Analisi Statica di "notepad-classico.exe"

1. Introduzione

In questa esercitazione ho condotto un'analisi statica preliminare su un campione malware denominato notepad-classico.exe. L'obiettivo principale è stato identificare le caratteristiche strutturali del file, specificamente le librerie importate (Import Address Table) e le sezioni del Portable Executable (PE), per comprenderne le potenziali funzionalità senza eseguirlo.

Tutte le operazioni sono state svolte all'interno di un ambiente isolato (**VirtualBox** con Windows 10 e strumenti di analisi disabilitati dalla rete per sicurezza), garantendo che l'host fisico non venisse compromesso.

2. Strumenti Utilizzati

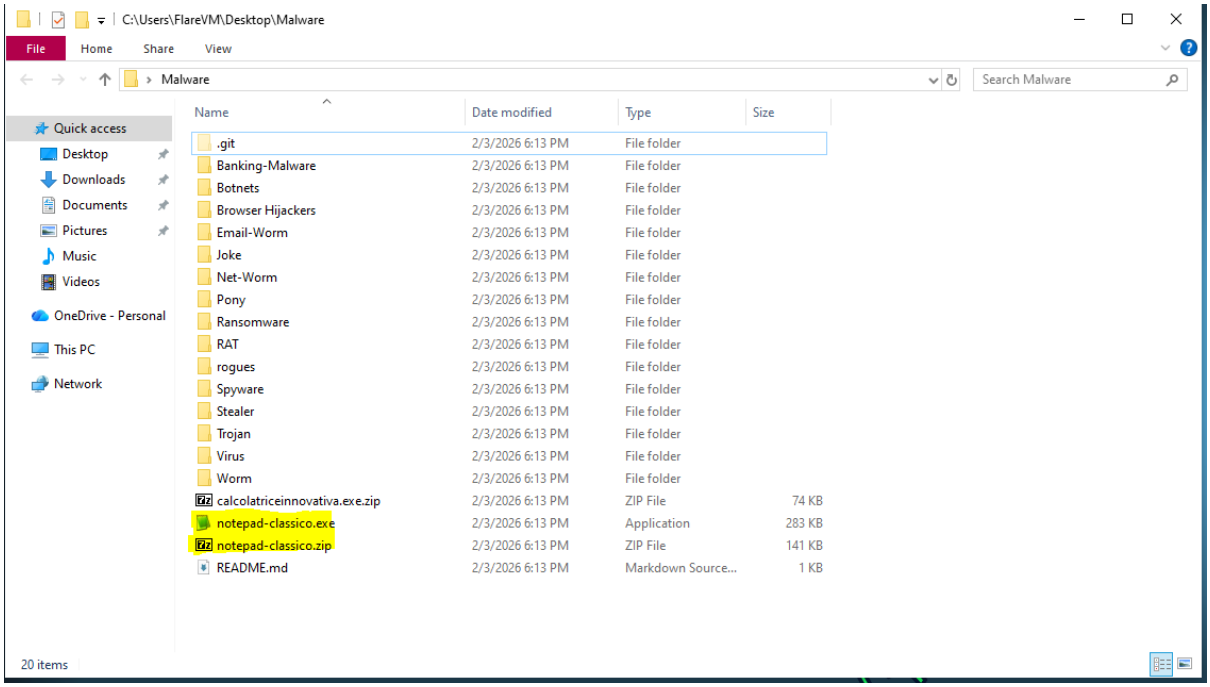
Per completare l'analisi, ho utilizzato i seguenti strumenti, scelti per la loro efficacia nel parsing degli header dei file eseguibili Windows:

- **CFF Explorer:** Per ispezionare l'header del file, le librerie importate, le stringhe e le sezioni.
- **Virtual Machine (VirtualBox):** Ambiente di sandboxing per la manipolazione sicura del file.
- **7-Zip:** Per l'estrazione dell'archivio protetto da password.

3. Procedura Operativa e Analisi

1: Preparazione e Estrazione

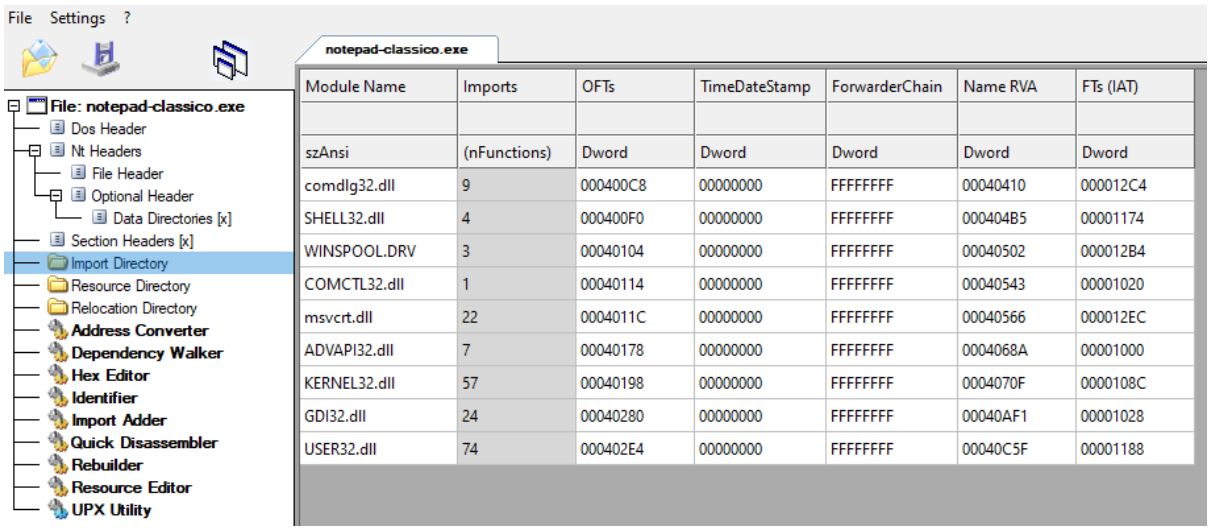
Ho scaricato il file compresso contenente il malware all'interno della mia Macchina Virtuale. Utilizzando la password fornita (infected), ho estratto il file notepad-classico.exe.



2: Analisi delle Librerie Importate

Ho aperto il file notepad-classico.exe all'interno di CFF Explorer e mi sono recato nella sezione Import Directory. Le librerie importate (DLL) ci dicono quali funzioni di Windows il malware intende utilizzare.

Ecco le librerie principali identificate e la relativa descrizione (generata tramite supporto AI come richiesto dalla traccia):



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

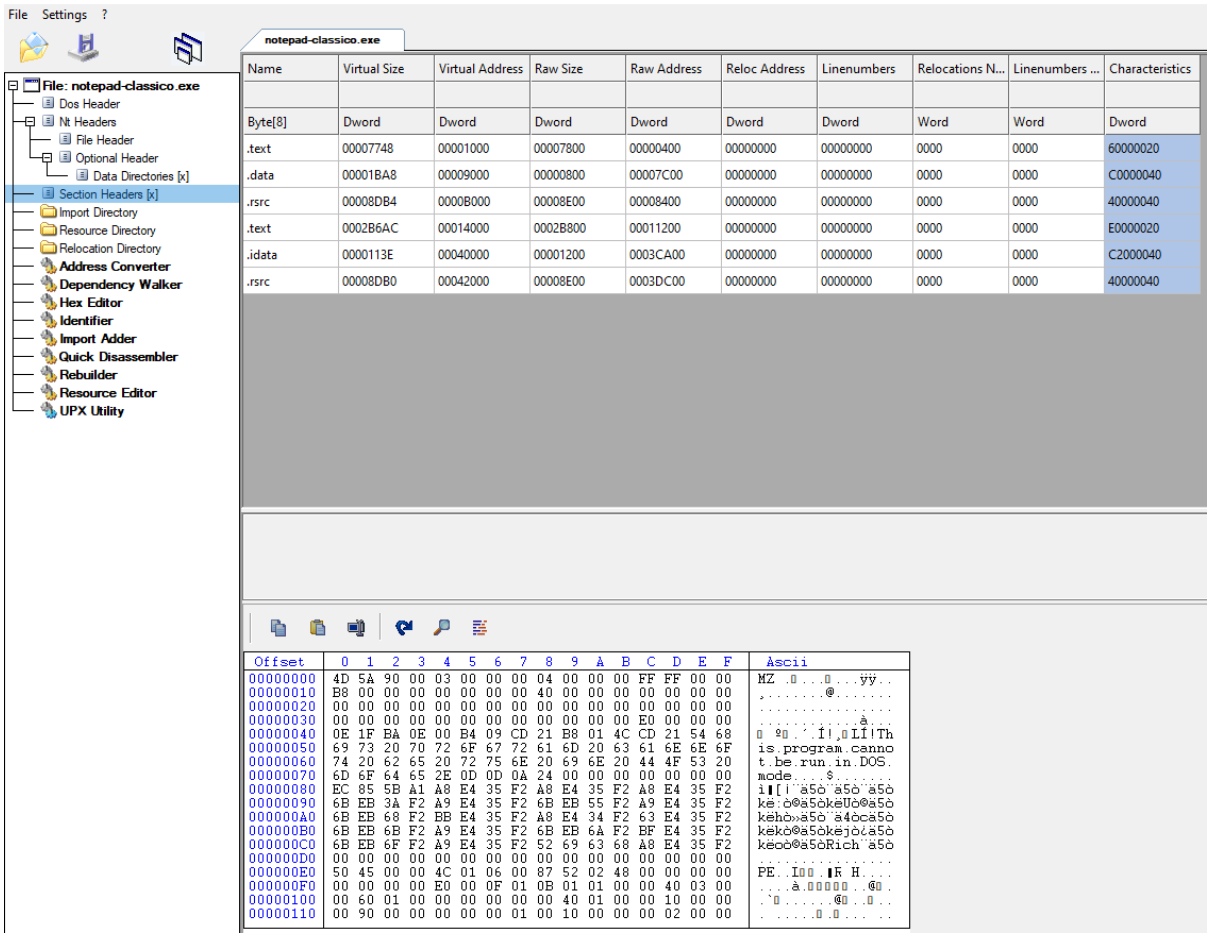
Dall'analisi emergono le seguenti librerie critiche:

1. **KERNEL32.dll**

    a. **Descrizione:** È la libreria fondamentale del sistema operativo Windows. Gestisce la memoria, i processi, i thread e le operazioni di input/output sui file.
    b. **Implicazione nel Malware:** Il malware la utilizza per avviarsi, nascondersi nella memoria, creare nuovi processi (process injection) o manipolare file sul disco.
2. **USER32.dll**
    a. **Descrizione:** Gestisce l'interfaccia utente (finestre, icone) e le interazioni come mouse e tastiera.
    b. **Implicazione nel Malware:** Spesso usata dai keylogger (come Agent Tesla) per intercettare i tasti premuti dall'utente (funzioni come GetAsyncKeyState) o per fare screenshot.
3. **ADVAPI32.dll** (Advanced Windows 32 Base API)
    a. **Descrizione:** Fornisce l'accesso al Registro di Sistema, alla gestione dei servizi e agli account utente/sicurezza.
    b. **Implicazione nel Malware:** Utilizzata per garantire la "persistenza" (modificare il registro per avviarsi automaticamente al riavvio del PC) o per tentare di scalare i privilegi.
4. **SHELL32.dll**
    a. **Descrizione:** Gestisce le operazioni della shell di Windows, come l'apertura di file o l'esecuzione di comandi di sistema.
    b. **Implicazione nel Malware:** Usata per eseguire comandi cmd o lanciare altri eseguibili.

3: Analisi delle Sezioni

Successivamente, ho analizzato la scheda **Section Headers** per osservare come è organizzato il codice binario. Le sezioni standard di un file PE (Portable Executable) sono solitamente .text, .data, .rsrc.



Ecco le sezioni identificate e la loro descrizione tecnica:

1. **.text**
    a. **Descrizione:** Questa sezione contiene il codice eseguibile vero e proprio del programma (le istruzioni CPU). È solitamente marcata come "eseguibile" e "sola lettura".
    b. **Analisi:** Se la dimensione "Raw Size" (su disco) è molto inferiore alla "Virtual Size" (in memoria), potrebbe indicare che il malware è "packato" (compresso/offuscato) per evadere gli antivirus.
2. **.data**
    a. **Descrizione:** Contiene le variabili globali e statiche inizializzate del programma. Qui vengono salvati i dati che il programma usa durante l'esecuzione.
    b. **Analisi:** I malware spesso usano questa sezione per decifrare configurazioni o stringhe nascoste.
3. **.rsrc** (Resources)

a. **Descrizione:** Contiene le risorse utilizzate dall'applicazione, come icone, immagini, menu e stringhe di versione.
b. **Analisi:** In molti malware, questa sezione è sospetta se contiene altri file eseguibili nascosti o script crittografati pronti per essere estratti ed eseguiti.

4. Conclusione

L'analisi statica di notepad-classico.exe ha rivelato l'importazione di librerie critiche che suggeriscono capacità di manipolazione del sistema (kernel32), interazione con l'utente (user32) e potenzialmente operazioni di rete o registro.