Tudorache Alexandru-Theodor

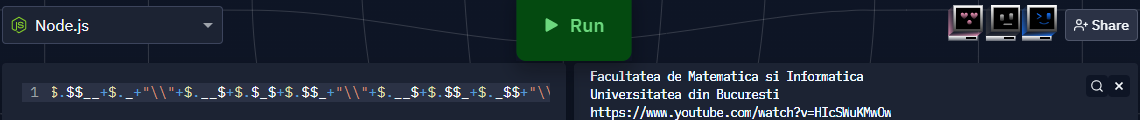
Grupa 342

Laborator 5

Securitatea Sistemelor Informatice

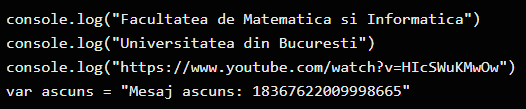
1.

Acest cod afiseaza in consola





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

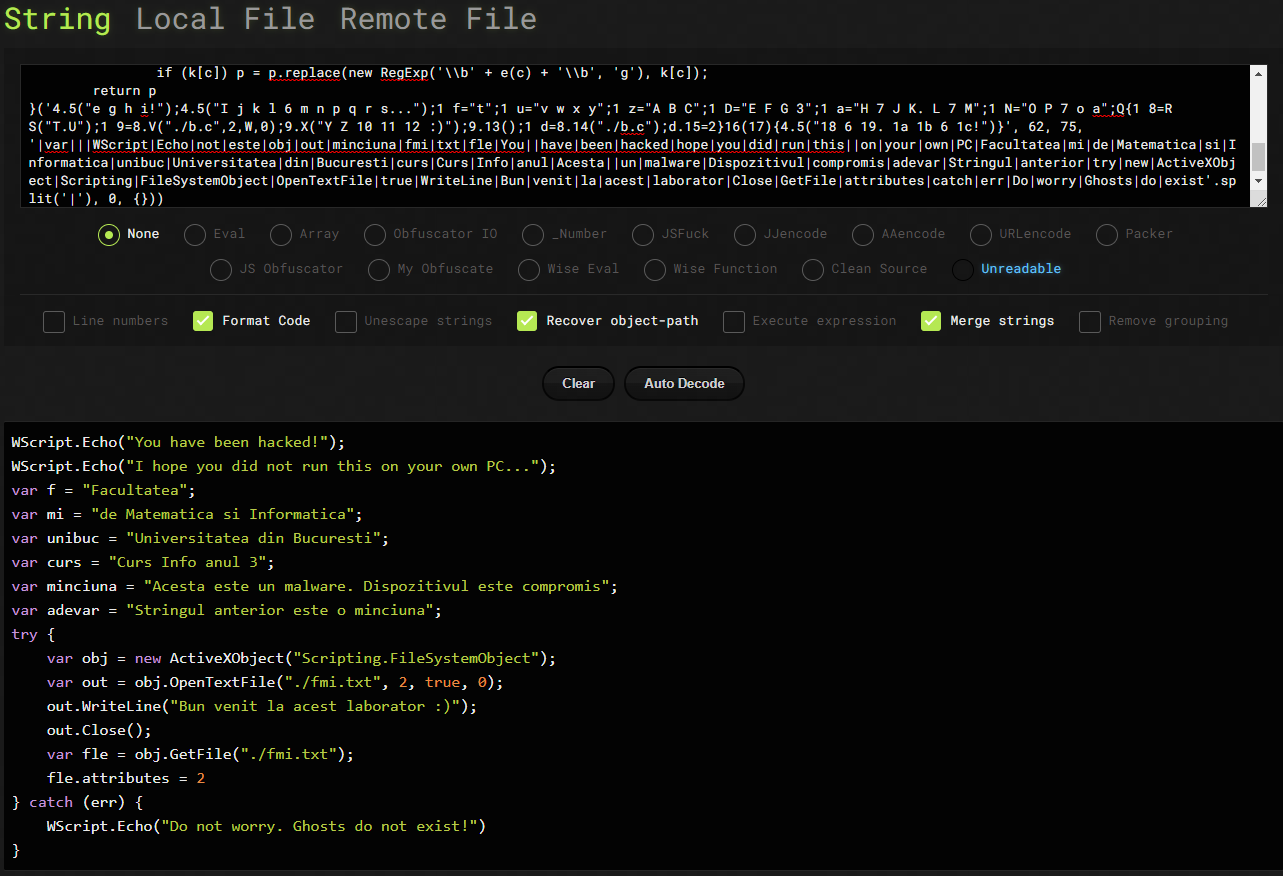


Mesajul ascuns este *18367622009998665.*

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

2.

Codul sursa deobfuscat este:



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:

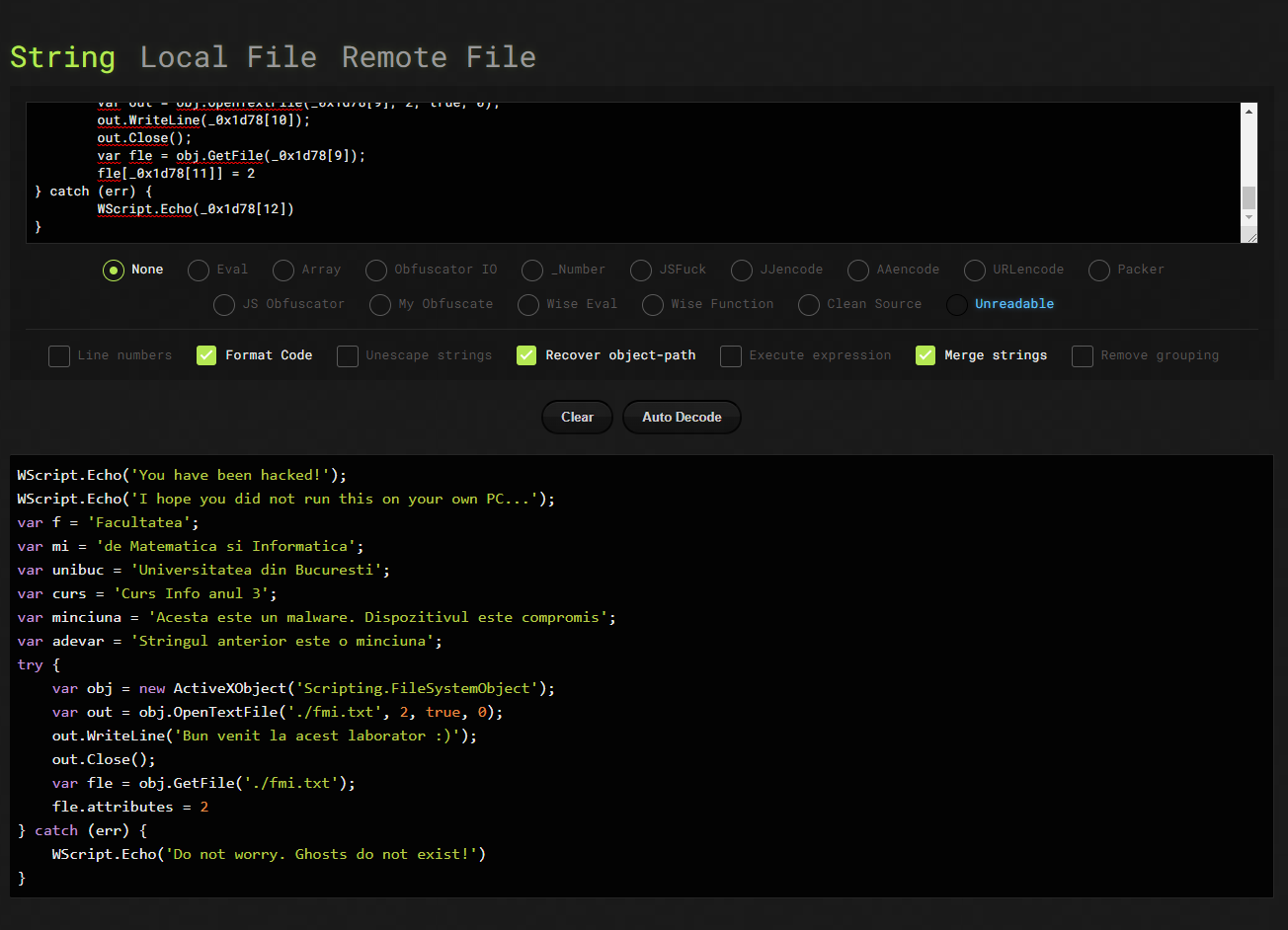
*I hope you did not run this on your own PC... ;*

*\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.

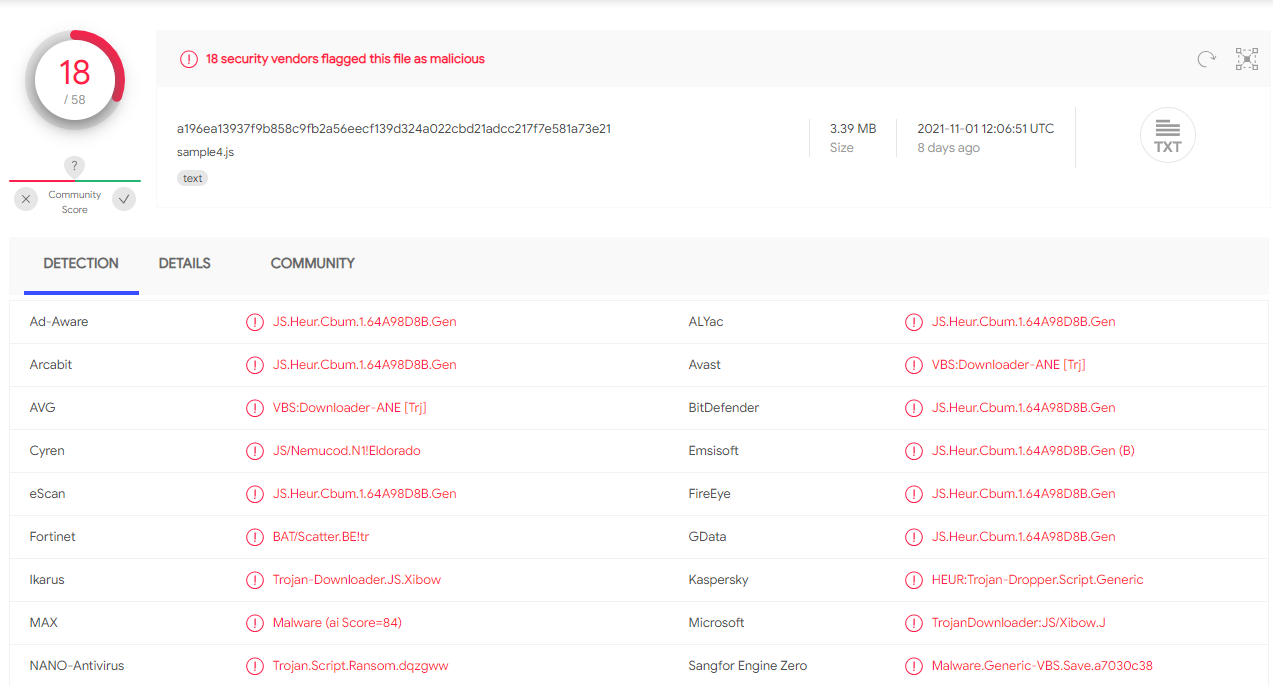
4.

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.



e.

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

