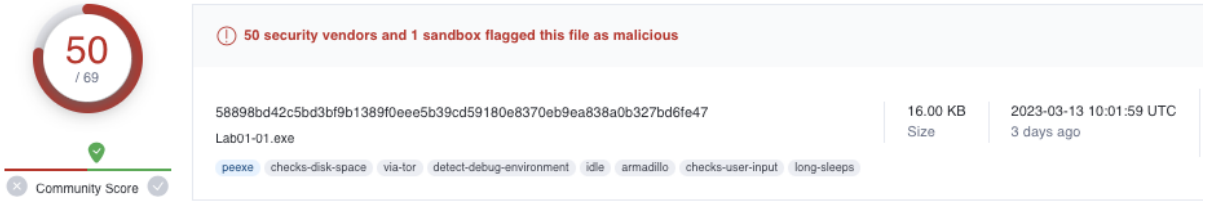


Plik: Lab02-01.exe

MD5: bb7425b82141a1c0f7d60e5106676bb1

SHA1: 9dce39ac1bd36d877fdb0025ee88fdaff0627cdb

SHA256: 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47



50 / 69

Community Score

50 security vendors and 1 sandbox flagged this file as malicious

58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Lab01-01.exe
peexe checks-disk-space via-tor detect-debug-environment idle armadillo checks-user-input long-sleeps

16.00 KB Size | 2023-03-13 10:01:59 UTC 3 days ago | EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30 +

Popular threat label: trojan.ulise/aenjaris | Threat categories: trojan | Family labels: ulise aenjaris r002c0dcd2

Security vendors' analysis — Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.C957604	Alibaba	Trojan:Win32/Aenjaris.2be74...
ALYac	Trojan.Agent.16384SS	Antiy-AVL	Trojan/Win32.TSGeneric
Arcabit	Trojan.Ulise.D1BC1E	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	HEUR/AGEN.1223661
BitDefender	Gen:Variant.Ulise.113694	ClamAV	Win.Malware.Agent-6342616-0
CrowdStrike Falcon	Win/malicious_confidence_1...	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Ulise.CK.gen!Eldorado
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Ulise.113694 (B)
eScan	Gen:Variant.Ulise.113694	ESET-NOD32	A Variant Of Win32/Agent.W...
Fortinet	W32/Agent.WOM!tr	GData	Gen:Variant.Ulise.113694
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.oa!s1
Ikarus	Trojan.SuspectCRC	Jiangmin	Trojan.Ulise.cr
K7AntiVirus	Trojan (004b6b551)	K7GW	Trojan (004b6b551)
Lionic	Trojan.Win32.Ulise.4!c	MAX	Malware (ai Score=100)
MaxSecure	Trojan.Malware.7164915.sus...	McAfee	GenericRXAA-AA!BB7425B...
McAfee-GW-Edition	BehavesLike.Win32.Worm.lz	Microsoft	Trojan:Win32/Aenjaris.CT!bit
NANO-Antivirus	Trojan.Win32.Generic.fhvmhd	Palo Alto Networks	Generic.ml
Rising	Trojan.Agent!8.B1E (TFE:5:...	Sangfor Engine Zero	Trojan.Win32.Aenjaris.V9fe
SecureAge	Malicious	Symantec	Trojan.Gen.2
Tencent	Malware.Win32.Gencirc.10b...	Trellix (FireEye)	Gen:Variant.Ulise.113694
TrendMicro	TROJ_GEN.R002C0DID20	TrendMicro-HouseCall	TROJ_GEN.R002C0DID20
VBA32	Trojan.Tiggre	VIPRE	Gen:Variant.Ulise.113694
VirIT	Trojan.Win32.Agent5.CDE	ViRobot	Trojan.Win32.Z.Agent.16384...
Webroot	W32.Malware.Gen	Xcitium	Malware@#3eb40r99afetz
Yandex	Trojan.GenAsa!cGc9XwKYsAs	Zillya	Downloader.Amonetize.Win3...
Acronis (Static ML)	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
CMC	Undetected	DrWeb	Undetected
F-Secure	Undetected	Kaspersky	Undetected
Malwarebytes	Undetected	Panda	Undetected
QuickHeal	Undetected	SentinelOne (Static ML)	Undetected
Sophos	Undetected	SUPERAntiSpyware	Undetected
TACHYON	Undetected	TEHTRIS	Undetected
Trapmine	Undetected	ZoneAlarm by Check Point	Undetected
Zoner	Undetected	Avast-Mobile	Unable to process file type

44 / 69

Community Score

44 security vendors and no sandboxes flagged this file as malicious

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Lab01-01.dll
pedll armadillo via-tor

160.00 KB Size | 2023-03-12 09:07:47 UTC 4 days ago | DLL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30 +

Popular threat label: trojan.ulise/skeeyah | Threat categories: trojan | Family labels: ulise skeeyah waski

Security vendors' analysis — Do you want to automate checks?

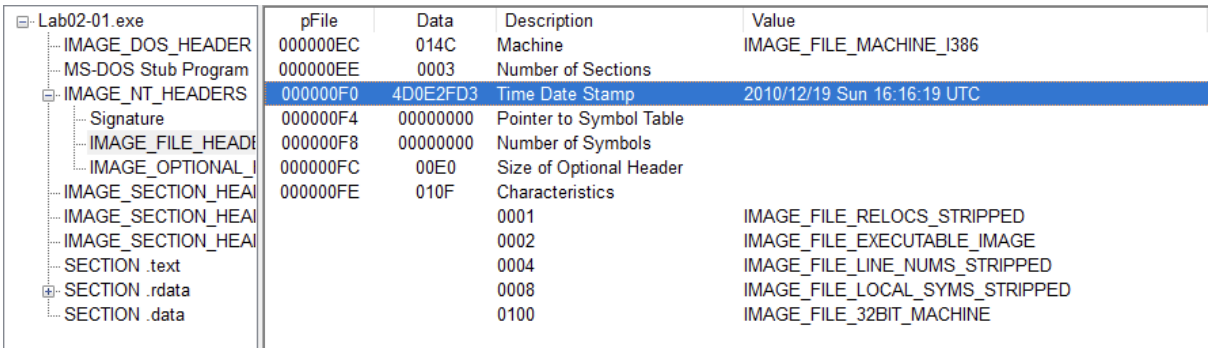
Alibaba	Trojan:Win32/Skeeyah.7fb0e...	ALYac	Trojan.Agent.Waski
Antiy-AVL	Trojan/Win32.BTSGeneric	Arcabit	Trojan.Ulise.D19D44
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
BitDefender	Gen:Variant.Ulise.105796	BitDefenderTheta	Gen:NN.ZedlaF.36308.kq4@...
ClamAV	Win.Malware.Agent-6369668-0	CrowdStrike Falcon	Win/malicious_confidence_1...
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Skeeyah.AK.gen!Eldor...	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Ulise.105796 (B)	eScan	Gen:Variant.Ulise.105796
ESET-NOD32	A Variant Of Generik.TGEWDD	GData	Gen:Variant.Ulise.105796
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.dg
Ikarus	Trojan.SuspectCRC	Lionic	Trojan.Win32.Generic.4!c
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.7164915.sus...
McAfee	GenericRXFO-RT!290934C6...	McAfee-GW-Edition	GenericRXFO-RT!290934C6...
Microsoft	Trojan:Win32/Skeeyah.A!MTB	NANO-Antivirus	Trojan.Win32.Waski.dfkvsp
Palo Alto Networks	Generic.ml	Rising	Trojan.Generic@AI.82 (RDM...
Sangfor Engine Zero	Trojan.Win32.Skeeyah.Vq32	SecureAge	Malicious
Sophos	Mal/Generic-R	Symantec	ML.Attribute.HighConfidence
Trapmine	Malicious.high.ml.score	Trellix (FireEye)	Generic.mg.290934c61de91...
TrendMicro	TROJ_GEN.R002C0PHF20	TrendMicro-HouseCall	TROJ_GEN.R002C0PHF20
VIPRE	Gen:Variant.Ulise.105796	VirIT	Trojan.Win32.X-Paxxess2_c...
Webroot	W32.Gen.BT	Xcitium	Malware@#2dsw4albnce61
Yandex	Trojan.GenAsa!HoPrb0Qvul0	Zillya	Adware.InstallCore.Win32.1...
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
Bkav Pro	Undetected	CMC	Undetected
DrWeb	Undetected	F-Secure	Undetected
Fortinet	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kaspersky	Undetected	Malwarebytes	Undetected
Panda	Undetected	QuickHeal	Undetected
SentinelOne (Static ML)	Undetected	SUPERAntiSpyware	Undetected
TACHYON	Undetected	TEHTRIS	Undetected
Tencent	Undetected	VBA32	Undetected
ViRobot	Undetected	ZoneAlarm by Check Point	Undetected
Zoner	Undetected	Avast-Mobile	Unable to process file type

Sumy kontrolne obu plików były już wcześniej poddawane analizie pod kątem szkodliwego oprogramowania, zostały uznane przez “security vendors” za złośliwe oprogramowanie.

50/69 oraz 44/69

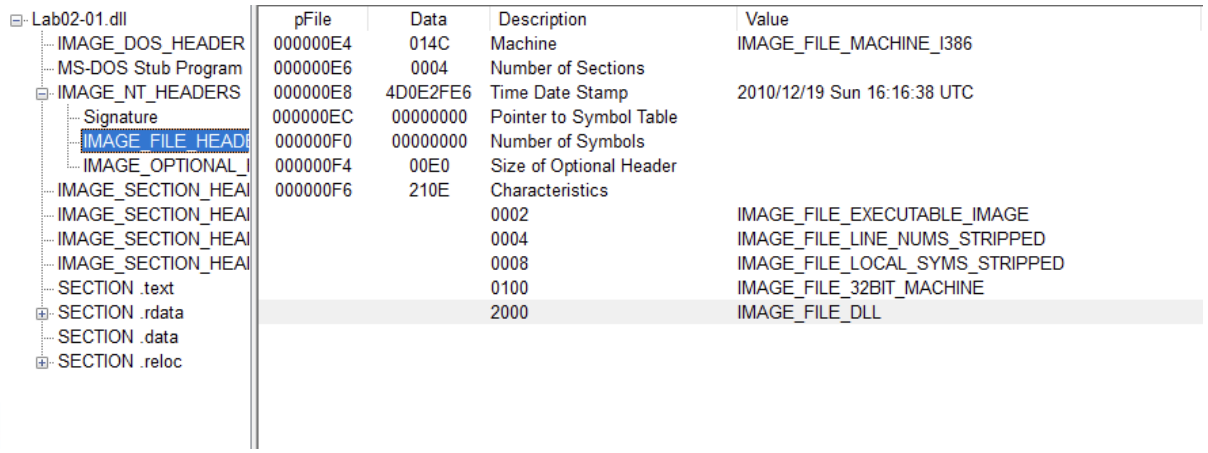
2. Daty kompilacji:

Plik: Lab02-01..exe



pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0003	Number of Sections	
000000F0	4D0E2FD3	Time Date Stamp	2010/12/19 Sun 16:16:19 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

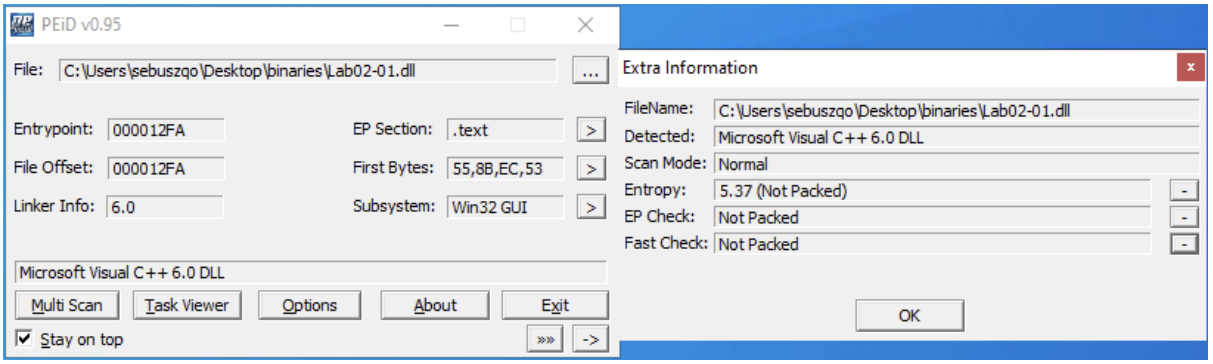
Plik: Lab02-01.dll



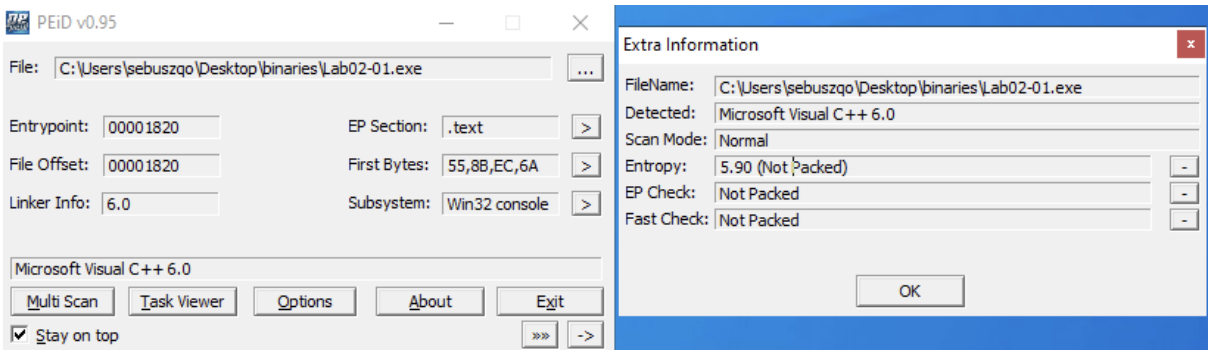
pFile	Data	Description	Value
000000E4	014C	Machine	IMAGE_FILE_MACHINE_I386
000000E6	0004	Number of Sections	
000000E8	4D0E2FE6	Time Date Stamp	2010/12/19 Sun 16:16:38 UTC
000000EC	00000000	Pointer to Symbol Table	
000000F0	00000000	Number of Symbols	
000000F4	00E0	Size of Optional Header	
000000F6	210E	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE
		2000	IMAGE_FILE_DLL

3. Narzędzie PEiD wskazało, że pliki nie są spakowane.

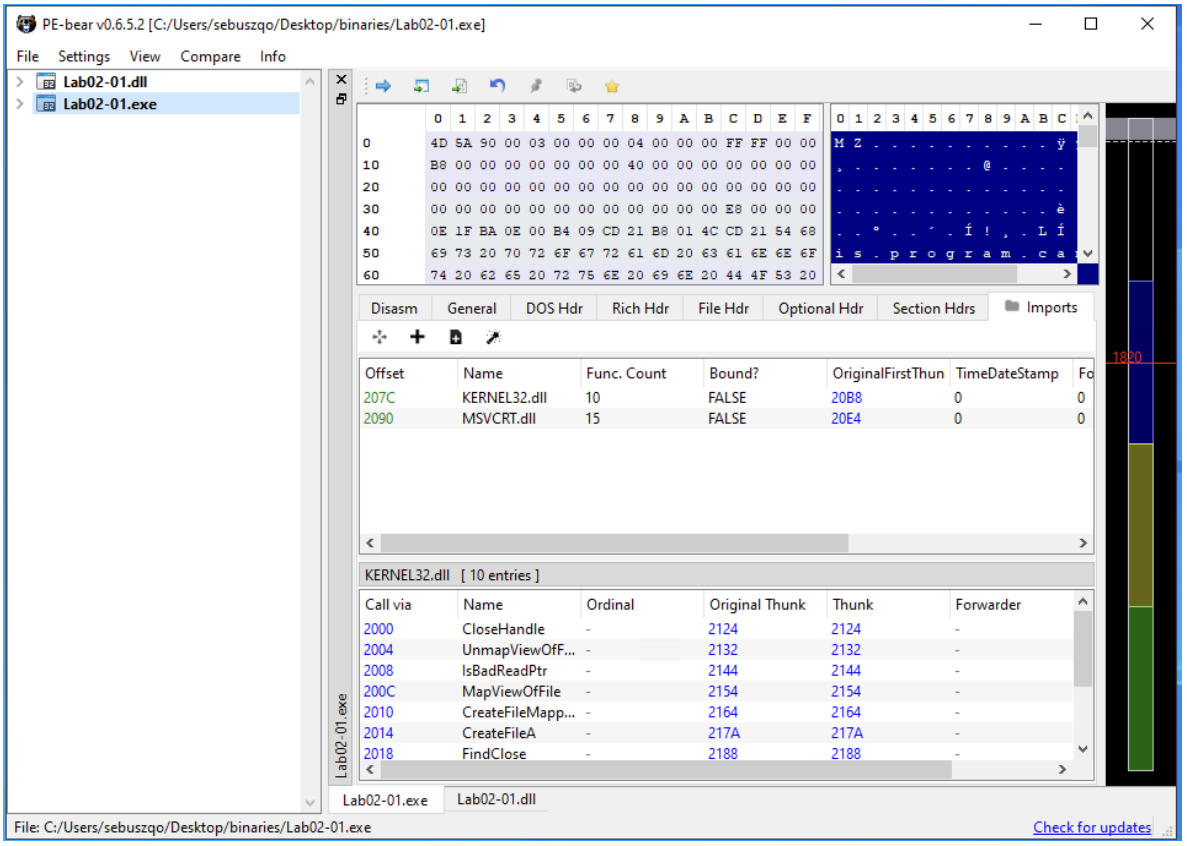
.dll:



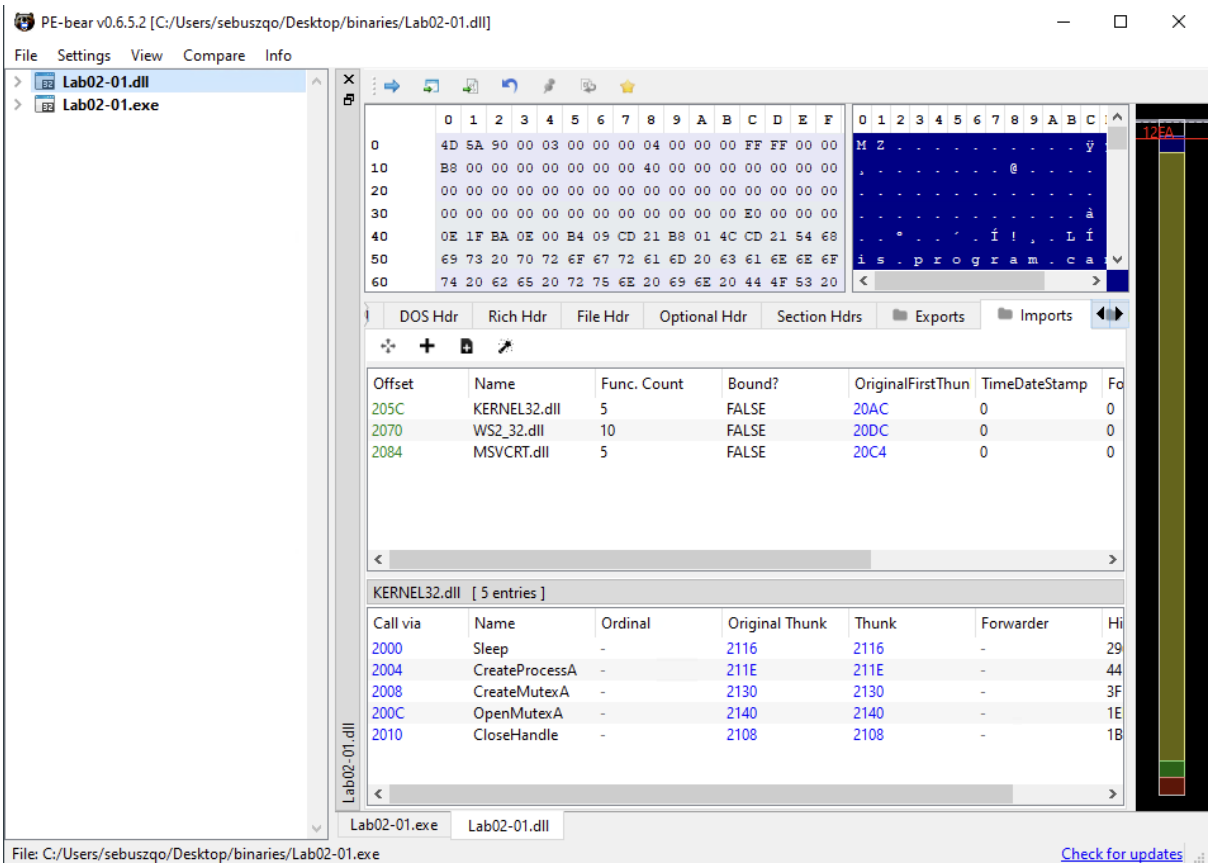
.exe:


PEiD v0.95
File: C:\Users\sebuszqo\Desktop\binaries\Lab02-01.exe
Entrypoint: 00001820
EP Section: .text
File Offset: 00001820
First Bytes: 55,8B,EC,6A
Linker Info: 6.0
Subsystem: Win32 console
Microsoft Visual C++ 6.0
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
Extra Information
FileName: C:\Users\sebuszqo\Desktop\binaries\Lab02-01.exe
Detected: Microsoft Visual C++ 6.0
Scan Mode: Normal
Entropy: 5.90 (Not Packed)
EP Check: Not Packed
Fast Check: Not Packed
OK

4. .exe:


PE-bear v0.6.5.2 [C:/Users/sebuszqo/Desktop/binaries/Lab02-01.exe]
File Settings View Compare Info
Lab02-01.dll
Lab02-01.exe
Disasm General DOS Hdr Rich Hdr File Hdr Optional Hdr Section Hdrs Imports
Offset Name Func. Count Bound? OriginalFirstThun TimeDateStamp
207C KERNEL32.dll 10 FALSE 20B8 0
2090 MSVCRT.dll 15 FALSE 20E4 0
KERNEL32.dll [10 entries]
Call via Name Ordinal Original Thunk Thunk Forwarder
2000 CloseHandle 2124 2124
2004 UnmapViewOfF... 2132 2132
2008 IsBadReadPtr 2144 2144
200C MapViewOfFile 2154 2154
2010 CreateFileMapp... 2164 2164
2014 CreateFileA 217A 217A
2018 FindClose 2188 2188
Lab02-01.exe
Lab02-01.dll
File: C:/Users/sebuszqo/Desktop/binaries/Lab02-01.exe
Check for updates

.dll:



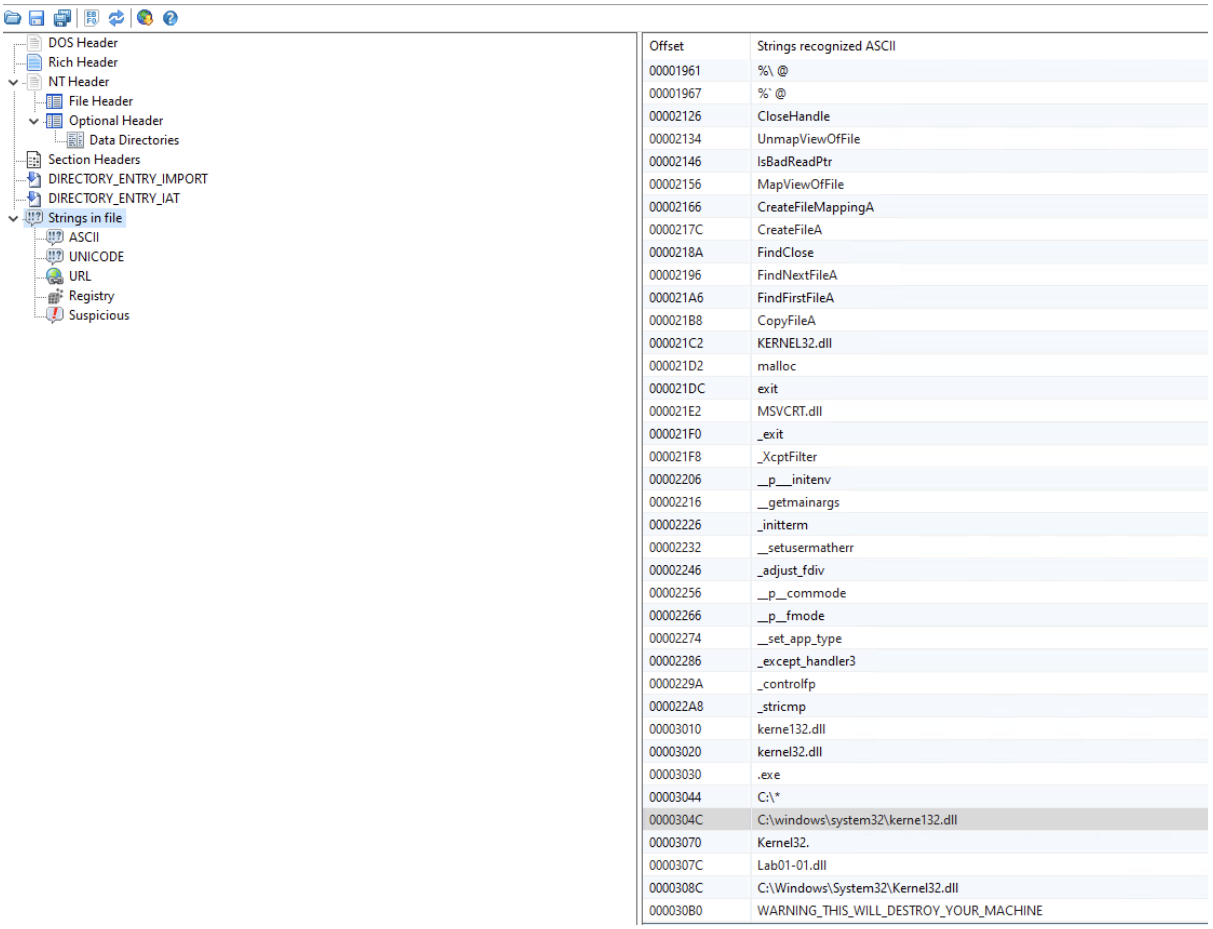
Warto zwrócić uwagę na importy z biblioteki **KERNEL32.dll**

1. **CreateFileA:** Funkcja ta tworzy lub otwiera plik i zwraca wskaźnik który może być używany do odczytu, zapisu i innych operacji wykonywanych na pliku. Funkcja ta jest używana w programowaniu systemowym w języku C i C++.
2. **CopyFileA:** Funkcja ta kopiuje istniejący plik do nowej lokalizacji i zwraca wartość logiczną, czy operacja kopiowania się powiodła czy nie. Funkcja ta jest używana w programowaniu systemowym w języku C i C++.
3. **CreateProcessA:** Funkcja ta tworzy nowy proces i zwraca wskaźnik do tego procesu, który może być używany do kontroli i komunikacji z nowo utworzonym procesem. Funkcja ta jest używana w programowaniu systemowym w języku C i C++.
4. **Sleep:** Funkcja ta zawiesza wykonywanie bieżącego wątku na określony czas (w milisekundach). Funkcja ta jest używana do opóźnienia działania programu, na przykład w celu symulowania procesów czasochłonnych lub do czasowego wstrzymania działania programu. Funkcja ta jest dostępna w języku C i C++.

5. Za co odpowiedzialna jest biblioteka WS2_32.dll (Lab02-01.dll)?

Biblioteka WS2_32.dll jest odpowiedzialna za obsługę gniazd sieciowych w systemie Windows. Jest to biblioteka dynamiczna (DLL), która udostępnia zestaw funkcji programistycznych do tworzenia, konfigurowania i zarządzania połączeniami sieciowymi, w tym protokołami takimi jak TCP/IP i UDP.

6.



0000304C	C:\windows\system32\kerne132.dll
00003070	Kernel32.
0000307C	Lab01-01.dll
0000308C	C:\Windows\System32\Kernel32.dll
000030B0	WARNING_THIS_WILL_DESTROY_YOUR_MACHINE

Dwa podobne rekordy mogą świadczyć o próbie ukrycia prawdziwej biblioteki "Kernel32.dll" poprzez zmianę jej nazwy na "kerne132.dll". Jest to częsty sposób, w jaki złośliwe oprogramowanie próbuje ukryć swoją aktywność przed systemem operacyjnym i programami antywirusowymi. Podmiana nazwy na podobną, ale z odmienną literą, może zmylić programy antywirusowe i uniemożliwić im wykrycie podejrzanych działań.

W przypadku podmiany nazwy pliku Kernel32.dll na kerne132.dll, program złośliwy może próbować wykorzystać zmodyfikowaną bibliotekę do wykonywania swojego kodu, jednocześnie udając, że korzysta z oryginalnej biblioteki Kernel32.dll.

7. Biblioteka zawiera adres IP na kóry prawdopodobnie została przypuszczona próba połączenia.

00026020	hello
00026028	127.26.152.13
00026038	SADFHUHF

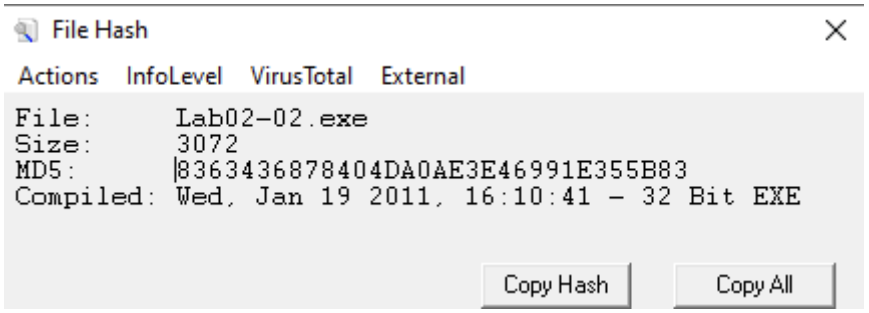
8. Na podstawie importowanych funkcjonalności można przypuszczać, że plik .dll jest używany przez plik ..exe w celu nawiązaia połączenia z serwerem.

Można przypuszczać, że z tego serwera zostaje pobrany plik, który zostaje uruchomiony hint: plik ..exe importuje CreateProcessA - wskazywało by to na uruchomienie pobranego pliku.

Można dodatkowo zauważyć na podstawie podobnych rekordów, że infekowana zostaje bilbioteka **Kernel32**, a jej oryginalna wersja prawdopodobnie zostaje zapisana w postaci **kerne123**

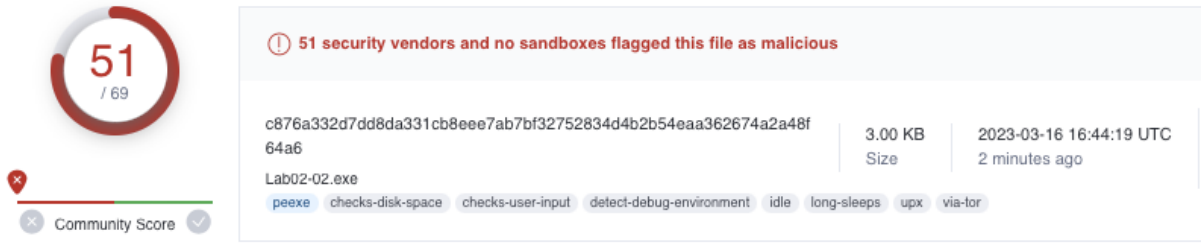
Zadanie 1.2 Lab02-02..exe

1. Analiza sum kontrolnych, sygnatury pliku



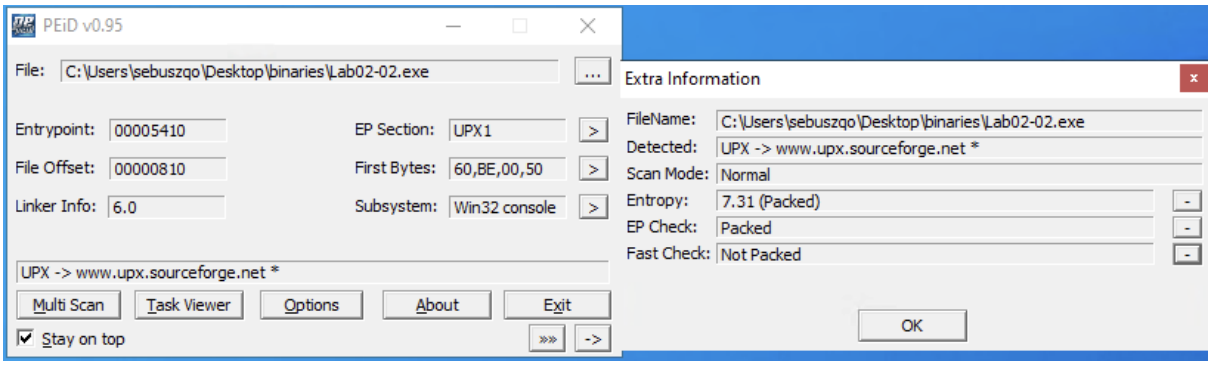
MD5: 8363436878404da0ae3e46991e355b83

SHA256:
c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6



Sygnatura analizowanego pliku była już wcześniej poddawana analizie, została oznaczona jako “malicious”. (51/69 narzdzędzi)

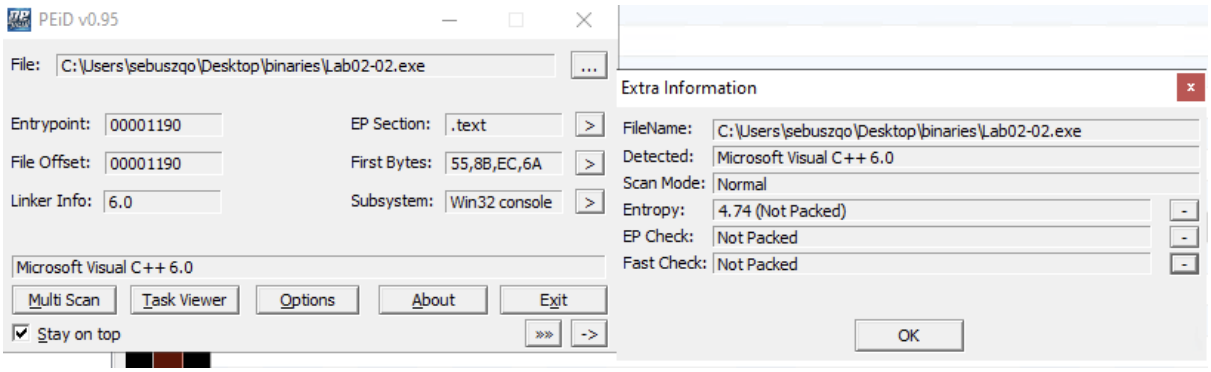
2.



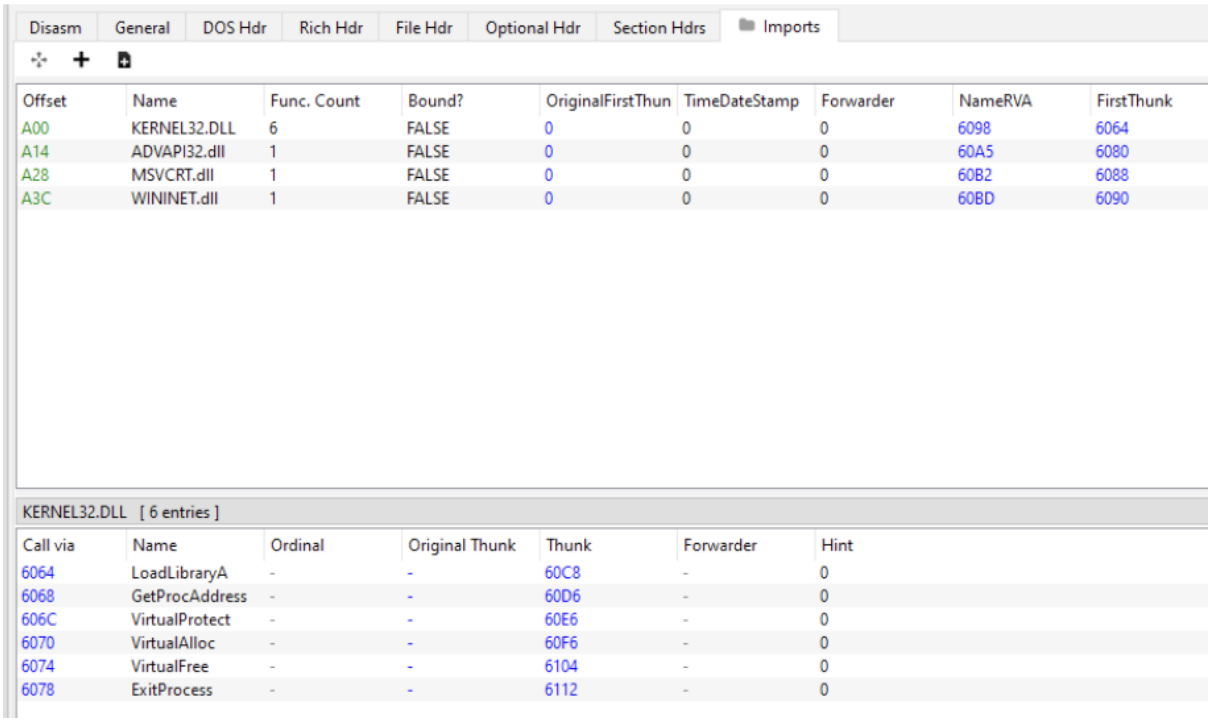
Program jest spakowany.

Używam UPX do rozpakowania

```
C:\Users\sebuszqo\Desktop\binaries>upx -d ./Lab02-02.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2010
UPX 3.05w       Markus Oberhumer, Laszlo Molnar & John Reiser   Apr 27th 2010

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     16384 <-      3072   18.75%    win32/pe     Lab02-02.exe

Unpacked 1 file.

C:\Users\sebuszqo\Desktop\binaries>
```



Spakowany:



Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
A00	KERNEL32.DLL	6	FALSE	0	0	0	6098	6064
A14	ADVAPI32.dll	1	FALSE	0	0	0	60A5	6080
A28	MSVCRT.dll	1	FALSE	0	0	0	60B2	6088
A3C	WININET.dll	1	FALSE	0	0	0	60BD	6090

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
6064	LoadLibraryA	-	-	60C8	-	0
6068	GetProcAddress	-	-	60D6	-	0
606C	VirtualProtect	-	-	60E6	-	0
6070	VirtualAlloc	-	-	60F6	-	0
6074	VirtualFree	-	-	6104	-	0
6078	ExitProcess	-	-	6112	-	0

Rozpakowany:

Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
208C	KERNEL32.DLL	9	FALSE	0	0	0	216C	2010
20A0	ADVAPI32.dll	3	FALSE	0	0	0	2179	2000
20B4	MSVCRT.dll	13	FALSE	0	0	0	2186	2038
20C8	WININET.dll	2	FALSE	0	0	0	2191	2070

KERNEL32.DLL [9 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
2010	SystemTimeToF...	-	-	219E	-	0
2014	GetModuleFile...	-	-	21B4	-	0
2018	CreateWaitable...	-	-	21C8	-	0
201C	ExitProcess	-	-	21DE	-	0
2020	OpenMutexA	-	-	21EC	-	0
2024	SetWaitableTimer	-	-	21F8	-	0
2028	WaitForSingleO...	-	-	220A	-	0
202C	CreateMutexA	-	-	2220	-	0
2030	CreateThread	-	-	222E	-	0

ADVAPI32.dll [3 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
2000	CreateServiceA	-	-	223C	-	0
2004	StartServiceCtrlDispatcherA	-	-	224C	-	0
2008	OpenSCManagerA	-	-	226A	-	0

WININET.dll [2 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
2070	InternetOpenUrlA	-	-	232A	-	0
2074	InternetOpenA	-	-	233C	-	0

Jak widać program tworzy między innymi wątki, usługi oraz wykonuje zapytania na adresy internetowe.

InternetOpenUrlA: Jest to funkcja, która umożliwia programowi otwarcie połączenia z adresem URL w celu pobrania zawartości strony internetowej lub pliku. Funkcja zwraca wskaźnik do otwartego połączenia, który może być następnie wykorzystany do pobrania zawartości za pomocą innych funkcji.

Obie funkcje, InternetOpenA i InternetOpenUrlA, są funkcjami z biblioteki WinINet.dll, które umożliwiają programiście nawiązanie połączenia z internetem i pobieranie danych z serwera. Różnią się jednak sposobem, w jaki są wykorzystywane w aplikacji.

Funkcja InternetOpenA służy do utworzenia sesji internetowej. Musi ona zostać utworzona przed rozpoczęciem komunikacji z internetem. Funkcja ta tworzy wskaźnik do nowej sesji internetowej i zwraca ten wskaźnik do programisty. Programista może następnie użyć tego wskaźniku w innych funkcjach WinINet, np. InternetConnect czy HttpOpenRequest.

Z kolei funkcja InternetOpenUrlA jest używana, gdy programista chce otworzyć konkretne połączenie z serwerem i pobrać dane z określonego zasobu. Funkcja ta wymaga podania wskaźnika do sesji internetowej (który został utworzony za pomocą funkcji InternetOpenA) oraz adres URL, na który ma zostać wykonane zapytanie.

ExitProcess: Jest to funkcja, która zamyka bieżący proces i zwraca kontrolę do systemu operacyjnego. Funkcja przyjmuje jeden parametr - kod wyjścia, który jest zwracany do systemu operacyjnego i może być wykorzystany przez proces nadrzędny.

CreateMutexA: Jest to funkcja, która tworzy nowy obiekt mutexa systemowego, który może być wykorzystywany do synchronizacji dostępu do współdzielonych zasobów przez różne procesy. Funkcja zwraca wskaźnik do nowo utworzonego mutexa, który może być następnie wykorzystany do dostępu do zasobów.

4. Informacje świadczące o połączeniach programu z internetem

- link url z którym prawdopodobnie łączy się program
- InternetOpenUrlA oraz InternetOpenA tuż przed podaniem url
- Internet Explorer 8.0 - wersja przeglądarki

0000230E	_except_handler3
00002320	_controlfp
0000232C	InternetOpenUrlA
0000233E	InternetOpenA
00003010	MalService
0000301C	Malservice
00003028	HGL345
00003030	http://www.malwareanalysisbook.com
00003054	Internet Explorer 8.0

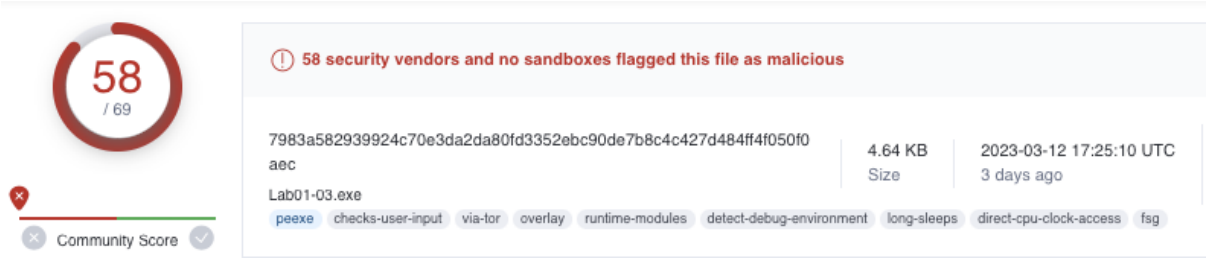
Zadanie 1.3 Lab02-03..exe

1. Analiza sum kontrolnych, sygnatury pliku

Filename:	Lab02-03.exe
MD5:	9c5c27494c28ed0b14853b346b113145
SHA1:	290ab6f431f46547db2628c494ce615d6061ceb8
CRC32:	b2164101
SHA-256:	7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec
SHA-512:	38741bd024904f21d424254c1fbb3c16c6925d60b34d85f9cecff5d973c6c823b6b5e5e61
SHA-384:	f9779784317b2e88af7db0a67d48c14433f42b453d0fbd851b4a43a14e35d774fcc47e6c1
Full Path:	C:\Users\sebuszqo\Desktop\binaries\Lab02-03.exe
Modified Time:	3/16/2023 3:05:14 PM
Created Time:	3/26/2011 7:54:40 AM
Entry Modified Time:	3/16/2023 3:05:14 PM

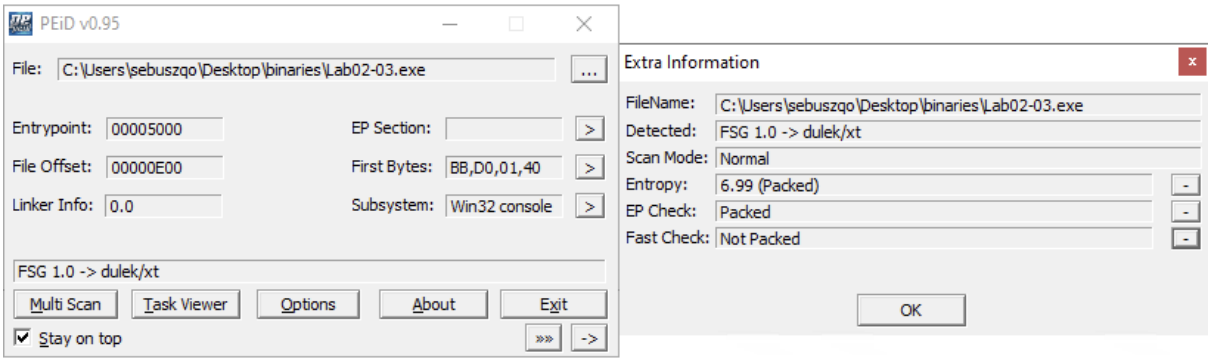
MD5: 9c5c27494c28ed0b14853b346b113145

SHA256:
7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec



Sygnatura analizowanego pliku była już wcześniej poddawana analizie, została oznaczona jako “malicious”. (58/69 narzdzędzi)

2.

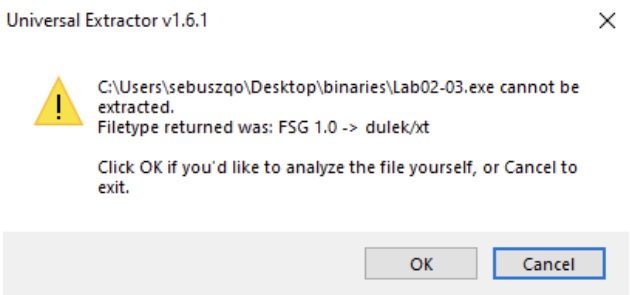


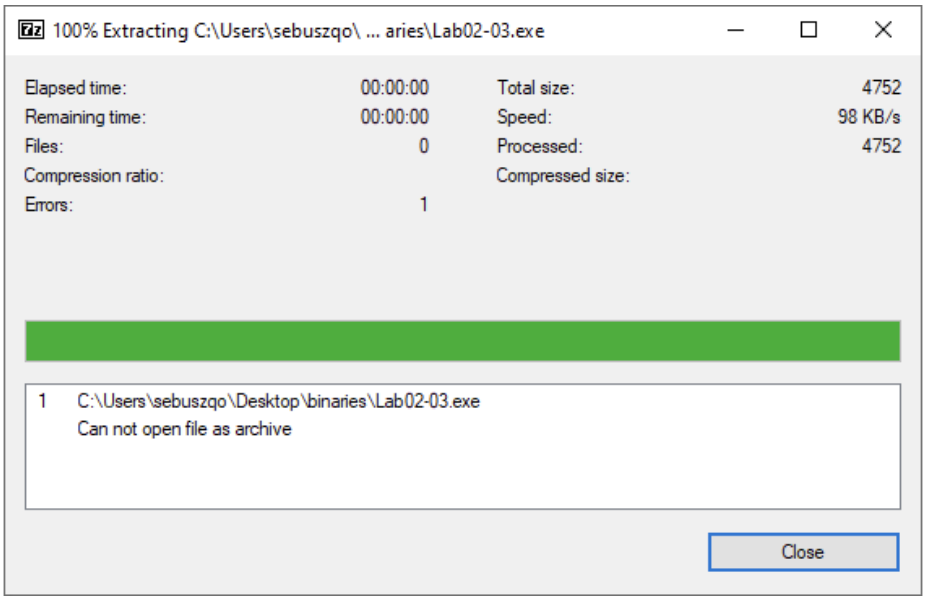
Program jest spakowany.

Niestety wszystkie próby rozpakowania, nie powiodły się.

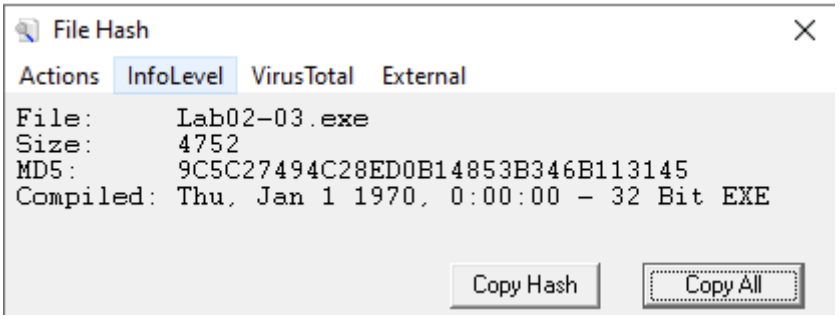
Próba za pomocą UPX → brak powodzenia, nie został spakowany przy użyciu UPX

```
        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: Lab02-03.exe: NotPackedException: not packed by UPX

Unpacked 0 files.
```

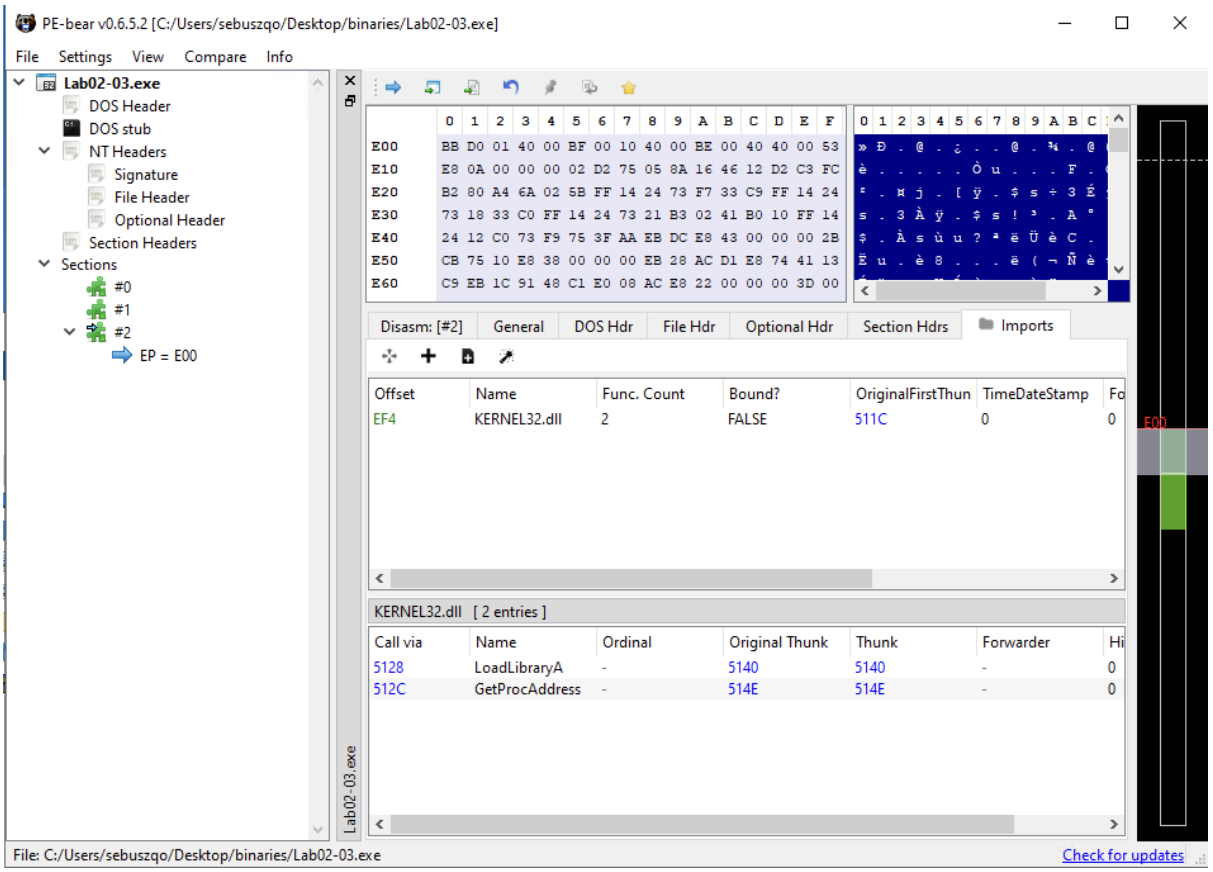




3. Tak, data kompilacji pliku:



4.



Niestety nie jestem w stanie sprawdzić funkcjonalność badanego pliku. Jedynie widać, że program ładuje jakąś bibliotekę.

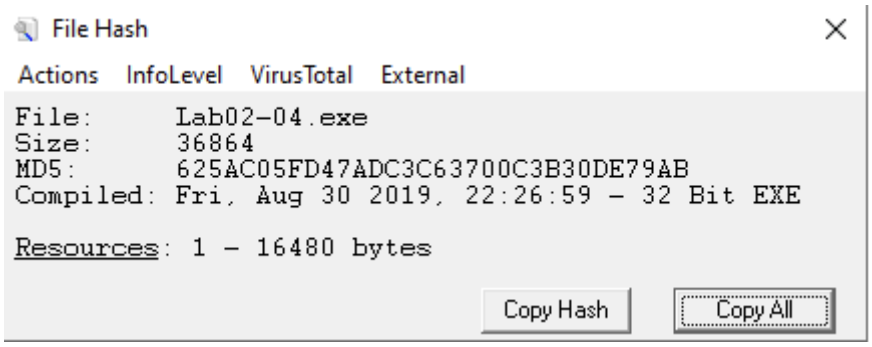
5. Żaden ze stringów nie wskazuje na żadną próbę połączenia z siecią internet.

WARTO nadmienić i pamiętać, że dany plik nie został rozpakowany.

Offset	Strings recognized ASCII
00000000	MZ
0000004D	!Windows Program
0000005F	$PE
00000184	ta
000001D6	b!@
0000020F	`.rdata
00000237	@.data
00000E0C	@@
00000E28	$s
00000E2F	$s
00000E36	$s!
00000E45	u?
00000E5D	tA
00000E7F	AA
00000E94	T$
00000E9A	T$
00000EA0	_[
00000EA4	;Ot
00000EA8	Ot
00000EB7	CC
00000EC0	(Q@
00000EE7	WU
00000F00	4Q
00000F04	(Q
00000F1C	@Q
00000F20	NQ
00000F28	@Q
00000F2C	NQ
00000F34	KERNEL32.dll
00000F42	LoadLibraryA
00000F50	GetProcAddress
00001003	$j
00001008	H @
0000100F	|v
00001015	Ph8
0000101C	0[X
00001020	":LI
00001025	3Bt>O
0000102E	VQ(8
0000103A	48
00001043	2]<,M
00001059	VP
0000105C	:R,
00001060	P@M^
00001066	3
00001076	hx
00001082	w(
00001089	S>VW
00001099	OY
000010A4	"*
000010A9	c|
000010B7	p1
000010BE	AQ=h
000010CA	"Z,
000010D1	5h
000010D5	3T
000010D8	)"

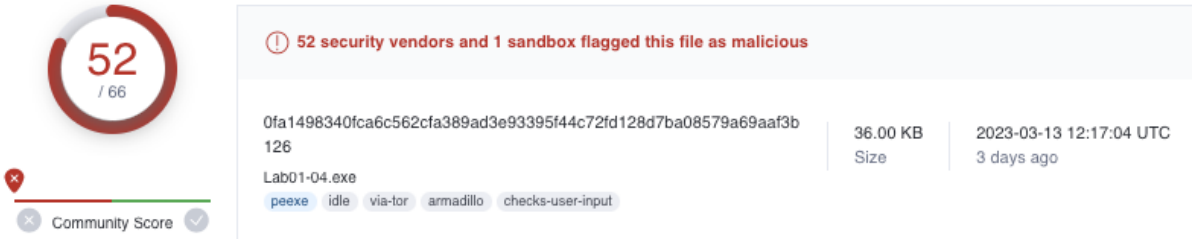
Zadanie 1.4 Lab02-04.exe

1. Analiza sum kontrolnych, sygnatury pliku



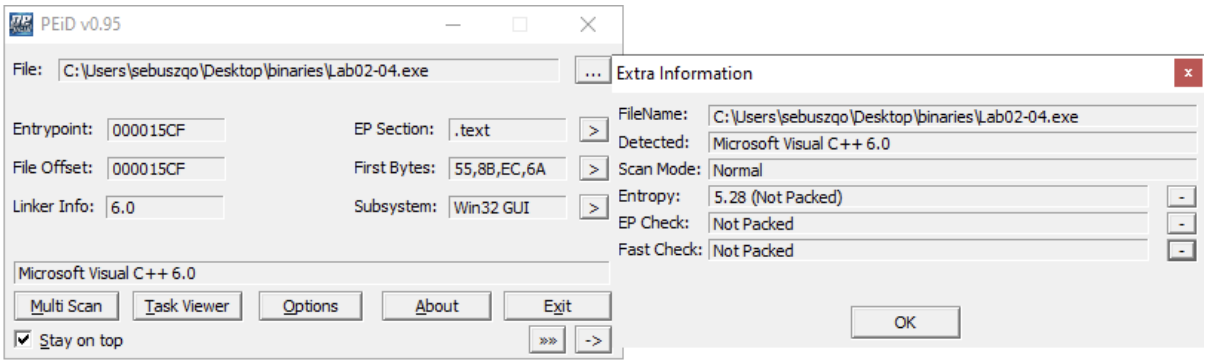
MD5: 625AC05FD47ADC3C63700C3B30DE79AB

SHA 256:
0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126



Sygnatura analizowanego pliku była już wcześniej poddawana analizie, została oznaczona jako “malicious”. (52/66 narzdzędzi)

2. Narzędzie PEiD wskazało stan “Not Packed”



3. Data kompilacji: **2019/08/30**

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0004	Number of Sections	
000000F0	5D69A2B3	Time Date Stamp	2019/08/30 Fri 22:26:59 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	

4.

Disasm: .text | General | DOS Hdr | Rich Hdr | File Hdr | Optional Hdr | Section Hdrs | Imports | Resources

Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
20A4	KERNEL32.dll	16	FALSE	2104	0	0	228E	2010
20B8	ADVAPI32.dll	3	FALSE	20F4	0	0	22E0	2000
20CC	MSVCRT.dll	15	FALSE	2148	0	0	22FA	2054

KERNEL32.dll [16 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
2010	GetProcAddress	-	21CE	21CE	-	13E
2014	LoadLibraryA	-	21E0	21E0	-	1C2
2018	WinExec	-	21F0	21F0	-	2D3
201C	WriteFile	-	21FA	21FA	-	2DF
2020	CreateFileA	-	2206	2206	-	34
2024	SizeofResource	-	2214	2214	-	295
2028	CreateRemoteT...	-	21B8	21B8	-	46
202C	FindResourceA	-	2236	2236	-	A3
2030	GetModuleHan...	-	2246	2246	-	126
2034	GetWindowsDir...	-	225A	225A	-	17D
2038	MoveFileA	-	2272	2272	-	1DD
203C	GetTempPathA	-	227E	227E	-	165
2040	GetCurrentProc...	-	21A4	21A4	-	F7
2044	OpenProcess	-	2196	2196	-	1EF
2048	CloseHandle	-	2188	2188	-	1B
204C	LoadResource	-	2226	2226	-	1C7

ADVAPI32.dll [3 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
2000	OpenProcessTo...	-	22CC	22CC	-	142
2004	LookupPrivileg...	-	22B4	22B4	-	F5
2008	AdjustTokenPri...	-	229C	229C	-	17

4. Tak jestem w stanie sprawdzić funkcjonalność badanego pliku. Program ładuje bilbioteki, wykonuje również operacje na plikach i katalogach (m.in. tworzenie, zapis, przenoszenie, odczyt ścieżki). Co więcej wchodzi też w interakcję z innymi procesami.

Można by przypuszczać, że program zapisuje bilbiotekę w folderze Windows tudzież innych podfolderach, a następnie ustawia jej odpowiednie uprawnienia i ją uruchamia. Wspomniana bilblioteka, może być wewnętrzną zawartością pliku ..exe, lub może być pobierana z interentu, jednakże ad. pkt 6 - brak importów świadczących o próbie komunikacji z internetem.

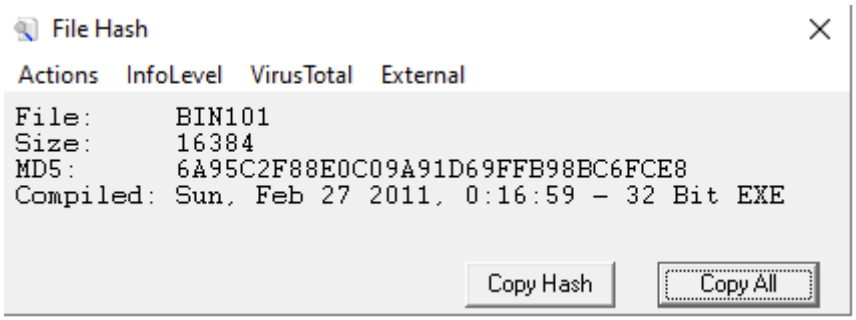
5. W strings, można odszukać następne informacje dot. połączenia z internetem

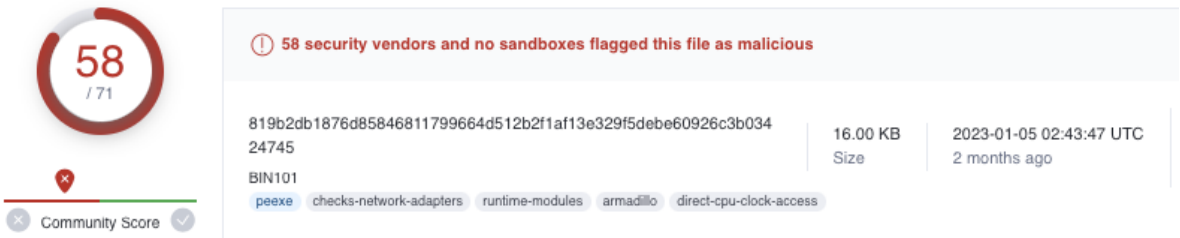
- **http://www.practicalmalwareanalysis.com/updater..exe**

00007070	\winup.exe
0000707C	%s%s
00007084	\system32\wupdmgrd.exe
0000709C	%s%s
000070A4	http://www.practicalmalwareanalysis.com/updater.exe

6. Poruszone w podpunkcie 4, brak importów świadczących o potencjalnych importach dotyczących połączenia z siecią internet.

7. Użycie Reasource Hacker, wyodrębnienie zasobu oraz jego analiza:





00007070	\winup.exe
0000707C	%s%s
00007084	\system32\wupdmgrd.exe
0000709C	%s%s
000070A4	http://www.practicalmalwareanalysis.com/updater.exe

Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
2064	KERNEL32.dll	3	FALSE	20B4	0	0	213A	2000
2078	urlmon.dll	1	FALSE	2100	0	0	215E	204C
208C	MSVCRT.dll	14	FALSE	20C4	0	0	2176	2010

urlmon.dll [1 entry]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
204C	URLDownloadToFileA	-	2148	2148	-	3E

Po użyciu programu Resource Haker, i analizie wyodrębionego zasobu. Można dojść do wniosku, że plik ten jest zapisywany, a następnie wykorzystywany do pobrania pliku wykonawczegom który zostaje uruchomiony (ze wcześniejszej analizy mamy informację, że importowoany jest Win.exec). Znaleziony wcześniej url znajduje się wewnątrz “wypakowanego” pliku. Możemy uznać, że plik jest dropperem.

(plik jest przeznaczony do instalowania i uruchamiania innych złośliwych plików na komputerze, nazywa się "dropperem". Dropper może być częścią szkodliwego oprogramowania lub sam w sobie może być złośliwy.)