E1

<https://www.53lu.com/tool/jjencode/>

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"

encodare de JJencode

E2

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 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 fle = obj.GetFile("./fmi.txt");

fle.attributes = 2

} catch (err) {

WScript.Echo("Do not worry. Ghosts do not exist!")

}

Nu ruleaza dar banuiesc ca ar trebui sa apara cateva text boxuri, si se creaza un fisier nou hidden (attribute 2) fmi.txt

E3

La fel ca cel de sus

Caractere in hexa, decodat:

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",

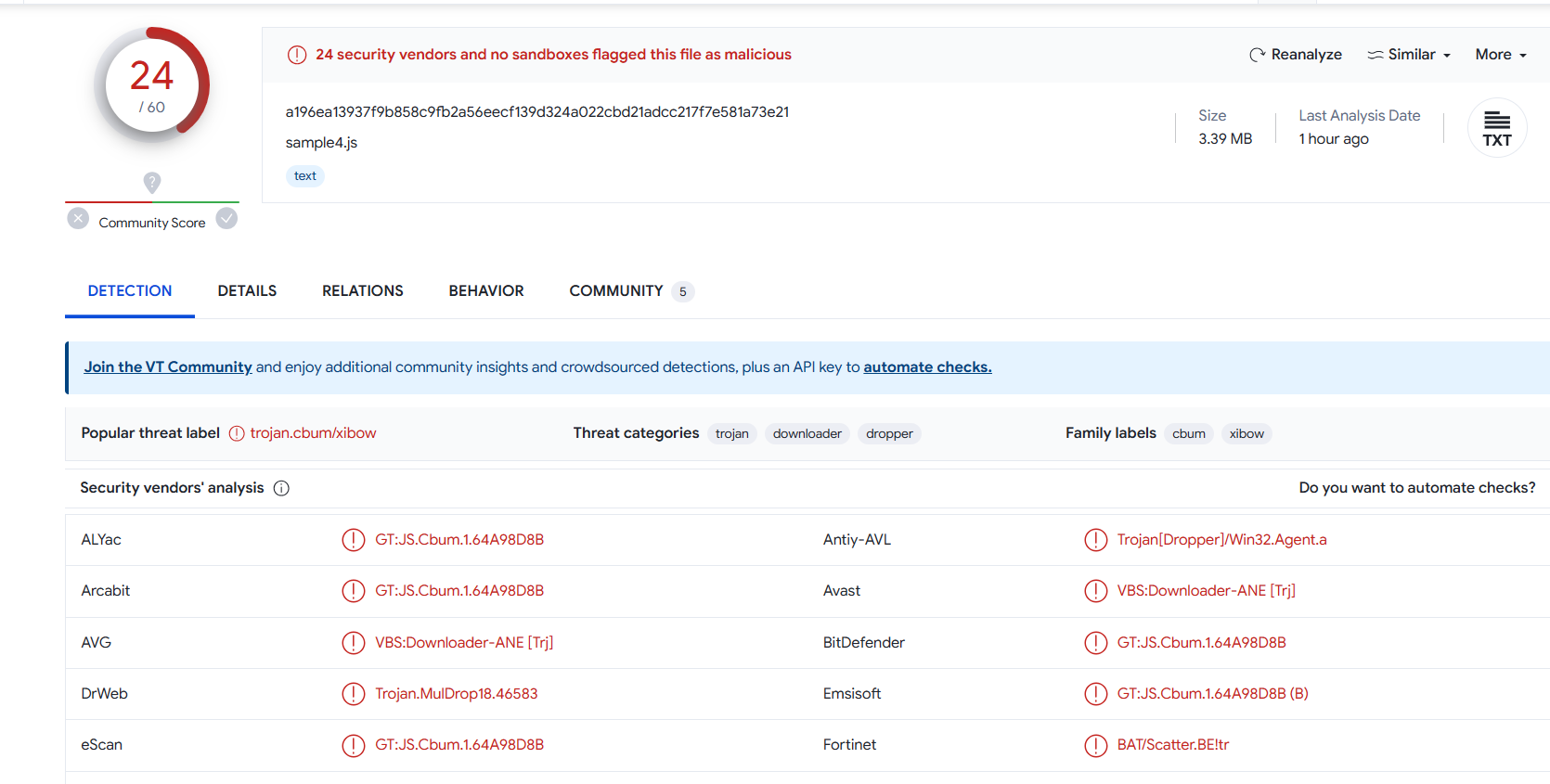
"Do not worry. Ghosts do not exist!"

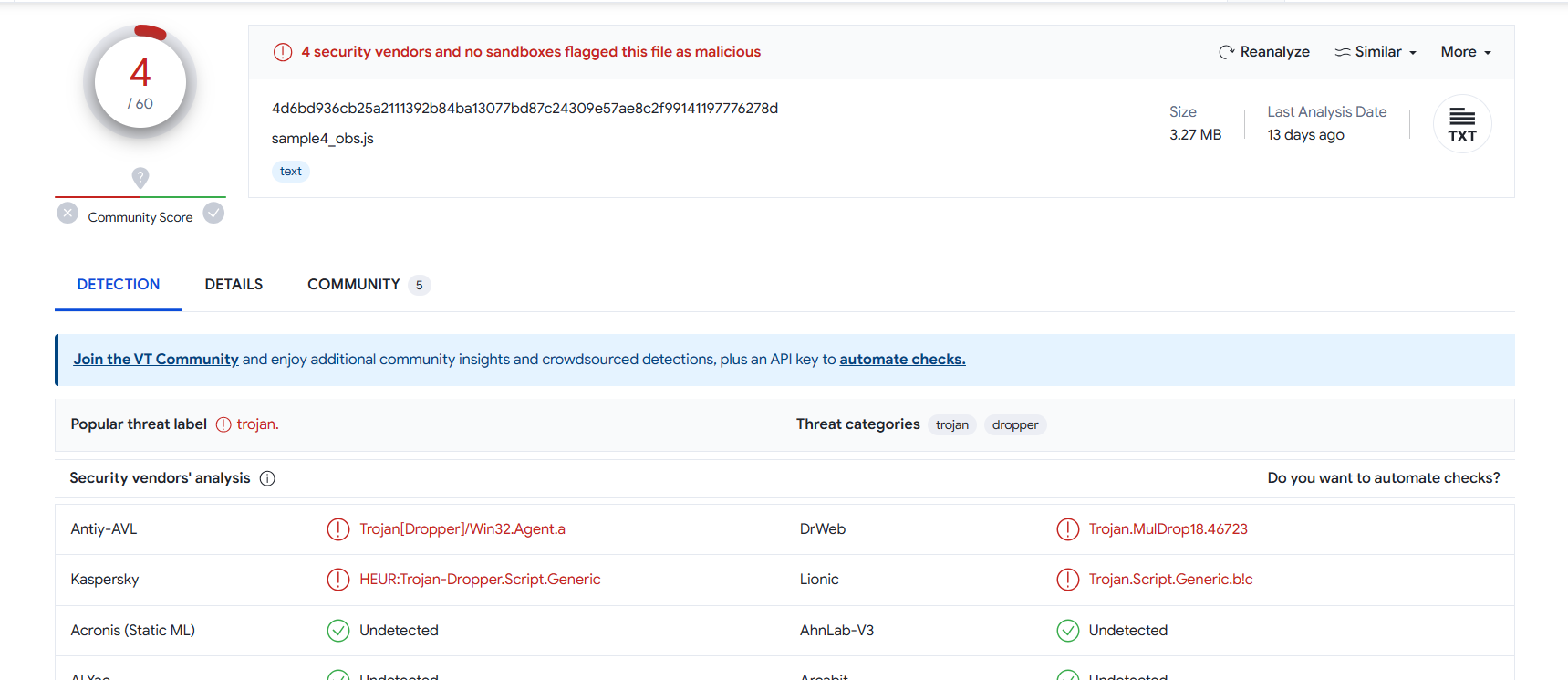
];

Primul foloseste eval care face ca analiza codului sa fie mai putin straight forward

s-a dovedit la e4 ca asta duce si la pacalirea antivirusului

E4





Obfuscarea face ca fisierul sa fie gasit drept malware de mai putine antivirusuri => le poate pacali