S9-L2
Analisi malware

Emanuele Benedetti | 4 febbraio 2025

Consegna

Sarà condiviso un malware relativamente innocuo.

Compiti:

1. **Analisi statica**: esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità
2. **Analisi dinamica**: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

Svolgimento

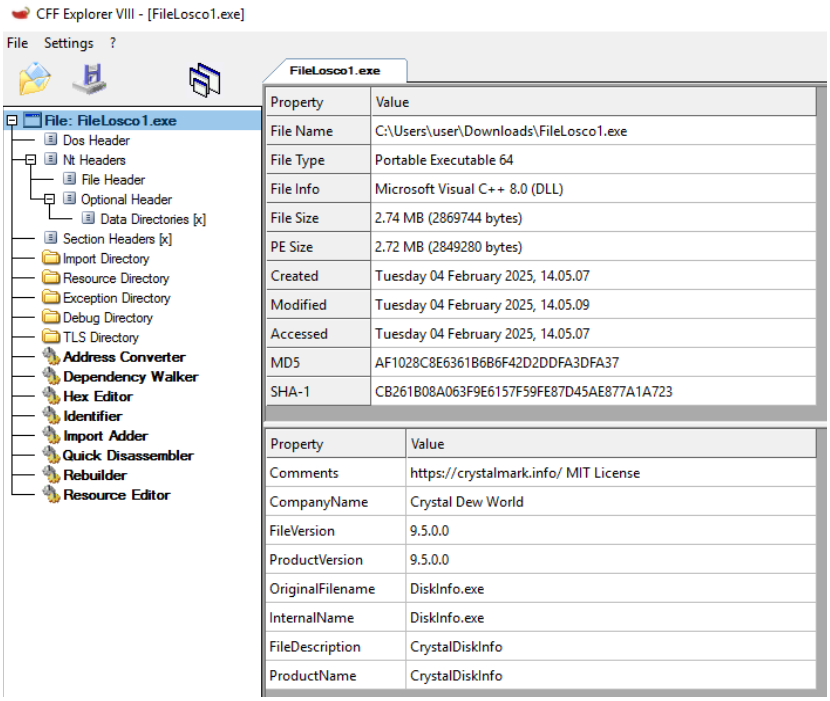
Ho svolto il laboratorio in una macchina virtuale Windows 10 in modo tale da avere un ambiente sicuro ed isolato in cui analizzare il file della consegna.

Analisi statica

Dopo aver scaricato il sospetto malware, ho effettuato un'analisi statica tramite il software *CFF explorer*. In questo modo è possibile comprendere la struttura e il funzionamento del programma ancor prima di eseguirlo.

Ho importato il *FileLosco1.exe* e nella pagina relativa alle informazioni sul file ho potuto vedere molte informazioni importanti come il tipo di file (Portable Executable 64), la data di creazione e modifica e l'hash del file in formato MD5 e SHA-1.

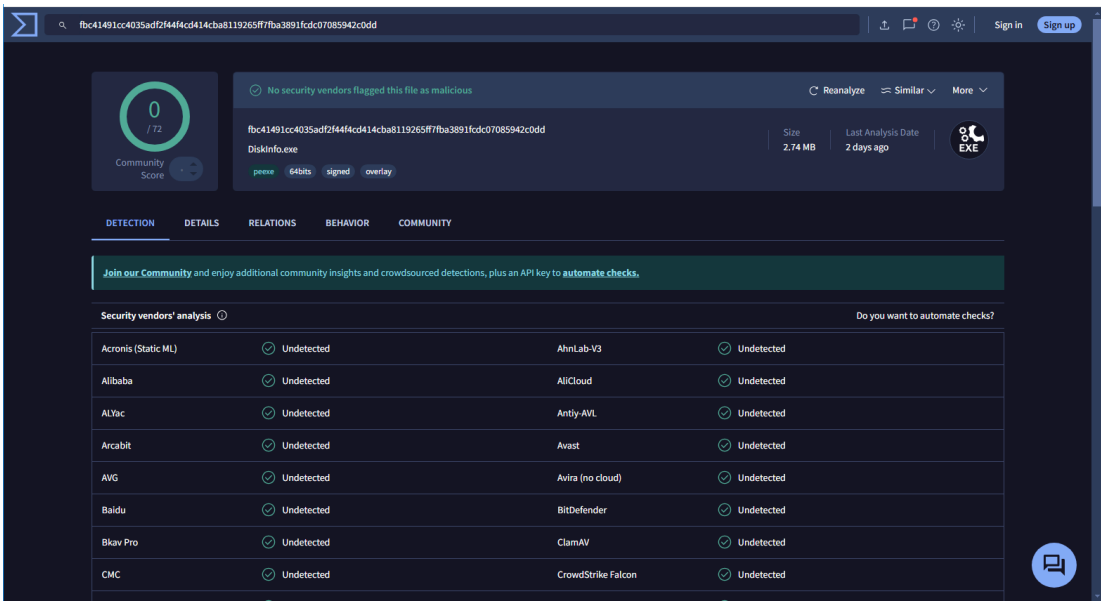
Come mostrato nello screen sono anche presenti informazioni sul file originale come il nome (***DiskInfo.exe***), la versione software e la casa produttrice.



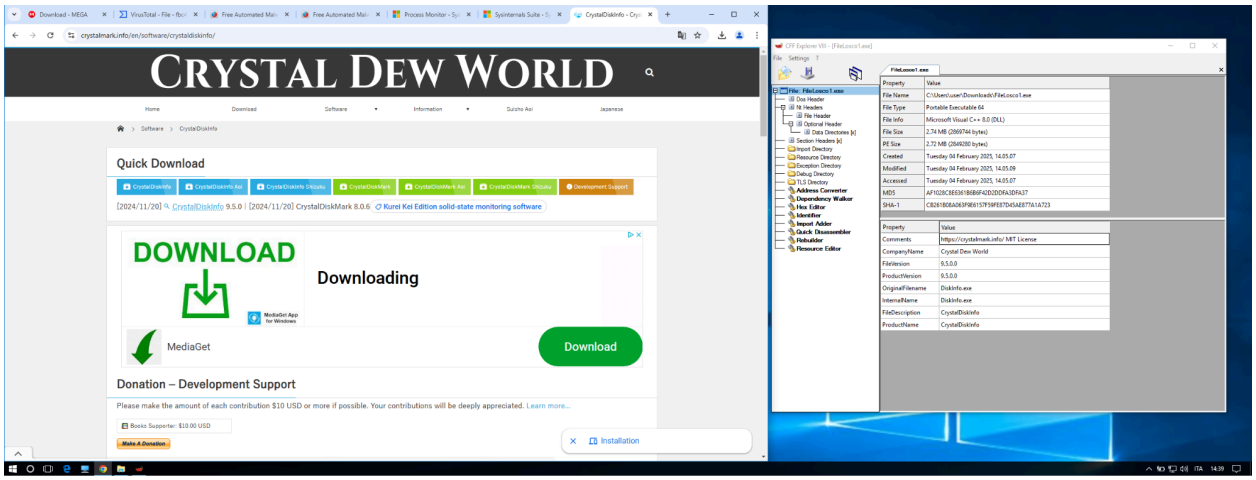
Property	Value
File Name	C:\Users\user\Downloads\FileLosco1.exe
File Type	Portable Executable 64
File Info	Microsoft Visual C++ 8.0 (DLL)
File Size	2.74 MB (2869744 bytes)
PE Size	2.72 MB (2849280 bytes)
Created	Tuesday 04 February 2025, 14.05.07
Modified	Tuesday 04 February 2025, 14.05.09
Accessed	Tuesday 04 February 2025, 14.05.07
MD5	AF1028C8E6361B6B6F42D2DDFA3DFA37
SHA-1	CB261B08A063F9E6157F59FE87D45AE877A1A723

Property	Value
Comments	https://crystalmark.info/ MIT License
CompanyName	Crystal Dew World
FileVersion	9.5.0.0
ProductVersion	9.5.0.0
OriginalFilename	DiskInfo.exe
InternalName	DiskInfo.exe
FileDescription	CrystalDiskInfo
ProductName	CrystalDiskInfo

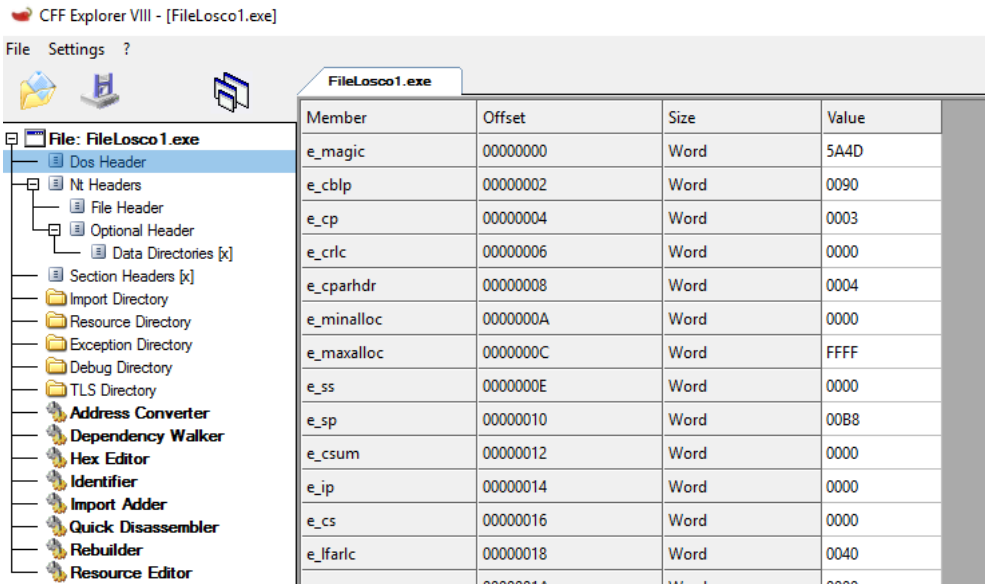
Ho utilizzato il codice hash SHA-1 per effettuare una verifica tramite VirusTotal del file fornito. Il risultato mostra che tutti i motori di ricerca antivirus non individuano alcuna criticità



Come abbiamo già avuto modo di vedere, questo risultato non ci garantisce che il file sia sicuro ma possiamo ulteriormente approfondire cercando online tramite le informazioni fornite da CFF. In questo caso siamo risaliti al sito del produttore ed al link per scaricare il software.

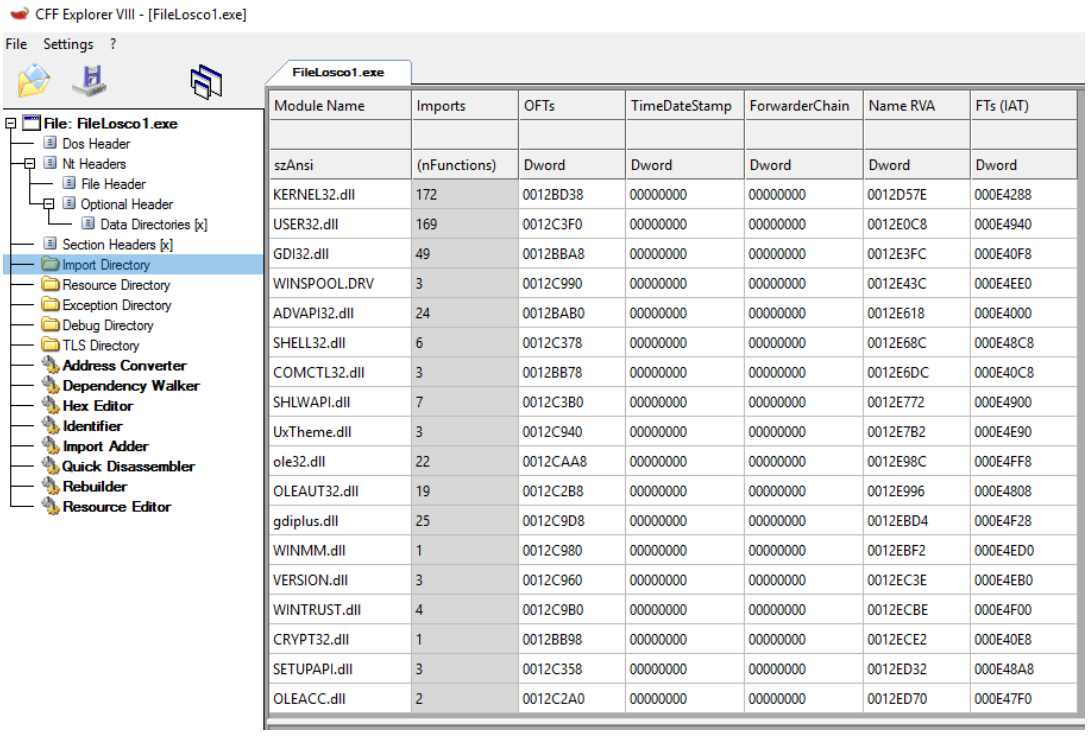


Controllando il *Dos header* possiamo verificare l'*e_magic* che ha un valore *5A4D* che corrisponde alle lettere "MZ" in ASCII, ovvero la firma standard di un file eseguibile.



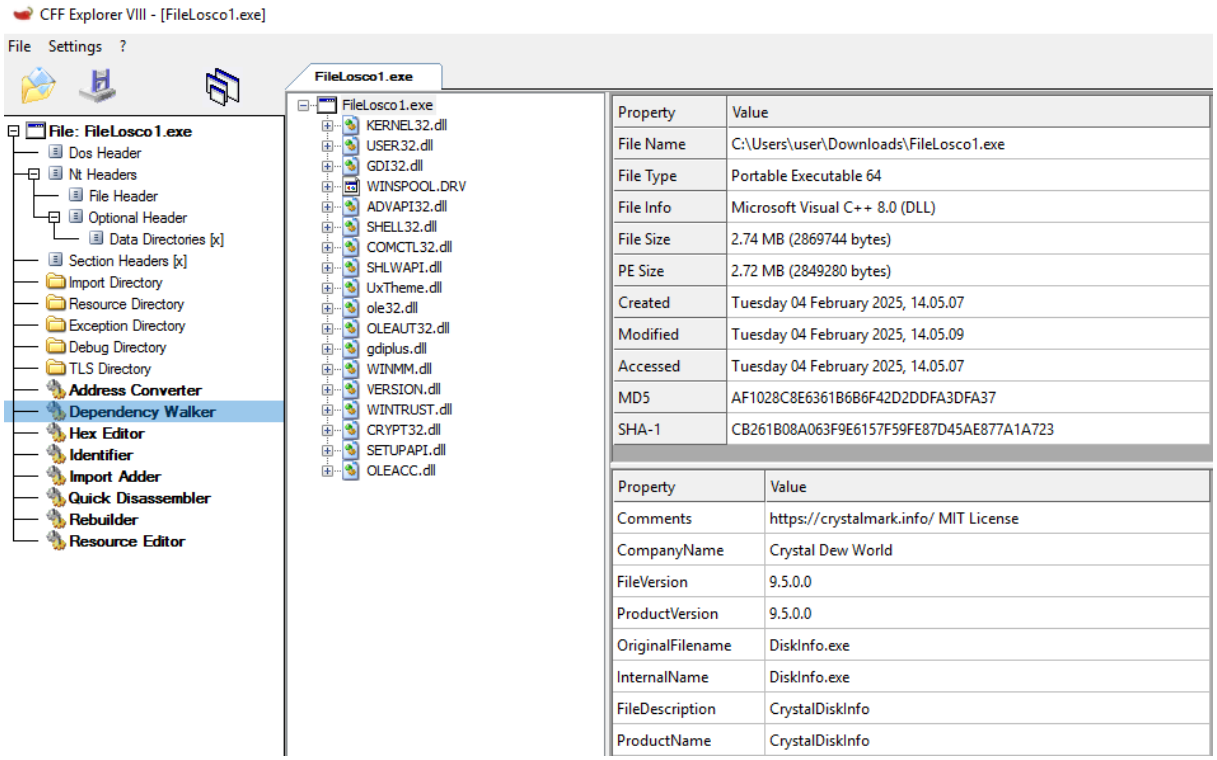
Member	Offset	Size	Value
e_magic	00000000	Word	5A4D
e_cblp	00000002	Word	0090
e_cp	00000004	Word	0003
e_crlc	00000006	Word	0000
e_cparhdr	00000008	Word	0004
e_minalloc	0000000A	Word	0000
e_maxalloc	0000000C	Word	FFFF
e_ss	0000000E	Word	0000
e_sp	00000010	Word	00B8
e_csum	00000012	Word	0000
e_ip	00000014	Word	0000
e_cs	00000016	Word	0000
e_lfarlc	00000018	Word	0040

Nella sezione *Import Directory* vediamo che vengono importate molte funzioni dalle librerie DLL di sistema, in particolare 172 da *KERNEL32* e 169 da *USER32*.



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

Infine nella sezione *Dependency Walker* vengono mostrate le DLL dalle quali l'eseguibile dipende e che vengono caricate per il funzionamento del programma.



Property	Value
File Name	C:\Users\user\Downloads\FileLosco1.exe
File Type	Portable Executable 64
File Info	Microsoft Visual C++ 8.0 (DLL)
File Size	2.74 MB (2869744 bytes)
PE Size	2.72 MB (2849280 bytes)
Created	Tuesday 04 February 2025, 14.05.07
Modified	Tuesday 04 February 2025, 14.05.09
Accessed	Tuesday 04 February 2025, 14.05.07
MD5	AF1028C8E6361B6B6F42D2DDFA3DFA37
SHA-1	CB261B08A063F9E6157F59FE87D45AE877A1A723

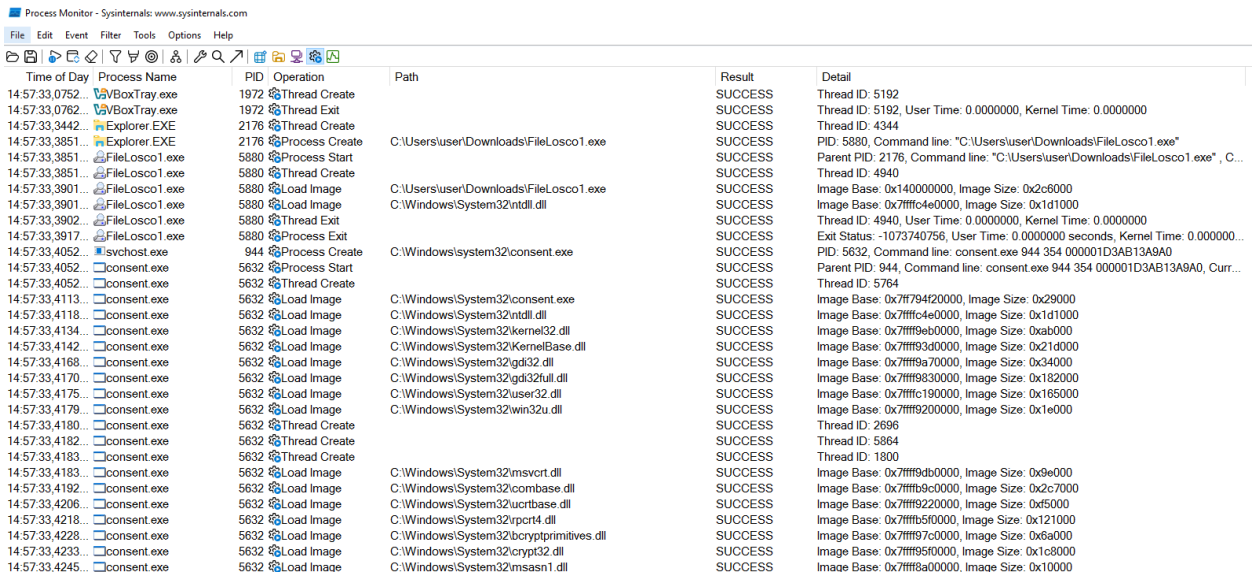
Property	Value
Comments	https://crystalmark.info/ MIT License
CompanyName	Crystal Dew World
FileVersion	9.5.0.0
ProductVersion	9.5.0.0
OriginalFilename	DiskInfo.exe
InternalName	DiskInfo.exe
FileDescription	CrystalDiskInfo
ProductName	CrystalDiskInfo

Analisi dinamica

L'analisi dinamica permette di eseguire il file in un ambiente isolato e sicuro riuscendo a comprendere il funzionamento effettivo del software.

Ho avviato il software *Procmon64* ed eseguito il file della consegna. Per prima cosa ho attivato il filtro per analizzare le attività e i processi di sistema. All'avvio dell'eseguibile viene creato un nuovo processo con PID 5880 e un thread tramite le operazioni *Process Create* e *Thread Create*.

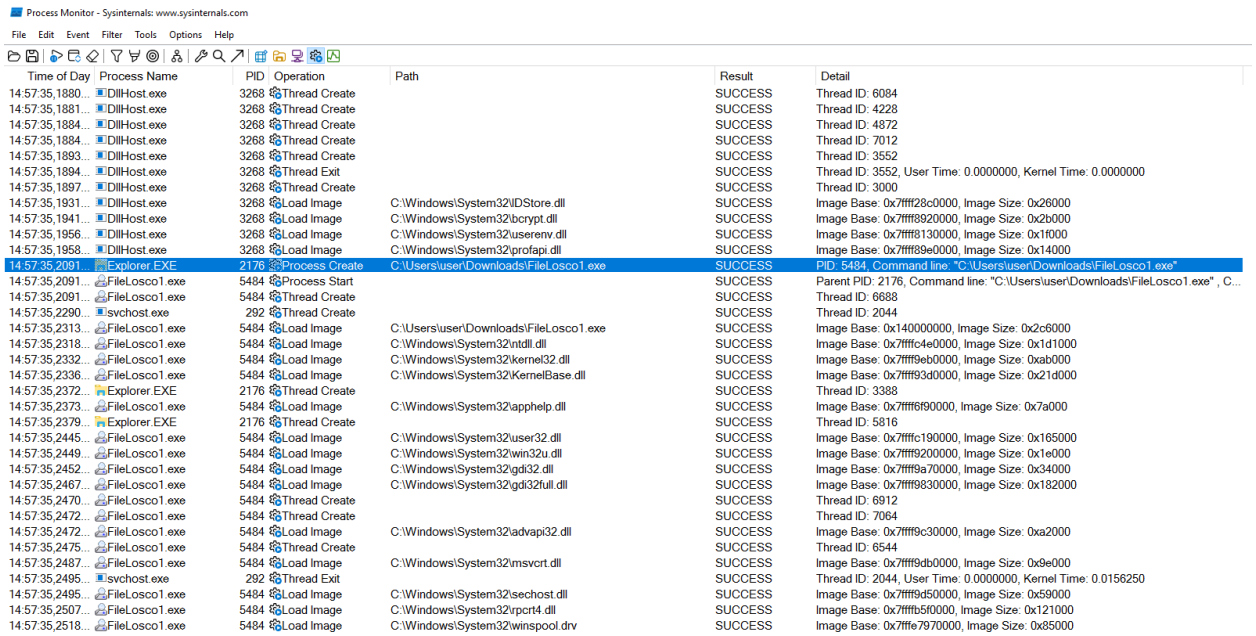
Nello screenshot vengono riportate le operazioni iniziali di avvio del programma e il caricamento di varie librerie di sistema.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
14:57:33,0752...	VBoxTray.exe	1972	Thread Create		SUCCESS	Thread ID: 5192
14:57:33,0762...	VBoxTray.exe	1972	Thread Exit		SUCCESS	Thread ID: 5192, User Time: 0.0000000, Kernel Time: 0.0000000
14:57:33,3442...	Explorer.EXE	2176	Thread Create		SUCCESS	Thread ID: 4344
14:57:33,3851...	Explorer.EXE	2176	Process Create	C:\Users\user\Downloads\FileLosco1.exe	SUCCESS	PID: 5880, Command line: "C:\Users\user\Downloads\FileLosco1.exe"
14:57:33,3851...	FileLosco1.exe	5880	Process Start		SUCCESS	Parent PID: 2176, Command line: "C:\Users\user\Downloads\FileLosco1.exe" , C...
14:57:33,3851...	FileLosco1.exe	5880	Thread Create		SUCCESS	Thread ID: 4940
14:57:33,3901...	FileLosco1.exe	5880	Load Image	C:\Users\user\Downloads\FileLosco1.exe	SUCCESS	Image Base: 0x140000000, Image Size: 0x2c6000
14:57:33,3901...	FileLosco1.exe	5880	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fffc4e0000, Image Size: 0x1d1000
14:57:33,3902...	FileLosco1.exe	5880	Thread Exit		SUCCESS	Thread ID: 4940, User Time: 0.0000000, Kernel Time: 0.0000000
14:57:33,3917...	FileLosco1.exe	5880	Process Exit		SUCCESS	Exit Status: -1073740756, User Time: 0.0000000 seconds, Kernel Time: 0.000000...
14:57:33,4052...	svchost.exe	944	Process Create	C:\Windows\system32\consent.exe	SUCCESS	PID: 5632, Command line: consent.exe 944 354 000001D3AB13A9A0
14:57:33,4052...	consent.exe	5632	Process Start		SUCCESS	Parent PID: 944, Command line: consent.exe 944 354 000001D3AB13A9A0, Curr...
14:57:33,4052...	consent.exe	5632	Thread Create		SUCCESS	Thread ID: 5764
14:57:33,4113...	consent.exe	5632	Load Image	C:\Windows\System32\consent.exe	SUCCESS	Image Base: 0x7ff794f20000, Image Size: 0x29000
14:57:33,4118...	consent.exe	5632	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fffc4e0000, Image Size: 0x1d1000
14:57:33,4134...	consent.exe	5632	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffff9eb0000, Image Size: 0xab000
14:57:33,4142...	consent.exe	5632	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffff93d0000, Image Size: 0x21d000
14:57:33,4168...	consent.exe	5632	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ffff9a70000, Image Size: 0x34000
14:57:33,4170...	consent.exe	5632	Load Image	C:\Windows\System32\gdi32full.dll	SUCCESS	Image Base: 0x7ffff9830000, Image Size: 0x182000
14:57:33,4175...	consent.exe	5632	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x7ffffc190000, Image Size: 0x165000
14:57:33,4179...	consent.exe	5632	Load Image	C:\Windows\System32\win32u.dll	SUCCESS	Image Base: 0x7ffff9200000, Image Size: 0x1e000
14:57:33,4180...	consent.exe	5632	Thread Create		SUCCESS	Thread ID: 2696
14:57:33,4182...	consent.exe	5632	Thread Create		SUCCESS	Thread ID: 5864
14:57:33,4183...	consent.exe	5632	Thread Create		SUCCESS	Thread ID: 1800
14:57:33,4183...	consent.exe	5632	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ffff9db0000, Image Size: 0x9e000
14:57:33,4192...	consent.exe	5632	Load Image	C:\Windows\System32\combase.dll	SUCCESS	Image Base: 0x7fffb9c0000, Image Size: 0x2c7000
14:57:33,4206...	consent.exe	5632	Load Image	C:\Windows\System32\ucrtbase.dll	SUCCESS	Image Base: 0x7ffff9220000, Image Size: 0xf5000
14:57:33,4218...	consent.exe	5632	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7fffb5f0000, Image Size: 0x121000
14:57:33,4228...	consent.exe	5632	Load Image	C:\Windows\System32\bcryptprimitives.dll	SUCCESS	Image Base: 0x7ffff97c0000, Image Size: 0x6a000
14:57:33,4233...	consent.exe	5632	Load Image	C:\Windows\System32\crypt32.dll	SUCCESS	Image Base: 0x7ffff95f0000, Image Size: 0x1c8000
14:57:33,4245...	consent.exe	5632	Load Image	C:\Windows\System32\msasn1.dll	SUCCESS	Image Base: 0x7ffff8a00000, Image Size: 0x10000

Al termine della validazione dei permessi per l'esecuzione, il flusso ritorna al programma che viene finalmente avviato, come mostrato nell'immagine che segue.

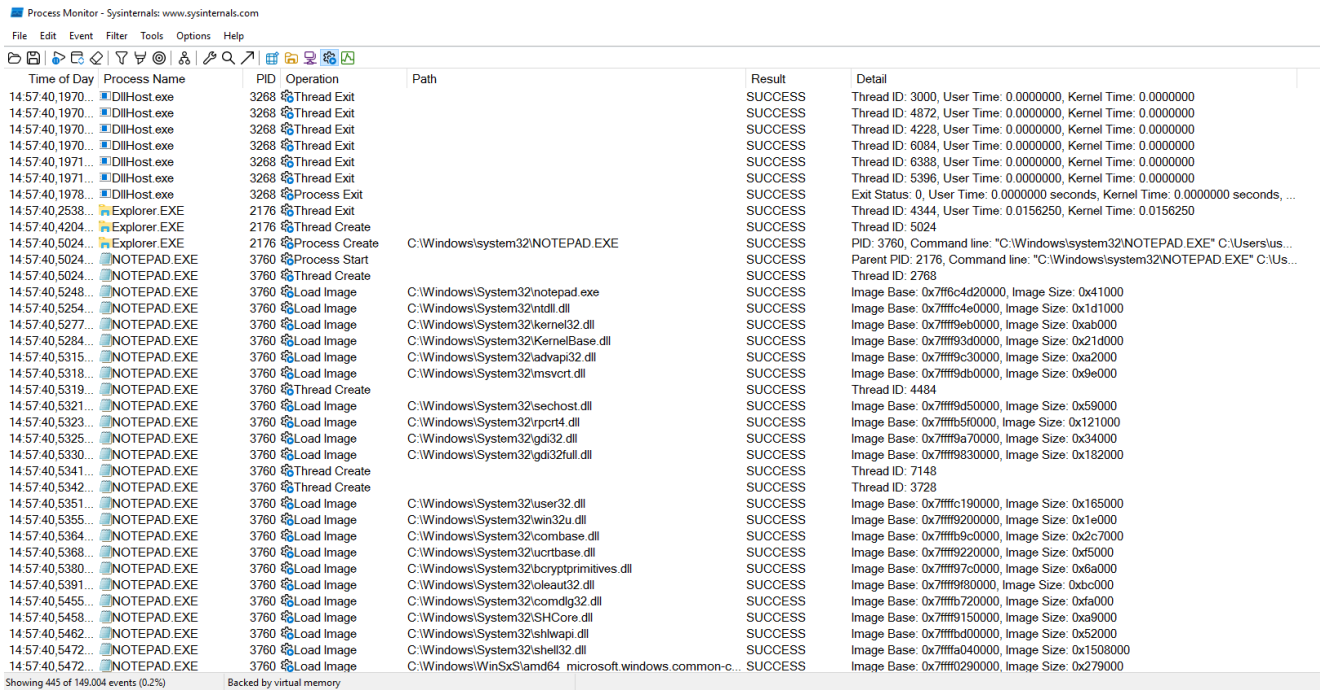
Tramite le operazioni *Load Image*, vengono caricati tutte le librerie necessarie al funzionamento del programma, come visto in precedenza nell'analisi statica .



Time of Day	Process Name	PID	Operation	Path	Result	Detail
14:57:35,1880...	DllHost.exe	3268	Thread Create		SUCCESS	Thread ID: 6084
14:57:35,1881...	DllHost.exe	3268	Thread Create		SUCCESS	Thread ID: 4228
14:57:35,1884...	DllHost.exe	3268	Thread Create		SUCCESS	Thread ID: 4872
14:57:35,1884...	DllHost.exe	3268	Thread Create		SUCCESS	Thread ID: 7012
14:57:35,1893...	DllHost.exe	3268	Thread Create		SUCCESS	Thread ID: 3552
14:57:35,1894...	DllHost.exe	3268	Thread Exit		SUCCESS	Thread ID: 3552, User Time: 0.0000000, Kernel Time: 0.0000000
14:57:35,1897...	DllHost.exe	3268	Thread Create		SUCCESS	Thread ID: 3000
14:57:35,1931...	DllHost.exe	3268	Load Image	C:\Windows\System32\IDStore.dll	SUCCESS	Image Base: 0x7ffff28c0000, Image Size: 0x26000
14:57:35,1941...	DllHost.exe	3268	Load Image	C:\Windows\System32\bcrypt.dll	SUCCESS	Image Base: 0x7ffff8920000, Image Size: 0x2b000
14:57:35,1956...	DllHost.exe	3268	Load Image	C:\Windows\System32\userenv.dll	SUCCESS	Image Base: 0x7ffff8130000, Image Size: 0x1f000
14:57:35,1958...	DllHost.exe	3268	Load Image	C:\Windows\System32\profapi.dll	SUCCESS	Image Base: 0x7ffff89e0000, Image Size: 0x14000
14:57:35,2091...	Explorer.EXE	2176	Process Create	C:\Users\user\Downloads\FileLosco1.exe	SUCCESS	PID: 5484, Command line: "C:\Users\user\Downloads\FileLosco1.exe"
14:57:35,2091...	FileLosco1.exe	5484	Process Start		SUCCESS	Parent PID: 2176, Command line: "C:\Users\user\Downloads\FileLosco1.exe" , C...
14:57:35,2091...	FileLosco1.exe	5484	Thread Create		SUCCESS	Thread ID: 6688
14:57:35,2290...	svchost.exe	292	Thread Create		SUCCESS	Thread ID: 2044
14:57:35,2313...	FileLosco1.exe	5484	Load Image	C:\Users\user\Downloads\FileLosco1.exe	SUCCESS	Image Base: 0x140000000, Image Size: 0x2c6000
14:57:35,2318...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffffc4e0000, Image Size: 0x1d1000
14:57:35,2332...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffff9eb0000, Image Size: 0xab000
14:57:35,2336...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffff93d0000, Image Size: 0x21d000
14:57:35,2372...	Explorer.EXE	2176	Thread Create		SUCCESS	Thread ID: 3388
14:57:35,2373...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\apphelp.dll	SUCCESS	Image Base: 0x7ffff6f90000, Image Size: 0x7a000
14:57:35,2379...	Explorer.EXE	2176	Thread Create		SUCCESS	Thread ID: 5816
14:57:35,2445...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x7ffffc190000, Image Size: 0x165000
14:57:35,2449...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\win32u.dll	SUCCESS	Image Base: 0x7ffff9200000, Image Size: 0x1e000
14:57:35,2452...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ffff9a70000, Image Size: 0x34000
14:57:35,2467...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\gdi32full.dll	SUCCESS	Image Base: 0x7ffff9830000, Image Size: 0x182000
14:57:35,2470...	FileLosco1.exe	5484	Thread Create		SUCCESS	Thread ID: 6912
14:57:35,2472...	FileLosco1.exe	5484	Thread Create		SUCCESS	Thread ID: 7064
14:57:35,2472...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ffff9c30000, Image Size: 0xa2000
14:57:35,2475...	FileLosco1.exe	5484	Thread Create		SUCCESS	Thread ID: 6544
14:57:35,2487...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ffff9db0000, Image Size: 0x9e000
14:57:35,2495...	svchost.exe	292	Thread Exit		SUCCESS	Thread ID: 2044, User Time: 0.0000000, Kernel Time: 0.0156250
14:57:35,2495...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ffff9d50000, Image Size: 0x59000
14:57:35,2507...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7ffffb5f0000, Image Size: 0x121000
14:57:35,2518...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\winspool.drv	SUCCESS	Image Base: 0x7fffe7970000, Image Size: 0x85000

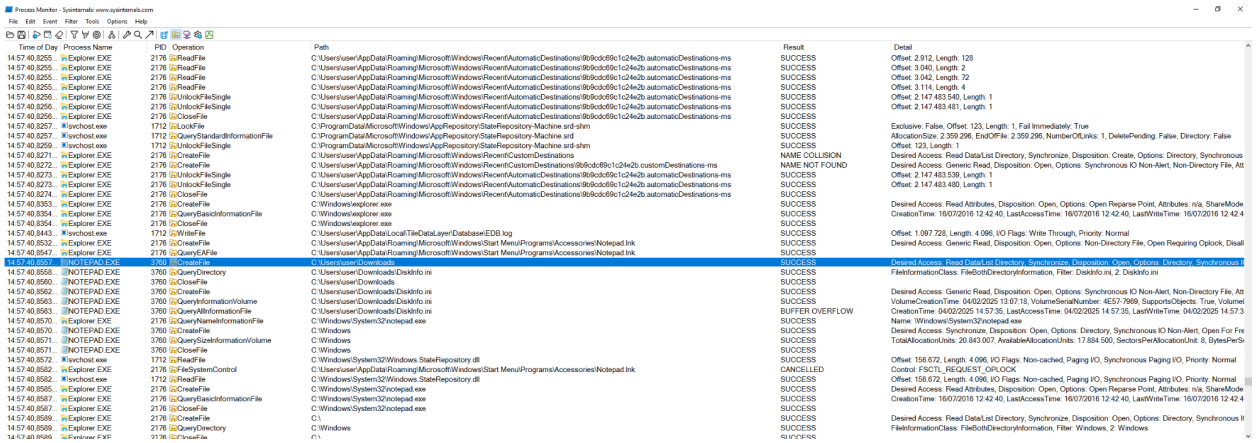
Al termine dell'esecuzione, vengono chiusi tutti i thread aperti tramite *Thread Exit*.

Ho quindi aperto il file *DiskInfo.ini* creato dal programma e come possiamo vedere le operazioni svolte dal sistema sono di creazione di un nuovo processo e di nuovi thread.



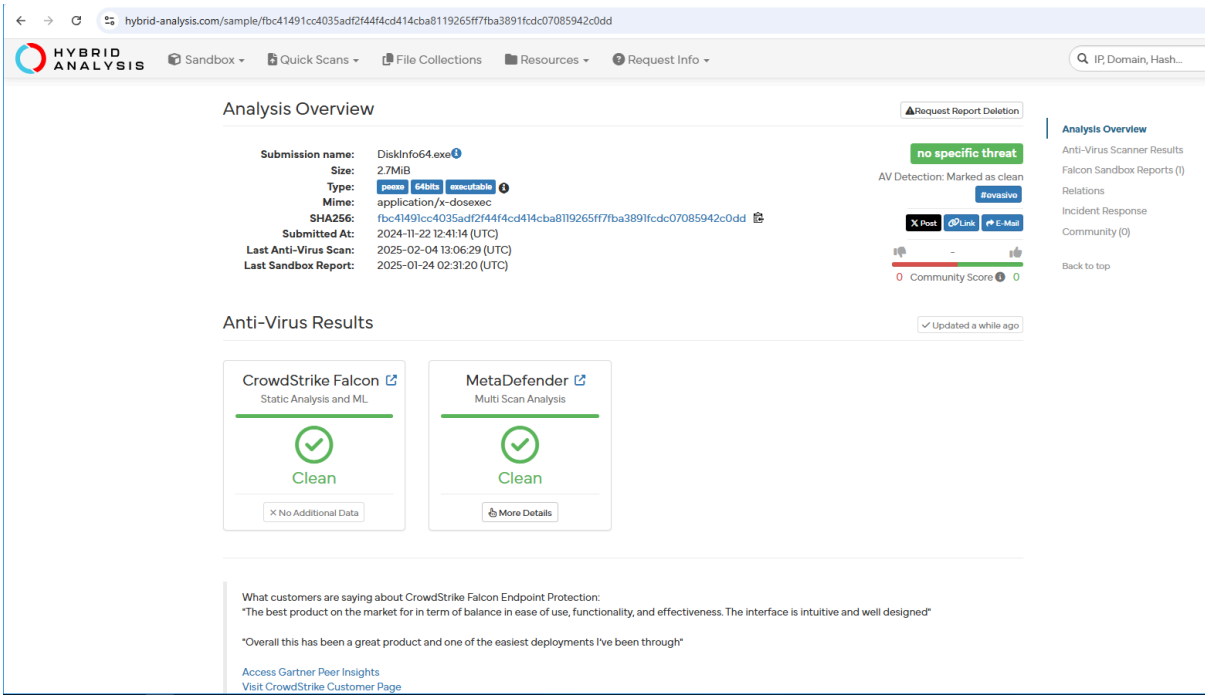
Time of Day	Process Name	PID	Operation	Path	Result	Detail
14:57:40,1970...	DllHost.exe	3268	Thread Exit		SUCCESS	Thread ID: 3000, User Time: 0.0000000, Kernel Time: 0.0000000
14:57:40,1970...	DllHost.exe	3268	Thread Exit		SUCCESS	Thread ID: 4872, User Time: 0.0000000, Kernel Time: 0.0000000
14:57:40,1970...	DllHost.exe	3268	Thread Exit		SUCCESS	Thread ID: 4228, User Time: 0.0000000, Kernel Time: 0.0000000
14:57:40,1970...	DllHost.exe	3268	Thread Exit		SUCCESS	Thread ID: 6084, User Time: 0.0000000, Kernel Time: 0.0000000
14:57:40,1971...	DllHost.exe	3268	Thread Exit		SUCCESS	Thread ID: 6388, User Time: 0.0000000, Kernel Time: 0.0000000
14:57:40,1971...	DllHost.exe	3268	Thread Exit		SUCCESS	Thread ID: 5396, User Time: 0.0000000, Kernel Time: 0.0000000
14:57:40,1978...	DllHost.exe	3268	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.0000000 seconds, ...
14:57:40,2538...	Explorer.EXE	2176	Thread Exit		SUCCESS	Thread ID: 4344, User Time: 0.0156250, Kernel Time: 0.0156250
14:57:40,4204...	Explorer.EXE	2176	Thread Create		SUCCESS	Thread ID: 5024
14:57:40,5024...	Explorer.EXE	2176	Process Create	C:\Windows\system32\NOTEPAD.EXE	SUCCESS	PID: 3760, Command line: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\us...
14:57:40,5024...	NOTEPAD.EXE	3760	Process Start		SUCCESS	Parent PID: 2176, Command line: "C:\Windows\system32\NOTEPAD.EXE" C:\Us...
14:57:40,5024...	NOTEPAD.EXE	3760	Thread Create		SUCCESS	Thread ID: 2768
14:57:40,5248...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\notepad.exe	SUCCESS	Image Base: 0x7ff6c4d20000, Image Size: 0x41000
14:57:40,5254...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffffc4e0000, Image Size: 0x1d1000
14:57:40,5277...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffff9eb0000, Image Size: 0xab000
14:57:40,5284...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffff93d0000, Image Size: 0x21d000
14:57:40,5315...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ffff9c30000, Image Size: 0xa2000
14:57:40,5318...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ffff9db0000, Image Size: 0x9e000
14:57:40,5319...	NOTEPAD.EXE	3760	Thread Create		SUCCESS	Thread ID: 4484
14:57:40,5321...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ffff9d50000, Image Size: 0x59000
14:57:40,5323...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7ffffb5f0000, Image Size: 0x121000
14:57:40,5325...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ffff9a70000, Image Size: 0x34000
14:57:40,5330...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\gdi32full.dll	SUCCESS	Image Base: 0x7ffff9830000, Image Size: 0x182000
14:57:40,5341...	NOTEPAD.EXE	3760	Thread Create		SUCCESS	Thread ID: 7148
14:57:40,5342...	NOTEPAD.EXE	3760	Thread Create		SUCCESS	Thread ID: 3728
14:57:40,5351...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x7ffffc190000, Image Size: 0x165000
14:57:40,5355...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\win32u.dll	SUCCESS	Image Base: 0x7ffff9200000, Image Size: 0x1e000
14:57:40,5364...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\combase.dll	SUCCESS	Image Base: 0x7ffffb9c0000, Image Size: 0x2c7000
14:57:40,5368...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\ucrtbase.dll	SUCCESS	Image Base: 0x7ffff9220000, Image Size: 0xf5000
14:57:40,5380...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\bcryptprimitives.dll	SUCCESS	Image Base: 0x7ffff97c0000, Image Size: 0x6a000
14:57:40,5391...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\oleaut32.dll	SUCCESS	Image Base: 0x7ffff9f80000, Image Size: 0xbc000
14:57:40,5455...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\comdlg32.dll	SUCCESS	Image Base: 0x7ffffb720000, Image Size: 0xfa000
14:57:40,5458...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\SHCore.dll	SUCCESS	Image Base: 0x7ffff9150000, Image Size: 0xa9000
14:57:40,5462...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\shlwapi.dll	SUCCESS	Image Base: 0x7ffffbd00000, Image Size: 0x52000
14:57:40,5472...	NOTEPAD.EXE	3760	Load Image	C:\Windows\System32\shell32.dll	SUCCESS	Image Base: 0x7ffffa040000, Image Size: 0x1508000
14:57:40,5472...	NOTEPAD.EXE	3760	Load Image	C:\Windows\WinSxS\amd64_microsoft.windows.common-c...	SUCCESS	Image Base: 0x7ffff0290000, Image Size: 0x279000

Possiamo utilizzare il filtro delle attività del file system per monitorare la lettura e la scrittura dei file nel sistema. Ad esempio possiamo seguire la creazione del file *DiskInfo.ini* come mostrato nell'immagine

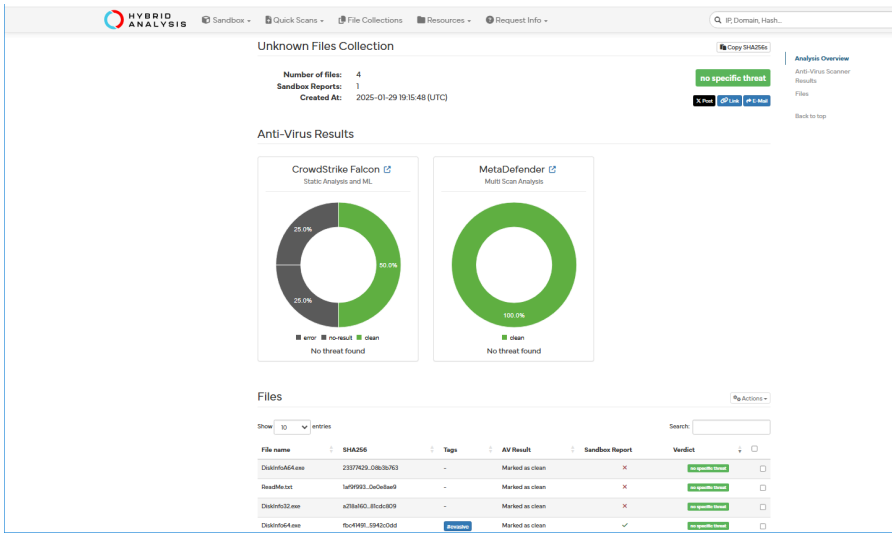


Ho inoltre caricato il file della consegna in una sandbox per ottenere ulteriori informazioni.

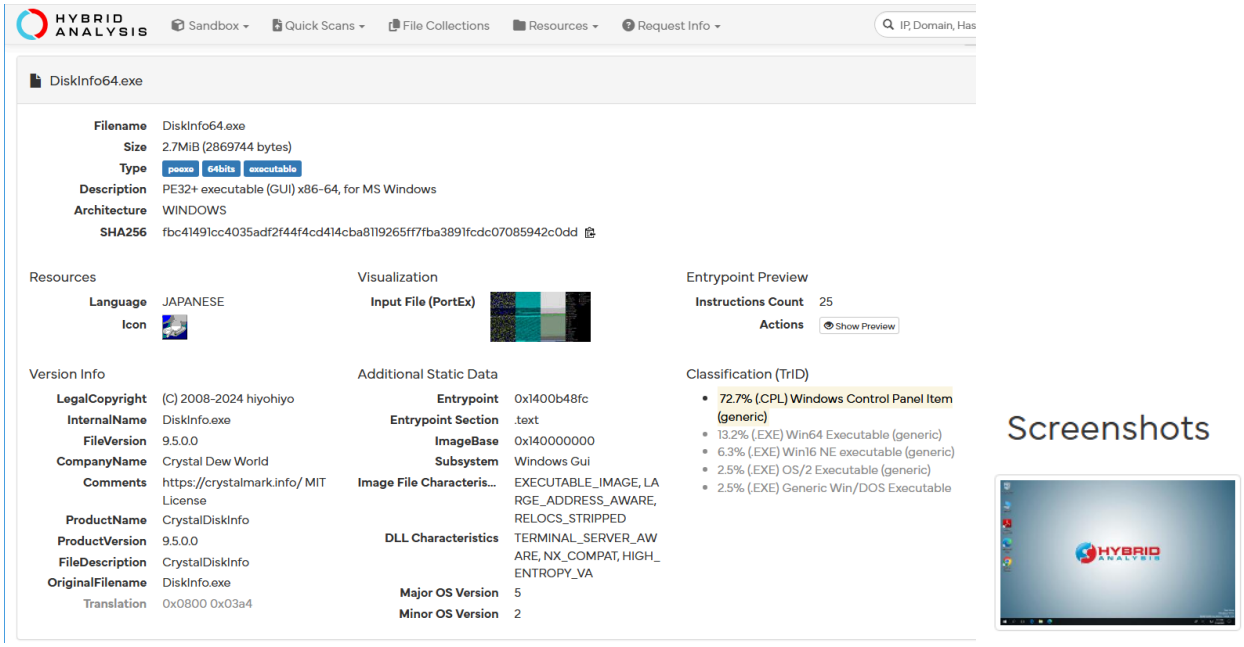
Ho utilizzato Hybrid Analysis e il risultato della scansione mostra che non viene rilevato alcun pericolo specifico a seguito dell'esecuzione del programma.

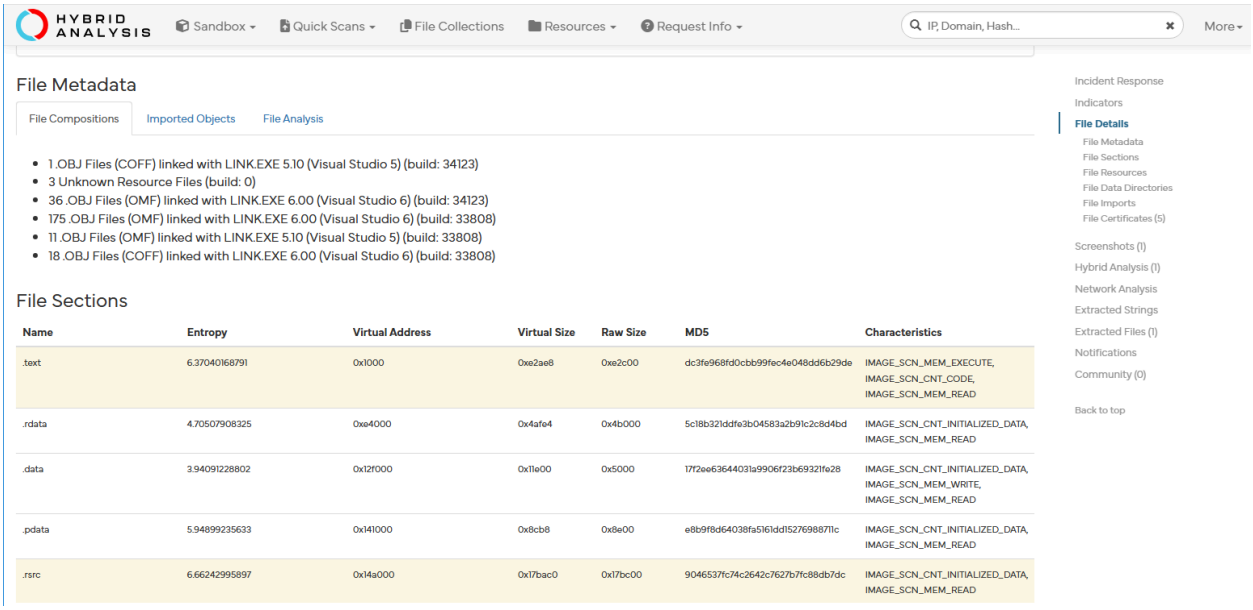


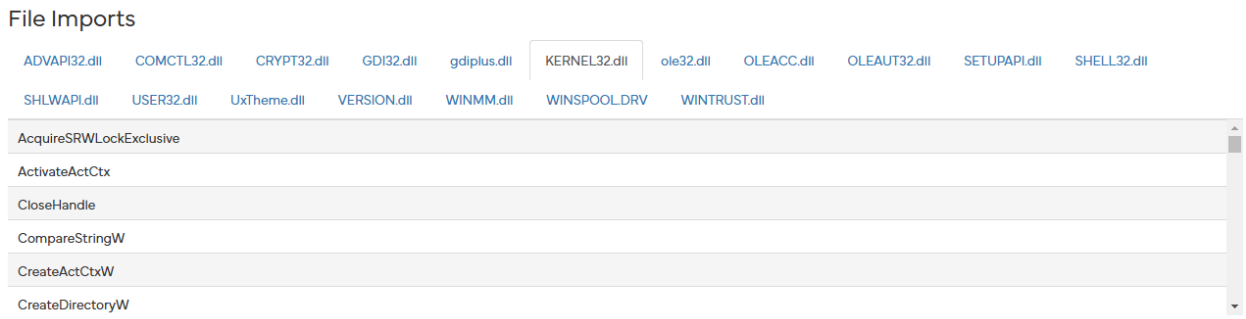
Vengono inoltre mostrate ulteriori informazioni sul nome originale del file caricato e le precedenti scansioni effettuate da altri utenti dello stesso programma (verifica tramite codice hash).



Analizzando approfonditamente i risultati vengono mostrate tutte le informazioni che abbiamo già precedentemente studiato (file e librerie importate, metadata ecc) ma anche ulteriori informazioni come screenshot durante l'esecuzione,







Poiché il tool esegue il programma, riesce a trovare i file che vengono estratti. In questo caso, come avevamo già osservato, viene creato il file *DiskInfo.ini* su cui è possibile eseguire ulteriori ricerche.