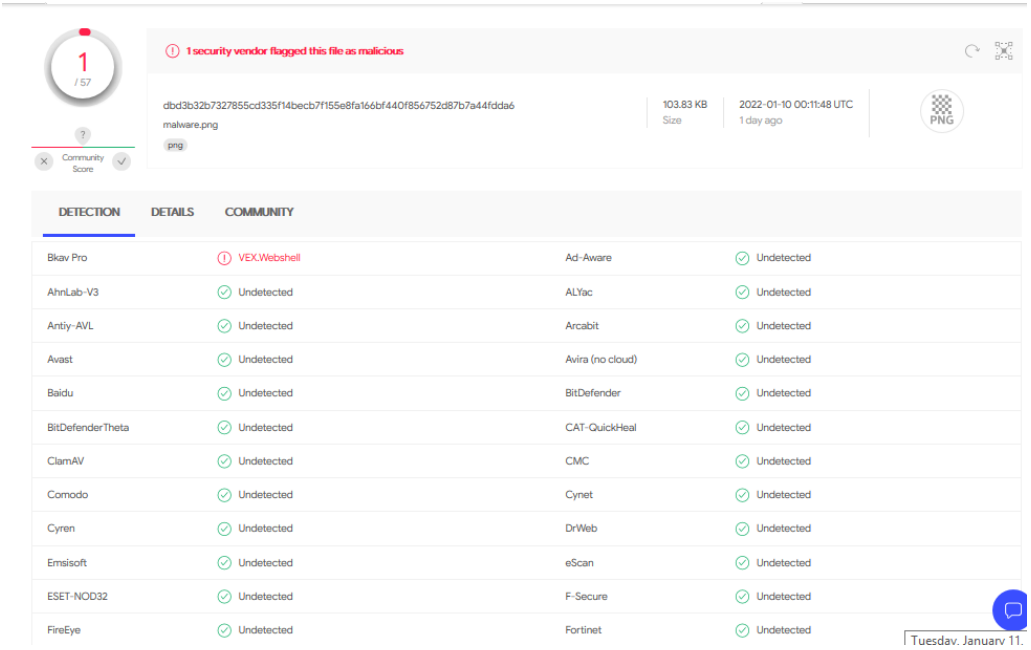
1.

a) nu s-a observat nimic suspicios, nu a aparut nicio eroare

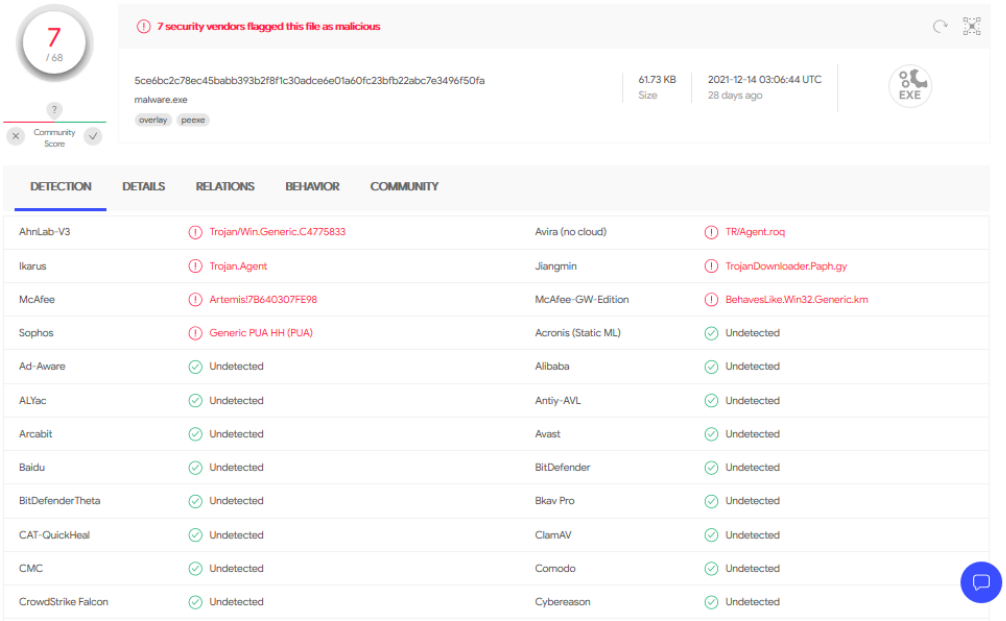
b) se observa flag-uri de compilator

```
00013480  00 02 2F C5 37 00 00 03 35 38 00 00 66 5F 5F 64  ../Å7...58..f__d
00013490  69 72 00 02 2F BF 37 00 00 00 67 6F 70 65 6E 64  ir../¿7...gopend
000134A0  69 72 00 02 2B BF 37 00 00 03 66 5F 5F 64 69 72  ir..+¿7...f__dir
000134B0  6E 61 6D 65 00 02 2B F3 1E 00 00 00 00 A3 00 00  name..+ó.....£..
000134C0  00 02 00 F0 05 00 00 04 01 FE 03 00 00 60 22 40  ...ð.....þ...`"@
000134D0  00 8A 22 40 00 2E 2E 2F 2E 2E 2F 2E 2E 2F 73 72  .Š"@.../../../sr
000134E0  63 2F 67 63 63 2D 36 2E 33 2E 30 2F 6C 69 62 67  c/gcc-6.3.0/libg
000134F0  63 63 2F 63 6F 6E 66 69 67 2F 69 33 38 36 2F 63  cc/config/i386/c
00013500  79 67 77 69 6E 2E 53 00 2F 68 6F 6D 65 2F 6B 65  ygwin.S./home/ke
00013510  69 74 68 2F 73 72 63 2F 6D 69 6E 67 77 2F 67 63  ith/src/mingw/gc
00013520  63 2D 62 75 69 6C 64 2F 67 63 63 2D 36 2E 33 2E  c-build/gcc-6.3.
00013530  30 2D 6D 69 6E 67 77 33 32 2D 63 72 6F 73 73 2D  0-mingw32-cross-
00013540  6E 61 74 69 76 65 2F 6D 69 6E 67 77 33 32 2F 6C  native/mingw32/l
00013550  69 62 67 63 63 00 47 4E 55 20 41 53 20 32 2E 32  ibgcc.GNU AS 2.2
00013560  38 00 01 80 54 1C 00 00 04 00 04 06 00 00 04 01  8..€T...........
00013570  47 4E 55 20 43 31 31 20 36 2E 33 2E 30 20 2D 6D  GNU C11 6.3.0 -m
00013580  74 75 6E 65 3D 67 65 6E 65 72 69 63 20 2D 6D 61  tune=generic -ma
00013590  72 63 68 3D 69 35 38 36 20 2D 67 20 2D 67 20 2D  rch=i586 -g -g -
```

c)



d) executabilele incep cu MZ asa ca am extras continutul incepand cu acel MZ



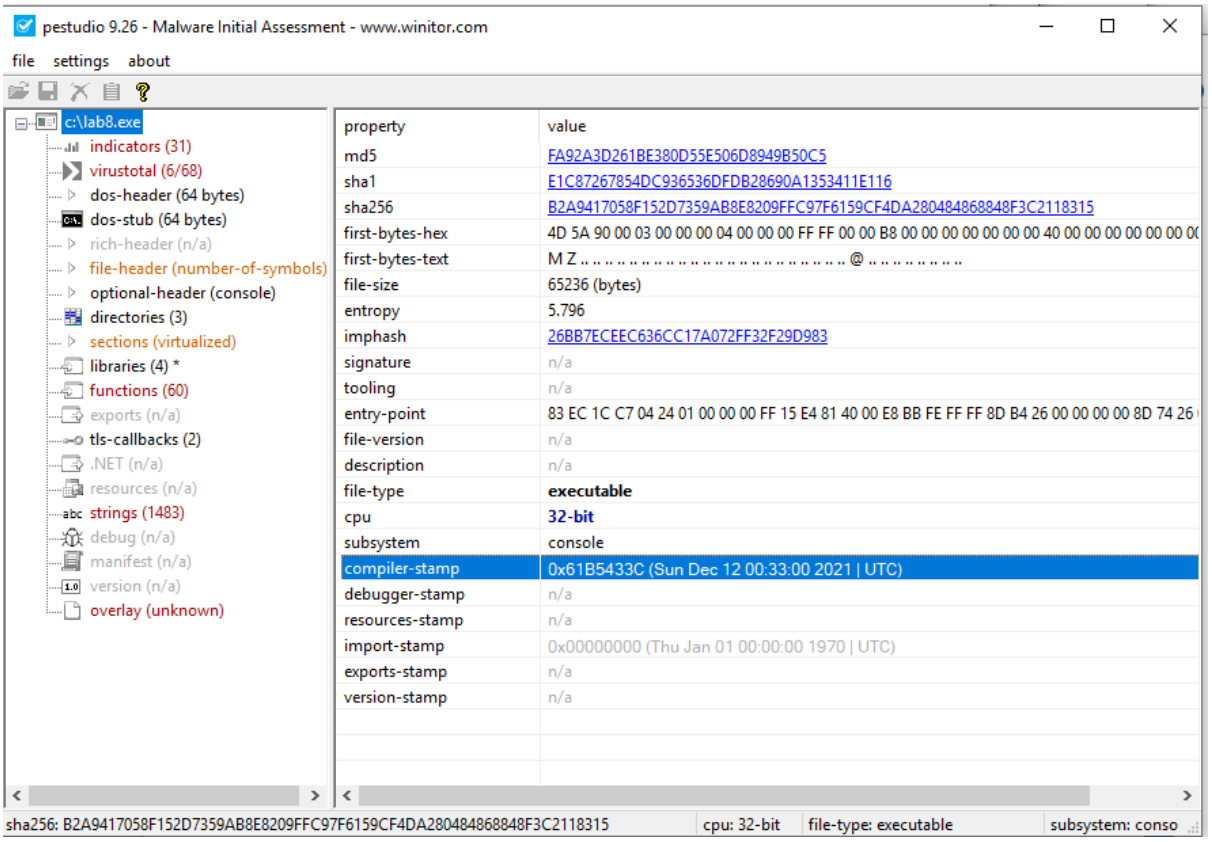
e) toate signaturile fisierelor incep cu MZ si sunt executabile deci am folosit acest lucru pentru a extrage executabilul pentru subpunctul d

f) daca executabilul este rulat intr-un fisier ce contine pdf uri, acestea vor fi sterse, deci se poate considera ca imaginea este malware

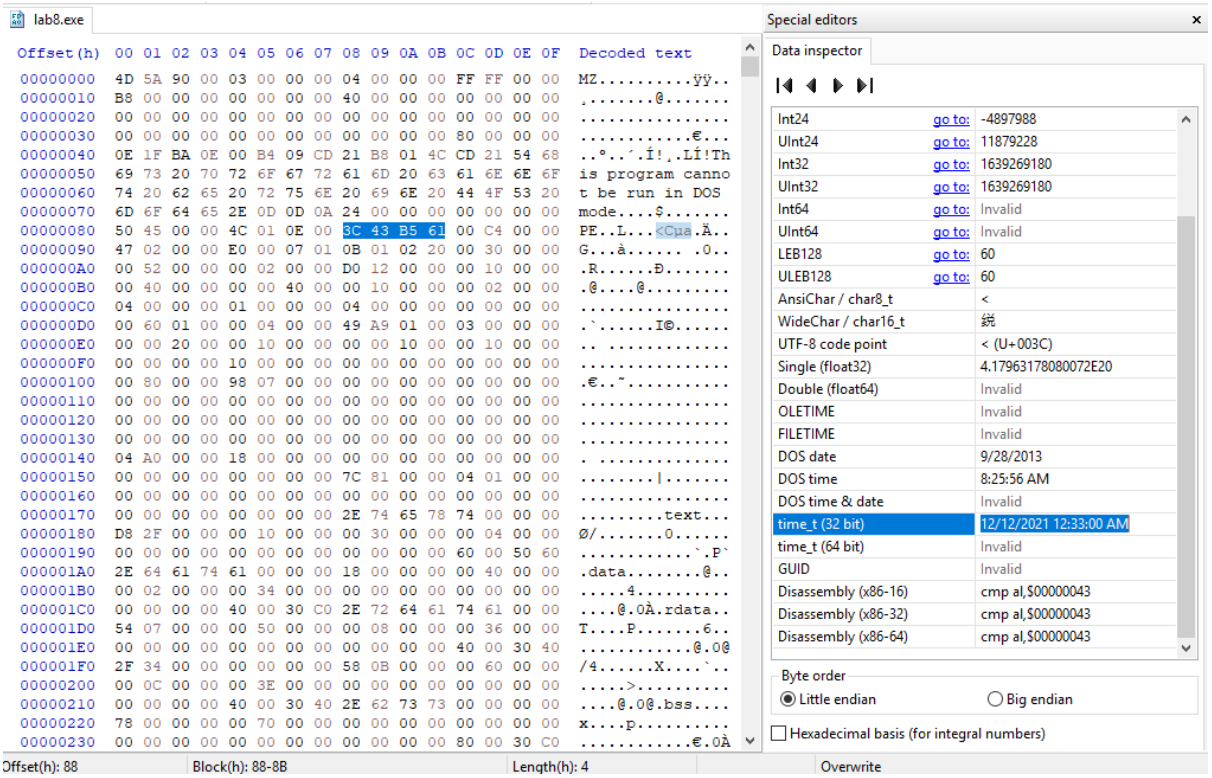
2. -> daca parola este mai lunga de 7 caractere atunci va aparea eroarea de tip buffer overflow
   -> daca parola are 14 caractere si este formata din 2 substringuri identice (Ex: fmiSSI1fmiSSI1) atunci va aparea mesajul parola corecta
3.

```
import json
import hashlib
import requests


f1 = open("ex3_file", "rb")
f2 = open("data.json", "w", encoding="utf-8")


def sha256_file():
    sha256_hash = hashlib.sha256()
    for block in iter(lambda: f1.read(4096), b""):
        sha256_hash.update(block)
    return sha256_hash.hexdigest()


def virustotal_api(sha256_file_key):
    url = 'https://www.virustotal.com/vtapi/v2/file/report'
    params = {'apikey':
'b2d70c91321acc48d9953037fe31ec17972cf88c0615f1737d247232f7cd96ba',
'resource': sha256_file_key}
    response = requests.get(url, params=params)
    json.dump(response.json(), f2, ensure_ascii=False, indent=2)


sha256_file_key = sha256_file()
print(sha256_file_key)
virustotal_api(sha256_file_key)

f1.close()
f2.close()
```

4. -> data la care a fost compilat binarul


pestudio 9.26 - Malware Initial Assessment - www.winitor.com
file settings about
c:\lab8.exe
indicators (31)
virustotal (6/68)
dos-header (64 bytes)
dos-stub (64 bytes)
rich-header (n/a)
file-header (number-of-symbols)
optional-header (console)
directories (3)
sections (virtualized)
libraries (4) *
functions (60)
exports (n/a)
tls-callbacks (2)
.NET (n/a)
resources (n/a)
strings (1483)
debug (n/a)
manifest (n/a)
version (n/a)
overlay (unknown)
property value
md5 FA92A3D261BE380D55E506D8949B50C5
sha1 E1C87267854DC936536DFDB28690A1353411E116
sha256 B2A9417058F152D7359AB8E8209FFC97F6159CF4DA280484868848F3C2118315
first-bytes-hex 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text M Z @
file-size 65236 (bytes)
entropy 5.796
imphash 26BB7ECEEC636CC17A072FF32F29D983
signature n/a
tooling n/a
entry-point 83 EC 1C C7 04 24 01 00 00 00 FF 15 E4 81 40 00 E8 BB FE FF FF 8D B4 26 00 00 00 00 8D 74 26
file-version n/a
description n/a
file-type executable
cpu 32-bit
subsystem console
compiler-stamp 0x61B5433C (Sun Dec 12 00:33:00 2021 | UTC)
debugger-stamp n/a
resources-stamp n/a
import-stamp 0x00000000 (Thu Jan 01 00:00:00 1970 | UTC)
exports-stamp n/a
version-stamp n/a
sha256: B2A9417058F152D7359AB8E8209FFC97F6159CF4DA280484868848F3C2118315
cpu: 32-bit
file-type: executable
subsystem: conso

->


lab8.exe
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 ....€...
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00000080 50 45 00 00 4C 01 0E 00 3C 43 B5 61 00 C4 00 00 PE..L...<Cua.Ä..
00000090 47 02 00 00 E0 00 07 01 0B 01 02 20 00 30 00 00 G...à..... .0..
000000A0 00 52 00 00 00 02 00 00 D0 12 00 00 00 10 00 00 .R......Ð.......
000000B0 00 40 00 00 00 00 40 00 00 10 00 00 00 02 00 00 .@....@.........
000000C0 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 ....
000000D0 00 60 01 00 00 04 00 00 49 A9 01 00 03 00 00 00 .`......I©......
000000E0 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 .. ..
000000F0 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ....
00000100 00 80 00 00 98 07 00 00 00 00 00 00 00 00 00 00 .€..˜...........
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000140 04 A0 00 00 18 00 00 00 00 00 00 00 00 00 00 00 . ...
00000150 00 00 00 00 00 00 00 00 7C 81 00 00 04 01 00 00 ....|.......
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000170 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00 ....text...
00000180 D8 2F 00 00 00 10 00 00 00 30 00 00 00 04 00 00 Ø/.......0......
00000190 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 ....`.P`
000001A0 2E 64 61 74 61 00 00 00 18 00 00 00 00 40 00 00 .data........@..
000001B0 00 02 00 00 00 34 00 00 00 00 00 00 00 00 00 00 .....4..........
000001C0 00 00 00 00 40 00 30 C0 2E 72 64 61 74 61 00 00 ....@.0À.rdata..
000001D0 54 07 00 00 00 50 00 00 00 08 00 00 00 36 00 00 T....P.......6..
000001E0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 ....@.0@
000001F0 2F 34 00 00 00 00 00 00 58 0B 00 00 00 60 00 00 /4......X....`..
00000200 00 0C 00 00 00 3E 00 00 00 00 00 00 00 00 00 00 .....>..........
00000210 00 00 00 00 40 00 30 40 2E 62 73 73 00 00 00 00 ....@.0@.bss....
00000220 78 00 00 00 00 00 70 00 00 00 00 00 00 00 00 00 x....p..........
00000230 00 00 00 00 00 00 00 00 00 00 00 00 80 00 30 C0 ....€.0À
Special editors
Data inspector
Int24 go to: -4897988
UInt24 go to: 11879228
Int32 go to: 1639269180
UInt32 go to: 1639269180
Int64 go to: Invalid
UInt64 go to: Invalid
LEB128 go to: 60
ULEB128 go to: 60
AnsiChar / char8_t <
WideChar / char16_t 㰼
UTF-8 code point < (U+003C)
Single (float32) 4.17963178080072E20
Double (float64) Invalid
OLETIME Invalid
FILETIME Invalid
DOS date 9/28/2013
DOS time 8:25:56 AM
DOS time & date Invalid
time_t (32 bit) 12/12/2021 12:33:00 AM
time_t (64 bit) Invalid
GUID Invalid
Disassembly (x86-16) cmp al,$00000043
Disassembly (x86-32) cmp al,$00000043
Disassembly (x86-64) cmp al,$00000043
Byte order
Little endian
Big endian
Hexadecimal basis (for integral numbers)
Offset(h): 88
Block(h): 88-8B
Length(h): 4
Overwrite