ESERCIZIO S9 L2

EPICODE

Esercizio
Traccia

Traccia:

Rispondere ai seguenti quesiti, con riferimento al file eseguibile **notepad-classico.exe** contenuto in questo **file compresso**:

https://drive.google.com/file/d/1HNnJDSY7FbD1KHfiRzA2wVNHhzTJndUD/view?usp=sharing

- Indicare le **librerie importate** dal malware, fornendo una **descrizione** per ognuna di esse tramite AI;
- Indicare le **sezioni** di cui si compone il malware, fornendo una **descrizione** per ognuna di essa tramite AI.

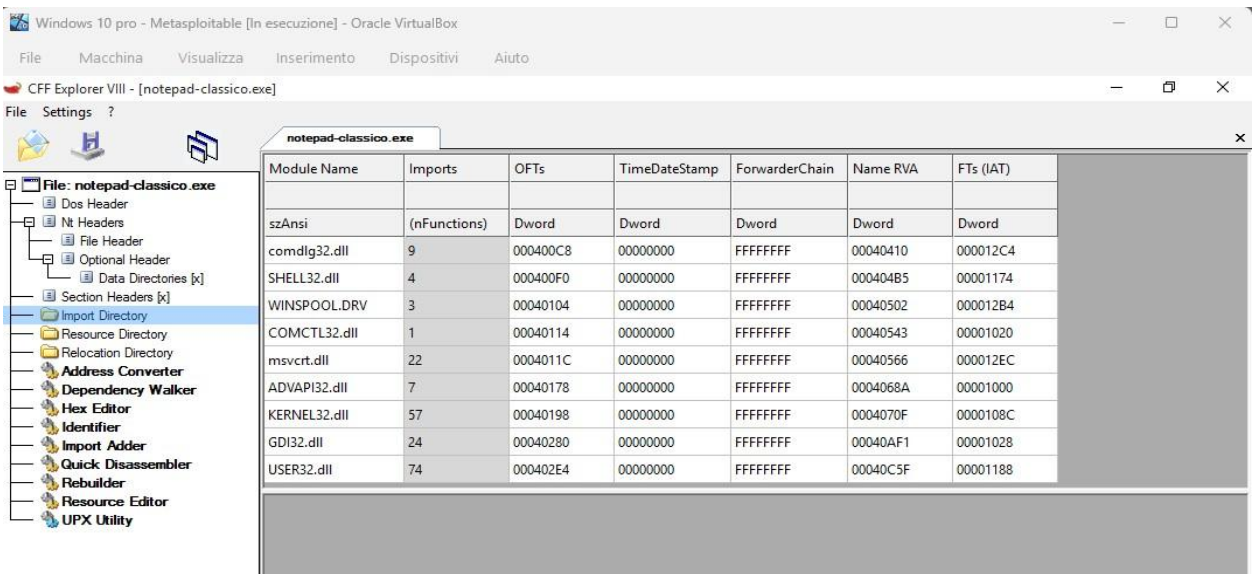
Suggerimento: ChatGPT (o altri LLM) possono ricevere in input degli screenshot da analizzare e cerca librerie caricate dinamicamente nei testi del codice.

SVOLGIMENTO

Come primo passo scarico il file compresso **notepad-classico** ed estraggo i file con **Winrar.**

ANALISI LIBRERIE TRAMITE AI DEL FILE notepad-classico.exe

Apro **ExplorerSuite** ed inizio l'analisi del file**.**



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

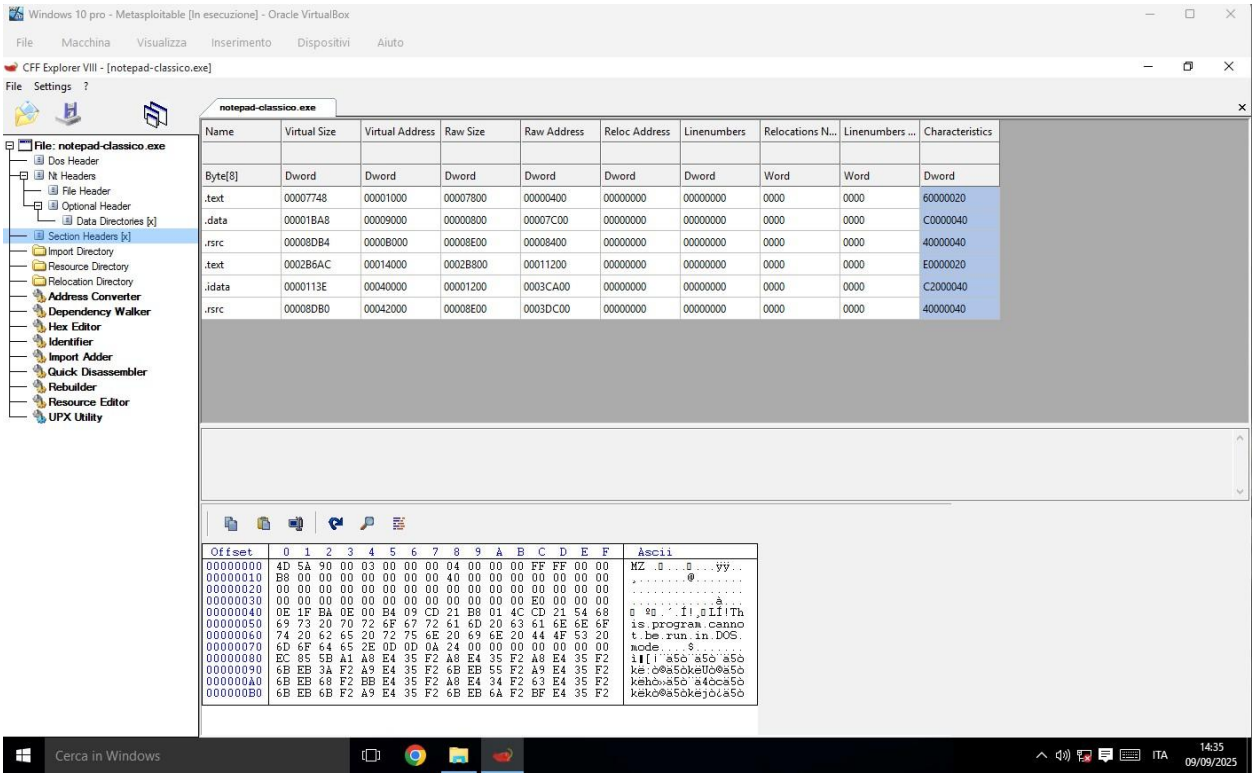
L'immagine mostra il programma **CFF Explorer (ExplorerSuite)** che analizza il file eseguibile **notepad-classico.exe**. Nello specifico, la sezione mostrata è la **Import Directory**, che elenca le **librerie** di cui l'eseguibile ha bisogno per funzionare.

Ecco una descrizione delle librerie (DLL) visibili nell'immagine:

- **szAnsi**: Non è una libreria, ma un segnaposto per le funzioni ANSI che il programma importa.
- **comdlg32.dll**: La **Common Dialogs Library**. Contiene funzioni per la creazione di finestre di dialogo standard di Windows, come la finestra di apertura o salvataggio file, la stampa, o la scelta del colore e del font.
- **SHELL32.dll**: Contiene funzioni di **Shell API** che permettono al programma di interagire con il sistema operativo Windows, ad esempio per l'esecuzione di programmi, la gestione dei file e delle cartelle, e l'accesso al desktop.
- **WINSPOOLDRV**: Probabilmente si tratta di una libreria legata alla stampa. Il nome suggerisce che si riferisce al driver dello **spooler di stampa** di Windows, un componente che gestisce le code di stampa.
- **COMCTL32.dll**: La **Common Controls Library**. Fornisce i controlli standard dell'interfaccia utente di Windows, come pulsanti, caselle di testo, barre di scorrimento, ecc.
- **msvcrt.dll**: La **Microsoft Visual C++ Runtime Library**. Contiene le funzioni di base necessarie per i programmi compilati con Visual C++, come la gestione della memoria e le operazioni di input/output.
- **ADVAPI32.dll**: L'**Advanced Windows 32 API Library**. Contiene funzioni avanzate di sistema, tra cui quelle per la gestione del registro di Windows, la sicurezza e la crittografia.
- **KERNEL32.dll**: Una delle librerie più importanti di Windows. La **Windows 32-bit Base API Library**. Contiene le funzioni di base per la gestione del sistema operativo, come la creazione e la gestione dei processi, dei thread e della memoria.
- **GDI32.dll**: La **Graphics Device Interface Library**. Contiene le funzioni per la gestione della grafica, come il disegno di linee, rettangoli e altri elementi sullo schermo.
- **USER32.dll**: Contiene le funzioni per la gestione dell'interfaccia utente di base, inclusa la creazione e la gestione delle finestre e la ricezione di input da mouse e tastiera.

In sintesi, l'analisi dell'**Import Directory** mostra che **notepad-classico.exe** è un programma grafico di base per Windows che gestisce file di testo, con funzioni di dialogo, interazione con la shell e la stampante.

ANALISI SEZIONI TRAMITE AI DEL FILE notepad-classico.exe



La sezione **Section Headers** descrive l'organizzazione del file in blocchi di memoria logici, ognuno con uno scopo preciso.

- **Due sezioni .text**: Entrambe contengono codice eseguibile. La presenza di due sezioni con lo stesso nome è insolita per un file eseguibile standard. Può essere il risultato di una particolare configurazione del linker, ma potrebbe anche indicare che il file è stato compattato o protetto con un "packer" per nascondere o offuscare il codice.
- **.data**: Contiene le **variabili globali e statiche** del programma che vengono inizializzate con dei valori predefiniti.
- **.rdata**: Contiene **dati di sola lettura**, come stringhe di testo e costanti che non possono essere modificate durante l'esecuzione del programma.
- **. Due sezioni .rsrc**: Entrambe contengono **risorse del programma** (icone, stringhe, immagini). Anche in questo caso, avere due sezioni con lo stesso nome non è comune.

- **.idata**: È la **Import Address Table (IAT)**. Questa sezione è cruciale perché elenca gli indirizzi di memoria esatti delle funzioni importate dalle librerie, permettendo al programma di chiamarle in modo corretto durante l'esecuzione.
- **.reloc**: Contiene informazioni necessarie per la **rilocazione** del codice in memoria. Se il sistema operativo carica il programma a un indirizzo diverso da quello predefinito, queste informazioni aiutano a correggere gli indirizzi interni per evitare errori.

In sintesi, l'analisi mostra che **notepad-classico.exe** è un programma Windows classico che si affida alle librerie di sistema per svolgere i suoi compiti, organizzando il suo codice, i dati e le risorse in sezioni ben definite.

CONSIDERAZIONE FINALE

L'analisi completa rivela che, sebbene le librerie importate siano tipiche di un'applicazione legittima, la struttura delle sezioni, con più sezioni **text** e **rsrc,** è insolita.

Mentre questa anomalia non è una prova definitiva di codice malevolo, è un comportamento che può essere associato a tecniche di offuscamento utilizzate dai malware o dai "packers" (programmi che comprimono un eseguibile per ridurne le dimensioni o offuscarne il codice).