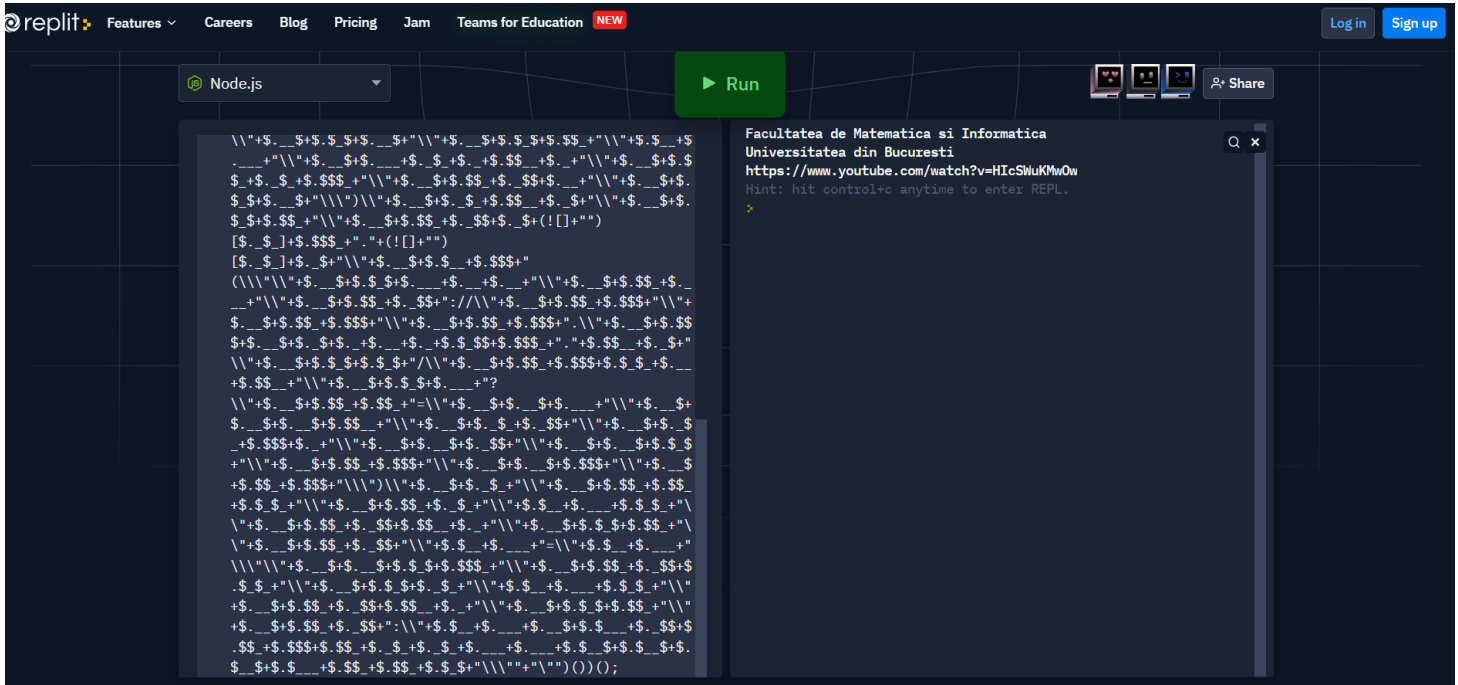


Laborator 5 – Securitatea Sistemelor Informatice

Exercitiul 1 – *sample1.js*



Pentru interpretarea codului am folosit <https://replit.com/languages/nodejs>

Textul rezultat este:

Facultatea de Matematica si Informatica

Universitatea din Bucuresti

<https://www.youtube.com/watch?v=HlcSWuKMwOw>

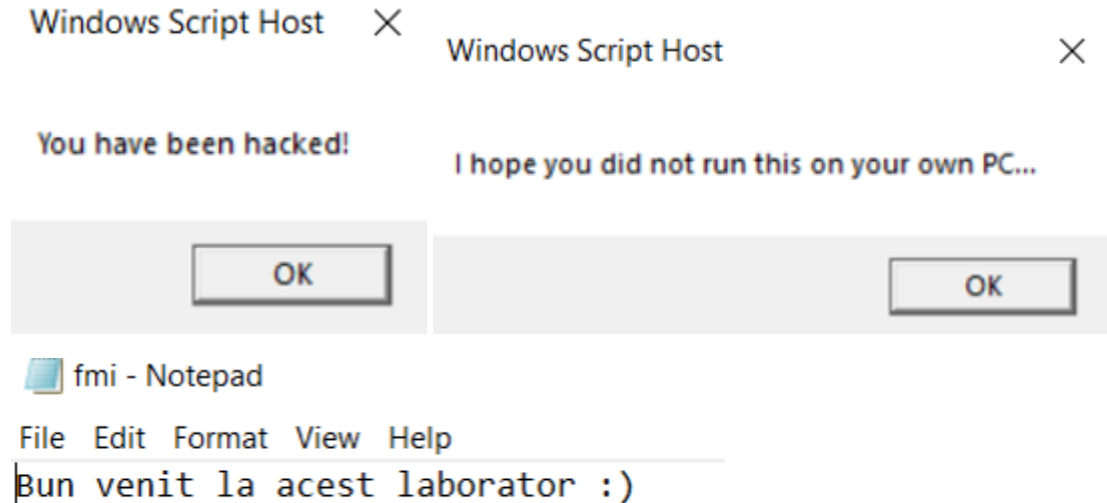
Pentru decode am folosit <https://lelinhtinh.github.io/de4js/> unde apare si mesajul ascuns

```
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"
```

Este cod generat automat de un executabil, deoarece este inteligibil, iar un om ar scrie un cod mult mai curat.

Exercitiul 2 – *sample2.js*

La prima vedere pare mai inteligibil decat codul din *sample1.js*, insa ultima parte nu are niciun sens, deci si acest cod este generat automat de un executabil. De asemenea, creeaza un fisier ascuns denumit **fmi.txt** in folderul samples. Nu este malware pentru ca nu afecteaza functionalitatea sistemului in vreun fel.



Prin deofuscare folosind <https://lelinhtinh.github.io/de4js/>, se poate vede si scriptul original:

```
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 comp
romis";
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!")
}
```

Exercitiul 3 – *sample3.js*

Acelasi comportament ca *sample2.js* (deschide ferestre de popup).

Folosind hex to ASCII converter (<https://www.rapidtables.com/convert/number/hex-to-ascii.html>), am transformat vectorul de la inceput care contine numere in hexa. Vectorul este format din mai multe stringuri de mesaje criptate in hexa:

Open File

Paste hex numbers or drop file

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

Character encoding

ASCII

Convert Reset Swap

You have been hacked!

Copy Save

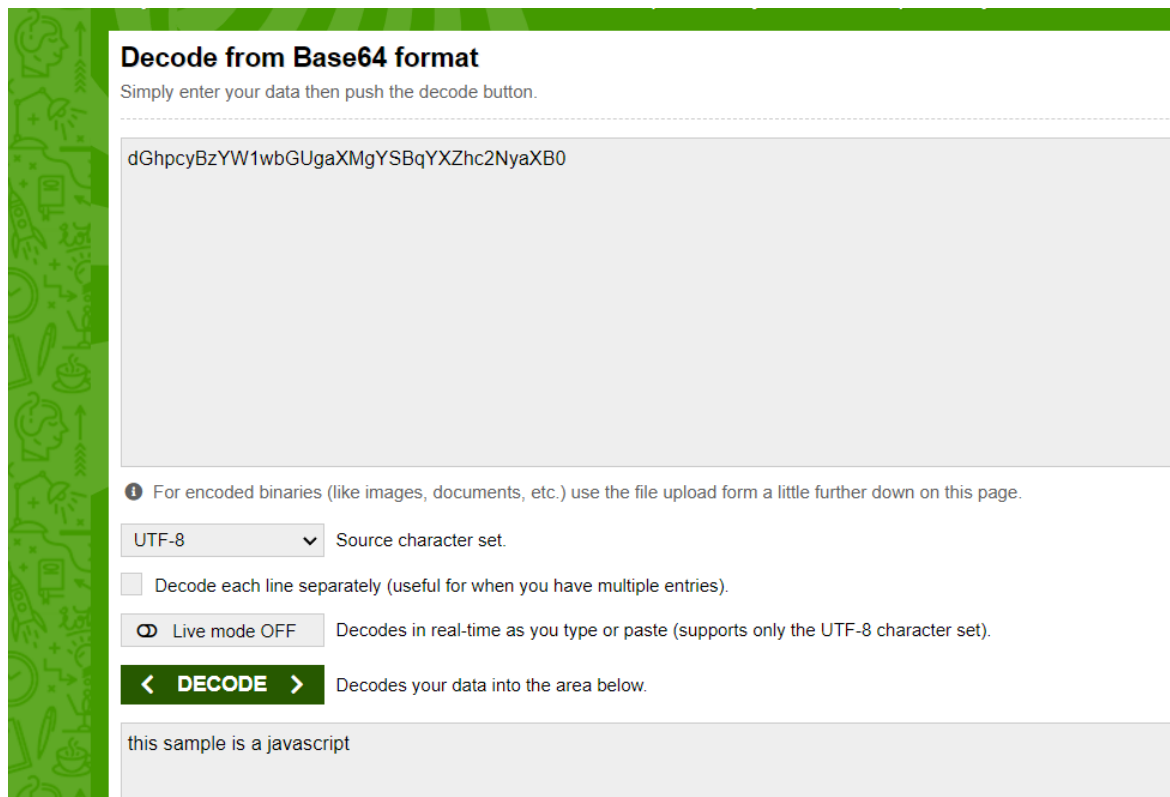
```
var _0x1d78 = ["You have been hacked!", "I hope you did not run this on your own PC...", "Facultatea", "de Matematica si Informatica", "Universitatea din Bucuresti", "Curs Info anul 3", "Acesta este un malware. Dispozitivul este compromis", "Stringul anterior este o minciuna", "Scripting.FileSystemObject", "./fmi.txt", "Bun venit la acest laborator :)", "attributes", "Do not worry. Ghosts do not exist!"];
WScript.Echo(_0x1d78[0]);
WScript.Echo(_0x1d78[1]);
var f = _0x1d78[2];
var mi = _0x1d78[3];
var unibuc = _0x1d78[4];
var curs = _0x1d78[5];
var minciuna = _0x1d78[6];
var adevar = _0x1d78[7];
try {
    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
} catch (err) {
    WScript.Echo(_0x1d78[12])
}
```

Exercitiul 4 – *sample4.js*

Comentariile sunt in base64. Folosesc decoderul online pentru a le decoda.

(<https://www.base64decode.org/>)

Este un virus, conform verificarii cu Virus Total, insa nu este malitios deoarece nu afecteaza sistemul in vreun fel.



Decode from Base64 format
Simply enter your data then push the decode button.

dGhpcyBzYW1wbGUgaXMgYSBqYXZhc2NyaXB0

i For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.


☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

this sample is a javascript

Virus Total: Pentru scriptul original – *sample4.js*



21 / 57

Community Score

21 security vendors flagged this file as malicious

a196ea13937f9b858c9fb2a56eef139d324a022cbd21adcc217f7e581a73e21
sample4.js


3.39 MB
Size

2021-11-18 16:27:46 UTC
6 days ago

TXT

DETECTION	DETAILS	COMMUNITY
Ad-Aware	JS.Heur.Cbum.1.64A98D8B.Gen	ALYac
Arcabit	JS.Heur.Cbum.1.64A98D8B.Gen	Avast
AVG	VBS:Downloader-ANE [Trj]	BitDefender
Cyren	JS/Nemucod.N1!Eldorado	DrWeb
Emsisoft	JS.Heur.Cbum.1.64A98D8B.Gen (B)	eScan
FireEye	JS.Heur.Cbum.1.64A98D8B.Gen	Fortinet
GData	JS.Heur.Cbum.1.64A98D8B.Gen	Ikarus
Kaspersky	HEUR:Trojan-Dropper.Script.Generic	Lionic

Virus Total: Pentru scriptul obtinut dupa obfuscare - *sample4v2.js*



3 / 57

Community Score

3 security vendors flagged this file as malicious

4d6bd936cb25a2111392b84ba13077bd87c24309e57ae8c2f99141197776278d
sample41.js

3.27 MB
Size

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

TXT

DETECTION	DETAILS	COMMUNITY
DrWeb	Trojan.MulDrop18.46723	Kaspersky
ZoneAlarm by Check Point	HEUR:Trojan-Dropper.Script.Generic	Ad-Aware
AhnLab-V3	Undetected	ALYac
Antiy-AVL	Undetected	Arcabit
Avast	Undetected	Avira (no cloud)
Baidu	Undetected	BitDefender
BitDefenderTheta	Undetected	Bkav Pro
CAT-QuickHeal	Undetected	ClamAV
CMC	Undetected	Comodo
Cynet	Undetected	Cyren
Emsisoft	Undetected	eScan
ESET-NOD32	Undetected	F-Secure