# **Laborator 7**

#### **Exercitiul 1**

- 1. Imaginea se deschide normal si nu apare nicio eroare
- 2. Imaginea are headerul PNG dar are un executabil ascuns

```
🔛 malware.png
 Offset(h) 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
 000077C0 F3 A7 C2 66 92 15 AA D4 A5 W*O-..¢ó§Âf'.ªÔ¥
 000077D0 BF C4 A4 09 B3 C0 BE 94 F9 3%PÊì%.¿Ä¤.³À%"ù
 000077E0 30 E1 6B C5 C7 61 58 F4 75 a-Z8QyÖ0ákÅÇaXôu
 000077F0 11 17 2C C6 EB 74 DD A5 CE °.à.^.8.., ÆëtÝ¥Î
 00007800 FF 2C C5 C5 AB 7D C5 52 7C Ódf.Yì.ÿ,åå«}åR|
 00007810 A6 71 05 DD 95 CE 5A C6 9C 4.0.14...q.Ý·ÎZÆœ
 00007820 64 BD A6 F4 D0 B9 5E B7 3D ..4æ+}Éd14;ôĐ1^:=
 00007830 9B 59 A8 50 25 6E DC 63 56 Öb DDT.>Y"P%nÜcV
 00007840 F3 28 D2 5B C9 8E 2F D4 61 ê±BÅCoÜó(Ò[ÉŽ/Ôa
 00007850 F0 E5 68 5A 72 61 C9 C4 19 . #@|Ĺ, ðåhZraÉÄ.
 00007860 6B AC 1B DE 68 69 4D 5A 76 Cd.~†D3k-.PhiMZv
 00007870 B8 23 5F 1E 7D 9C D5 64 EE -%<æ^fF.# .}@Odî
 00007880 DA E9 49 C2 F3 3A EE 9B B4 M.j%% 2ÚéIÂó:î>
 00007890 88 67 AC 6F BC 0B 90 E1 D7 Ù÷.4ëšÞ^g-o4..á×
000070%0 60 50 71 DE C7 75 17 05 DD h2 10 m.a.A.C.. >
```

3. Snippet raport image din VirusTotal:

```
"description": "This signature detects the presence of a number of Windows API function
ality often seen within embedded executables. When this signature alerts on an executab
le, it is not an indication of malicious behavior. However, if seen firing in other fil
e types, deeper investigation may be warranted."
"last_analysis_stats": {
        "harmless": 0,
        "type-unsupported": 14,
        "suspicious": 0,
        "confirmed-timeout": 0,
        "timeout": 1,
        "failure": 0,
        "malicious": 1,
        "undetected": 60
}
```

4. Snippet raport continut suspicios din VirusTotal:

```
"type_extension": "exe",
"last_analysis_stats": {
    "harmless": 0,
```

Laborator 7

```
"type-unsupported": 12,
   "suspicious": 0,
   "confirmed-timeout": 0,
   "timeout": 0,
   "failure": 0,
   "malicious": 0,
   "undetected": 64
}
```

- 5. Fisierele DLL ajuta la rularea executabilului
- 6. Imaginea este un malware deoarece contine un executabil ce sterge fisierele pdf

#### **Exercitiul 2**

```
#include <iostream>
#include <string.h>
using namespace std;
int main()
    char pass[7] = "fmiSSI";
    char input[7];
    int passLen = strlen(pass);
    cout << "Introduceti parola: ";</pre>
    cin >> input;
    if (strncmp(input, pass, passLen) == 0)
        cout << "Parola introdusa este corecta!\n";</pre>
    }
    else
    {
        cout << "Ati introdus o parola gresita\n";</pre>
    return 0;
}
```

Daca introducem o parola de 14 caractere orice input va fi consider corect deoarece bufferul va fi suprascris. Aceasta vulnerabilitate exista pentru versiunile de C++ mai vechi de C++ 17 si se numeste **buffer overflow** 

## **Exercitiul 3**

Calcularea valorii SHA256 a unui fisier in Python:

```
import hashlib
with open("fisier.txt", "rb") as f:
   bytes = f.read()
   readable_hash = hashlib.sha256(bytes).hexdigest()
   print(f"SHA-256 value: {readable_hash}")
```

Laborator 7 2

# Output: SHA-256 value: ea483198f5f978d1c59727f042d62598469897afa658aeb43bef2bb2fe8709cc

### VirusTotal Api Key:

b3aff7d0c046094bf22521188361a49ba48410ce0fd6cb3e5745a6be42a0ec70

- 1. Facem un request de <u>upload file</u> pentru a scana fisierul.
- 2. Facem un request the <u>get file report</u> folosing valoarea SHA256 calculata in programul de Python pentru a vedea raportul despre fisierul incarcat
- 3. Raspunsul primit de la ultimul request:

```
{
"last_analysis_stats": {
        "harmless": 0,
        "type-unsupported": 15,
        "suspicious": 0,
        "confirmed-timeout": 0,
        "timeout": 0,
        "failure": 0,
        "malicious": 0,
        "undetected": 61
    }
}
```

Laborator 7