Lab9

joi, 21 decembrie 2023 17:49

1.

a) codul dat genereaza urmatorul mesaj pe ecran:

Facultatea de Matematica si Informatica
Universitatea din Bucuresti
https://www.youtube.com/watch?v=HIcSWuKMwOw

b) am rulat scriptul online - folosind o analizare dinamica

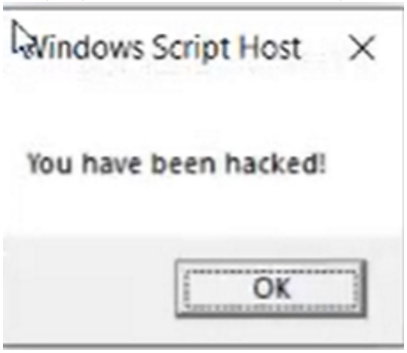
c) mesajul ascuns este: 18367622009998665

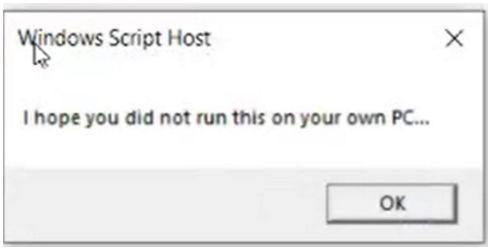
am deobfuscat mesajul folosind https://lelinhtinh.github.io/de4js/

d) obfuscator online

2. a. apar pe ecran două ferestre la care facem un ups maricel:

You have been hacked!
I hope you did not run this on your own PC...





si incearca sa creeze un fisier text 'fmi.txt' cu mesajul:

Bun venit la acest laborator ;)

b) nu este considerat malware

c) -

3. a) apar pe ecran aceleasi două ferestre :

You have been hacked!
I hope you did not run this on your own PC...
daaar apoi incearca doar sa creeze un fisier text 'fmi.txt' cu mesajul:

Bun venit la acest laborator ;)

b) \x$$ reprezinta valorile in hexa (deci codul e mai greu de analizat la prima vedere)

c) diferenta este ca 3 foloseste caractere in hexa ca sa nu ne putem da seama direct de ce face codul (sa nu il putem analiza static)

4. a) Afiseaza pe ecran mesajul Hello

b) ca sa putem extrage payload ul putem sa convertim load-urile din base64 in ascii

c) nu este malware

d) pe VirusTotal apare ca 30% malware, deci putem considera ca nu e malware

e) sample4_obs.js - 5% safe - nu il recunoaste ca virus