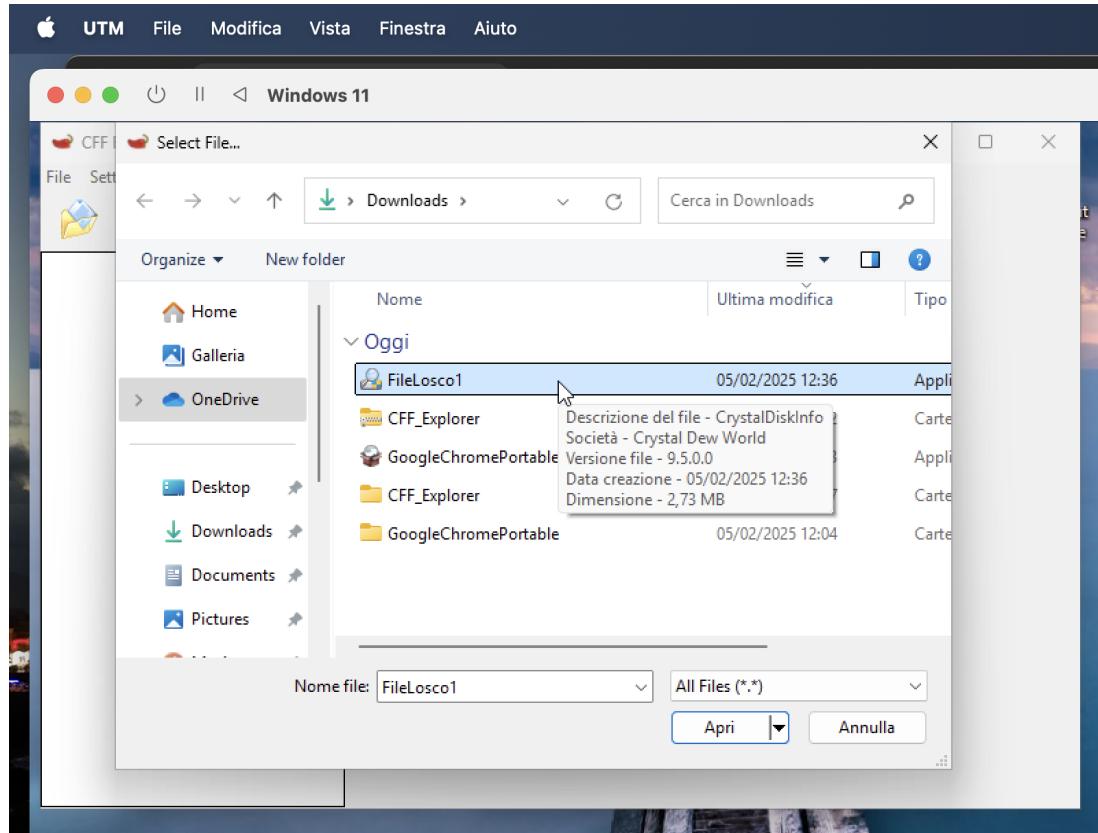


Nel esercizio di oggi è stato chiesto di eseguire le seguenti operazioni:

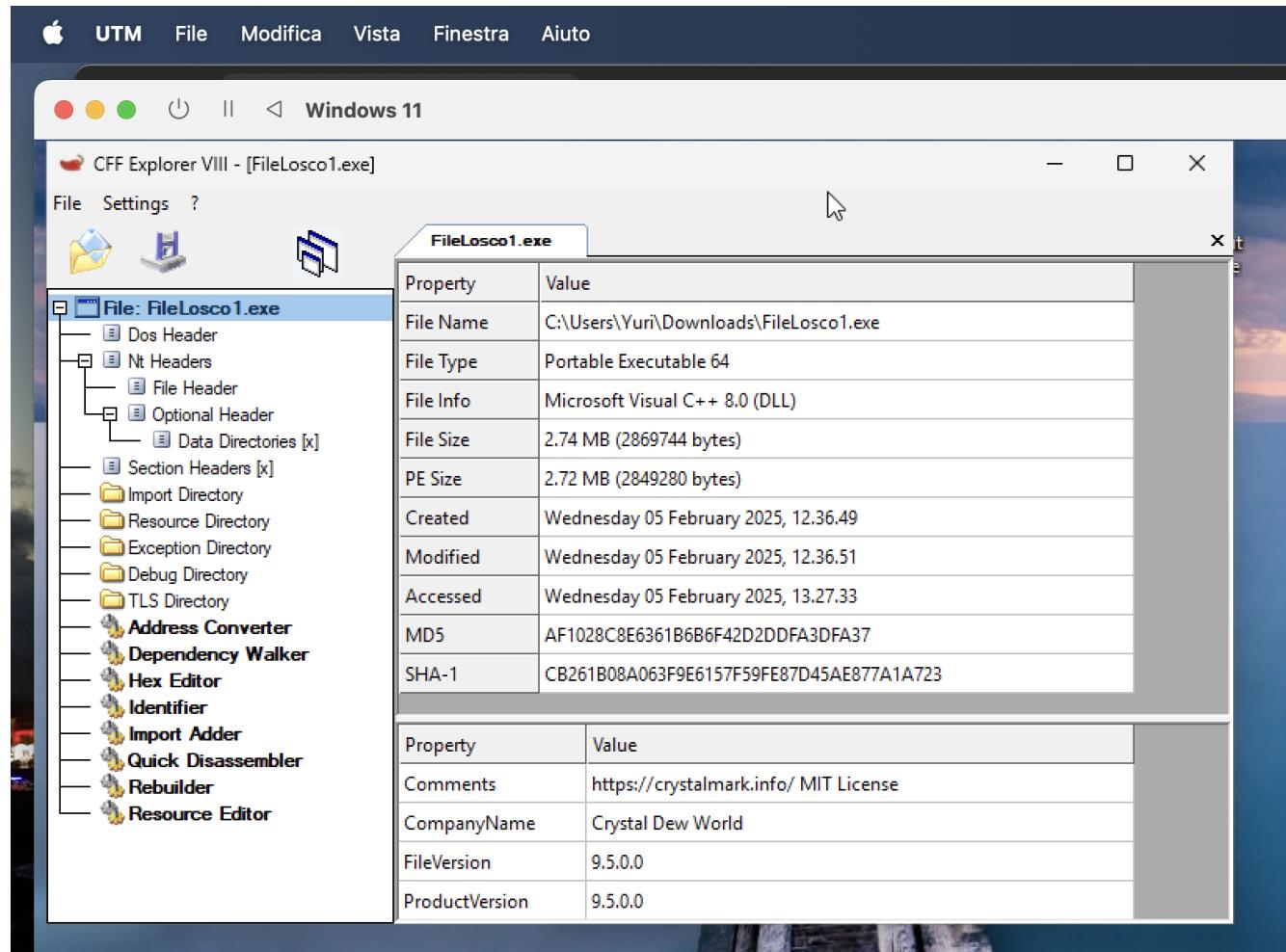
1. Analisi Statica: Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.

2. Analisi Dinamica: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

Su windows procediamo in questo modo, si scarica CFF Exploer per esaminare i dettagli del programma eseguito e successivamente si apre il file con cff, come mostrato nel immagine di seguito:



Una volta che è stato aperto il file in CFF Explorer, quest'ultimo permette di analizzare i file eseguibili mostrando l'**header PE**, le **sezioni di codice, dati e risorse**, la **Import Table** con le DLL e funzioni usate, la **Export Table** con le funzioni esportate, e offre strumenti per la **modifica e il reverse engineering**.



Ora apriamo il file **losco.exe** e andiamo nel programma **Procmon64**; se tutto è andato bene, noteremo che il risultato è il **SUCCESS**, confermando che l'analisi sta funzionando correttamente.

Time ...	Process Name	PID	Operation	Path	Result	Detail
14:01:...	Procmon64a.exe	12164	QueryBasicInfor...	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	CreationTime: 12/0...
14:01:...	Procmon64a.exe	12164	CloseFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	
14:01:...	Procmon64a.exe	12164	CreateFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Desired Access: G...
14:01:...	Procmon64a.exe	12164	CreateFileMapp...	C:\Windows\System32\IPHLPAPI.DLL	FILE LOCKED WI...	SyncType: SyncTy...
14:01:...	Procmon64a.exe	12164	CreateFileMapp...	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	SyncType: SyncTy...
14:01:...	SetupHost.Exe	1468	CreateFile	C:\\$WINDOWS.~BT\NewOS\Window...	NAME NOT FOUND	Desired Access: R...
14:01:...	Procmon64a.exe	12164	CloseFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	
14:01:...	Procmon64a.exe	12164	RegOpenKey	HKEY_LOCAL_MACHINE\Software\Microsoft\LanguageO...	SUCCESS	Desired Access: R...
14:01:...	Procmon64a.exe	12164	RegQueryValue	HKEY_LOCAL_MACHINE\Software\Microsoft\LanguageO...	SUCCESS	Type: REG_DWO...
14:01:...	Procmon64a.exe	12164	RegQueryValue	HKEY_LOCAL_MACHINE\Software\Microsoft\LanguageO...	SUCCESS	Type: REG_SZ, Le...
14:01:...	Procmon64a.exe	12164	RegCloseKey	HKEY_LOCAL_MACHINE\Software\Microsoft\LanguageO...	SUCCESS	
14:01:...	Procmon64a.exe	12164	CreateFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Desired Access: R...
14:01:...	Procmon64a.exe	12164	CreateFileMapp...	C:\Program Files\WindowsApps\Micros...	FILE LOCKED WI...	SyncType: SyncTy...
14:01:...	Procmon64a.exe	12164	QueryStandardI...	C:\Program Files\WindowsApps\Micros...	SUCCESS	AllocationSize: 12...
14:01:...	Procmon64a.exe	12164	CreateFileMapp...	C:\Program Files\WindowsApps\Micros...	SUCCESS	SyncType: SyncTy...
14:01:...	Procmon64a.exe	12164	CloseFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	
14:01:...	SetupHost.Exe	1468	CreateFile	C:\\$WINDOWS.~BT\NewOS\Window...	NAME NOT FOUND	Desired Access: R...
14:01:...	svchost.exe	2032	CreateFile	C:\Windows\Prefetch\FILELOSCO1.EX...	NAME NOT FOUND	Desired Access: R...
14:01:...	Procmon64a.exe	12164	CreateFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Desired Access: R...
14:01:...	SetupHost.Exe	1468	CreateFile	C:\\$WINDOWS.~BT\NewOS\Window...	SUCCESS	Desired Access: G...
14:01:...	Procmon64a.exe	12164	QueryBasicInfor...	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	CreationTime: 12/0...
14:01:...	Procmon64a.exe	12164	CloseFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	
14:01:...	svchost.exe	2032	CreateFile	C:\Windows\Prefetch\FILELOSCO1.EX...	SUCCESS	Desired Access: G...
14:01:...	Procmon64a.exe	12164	CreateFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Desired Access: G...
14:01:...	Procmon64a.exe	12164	CreateFileMapp...	C:\Windows\System32\IPHLPAPI.DLL	FILE LOCKED WI...	SyncType: SyncTy...
14:01:...	Procmon64a.exe	12164	CreateFileMapp...	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	SyncType: SyncTy...