REPORT S9/L2

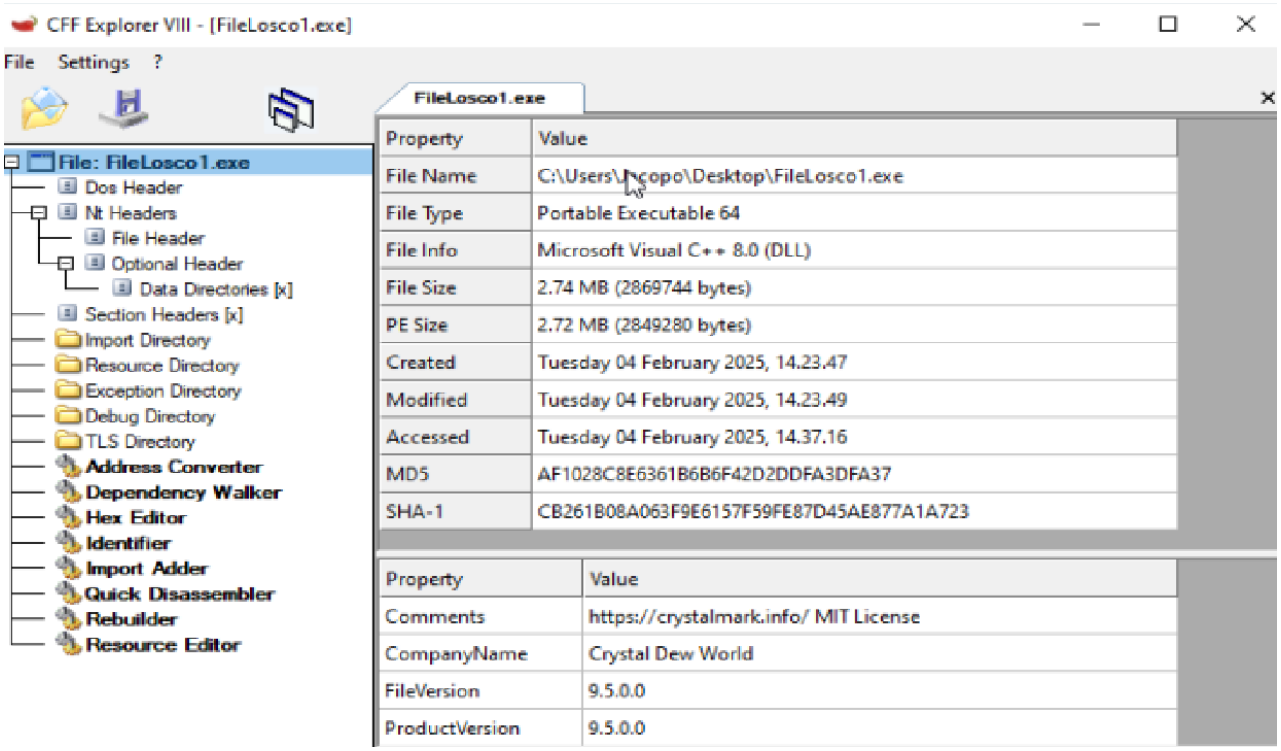
Lo scopo dell' esercizio è quello di analizzare un malware relativamente innocuo:

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.

ANALISI STATICA

Dopo aver avviato la macchina virtuale di Windows 10 posso procedere con l' ***analisi statica*** del malware, **filelosco.** Mediante il software di analisi ***CFF EXPLORER VIII.***



Carico quindi il malware e procedo con l' anlisi. Dalla prima schermata abbiamo modo di raccogliere delle informazioni base sull' eseguibile.

- ***File name:*** contiene il percorso del file, in questo caso il file è nel Desktop.
- ***File type:*** indica il tipo, nello specifico Portable Executable.
- ***File Info:*** in questo caso indica che la dll in questione è compilata con visual c++.
- ***Pe size*****:** indica la dimensione.
- ***MD5:*** L' hash del file, usato per identificare univocamente il file e verificarne l' integrità
- ***SHA-1:*** un altro identificatore univoco del file piu resistente alle collisioni.

Nella sezione ***DOS Header*** è fondamentale notare la presenza della firma ***MZ*** che certifica che il file sia eseguibile su ***windows***, ovviamente non certifica il fatto che non si tratti di malware.

Approfondisco ora l' analisi accedendo alla sezione IMPORT DIRECTORY, in questo caso nella sezione KERNEL32 vengono importate 172 funzioni, se procedo nell' analisi vedo come siano presenti delle funzioni anomale, quali WriteFile, DeleteFileW, CreateFIleW.

000000000012CD64	000000000012CD64	0258	GetExitCodeProcess
000000000012CD4E	000000000012CD4E	0610	WaitForSingleObject
000000000012CD3E	000000000012CD3E	0319	GetTempPathW
000000000012CD32	000000000012CD32	064B	WriteFile
000000000012CD24	000000000012CD24	0128	DeleteFileW
000000000012CD16	000000000012CD16	00DA	CreateFileW
000000000012CCFE	000000000012CCFE	02C4	GetPrivateProfileIntW
000000000012CCE8	000000000012CCE8	0291	GetModuleFileNameW
000000000012CCF0	000000000012CCF0	05B4	Sleep

Discorso analogo nella sezione ADVAPI32, nello specifico in questo caso vengono importate 24 funzione, ma come in precedenza noto delle funzioni anomale che vanno ad agire sulle chiavi registro, RegCreateKeyExW, RegDeleteValueW, RegSetValue.

000000000012E458	000000000012E458	025A	RegCreateKeyExW
000000000012E46A	000000000012E46A	0269	RegDeleteValueW
000000000012E47C	000000000012E47C	029F	RegSetValueExW
000000000012E48E	000000000012E48E	0282	RegOpenKeyExW
000000000012E49E	000000000012E49E	028F	RegQueryValueExW

In sostanza quindi noto sicuramente che nelle sezioni ***Kernel32*** e ***User32*** vi è un numero insolitamente alto di importazioni a questo aggiungo l' evidenza di funzioni come ***createfile***, ***deletefile***, ***setvalue*** e ***createkey***, l' insieme di questi elementi mi fanno sospettare con ragionevole sicurezza di essere in presenza di un malware.

ANALISI DINAMICA

Mentre nel caso precedente mi sono soffermato ad analizzare l' eseguibile in questo caso procedo con l' esecuzione dello stesso, con lo scopo di andare a monitorare gli IOC per notare eventuali cambiamenti. In questo caso andrò a monitorare, le attività del registro, il file system e la rete mediante il software ProcessMonitor, dopo averlo avviato procedo quindi ad avviare il malware.

Mi focalizzo in primis sui registri e noto come anche in questo caso siano presenti delle operazioni di RegSetValue, inoltre noto come

Nella sezione SystemFile sono presenti operazioni di creazioni e eliminazioni file, altro elemento che mi conferma la poca bontà del file.

Time ...	Process Name	PID	Operation	Path
15:06:...	Explorer.EXE	4372	ReadFile	C:\Windows\System32\UIAnimation.dll
15:06:...	svchost.exe	1808	ReadFile	C:\Windows\System32\StateRepository.Core.dll
15:06:...	svchost.exe	1808	ReadFile	C:\Windows\System32\StateRepository.Core.dll
15:06:...	MsMpEng.exe	2512	CreateFile	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	FileSystemControl	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	FileSystemControl	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	CloseFile	C:\Windows\System32\ucrtbase.dll
15:06:...	svchost.exe	1808	ReadFile	C:\Windows\System32\StateRepository.Core.dll
15:06:...	MsMpEng.exe	2512	CreateFile	C:\Windows\System32\shlwapi.dll
15:06:...	MsMpEng.exe	2512	FileSystemControl	C:\Windows\System32\shlwapi.dll
15:06:...	MsMpEng.exe	2512	FileSystemControl	C:\Windows\System32\shlwapi.dll
15:06:...	MsMpEng.exe	2512	CloseFile	C:\Windows\System32\shlwapi.dll
15:06:...	MsMpEng.exe	2512	CreateFile	C:\Windows\System32\advapi32.dll
15:06:...	MsMpEng.exe	2512	FileSystemControl	C:\Windows\System32\advapi32.dll
15:06:...	MsMpEng.exe	2512	FileSystemControl	C:\Windows\System32\advapi32.dll
15:06:...	MsMpEng.exe	2512	CloseFile	C:\Windows\System32\advapi32.dll
15:06:...	svchost.exe	1808	ReadFile	C:\Windows\System32\Windows.StateRepository.dll
15:06:...	MsMpEng.exe	2512	CreateFile	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	QueryInformationVolume	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	QueryAllInformationFile	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	QueryInformationVolume	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	QueryAllInformationFile	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	FileSystemControl	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	QueryIdInformation	C:\Windows\System32\ucrtbase.dll
15:06:...	MsMpEng.exe	2512	CloseFile	C:\Windows\System32\ucrtbase.dll

Nella sezione rete infine ho la conferma che non si tratti di un file benevolo, qui infatti sono presenti ripetute operazioni di ***TCP Connect e Udp Send/Receive***,

15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:63949 -> fd00::3:domain
15:06:...	svchost.exe	1844	UDP Receive	DESKTOP-I0VLN1F.Home:58824 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Receive	DESKTOP-I0VLN1F.Home:63949 -> fd00::3:domain
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:64599 -> 10.0.2.3:domain
15:06:...	MsMpEng.exe	2512	TCP Reconnect	DESKTOP-I0VLN1F.Home:50122 -> 20.31.61.205:https
15:06:...	svchost.exe	1844	UDP Receive	DESKTOP-I0VLN1F.Home:64599 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:58552 -> ff02::1:3:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:58552 -> 224.0.0.252:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:58552 -> ff02::1:3:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:58552 -> 224.0.0.252:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:53595 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Receive	DESKTOP-I0VLN1F.Home:53595 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:57939 -> ff02::1:3:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:57939 -> 224.0.0.252:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:57939 -> ff02::1:3:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:57939 -> 224.0.0.252:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:64872 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Receive	DESKTOP-I0VLN1F.Home:64872 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:62068 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:61363 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:62068 -> fd00::3:domain
15:06:...	svchost.exe	1844	UDP Receive	DESKTOP-I0VLN1F.Home:62068 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:60100 -> ff02::1:3:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:60100 -> 224.0.0.252:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:60100 -> ff02::1:3:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:60100 -> 224.0.0.252:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:61363 -> fd00::3:domain
15:06:...	svchost.exe	1844	UDP Receive	DESKTOP-I0VLN1F.Home:61363 -> 10.0.2.3:domain
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:53895 -> ff02::1:3:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:53895 -> 224.0.0.252:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:53895 -> ff02::1:3:llmnr
15:06:...	svchost.exe	1844	UDP Send	DESKTOP-I0VLN1F.Home:53895 -> 224.0.0.252:llmnr
15:06:...	MsMpEng.exe	2512	TCP Reconnect	DESKTOP-I0VLN1F.Home:50122 -> 20.31.61.205:https

Sono presenti anche in questo caso quindi tutti gli elementi per confermarmi di essere in presenza di un file malevolo.