**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**

**RAPORT**

Lucrarea de laborator nr.1

*la Tehnologii de Securitatea Informațională*

A efectuat:

st. gr. TI-214 Buza Cătălin

A verificat: Bulai Rodica

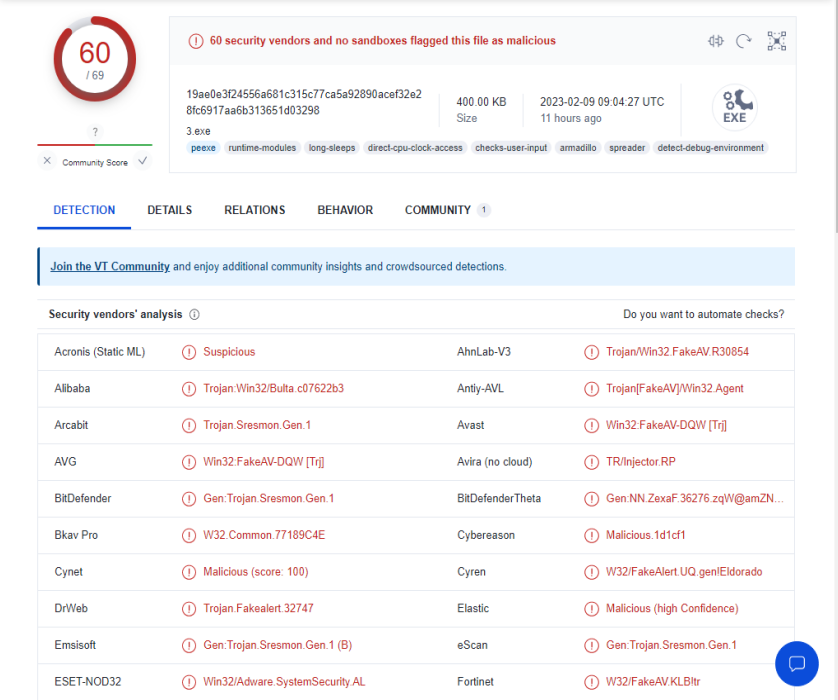
Chişinău - 2023

**Scopul lucrării:**

Analiza a 3 pograme malware, recunoașterea tipului, analiză statică și analiză dinamică.

**Analiza aplicației x 001**

Inițierea analizei unui virus începe cu identificarea acestuia, care poate fi realizată prin intermediul unui serviciu precum VirusTotal (Figura 1). Acest site oferă gratuit verificarea fișierelor împotriva virușilor prin utilizarea mai multor tipuri de produse antivirus și motoare de scanare. După scanarea aplicației noastre, rezultatele arată că 60 din cele 69 de antivirusuri au identificat prezența unui Trojan în fișier, în timp ce restul de 9 au considerat fișierul inofensiv.



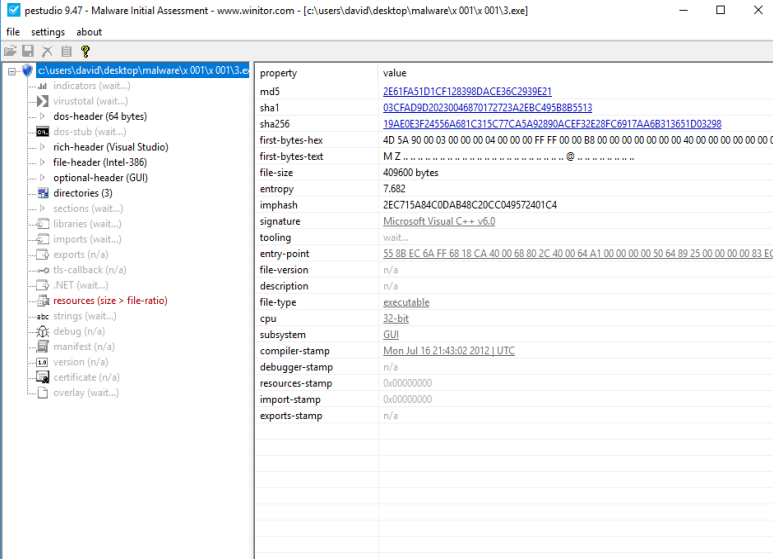
**Figura 1 – Recunoasterea virusului**

Un trojan este un tip de virus de computer care se ascunde în spatele unui program sau fișier aparent inofensiv și își încearcă să își acceseze obiectivele malițioase, fără a fi detectat. Acesta poate fi utilizat pentru a obține acces nedorit la sistemul de calculator, a fura informații confidentiale sau a instala alte tipuri de malware. Deși un trojan poate fi descărcat prin intermediul unui link sau fișier suspect, acesta poate fi, de asemenea, îmbinat cu alte programe și distribuit prin intermediul e-mailurilor sau rețelele sociale. Este important să se adopte măsuri de securitate și să se utilizeze programe antivirus actualizate pentru a preveni infectarea cu acest tip de malware.

În analiza unui virus, pasul următor este evaluarea statică. Această evaluare poate fi realizată prin intermediul unui program precum Pestudio, un instrument gratuit care permite examinarea unui malware fără a-l activa sau a analiza codul acestuia.

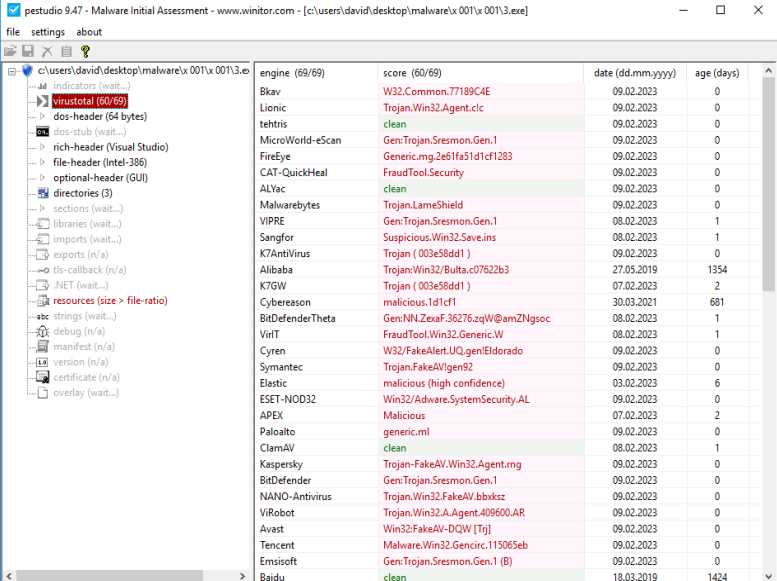
Informații valoroase pot fi obținute prin intermediul acestui program, inclusiv detalii despre fișier, precum hash-urile, punctul de intrare hex, tipul de fișier, dacă este executabil pe 32 sau 64 de biți, și multe altele (vezi Figura 2). Aceste informații pot fi utilizate pentru a căuta detalii suplimentare despre malware pe internet, bazându-se pe valoarea hash a fișierului.

Valoarea entropiei, care măsoară gradul de aleatorie al unui set de date, este de asemenea prezentată. Aceasta poate fi utilizată pentru a determina dacă datele sunt criptate sau comprimate. De obicei, o entropie mai mare indică prezența unei criptări puternice.



**Figura 2 – Analiza statica, Main tab**

În Figura 3 este afișat recunoașterea realizată de aplicația VirusTotal, la fel, observăm că este același rezultatul ca și la prima etapă.

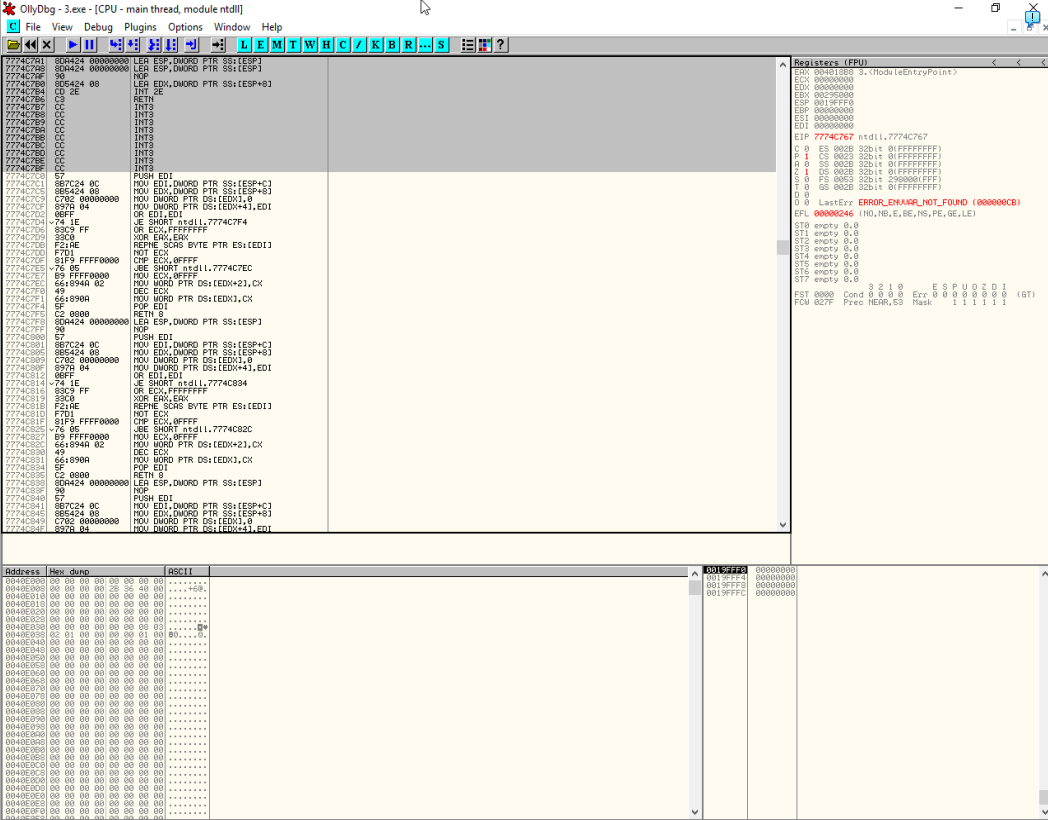


**Figura 3 – Analiza statica, Virus Total**

Etapa următoare în analiza unui virus este Analiza Dinamică, care este realizată prin intermediul instrumentului Ollydbg. Această analiză diferă de cea statică, deoarece ne permite să observăm comportamentul malware-ului în timp real.

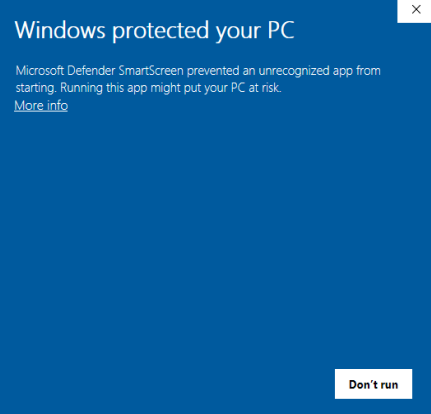
În imaginea din Figura 4, putem vedea cum aplicația noastră apare în Ollydbg după ce a fost introdusă. Acest lucru ne oferă o vizualizare în profunzime a activității malware-ului, inclusiv Adresa Virtuală a Instrucțiunii, Regiștrii și Statutul la Debugger.

Analiza dinamică ne oferă informații esențiale despre comportamentul malware-ului, cum ar fi modul în care acesta își îndeplinește sarcinile nedorite, cum poate fi detectat și oprit, și cum poate fi prevenit în viitor.



**Figura 4 – Analiza Dinamica**

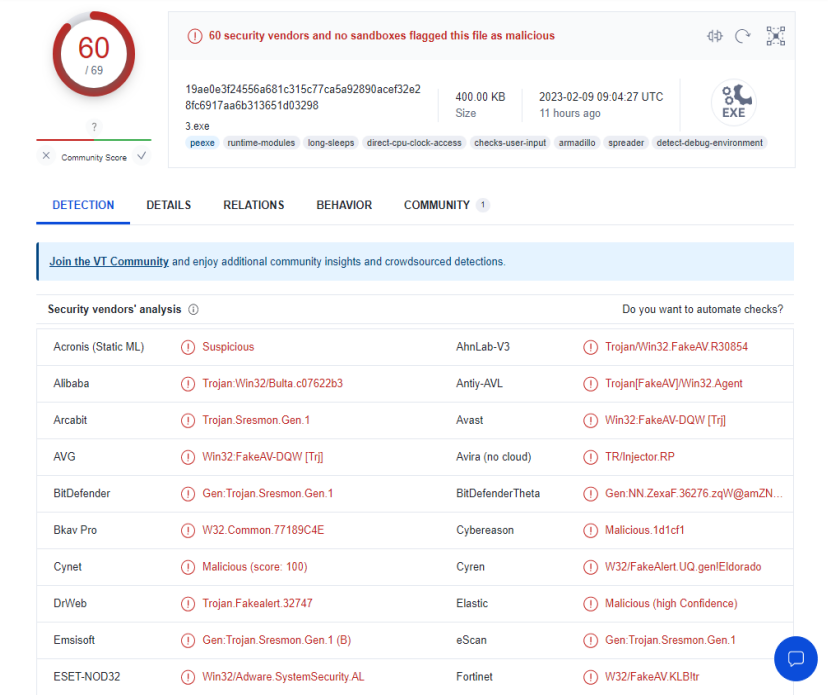
După ce am dat la execuție, nu a fost posibil de determinat comportamentul aplicației, pentru că Windows a protejat calculatorul .



**Figura 5 – Executarea Aplicatiei**

**Analiza aplicației x 0002**

Inițierea analizei unui virus începe cu identificarea acestuia, care poate fi realizată prin intermediul unui serviciu precum VirusTotal (Figura 6). Acest site oferă gratuit verificarea fișierelor împotriva virușilor prin utilizarea mai multor tipuri de produse antivirus și motoare de scanare. După scanarea aplicației noastre, rezultatele arată că 60 din cele 69 de antivirusuri au identificat prezența unui Trojan în fișier, în timp ce restul de 9 au considerat fișierul inofensiv.

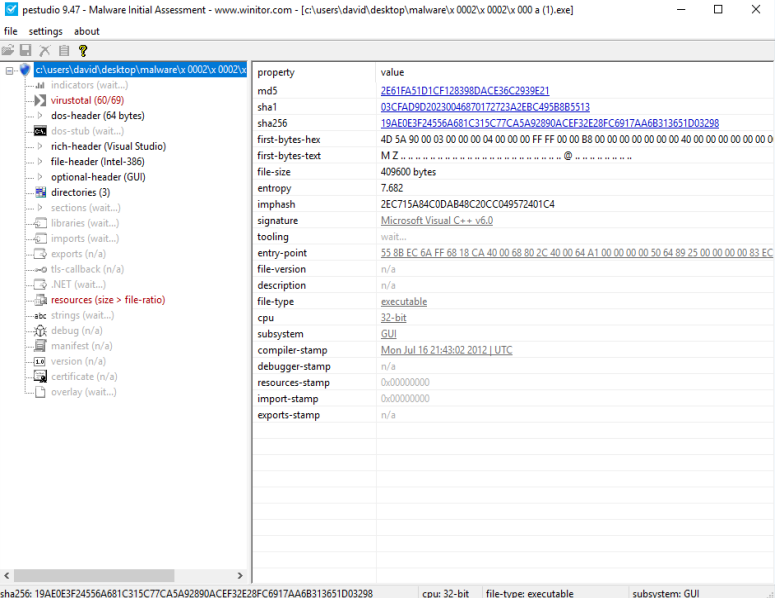


**Figura 6 – Recunoasterea virusului**

Un cal troian descrie un anumit tip de program spion, care realizează funcțiile malefice care permit accesarea neautorizată a unui calculator. Fiecare tip de cal troian are o sarcină specifică de făcut, printre acestea se numără: interceptarea parolelor și a datelor personale, furtul detaliilor bancare, obținerea controlului asupra rețelei de calculatoare și altele.

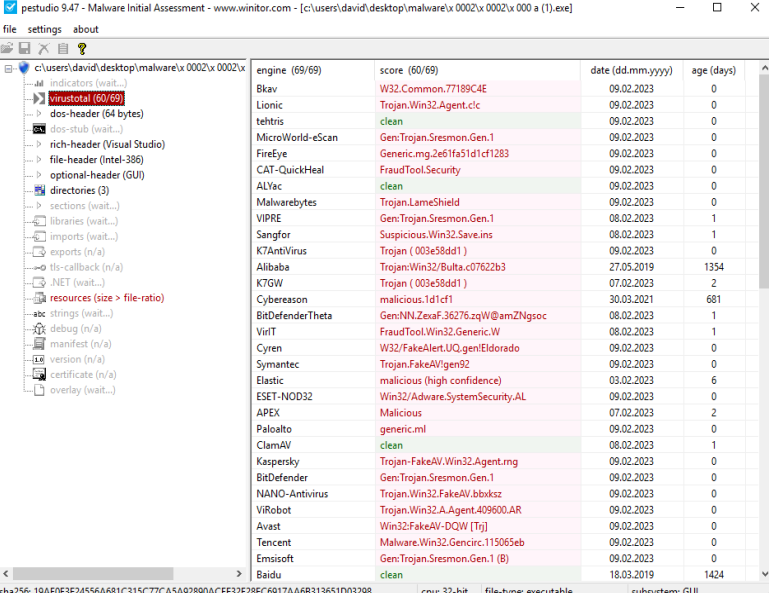
Următorul pas este analiza statică, de asemena realizată cu ajutorul aplicației Pestudio.

După cum putem vedea în Figura 7, unde este afișată fila indicatori, Pestudio a identificat un număr de indicatori și i-a clasificat pe o scară de la 1 la 3, 1 fiind un indicator rău intenționat. Au fost identificate , la fel, unele șiruri, secțiuni importuri rău intenționate.



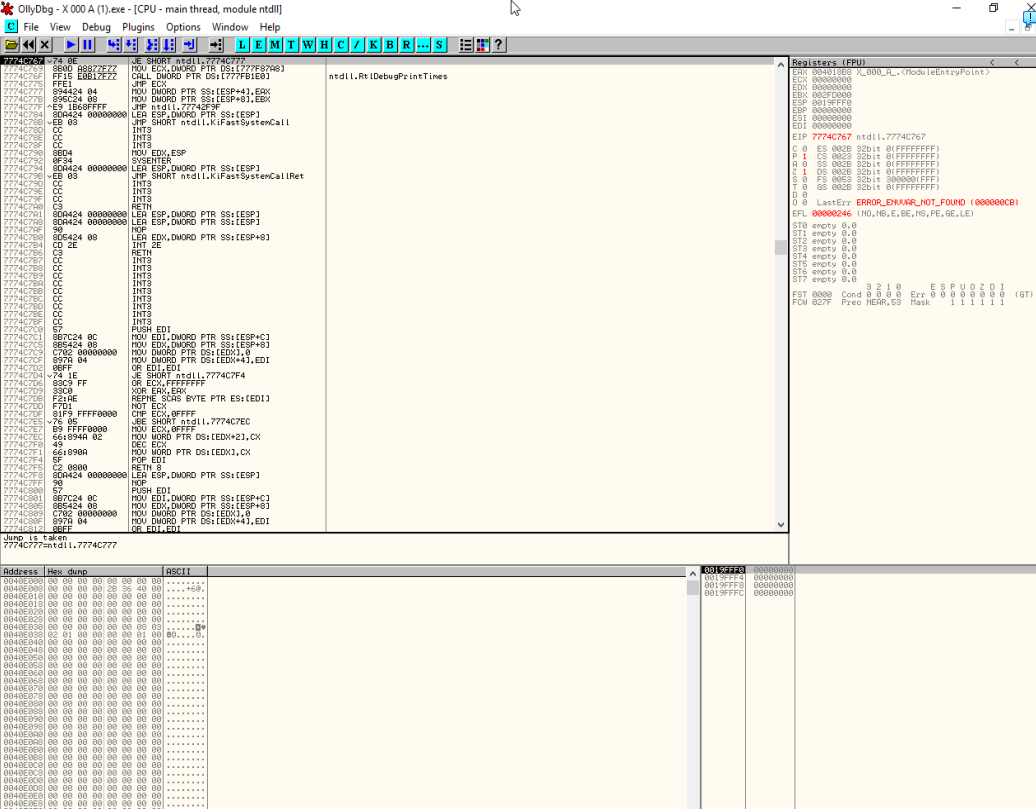
**Figura 7 – Analiza statica, Main tab**

În Figura 8 este afișată secțiunea resurse, unde sunt stocate resurse care pot fi utizate de malware, cum ar fi șiruri de caractere și fițiere suplimentare.



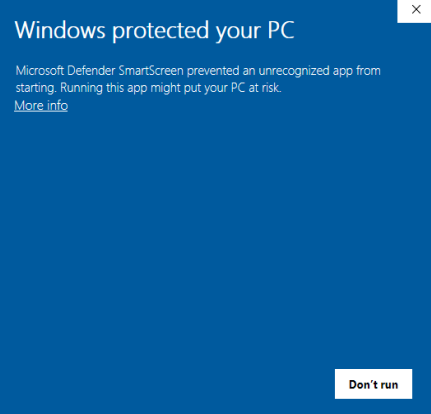
**Figura 8 – Analiza statica, Virus Total**

A treia etapă este Analiza Dinamică, realizată cu ajutorul aplicației Ollydbg. În Figura 9, observăm cum arată aplicația noastră după ce a fost introdusă în aplicația Ollydbg.



**Figura 9 – Analiza Dinamica**

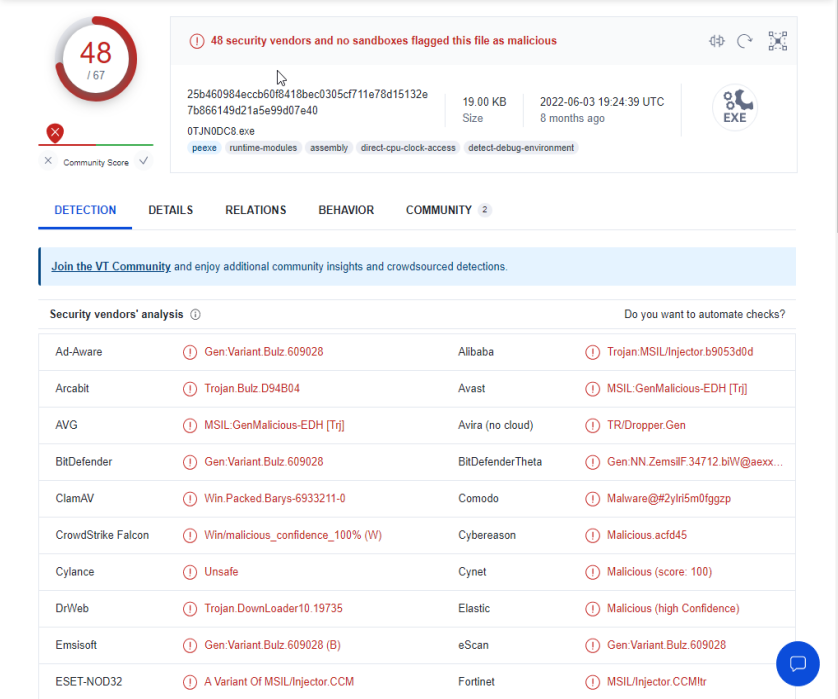
După ce am dat la execuție, nu a fost posibil de determinat comportamentul aplicației, pentru că Windows a protejat calculatorul



**Figura 10 – Executarea Aplicatiei**

**Analiza aplicației 78-suspect-files**

Inițierea analizei unui virus începe cu identificarea acestuia, care poate fi realizată prin intermediul unui serviciu precum VirusTotal (Figura 11). Acest site oferă gratuit verificarea fișierelor împotriva virușilor prin utilizarea mai multor tipuri de produse antivirus și motoare de scanare. După scanarea aplicației noastre, rezultatele arată că 48 din cele 67 de antivirusuri au identificat prezența unui Trojan în fișier, în timp ce restul de 9 au considerat fișierul inofensiv.

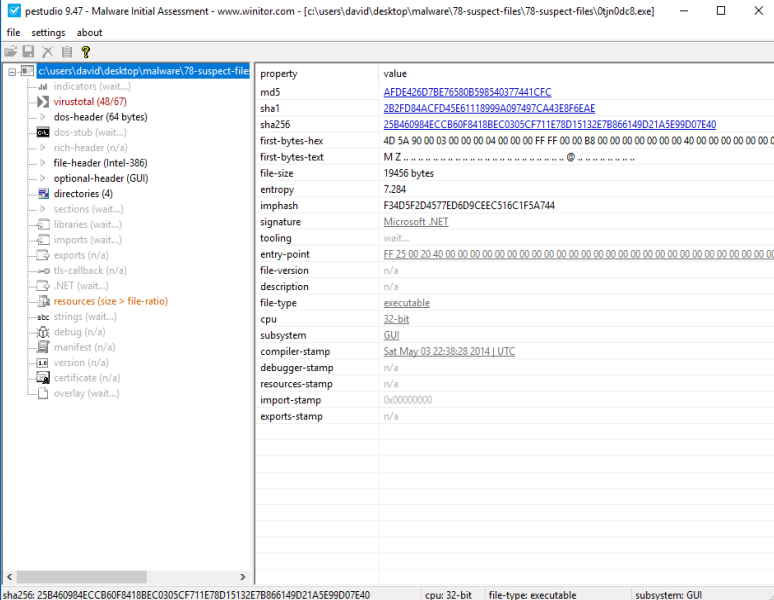


**Figura 11 – Recunoasterea virusului**

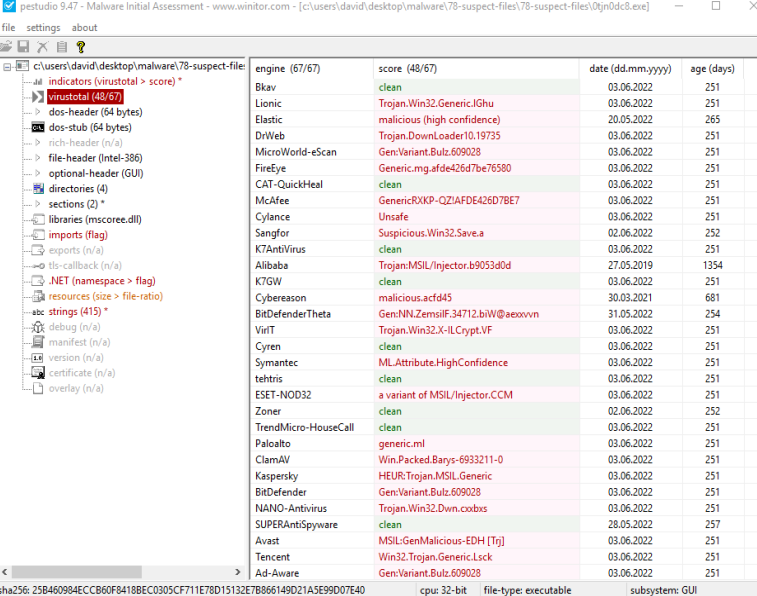
Un virus Trojan este o formă periculoasă de malware care își ascunde adevăratele intenții sub aparența unui program sau fișier inofensiv. Acesta poate fi transmis prin intermediul unui fișier descărcat de pe Internet sau prin intermediul unui e-mail spam și are capacitatea de a accesa informațiile confidențiale ale victimei, cum ar fi parolele sau informațiile de card de credit. De asemenea, un virus Trojan poate fi utilizat pentru a descărca și instala alte tipuri de malware, cum ar fi viermii sau ransomware-ul.

Pentru a preveni infecția cu acest tip de malware, este esențial să se adopte măsuri precaute, cum ar fi descărcarea software-ului numai de la surse de încredere, actualizarea constantă a software-ului și utilizarea unui software antivirus actualizat. Dacă totuși sistemul devine infectat cu un virus Trojan, este important să se solicite ajutor de la un specialist în securitatea informatică pentru a elimina complet malware-ul și a preveni orice daune ulterioare.

Următorul pas este analiza statică, de asemena realizată cu ajutorul aplicației Pestudio.

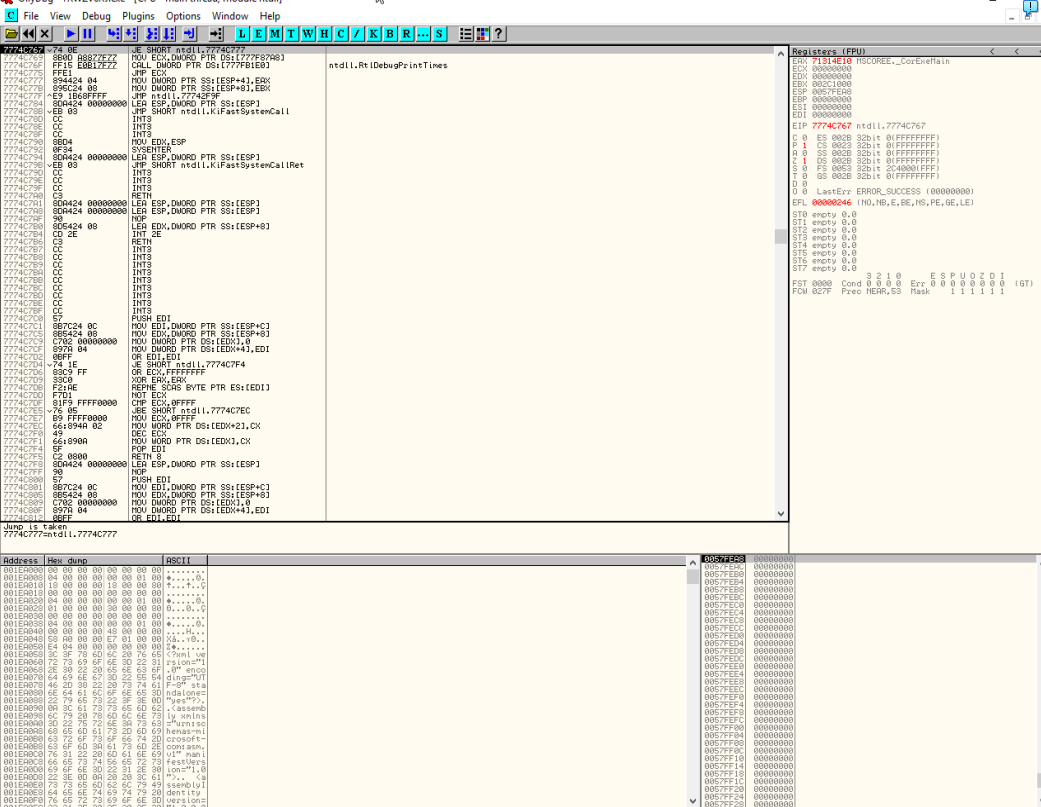


**Figura 12 – Analiza statica, Main tab**



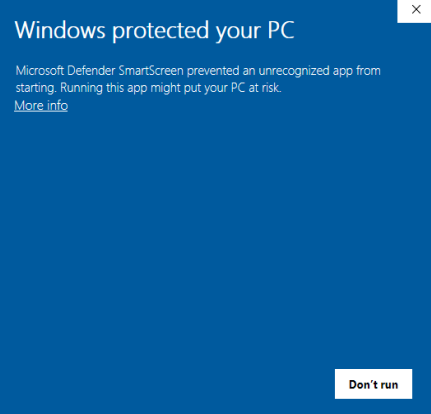
**Figura 13 – Analiza statica, Virus Total**

Analiza dinamică este reprezentată în Figura 14, de asemenea executată cu ajutorul aplicației Ollydbg.



**Figura 14 – Analiza Dinamica**

După ce am dat la execuție, nu a fost posibil de determinat comportamentul aplicației, pentru că Windows a protejat calculatorul



**Figura 5 – Executarea Aplicatiei**

Bitdefender, unul dintre cei mai renumiți producători de software antivirus, oferă mai multe tipuri de scanări și tehnologii de detecție pentru a proteja sistemele utilizatorilor. În figura 6 este arătată interfața antivirusului.

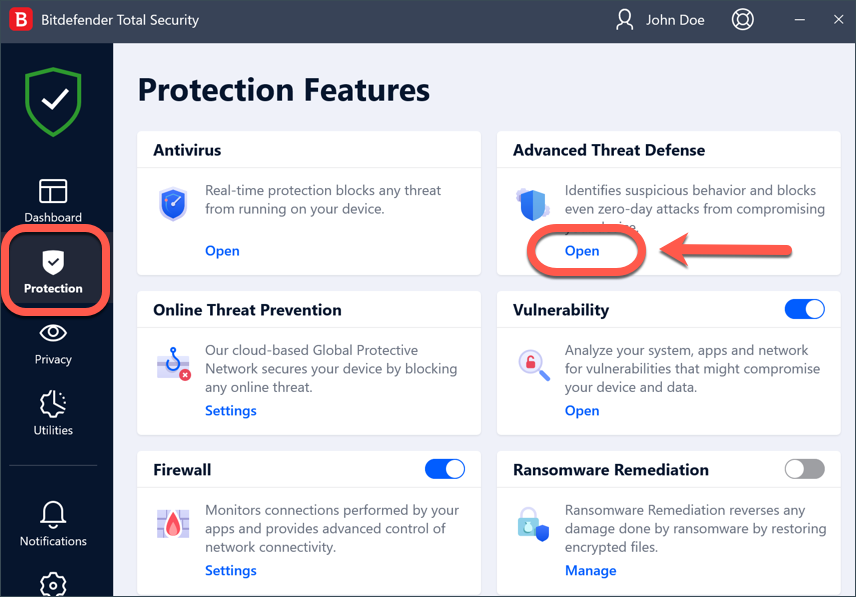
Tipuri de scanări:

* Scanare rapidă: Scanează zonele cele mai vulnerabile ale sistemului într-un timp scurt.
* Scanare completă: Scanează întregul sistem pentru a identifica orice amenințare.
* Scanare personalizată: Permite utilizatorilor să selecteze zonele specifice ale sistemului pentru a fi scanate.

Tehnologii de detecție:

* Protecție în timp real: Detectează și blochează automat orice amenințare în timp ce utilizatorul navighează pe internet.
* Protecție împotriva amenințărilor cibernetice avansate: Utilizează tehnologii avansate de analiză comportamentală și inteligență artificială pentru a detecta și elimina amenințări avansate, cum ar fi ransomware.
* Protecție împotriva atacurilor de tip phishing: Blochează site-urile false sau malițioase care încearcă să obțină informații personale sau financiare de la utilizatori.

Nivelurile de protecție: Bitdefender oferă mai multe produse care oferă niveluri diferite de protecție, inclusiv Bitdefender Antivirus Plus, Bitdefender Internet Security și Bitdefender Total Security. Acestea variază în funcție de numărul de dispozitive protejate, caracteristicile de protecție și preț.



**Figura 6 – Bitdefender**

**Concluzie**

După efectuarea experimentului de laborator, am analizat trei tipuri diferite de malware prin intermediul serviciilor gratuite oferite de VirusTotal, care ne-au permis să identificăm tipurile de malware. Ulterior, am efectuat o evaluare mai detaliată prin intermediul unei analize statice utilizând instrumentul Pestudio. Această analiză ne-a oferit informații valoroase despre amenințările potențiale asociate fiecărui program malware și ne-a permis să estimăm nivelul lor de pericol pentru sistemele utilizatorilor.

Pentru a evalua comportamentul malware-ului în condiții reale, am efectuat o analiză dinamică executând fiecare program malware într-un mediu sigur și controlat. Acest mediu de lucru a fost realizat prin utilizarea unei mașini virtuale, care a permis evitarea infectării sistemului personal și lucrul într-un mediu izolat.

În concluzie, am utilizat o abordare integrată pentru a analiza aceste programe malware, combinând informații obținute prin intermediul serviciilor VirusTotal, analize statice și dinamice, astfel încât să obținem o imagine completă a amenințărilor potențiale și a nivelului lor de pericol pentru sistemele utilizatorilor.