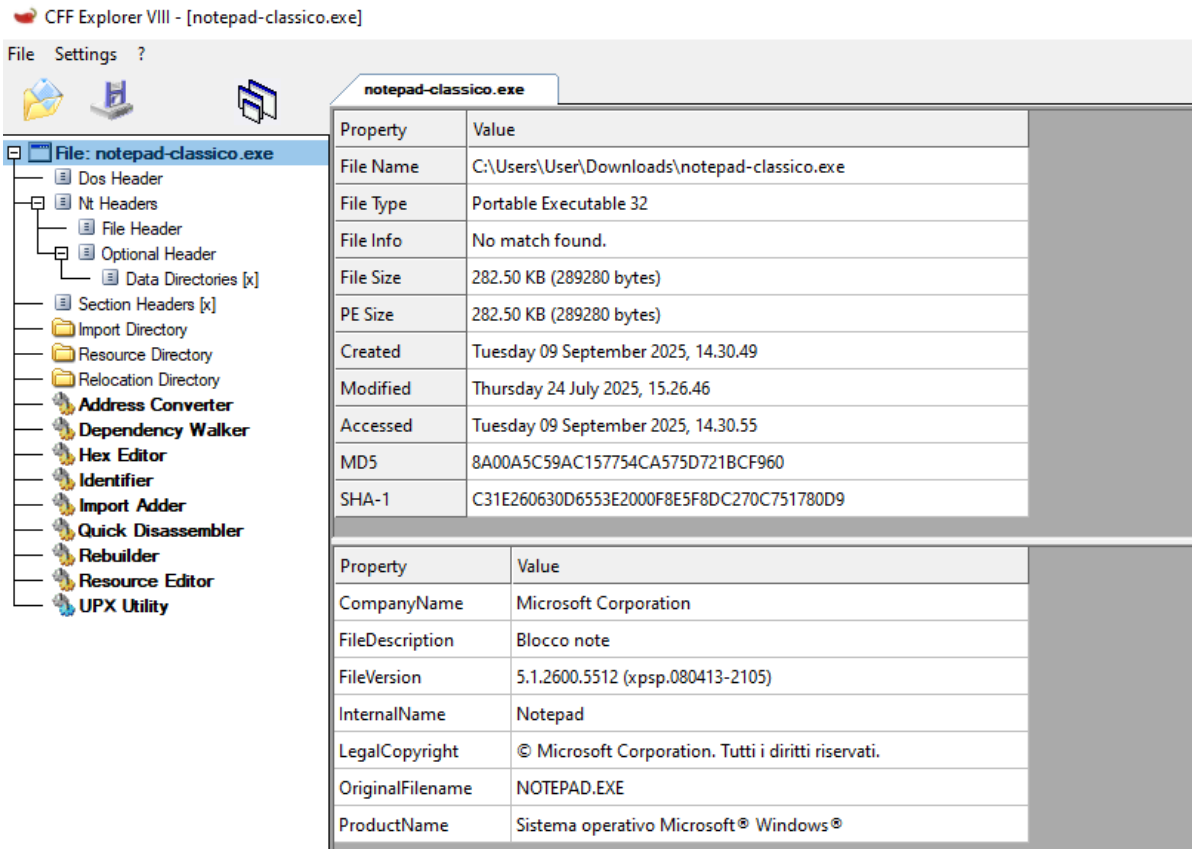
Analisi Malware - notepad-classico.exe

L’esercizio di oggi consiste nell’analisi di un malware denominato notepad-classico.exe .

Fase 1
Per effettuare l’analisi apriamo il malware con CFF explorer, un utility software molto utilizzato nell’analisi, nel capirne il funzionamento e identificare le loro funzionalità nascoste.

1. Inserimento malware in CFF explorer
   Una volta inserito il file all’interno dell'applicazione avremo questa schermata



Property	Value
File Name	C:\Users\User\Downloads\notepad-classico.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	282.50 KB (289280 bytes)
PE Size	282.50 KB (289280 bytes)
Created	Tuesday 09 September 2025, 14.30.49
Modified	Thursday 24 July 2025, 15.26.46
Accessed	Tuesday 09 September 2025, 14.30.55
MD5	8A00A5C59AC157754CA575D721BCF960
SHA-1	C31E260630D6553E2000F8E5F8DC270C751780D9

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Blocco note
FileVersion	5.1.2600.5512 (xpsp.080413-2105)
InternalName	Notepad
LegalCopyright	© Microsoft Corporation. Tutti i diritti riservati.
OriginalFilename	NOTEPAD.EXE
ProductName	Sistema operativo Microsoft® Windows®

   In questa schermata abbiamo alcune informazioni di base sul file, come il tipo, la grandezza e le date di creazione, modifica e accesso.

2. Visualizzazione librerie importate

   Per visualizzare le varie librerie importate ci spostiamo su Import directory nel menù a sinistra

notepad-classico.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
comdlg32.dll	9	000400C8	00000000	FFFFFFFF	00040410	000012C4
SHELL32.dll	4	000400F0	00000000	FFFFFFFF	000404B5	00001174
WINSPOOL.DRV	3	00040104	00000000	FFFFFFFF	00040502	000012B4
COMCTL32.dll	1	00040114	00000000	FFFFFFFF	00040543	00001020
msvcrt.dll	22	0004011C	00000000	FFFFFFFF	00040566	000012EC
ADVAPI32.dll	7	00040178	00000000	FFFFFFFF	0004068A	00001000
KERNEL32.dll	57	00040198	00000000	FFFFFFFF	0004070F	0000108C
GDI32.dll	24	00040280	00000000	FFFFFFFF	00040AF1	00001028
USER32.dll	74	000402E4	00000000	FFFFFFFF	00040C5F	00001188

Descrizione librerie

- **comdlg32.dll (Common Dialog Box Library):** Gestisce le finestre di dialogo standard di Windows (ad esempio, "Apri file", "Salva file", "Stampa"). I malware possono sfruttarla per ingannare l'utente o mostrare false finestre di dialogo.

- **SHELL32.dll (Windows Shell API):** Consente l'accesso a funzioni della shell di Windows come la gestione di file, cartelle e l'esecuzione di programmi. I malware possono utilizzarla per:
  - Navigare nel filesystem.
  - Creare, copiare o eliminare file.
  - Eseguire altri file eseguibili.
  - Gestire icone e la visualizzazione del desktop.

- **WINSPool.DRV (Windows Spooler Driver):** Controlla le operazioni di stampa. La sua presenza in un malware è insolita, a meno che l'aggressore non intenda:
  - Stampare documenti indesiderati.
  - Sfruttare vulnerabilità nello spooler di stampa (ad esempio,

PrintNightmare).

- **COMCTL32.dll (Common Controls Library):** Contiene i controlli standard dell'interfaccia utente di Windows (pulsanti, caselle di testo, barre di scorrimento). Un malware la utilizzerebbe se disponesse di un'interfaccia grafica (GUI) per interagire con l'utente.

- **msvcrt.dll (Microsoft Visual C Runtime Library):** Contiene le funzioni base del linguaggio C (gestione della memoria, operazioni su stringhe, I/O). È una dipendenza comune per molti programmi C/C++, e la sua presenza non è di per sé indicativa di un comportamento malevolo.

- **ADVAPI32.dll (Advanced Windows 32 API):** Fornisce accesso a funzioni avanzate del sistema operativo, in particolare quelle di sicurezza (gestione del registro, credenziali, servizi). I malware possono utilizzarla per:
    - Modificare chiavi di registro per la persistenza all'avvio.
    - Interrogare o modificare le impostazioni di sicurezza.
    - Eseguire operazioni con privilegi elevati.

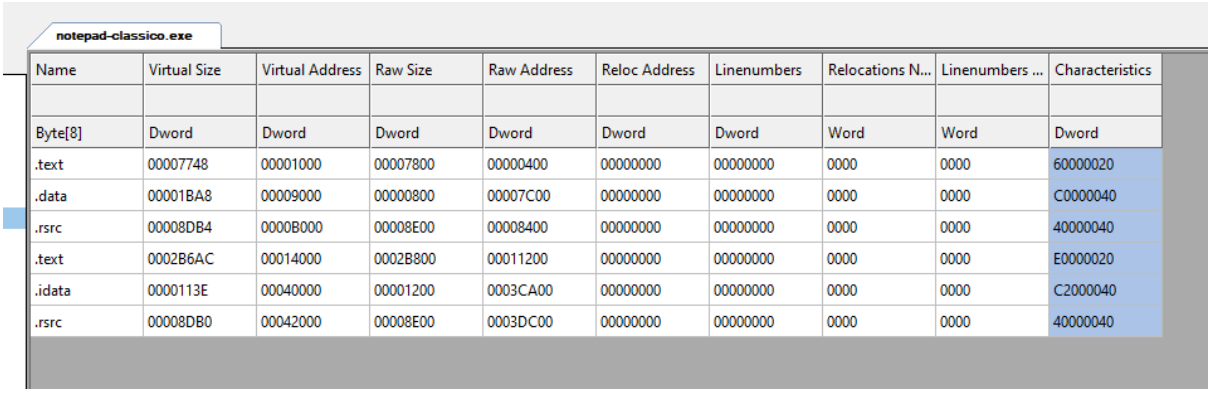
- **KERNEL32.dll (Kernel 32-bit Library):** La libreria più cruciale di Windows, include funzioni fondamentali per la gestione di memoria, processi, thread e file. Tutti i programmi dipendono da KERNEL32.dll. I malware possono utilizzarla per:
    - Creare, iniettare o terminare processi.
    - Leggere e scrivere memoria in altri processi.
    - Gestire la comunicazione tra processi.
    - Gestire le operazioni di I/O su file.

- **GDI32.dll (Graphics Device Interface Library):** Offre funzioni per disegnare grafica e testo sullo schermo. I malware potrebbero utilizzarla per:
    - Creare una finestra popup o un'interfaccia utente.
    - Catturare schermate (se usata in combinazione con altre API).
    - Sovrapporre immagini sullo schermo per ingannare l'utente.

- **USER32.dll (User Interface Library):** Gestisce gli elementi dell'interfaccia utente (finestre, menu, pulsanti, input utente). I malware possono utilizzarla per:
    - Interagire con finestre di altre applicazioni.
    - Registrare le sequenze di tasti (keylogging).
    - Catturare il movimento del mouse.
    - Mostrare o nascondere finestre.

3. Sezioni di cui si compone il malware

   Per visualizzare le sezioni del malware ci spostiamo nella sezione del menù "Section Headers", dove possiamo vedere come è organizzato più internamente



notepad-classico.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00007748	00001000	00007800	00000400	00000000	00000000	0000	0000	60000020
.data	00001BA8	00009000	00000800	00007C00	00000000	00000000	0000	0000	C0000040
.rsrc	00008DB4	0000B000	00008E00	00008400	00000000	00000000	0000	0000	40000040
.text	0002B6AC	00014000	0002B800	00011200	00000000	00000000	0000	0000	E0000020
.idata	0000113E	00040000	00001200	0003CA00	00000000	00000000	0000	0000	C2000040
.rsrc	00008DB0	00042000	00008E00	0003DC00	00000000	00000000	0000	0000	40000040

Ecco un'analisi delle sezioni elencate:

Il testo descrive le sezioni chiave di un file eseguibile, ognuna con un ruolo specifico e caratteristiche distintive.

- **. text (Sezione Codice):** Questa sezione contiene il codice eseguibile del programma. La "Virtual Size" indica la sua dimensione in memoria, mentre la "Raw Size" si riferisce alla dimensione su disco. I "Characteristics" definiscono le sue proprietà: **60000020** è il valore tipico per il codice eseguibile. Tuttavia, un valore come **E0000020** (eseguibile e scrivibile) è sospetto e può indicare la presenza di malware, poiché un codice eseguibile non dovrebbe essere modificabile in memoria durante l'esecuzione.
- **.data (Sezione Dati Inizializzati):** In questa sezione sono archiviate le variabili globali e tutti i dati inizializzati all'avvio del programma. Le dimensioni sono indicate dalla "Virtual Size" e dalla "Raw Size". I "Characteristics" **C0000040** (scrivibile, leggibile, dati inizializzati) sono considerati normali per questa sezione, riflettendo la sua natura di contenitore per dati che possono essere letti e modificati.
- **.rsrc (Sezione Risorse):** Questa sezione è dedicata all'archiviazione di risorse come

icone, immagini, menu, cursori e altri elementi grafici o non eseguibili utilizzati dal programma. I "Characteristics" **40000040** (leggibile, dati inizializzati) sono tipici. È un punto di interesse per l'analisi di malware, in quanto i payload dannosi possono essere nascosti all'interno delle risorse per eludere il rilevamento.
- **.idata (Sezione Importazioni):** Questa sezione gestisce le importazioni da librerie di collegamento dinamico (DLL), ovvero le funzioni esterne che il programma utilizza. I "Characteristics" **C2000040** (leggibile e scrivibile) possono rappresentare un segnale di allarme. La capacità di scrittura in questa sezione può indicare tecniche di offuscamento utilizzate da malware, come l'IAT (Import Address Table) hooking, dove il malware modifica gli indirizzi delle funzioni importate per reindirizzare le chiamate a codice malevolo.

Come possiamo notare le sezioni `.text` e `.rsrc` sono duplicate, viene fatto questo procedimento per confondere gli analisti e i programmi antivirus. Facendo questo passaggio è possibile nascondere i payload dannosi all'interno di uno dei due mentre nell'altro viene lasciato il codice innocuo.

Conclusione

L'analisi del file notepad-classico.exe tramite CFF Explorer ha rivelato diverse caratteristiche sospette che suggeriscono la sua natura malevola. In particolare, la combinazione di permessi di scrittura ed esecuzione nella sezione .text (indicata dal flag E0000020) è un forte indicatore di codice polimorfico o auto-modificante, tipico dei malware.
Le librerie importate, come SHELL32.dll e ADVAPI32.dll, confermano le potenziali capacità del malware di manipolare file, cartelle, eseguire programmi, e interagire con il registro di sistema e le impostazioni di sicurezza.
In sintesi, notepad-classico.exe non sembra essere un'applicazione legittima e presenta le firme di un software malevolo progettato per alterare il proprio comportamento in memoria e interagire con funzioni sensibili del sistema operativo.