Analisi del Malware notepad-classico.exe: con CFF Explorer

Profilo studente

data:03/02/2026
studente: Gabriel Giustinelli 15/06/2004
Epicode classe: CS0525
Cyber Security Specialist

progetto

Il progetto consiste nell'analisi tecnica dell'eseguibile `notepad-classico.exe` per verificarne l'integrità e identificare potenziali comportamenti malevoli. Nonostante il file si presenti con l'icona e i metadati del legittimo Blocco Note di Windows, l'indagine mira a scovare anomalie strutturali.

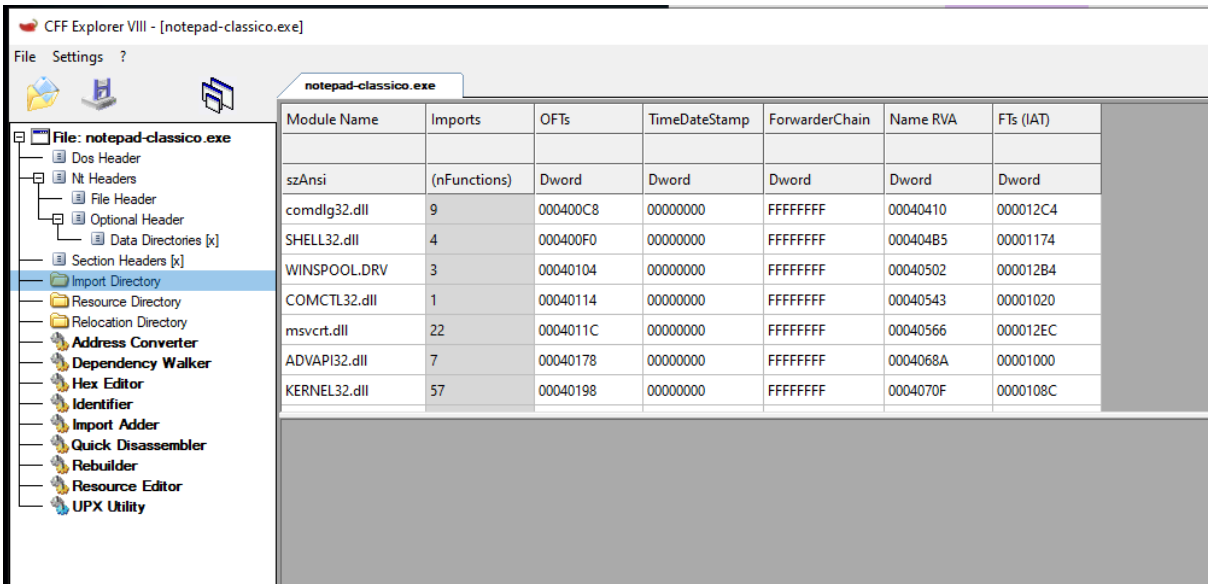
L'analisi è stata condotta tramite il software **CFF Explorer**, esaminando le librerie dinamiche (DLL) importate e la configurazione delle sezioni interne del file (sezioni PE) per determinare se il software originale sia stato alterato con l'inserimento di codice dannoso.

1. Librerie Importate (Imports)

L'analisi della *Import Directory* ha rivelato l'utilizzo di diverse librerie dinamiche (DLL). Di seguito sono elencate le principali con la relativa descrizione tecnica:

- **KERNEL32.dll**: Fornisce le API core di Windows per la gestione della memoria, dei processi e dei thread, oltre all'accesso fondamentale al file system.
- **ADVAPI32.dll**: Libreria critica che permette l'interazione con il Registro di sistema, la gestione degli account utente e il controllo dei servizi di sistema.
- **USER32.dll**: Gestisce tutti gli elementi dell'interfaccia utente (finestre, menu) e riceve gli input da tastiera e mouse.
- **GDI32.dll**: Utilizzata per le operazioni grafiche, come il rendering di testo e immagini sullo schermo.
- **SHELL32.dll**: Permette al programma di eseguire comandi tramite la shell di Windows e interagire con le cartelle di sistema.
- **MSVCRT.dll**: Libreria standard del runtime C, utilizzata per funzioni comuni di programmazione come l'allocazione di memoria e la manipolazione di stringhe.

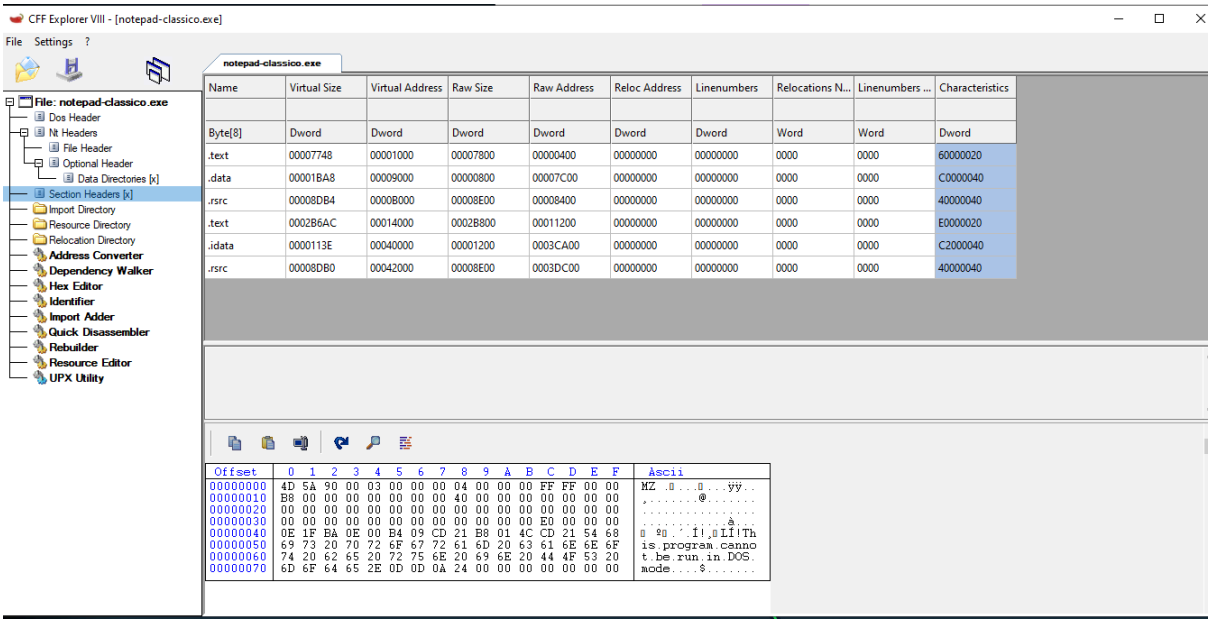
- **COMDLG32.dll**: Contiene le finestre di dialogo standard (Apri/Salva), necessarie per simulare l'interfaccia del Blocco Note originale.



2. Analisi delle Sezioni

L'analisi dell'intestazione PE (*Section Headers*) evidenzia una struttura anomala composta dalle seguenti sezioni:

- **.text (doppia)**: La sezione principale del codice eseguibile. La presenza di una seconda sezione `.text` suggerisce l'inserimento di codice non originale o di un modulo malevolo aggiuntivo.
- **.data**: Area dedicata alle variabili globali e ai dati statici utilizzati durante l'esecuzione.
- **.rsrc (doppia)**: Contiene le risorse del file (icone, menu). La duplicazione di questa sezione è spesso usata per occultare file secondari o configurazioni del malware.
- **.idata**: Ospita la *Import Address Table* (IAT), ovvero i riferimenti alle funzioni esterne elencate nella sezione precedente.
- **.reloc**: Contiene i dati necessari per il rilocamento del codice in memoria (Base Relocation), essenziali per il corretto funzionamento su diverse configurazioni di sistema.



Nota Tecnica Finale

"L'eseguibile analizzato è un esempio di **malware 'backdoored'** o infetto, progettato per camuffarsi da applicazione legittima (`Notepad.exe`) tramite il mascheramento dei metadati e delle icone. La struttura interna presenta evidenti anomalie, tra cui la duplicazione delle sezioni `.text` e `.rsrc`, tattica comunemente utilizzata per iniettare codice malevolo o payload compressi all'interno di un file originale. L'importazione di funzioni tramite **ADVAPI32.dll** suggerisce che il programma esegua operazioni non autorizzate sul Registro di sistema o sulla sicurezza degli account, rendendolo potenzialmente pericoloso per la persistenza nel sistema e per l'esfiltrazione di informazioni."