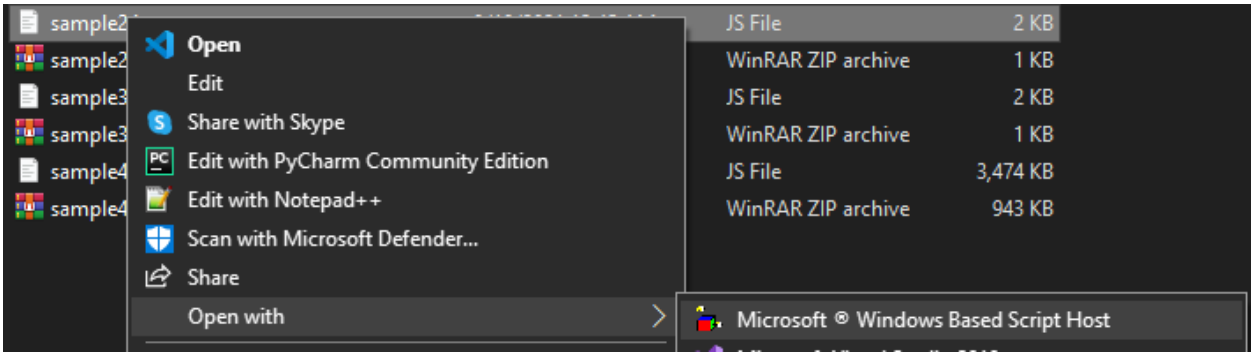
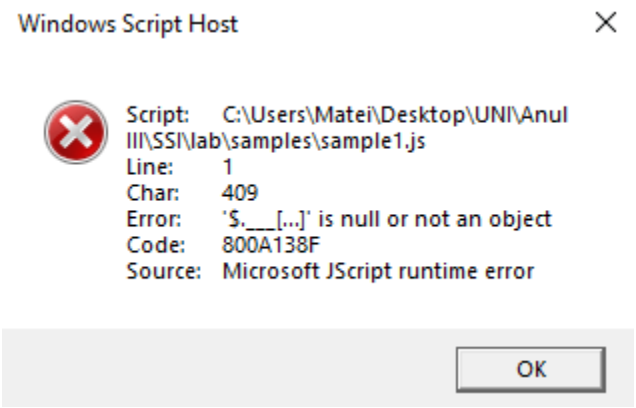
Mîndruleanu Matei Daniel - tema 5 SSI

Exercitiul 1:

Am incercat sa rulez scriptul cu Microsoft Windows Based Script Host si am obtinut urmatoarele rezultate:

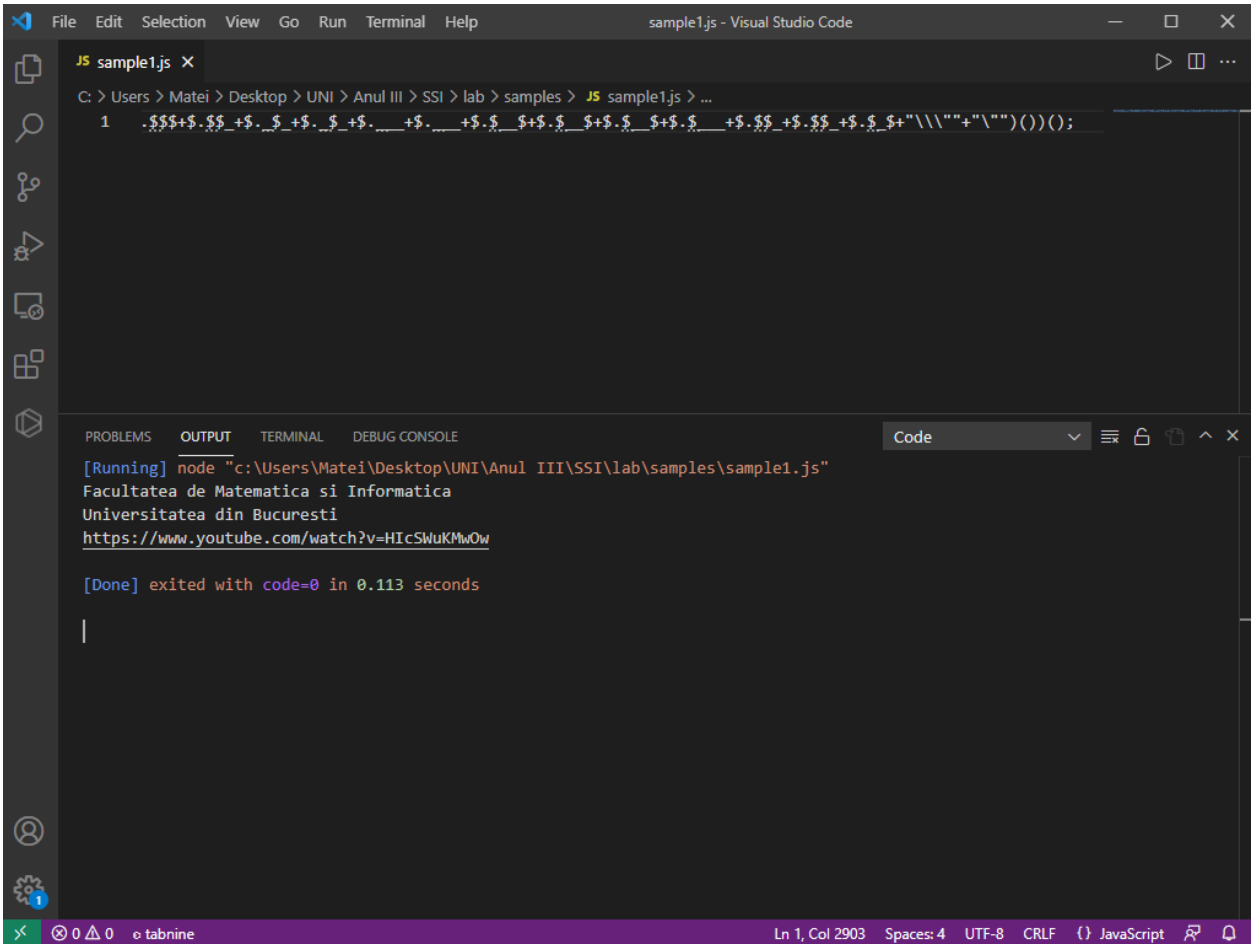




Am rulat codul din arhiva de la primul sample in visual studio code si am aflat ca acesta afiseaza in consola

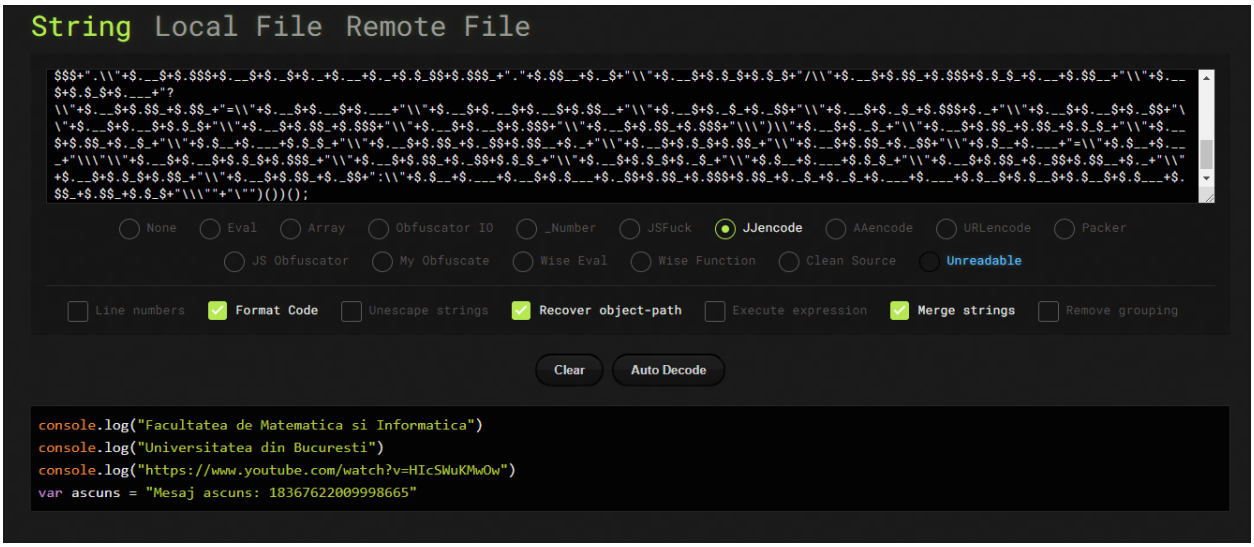
```
[Running] node "c:\Users\Matei\Desktop\UNI\Anul III\SSI\lab\samples\sample1.js"
Facultatea de Matematica si Informatica
Universitatea din Bucuresti
https://www.youtube.com/watch?v=HIcSWuKMwOw
```

,link-ul fiind “rickroll, but it never starts 10 HOURS” de pe YouTube.



Am aflat faptul ca programul este de tip JJencode si am folosit site-ul https://lelinhtinh.github.io/de4js/ pentru a afla mai multe despre acesta (mesajul ascuns?).

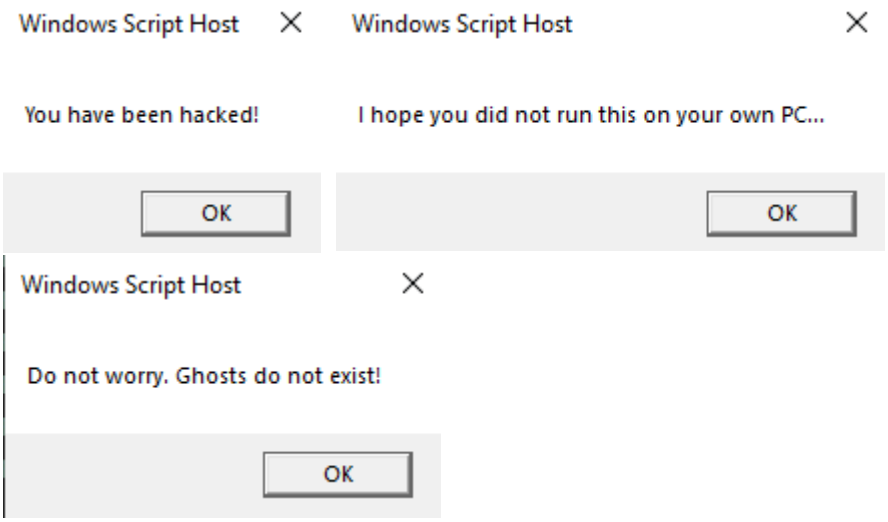
```
Mesajul ascuns este: "Mesaj ascuns: 18367622009998665"
```



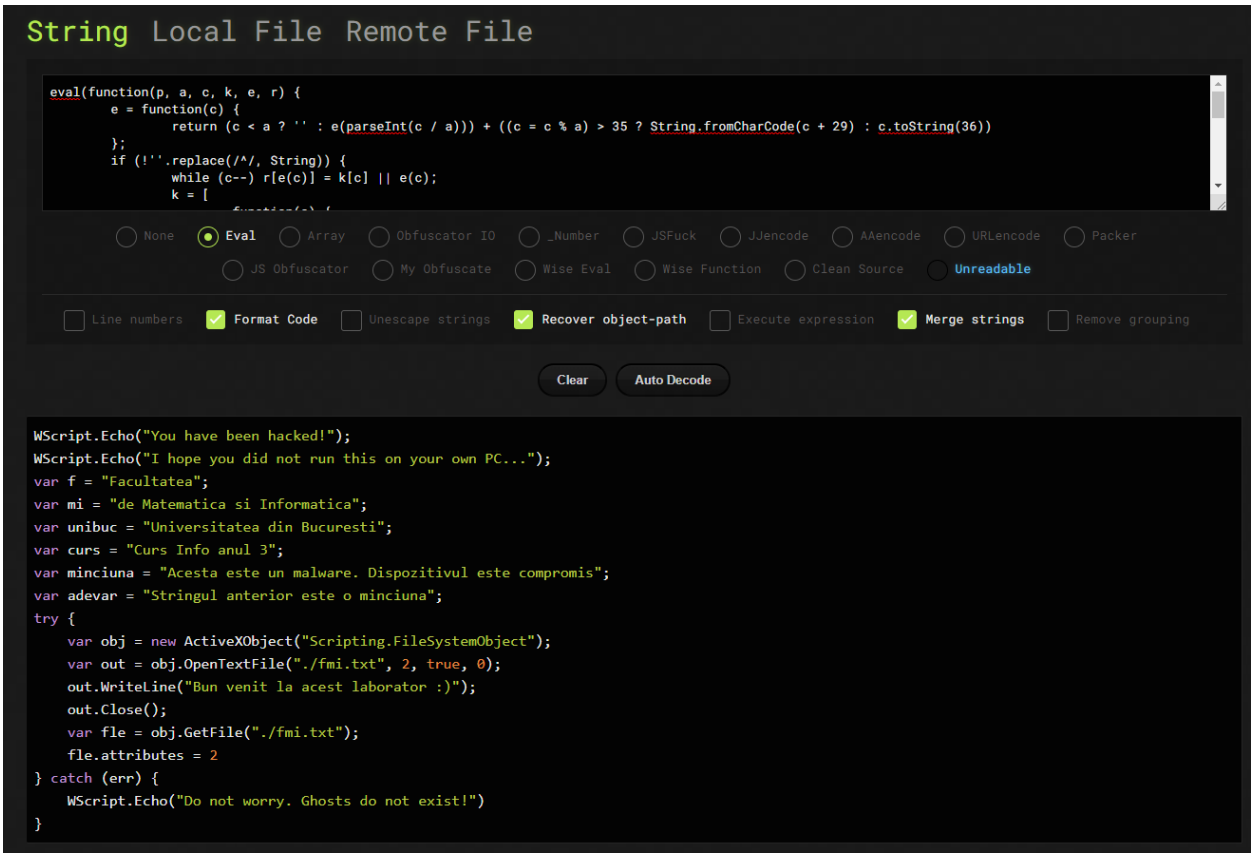
Codul a fost scris de o persoana care a vrut ca cei la care ajunge acesta sa nu il poata descifra.

Exercitiul 2:

Am incercat sa rulez scriptul cu Microsoft Windows Based Script Host si am obtinut urmatoarele rezultate:



Rularea codului in visual studio code nu s-a putut realiza, asa ca am trecut la analizarea codului direct in https://lelinhtinh.github.io/de4js/ folosind Eval pentru urmatoarele rezultate:



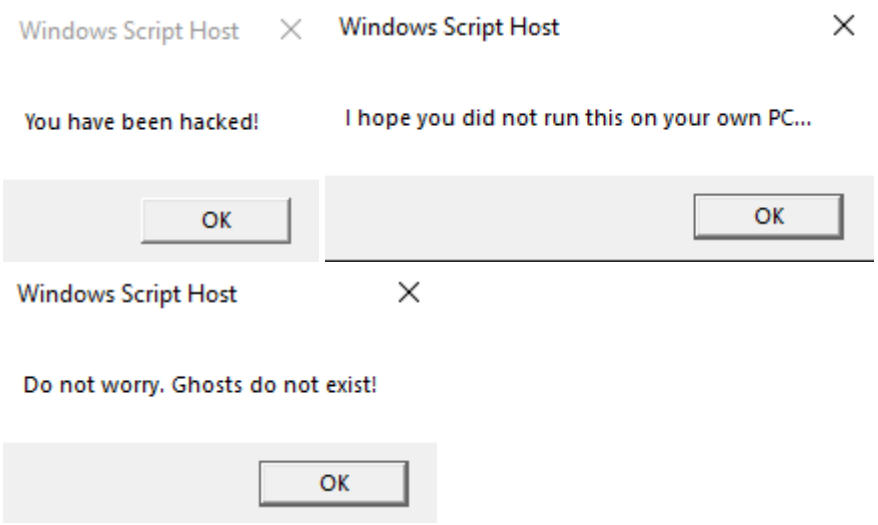
Codul afiseaza mesajele: "You have been hacked!" si "I hope you did not run this on your own PC..."

Dupa care incearca sa creeze fisierul fmi.txt in care sa scrie “Bun venit la acest laborator”, dar daca prinde vreo eroare afiseaza mesajul "Do not worry. Ghosts do not exist!".

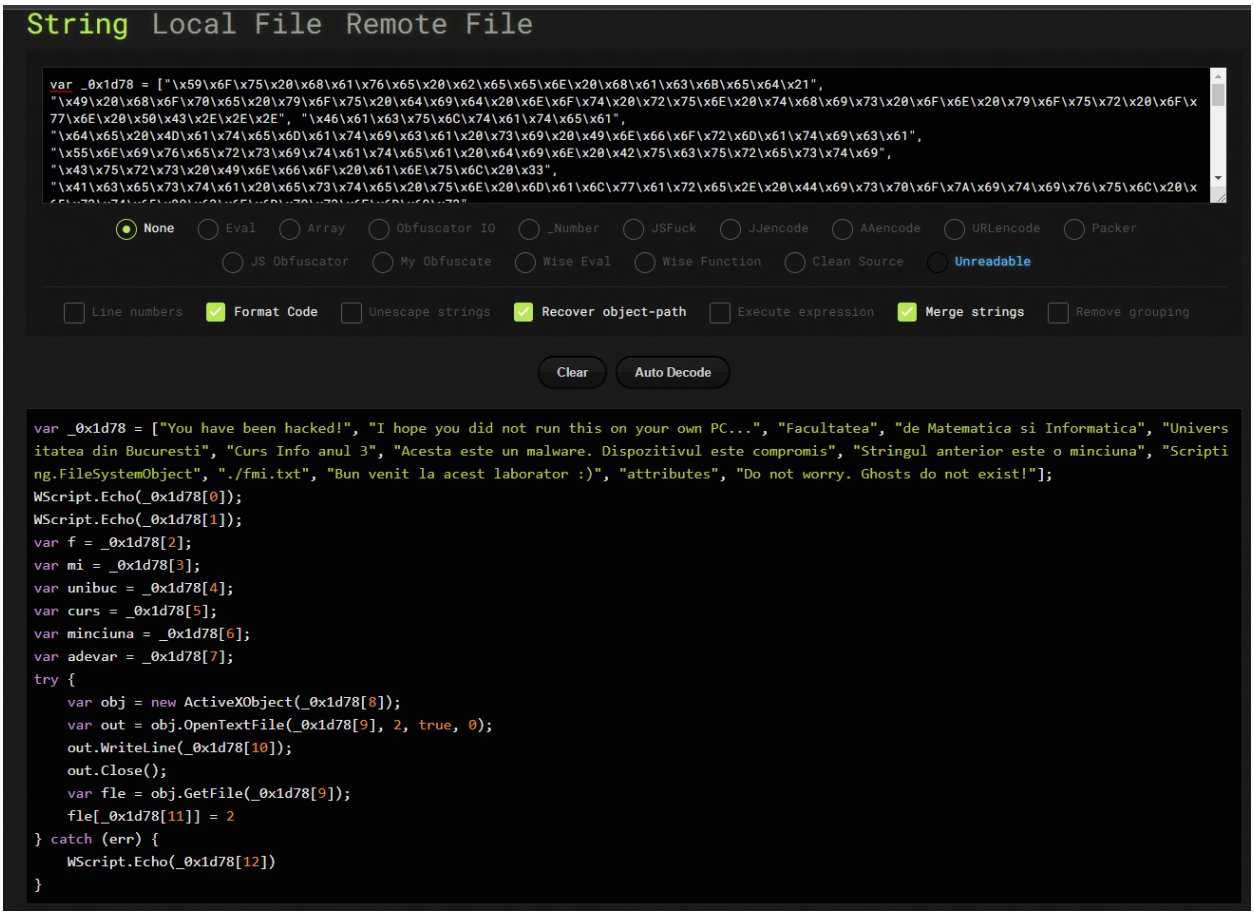
Fisierul nu este un malware deoarece, in mod evident, nu are scop malitios, acesta este menit doar sa afiseze niste mesaje sau/si sa creeze un fisier de tip txt inofensiv fiind realizat de o persoana in scop informativ.

Exercitiul 3:

Am incercat sa rulez scriptul cu Microsoft Windows Based Script Host si am obtinut urmatoarele rezultate:



Dupa trecerea codului prin https://lelinhtinh.github.io/de4js/ observam ca acesta are acelasi rol ca sample 2.



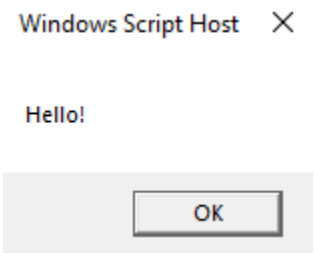
Codul nu ruleaza in vsc, dar observam ca acesta este scris direct in js. Mesajele acum sunt scrise in hexa.

Fata de codul din sample 2, acum mai avem si un array de stringuri, fiecare variabila avand un indice pentru un string din sirul definit la inceput.

‘\x$$’ reprezinta faptul ca valorile sunt scrise in hexa.

Exercitiul 4:

Am incercat sa rulez scriptul cu Microsoft Windows Based Script Host si am obtinut urmatoarele rezultate:



Daca convertim fiecare comentariu din base 64 in string obtinem urmatoarele:

hello world

this sample is a javascript

JavaScript sample

FMI UNIBUC

Facultatea de Matematica si Informatica

Felicitari

Universitatea din Bucuresti

Dezactivati antivirusul inainte de a rula acest exercitiu

unibuc in hex <- in hexa

Suspicios

Laborator

UNIBUC FMI

Universitatea din Bucuresti Facultatea de Matematica si Informatica

Acesta este un script

Acesta este un comentariu

Comentariu

Universitate

Run

Acest comentariu este ascuns <- 2x

Acest comentariu este ascuns <- 3x

Daca incercam sa convertim stringul din base64 din primul apel al functiei JSZQ92 obtinem ceva de genul:

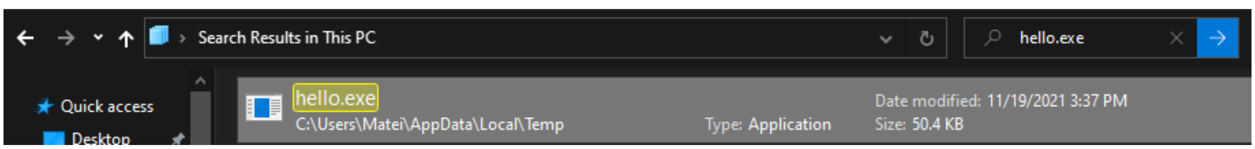
MZ□□@□□□ !□L!This program cannot be run in DOS mode.

$PEL□□'<a□□□□□□□□□,□□□0@□□□□□P□□□ □□□□pX□□□Dq.text(□□□□`P`.data□0□□@0.rdata□@□□@0@/4
d□P□□@0@.bssp`0.idataX□p□$@0.CRT□□,@0.tls □.@0/14X□0@@B/29UST2@□B/41c□□□□@□B/55O□ □□@□B/
6780□□@0B/80@□□@□B□D$ =wN=s`=□□D$□□$□□□□H□□&1□□&=tl=□=uD$□□$□□□□t□$□и뽍D$□□$□`□□uD
$□□□$□G□k'=□□UD$□□$□□□□tY□4□$□и#□$□и□D$□□□$□□□$□D$□□□$□□D$□□□$□□t&'US□x@@t□D$□D
$□□□$Ѓ□$□@□□□□0@□$□>□$`@tB□q@0@D$□C□□$/□$`@D$□C0□$□□$`@D$□CP□$□□□□□0@□  □□□D$□`
@D$□□`@□$□□□$M□'<D$,D$□`@□$□`@D$,D$□□0@□DD(D$□□<Đ□□$□□q@t&'□□$□□q@t&'%q@v'%q@UV
S□□$@@p□□□□$@@7□□l`@D$□□@@□$7□□D$□)@@□$"□□0@t□D$□□`@□$P@□0@t:□$A@@
□t□D$□O@@□$
□□t □$□0@□$0□@□e[^]Ív□0@ @ @
U□0@t   □$P@Cl`@t□□$

Observam ca toate cele 4 apeluri ale functiei incep cu “MZ—
@ !L!This program cannot be run in DOS mode.”

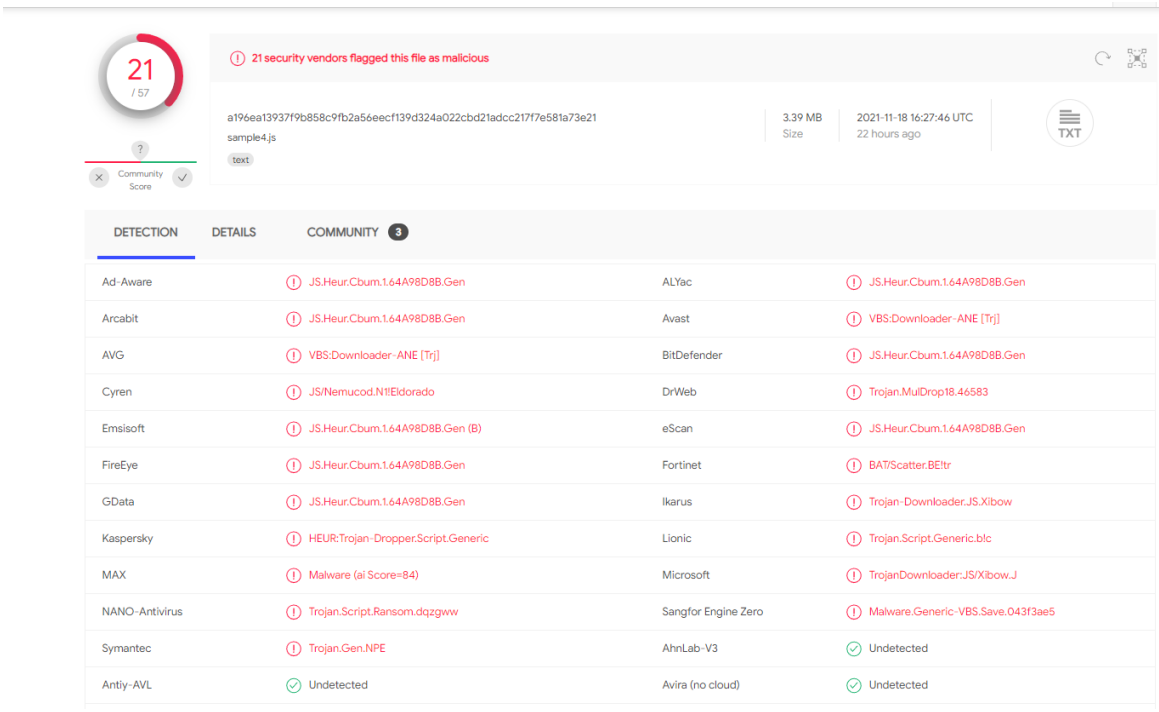
Observam din analiza statica faptul ca sample-ul incearca sa execute un try care vrea sa creeze un obiect cu ajutorul functiei JSZQ99, si sa scrie ceva in acest obiect, dupa care sa il lase in calculator(un executabil), dar prinde o eroare, deci afiseaza doar “Hello!”.

Teoretic programul este malware, deoarece el instaleaza in calculator un .exe.



Din fericire, acest executabil este inofensiv.

Site-ul VirusTotal detecteaza fisierul ca fiind un malware.



Observam ca dupa obfuscarea fisierului, numarul de flaguri a scazut drastic, acesta continuand sa fie semnalat ca malware.