

Laborator 5

Securitatea Sistemelor Informatice

1.

Acest cod afiseaza in consola



Pentru deobfuscare, am folosit tool-ul <https://lelinhtinh.github.io/de4js/> cu ajutorul caruia am obtinut:

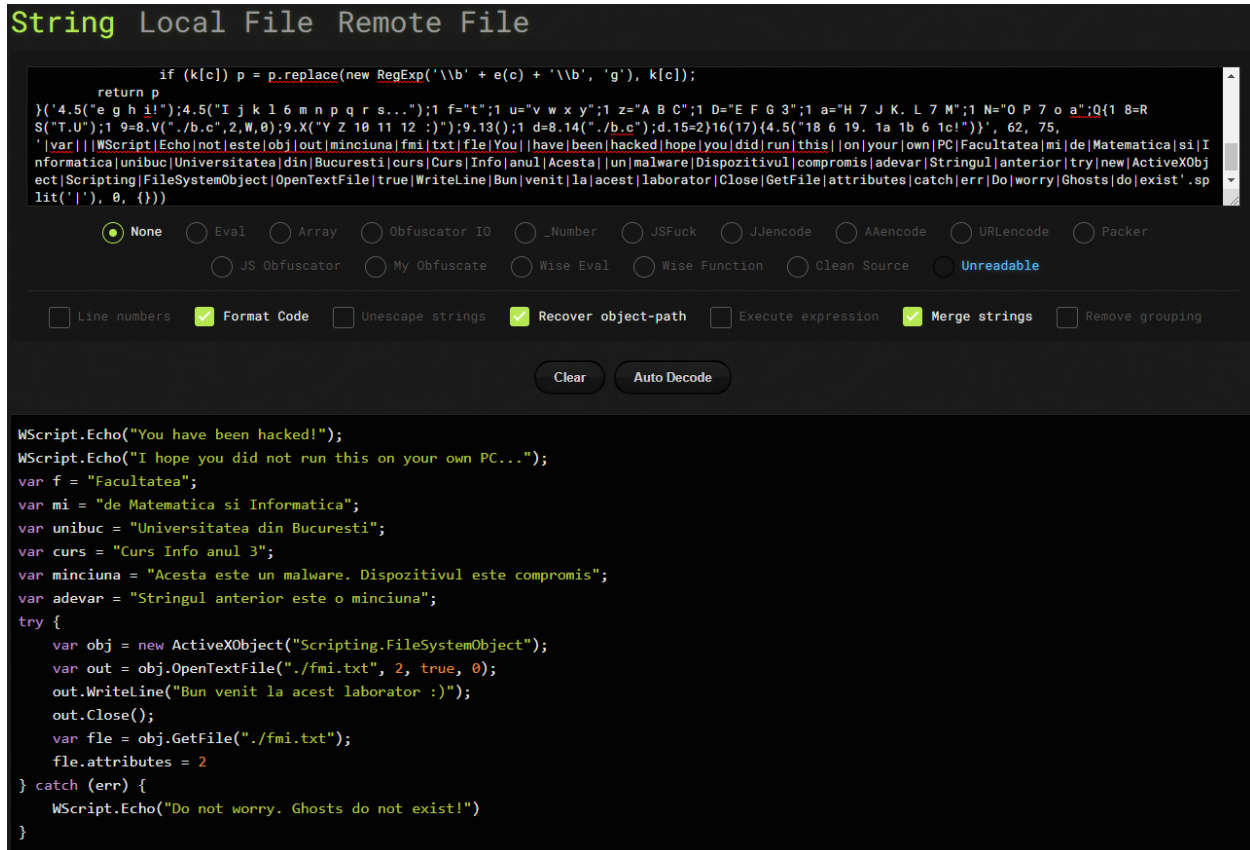
```
console.log("Facultatea de Matematica si Informatica")
console.log("Universitatea din Bucuresti")
console.log("https://www.youtube.com/watch?v=HicSWuKMwOw")
var ascuns = "Mesaj ascuns: 18367622009998665"
```

Mesajul ascuns este 18367622009998665.

Codul a fost realizat in acest format in mod automat, folosind un soft de obfuscare.

2.

Codul sursa deobfuscata este:



The screenshot shows a web-based JavaScript deobfuscator tool. At the top, there are tabs for 'String', 'Local File', and 'Remote File', with 'String' selected. The main area displays the deobfuscated JavaScript code. Below the code, there are various options for deobfuscation, including 'None' (selected), 'Eval', 'Array', 'Obfuscator IO', '_Number', 'JSFuck', 'JJencode', 'AAencode', 'URLEncode', 'Packer', 'JS Obfuscator', 'My Obfuscate', 'Wise Eval', 'Wise Function', 'Clean Source', and 'Unreadable'. There are also checkboxes for 'Line numbers', 'Format Code' (checked), 'Unescape strings', 'Recover object-path' (checked), 'Execute expression', 'Merge strings' (checked), and 'Remove grouping'. At the bottom, there are 'Clear' and 'Auto Decode' buttons. The deobfuscated code is as follows:

```
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 file = obj.GetFile("./fmi.txt");
    file.attributes = 2
} catch (err) {
    WScript.Echo("Do not worry. Ghosts do not exist!")
}
```

Pentru deobfuscare, am folosit tool-ul <https://lelinhtinh.github.io/de4js/>.

Fisierul nu poate fi considerat malware, deoarece acesta doar afiseaza 2 mesaje si creeaza un fisier txt ascuns. Fisierul este benign.

Codul a fost realizat in acest format in mod automat, folosind un soft de obfuscare.

3.

In sample exista un array cu valori de string-uri exprimate in hexa. Cateva exemple ar fi:

`\x59\x6F\x75\x20\x68\x61\x76\x65\x20\x62\x65\x65\x6E\x20\x68\x61\x63\x6B\x65\x64\x21`

care s-ar traduce in

You have been hacked! ;

`\x49\x20\x68\x6F\x70\x65\x20\x79\x6F\x75\x20\x64\x69\x64\x20\x6E\x6F\x74\x20\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`

care s-ar traduce in:

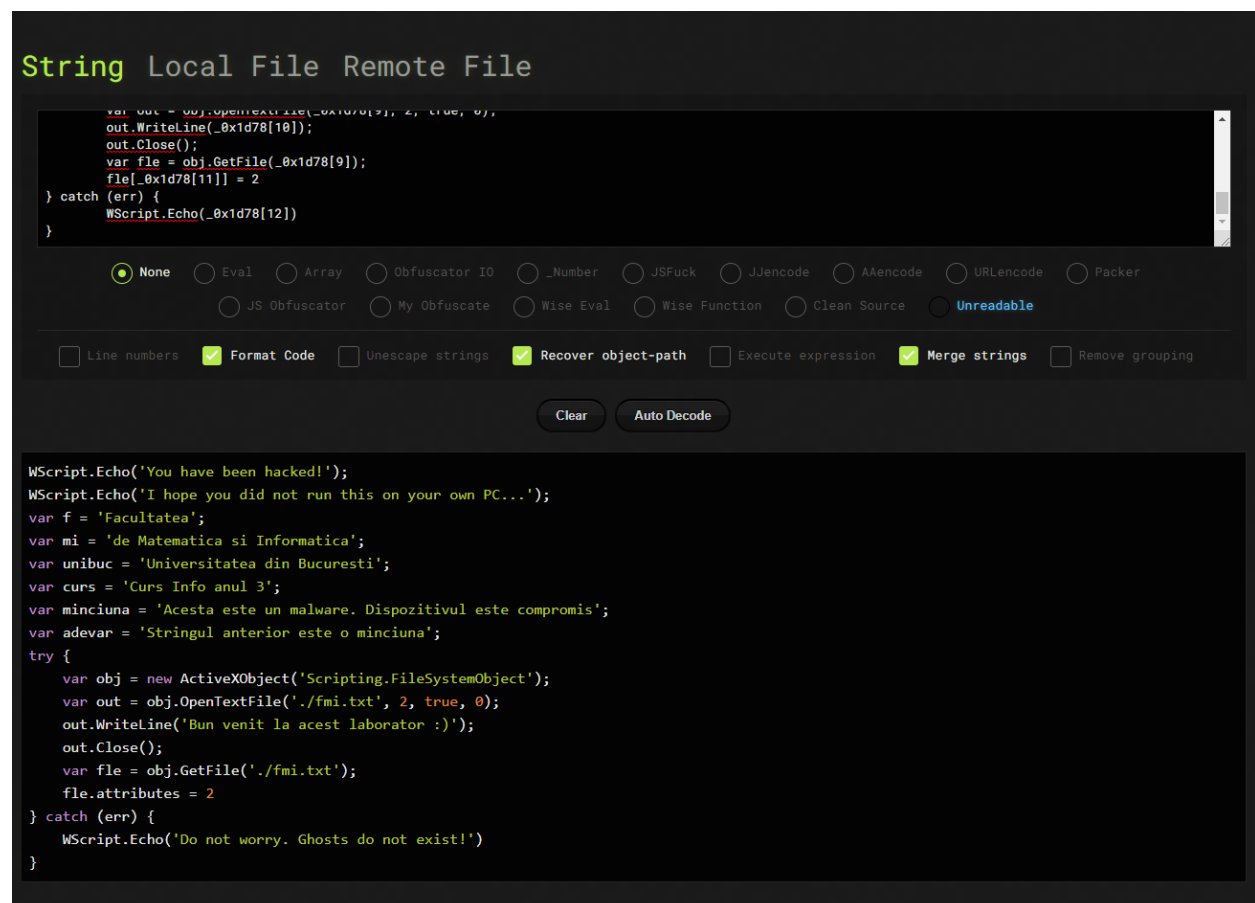
I hope you did not run this on your own PC... ;

`\x43\x75\x72\x73\x20\x49\x6E\x66\x6F\x20\x61\x6E\x75\x6C\x20\x33`

care s-ar traduce in:

Curs Info anul 3

a. Dupa deobfuscare, codul arata astfel:



Acesta printeaza 2 mesaje si creeaza un fisier txt ascuns. (Si afiseaza ‘Ghosts do not exist’ in cazul in care fisierul txt exista deja)

b. Valorile de tipul `\x$$` reprezinta caractere scrise in format hexa, acestea formand string-uri.

c. Diferenta dintre cele doua sample-uri este metoda de obfuscare.

4.

a. Scriptul creeaza 3 fisierele dll si un fisier executabil.

b. Putem extrage payload-ul fara sa rulam scriptul astfel: transformam string-urile din Base64 in fisiere binare.

c. Scriptul nu poate fi considerat malware deoarece fisierele create de el nu sunt malitioase.

d.

18
/ 58

Community Score

18 security vendors flagged this file as malicious

a196eat3937f9b858c9fb2a56eef139d324a022cbd21adcc217f7e581a73e21
sample4.js
text

3.39 MB
Size

2021-11-01 12:06:51 UTC
8 days ago

TXT

DETECTION	DETAILS	COMMUNITY
Ad-Aware	JS.Heur.Cbum.1.64A98D8B.Gen	ALYac JS.Heur.Cbum.1.64A98D8B.Gen
Arcabit	JS.Heur.Cbum.1.64A98D8B.Gen	Avast VBS:Downloader-ANE [Trj]
AVG	VBS:Downloader-ANE [Trj]	BitDefender JS.Heur.Cbum.1.64A98D8B.Gen
Cyren	JS/Nemucod.N1Eldorado	Emsisoft JS.Heur.Cbum.1.64A98D8B.Gen (B)
eScan	JS.Heur.Cbum.1.64A98D8B.Gen	FireEye JS.Heur.Cbum.1.64A98D8B.Gen
Fortinet	BAT/Scatter.BE!tr	GData JS.Heur.Cbum.1.64A98D8B.Gen
Ikarus	Trojan-Downloader.JS.Xibow	Kaspersky HEUR:Trojan-Dropper.Script.Generic
MAX	Malware (ai Score=84)	Microsoft TrojanDownloader:JS/Xibow.J
NANO-Antivirus	Trojan.Script.Ransom.dqzgw	Sangfor Engine Zero Malware.Generic-VBS.Save.a7030c38

e.

Dupa obfuscare, incarcata pe VirusTotal, fisierul nu mai este detectat de cele 18 motoare, ci doar de 3.

3
/ 57

Community Score

3 security vendors flagged this file as malicious

4d6bd936cb25a2111392b84ba13077bd87c24309e57ae8c2f99141197776278d
sample41.js
text

3.27 MB
Size

2021-11-03 03:05:01 UTC
7 days ago

TXT

DETECTION	DETAILS	COMMUNITY 1
DrWeb	1 Trojan:MulDrop18.46723	Kaspersky 1 HEUR:Trojan-Dropper.Script.Generic
ZoneAlarm by Check Point	1 HEUR:Trojan-Dropper.Script.Generic	Ad-Aware 1 Undetected