Ministerul Educaţiei și Cercetării

al Republicii Moldova   
Universitatea Tehnică a Moldovei

Faculatea Calculatoare, Infromatică și Microelectronică   
  
  
  
  
  
  
  
RAPORT

# LUCRARE DE LABORATOR NR. 1

# la Tehnologii ale securității informaționale

**Tema:** Analiza programelor malware. Analiza statică și dinamică. Configurarea programelor antivirus

A efectuat:

st. gr. TI-211 Popa Cătălin

A verificat: Octavian Răducanu

UTM, Chișinău 2023

**Tema:**

Analiza programelor malware. Analiza statică și dinamică. Configurarea programelor antivirus

**Scopul lucrării:**

1. Recunoașterea.

2. Analiza statică.

3. Analiza dinamică.

4. Studierea și configurarea nivelurilor de protecție a unui antivirus.

**Sarcina de bază:**

1. Utilizarea instrumentelor de identificare malware (VirusTotal, Intezer).

2. Analiza fără a executa și studiul structurii programelor malițioase (Pstudio).

3. Analiza cu executarea fișierelor în mediu controlat securizat, în scopul vizualizării comportamentului acestora (OllyDbg).

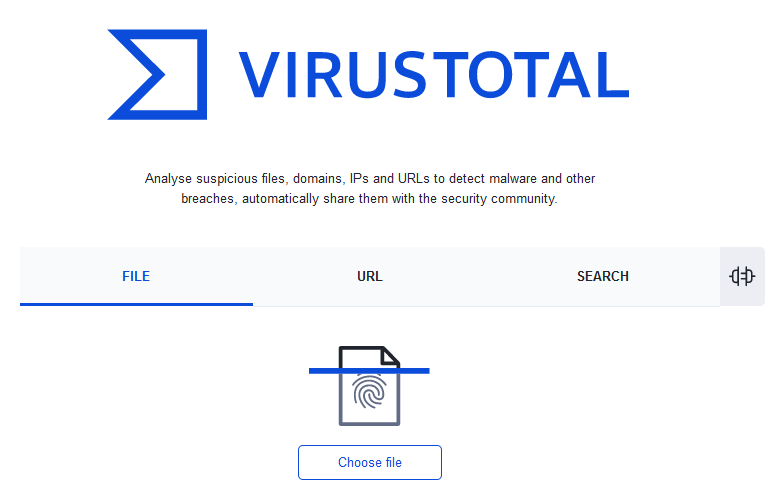
4. Tipuri de scanări, tehnologiile de detecție, nivelurile de protecție (Bitdefender).

**1. Recunoașterea**

**VirusTotal**

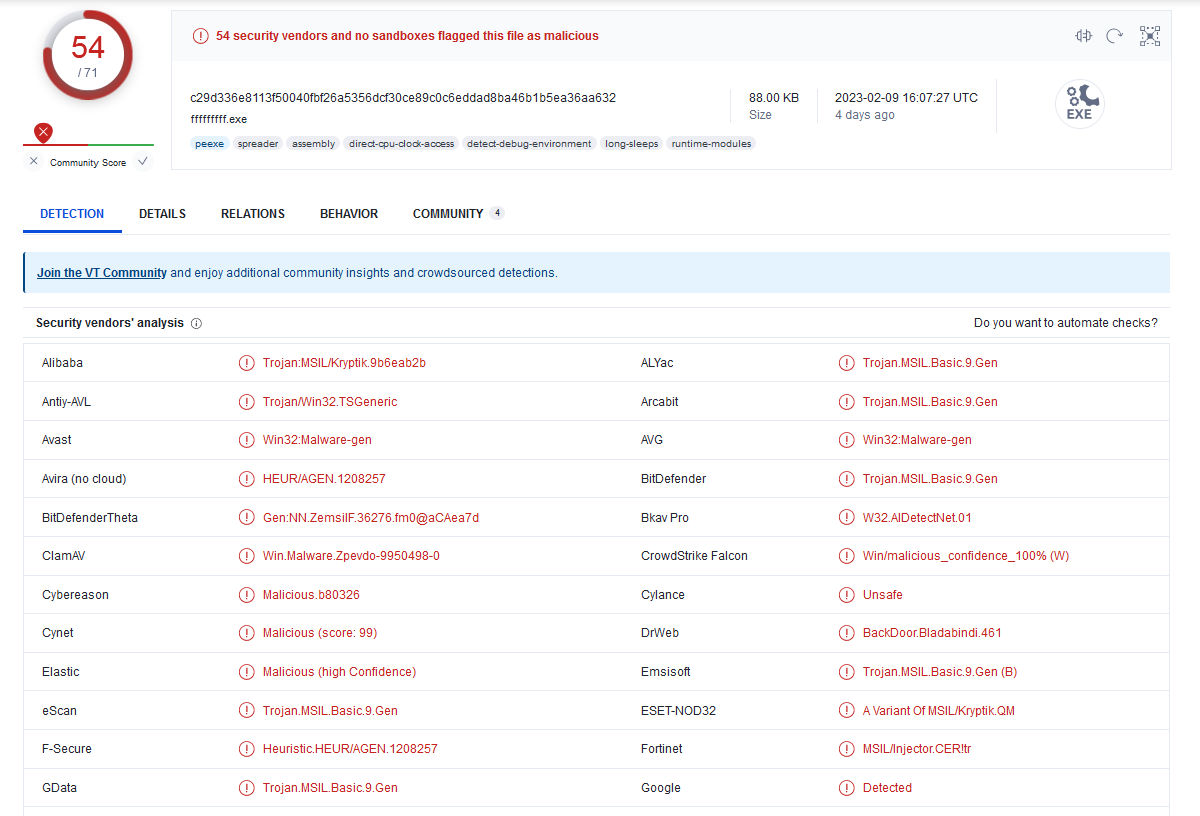
Pentru început, am analizat VirusTotal, care este un serviciu de analiză de fișiere și URL-uri, care a fost fondat în 2004 și acum este deținut de Google. Acesta utilizează tehnologii anti-virus multiple și algoritmi de detectare a amenințărilor pentru a analiza fișiere și URL-uri încărcate de utilizatori în căutarea de malware sau alte amenințări digitale.

VirusTotal oferă o interfață web gratuită pentru utilizatorii individuali și o interfață API pentru dezvoltatorii și organizații. Utilizatorii pot încărca fișiere sau introduce URL-uri pentru a fi scanate, iar VirusTotal va afișa rezultatele scanării, incluzând numărul de detectări ale fiecărui anti-virus și informații despre amenințările identificate. VirusTotal este considerat un instrument important pentru identificarea amenințărilor digitale și ajută la prevenirea răspândirii de malware prin detectarea acestora. Cu toate acestea, trebuie să înțelegem că acesta nu ne va oferi siguranță maximă, deoarece amenințările digitale mereu sunt în dezvoltare.



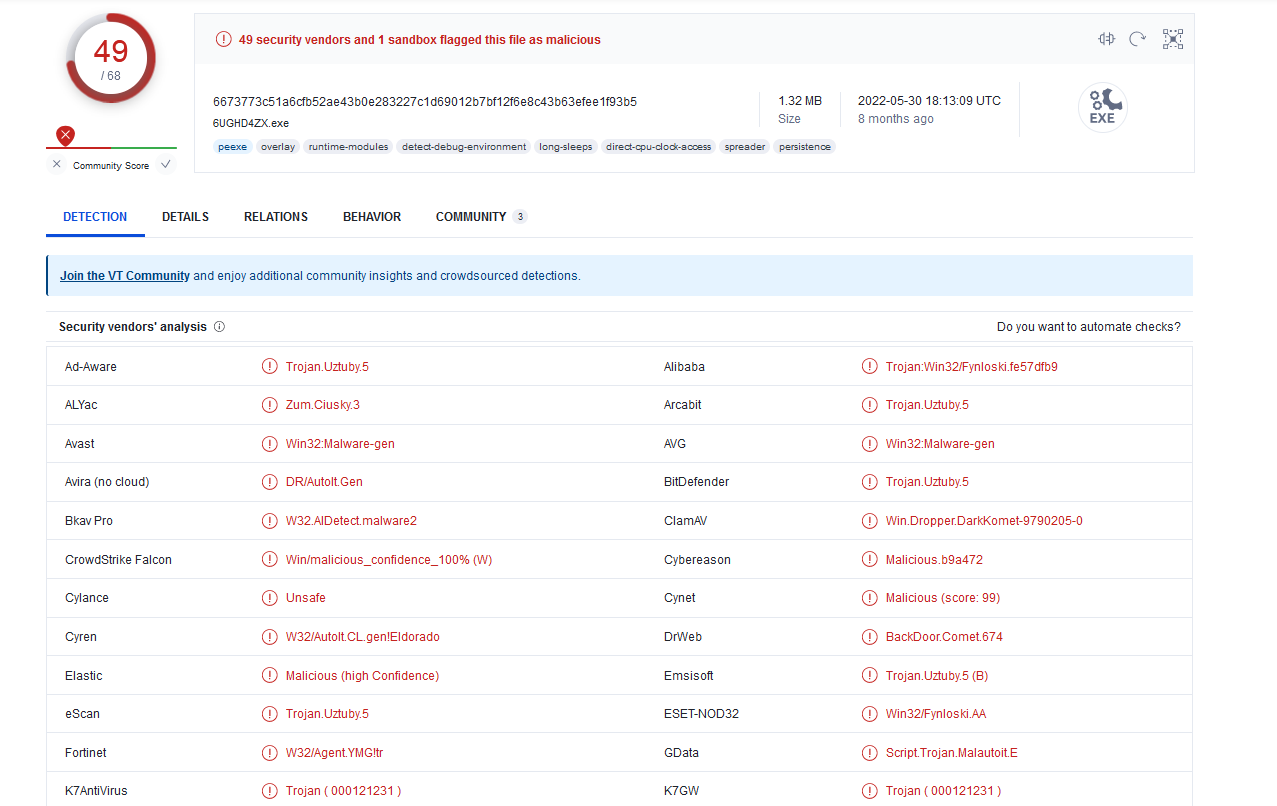
**Figura 1 - Interfața VirusTotal**

Pentru a putea vizualiza funcționalitatea, am luat două exemple în practică și le-am analizat.



**Figura 2 – Verificare fișier suspect**

În figura 2, observăm că în urma verificării fișierului, din cele 68 de antiviruși, 49 au considerat că acesta conține cirus, și anume un Trojan, celelalte 19 au considerat că este inofensivă. Trojan este o fromă de malware care se ascunde sub aparența unui program sau fișier aparent inofensiv, dar care, de fapt, are scopuri malițioase. Acestea pot include, de exemplu, accesarea neautorizată a datelor personale, redirecționarea traficului de internet, utilizarea neautorizată a resurselor sistemului, instalarea altor tipuri de malware sau monitorizarea activității utilizatorilor.



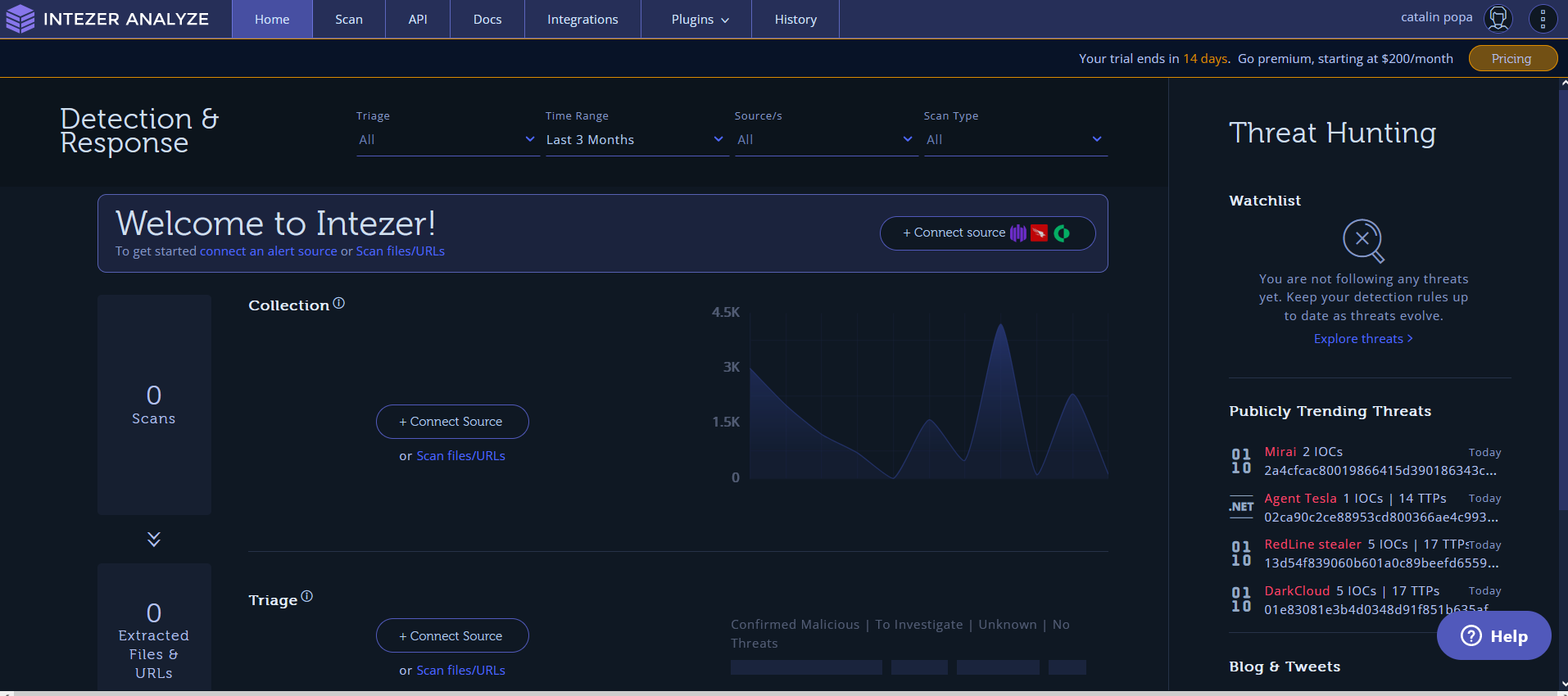
**Figura 3 – Verificare fișier suspect 2**

În figura 3, de asemenea avem rezultatul verificării unui fișier suspect. Observăm de asemenea multe situații malențioase, care pot provoca daune calculatorului și datelor.

**Intezer Analyze**

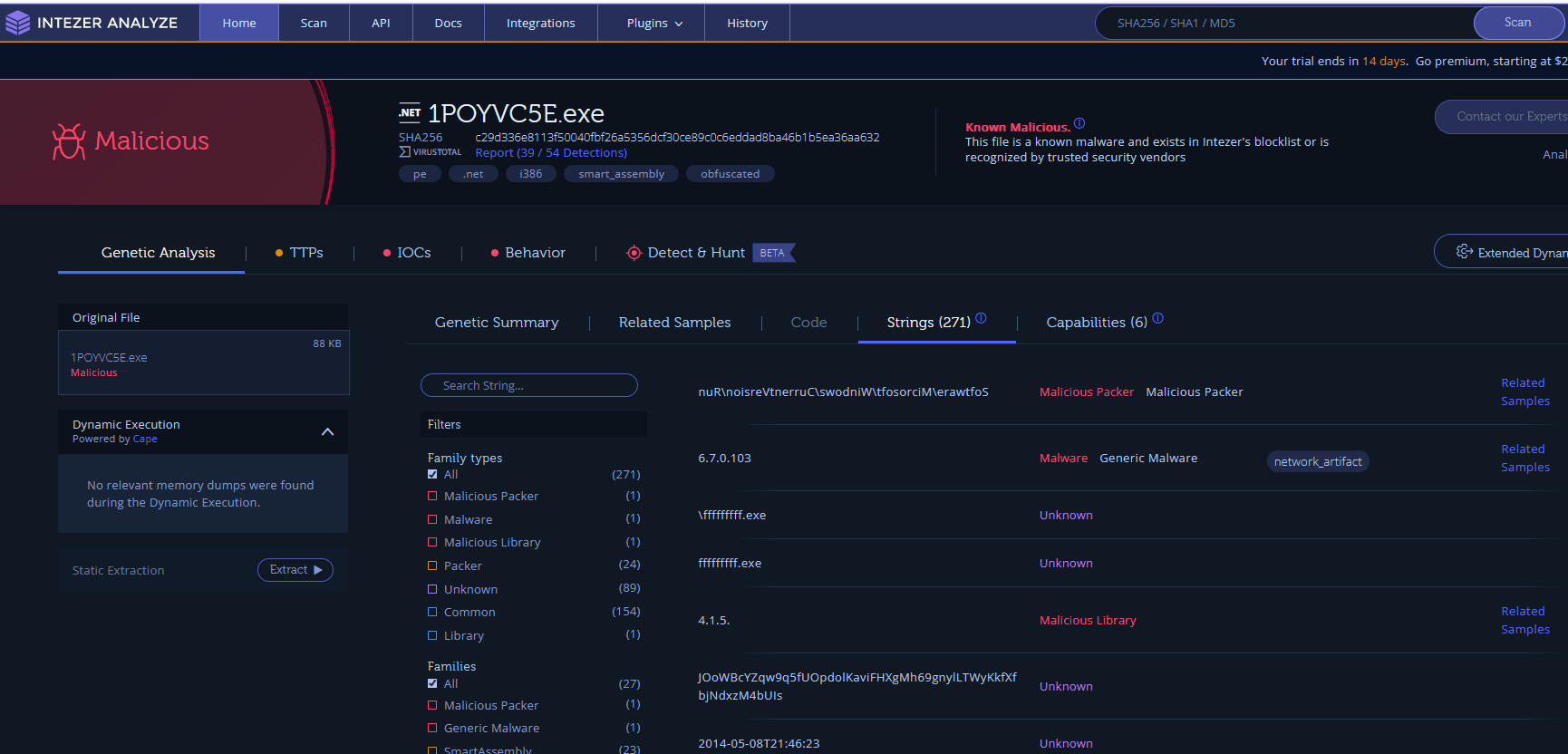
În continuare am analizat Intezer Analyze, care de asemenea este o platformă bazată pe detectarea și analiza amenințărilor, care oferă o vizibilitate profundă asupra funcționării interne a malware-ului, incluzând Troienii. Platforma se bazează pe inteligența artificială și pe algoritmi de învățare automată pentru a analiza și a clasifica malware-ul, permițând înțelegerea mai profundă ale caracteristicilor acestuia. De asemenea, Intezer oferă informații detaliate despre modul în care malware-ul interacționează cu sistemele și aplicațiile, ceea ce ajută la identificarea vulnerabilităților și la îmbunătățirea securității sistemelor.

În figura 4, putem observa interfața grafică a platformei respective.



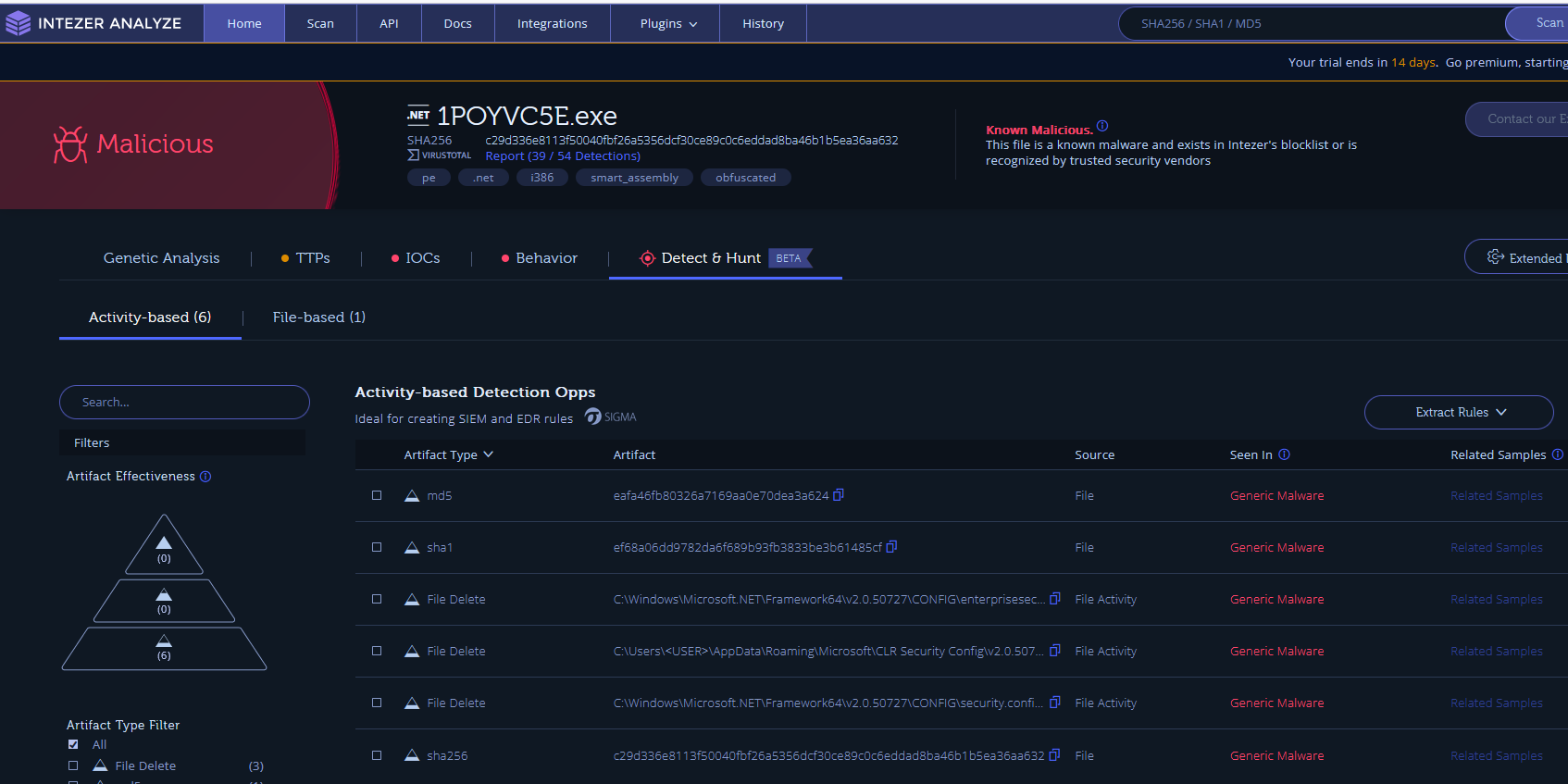
**Figura 4 – Interfața Intezer Analyze**

După cum observăm, platforma Intezer de asemenea ne propune un buton Scan, cu ajutorul căreea ușor putem verifica fișierul dorit. Pentru verificarea eficienții, am luat ca exemplu aceleași file-uri suspecte folosite la VirusTotal. După cum vedem în figura 5, platforma Intezer de asemenea ne informează că fișierul este malențioas și periculoas.

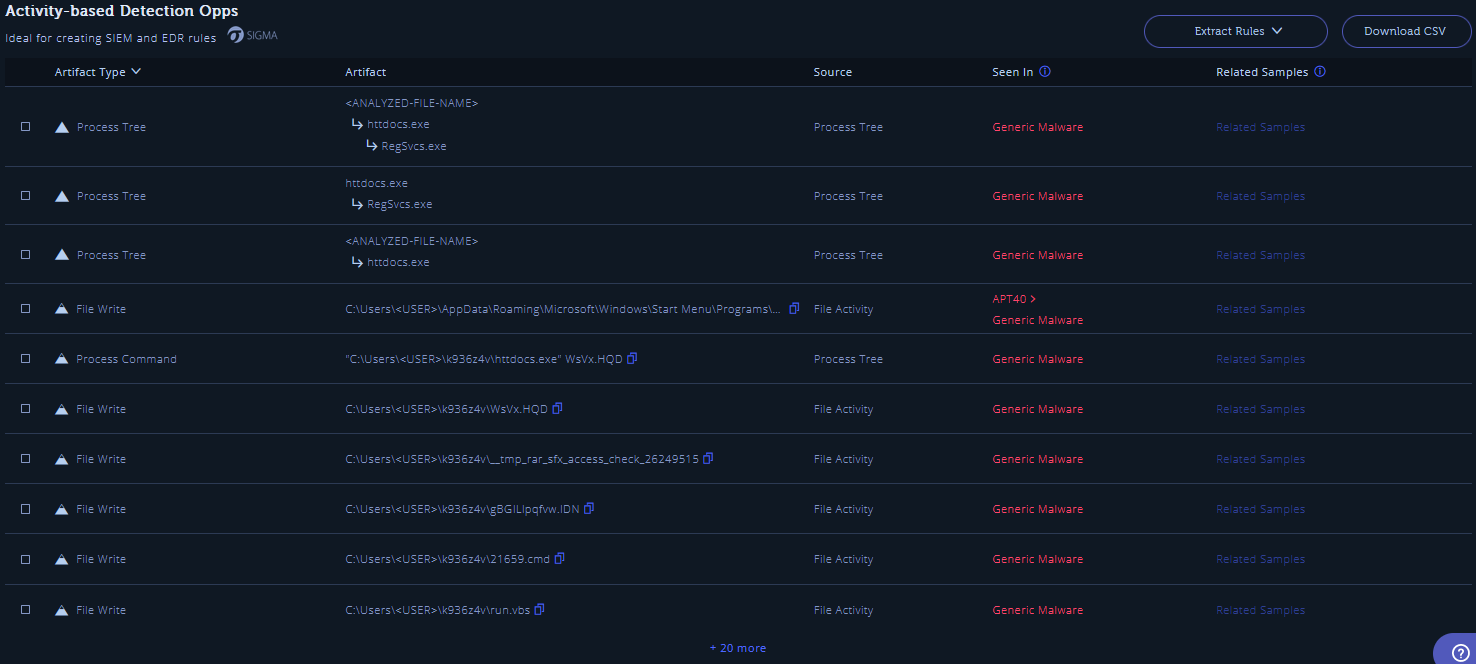


**Figura 5 – Intezer Analyze exemplu 1**

De asemenea, în figura 6.1 și 6.2 de mai jos, putem observa ce a detectat platforma în fișierul dat și ce schimbări poate provoca.



**Figura 6.1 – Intezer Analyze detectare**

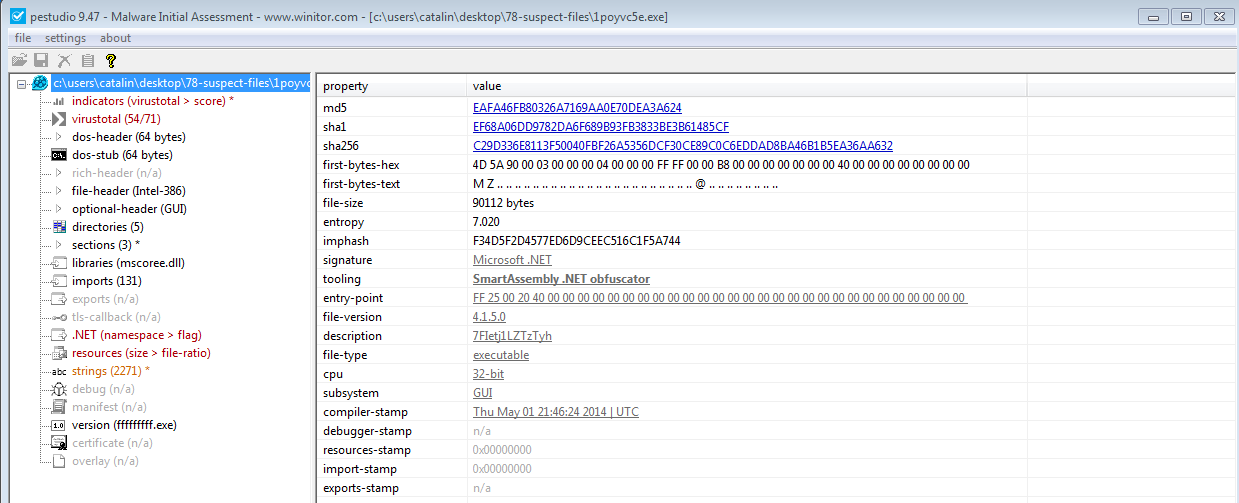


**Figura 6.2 – Intezer Analyze detectare**

După analizarea ambelor platforme, consider că, pentru începători sau pentru utilizatori care nu dispun de cunoștințe mai multe în domeniul dat, va fi mai ușor de folosit VirusTotal, deoarece are o interfață mai simplă și ușor de utlizat. Pe când pe platforma Intezer, este necesitatea de a analiza mai detaliat.

**2. Analiza statică**

Pentru analiza statică am folosit aplicația Pstudio. După cum vedem, în figura 7, unde este afișat câmpul executabil, ne este oferită informații generale despre aplicația noastră, cum ar fi hasuri, punctul de intrare hex, tipul de fișier, dacă se execută pe 32 de biți sau 64 de biți. Aceste informații pot fi utile pentru a aduna informațiile disponibile de pe internet despre malware folosind valoarea hash a fișierului. De asemenea, este afișată și valoarea entropiei care măsoară graful de aleatorie într-un anumit set de date poate ajuta la estimarea dacă datele sunt sau nu criptate sau comprimate. Entropia mai mare înseamnă adesea criptare.



**Figura 7 – Analiza statică pstudio**

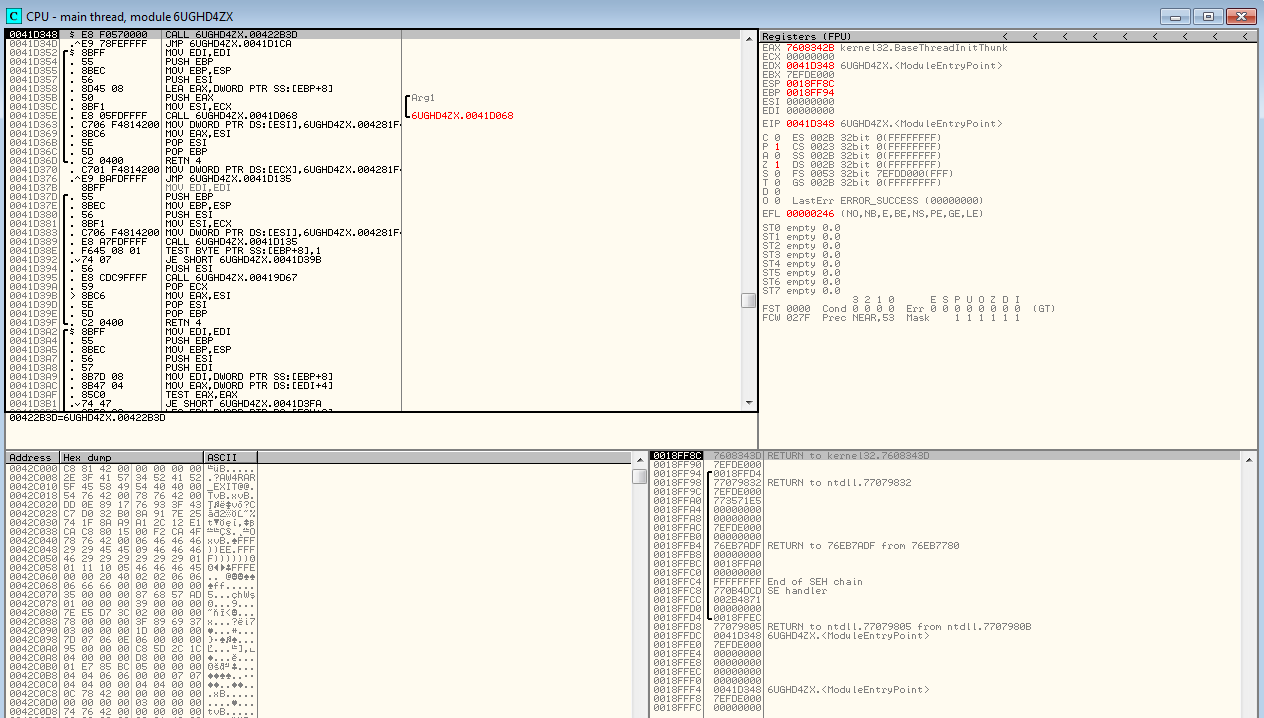
În figura 8 este afișată recunoașterea realizată de aplicația VirusTotal, observăm că este același rezultat ca și la prima etapă.



**Figura 8 – Analiza statică, VirusTotal**

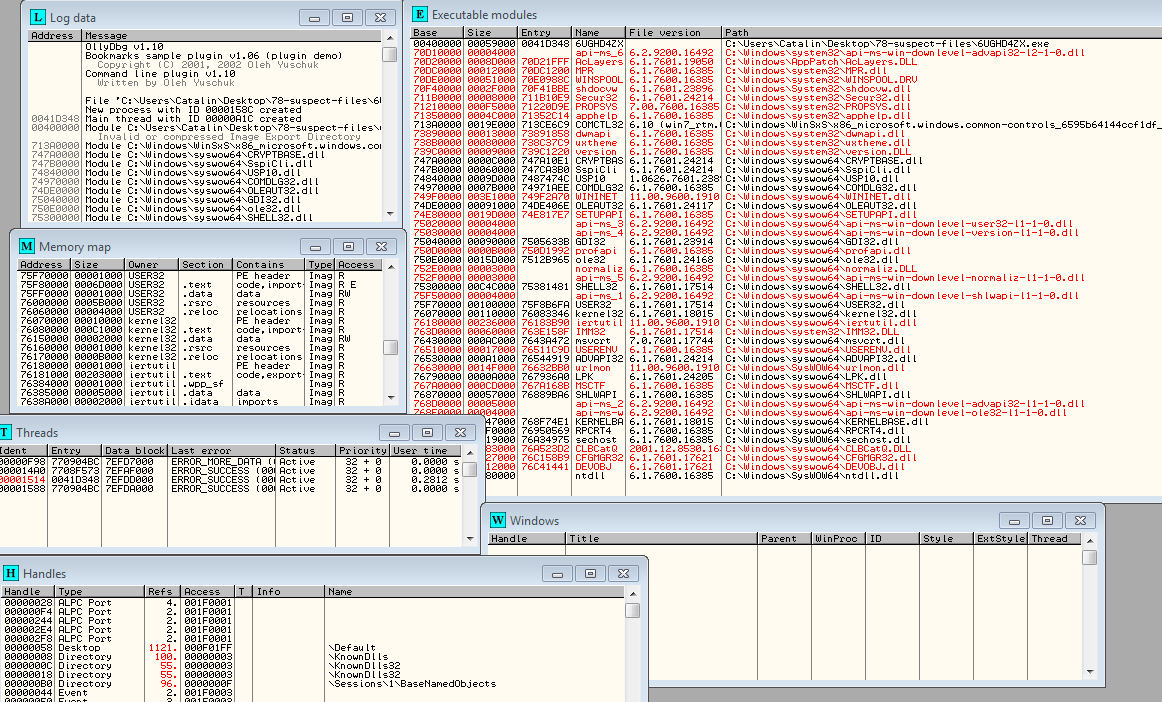
**3. Analiza dinamică**

În această etapă, vom realiza analiza dinamică cu ajutorul aplicației Ollydbg. În comparație cu analiza statică, unde codul nu este executat, în această etapă observăm în format live cdul și ne este oferită o imagine mai profundă a funcționalității malware-ului. În figura 9, observăm cum arată aplicația noastră după ce a fost introdusă în aplicația Ollydbg. Aici, se poate observa de asemenea și adresa virtuală a instrucțiunii, regiștri, statutul la debugger.



**Figura 9 – Analiza diamică, Ollydbg**

De asemenea, Ollydbg ne oferă mai multe informații necesare, le putem observa în figura 9.1.

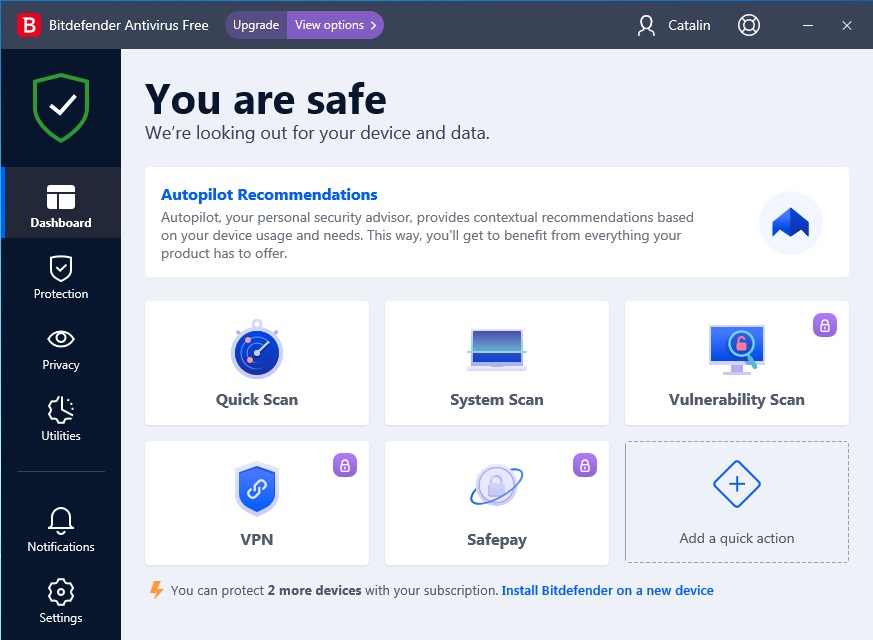


**Figura 9.1 – Analiza diamică, Ollydbg**

După ce am dat la executare, nu am putut observa ce va afișa fișierul deoarece, antivirusul care este alocat nu pe VirtualBox, nu ia permis aceasta.

**4. Studierea și configurarea nivelurilor de protecție a unui antivirus**

Pentru exemplu am luat Bitdefender Antivirus, deoarece deja era instalat pe dispozitiv. Acesta este un program antivirus dezvoltat de compania Bitdefender, care protejează dispozitivele împotriva amenințărilor de securitate, inclusiv viruși, malware, spyware și ransomware. Bitdefender oferă o gamă largă de funcții de securitate, inclusiv protecție în timp real, scanare aprofundată a sistemului, protecția anit-sphishing, protecție pentru rețelele Ei-Fi publice și un firewall bidirecțional. Acesta este recunoscut pentru performanța excelentă în testele de laborator și recenziile de utilizatori. În figura 10, putem observa interfața grafică a aplicației.



Putem observa că antivirusul dat ne oferă o gamă largă de protecție, cum ar fi:

* scanare rapidă;
* scanare detaliată;
* verificare vulnerabilitate system;
* protecție video și audio;
* pretecție urmărire.

De asemenea ne oferă și posibilitatea de a folosi unui VPN, doar ca este necesar de versiunea cu plată.

**Concluzii**

În urma efectuării lucrării de laborator am analizat detaliat programe malițioase. Am identificat tipul lor cu ajutorul la VirusTotal și Intezer, le-am analizat static, pentru a observa nivelurile lor și indicatorii de amenințare cu ajutorul la Pstudio. De amenea am efectuat și analiza dinamică, care presupune executarea lor într-un mod sigur cu ajutorul aplicației Ollydbg. Toate procesele au fost realizate în mediu securizat cu ajutotul al mașina virtuala VrtualBox. În final am realizat și o analiza asupra antivirusului Bitdefender, care presupune o gamă largă de protecție.