Kraków, 28.03.23

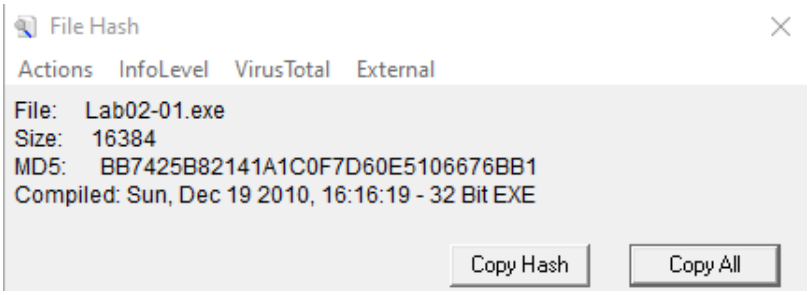
Laboratorium 2 - Analiza Statyczna

Julia Sadecka, Cyberbezpieczeństwo

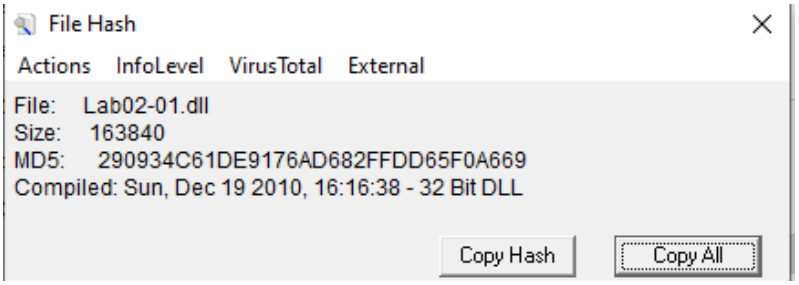
Laboratorium 1.1

1. Hash i VirusTotal

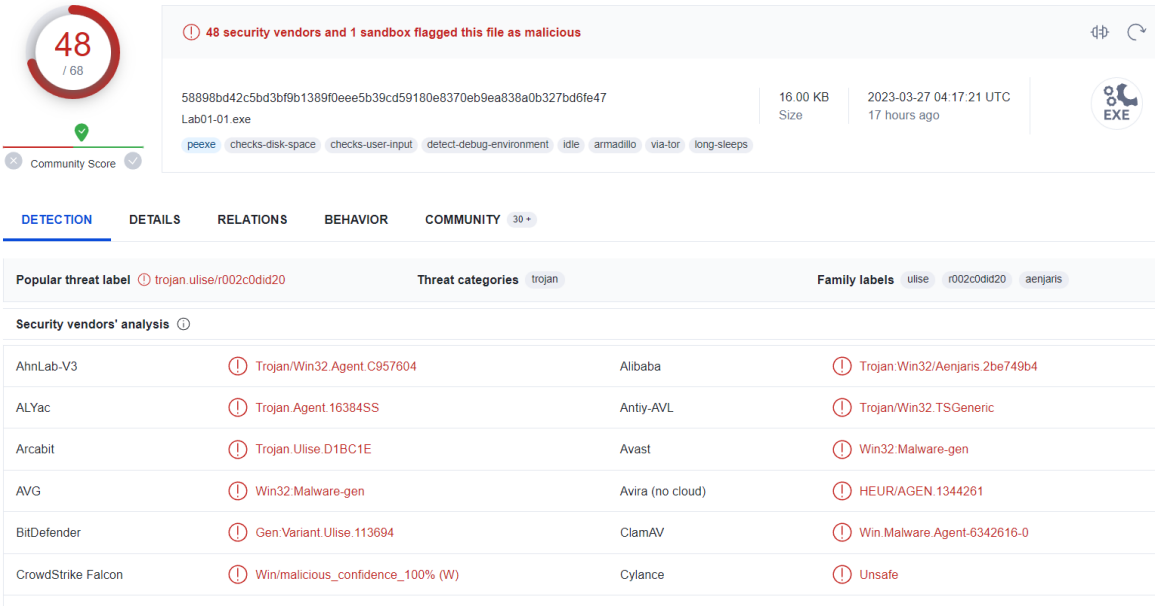
Wyciągnięty hash z programu Md5 Hash dał taki rezultat dla pliku .exe:



a taki dla pliku .dll

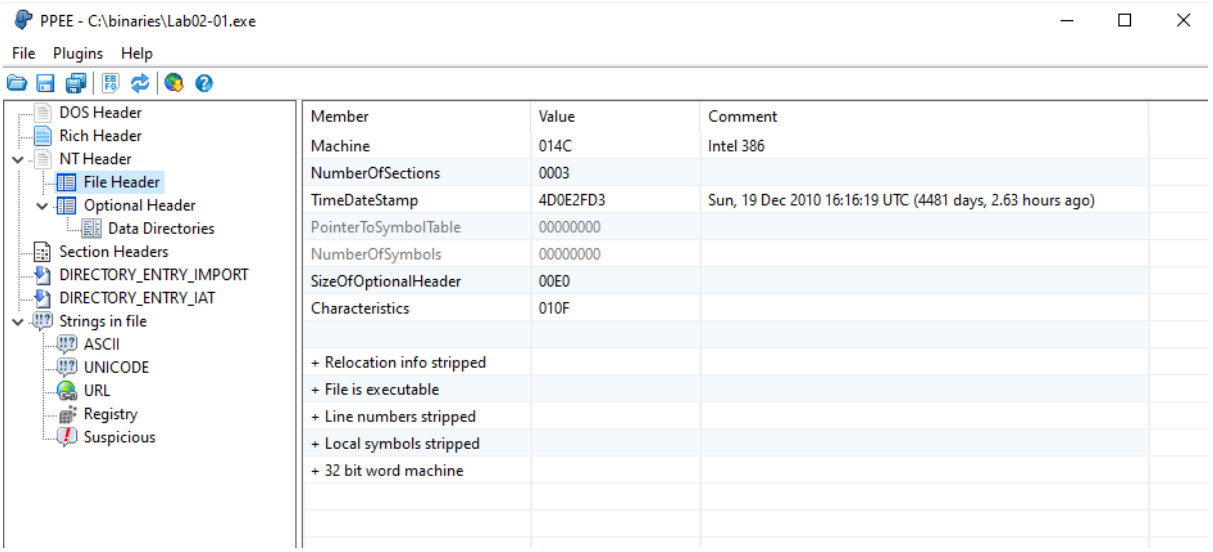


Gdy wrzuciłam hash na stronę VirusTotal.com wyskoczył komunikat, że jest to plik typu trojan. Był on oznaczony 48/69 razy jako wirus.



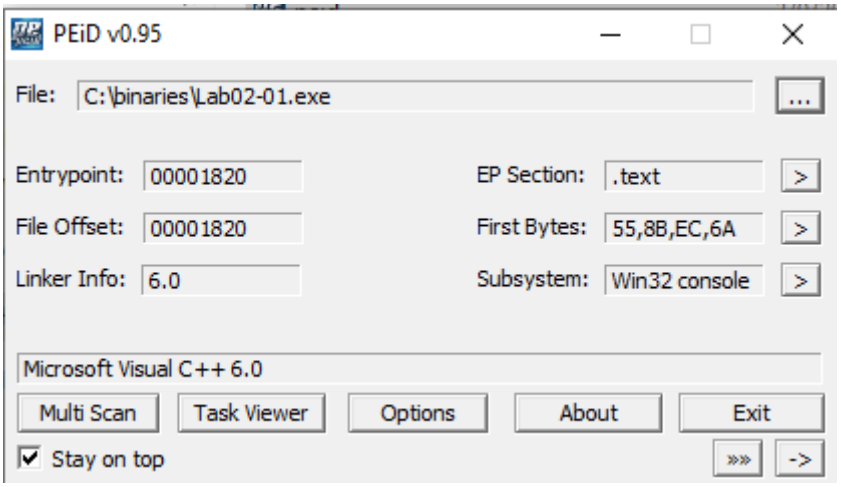
2. Data kompilacji

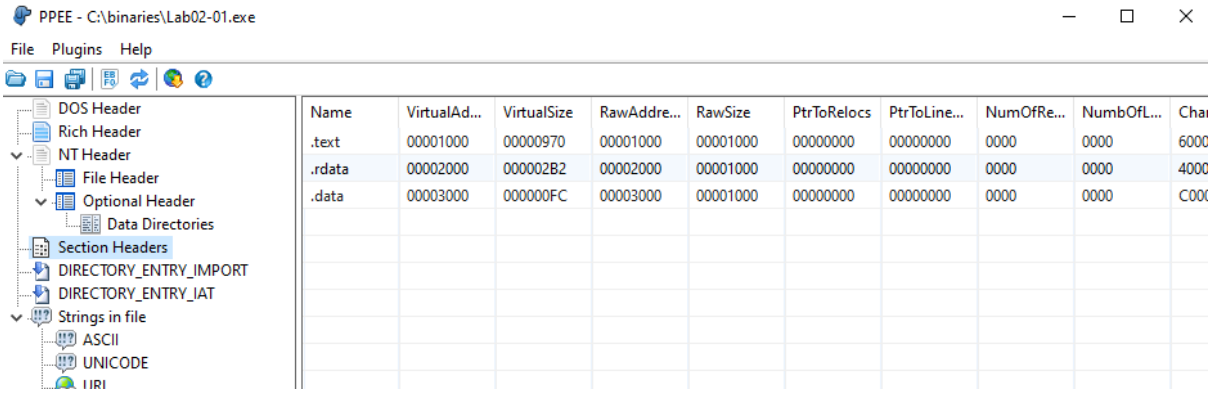
Program był skompilowany 19 Grudnia 2010. Mówi o tym TimeDateStamp.



3. Spakowanie i zaciemnienie

Program po wrzuceniu do PEiD dał rezultat : Microsoft Visual C ++ 6.0 co oznacza, że nie jest spakowany. Plik nie jest także zaciemniony, ponieważ w Section Header (program PPEE) posiada typowe sekcje dla programu PE.





4. Biblioteki

Plik Lab02-01.dll posiada takie biblioteki:

- KERNEL32.dll - biblioteka DLL zawierająca funkcje systemowe używane przez wiele aplikacji w systemie Windows. Zawiera między innymi funkcje służące do zarządzania procesami, pamięcią, plikami, mutexami i wątkami.
  - CloseHandle
  - **CreateMutexA** (Tworzy obiekt wzajemnego wykluczania, który może być wykorzystany przez złośliwe oprogramowanie, aby to zapewnić w danym momencie w systemie działa np. tylko jeden proces.)
  - **CreateProcessA** (Tworzy nowy proces w programie)
  - OpenMutexA
  - Sleep
  - **CreateFileA** (Tworzy lub otwiera istniejący dokument)
  - FindFirstFileA i FindNextFileA (przeszukuje katalogi)
- MSVCRT.dll - standardowa biblioteka C

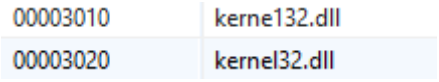
- _adjust_fdiv
- _initterm
- free
- malloc
- strncmp

- WS2_32.dll - bibliotekę tą wykorzystujemy do tworzenia API (interfejsu programistycznego) dla aplikacji sieciowych. Zawiera między innymi funkcje służące do tworzenia i zarządzania gniazdami sieciowymi, nawiązywania połączeń sieciowych i przesyłania danych przez sieć.

  Funkcje, które są wykorzystywane:
  - closesocket
  - **connect** (służy do połączenia zdalnego, używane jest przez złośliwe oprogramowanie aby połączyć się z serwerami
  - htons
  - **inet_addr** (konwertuje ciąg adresu IP, aby mógł być używany przez funkcje takie jak connect.)
  - recv
  - send
  - shutdown
  - socket
  - WSACleanup
  - **WSAStartup** (służy do inicjowania funkcji sieciowych niskiego poziomu.)

6. Podobne rekordy

Istnieją dwa podobne rekordy kernel32.dll i kerne132.dll. Może to świadczyć o tym, że ten pierwszy jest poprawną ścieżką dostępową do biblioteki, a drugi jest potencjalnie podejrzany o bycie niebezpieczny. Próbuje się on zamaskować przez zamianę podobny znaków “l” na “1”



7. Połączenie z Internetem

W jednym z rekordów jest wpisany adres IP co może sugerować komunikację internetową
dodatkowo jest wykorzystywana biblioteka WS2_32.dll, która też służy do aplikacji sieciowych.

00026028	127.26.152.13
0000215C	WS2_32.dll

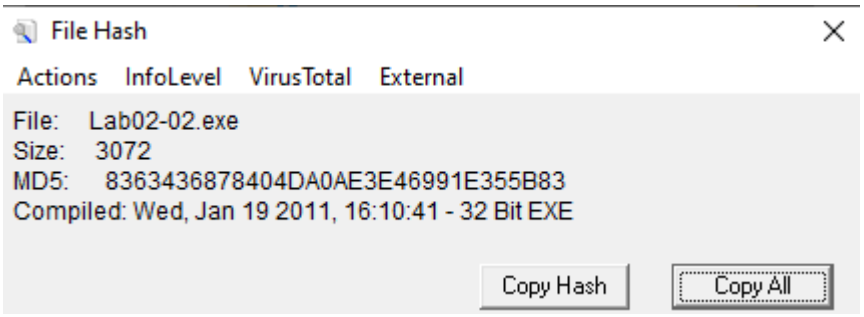
8. Podsumowanie

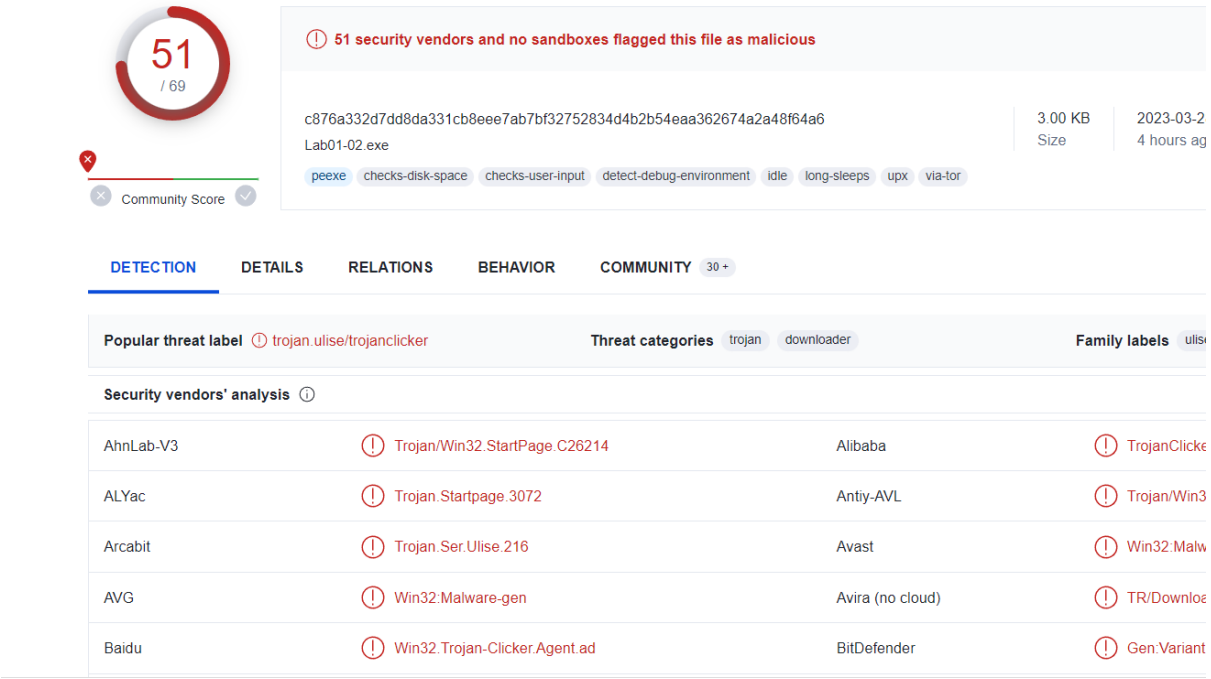
Posiadając aktualne informacje nie mogę do końca stwierdzić jak działają analizowane pliki. Można przypuszczać, że komunikują się z jakimś zewnętrznym serwerem (wykorzystanie biblioteki WS2_32.dll). Można też pomyśleć, że analizują drzewo plików wewnętrznych w systemie użytkownika (użycie funkcji FindNextFileA)

Laboratorium 1.2

1. Hash i VirusTotal

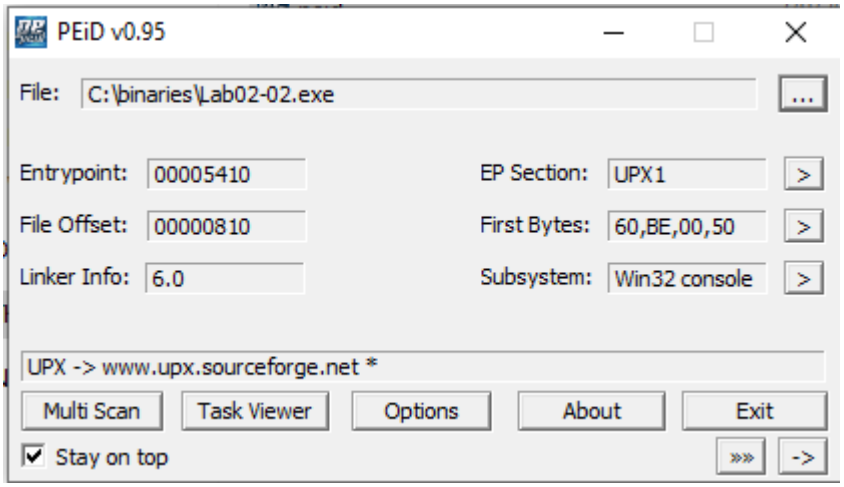
Po wyciągnięciu hashu aplikacją Md5 Hash i przepisaniu go na VirusTotal, wirusa wykryło 51/69 antywirusów i był wcześniej analizowany.





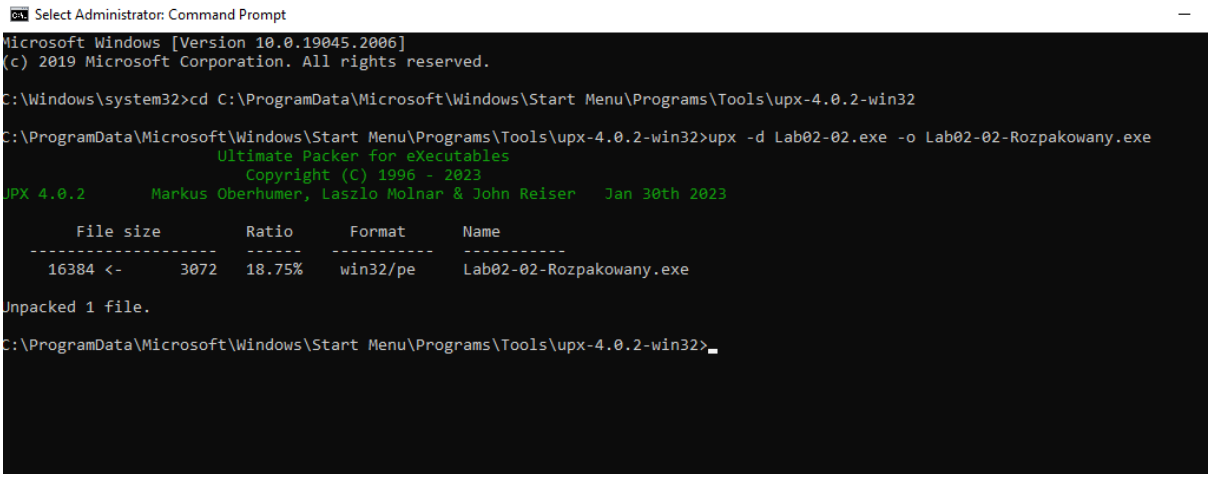
2. Spakowanie i zaciemnienie

Komunikat UPX świadczy o tym, że plik jest spakowany. Plik jest także zaciemniony, widać to po nagłówkach w programie PPEE w Section Header w kolorze pomarańczowym i nietypowych nazwach (UPX0, UPX1, UPX2), które świadczą o zaciemnieniu.



Name	VirtualAd...	VirtualSize	RawAddre...	RawSize	PtrToRelocs	PtrToLine...	NumOfRe...	NumbO
UPX0	00001000	00004000	00000400	00000000	00000000	00000000	0000	0000
UPX1	00005000	00001000	00000400	00000600	00000000	00000000	0000	0000
UPX2	00006000	00001000	00000A00	00000200	00000000	00000000	0000	0000

Plik został rozpakowany za pomocą UPX.



3. Biblioteki

Po rozpakowaniu ukazały się takie same biblioteki jak wcześniej, jednak różniły się one ilością funkcji, ale także różniły się funkcje w obu tych bibliotekach.

- KERNEL32.DLL (przed rozpakowaniem: 6, po: 9)
  - **GetModuleFileName** (zwraca nazwę modułu, który obecnie działa)
  - **GetProcAddress** (pobiera adres funkcji z biblioteki DLL załadowanej do pamięci)
- ADVAPI32.dll (przed: 1, po: 3)
  - **CreateServiceA** (tworzy usługę, którą można uruchomić podczas rozruchu systemu)
  - **StartServiceCtrlDispatcherA** (używana przez usługę do połączenia głównego wątku procesu z menadżerem kontroli usług - dzięki temu dowiadujemy się, że dana funkcja zostanie uruchomiona jako usługa)
  - **OpenSCManagerA** (Otwiera uchwyt do menadżera kontroli usług)
- MSVCRT.dll (przed tylko 1, po: 13)
- WINNET.dll (przed: 1, po 2)
  - **InternetOpenUrlA** (inicjuje funkcje dostępu do Internetu)
  - **InternetOpenA**

4. Połączenia z Internetem

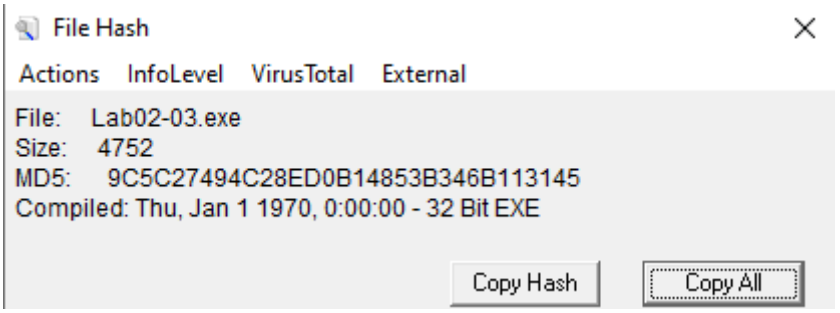
W stringach znalazłam adres URL do strony http://www.malwareanalysisbook.com, a także odnośnik do Internet Explorer 8.0

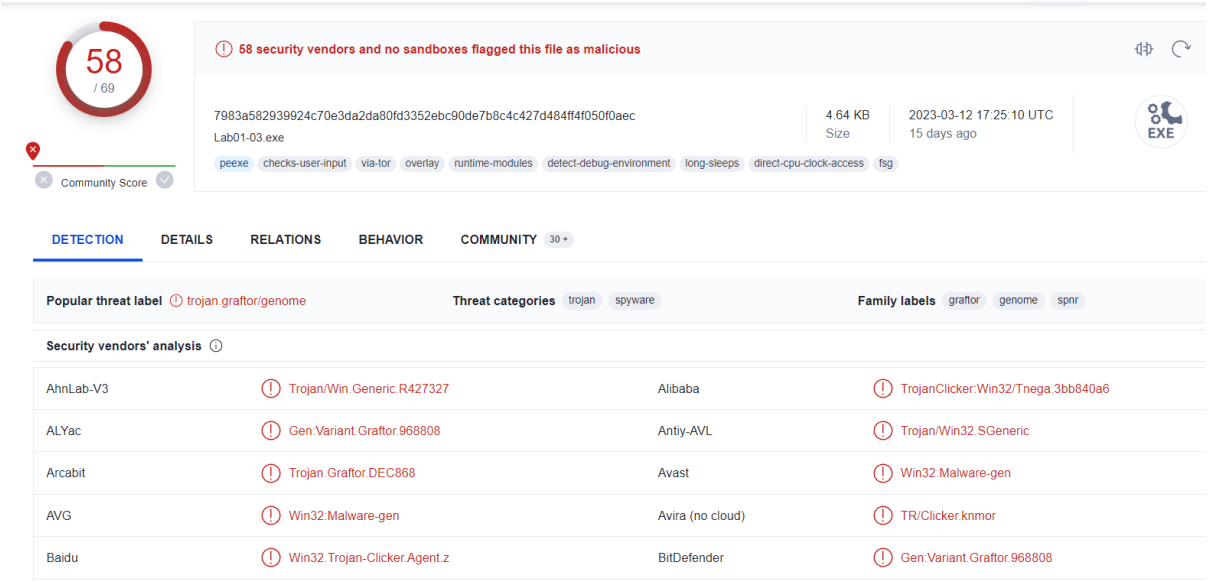
00003030	http://www.malwareanalysisbook.com
00003054	Internet Explorer 8.0

Laboratorium 1.3

1. Hash i VirusTotal

Po wyciągnięciu hashu aplikacją Md5 Hash i przepisaniu go na VirusTotal, wirusa wykryło 58/69 antywirusów i był wcześniej analizowany.

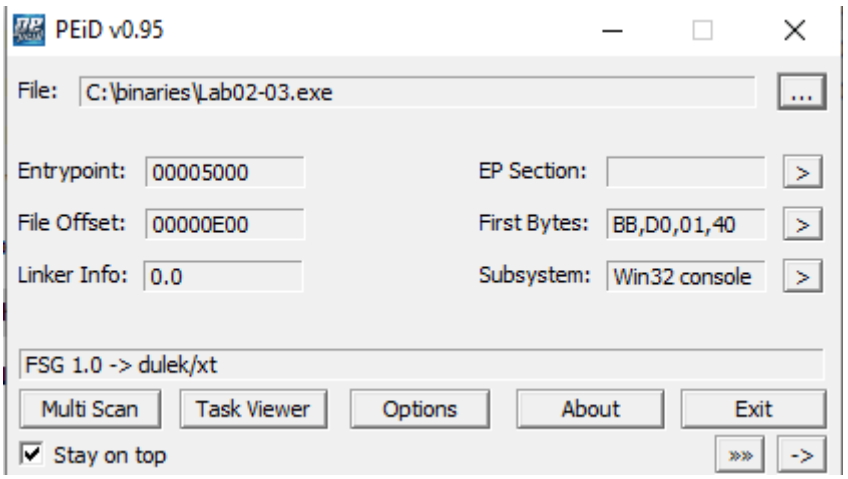




2. Spakowanie i zaciemnienie

Po wrzuceniu pliku do PEiD wyskoczyła informacja FSG 1.0, która oznacza, że plik został zaciemniony. FSG to jeden z wielu programów stosowanych do zaciemniania plików, który używa techniki deobfuskacji, aby ukryć oryginalny kod programu. Po nagłówkach z PPEE też możemy wywnioskować, że program jest zaciemniony.

Programu nie da się rozpakować przy pomocy UPX, ponieważ został on spakowany za pomocą FSG i nie został spakowany za pomocą UPX.



Name	VirtualAd...	VirtualSize	RawAddre...	RawSize	PtrToRelocs	PtrToLine...	NumOfRe...	Numb(
	00001000	00003000	00000000	00000000	00000000	00000000	0000	0000
	00004000	00001000	00001000	0000028C	00000000	00000000	0000	0000
	00005000	00001000	00000E00	00000200	00000000	00000000	0000	0000

3. Data

Daty pliku nie da się stwierdzić, w TimeData Stamp wyskakuje data 1 stycznia 1970 co jest “dniem zerowym” w informatyce czyli datą od której liczymy liczbę sekund w komputerach czy telefonach.

TimeDateStamp	00000000	Thu, 01 Jan 1970 00:00:00 UTC (19444 days, 22.65 hours ago)

4. Importy plików

Podczas przeszukiwania importów do bibliotek znalazłam tylko bibliotkę KERNEL32.dll razem z funkcjami LoadLibraryA i GetProcAddress. Sądzę, że gdyby rozpakować plik byłoby ich więcej.

00000F34	KERNEL32.dll
00000F42	LoadLibraryA
00000F50	GetProcAddress

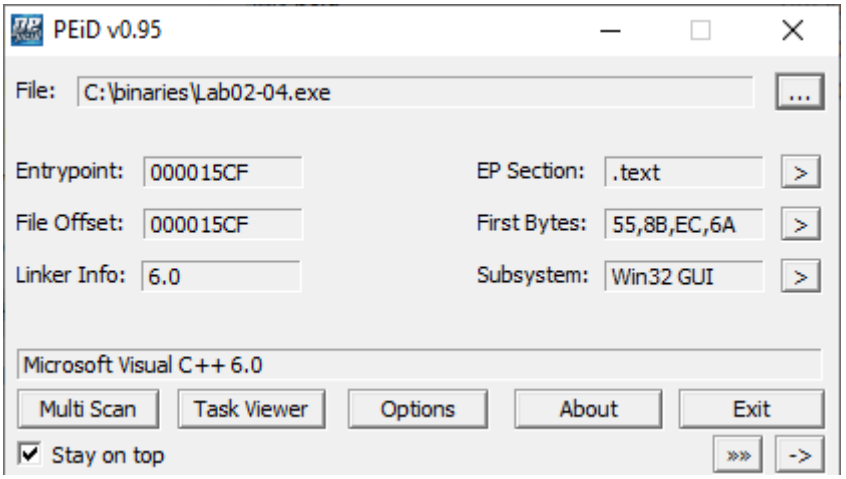
5. Komunikacja internetowa

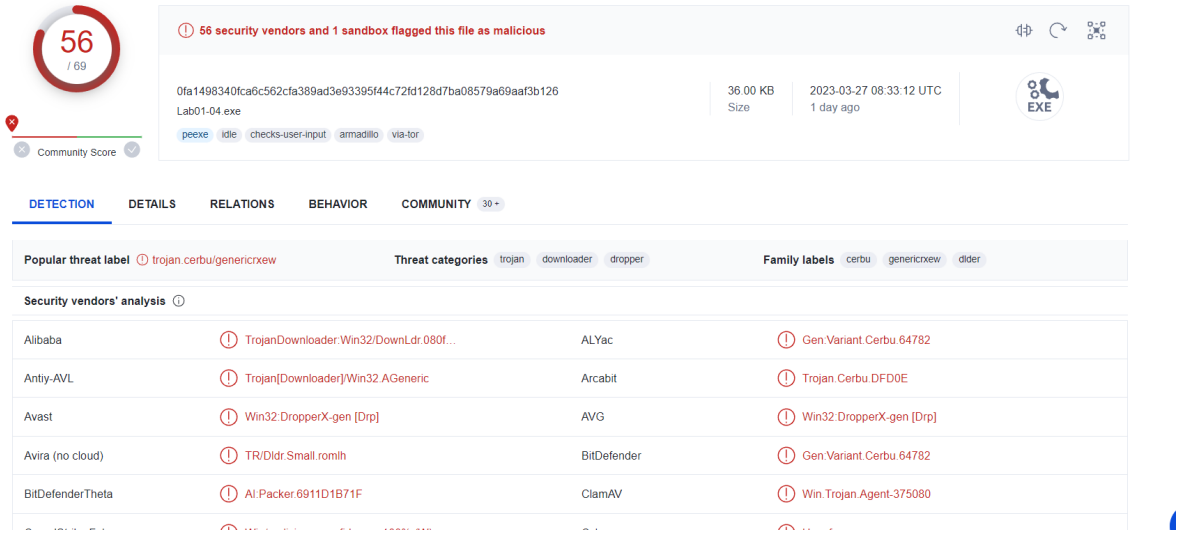
Nie znalazłam w stringach żadnych informacji świadczących o połączeniu z internetem. Możliwe, że są ukryte z tego względu, że plik jest spakowany.

Laboratorium 1.4

1. Hash i VirusTotal

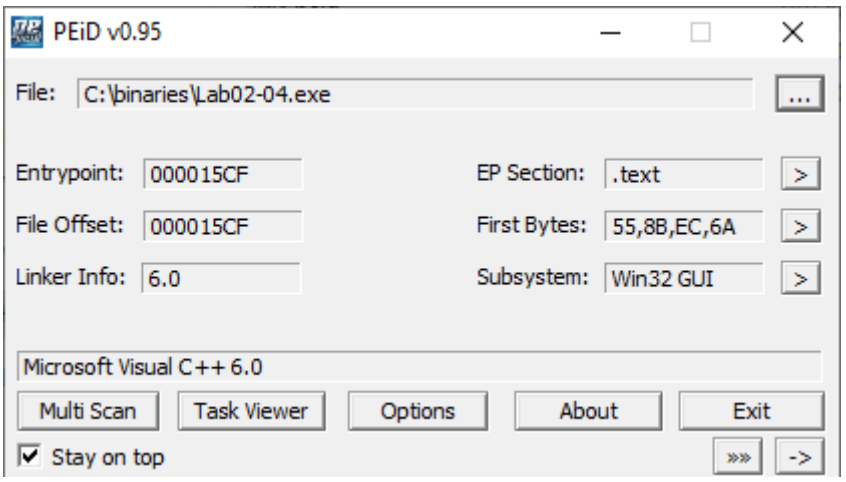
Po wyciągnięciu hashu aplikacją Md5 Hash i przepisaniu go na VirusTotal, wirusa wykryło 56/69 antywirusów i był wcześniej analizowany.





2. Spakowanie i zaciemnienie

Nic nie świadczy o tym, że plik jest spakowany czy zaciemniony. Po wrzucenu do PEiD wyskakuje, że jest to zwykły plik PE, a w “Section Headers” występują nagłówki typowe dla programu PE.



Name	VirtualAd...	VirtualSize	RawAddre...	RawSize	PtrToRelocs	PtrToLine...	NumOfRe...	Num
.text	00001000	00000720	00001000	00001000	00000000	00000000	0000	0000
.rdata	00002000	000003D2	00002000	00001000	00000000	00000000	0000	0000
.data	00003000	0000014C	00003000	00001000	00000000	00000000	0000	0000
.rsrc	00004000	00004060	00004000	00005000	00000000	00000000	0000	0000

3. Data kompilacji

Program był skompilowany 30 sierpnia 2019

NumberOfSections	0004	
TimeDateStamp	5D69A2B3	Fri, 30 Aug 2019 22:26:59 UTC (1305 days, 0.72 hours ago)
PointerToSymbolTable	00000000	
NumberOfSymbols	00000000	

4. Biblioteki

Można poznać funkcjonalność tego pliku tak samo jak w laboratorium 1.1.

Występują w nim takie biblioteki jak:

- **KERNEL32.dll** (opis w lab 1.1)
- **ADVAPI32.dll** (biblioteka ta zawiera funkcje systemowe związane z bezpieczeństwem, takie jak uwierzytelnianie, kontrola dostępu, szyfrowanie i deszyfrowanie danych. Złośliwe oprogramowanie może próbować wykorzystać niektóre z tych funkcji, aby uzyskać dostęp do systemu lub ukryć swoje działania przed użytkownikiem)
- **MSVCRT.dll** (opis w lab 1.1)

Name RVA	Name	OriginalFirstThunk	TimeDate Stamp	ForwarderChain	FirstThunk	Description (Read from file)
0000228E	KERNEL32.dll	00002104	00000000	00000000	00002010	Windows NT BASE API Client DLL
000022E0	ADVAPI32.dll	000020F4	00000000	00000000	00002000	Advanced Windows 32 Base API
000022FA	MSVCRT.dll	00002148	00000000	00000000	00002054	Windows NT CRT DLL

Type to filter...

OFT	FT	Hint	Name	Ordinal
000022CC	000022CC	0142	OpenProcessToken	
000022B4	000022B4	00F5	LookupPrivilegeValueA	
0000229C	0000229C	0017	AdjustTokenPrivileges	

5, 6. Połączenia z Internetem

Przy przeszukaniu stringów odnalazłam string z adresem malwareanalysis.com/updater.exe, które mogą świadczyć o połączeniu z Internetem.
Jest także string URLDownloadToFileA, która nie była wyświetlona jako funkcja importowana z żadnej z tych trzech bibliotek. Funkcja ta służy do pobierania pliku z serwisu internetowego i zapisywania go na dysk.

Offset	Type	Strings found
000070B8	ASCII	malwareanalysis.com/updater.exe
00003010	ASCII	winlogon.exe

000061AA	URLDownloadToFileA

W zakładce “Suspicious” znajduje się także podejrzany string winlogon.exe. Jest to proces systemowy w systemie operacyjnym Windows, który jest odpowiedzialny za proces uwierzytelniania i logowania użytkowników. Proces ten jest uruchamiany zaraz po uruchomieniu systemu i działa przez cały czas, w którym użytkownik jest zalogowany.Winlogon.exe monitoruje proces logowania użytkownika i reaguje na zdarzenia związane z uwierzytelnianiem, takie jak

wprowadzanie hasła, wybór konta użytkownika czy wybór innych opcji logowania. Wirusy mogą go wykorzystywać w taki sposób, że gdy wirus przeniknie do systemu, tworzy plik winlogon.exe i zaczyna go używać np. do uruchamiania samego siebie.