
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

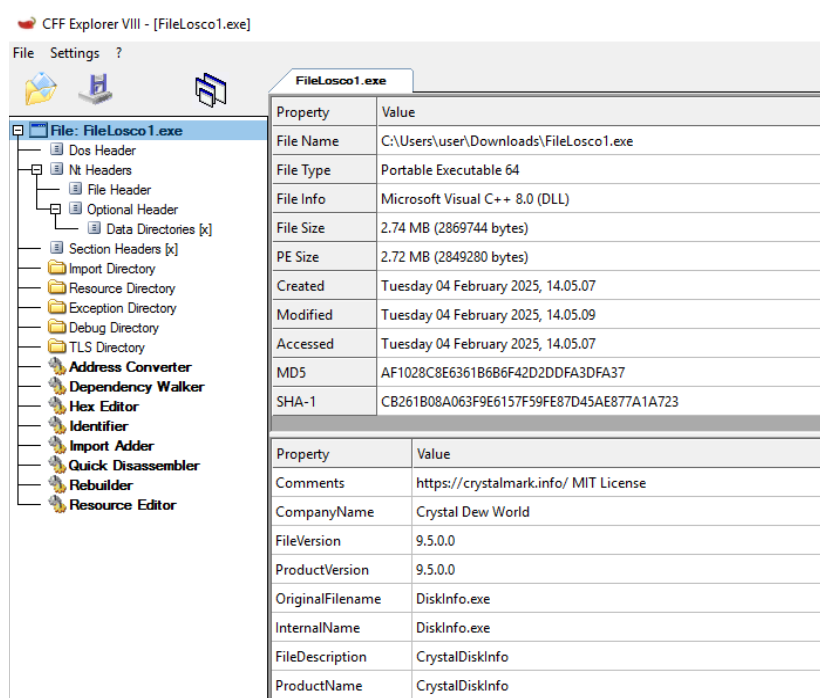
Ho svolto il laboratorio in una macchina virtuale Windows 10 in modo tale da avere un ambiente sicuro ed isolato in cui analizzare il file della consegna.

Analisi statica

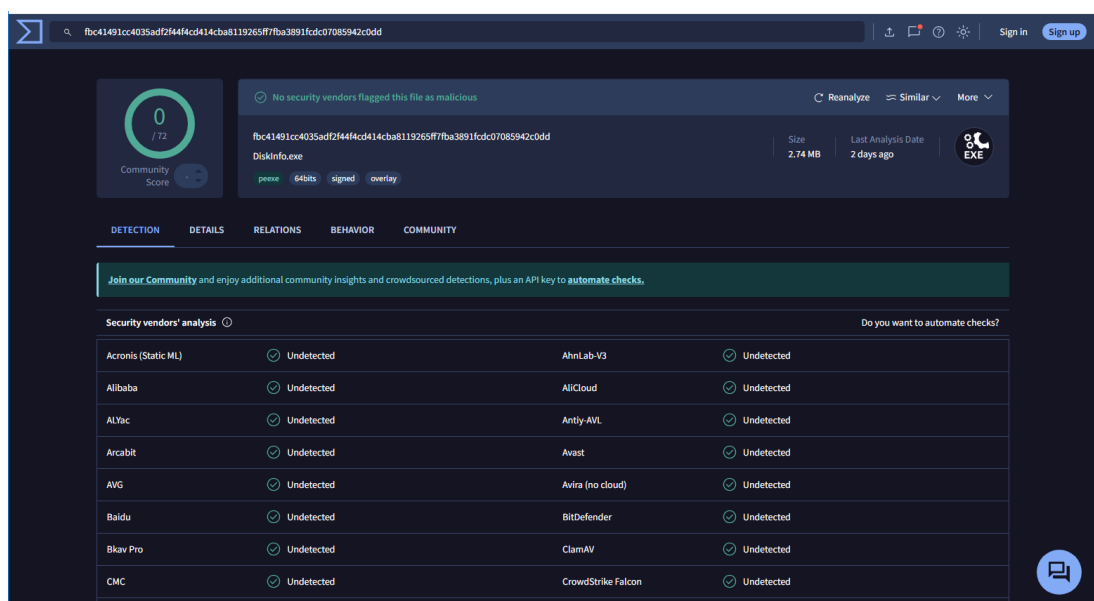
Dopo aver scaricato il sospetto malware, ho effettuato un'analisi statica tramite il software *CFF explorer*. In questo modo è possibile comprendere la struttura e il funzionamento del programma ancor prima di eseguirlo.

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.

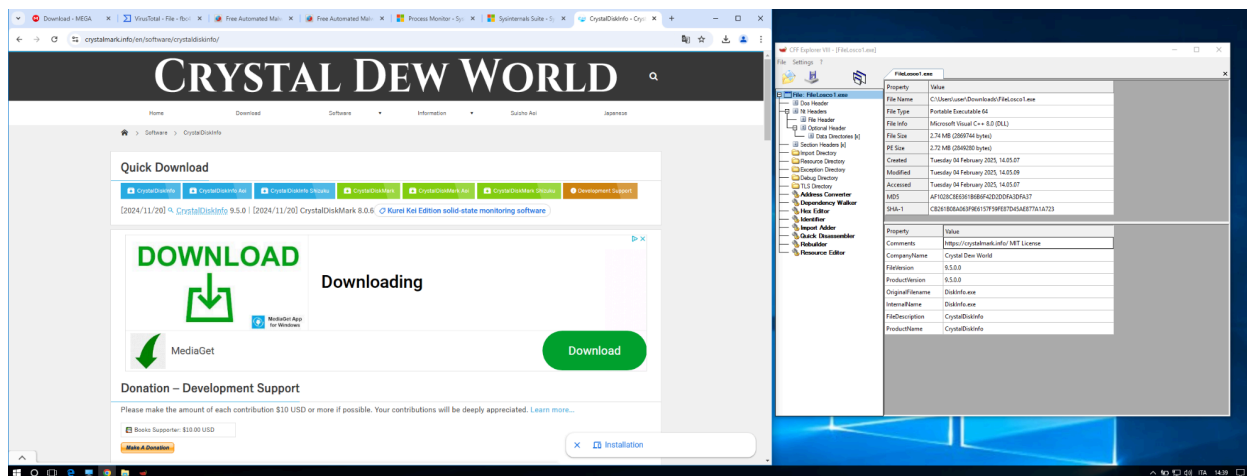
Come mostrato nello screen sono anche presenti informazioni sul file originale come il nome (**DiskInfo.exe**), la versione software e la casa produttrice.



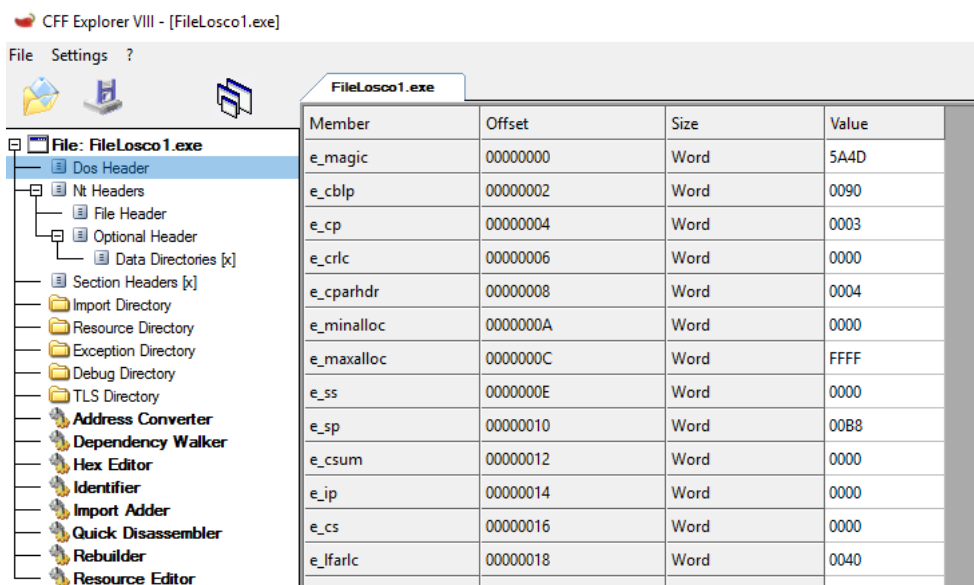
Ho utilizzato il codice hash SHA-1 per effettuare una verifica tramite VirusTotal del file fornito. Il risultato mostra che tutti i motori di ricerca antivirus non individuano alcuna criticità



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.



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

CFF Explorer VIII - [FileLosco1.exe]

File Settings ?

FileLosco1.exe

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.

CFF Explorer VIII - [FileLosco1.exe]

File Settings ?

FileLosco1.exe

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

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

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

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

5

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

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: 0x7fff28c0000, Image Size: 0x26000
14:57:35,1941...	DllHost.exe	3268	Load Image	C:\Windows\System32\bcrypt.dll	SUCCESS	Image Base: 0x7fff8920000, Image Size: 0x2b000
14:57:35,1956...	DllHost.exe	3268	Load Image	C:\Windows\System32\userenv.dll	SUCCESS	Image Base: 0x7fff8130000, Image Size: 0x1f000
14:57:35,1958...	DllHost.exe	3268	Load Image	C:\Windows\System32\profapi.dll	SUCCESS	Image Base: 0x7fff89e0000, 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: 6888
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: 0xd1d000
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: 0x7ffff8f90000, 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: 0x7ffff5d0000, Image Size: 0x121000
14:57:35,2518...	FileLosco1.exe	5484	Load Image	C:\Windows\System32\winspool.drv	SUCCESS	Image Base: 0x7ffe7970000, 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.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

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: 0x7fff6c4d20000, Image Size: 0x41000
14:57:40,5254...	NOTEPAD EXE	3760	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffffc4e0000, Image Size: 0xd1d000
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: 0x7ffff5d0000, 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\oleaut32.dll	SUCCESS	Image Base: 0x7ffff9220000, Image Size: 0x5f000
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: 0x7ffff980000, Image Size: 0x6c000
14:57:40,5455...	NOTEPAD EXE	3760	Load Image	C:\Windows\System32\comdlg32.dll	SUCCESS	Image Base: 0x7ffff720000, Image Size: 0xfda000
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: 0x7ffffd00000, 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

Showing 445 of 149,004 events (0.2%)

Backed by virtual memory

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

Time of Day	Process Name	PID	Operation	Path	Result	Detail
14:57:40.8255	explorer.exe	2176	ReadFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	Offset: 2,812, Length: 128
14:57:40.8255	explorer.exe	2176	ReadFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	Offset: 3,040, Length: 2
14:57:40.8255	explorer.exe	2176	ReadFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	Offset: 3,042, Length: 72
14:57:40.8255	explorer.exe	2176	ReadFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	Offset: 3,114, Length: 4
14:57:40.8256	explorer.exe	2176	UnlinkFileSingle	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	Offset: 2,147,483,540, Length: 1
14:57:40.8256	explorer.exe	2176	UnlinkFileSingle	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	Offset: 2,147,483,541, Length: 1
14:57:40.8256	explorer.exe	2176	CloseFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	
14:57:40.8257	explorer.exe	1712	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository\Machine and	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
14:57:40.8259	explorer.exe	1712	UnlinkFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository\Machine and	SUCCESS	AllocationSize: 2,359,296, EndOfFile: 2,359,296, NumberOfLinks: 1, DeletePending: False, Directory: False
14:57:40.8271	explorer.exe	2176	CreateFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\9b0c0d9c1c2442b customDestinations.ms	NAME COLLISION	Offset: 123, Length: 1
14:57:40.8272	explorer.exe	2176	UnlinkFileSingle	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\9b0c0d9c1c2442b customDestinations.ms	SUCCESS	Desired Access: Read Data, List Directory, Synchronize, Disposition: Create, Options: Directory, Synchronous
14:57:40.8273	explorer.exe	2176	UnlinkFileSingle	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: 0x00000000
14:57:40.8274	explorer.exe	2176	CloseFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	Offset: 2,147,483,539, Length: 1
14:57:40.8353	explorer.exe	2176	CloseFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b0c0d9c1c2442b automaticDestinations.ms	SUCCESS	Offset: 2,147,483,540, Length: 1
14:57:40.8354	explorer.exe	2176	QueryFileInformationFile	C:\Windows\explorer.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: CreationTime: 16072016 12:42:40, LastAccessTime: 16072016 12:42:40, LastWriteTime: 16072016 12:42:40
14:57:40.8354	explorer.exe	2176	CloseFile	C:\Windows\explorer.exe	SUCCESS	
14:57:40.8443	explorer.exe	1712	WriteFile	C:\Users\User\AppData\Local\Temp\DiskInfo.ini	SUCCESS	Offset: 1,987,728, Length: 4,096, IO Flags: Write Through, Priority: Normal
14:57:40.8522	explorer.exe	2176	CreateFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Non-Directory File, Open Requiring Optlock, Disal
14:57:40.8547	explorer.exe	2176	QueryFile	C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk	SUCCESS	
14:57:40.8552	explorer.exe	3760	QueryDirectory	C:\Users\User\Downloads\DiskInfo.ini	SUCCESS	Desired Access: Read Data, List Directory, Synchronize, Disposition: Open, Options: Directory, Synchroniz
14:57:40.8558	explorer.exe	3760	CloseFile	C:\Users\User\Downloads\DiskInfo.ini	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: DiskInfo.ini, 2, DiskInfo.ini
14:57:40.8562	explorer.exe	3760	CreateFile	C:\Users\User\Downloads\DiskInfo.ini	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Att
14:57:40.8562	explorer.exe	3760	QueryFileInformationVolume	C:\Users\User\Downloads\DiskInfo.ini	SUCCESS	CreationTime: 04/02/2025 14:57:35, VolumeSerialNumber: 4E57-7969, SupportsObjects: True, Volume
14:57:40.8563	explorer.exe	3760	QueryFileInformationFile	C:\Users\User\Downloads\DiskInfo.ini	BUFFER OVERFLOW	CreationTime: 04/02/2025 14:57:35, LastAccessTime: 04/02/2025 14:57:35, LastWriteTime: 04/02/2025 14:57:35
14:57:40.8570	explorer.exe	2176	QueryNameInformationFile	C:\Windows\System32\Notepad.exe	SUCCESS	Name: Windows\System32\Notepad.exe
14:57:40.8570	explorer.exe	3760	CreateFile	C:\Windows\System32\Notepad.exe	SUCCESS	Desired Access: Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Fi
14:57:40.8571	explorer.exe	3760	QuerySystemInformationVolume	C:\Windows	SUCCESS	TotalAllocationSize: 20,843,007, AvailableAllocationUnits: 17,884,500, SectorSizeAllocationUnit: 8, BytesPerB
14:57:40.8571	explorer.exe	3760	CloseFile	C:\Windows	SUCCESS	
14:57:40.8572	explorer.exe	1712	ReadFile	C:\Windows\System32\Windows.StateRepository.dll	SUCCESS	Offset: 158,672, Length: 4,096, IO Flags: Non-cached, Paging IO, Synchronous Paging IO, Priority: Normal
14:57:40.8582	explorer.exe	2176	FileSystemControl	C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk	CANCELLED	Control: FSCTL_REQUEST_OPLOCK
14:57:40.8582	explorer.exe	1712	ReadFile	C:\Windows\System32\Windows.StateRepository.dll	SUCCESS	Offset: 158,672, Length: 4,096, IO Flags: Non-cached, Paging IO, Synchronous Paging IO, Priority: Normal
14:57:40.8585	explorer.exe	2176	CreateFile	C:\Windows\System32\Notepad.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode
14:57:40.8587	explorer.exe	2176	QueryFileInformationFile	C:\Windows\System32\Notepad.exe	SUCCESS	CreationTime: 16072016 12:42:40, LastAccessTime: 16072016 12:42:40, LastWriteTime: 16072016 12:42:40
14:57:40.8587	explorer.exe	2176	CloseFile	C:\Windows\System32\Notepad.exe	SUCCESS	
14:57:40.8588	explorer.exe	2176	CreateFile	C:\Windows	SUCCESS	Desired Access: Read Data, List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous I
14:57:40.8588	explorer.exe	2176	QueryDirectory	C:\Windows	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: Windows, 2, Windows
14:57:40.8588	explorer.exe	2176	CreateFile	C:\Windows	SUCCESS	

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.

hybrid-analysis.com/sample/fbc41491cc035adf2f44f4cd414c8a8119265ff7fba3891fcd0c7085942c0dd

Analysis Overview

Submission name: DiskInfo64.exe
Size: 2.7MiB
Type: **posix 64bits executable**
Mime: application/x-dosexec
SHA256: fbc41491cc035adf2f44f4cd414c8a8119265ff7fba3891fcd0c7085942c0dd
Submitted At: 2024-11-22 12:41:14 (UTC)
Last Anti-Virus Scan: 2025-02-04 13:06:29 (UTC)
Last Sandbox Report: 2025-01-24 02:31:20 (UTC)

no specific threat
AV Detection: Marked as clean
Reactive

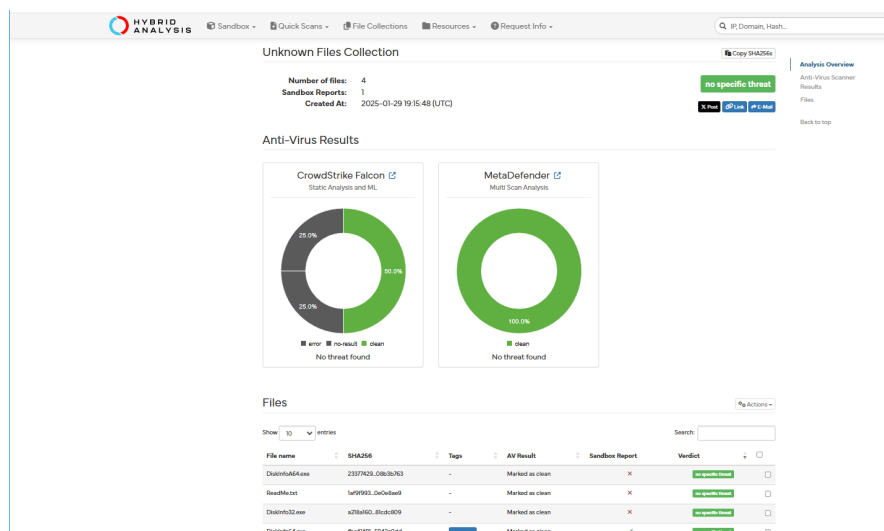
Anti-Virus Results

CrowdStrike Falcon: Static Analysis and ML. **Clean**
MetaDefender: Multi Scan Analysis. **Clean**

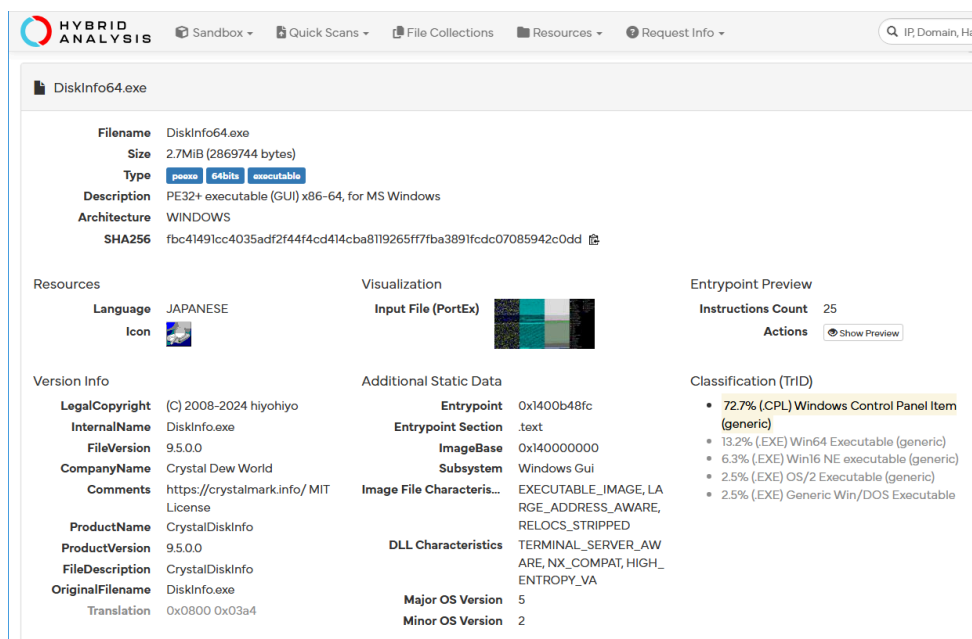
What customers are saying about CrowdStrike Falcon Endpoint Protection:
"The best product on the market for in term of balance in ease of use, functionality, and effectiveness. The interface is intuitive and well designed"
"Overall this has been a great product and one of the easiest deployments I've been through"

Access Gartner Peer Insights
Visit CrowdStrike Customer Page

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,



HYBRID ANALYSIS

Sandbox
Quick Scans
File Collections
Resources
Request Info

More

File Metadata

File Compositions
Imported Objects
File Analysis

- 1 OBJ Files (COFF) linked with LINK.EXE 5.10 (Visual Studio 5) (build: 34123)
- 3 Unknown Resource Files (build: 0)
- 36 OBJ Files (OMF) linked with LINK.EXE 6.00 (Visual Studio 6) (build: 34123)
- 175 OBJ Files (OMF) linked with LINK.EXE 6.00 (Visual Studio 6) (build: 33808)
- 11 OBJ Files (OMF) linked with LINK.EXE 5.10 (Visual Studio 5) (build: 33808)
- 18 OBJ Files (COFF) linked with LINK.EXE 6.00 (Visual Studio 6) (build: 33808)

File Sections

Name	Entropy	Virtual Address	Virtual Size	Raw Size	MD5	Characteristics
.text	6.37040168791	0x1000	0xe2ae8	0xe2c00	dc3fe968fd0cbb99fec4e048dd6b29de	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	4.70507908325	0xe4000	0x4afe4	0x4b000	5c18b321ddfe3b04583a2b91c2c8d4bd	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	3.94091228802	0x12f000	0x11e00	0x5000	172ee63644031a9906f23b69321fe28	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	5.94899235633	0x141000	0x8cb8	0x8e00	e8b9f8d64038fa5161dd1527698871c	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	6.66242995897	0x14a000	0x17bac0	0x17bc00	90465371c74c2642c7627b7fc88db7dc	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Incident Response
Indicators
File Details
File Metadata
File Sections
File Resources
File Data Directories
File Imports
File Certificates (5)
Screenshots (1)
Hybrid Analysis (1)
Network Analysis
Extracted Strings
Extracted Files (1)
Notifications
Community (0)
Back to top

File Imports

ADVAPI32.dll
COMCTL32.dll
CRYPT32.dll
GDI32.dll
gdiplus.dll
KERNEL32.dll
ole32.dll
OLEACC.dll
OLEAUT32.dll
SETUPAPI.dll
SHELL32.dll
SHLWAPI.dll
USER32.dll
UxTheme.dll
VERSION.dll
WINMM.dll
WINSPOOL.DRV
WINTRUST.dll

```

AcquireSRWLockExclusive
ActivateActCtx
CloseHandle
CompareStringW
CreateActCtxW
CreateDirectoryW

```

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.

Extracted Files

Informative Selection
1

DiskInfo.ini

Overview
Download Disabled
Hash Seen Before

Size

26B (26 bytes)

Type

text

Description

ASCII text, with CRLF line terminators

Runtime Process

DiskInfo64.exe (PID: 4772)

MD5

845cfadc36bf68dd7b619214675d5605

SHA1

e806406c94db7ff43bc87ebdb1b44acaaace4268

SHA256

c0c15dd2e792406d8e89b2f81d0fd635ec622d72db643cac3851dcabce6a3452