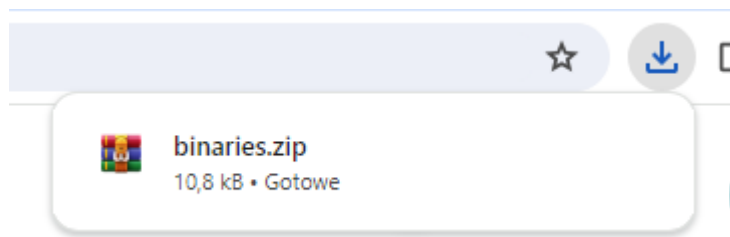
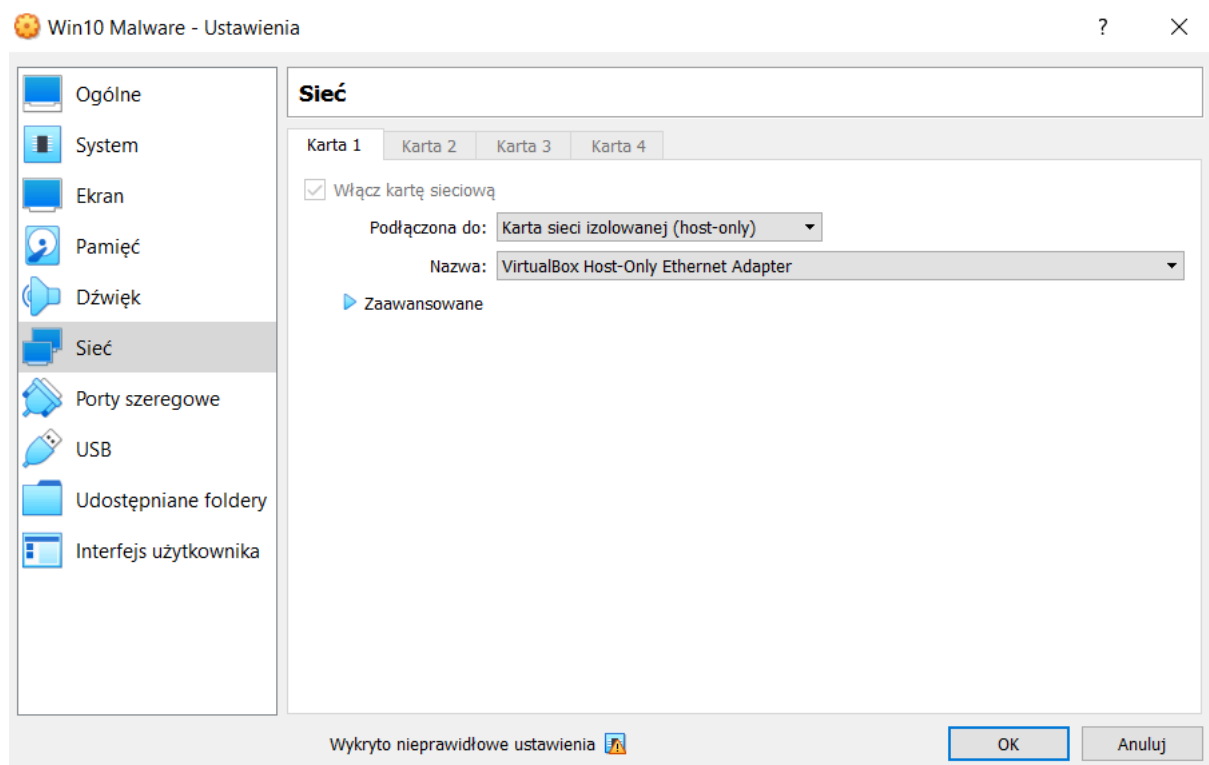


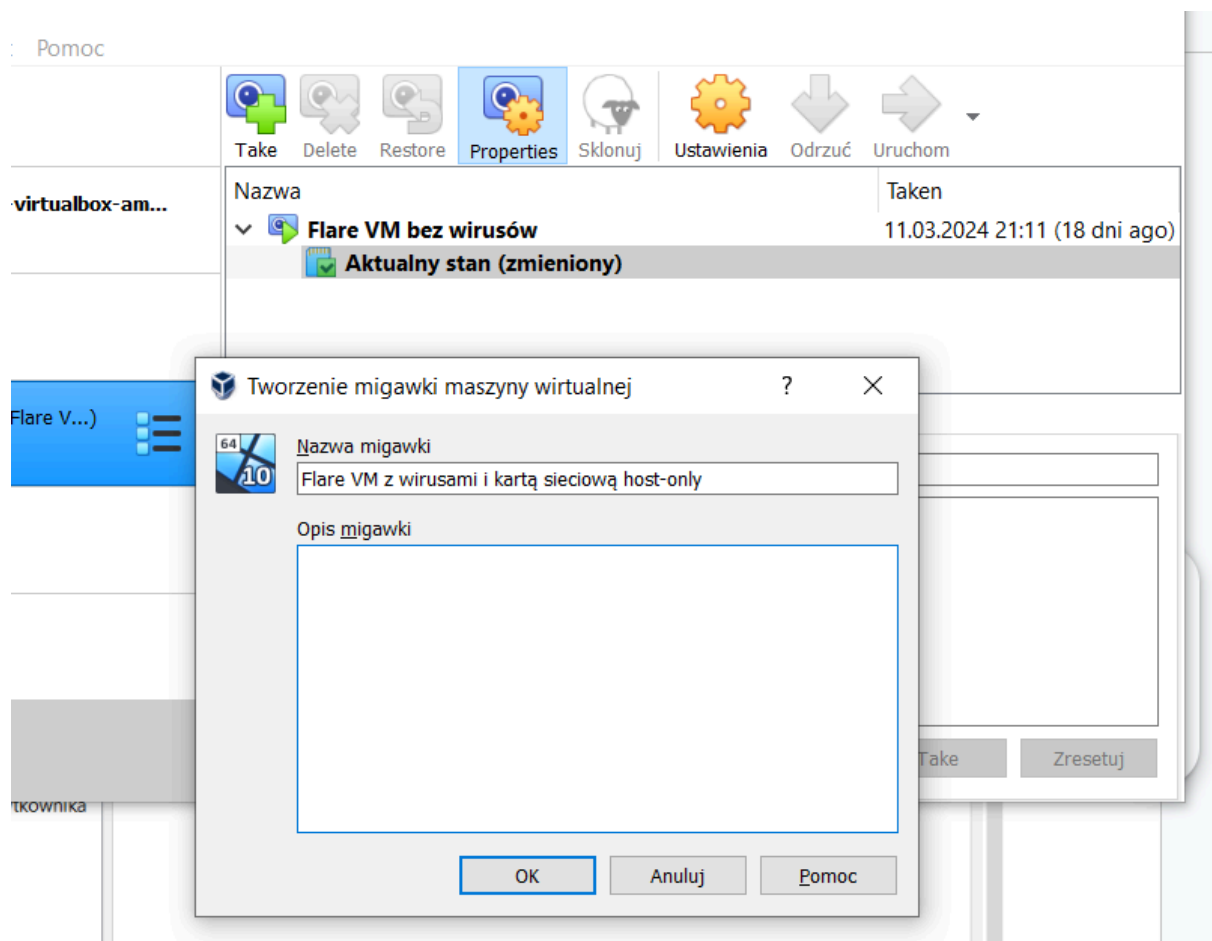
Szymon Kozioł



Plik szybko został pobrany, ponieważ Windows Defender został w ramach LAB1 całkowicie wyłączony.



Zmieniłem kartę sieciową na host only, co pominąłem w poprzednim laboratorium.

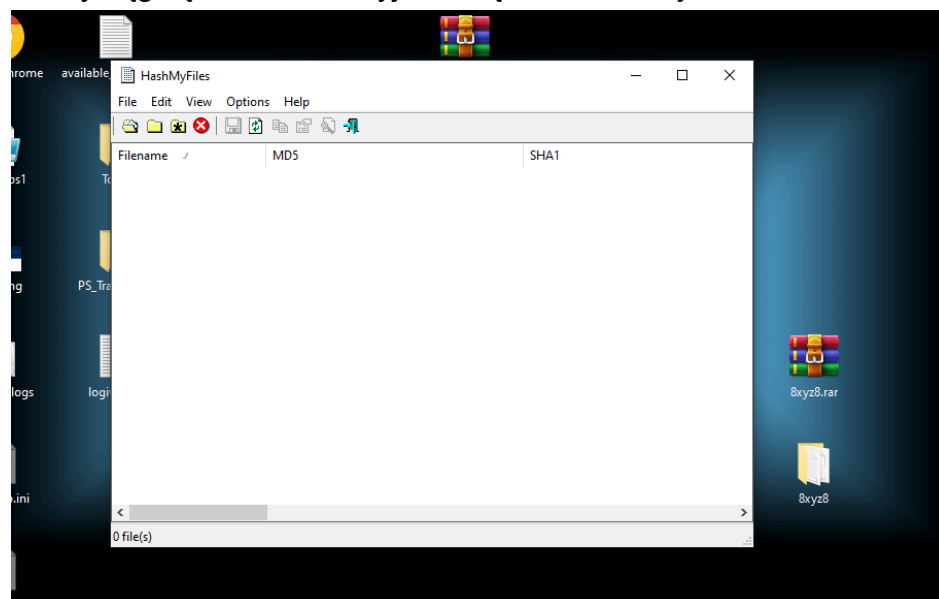


Stworzyłem kolejną migawkę.

1.1

1)

Do wyciągnięcia hasha użyje narzędzia HashMyFiles:



HashMyFiles		
File Edit View Options Help		
Filename	MD5	SHA1
Lab02-01.dll	290934c61de9176ad682ffdd65f0a669	a4b35de71ca20fe776dc72d12fb2
Lab02-01.exe	bb7425b82141a1c0f7d60e5106676bb1	9dce39ac1bd36d877fdb0025ee8f

Plik Lab02-01.dll został wykryty przez VirusTotal:

37 / 70 security vendors and no sandboxes flagged this file as malicious

Size: 160.00 KB | Last Modification Date: 2 minutes ago

Community Score: 37 / 70

Popular threat label: trojan.skeeyah/genericrxf

Threat categories: trojan

Family labels: skeeyah, genericrxf, r002cph20

Security vendors' analysis:

Vendor	Detection	Vendor	Detection
Alibaba	Trojan:Win32/Skeeyah.7fb0ebff	AllCloud	Trojan:Win/Skeeyah.AIMTB
ALYac	Trojan.Agent.Waski	Antiy-AVL	Trojan/Win32.BTSGeneric
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
BitDefenderTheta	Gen:NN.ZedlaF.36802.kq4@aGkQVtp	Bkav Pro	W32.Common.EDE63FAA
ClamAV	Win.Malware.Agent-6369668-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)

Plik Lab02-01.exe również:

52 / 72 security vendors and 1 sandbox flagged this file as malicious

Size: 16.00 KB | Last Modification Date: 1 hour ago

Community Score: 52 / 72

Popular threat label: trojan.ulise/aenjaris

Threat categories: trojan

Family labels: ulise, aenjaris, kkbv

Security vendors' analysis:

Vendor	Detection	Vendor	Detection
AhnLab-V3	Trojan/Win32.Agent.C957604	Alibaba	Trojan:Win32/Aenjaris.2be749b4
AllCloud	Backdoor	ALYac	Trojan.Agent.163845S
Antiy-AVL	Trojan/Win32.TSGeneric	Arcabit	Trojan.Ulise.D1BC1E
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Agent.kkbv	BitDefender	GenVariant.Ulise.113694

2)

Program PView z jakiegoś powodu nie zainstalował mi się wraz z pakietem FLARE.

Do tego podpunktu wykorzystam narzędzie CFF Explorer, które działa podobnie, aby zaoszczędzić czas i nie podłączać maszyny do domowej sieci.

CFF Explorer VIII - [Lab02-01.dll]

File Settings ?

Lab02-01.dll

Property	Value
File Name	C:\Users\SzymonMalware\Desktop\binaries\Lab02-01.dll
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0 DLL
File Size	160.00 KB (163840 bytes)
PE Size	160.00 KB (163840 bytes)
Created	Saturday 30 March 2024, 10.22.05
Modified	Sunday 19 December 2010, 11.16.38
Accessed	Saturday 30 March 2024, 10.41.48
MD5	290934C61DE9176AD682FFDD65F0A669
SHA-1	A4B35DE71CA20FE776DC72D12FB2886736F43C22

Property	Value
Empty	No additional info available

Plik Lab02-01.dll był ostatni raz kompilowany 19.12.2010 o godz. 11:16.

CFF Explorer VIII - [Lab02-01.exe]

File Settings ?

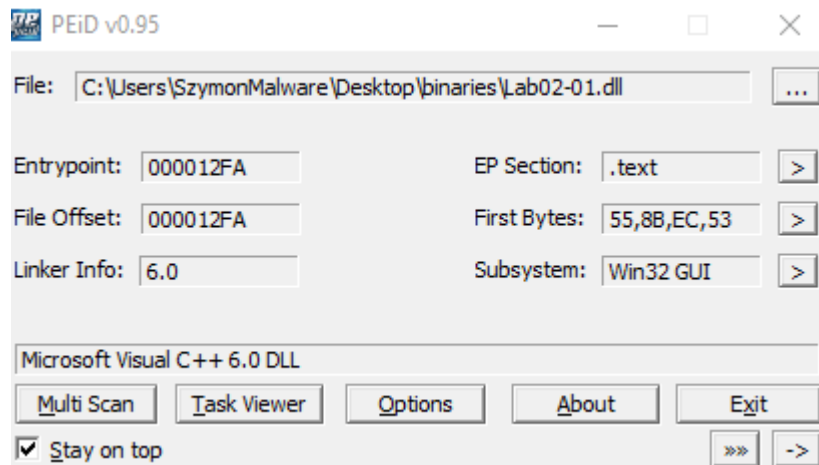
Lab02-01.exe

Property	Value
File Name	C:\Users\SzymonMalware\Desktop\binaries\Lab02-01.exe
File Type	Portable Executable 32
File Info	Microsoft Visual C++
File Size	16.00 KB (16384 bytes)
PE Size	16.00 KB (16384 bytes)
Created	Saturday 30 March 2024, 10.22.05
Modified	Sunday 08 January 2012, 02.19.04
Accessed	Saturday 30 March 2024, 10.47.26
MD5	BB7425B82141A1C0F7D60E5106676BB1
SHA-1	9DCE39AC1BD36D877FDB0025EE88FDAFF0627CDB

Property	Value
Empty	No additional info available

Plik Lab02-01.exe był ostatni raz kompilowany 8.01.2012 o godz 02:19.

3)

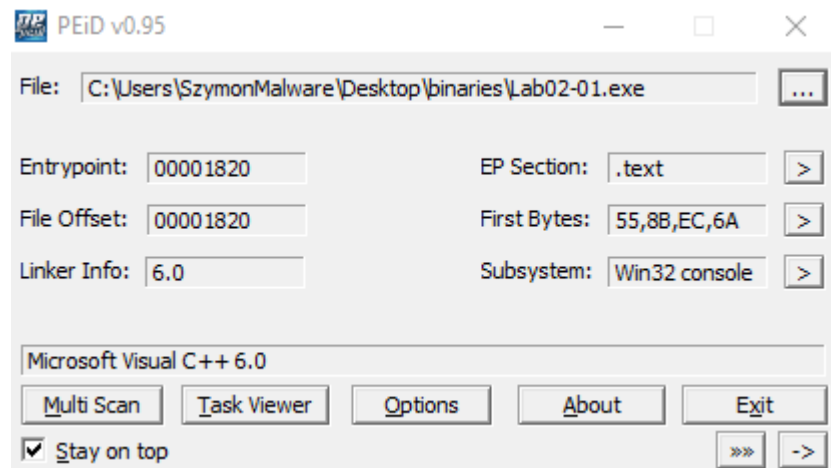


Typ pliku: Microsoft Visual C++ 6.0 DLL

Typ podsystemu: Win32 GUI

Pierwsze bajty: 55,8B,EC,53 (typowe dla plików wykonywalnych w systemie Windows)

Wyniki wydają się być normalne i nie wskazują na to, że plik jest spakowany lub ma inne nietypowe cechy. Oznacza to, że plik Lab02-01.dll jest w formacie umożliwiającym pełną analizę.



Typ pliku: Microsoft Visual C++ 6.0

Typ podsystemu: Win32 console

Pierwsze bajty: 55,8B,EC,6A (typowe dla plików wykonywalnych w systemie Windows)

Co oznacza każdy z tych wyników:

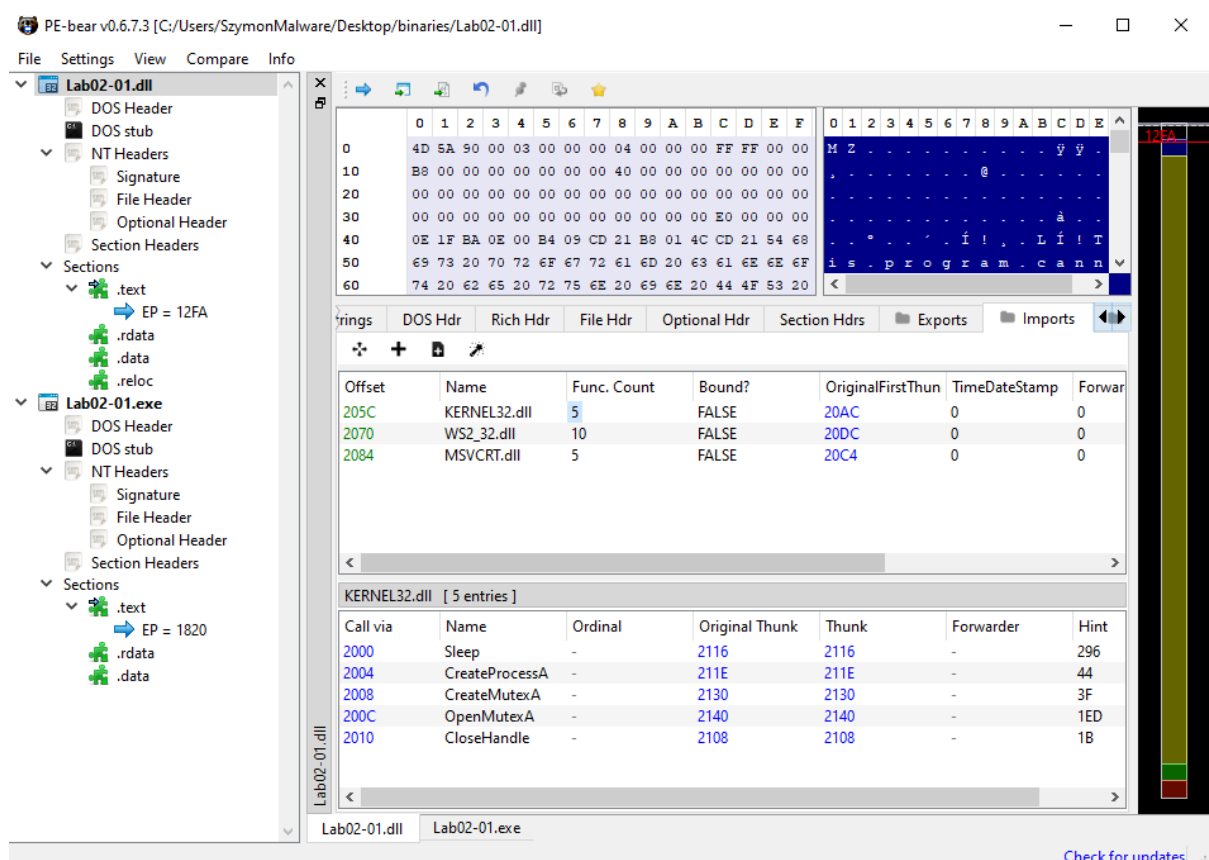
Typ pliku: Wskazuje na to, że plik jest typu EXE skompilowany w środowisku Microsoft Visual C++ 6.0.

Typ podsystemu: Wskazuje, że plik jest przeznaczony dla środowiska konsolowego (Console) w systemie Windows.

Pierwsze bajty: Te bajty są typowe dla plików wykonywalnych w systemie Windows.

Na podstawie tych wyników można stwierdzić, że plik Lab02-01.exe również jest w formacie umożliwiającym pełną analizę w PEiD.

4)



Importy pliku Lab02-01.dll:

KERNEL32.dll

Liczba funkcji: 5

Jest podstawową biblioteką dla systemów operacyjnych Windows i zawiera podstawowe funkcje systemowe.

Zawiera:

Sleep

Opis: Funkcja używana do opóźnienia wykonywania programu na określoną liczbę milisekund.

CreateProcessA

Opis: Funkcja używana do tworzenia nowego procesu.

CreateMutexA

Opis: Funkcja używana do tworzenia obiektu mutexu.

OpenMutexA

Opis: Funkcja używana do otwierania istniejącego obiektu mutexu.

CloseHandle

Opis: Funkcja używana do zamykania uchwytu do obiektu.

Co to oznacza?

Sleep: Program korzysta z funkcji Sleep do opóźniania wykonywania programu na określoną liczbę milisekund.

CreateProcessA: Program może tworzyć nowe procesy.

CreateMutexA i OpenMutexA: Program może tworzyć oraz otwierać obiekty mutexu, co jest często używane w celu synchronizacji dostępu do zasobów w systemie.

CloseHandle: Program korzysta z funkcji CloseHandle do zamykania uchwytu do obiektu.

(Nie wiem, czy to dobrze przetłumaczyłem. Uchwyt obiektu jest abstrakcyjnym pojęciem, które służy jako interfejs między aplikacją a systemem operacyjnym. Kiedy program otwiera zasób, system operacyjny przydziela mu uchwyt.)

WS2_32.dll

Jest biblioteką odpowiedzialną za obsługę gniazd i komunikacji sieciowej w systemie Windows.

MSVCRT.dll

Liczba funkcji: 5

Jest biblioteką standardową języka C dla systemu Windows.

Zawiera:

`_adjust_fdiv`

Opis: Funkcja używana do korekty dzielenia przez zero dla liczb zmiennoprzecinkowych.

`malloc`

Opis: Funkcja używana do alokacji pamięci dynamicznej.

`_initterm`

Opis: Funkcja używana do inicjalizacji tablic globalnych w C++.

`free`

Opis: Funkcja używana do zwalniania zaalokowanej wcześniej pamięci.

`strncmp`

Opis: Funkcja używana do porównywania dwóch ciągów znaków do określonej liczby znaków.

Co to oznacza?

Program korzysta z funkcji “`_adjust_fdiv`” do korekty dzielenia przez zero dla liczb zmiennoprzecinkowych, co może sugerować operacje na liczbach zmiennoprzecinkowych.

Program korzysta z funkcji “`malloc`” i “`free`” do zarządzania pamięcią dynamiczną, co jest typowe dla programów napisanych w języku C lub C++.

Program korzysta z funkcji “`_initterm`” do inicjalizacji tablic globalnych w C++, co sugeruje, że program może być napisany w języku C++.

Program korzysta z funkcji “`strncmp`” do porównywania ciągów znaków, co jest typowe dla operacji porównywania w języku C lub C++.

Importy pliku Lab02-01.exe:

KERNEL32.dll

Liczba funkcji: 10

Nie zawiera podobnych funkcji do .dll, posiada jednak szereg innych funkcji takich jak np.:

Funkcja **CreateFileA** jest używana w systemie Windows do tworzenia lub otwierania pliku lub urządzenia. Jest to jedna z podstawowych funkcji systemowych do zarządzania plikami i urządzeniami w systemie Windows.

Funkcja **FindClose** służy do zamykania uchwytu do wyszukiwania plików, który został wcześniej otwarty za pomocą funkcji FindFirstFile lub FindNextFile.

Funkcja **FindNextFileA** jest używana do kontynuowania wyszukiwania plików po wywołaniu funkcji FindFirstFile.

MSVCRT.dll

Liczba funkcji: 15

Zawiera m.in również malloc, czy _adjust_fdiv, posiadając jednak szereg innych funkcji takich jak np.:

Funkcja **__set_app_type** jest często używana w aplikacjach napisanych w C lub C++ kompilowanych za pomocą kompilatora Microsoft Visual C++. Służy ona do ustawiania typu aplikacji, na przykład konsolowej lub okienkowej.

5)

Z poprzedniego podpunktu:

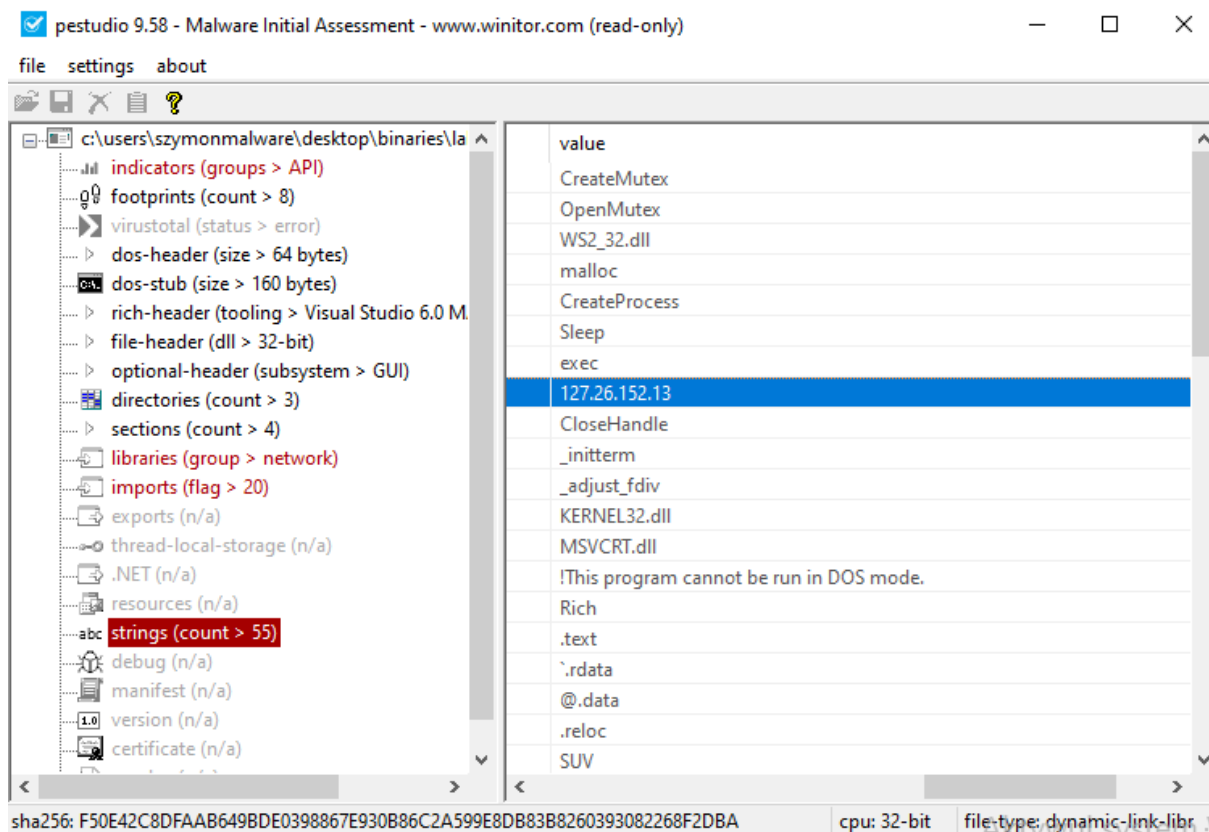
WS2_32.dll

Jest biblioteką odpowiedzialną za obsługę gniazd i komunikacji sieciowej w systemie Windows.

6)

Użyłem programu PEStudio, ponieważ nie posiadałem PPEE

7)



Posiada, chociażby wartość, która jest adresem IPv4 w labelu url-pattern.

8)

Lab02-01.exe:

- Dokonuje operacji na plikach, takich jak odczyt, zapis lub modyfikacja.
- Zarządza pamięcią dynamiczną przez alokację i zwalnianie pamięci.
- Przetwarza dane, w tym operuje na ciągach znaków.

Lab02-01.dll:

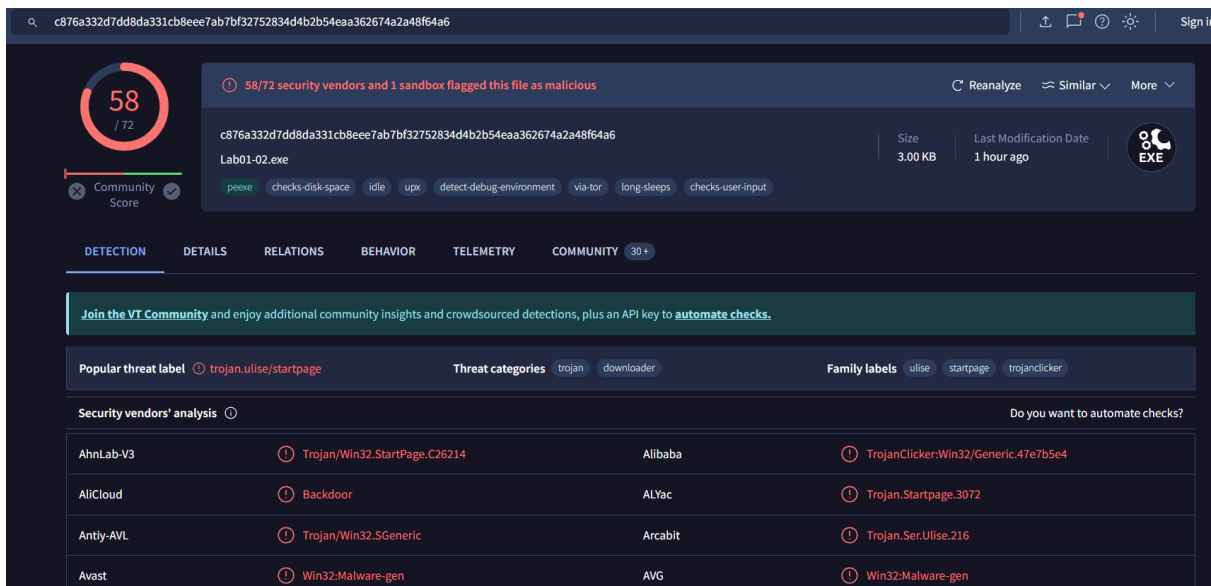
- Zawiera funkcje pomocnicze wykorzystywane przez Lab02-01.exe.
- Umożliwia komunikację sieciową.
- Tworzy i zarządza procesami oraz obiektami mutex.

1.2

1)

MD5

8363436878404da0ae3e46991e355b83

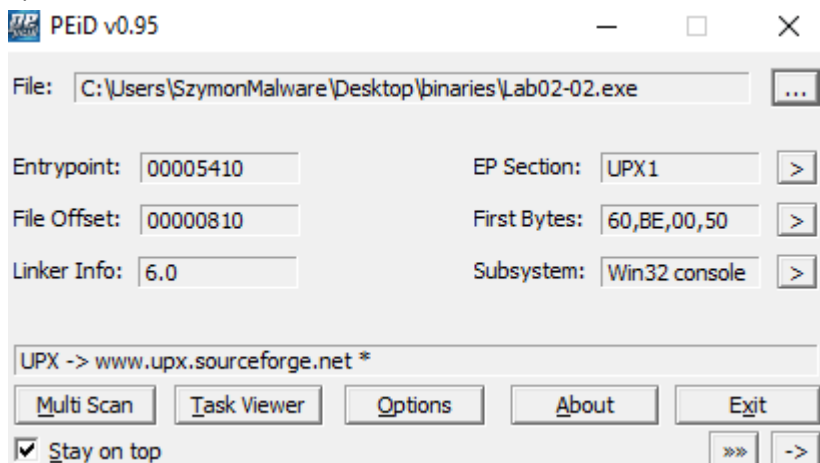


The screenshot shows the VirusTotal interface for the file `Lab01-02.exe` (MD5: `c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6`). The file is 3.00 KB and was last modified 1 hour ago. It has a Community Score of 58/72. A warning indicates that 58/72 security vendors and 1 sandbox flagged this file as malicious. The file is categorized as `trojan.ulise/startpage` and belongs to the `ulise` family. The security vendors' analysis table shows the following results:

Security Vendor	Detection
AhnLab-V3	Trojan.Win32.StartPage.C26214
Alibaba	TrojanClicker.Win32/Generic.47e7b5e4
AliCloud	Backdoor
ALYac	Trojan.Startpage.3072
Antiy-AVL	Trojan.Win32.SGeneric
Arcabit	Trojan.Ser.Ulise.216
Avast	Win32:Malware-gen
AVG	Win32:Malware-gen

Plik był wcześniej analizowany w VirusTotal.

2)



Plik `Lab02-02.exe` został spakowany za pomocą UPX (Ultimate Packer for eXecutables).

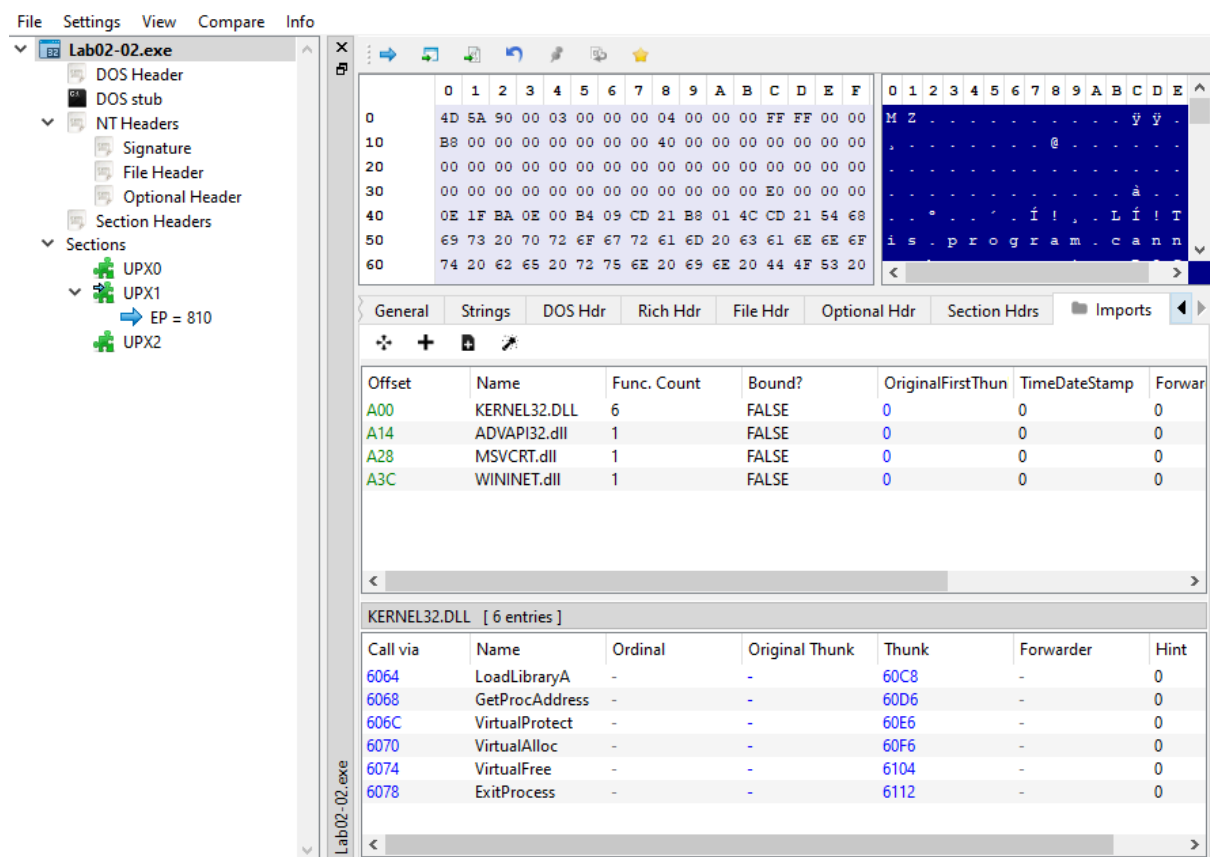
```
FLARE-VM 30.03.2024 13:08:33,30
C:\Users\SzymonMalware\Desktop\binaries>upx -d Lab02-02.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2024
UPX 4.2.2      Markus Oberhumer, Laszlo Molnar & John Reiser      Jan 3rd 2024

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

Unpacked 1 file.
```

3)

Importy przed rozpakowaniem:



Importy po rozpakowaniu:

PE-bear v0.6.7.3 [C:/Users/SzymonMalware/Desktop/binaries/Lab02-02.exe]

File Settings View Compare Info

Lab02-02.exe

- DOS Header
- DOS stub
- NT Headers
 - Signature
 - File Header
 - Optional Header
- Section Headers
- Sections
 - .text (EP = 1190)
 - .rdata
 - .data

General Strings DOS Hdr Rich Hdr File Hdr Optional Hdr Section Hdrs Imports

Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forward
208C	KERNEL32.DLL	9	FALSE	0	0	0
20A0	ADVAPI32.dll	3	FALSE	0	0	0
20B4	MSVCRT.dll	13	FALSE	0	0	0
20C8	WININET.dll	2	FALSE	0	0	0

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
----	----	----	----	----	----	----

File: C:/Users/SzymonMalware/Desktop/binaries/Lab02-02.exe [Check for](#)

Jak możemy zauważyć, ilość funkcji zwiększyła się.

Pliki spakowane często zawierają zaciemniony kod, co znacząco utrudnia jego analizę. Rozpakowanie pliku pozwala na odsłonięcie oryginalnego kodu źródłowego i ułatwia dokładniejszą analizę oraz zrozumienie jego działania.

W tym przypadku importy nie wskazywały szczegółowo na to, że plik ten jest z kategorii malware, dopiero po rozpakowaniu można było klarownie wysunąć takie wnioski.

Najciekawsze importy z Lab02-02.exe:

MSVCRT.dll

_setusermatherr

Opis: Funkcja używana do ustawienia funkcji obsługi błędów matematycznych użytkownika.

`_adjust_fdiv`

Opis: Funkcja używana do korekty dzielenia przez zero dla liczb zmiennoprzecinkowych.

`_P_commode`

Opis: Funkcja używana do ustawienia trybu komunikacji dla plików.

`_P_fmode`

Opis: Funkcja używana do ustawienia trybu otwierania plików (tekstowy lub binarny).

`_set_app_type`

Opis: Funkcja używana do ustawienia typu aplikacji (np. konsolowa, GUI).

`_except_handler3`

Opis: Funkcja używana do obsługi wyjątków w aplikacji.

`_controlfp`

Opis: Funkcja używana do ustawienia i sprawdzenia flagi kontrolną zmiennoprzecinkową.

ADVAPI32.dll

CreateServiceA

Opis: Funkcja używana do tworzenia nowej usługi w systemie Windows.

StartServiceCtrlDispatcherA

Opis: Funkcja używana do uruchomienia kontrolera usług, który zarządza usługami serwisów.

OpenSCManagerA

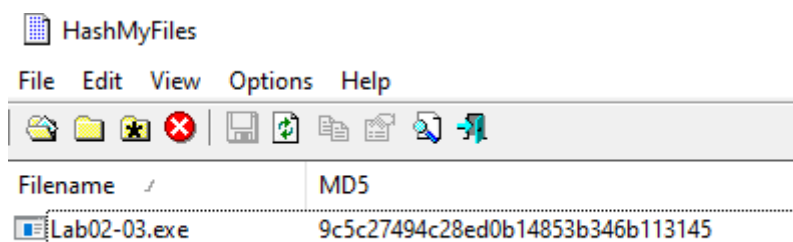
Opis: Funkcja używana do otwarcia menedżera usług, co umożliwia zarządzanie usługami systemowymi.

4)

network	-	InternetOpenUrl
network	-	InternetOpen
network	-	WININET.dll

1.3

1)



MD5

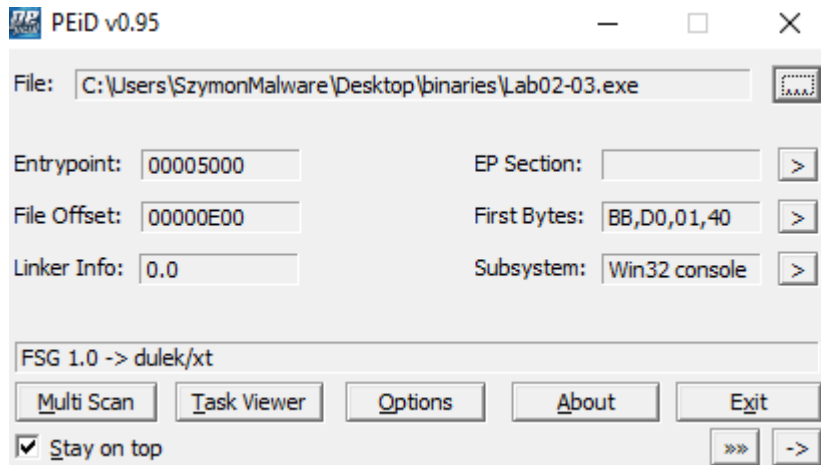
9c5c27494c28ed0b14853b346b113145

The screenshot displays the VirusTotal analysis interface for the file 'Lab18-02.exe' (SHA256: 7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aef). The interface shows a '66 / 72' security score, indicating that 66 out of 72 security vendors flagged the file as malicious. The file size is 4.64 KB, and it was last modified 3 hours ago. The analysis includes a list of security vendors and their respective detections:

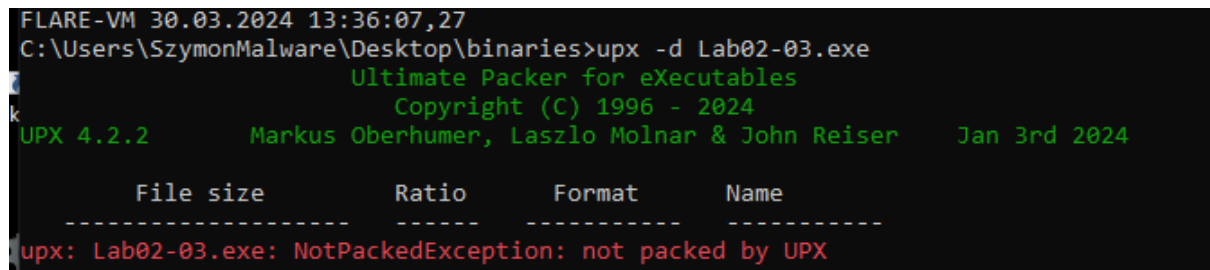
Security vendors' analysis	Detection
AhnLab-V3	Trojan.Win.Generic.R427327
Alibaba	TrojanClicker.Win32/Tnega.79cba6fb
AliCloud	Trojan:Win/Agentb.bquu
ALYac	Gen:Variant.Graftor.968808
Antiy-AVL	Trojan/Win32.SGeneric
Arcabit	Trojan.Graftor.DEC868
Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]

Sygnatura była skanowana w VirusTotal.

2)



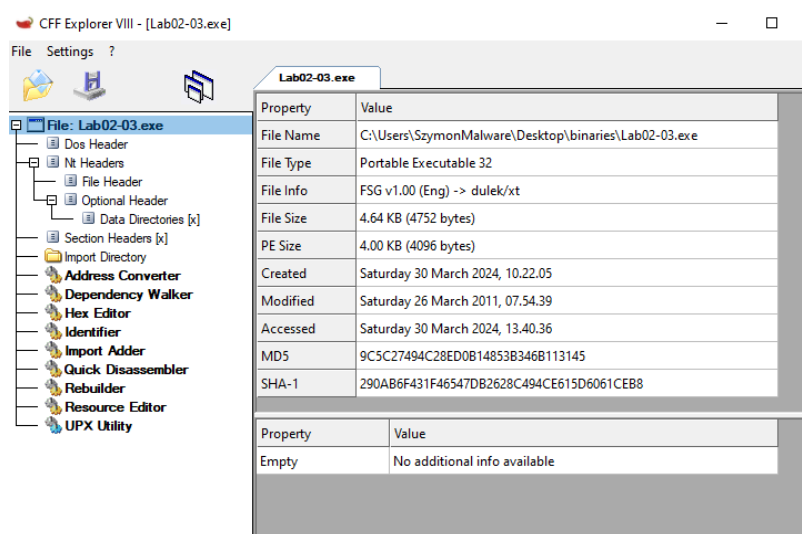
FSG 1.0->dulek/xt: Wskazuje, że plik został spakowany za pomocą kompresora FSG.



Nie mogę rozpakować go za pomocą UPX.

Plik został spakowany innym kompresorem.

3)



26.03.2011 o godz. 7:54

4)

KERNEL32.dll [2 entries]					
Call via	Name	Ordinal	Original Thunk	Thunk	Forward
5128	LoadLibraryA	-	5140	5140	-
512C	GetProcAddress	-	514E	514E	-

KERNEL32.dll

LoadLibraryA

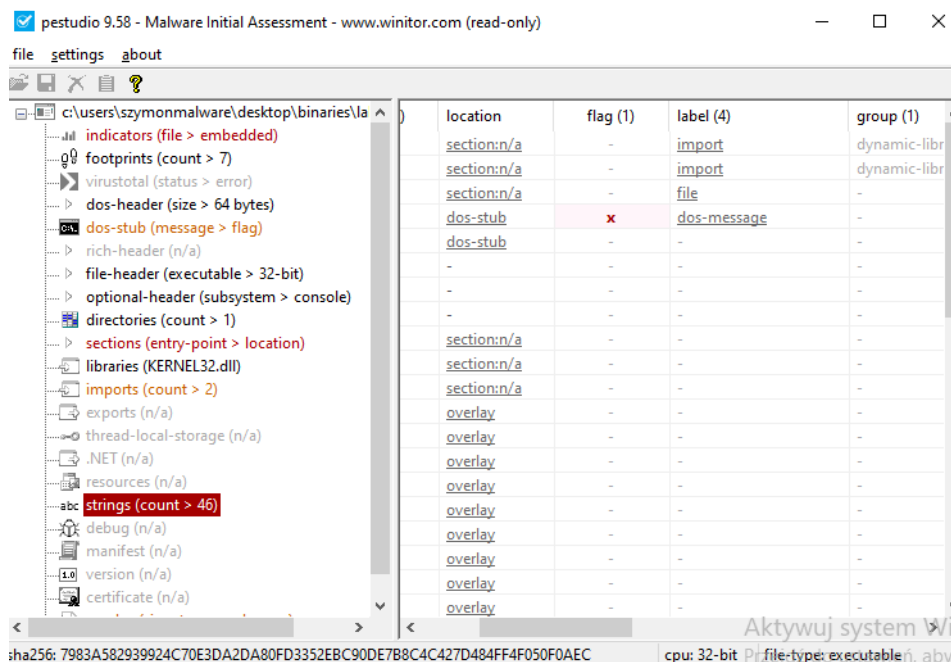
Opis: Funkcja używana do ładowania dynamicznie bibliotek DLL w trakcie działania programu.

GetProcAddress

Opis: Funkcja używana do pobierania adresu funkcji eksportowanej z określonej biblioteki DLL.

Nie będę w stanie sprawdzić funkcjonalności tego pliku, dopóki go nie rozpakuję. Skompresowany posiada za mało jawnych informacji.

5)



Nic nie udało się znaleźć. Prawdopodobnie dlatego, że plik jest skompresowany.

Próbowałem go odpakować na wiele sposobów i każda próba zakończyła się niepowodzeniem.

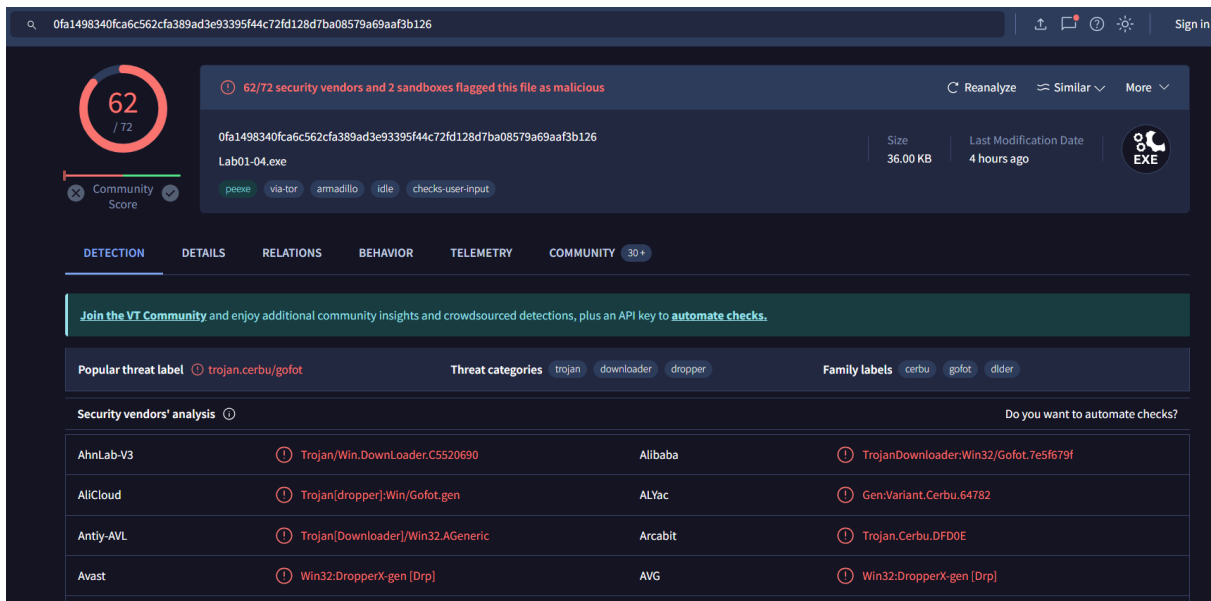
1.4

1)

Filename	MD5
Lab02-04.exe	625ac05fd47adc3c63700c3b30de79ab

MD5

625ac05fd47adc3c63700c3b30de79ab

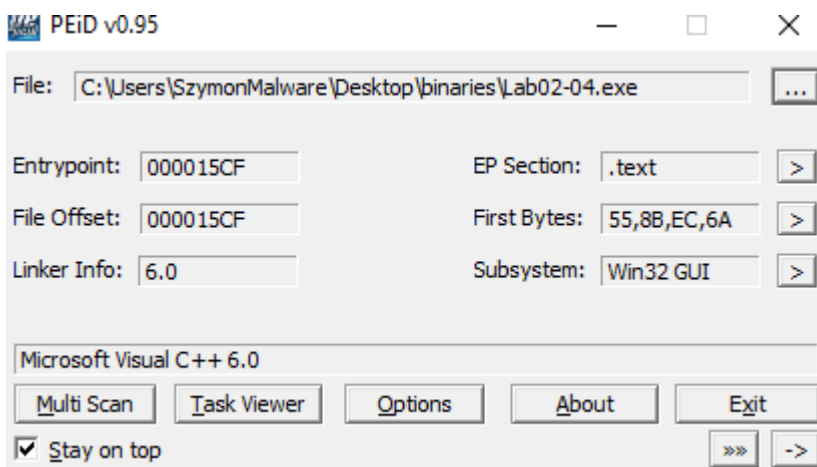


The screenshot shows the VirusTotal interface for the file Lab01-04.exe. The file's MD5 hash is 0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126. The file size is 36.00 KB and it was last modified 4 hours ago. A red circle with the number 62 indicates that 62 out of 72 security vendors and sandboxes flagged this file as malicious. The file is identified as a Trojan (Trojan.Cerbu.Gofot). The 'Security vendors' analysis' section shows that several vendors, including AhnLab-V3, AliCloud, Antiy-AVL, and Avast, have flagged the file as malicious. The file is also identified as a Trojan (Trojan.Cerbu.DFD0E).

Vendor	Detection
AhnLab-V3	Trojan.Win.DownLoader.C5520690
AliCloud	Trojan[dropper].Win/Gofot.gen
Antiy-AVL	Trojan[Downloader].Win32.AGeneric
Avast	Win32:DropperX-gen [Drp]

Był skanowany.

2)



The screenshot shows the PEiD v0.95 interface. The file being analyzed is C:\Users\Szymon\Malware\Desktop\binaries\Lab02-04.exe. The entry point is 000015CF, and the EP section is .text. The file offset is 000015CF, and the first bytes are 55,8B,EC,6A. The linker info is 6.0, and the subsystem is Win32 GUI. The file is identified as Microsoft Visual C++ 6.0. The interface includes buttons for Multi Scan, Task Viewer, Options, About, and Exit. The 'Stay on top' checkbox is checked.

Plik nie jest zaciemniony.

3)

Property	Value
File Name	C:\Users\SzymonMalware\Desktop\binaries\Lab02-04.exe
File Type	Portable Executable 32
File Info	Microsoft Visual C++
File Size	36.00 KB (36864 bytes)
PE Size	36.00 KB (36864 bytes)
Created	Saturday 30 March 2024, 10.22.05
Modified	Tuesday 05 July 2011, 18.16.15
Accessed	Saturday 30 March 2024, 13.54.24
MD5	625AC05FD47ADC3C63700C3B30DE79AB
SHA-1	9369D80106DD245938996E245340A3C6F17587FE

Property	Value
Empty	No additional info available

5.07.2011 godz. 18:16

4)

Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwar
20A4	KERNEL32.dll	16	FALSE	2104	0	0
20B8	ADVAPI32.dll	3	FALSE	20F4	0	0
20CC	MSVCRT.dll	15	FALSE	2148	0	0

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hin
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

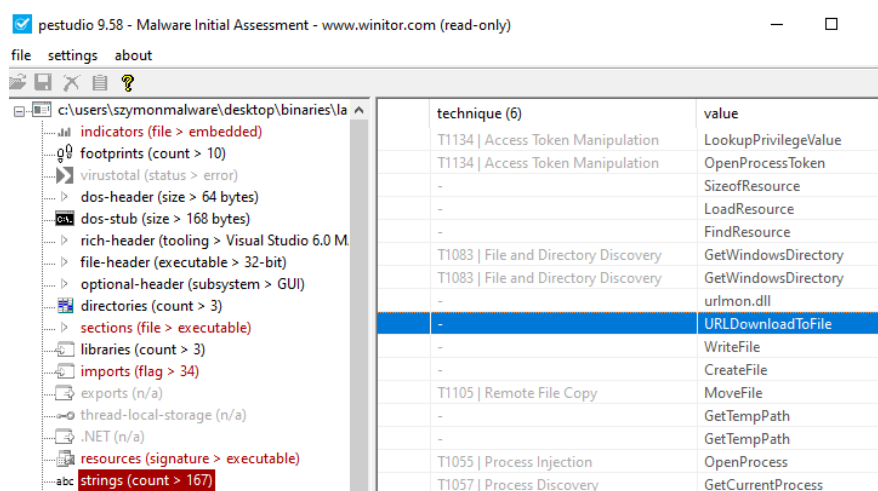
Możliwe funkcje szkodliwego oprogramowania:

- Uruchamianie nowych procesów (WinExec)
- Uruchamianie innych szkodliwych plików lub komponentów.
- Manipulacja plikami (WriteFile, CreateFileA)
- Zapisywanie lub tworzenie plików na dysku, np. logów, konfiguracji czy plików wynikowych.
- Iniekcja kodu w zdalne procesy (CreateRemoteThread)
- Wstrzykiwanie kodu do innych procesów w celu ukrycia aktywności lub wykonania szkodliwych operacji.
- Ładowanie dynamicznych bibliotek DLL (LoadLibraryA, GetProcAddress)
- Dynamiczne ładowanie dodatkowych modułów z kodem szkodliwym.
- Obsługa wyjątków (XcptFilter)
- Może być używane do obsługi błędów i unikania detekcji.
- Zakończenie procesu (_exit, exit)
- Zakończenie procesu w celu ukrycia aktywności lub po zakończeniu działania szkodliwego kodu.
- Inicjalizacja środowiska i tablic globalnych

Możliwe typy malware:

- Trojan - Złośliwe oprogramowanie udające inną, często nieszkodliwą aplikację.
- Ransomware - Oprogramowanie szantażujące użytkownika, blokujące dostęp do systemu lub szyfrujące pliki w celu żądania okupu.
- Backdoor - Oprogramowanie pozwalające na zdalny dostęp do komputera i umożliwiające jego kontrolę przez cyberprzestępcę.

5)



Udało znaleźć się funkcję URLDownloadToFile.

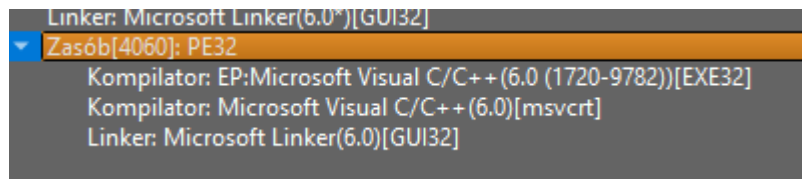
Jest często używana w programach napisanych w języku C++ do pobierania plików z Internetu i zapisywania ich na dysku.

6)

208C _stricmp - 23C6 23C6 -

Wydaje się, że tak.

7)



Zasób [4060]: PE32

Znaczenie: Plik wykonywalny używa formatu PE32, który jest standardowym formatem plików wykonywalnych dla systemu Windows. Jest to odpowiedni i prawidłowy typ pliku.

Kompilator: Microsoft Visual C/C++ (6.0)

Znaczenie: Plik został stworzony za pomocą programu Microsoft Visual C/C++ w wersji 6.0. To jest narzędzie, które użyto do napisania i kompilacji programu.

Linker: Microsoft Linker (6.0)

Znaczenie: Plik został połączony (zlinkowany) z użyciem programu Microsoft Linker w wersji 6.0. To jest proces łączenia różnych części programu w jedną całość.

EP: Microsoft Visual C/C++ (6.0)

Znaczenie: Punktem wejścia do programu (miejsce, od którego zaczyna się wykonywanie programu) jest kod stworzony przez kompilator Microsoft Visual C/C++ w wersji 6.0.

Kompilator: Microsoft Visual C/C++ (6.0) [msvcrt]

Znaczenie: Plik korzysta z biblioteki standardowej języka C/C++ (MSVCRT), która jest częścią kompilatora Microsoft Visual C/C++ w wersji 6.0.

Linker: Microsoft Linker (6.0) [GUI32]

Znaczenie: Połączenie (linkowanie) pliku zostało wykonane w trybie graficznym (GUI) przy użyciu programu Microsoft Linker w wersji 6.0.