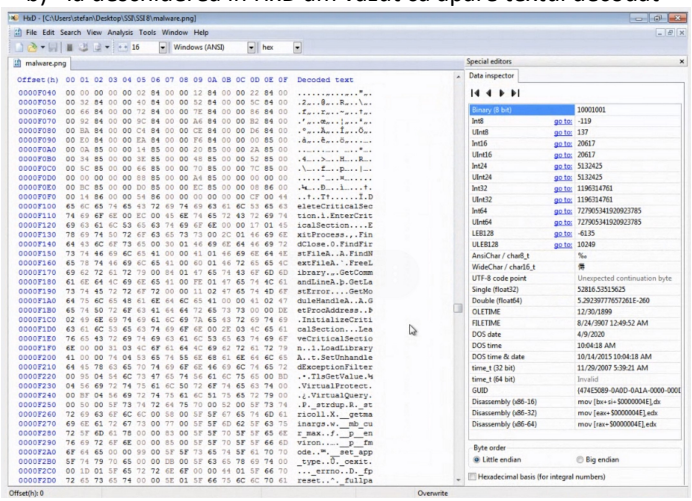
Lab 8

joi, 14 decembrie 2023 20:11

ex.1

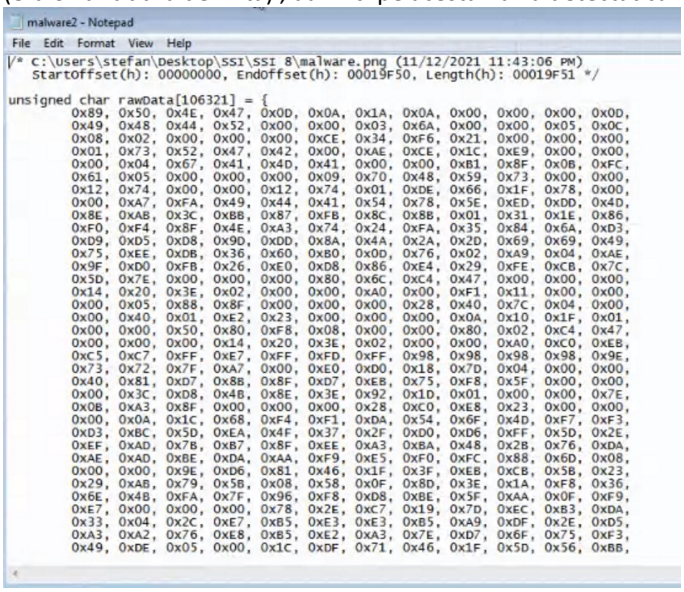
a) dupa deschiderea imaginii am vazut poza cu programul c++, fara vreo eroare. Singurul lucru suspicios poate fi din cod, dar poza pare foarte normala (in codul scris apare ”hacked”)

b) la deschiderea in HxD am vazut ca apare textul decodat



c) in detectorul de virusi apare totul in regula, fara sa para a fi vreo problema

d) am dat export la fisier in format c si s a generat ca un fel de cod (era o variabbila definita) , dar nici pe acesta nu l a detectat ca fiind virus



e)

-libstdc++-6.dll: This library contains the standard C++ runtime support provided by GCC. It includes implementations of the C++ Standard Library, such as containers, algorithms, and other utilities. Programs compiled with GCC that use C++ features will depend on this DLL.

-libmingwex-0.dll: The libmingwex-0.dll library contains additional runtime support for certain functions that are not part of the C or C++ standard libraries but are commonly

used in programs compiled with GCC under the MinGW environment. It provides compatibility functions and extensions for Windows development. --

-libgcc_s_dw2-1.dll: This library contains support for the Dwarf 2 exception handling model, which is used by GCC on Windows. It provides functionality related to exception handling, stack unwinding, and other low-level operations required by programs compiled with GCC that use exceptions.

f) eu zic ca nu dar nu sunt deloc sigur pe raspunsul meu =)

ex.2 -BUFFER OVERFLOW
ce am observat?
Programul compară parola introdusă de utilizator (input) cu parola prestabilită (pass) folosind strncmp.

- Ce observați? Programul compară parola introdusă de utilizator cu o parolă prestabilită și afișează un mesaj corespunzător.
Ca sa gasim alta parola corecta trebuie sa **buffer overflow**, unde se introduce un input mai lung decât este așteptat, astfel încât să afecteze stiva și să schimbe comportamentul programului.

Prin introducerea unui input mai lung decât spațiul alocat (input[7]), se poate suprascrie stiva și pot fi modificate variabilele din apropiere. În acest caz, se poate modifica adresa de retur a funcției main și să se forțeze programul să execute cod nedorit. Este un atac comun și poate duce la execuție de cod arbitrar.

!!! pe codeblocks am incercat si am reusit cu 13 caractere sa obtin o parola corecta

3.

Am generat un sha256 pt fisierul malware

am dat asta ca parametru catre api ul de la site ul virustotal
am pus api key ul meu dupa ce mi am facut si cont
am luat response si l am afisat pe ecran (datele de pe site)

```
def getFileSha256(file_path):
    with open(file_path, "rb") as f:
        readable_hash = hashlib.sha256(f.read()).hexdigest()
    return readable_hash
def getFileInfo(file_path):
    api_url = 'https://www.virustotal.com/api/v3/files'
    headers = {'x-apikey':
'15e887b8b739a6e7d89072b818110fff56bbb308c1a43e4a6e627124f55ed6bb'}

file_identifier = getFileSha256(file_path)
        url = f"https://www.virustotal.com/api/v3/files/{file_identifier}"
        response2 = requests.request("GET", url, headers=headers)
        print(response2.json()['data']['attributes']['last_analysis_stats'])
    return None
```

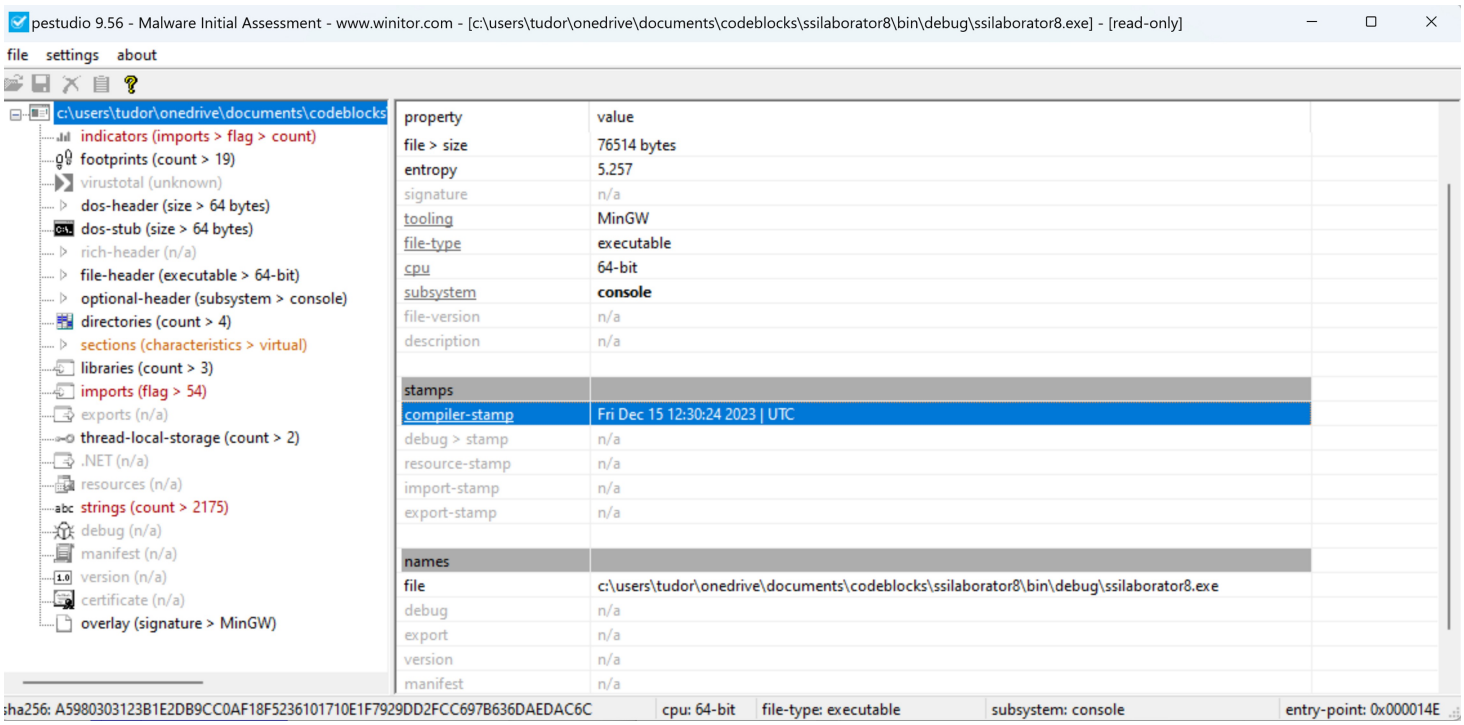
```python
import hashlib
import requests


def getFileSha256(file_path):
    with open(file_path, "rb") as f:
        readable_hash = hashlib.sha256(f.read()).hexdigest()
    return readable_hash


if __name__ == '__main__':
    headers = {'x-apikey': 'a31290b9de604184c69995f2ece10292e2d3f91c2f9be3cbc985d4ca5ebe6b24'}
    file_identifier = getFileSha256("malware.pdf")
    url = f"https://www.virustotal.com/api/v3/files/{file_identifier}"
    response = requests.request("GET", url, headers=headers)
    print(response.json()['data']['attributes']['last_analysis_stats'])
```

4.

Data la care a fost compilat programul:



compiler-stamp: 0x657C46E0 (Fri Dec 15 12:30:24 2023 | UTC)

little endian: 7DABAF61// se poate gasi in HxD (offset 88).

hex -> decimal: 2108403553

Valoarea decimal reprezinta timestamp-ul la care a fost compilat codul.

https://www.epochconverter.com/hex.