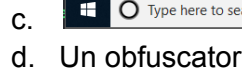


- Afiseaza un mesaj si un link catre un filmulet pe youtube
- Am rulat codul in compilator online



The screenshot shows the Programiz Online JavaScript Compiler interface. The code in `main.js` defines a function `eval` that checks for a backdoor. The output shows a successful execution with a message about a backdoor being found.

```

main.js
1- eval(function(p, a, c, k, e, r) {
2-   e = function(c) {
3-     return (c < a ? '' : e(parseInt(c / a)))
4-       + ((c = c % a) > 35 ? String
5-         .fromCharCode(c + 29) : c.toString
6-         (36))
7-   };
8-   if (!''.replace(/^/, String)) {
9-     while (c--) r[e(c)] = k[c] || e(c);
10-    k = [
11-      function(e) {
12-        return r[e]
13-      }
14-    ];
15-    e = function() {
16-      return '\\w+'
17-    };
18-    c = 1
19-  };
20-  while (c--)
21-    if (k[c]) p = p.replace(new RegExp('\\w+'
22-      + e(c) + '\\b', 'g'), k[c]);
23-  return p
24-});
25-
26-
27-
28-
29-
30-
31-
32-
33-
34-
35-
36-
37-
38-
39-
40-
41-
42-
43-
44-
45-
46-
47-
48-
49-
50-
51-
52-
53-
54-
55-
56-
57-
58-
59-
60-
61-
62-
63-
64-
65-
66-
67-
68-
69-
70-
71-
72-
73-
74-
75-
76-
77-
78-
79-
80-
81-
82-
83-
84-
85-
86-
87-
88-
89-
90-
91-
92-
93-
94-
95-
96-
97-
98-
99-
100-

```

```

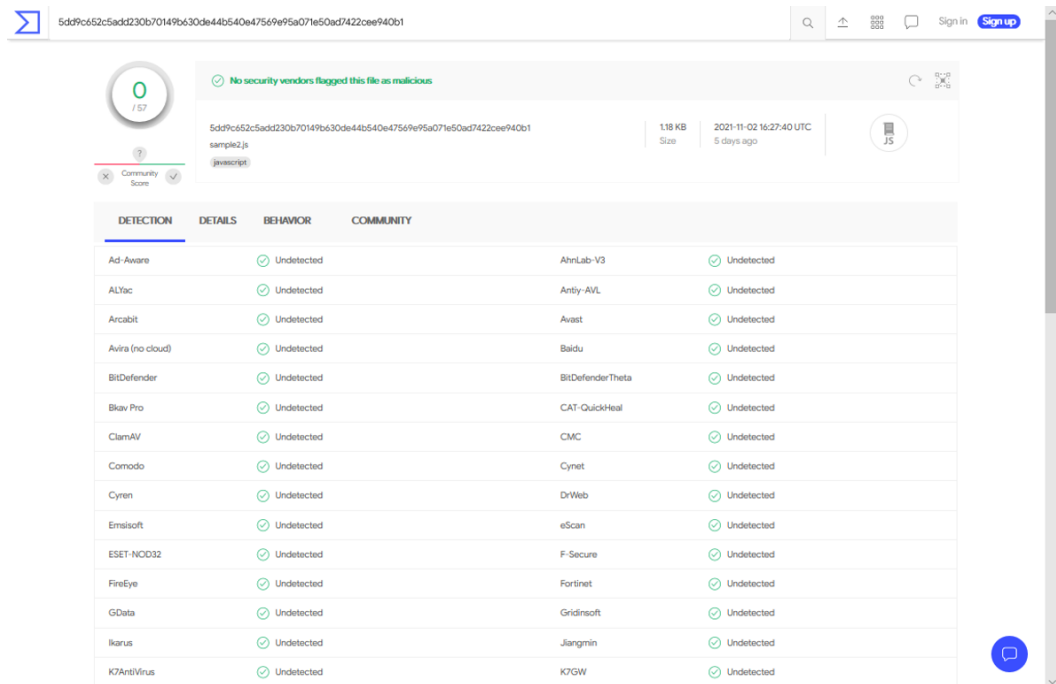
node /tmp/UfdPF5X4jZ.js
undefined:1
WScript.Echo("You have been hacked!");WScript.Echo("I
hope you did not run this on your own PC...");var
f="Facultatea";var m1="de Matematica si
Informatica";var unibuc="Universitatea din
Bucuresti";var curs="Curs Info anul 3";var
minciuna="Acesta este un malware. Dispozitivul
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!")}}

ReferenceError: WScript is not defined
    at eval (eval at <anonymous> (/tmp/UfdPF5X4jZ.js:1:1), <anonymous>:1:1)
    at Object.<anonymous> (/tmp/UfdPF5X4jZ.js:1:1)

```

Your device is missing important updates  
Select this icon for more info.

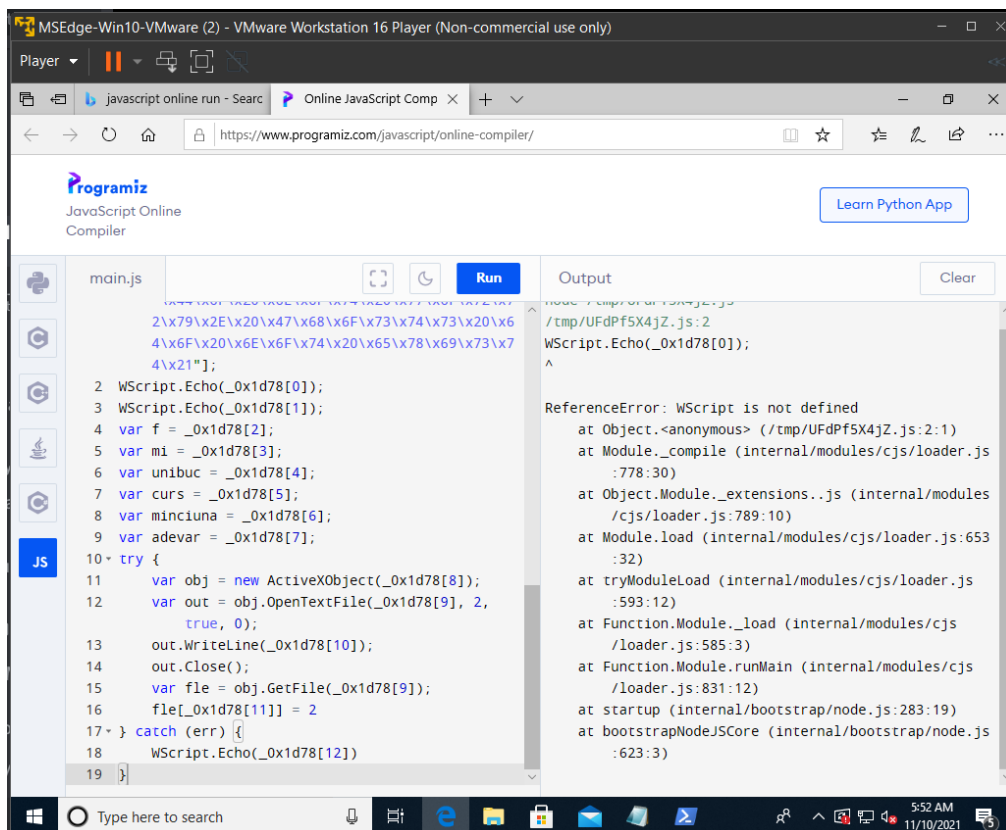
b. Nu



DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Ad-Aware	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Anly-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
BitDefender	Undetected	CAT-QuickHeal	Undetected
ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	Cynet	Undetected
Cyren	Undetected	DrWeb	Undetected
Emsisoft	Undetected	eScan	Undetected
ESET-NOD32	Undetected	F-Secure	Undetected
FireEye	Undetected	Fortinet	Undetected
GData	Undetected	Gridinsoft	Undetected
Ikarus	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected

c.

3.



```

main.js
1 2\x79\x2E\x20\x47\x68\x6F\x73\x74\x20\x6
4\x6F\x20\x6E\x6F\x74\x20\x65\x78\x69\x73\x7
4\x21"];
2 WScript.Echo(_0x1d78[0]);
3 WScript.Echo(_0x1d78[1]);
4 var f = _0x1d78[2];
5 var m1 = _0x1d78[3];
6 var unibuc = _0x1d78[4];
7 var curs = _0x1d78[5];
8 var minciuna = _0x1d78[6];
9 var adevar = _0x1d78[7];
10 try {
11 var obj = new ActiveXObject(_0x1d78[8]);
12 var out = obj.OpenTextFile(_0x1d78[9], 2,
true, 0);
13 out.WriteLine(_0x1d78[10]);
14 out.Close();
15 var file = obj.GetFile(_0x1d78[9]);
16 file[_0x1d78[11]] = 2
17 } catch (err) {
18 WScript.Echo(_0x1d78[12])
19 }
  
```

```

Output
/tmp/UFdPf5X4jZ.js:2
WScript.Echo(_0x1d78[0]);
^
ReferenceError: WScript is not defined
    at Object.<anonymous> (/tmp/UFdPf5X4jZ.js:2:1)
    at Module._compile (internal/modules/cjs/loader.js
:778:30)
    at Object.Module._extensions..js (internal/modules
/cjs/loader.js:789:10)
    at Module.load (internal/modules/cjs/loader.js:653
:32)
    at tryModuleLoad (internal/modules/cjs/loader.js
:593:12)
    at Function.Module._load (internal/modules/cjs
/loader.js:585:3)
    at Function.Module.runMain (internal/modules/cjs
/loader.js:831:12)
    at startup (internal/bootstrap/node.js:283:19)
    at bootstrapNodeJSCore (internal/bootstrap/node.js
:623:3)
  
```

a.

b. Continutul de tipul 'x\$\$' este facut pentru a evita programele de antivirus si reprezinta un numar in hexa.

c. Spre deosebire de sample2, in sample3 avem nume de variabile in format hexa:

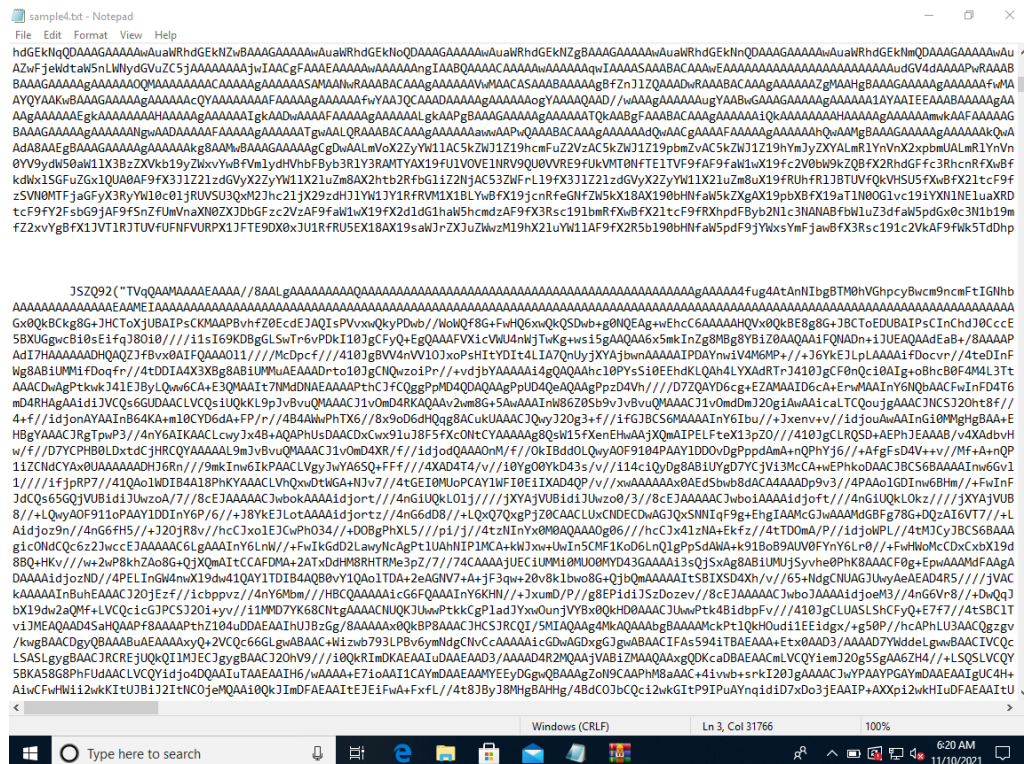
4.

a. Ruleaza la infinit (pentru o perioada foarte mare de timp). Compilatorul online s-a blocat in timp ce rulam

b. In urma unei analize statice se pot observa urmatoarele apeluri de functii in cod:

```
JSZQ92("ceva" + "" FZ52 + "hello.exe");
JSZQ92("ceva" + "" FZ52 + "libstdc++-6.dll");
JSZQ92("ceva" + "" FZ52 + "libgcc_s_dw2-1.dll");
JSZQ92("ceva" + "" FZ52 + "libmingwex-0.dll");
JSZQ99("" + FZ52 + "hello.exe");
```

c. Da, pentru ca continutul fisierului este neinteligibil si suspicios



MSEdge-Win10-VMware (2) - VMware Workstation 16 Player (Non-commercial use only)

Player

javascript online run - Search Online JavaScript Compiler VirusTotal - File - a196e

https://www.virustotal.com/gui/file/a196ea13937f9b858c9fb2a56eef139d324a022cbd21adcc217f7e581a73e21

a196ea13937f9b858c9fb2a56eef139d324a022cbd21adcc217f7e581a73e21

18 / 58

18 security vendors flagged this file as malicious

a196ea13937f9b858c9fb2a56eef139d324a022cbd21adcc217f7e581a73e21  
sample4.js  
text

3.39 MB  
Size

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

Community Score

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.BEtr	GData	JS.Heur.Cbum.1.64A98D8B.Gen
Ikarus	Trojan-Downloader.JS.Xibow	Kaspersky	HEUR:Trojan-Dropper.Script.Generic

Type here to search

6:18 AM 11/10/2021

d.

e.

18 / 58

18 security vendors flagged this file as malicious

a196ea13937f9b858c9fb2a56eef139d324a022cbd21adcc217f7e581a73e21  
sample4.js  
text

3.39 MB  
Size

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

Community Score

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.BEtr	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.dqzgww	Sangfor Engine Zero	Malware.Generic-VBS.Save.a7030c38
AhnLab-V3	Undetected	Antiy-AVL	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender Theta	Undetected	Bkav Pro	Undetected
CAT-QuickHeal	Undetected	ClamAV	Undetected
CMC	Undetected	Comodo	Undetected
Cynet	Undetected	DrWeb	Undetected