Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 2

# La disciplina „Managementul și auditul securității informaționale”

**Tema:**

A efectuat: st. gr. SI-211 S. Chirița

A verificat: C. Mîtu

Chișinău – 2024

**Lucrare de laborator nr. 2**

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

**Scopul lucării:**Analiza a 3 pograme malware, recunoașterea tipului, analiză statică și analiză dinamică.

**Obiective:**

**1. Recunoașterea**

* Utilizarea instrumentelor de identificare malware

**2. Analiza Statică**

* Analiza fără a executa și studiul structurii programelor malițioase

**3. Analiza dinamică**

* Analiza cu exeutarea fișierelor în mediu controlat securizat, în scopul vizualizării comportamentului acestora

**Mersul lucrări:**

**Datele criptate de WannaCry sunt fișierele de pe hard disk ale sistemelor infectate. Acestea pot include:**

1. **Documente personale**: Fișierele de tip document (cum ar fi documente Word, Excel, PowerPoint, PDF-uri) pot fi criptate.
2. **Fișiere media**: Fotografii, videoclipuri, fișiere audio și alte fișiere media pot fi afectate.
3. **Baze de date**: Bazele de date personale sau de afaceri pot fi criptate.
4. **Fișiere de sistem**: Fișierele de sistem ale sistemului de operare Windows pot fi afectate, ceea ce poate duce la nefuncționarea corectă a sistemului.

**Punctele vulnerabilite:**

Organizațiile care nu instalaseră actualizarea de securitate a Microsoft din mai au fost afectate de atac. Cei care încă foloseau versiuni nesuportate de Microsoft Windows, cum ar fi Windows XP și Windows Server 2003, erau într-un risc deosebit de mare, deoarece nu fuseseră lansate patch-uri de securitate din aprilie 2014 pentru Windows XP și iulie 2015 pentru Windows Server 2003. Cu toate acestea, un studiu realizat de Kaspersky Lab a raportat că mai puțin de 0,1% dintre calculatoarele afectate rulau Windows XP, iar 98% dintre calculatoarele afectate rulau Windows 7. Într-un mediu de testare controlat, firma de securitate cibernetică Kryptos Logic a constatat că nu a putut infecta un sistem Windows XP cu WannaCry folosind doar exploit-urile, deoarece payload-ul a eșuat să se încarce, sau a provocat prăbușirea sistemului de operare în loc să execute și să cripteze fișierele. Cu toate acestea, atunci când a fost executat manual, WannaCry putea încă să funcționeze pe Windows XP.

**Iată cum funcționează WannaCry:**

Iată cum funcționează WannaCry:

1. Infectarea: WannaCry ajunge pe computerul infectat sub forma unui dropper, un program autonom care extrage alte componente ale aplicației încorporate în sine
2. Criptarea: Odată lansat, WannaCry încearcă să acceseze un URL codat în dur - acesta este un comutator de oprire. Dacă ransomware-ul poate conecta la acel URL, se închide; dacă nu, începe să caute și să cripteze fișiere într-o serie de formate importante, de la fișiere Microsoft Office la MP3 și MKV, lăsându-le inaccesibile utilizatorului
3. Cererea de răscumpărare: Apoi afișează o notificare de răscumpărare, cerând o anumită sumă de Bitcoin - adesea în jur de 300 de dolari - pentru a decripta fișierele2.

**Iată cum funcționează criptarea WannaCry:**

* 1. Criptarea: WannaCry ajunge pe computerul infectat sub forma unui dropper, un program autonom care extrage alte componente ale aplicației încorporate în sine
* 2. Fișierele cu chei de criptare: WannaCry conține fișiere cu chei de criptare. Aceste chei sunt utilizate pentru a cripta și decripta datele. Procesul de criptare nu suprascrie direct datele fișierului, astfel încât recuperarea conținutului fișierului poate fi posibilă în funcție de mediul de lucru
* 3.Fișierele cu chei de criptare: WannaCry conține fișiere cu chei de criptare. Aceste chei sunt utilizate pentru a cripta și decripta datele.
* 4. Wana Decrypt0r 2.0: Componenta de criptare este cunoscută sub numele de Wana Decrypt0r 2.0, iar în interiorul acesteia se afla un fișier ZIP protejat cu parolă.

**Algoritmul:**

Generarea cheilor: WannaCry generează o nouă pereche de chei RSA (doar una pentru fiecare victimă), pentru a cripta toate cele 10000 de chei AES de pe sistemul victimei3.

Criptarea cheilor: Apoi, cheia privată RSA specifică fiecărei victime este criptată cu cheia publică RSA furnizată de WannaCry3.

Transferul cheilor criptate: În final, WannaCry transferă textul criptat (cheia privată RSA criptată a victimei) către autor

Simptomele infecției includ:

- Extensia fișierelor se schimbă ". WNRY".

- Un executabil numit @WanaDecryptor@.exe este adăugat pe desktop.

- Note de răscumpărare și 2 imagini (cu extensie.bmp) sunt, de asemenea, adăugate pe desktop

- Imaginea de fundal a desktopului este modificată, indicând faptul că fișierele noastre au fost criptate.

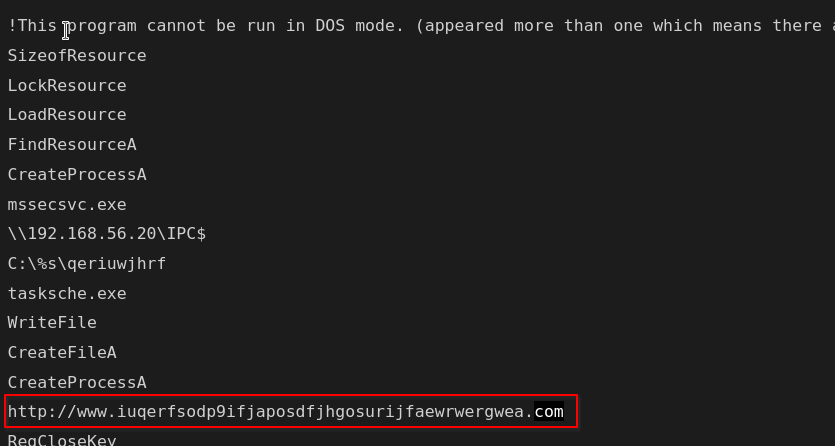
- Sunt create două servicii numite mssecsvc2.0 și ochuttdlb605

- Un director ascuns numit ochuttdlb605 (caractere aleatorii și variază) C:\ProgramData\ - tasksche.exe este adăugat la pornire.

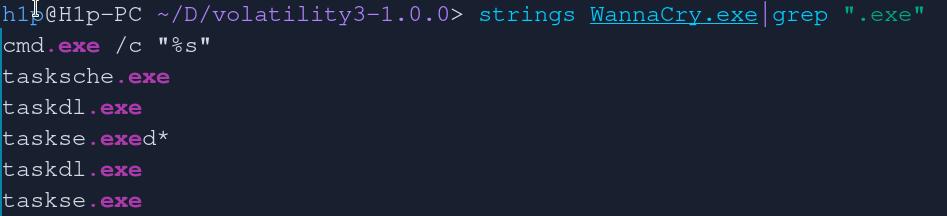
- Copiile shadow și copiile de rezervă sunt șterse. - Un executabil numit taskhsvc.exe ascultă în portul 9050 pentru conexiuni la distanță.

**Analiză statică:**

Atunci când este rulată comanda pentru strings sau floss, se va genera un număr semnificativ de rezultate. Aceste rezultate pot fi ordonate în funcție de importanță, astfel încât cele mai relevante să fie plasate în partea superioară a listei.

Figura 1 – Rezultatul comenzii Strings

Cu siguranță există încă mai multe șiruri găsite, dar sunt mulțumit de acest lucru deocamdată. Se pare că se va conecta la adresa URL **http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com** dar încă nu știm de ce deocamdată.

Figura 2 – Toate fișierele cu extensie .exe

# Figura 3 - Metadatele fișierului WannaCry.exe

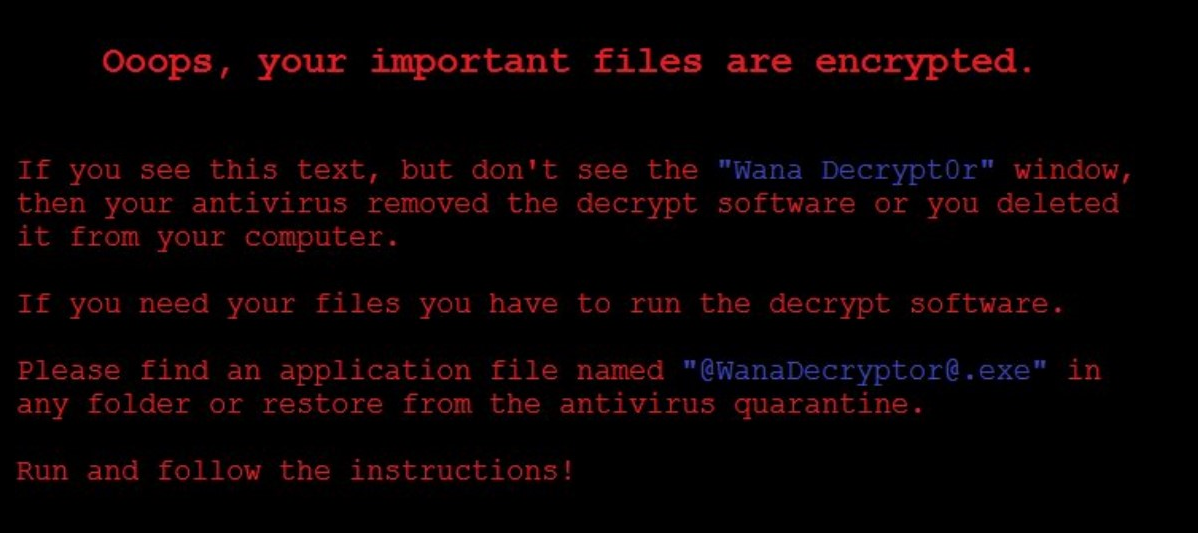
# Figura 4 - Algoritmul de criptare

# Analiza dinamică

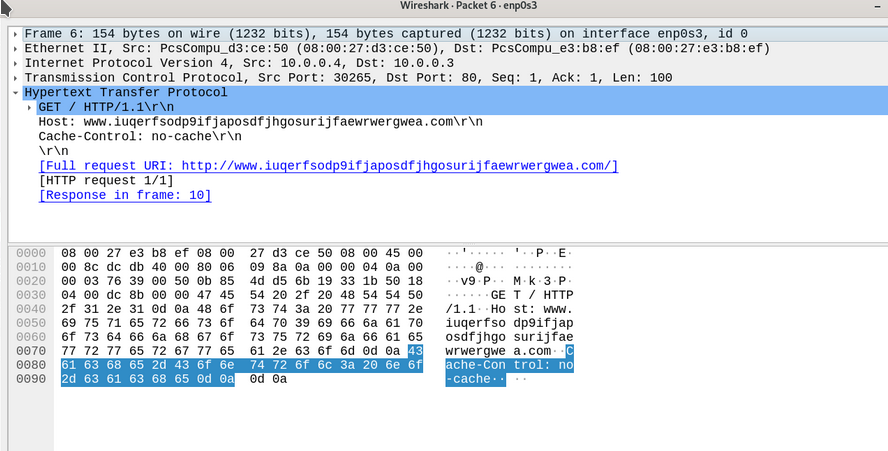
# Rularea `WannaCry.exe`

# Figura 5 - Schimbat fundalul

După cum puteți vedea, a schimbat fundalul, a scăzut EXE-urile și a criptat toate fișierele și adăugați **.**

**Figura 6** - ReadMe

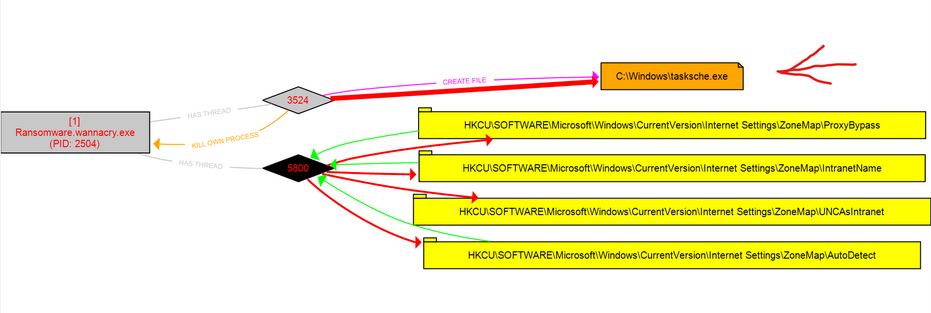
Acum să deschidem **wireshark** pentru a analiza traficul:

**Figura 7** — Wireshark

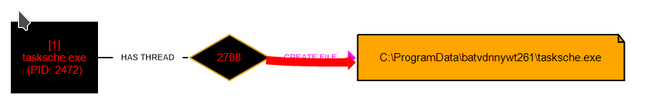
Malware-ul a trimis o cerere **către http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com** și a avut succes.

După ce am înțeles cum funcționează WannaCry, să ne scufundăm într-o analiză mai detaliată în timp ce o rulăm. Voi folosi **ProcMon** pentru a urmări WannaCry EXE :-

* deci wannacry EXE va crea un proces copil numit **tasksche.exe**

Figura 8 - ProcDot

Să urmărim procesul copilului:

 **Figura 9** — Procesul copiil

A creat un director cu nume aleatoriu, de asemenea, a creat un serviciu cu același nume, care va fi responsabil pentru persistență.

Figura 10 - Serviciul creat

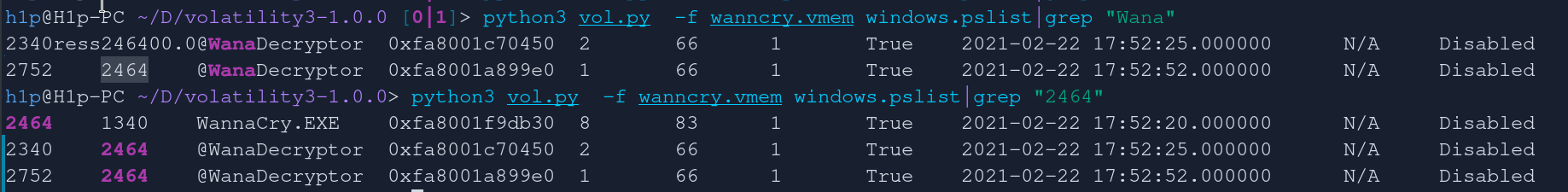
**Analiza memoriei RAM**

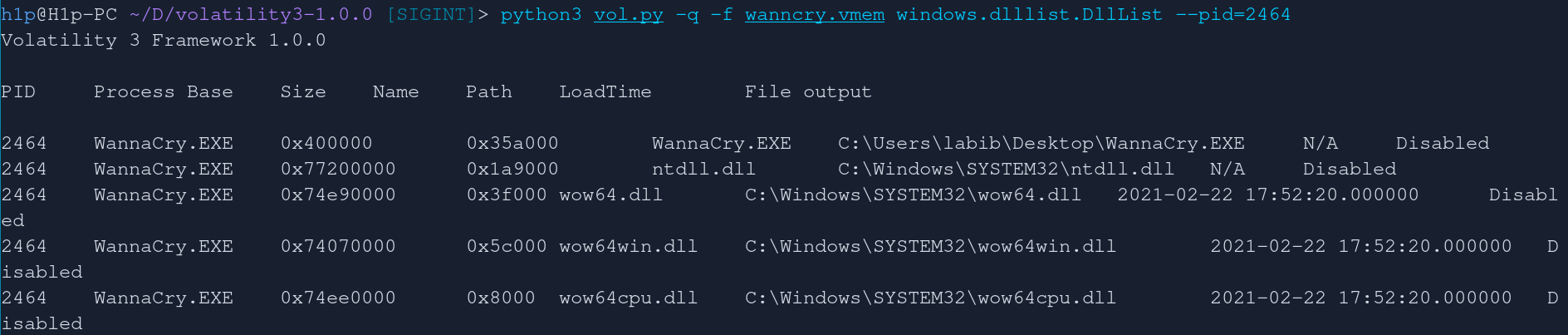
Analiza memorie RAM cu utitlita [**volatility**](https://github.com/volatilityfoundation/volatility)**.**

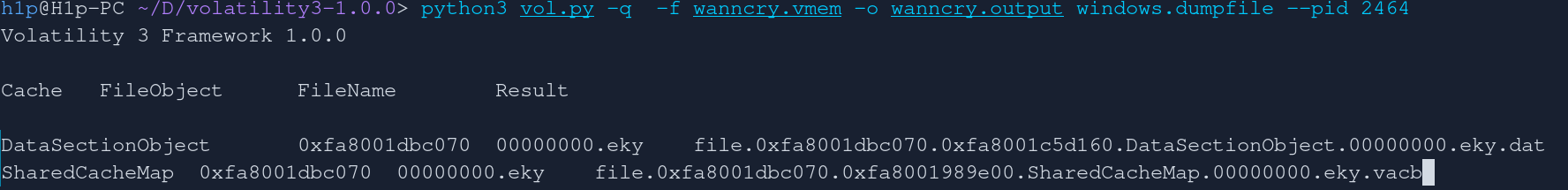
  
**Figura 11** - Analizei virusului **Wannacry (informatie generale)**

Imaginea prezintă un **text** care reprezintă **rezultatele analizei** efectuate asupra virusului **Wannacry**.

1. Acest text pare să fie **output-ul** obținut în urma rulării scriptului **vol.py** într-o **fereastră de terminal sau prompt de comandă**.
2. În coloanele din imagine, sunt listate **variabile** și **valorile** lor corespunzătoare. Acestea includ:
   * **KernelBase**: Adresa de bază a kernelului (0xf80002616000).
   * **DTB**: Adresa tabelului de descriptori (0x187000).
   * **SymbolsFile**: Calea către fișierul de simboluri (//home//hpl//Downloads//volatility3-1.0.0//volatility3//symbols//windows//ntkrnlmp.pdb/3844DBB920174967BE77AA2C2C04302A2.json).
   * **Is64Bit**: Indică dacă sistemul este pe 64 de biți (True).
   * **SystemTime**: Data și ora la care au fost generate aceste informații (2021-02-22 17:55:26).
   * Alte detalii tehnice despre arhitectura sistemului și sistemul de operare sunt, de asemenea, prezente.

**Figura 12** - Analizei virusului **Wannacry (lista procesele infectate)**

**Figura 13 - Analizei virusului Wannacry (librariele dll)**

Figura 14 — Cheile de tipul RSA

Fișierul **tasksche.exe** preia numele calculatorului și îl **obfuscatează** (conform imaginilor de mai sus). După aceasta, se copiază singur în locația „C:\ProgramData<NumeObfuzicat>\tasksche.exe”. **tasksche.exe** este apoi încercat să ruleze ca un serviciu.

**Concluzie:** WannaCry a fost cel mai mare atac ransomware din istorie, a fost diferit de orice alt tip de răscumpărare, deoarece s-ar putea răspândi prin rețeaua locală prin exploatarea vulnerabilității SMB. Dar un kill switch a fost descoperit de cercetătorul britanic Marcus Hutchins, care a oprit atacul înregistrând domeniul web găsit în codul malware-ului. După cum am spus mai sus, WannaCry verifică dacă conexiunea are succes, aceasta înseamnă că este moniterd, deci se termină.