Lab 5 - Theodor Moroianu (334)

Ex 1

Codul afiseaza in terminal:

```
$ node sample1.js
> Facultatea de Matematica si Informatica
> Universitatea din Bucuresti
> https://www.youtube.com/watch?v=HIcSWuKMwOw
```

a. Ce face acest cod?

- Codul afiseaza un mesaj in consola. b. Cum ati ajuns la aceasta concluzie:
- Am executat codul intr-o masina virtuala. c. Care este mesajul ascuns?
- Mesajul ascuns este descris mai sus. d. Cine a realizat acest cod?
- Codul este creat cu ajutorul site-ului jencode.

Ex 2

Cu ajutorul deobufscatorului de aici, vedem ca scriptul dat incearca sa scrie "Bun venit la acest laborator" in fisierul "./fmi.txt".

```
WScript.Echo("You have been hacked!");
WScript.Echo("I hope you did not run this on your own PC...");
var f = "Facultatea";
var mi = "de Matematica si Informatica";
var unibuc = "Universitatea din Bucuresti";
var curs = "Curs Info anul 3";
var minciuna = "Acesta este un malware. Dispozitivul este compromis";
var adevar = "Stringul anterior este o minciuna";
try {
    var obj = new ActiveXObject("Scripting.FileSystemObject");
    var out = obj.OpenTextFile("./fmi.txt", 2, true, 0);
    out.WriteLine("Bun venit la acest laborator :)");
    out.Close();
    var fle = obj.GetFile("./fmi.txt");
    fle.attributes = 2
} catch (err) {
    WScript.Echo("Do not worry. Ghosts do not exist!")
}
```

a. Ce face acest cod?

- Acest cod incearca sa foloseasca API-ul Windows pentru a deschide un fisier "./fmi.txt" si a scrie date in el. De asemenea afiseaza si un pop-up. b. Putem sa consideram ca acest fisier este malware?

- Nu, de oarece nu are intentii malitioase (fisierul pe care il creaza nu este ascuns / fisier care sa incerce sa compromita sigurata userului). c. Cine a realizat acest cod?
- Codul a fost obfuscat cu ajutorul site-ului BeutifyConverter.

Ex 3

Programul scrie de asemenea "Bun venit la acest laborator" in fisierul "./fmi", dar foloseste encodare hexadecimala pentru a ascunde mesajele scrise.

putem decoda lista de striguri ale scriputului:

```
$ echo -e
'["\x59\x6F\x75\x20\x68\x61\x76\x65\x20\x62\x65\x65\x6E\x20\x68\x61\x63\x6B
\x65\x64\x21",
"\x49\x20\x68\x6F\x70\x65\x20\x79\x6F\x75\x20\x64\x69\x64\x20\x6E\x6F\x74\x
20\x72\x75\x6E\x20\x74\x68\x69\x73\x20\x6F\x6E\x20\x79\x6F\x75\x72\x20\x6F\
x77\x6E\x20\x50\x43\x2E\x2E\x2E",
"\x46\x61\x63\x75\x6C\x74\x61\x74\x65\x61",
"\x64\x65\x20\x4D\x61\x74\x65\x6D\x61\x74\x69\x63\x61\x20\x73\x69\x20\x49\x
6E\x66\x6F\x72\x6D\x61\x74\x69\x63\x61",
"\x55\x6E\x69\x76\x65\x72\x73\x69\x74\x61\x74\x65\x61\x20\x64\x69\x6E\x20\x
42\x75\x63\x75\x72\x65\x73\x74\x69",
"\x43\x75\x72\x73\x20\x49\x6E\x66\x6F\x20\x61\x6E\x75\x6C\x20\x33",
"\x41\x63\x65\x73\x74\x61\x20\x65\x73\x74\x65\x20\x75\x6E\x20\x6D\x61\x6C\x
77\x61\x72\x65\x2E\x20\x44\x69\x73\x70\x6F\x7A\x69\x74\x69\x76\x75\x6C\x20\
x65\x73\x74\x65\x20\x63\x6F\x6D\x70\x72\x6F\x6D\x69\x73",
"\x53\x74\x72\x69\x6E\x67\x75\x6C\x20\x61\x6E\x74\x65\x72\x69\x6F\x72\x20\x
65\x73\x74\x65\x20\x6F\x20\x6D\x69\x6E\x63\x69\x75\x6E\x61",
"\x53\x63\x72\x69\x70\x74\x69\x6E\x67\x2E\x46\x69\x6C\x65\x53\x79\x73\x74\x
65\x6D\x4F\x62\x6A\x65\x63\x74", "\x2E\x2F\x66\x6D\x69\x2E\x74\x78\x74",
"\x42\x75\x6E\x20\x76\x65\x6E\x69\x74\x20\x6C\x61\x20\x61\x63\x65\x73\x74\x
20\x6C\x61\x62\x6F\x72\x61\x74\x6F\x72\x20\x3A\x29",
"\x61\x74\x74\x72\x69\x62\x75\x74\x65\x73",
"\x44\x6F\x20\x6E\x6F\x74\x20\x77\x6F\x72\x72\x79\x2E\x20\x47\x68\x6F\x73\x
74\x73\x20\x64\x6F\x20\x6E\x6F\x74\x20\x65\x78\x69\x73\x74\x21"]'
> ["You have been hacked!", "I hope you did not run this on your own
PC...", "Facultatea", "de Matematica si Informatica", "Universitatea din
Bucuresti", "Curs Info anul 3", "Acesta este un malware. Dispozitivul este
compromis", "Stringul anterior este o minciuna",
"Scripting.FileSystemObject", "./fmi.txt", "Bun venit la acest laborator
:)", "attributes", "Do not worry. Ghosts do not exist!"]
```

a. Ce face acest cod?

- Acest cod scrie, asemenea scriptului `sample2.js`, "Bun venit la acest laborator 😃" in "./fmi.txt". Putem vedea din cod ca acestea sunt actiunile facute, cu ajutorul de-obfuscarii a listei de stringuri si a secventei:

```
var obj = new ActiveXObject(_0x1d78[8]);
   var out = obj.OpenTextFile(_0x1d78[9], 2, true, 0);
   out.WriteLine(_0x1d78[10]);
   out.Close();
   var fle = obj.GetFile(_0x1d78[9]);
   fle[_0x1d78[11]] = 2
```

b. Explicati continutul de tipul `\x$$`.

- Continutul de tipul `\x$$` reprezinta bytes (reprezentat ca doua valori hexadecimale de 4 biti). c. Care este diferenta cu al doilea cod?
- Scriptul foloseste o alta metoda de obfuscare a continutului. Fata de `sample1.js`, scriptul creaza fisierul "./fmi.txt".

Ex 4

Scriptul 4 are un payload, encriptat in `base64`, care, odata executat, injecteaza executabilul `hello.txt` in `%USER_FOLDER\AppData\Local\Temp`.

a. Ce face acest script?

- Acest script injecteaza in `%USER_FOLDER\AppData\Local\Temp` un executabil numit `hello.txt`, si mai multe dll necesare pentru executarea acestuia. b. Cum putem extrage payloadul?
- Pentru a extrage payload-ul, este suficient sa scoatem continutul din script:
    1. Copiem continutul liniei 43, pe care il punem intr-un fisier numit "exec".
    2. Decompresam fisierul cu ajutorul functiei `base64`: `$ base64 -d < exec > bin`.
    3. Putem analiza tiput fisierului `bin`:

```
$ file bin
> bin: PE32 executable (console) Intel 80386, for MS Windows
```

    4. Putem dezasambla binarul:

```
$ gdb bin
(gdb) disassemble main
Dump of assembler code for function main():
0x00401460 <+0>:    lea    0x4(%esp),%ecx
0x00401464 <+4>:    and    $0xfffffff0,%esp
0x00401467 <+7>:    push   -0x4(%ecx)
0x0040146a <+10>:   push   %ebp
0x0040146b <+11>:   mov    %esp,%ebp
0x0040146d <+13>:   push   %ecx
0x0040146e <+14>:   sub    $0x14,%esp
0x00401471 <+17>:   call   0x401a70 <__main>
0x00401476 <+22>:   movl   $0x404065,0x4(%esp)
0x0040147e <+30>:   movl   $0x407200,(%esp)
0x00401485 <+37>:   call   0x401510
```

```
<_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc>
0x0040148a <+42>:   movl   $0x401518,(%esp)
0x00401491 <+49>:   mov    %eax,%ecx
0x00401493 <+51>:   call   0x401530 <_ZNSolsEPFRSoS_E>
0x00401498 <+56>:   sub    $0x4,%esp
0x0040149b <+59>:   movl   $0x404072,(%esp)
0x004014a2 <+66>:   call   0x402114 <system>
0x004014a7 <+71>:   mov    $0x0,%eax
0x004014ac <+76>:   mov    -0x4(%ebp),%ecx
0x004014af <+79>:   leave
0x004014b0 <+80>:   lea    -0x4(%ecx),%esp
0x004014b3 <+83>:   ret
```

c. Putem considera acest script malware?

- Da, acest script este un malware, deoarece:
    1. Isi ascunde payloadul, encodand-ul in base64.
    2. Introduce fisiere executabile fara a cere acordul utilizatorului.
    3. Introduce fisierele intr-o locatie ascunsa, pe care majoritatea utilizatorilor nu o cunosc. Putem considera programul ca un trojan, care injecteaza un alt malware in pc. d. Cautati pe virustotal.
- Virustotal gaseste o groaza de antivirusuri care clasifica fisierul ca malware. e. Obfuscam codul. Ce se schimba?
- Doua antivirusuri tot il detecteaza ca fiind un trojan dropper (script generic). Probabil ca vad obfuscarea si il considera malware implicit. Totusi, obfuscarea scade semnificativ numarul de detectii ca malware, antivirusurile ne mai putand sa inteleaga ce se intampla.