

# Report Esercizio 04/02/2025

## Analisi Malware Windows 10 Leonardo Catalano

“La traccia di oggi ci chiede di effettuare 2 analisi Statica e Dinamica su un malware innocuo.

Le fasi da effettuare saranno le seguenti:

### 1. Configurazione della macchina VM Windows:

La macchina Windows dovrà essere in un ambiente di lavoro sicuro e isolato.

### 2. Analisi Statica: Utilizzo MsfVenom per generare il malware:

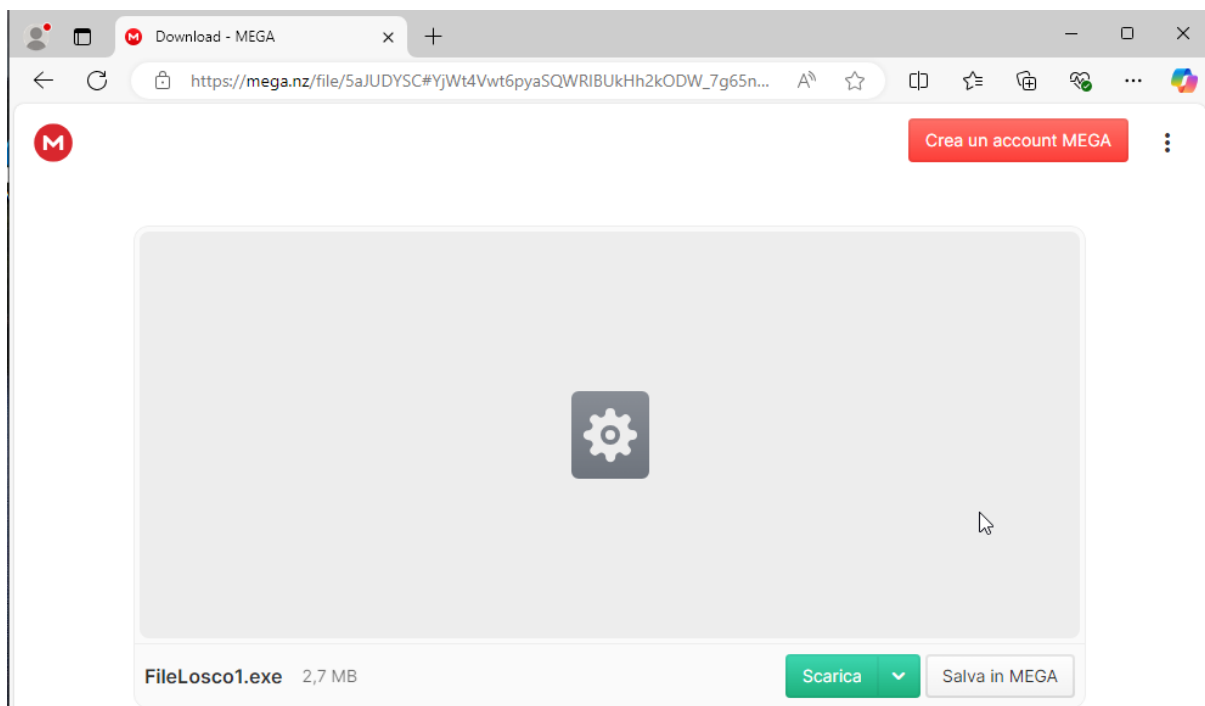
Utilizzare Msfvenom per esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.

### 3. Analisi Dinamica: Utilizzare per eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

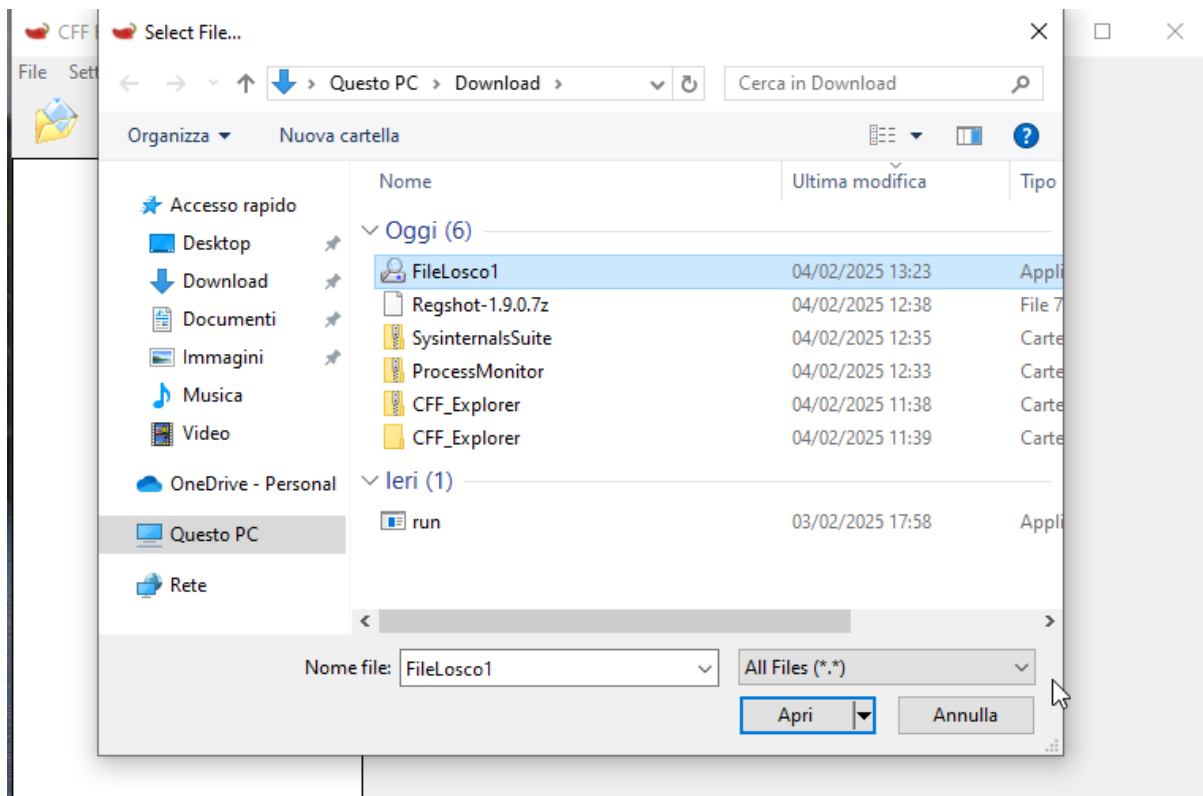
### -Analisi Statica CFF Explorer:

Per effettuare l'analisi statica utilizziamo il programma CFF Explorer che permetterà di scansionare il file interessato (in questo caso il malware innocuo) senza eseguirlo, andando ad esaminare il codice del file/programma stesso.

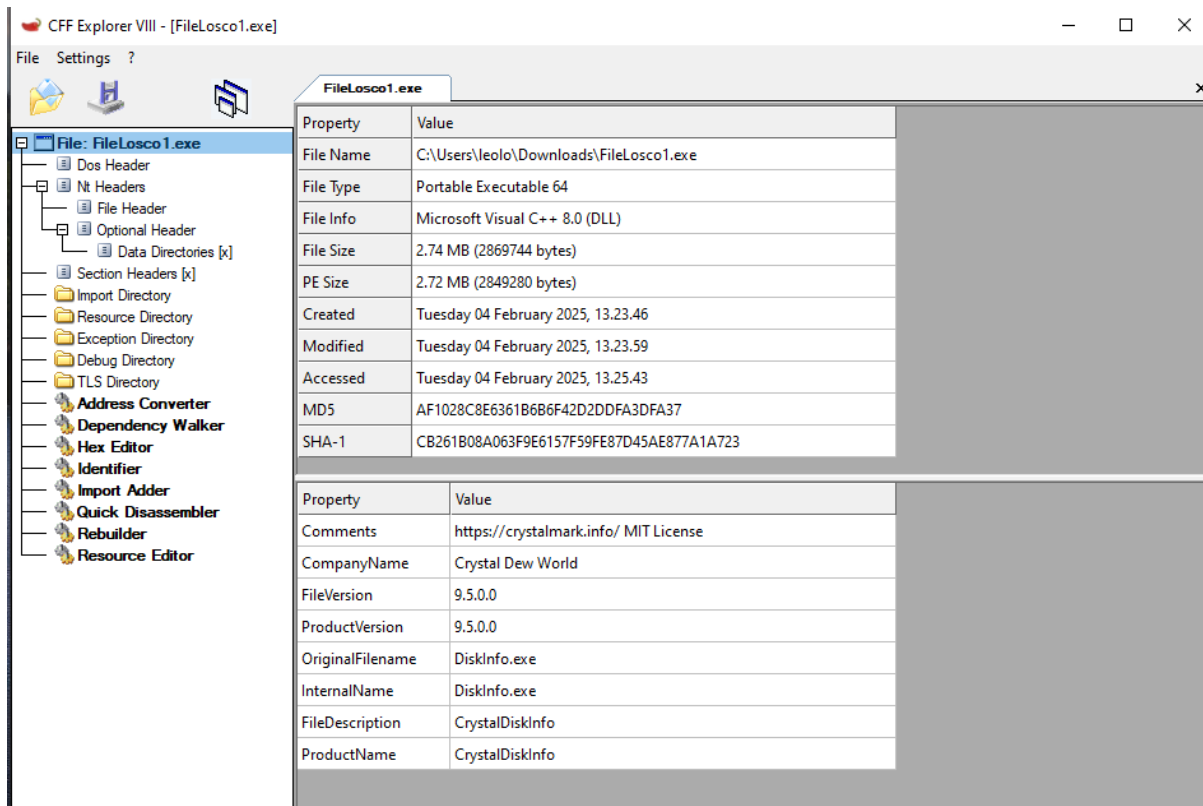
Per prima cosa scarichiamo il file da analizzare:



Successivamente apriamo CFF\_Explorer e scegliamo di analizzare il file scaricato.



Una volta selezionato il programma effettuerà l'analisi statica:



Nella prima schermata possiamo trovare delle prime informazioni sul tipo di file, lo SHA-1 E MD5 (gli hash del file), e nelle proprietà troviamo delle informazioni riguardanti

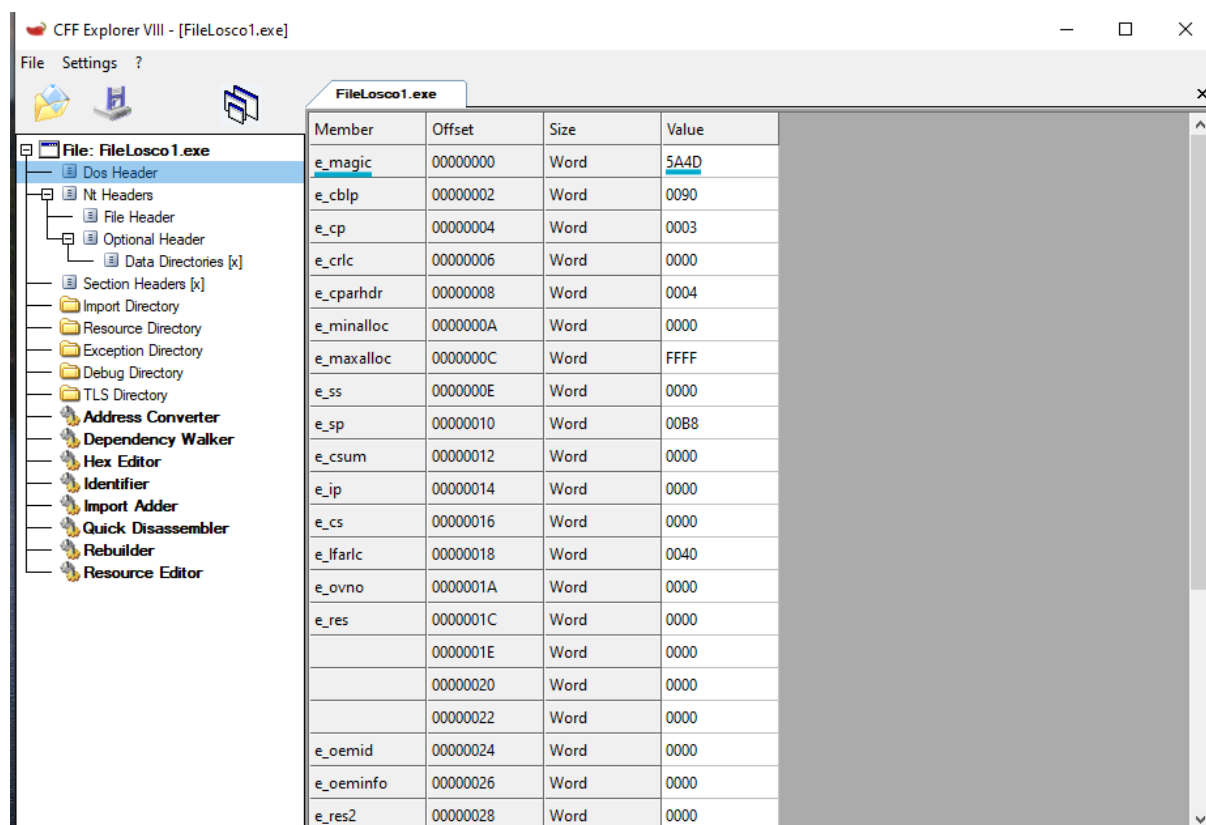
il nome originario del file e dei commenti del file originale stesso.  
(L'hash SHA-1 generalmente è più attendibile rispetto a quello MD5).

Vediamo che il file è stato creato dalla compagnia Crystal Dew World, che il nome originale era DiskInfo.exe e nella descrizione del programma CrystalDiskInfo.

CrystalDiskInfo è un programma molto conosciuto gratuito che viene molto spesso utilizzato per verificare l'integrità dei dischi rigidi all'interno del computer, o altri dettagli di essi : temperatura, nome, RPM, o errori specifici in caso di problemi con il disco rigido.

In questo caso solamente con questa schermata io che conosco il programma CrystalDiskInfo perchè l'ho utilizzato già in passato capisco cos'è senza andare ad effettuare una ricerca online, ma cmq in caso contrario è necessario anche fare una fase di OSINT online per acquisire delle informazioni sul programma specifico.

Spostandoci su Dos Header potremmo vedere le informazioni riguardanti gli Header eseguibili DOS.



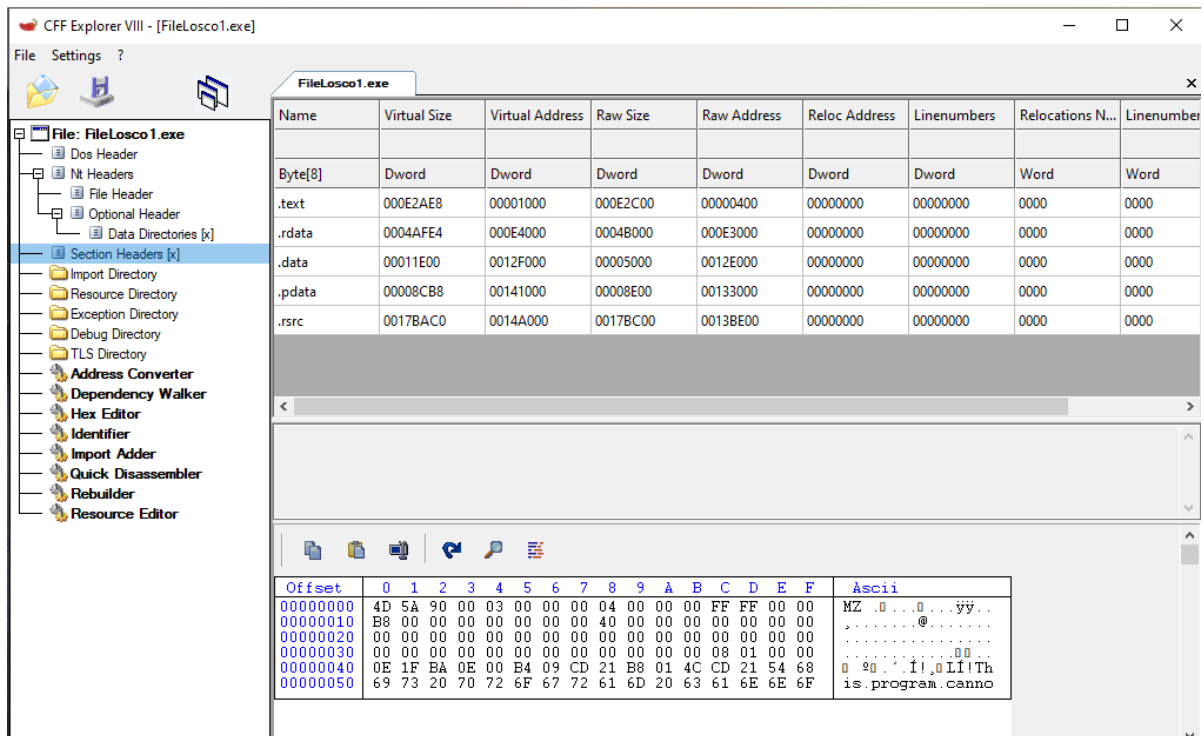
Member	Offset	Size	Value
e_magic	00000000	Word	5A4D
e_cblp	00000002	Word	0090
e_cp	00000004	Word	0003
e_crlc	00000006	Word	0000
e_cparhdr	00000008	Word	0004
e_minalloc	0000000A	Word	0000
e_maxalloc	0000000C	Word	FFFF
e_ss	0000000E	Word	0000
e_sp	00000010	Word	00B8
e_csum	00000012	Word	0000
e_ip	00000014	Word	0000
e_cs	00000016	Word	0000
e_lfarlc	00000018	Word	0040
e_ovno	0000001A	Word	0000
e_res	0000001C	Word	0000
	0000001E	Word	0000
	00000020	Word	0000
	00000022	Word	0000
e_oemid	00000024	Word	0000
e_oeminfo	00000026	Word	0000
e_res2	00000028	Word	0000

Come primo campo troviamo e\_magic che è specifico del campo di firma del DOS Header, il valore 5A4D indica in ASCII "MZ" ossia la firma standard che indica che il file eseguibile DOS è valido.

### -Sezione Section Headers:

In questa sezione troviamo gli Headers, che nello specifico andranno ad effettuare una

determinata funzione.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumber
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word
.text	000E2AE8	00001000	000E2C00	00000400	00000000	00000000	0000	0000
.rdata	0004AFE4	000E4000	0004B000	000E3000	00000000	00000000	0000	0000
.data	00011E00	0012F000	00005000	0012E000	00000000	00000000	0000	0000
.pdata	00008CB8	00141000	00008E00	00133000	00000000	00000000	0000	0000
.rsrc	0017BAC0	0014A000	0017BC00	0013BE00	00000000	00000000	0000	0000

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ .0 . . . . .yy . .
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	, . . . . .@ . . . . .
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	. . . . .
00000030	00	00	00	00	00	00	00	00	00	00	00	00	08	01	00	00	. . . . .0 . .
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	0 0 . . .I! ,0LI!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is .program .canno

La sezione .text contiene il contenuto del codice del file.

La sezione .rdata contiene dati di sola lettura, come stringhe e indirizzi di funzioni.

La sezione .data contiene dati globali e statici, memorizza variabili e configurazioni critiche necessarie per l'esecuzione del file.

La sezione .rsrc contiene risorse come icone e dati di configurazioni.

### -Sezione Import Directory:

Nella sezione Import Directory troviamo i principali moduli di sistema utilizzati dall'applicazione:

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	172	0012BD38	00000000	00000000	0012D57E	000E4288
USER32.dll	169	0012C3F0	00000000	00000000	0012E0C8	000E4940
GDI32.dll	49	0012BBA8	00000000	00000000	0012E3FC	000E40F8
WINSPOOL.DRV	3	0012C990	00000000	00000000	0012E43C	000E4EE0
ADVAPI32.dll	24	0012BAB0	00000000	00000000	0012E618	000E4000
SHELL32.dll	6	0012C378	00000000	00000000	0012E68C	000E48C8
COMCTL32.dll	3	0012BB78	00000000	00000000	0012E6DC	000E40C8
SHLWAPI.dll	7	0012C3B0	00000000	00000000	0012E772	000E4900
UxTheme.dll	3	0012C940	00000000	00000000	0012E7B2	000E4E90
ole32.dll	22	0012CAA8	00000000	00000000	0012E98C	000E4FF8
OLEAUT32.dll	19	0012C2B8	00000000	00000000	0012E996	000E4808
gdiplus.dll	25	0012C9D8	00000000	00000000	0012EBD4	000E4F28
WINMM.dll	1	0012C980	00000000	00000000	0012EBF2	000E4ED0
VERSION.dll	3	0012C960	00000000	00000000	0012EC3E	000E4EB0
WINTRUST.dll	4	0012C9B0	00000000	00000000	0012ECBE	000E4F00
CRYPT32.dll	1	0012BB98	00000000	00000000	0012ECE2	000E40E8
SETUPAPI.dll	3	0012C358	00000000	00000000	0012ED32	000E48A8
OLEACC.dll	2	0012C2A0	00000000	00000000	0012ED70	000E47F0

Analizzerò nello specifico soltanto i moduli più importanti:

#### 1. Kernel32.dll:

Funzioni Importate: 172

Descrizione: Questo modulo è uno dei più importanti perchè qui sono contenute le funzioni base del sistema operativo Windows (dll di sistema), come la gestione della memoria, dei processi, thread, l'I/O (input output) e altre funzionalità di sistema.

#### 2. User32.dll:

Funzioni importate: 169

Descrizione: Anche questo modulo è uno dei più importanti perchè fornisce le funzioni per l'interfaccia utente, come la gestione delle finestre, il controllo delle tastiere e i messaggi di sistema.

#### 3. GDI32.dll:

Funzioni importate: 49

Descrizione: Contiene funzioni per la grafica di base, come il disegno di testo, forme e gestione delle immagini.

Essendo che il programma so che ha una GUI vedo anche che il numero di funzioni importate non sono poche.

#### 4. SHELL32.dll:

Funzioni importate: 6

Descrizione: Fornisce funzioni per interagire con la shell di Windows, inclusa la gestione dei file, delle cartelle e delle operazioni di shell comuni.

5. ADVAPI32.dll:

Funzioni importate: 24

Descrizione: Contiene funzioni avanzate per la gestione delle applicazioni, come la gestione dei servizi di Windows, la sicurezza e la registrazioni di eventi.

6. COMCTL32.dll:

Funzioni importate: 3

Descrizione: Fornisce controlli comuni per l'interfaccia utente, come barre degli strumenti, progress bar, e altre componenti GUI.

Dettagli della Import Directory:

-Kernel32.dll e User32.dll sono moduli che permettono l'accesso a funzioni di sistema interne a windows fondamentali, quindi in caso il file sia un malware potrebbe avere accesso a tali funzioni.

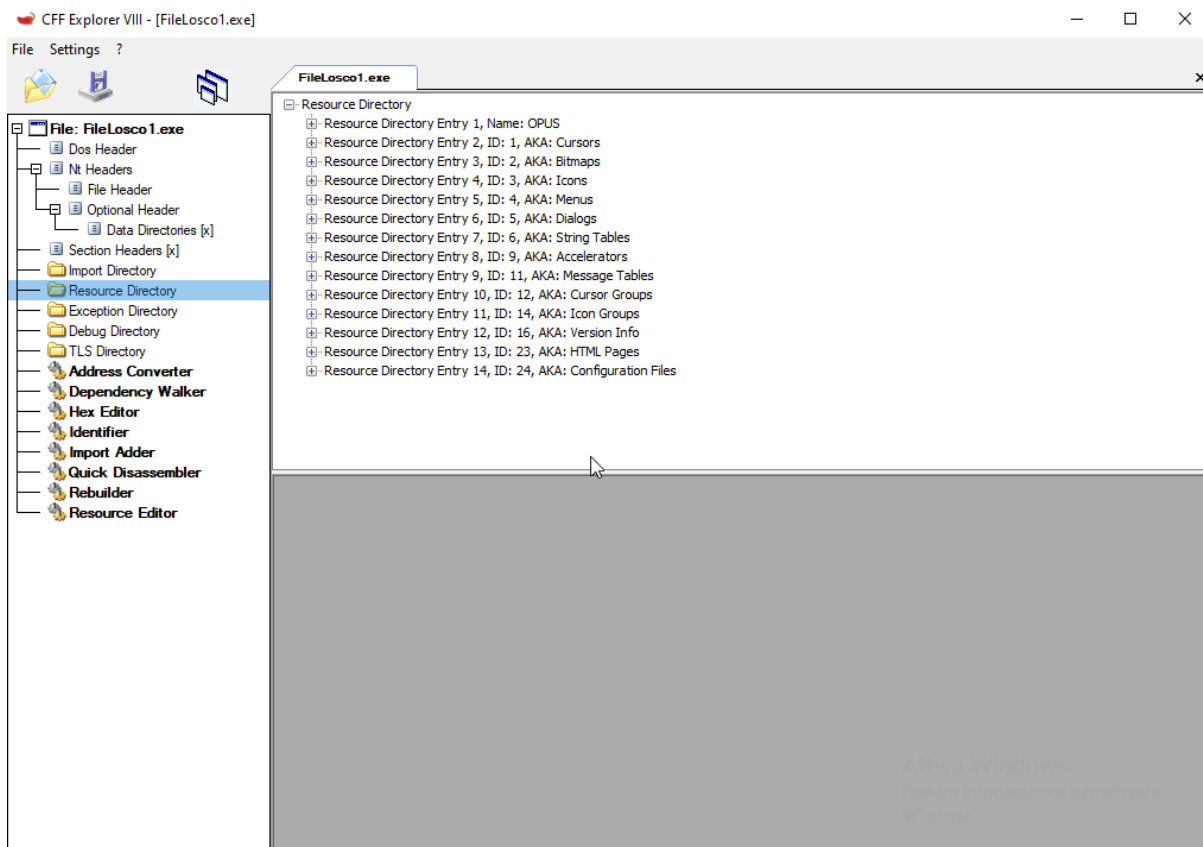
-ADVAPI32.dll è un modulo che indica che il file potrebbe interagire con il registro di windows, servizi di sistema, e funzioni di sicurezza.

-Shell32.dll e COMCTL32.dll sono moduli che indicano che il file potrebbe avere componenti di interfaccia utente GUI e interagire con il filesystem di Windows.

**-Resource Directory:**

In questa sezione troviamo le risorse incorporate nel file eseguibile, come icone, dialoghi, gruppi di icone e file di configurazione.

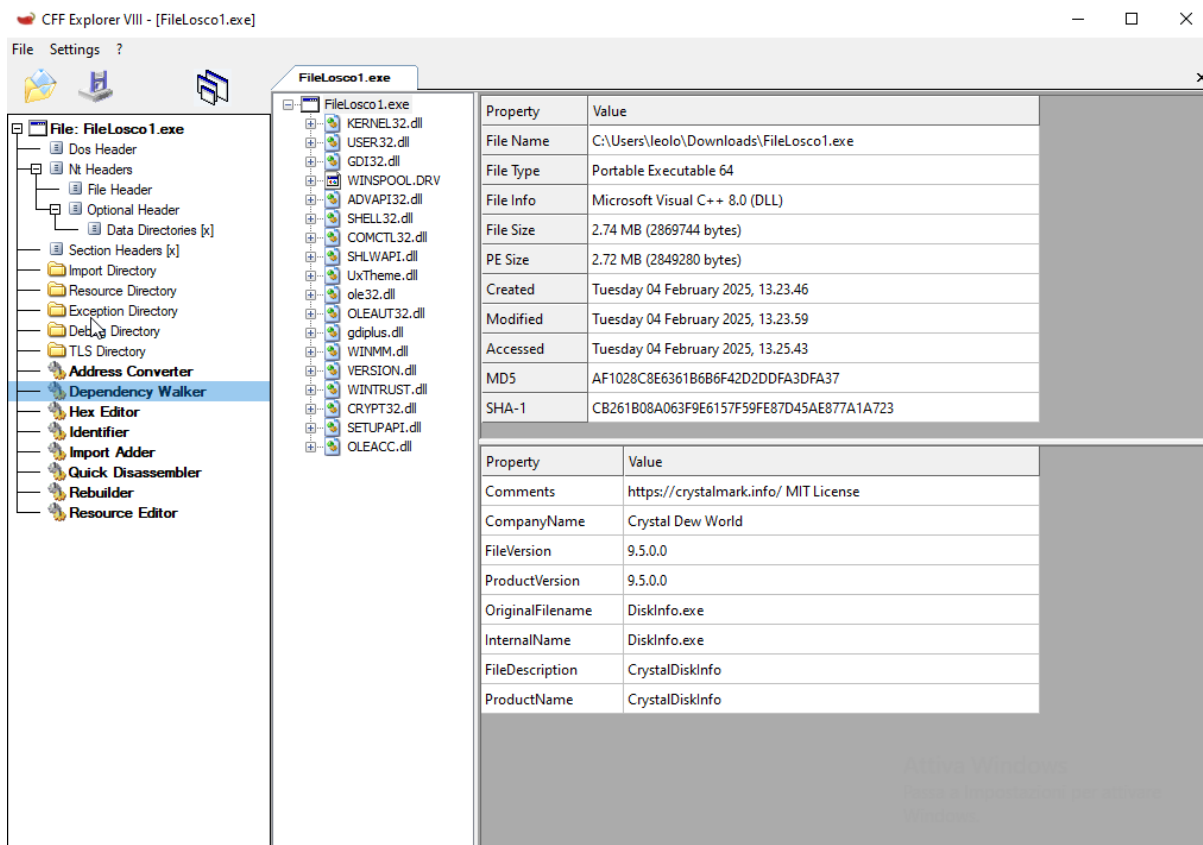
Queste risorse vengono utilizzate dall'applicazione durante la sua esecuzione.



Come da screen possiamo notare che ci sono varie tipi di Risorse, Cursors, Bitmaps, Icons, Menus, Dialogs, conoscendo il programma so che ci sono vari menu' di scelta con delle varie impostazioni per analizzare i vari tipi di dischi rigidi, e varie icone e tabelle dove sono riportati i dettagli del disco rigido specifico.

### -Dependency Walker:

Il Dependency Walker elenca tutte le librerie (DLL) delle quali il file eseguibile dipende, cioè le librerie che deve caricare per funzionare correttamente.



Qui ritroviamo le varie librerie .dll Kernel32, User32, GDI32, Comctl32, precedentemente analizzate.

Riassumendo le dll:

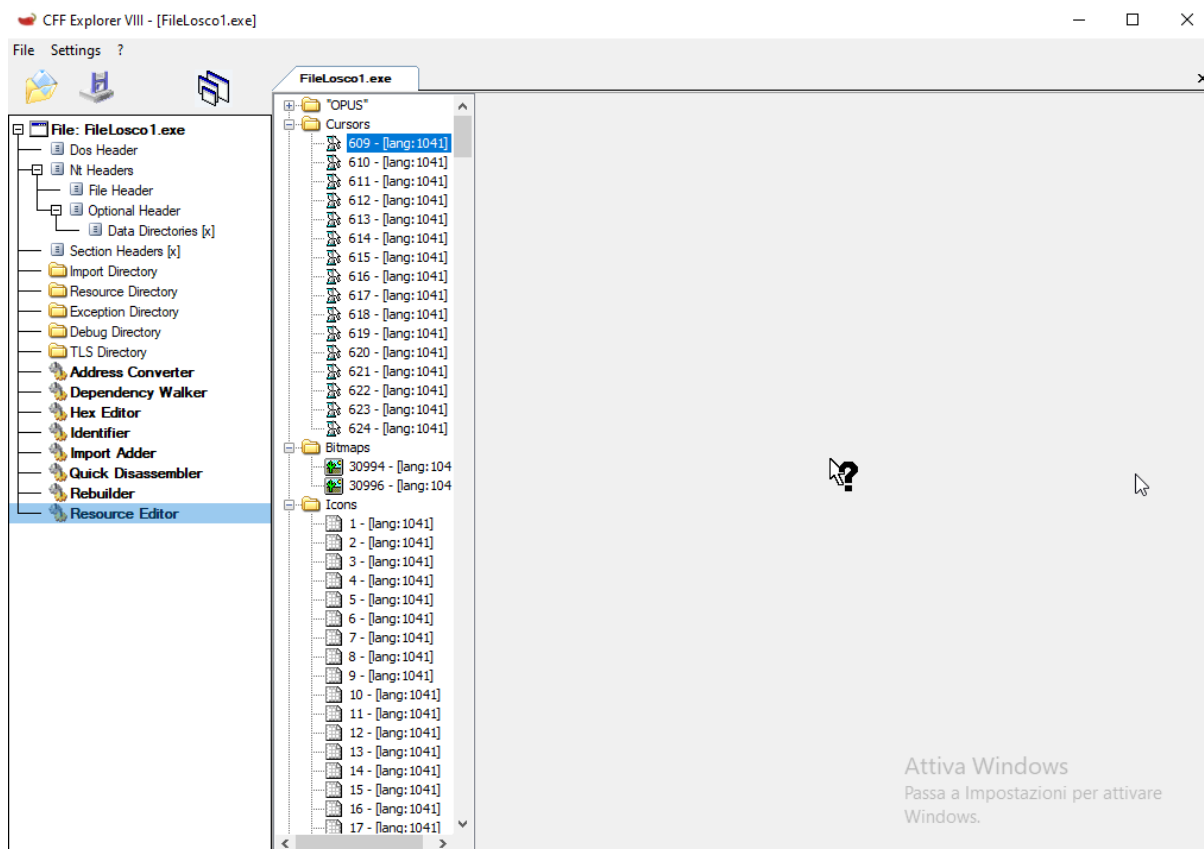
- KERNEL32.dll: Gestione di processi e file
- USER32.dll: Interazione con l'utente
- GDI32.dll: Funzioni grafiche
- SHELL32.dll: Accesso a file e cartelle.
- ADVAPI32.dll: Accesso e modifica della sicurezza e del registro di sistema.
- COMCTL32.dll: Componenti dell'interfaccia utente.

### -Resource Editor:

Questa sezione elenca le risorse incorporate nel file eseguibile, organizzate in categorie come icone, dialoghi, gruppi di icone e file di configurazioni.

Le risorse sono identificate tramite un ID e una lingua:





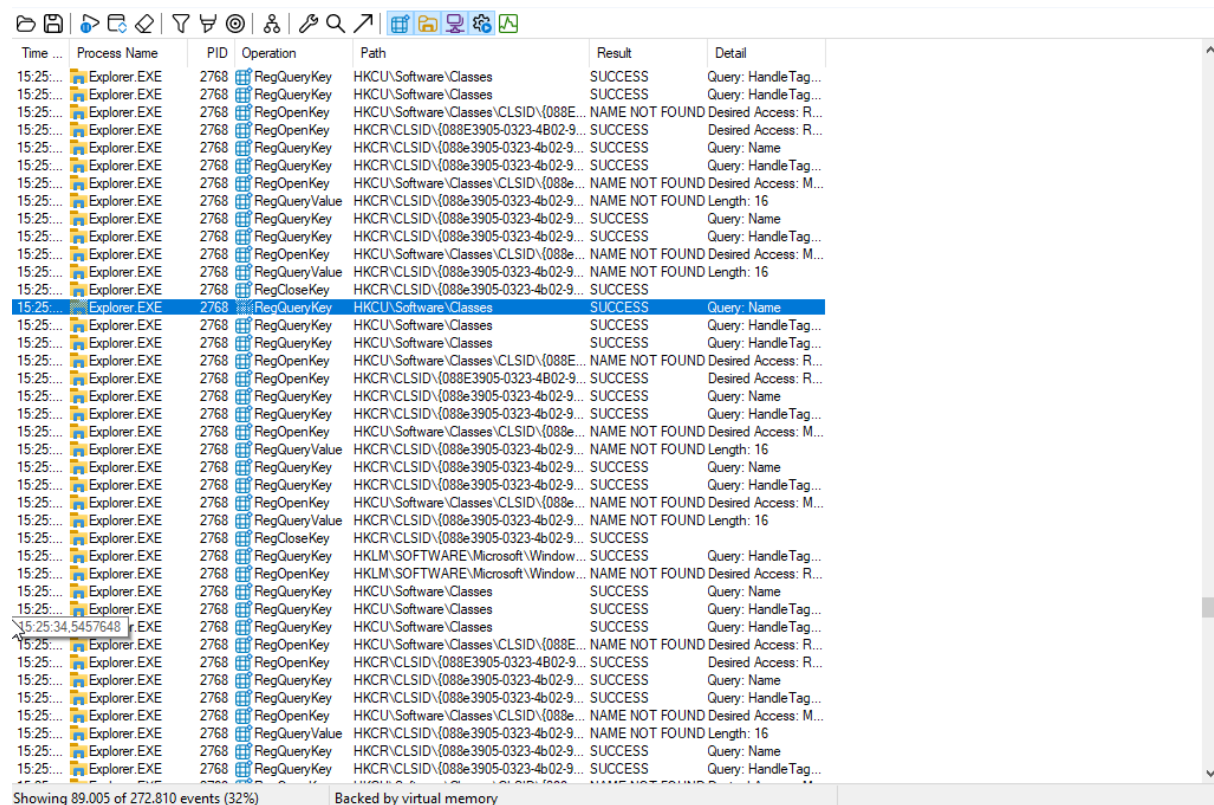
### -Analisi Dinamica:

Con l'analisi dinamica andiamo ad eseguire il file sospetto in un ambiente controllato, come una macchina virtuale o un sandbox.

Il pro dell'analisi Dinamica è che abbiamo un'osservazione diretta del comportamento specifico del file sospetto, andando a monitorare tutte le sue azioni e andando alla fine ad analizzare i risultati.

Utilizziamo il programma Procmon64.

Avviamo il programma e facciamo partire il file.exe sospetto.



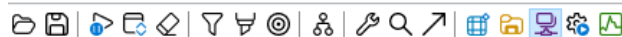
The screenshot shows the Process Monitor (ProcMon) application window. The top toolbar includes icons for file operations, process management, and search. The main window displays a table of registry operations performed by Explorer.EXE. The table has columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The operations are listed in chronological order, showing various registry queries and modifications. The status bar at the bottom indicates that 89,005 of 272,810 events (32%) are shown, and the data is backed by virtual memory.

Time ...	Process Name	PID	Operation	Path	Result	Detail
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCU\Software\Classes\CLSID\{088E...	NAME NOT FOUND	Desired Access: R...
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Desired Access: R...
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Name
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Handle Tag...
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCU\Software\Classes\CLSID\{088E...	NAME NOT FOUND	Desired Access: M...
15:25:...	Explorer.EXE	2768	RegQueryValue	HKCR\CLSID\{088E3905-0323-4B02-9...	NAME NOT FOUND	Length: 16
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Name
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Handle Tag...
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCU\Software\Classes\CLSID\{088E...	NAME NOT FOUND	Desired Access: M...
15:25:...	Explorer.EXE	2768	RegQueryValue	HKCR\CLSID\{088E3905-0323-4B02-9...	NAME NOT FOUND	Length: 16
15:25:...	Explorer.EXE	2768	RegCloseKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCU\Software\Classes\CLSID\{088E...	NAME NOT FOUND	Desired Access: R...
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Desired Access: R...
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Name
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Handle Tag...
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCU\Software\Classes\CLSID\{088E...	NAME NOT FOUND	Desired Access: M...
15:25:...	Explorer.EXE	2768	RegQueryValue	HKCR\CLSID\{088E3905-0323-4B02-9...	NAME NOT FOUND	Length: 16
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Name
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Handle Tag...
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCU\Software\Classes\CLSID\{088E...	NAME NOT FOUND	Desired Access: M...
15:25:...	Explorer.EXE	2768	RegQueryValue	HKCR\CLSID\{088E3905-0323-4B02-9...	NAME NOT FOUND	Length: 16
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Name
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Handle Tag...
15:25:...	Explorer.EXE	2768	RegOpenKey	HKCU\Software\Classes\CLSID\{088E...	NAME NOT FOUND	Desired Access: M...
15:25:...	Explorer.EXE	2768	RegQueryValue	HKCR\CLSID\{088E3905-0323-4B02-9...	NAME NOT FOUND	Length: 16
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Name
15:25:...	Explorer.EXE	2768	RegQueryKey	HKCR\CLSID\{088E3905-0323-4B02-9...	SUCCESS	Query: Handle Tag...

Showing 89,005 of 272,810 events (32%)      Backed by virtual memory

Vediamo che Explorer.EXE sta interrogando le chiavi di registro con successo:

Successivamente lascio in monitoraggio solamente la rete:



Time ...	Process Name	PID	Operation	Path	Result	Detail
15:25:...	SkypeApp.exe	6992	TCP Receive	DESKTOP-1NE9OHLan:49807 -> 51.1...	SUCCESS	Length: 0, seqnum:...
15:25:...	OneDrive.exe	4208	TCP Send	DESKTOP-1NE9OHLan:49732 -> 40.8...	SUCCESS	Length: 43, startin...
15:25:...	OneDrive.exe	4208	TCP Receive	DESKTOP-1NE9OHLan:49732 -> 40.8...	SUCCESS	Length: 174, seqn...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:54150 -> 10.0...	SUCCESS	Length: 44, sequ...
15:25:...	svchost.exe	1348	UDP Receive	DESKTOP-1NE9OHLan:54150 -> 10.0...	SUCCESS	Length: 130, seqn...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:54150 -> fd00...	SUCCESS	Length: 44, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:50052 -> 10.0...	SUCCESS	Length: 44, sequ...
15:25:...	svchost.exe	1348	UDP Receive	DESKTOP-1NE9OHLan:50052 -> 10.0...	SUCCESS	Length: 118, seqn...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:60780 -> 10.0...	SUCCESS	Length: 39, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:51878 -> 10.0...	SUCCESS	Length: 90, sequ...
15:25:...	svchost.exe	1348	UDP Receive	DESKTOP-1NE9OHLan:51878 -> 10.0...	SUCCESS	Length: 154, seqn...
15:25:...	svchost.exe	1348	UDP Receive	DESKTOP-1NE9OHLan:60780 -> 10.0...	SUCCESS	Length: 39, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:61127 -> ff02...	SUCCESS	Length: 39, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:62439 -> ff02...	SUCCESS	Length: 90, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:61127 -> 224...	SUCCESS	Length: 39, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:62439 -> 224...	SUCCESS	Length: 90, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:62439 -> ff02...	SUCCESS	Length: 90, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:62439 -> 224...	SUCCESS	Length: 90, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:61127 -> ff02...	SUCCESS	Length: 39, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:63996 -> 10.0...	SUCCESS	Length: 90, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:59284 -> 10.0...	SUCCESS	Length: 42, sequ...
15:25:...	svchost.exe	1348	UDP Receive	DESKTOP-1NE9OHLan:63996 -> 10.0...	SUCCESS	Length: 154, seqn...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:63582 -> ff02...	SUCCESS	Length: 90, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:63582 -> 224...	SUCCESS	Length: 90, sequ...
15:25:...	svchost.exe	1348	UDP Receive	DESKTOP-1NE9OHLan:59284 -> 10.0...	SUCCESS	Length: 99, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:64760 -> ff02...	SUCCESS	Length: 42, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:64760 -> 224...	SUCCESS	Length: 42, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:63582 -> ff02...	SUCCESS	Length: 90, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:64760 -> ff02...	SUCCESS	Length: 42, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:64760 -> 224...	SUCCESS	Length: 42, sequ...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:63582 -> 224...	SUCCESS	Length: 90, sequ...
15:25:...	SkypeApp.exe	6992	TCP Receive	DESKTOP-1NE9OHLan:49809 -> 52.1...	SUCCESS	Length: 0, seqnum:...
15:25:...	svchost.exe	1348	UDP Send	DESKTOP-1NE9OHLan:52221 -> 10.0...	SUCCESS	Length: 45, sequ...
15:25:...	svchost.exe	1348	UDP Receive	DESKTOP-1NE9OHLan:52221 -> 10.0...	SUCCESS	Length: 119, seqn...
15:26:...	OneDrive.exe	4208	TCP Send	DESKTOP-1NE9OHLan:49732 -> 40.8...	SUCCESS	Length: 43, startin...
15:26:...	OneDrive.exe	4208	TCP Receive	DESKTOP-1NE9OHLan:49732 -> 40.8...	SUCCESS	Length: 174, seqn...

Si può vedere come il file.exe sospetto stia inviando dati verso altri indirizzi IP utilizzando TCP e UDP.