

160

Community Score

✔ No security vendors and no sandboxes flagged this file as malicious

9202b5389a1a4a3c045789c8e3a8b22cb04955c71e90543d0d4c0bfca2afbe0d

suspicios.cpp

cpp

Reanalyze Similar More

Size: 827 B

Last Analysis Date: a moment ago

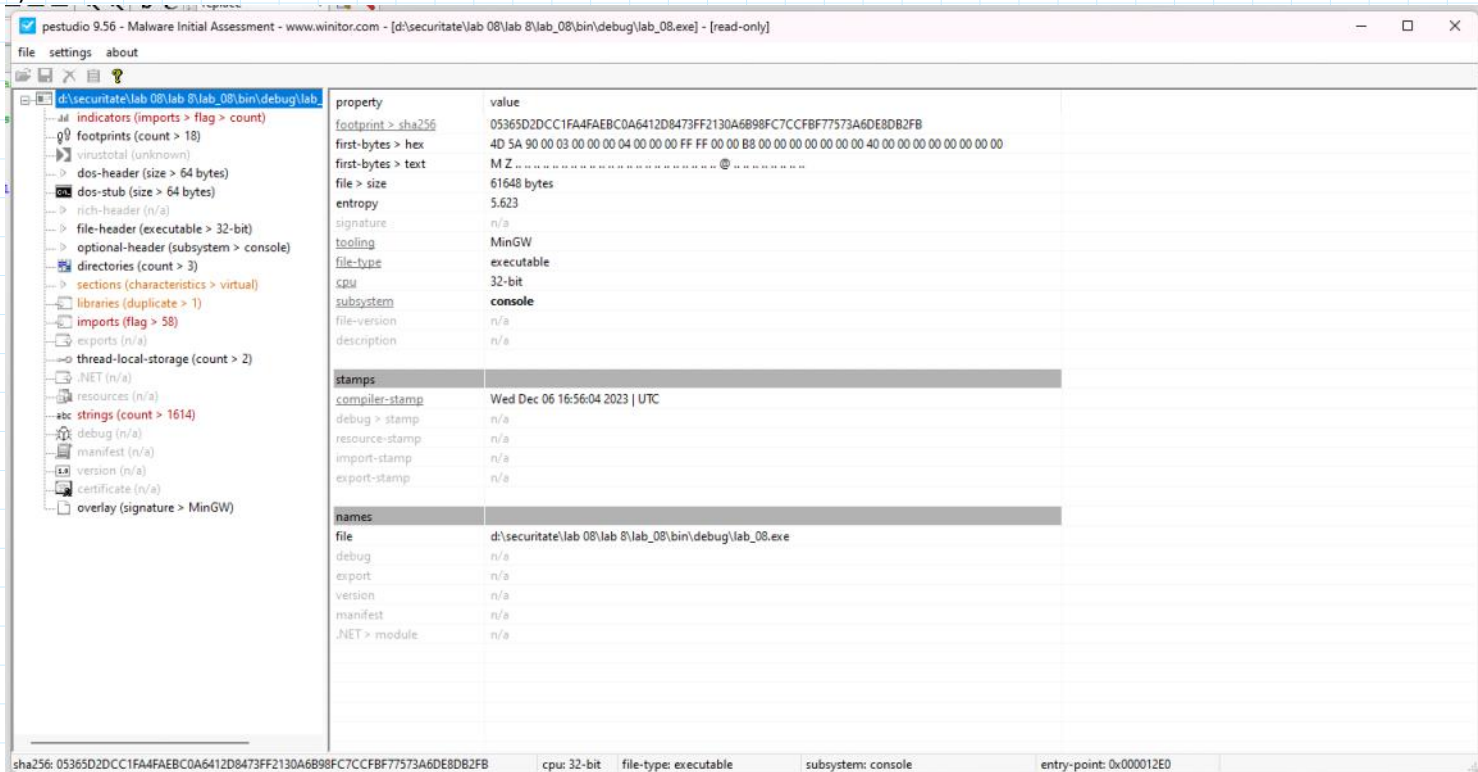
C++ CPP

- e) Fișierele dll au rolul de a rula codul c++, si impreuna sterg toate fișierele pdf din folder.
- f) Imaginea singura nu este malware, contine doar un malware, care este activat cu ajutorul fișierelor dll.
2. a) Testeaza parola corecta ("fmiSSI"), restul parolelor spune ca sunt incorecte.
- b) Putem obtine "parola corecta" daca ii oferim un string de 14 caractere, pt ca inputul asteapta 7 caractere.

```
Introduceti parola:12345671234567
Parola introdusa este corecta!
Process finished with exit code 0
```

- c) Buffer overflow

4. a)



pestudio 9.56 - Malware Initial Assessment - www.winitor.com - [d:\securitate\lab 08\lab 8\lab_08\bin\debug\lab_08.exe] - [read-only]

file settings about

d:\securitate\lab 08\lab 8\lab_08\bin\debug\lab_08.exe

indicators (imports > flag > count)

footprints (count > 18)

virustotal (unknown)

dos-header (size > 64 bytes)

dos-stub (size > 64 bytes)

rich-header (n/a)

file-header (executable > 32-bit)

optional-header (subsystem > console)

directories (count > 3)

sections (characteristics > virtual)

libraries (duplicate > 1)

imports (flag > 58)

exports (n/a)

thread-local-storage (count > 2)

.NET (n/a)

resources (n/a)

strings (count > 1614)

debug (n/a)

manifest (n/a)

version (n/a)

certificate (n/a)

overlay (signature > MinGW)

property	value
footprint > sha256	05365D2DCC1FA4FAEBC0A6412D8473FF2130A6B98FC7CCFBF77573A6DE8DB2FB
first-bytes > hex	4D 5A 90 00 03 00 00 00 04 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes > text	M Z
file > size	61648 bytes
entropy	5.623
signature	n/a
tooling	MinGW
file-type	executable
cpu	32-bit
subsystem	console
file-version	n/a
description	n/a

stamps	
compiler-stamp	Wed Dec 06 16:56:04 2023 UTC
debug > stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a

names	
file	d:\securitate\lab 08\lab 8\lab_08\bin\debug\lab_08.exe
debug	n/a
export	n/a
version	n/a
manifest	n/a
.NET > module	n/a

sha256: 05365D2DCC1FA4FAEBC0A6412D8473FF2130A6B98FC7CCFBF77573A6DE8DB2FB cpu: 32-bit file-type: executable subsystem: console entry-point: 0x000012E0

- b)

Special editors

Data inspector



Binary (8 bit)	01001101
Int8	go to: 77
UInt8	go to: 77
Int16	go to: 23117
UInt16	go to: 23117
Int24	go to: -7316915
UInt24	go to: 9460301
Int32	go to: 9460301
UInt32	go to: 9460301
Int64	go to: 12894362189
UInt64	go to: 12894362189
LEB128	go to: -51
ULEB128	go to: 77
AnsiChar / char8_t	M
WideChar / char16_t	𐀀
UTF-8 code point	M (U+004D)
Single (float32)	1.32567052633505E-38
Double (float64)	6.37066138261923E-314
OLETIME	30.12.1899
FILETIME	01.01.1601 00:21:29
DOS date	13.02.2025
DOS time	11:18:26
DOS time & date	16.04.1980 11:18:26
time_t (32 bit)	20.04.1970 11:51:41
time_t (64 bit)	10.08.2378 07:16:29
GUID	{00905A4D-0003-0000-0400-0000FFFF0000}
Disassembly (x86-16)	dec bp
Disassembly (x86-32)	dec ebp
Disassembly (x86-64)	pop r10