Attività di Analisi del Malware

04/02/2025

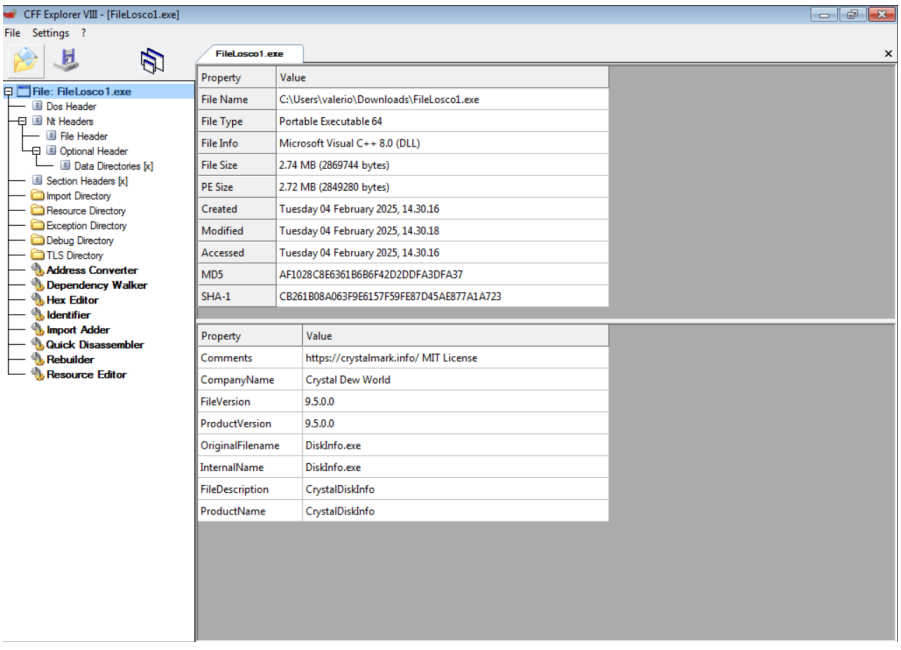
TRACCIA

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

Per prima cosa apriamo il file con CFF_Explorer per esaminare il codice del malware con l'analisi statica:



L'analisi statica è una tecnica di analisi del malware che consiste nell'esaminare il codice di un programma senza eseguirlo.

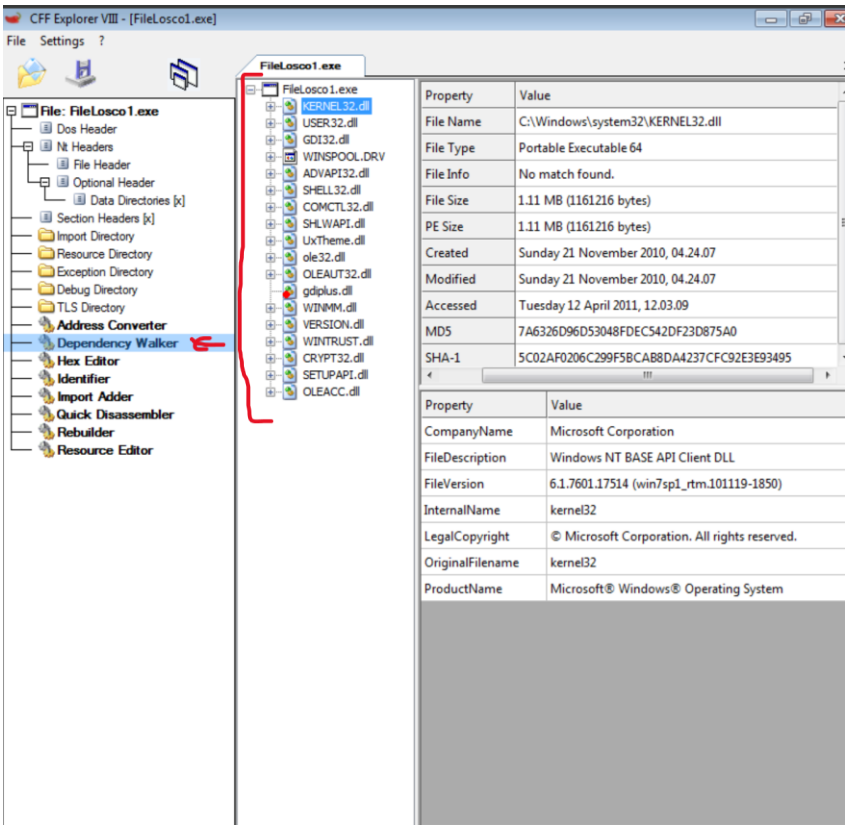
Pro dell'Analisi Statica

1. **Sicurezza**: Poiché il malware non viene eseguito, non c'è rischio di infezione o di danni al sistema di analisi.
2. **Completezza**: L'analisi statica permette di esaminare tutte le parti del codice, comprese quelle che potrebbero non essere eseguite in un ambiente dinamico.
3. **Velocità**: Può essere più rapida rispetto all'analisi dinamica, poiché non richiede l'esecuzione del malware e l'osservazione del suo comportamento nel tempo.
4. **Individuazione di Vulnerabilità**: Può aiutare a identificare vulnerabilità nel codice che potrebbero essere sfruttati da altri malware.

Contro dell'Analisi Statica

1. **Limitazioni nell'Interpretazione**: Non può rilevare comportamenti dinamici che si verificano solo durante l'esecuzione, come la decrittazione di codice o il carico dinamico di librerie.
2. **Offuscamento del Codice**: Malware sofisticato può usare tecniche di offuscamento e di crittografia che rendono difficile o impossibile l'analisi statica completa.
3. **Tempo e Risorse**: In alcuni casi, l'analisi statica può richiedere molto tempo e risorse se il malware è molto complesso o offuscato.
4. **Conoscenza Tecnica**: Richiede una conoscenza approfondita dell'architettura del codice e delle tecniche di offuscamento per essere efficace.
5. **Falsi Positivi**: Potrebbe identificare comportamenti sospetti che non sono effettivamente malevoli, causando falsi allarmi.

Andiamo nella sezione “Dependency Walker”; essa elenca tutte le librerie (DLL) dalle quali il file eseguibile dipende, cioè le librerie che deve caricare per funzionare correttamente.



Possiamo notare come il file dipenda, tra le tante, dalle librerie: KERNEL32.DLL, USER32.DLL, GDI32.DLL, ADVAPI32.DLL, SHELL32.DLL, COMCTL32.DLL, OLE32.DLL

Alcuni dettagli su queste librerie:

1. **KERNEL32.dll:** Fornisce funzioni fondamentali per la gestione dei processi, memoria, file e altre operazioni di sistema.
2. **USER32.dll:** Contiene funzioni per la gestione dell'interfaccia utente, come finestre, messaggi di sistema e input da tastiera e mouse.
3. GDI32.dll: Fornisce funzioni grafiche per il disegno di testo e grafica.
4. ADVAPI32.dll: Contiene funzioni avanzate per la gestione della sicurezza, il registro di sistema e i servizi di Windows.
5. **SHELL32.dll**: Include funzioni per l'interazione con il sistema operativo e il file system, come l'accesso a cartelle e operazioni di shell.

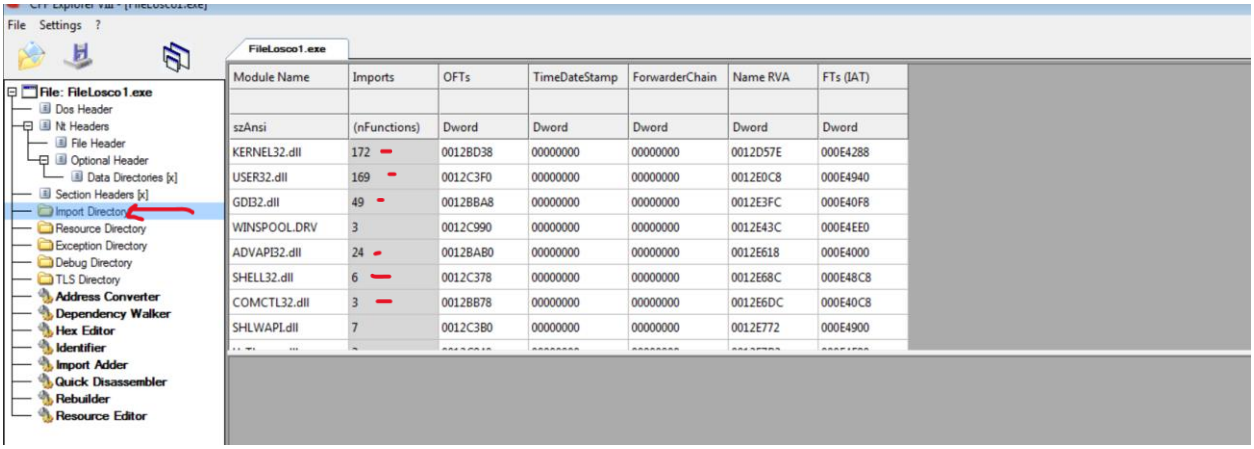
6. **COMCTL32.dll:** Fornisce controlli comuni dell'interfaccia utente, come toolbar, progress bar e altre componenti GUI.
7. **Ole32.dll**: Supporta l'Object Linking and Embedding (OLE), utilizzato per la gestione dei contenuti composti di applicazioni.

- KERNEL32.dll e USER32.dll sono critiche per il funzionamento del malware poiché forniscono accesso a funzioni di sistema fondamentali.
- ADVAPI32.dll indica che il malware potrebbe interagire con il registro di Windows, servizi di sistema e funzioni di sicurezza.
- SHELL32.dll e COMCTL32.dll suggeriscono che il malware potrebbe avere componenti di interfaccia utente o interagire con il filesystem di Windows.

Tra le Funzioni Comuni Importate dai Malware in queste librerie troviamo:

- **Creazione di processi**: Funzioni come CreateProcess da KERNEL32.dll.
- **Lettura/scrittura file**: Funzioni come ReadFile e WriteFile da KERNEL32.dll.
- **Accesso al registro di sistema**: Funzioni come RegOpenKeyEx da ADVAPI32.dll.
- **Interazione con l'interfaccia utente**: Funzioni come SendMessage e GetAsyncKeyState da USER32.dll.

Andiamo in import Directory per analizzare i moduli e verifichiamo la presenza di queste funzioni comuni dentro di essi:



Un numero insolitamente alto di importazioni, o l'importazione di funzioni che manipolano direttamente la sicurezza del sistema, i file, o le comunicazioni di rete, possono segnalare comportamenti potenzialmente dannosi o sospetti. Ad esempio, se un file eseguibile importa funzioni che permettono di modificare il registro di sistema, di avviare processi o di ascoltare connessioni di rete, questi possono essere segnali che il file è parte di un malware o di un software potenzialmente indesiderato. Tuttavia, è importante considerare il contesto generale dell'applicazione e il suo scopo previsto prima di trarre conclusioni definitive.

000000000012CD7A	000000000012CD7A	00F6	CreateProcessW

La funzione CreateProcess è spesso utilizzata nei malware per avviare nuovi processi o eseguire codice arbitrario. I malware possono sfruttare questa funzione per eseguire codice dannoso, avviare servizi o eseguire comandi di sistema.

000000000012CD32	000000000012CD32	064B	WriteFile

I malware spesso utilizzano la funzione WriteFile per creare o modificare file su un sistema infettato. Questa funzione consente al malware di scrivere dati su un file aperto, il che può includere la creazione di nuovi file, la modifica di file esistenti o l'aggiunta di codice dannoso a file legittimi.

000000000012CD16	000000000012CD16	00DA	CreateFileW

I malware spesso utilizzano la funzione CreateFile per creare nuovi file su un sistema infettato. Questa funzione consente al malware di aprire o creare file, inclusi file di testo, eseguibili, o altri tipi di file che possono essere utilizzati per diffondere il malware o eseguire codice dannoso.

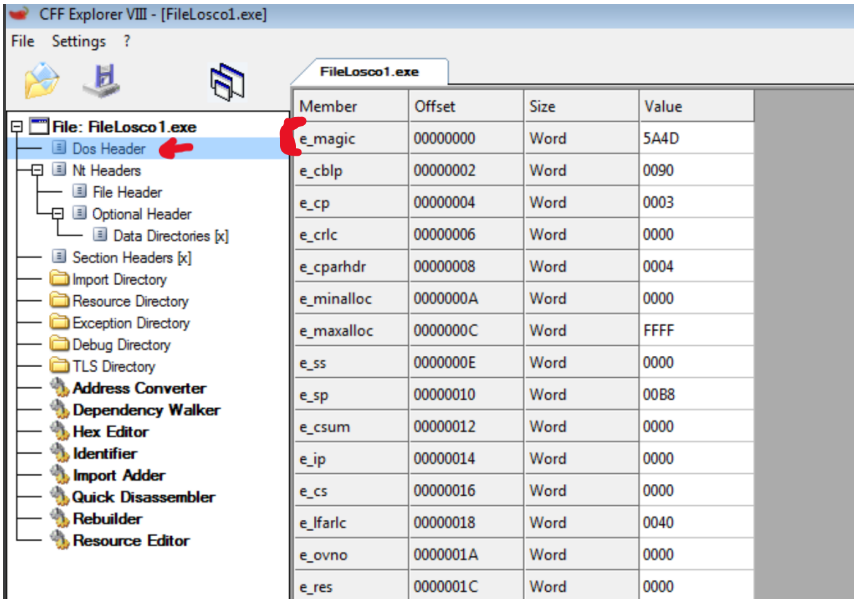
000000000012E48E	000000000012E48E	0282	RegOpenKeyExW

La funzione RegOpenKeyEx è spesso utilizzata dai malware per accedere e modificare le chiavi di registro di Windows. Questo permette al malware di ottenere persistenza, cioè di rimanere attivo anche dopo riavvii del sistema.

000000000012D5EC	000000000012D5EC	031B	SendMessageW

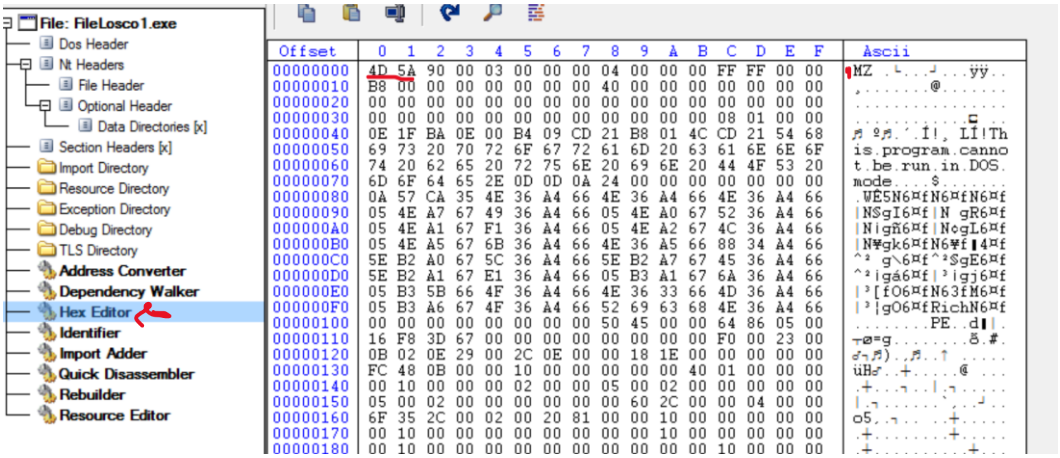
La funzione "send message" nei malware è utilizzata per distribuire messaggi dannosi tramite SMS o altri canali di comunicazione. Questa funzione può essere parte di uno script o di un programma che invia messaggi di phishing o spam per rubare informazioni personali o finanziarie.

Andando nel DOS header invece possiamo trovare la firma ‘MZ’; La firma "MZ" nei file eseguibili di Windows è un identificatore cruciale, utilizzato per denotare che un file è effettivamente un eseguibile. Questi due caratteri corrispondono agli ASCII delle lettere "M" e "Z" e sono posti all'inizio di ogni file eseguibile in formato PE (ortable Executable), che include i file .EXE, .DLL e altri tipi di file eseguibili in ambiente Windows.

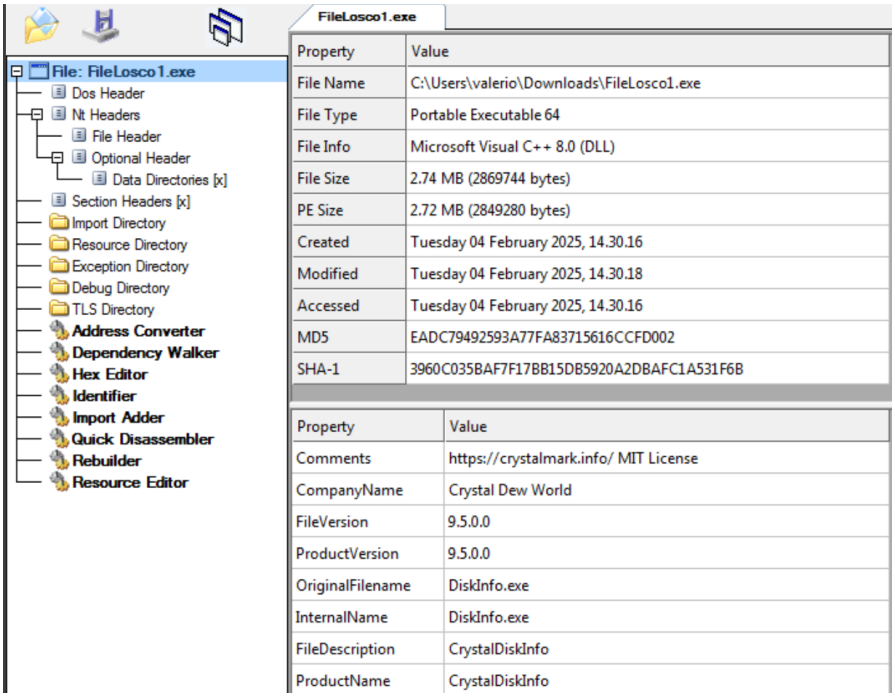


La troviamo sotto il nome di e_magic, Questo è il campo di firma del DOS Header. Il valore 5A4D corrisponde alle lettere "MZ" in ASCII.

Possiamo verificarlo andando su Hex Editor:



Nella prima sezione (file:...) possiamo vedere diverse informazioni quali il nome del file, il tipo, info, dimensioni, data creazione e data modifica del file, funzione crittografica MD-5 e l'algoritmo di SHA.



Property	Value
File Name	C:\Users\valerio\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, 14.30.16
Modified	Tuesday 04 February 2025, 14.30.18
Accessed	Tuesday 04 February 2025, 14.30.16
MD5	EADC79492593A77FA83715616CCFD002
SHA-1	3960C035BAF7F17BB15DB5920A2DBAFC1A531F6B

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