

ESERCIZIO W21D4

ANALISI STATICA BASICA

Mungiovì Fabio

TASK

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.

Facoltativo:

Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.

ESECUZIONE

Per l'esecuzione dell'esercizio, il file **notepad-classico.exe** è stato analizzato tramite il tool **CFF explorer**.

Sono stati analizzati i seguenti sezioni:

Schermata iniziale di CFF Explorer, che fornisce una panoramica generale del file

Property	Value
File Name	C:\Users\haunter\Desktop\notepad-classico\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	Friday 25 July 2025, 20.31.50
Modified	Friday 25 July 2025, 20.31.50
Accessed	Saturday 26 July 2025, 01.08.46
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®

Import Directory, che mostra le librerie (DLL) che l'eseguibile importa.

Module Name	Imports	OFTs	TimeStamp	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

Section Headers, che mostra le diverse sezioni logiche del file eseguibile

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

Gli screenshot allegati sono stati dati da analizzare al modello di intelligenza artificiale **Gemini** con il seguente risultato:

Ecco l'analisi statica del file notepad-classico.exe basata sulle informazioni fornite.

Librerie Importate

Il file eseguibile importa diverse librerie di sistema standard di Windows, essenziali per il funzionamento di applicazioni con interfaccia grafica. Di seguito l'elenco e la loro funzione principale:

- **KERNEL32.dll:** È la libreria principale del sistema operativo. Gestisce operazioni fondamentali come la memoria, i processi e i thread. È indispensabile per quasi tutte le applicazioni Windows.
- **USER32.dll:** Gestisce tutti gli aspetti dell'interfaccia utente, come la creazione e la gestione di finestre, menu, dialoghi e la ricezione di input dall'utente (mouse e tastiera).
- **GDI32.dll:** (Graphics Device Interface) È responsabile del rendering di grafica e testo sullo schermo e su altri dispositivi di output come le stampanti.
- **ADVAPI32.dll:** (Advanced API) Fornisce l'accesso a funzionalità di sistema avanzate, tra cui il registro di Windows, la gestione degli account utente e i servizi di sicurezza.
- **msvcrt.dll:** (Microsoft Visual C++ Runtime) Contiene le funzioni standard del linguaggio C (es. manipolazione di stringhe, operazioni matematiche, gestione di file) necessarie per l'esecuzione del programma.
- **SHELL32.dll:** Permette all'applicazione di interagire con la shell di Windows, ad esempio per gestire file, cartelle e collegamenti.
- **comdlg32.dll:** (Common Dialogs) Fornisce le finestre di dialogo standard di Windows, come "Apri", "Salva con nome" e "Stampa".
- **WINSPOOL.DRV:** Gestisce le operazioni di stampa, permettendo all'applicazione di inviare documenti alla coda di stampa.
- **COMCTL32.dll:** (Common Controls) Fornisce i controlli comuni dell'interfaccia grafica, come pulsanti, barre di stato, barre degli strumenti e schede.

Sezioni del File

L'eseguibile è suddiviso in sezioni standard, ognuna con uno scopo specifico. Le sezioni principali identificate sono:

- **.text:** Questa è la sezione più importante, poiché **contiene il codice eseguibile** del programma, ovvero le istruzioni che la CPU eseguirà. Le sue caratteristiche indicano che è una sezione che può essere eseguita e letta.
- **.data:** Contiene i **dati inizializzati** del programma, come variabili globali e statiche che hanno un valore predefinito all'avvio dell'applicazione. È una sezione scrivibile e leggibile.

- **.rsrc:** Contiene le **risorse** utilizzate dall'applicazione. Queste non sono codice eseguibile ma elementi come icone, immagini, menu, stringhe di testo (es. messaggi di errore) e informazioni sulla versione del file. È una sezione di sola lettura.

La presenza di sezioni multiple con lo stesso nome (es. due .text, due .data e due .rsrc) è comune e dipende da come il compilatore e il linker hanno organizzato il file eseguibile finale.

Considerazione Finale (Facoltativo)

Basandosi sull'analisi statica, il file notepad-classico.exe **non presenta caratteristiche tipiche di un malware**.

Le informazioni del file (nome prodotto, azienda, copyright di Microsoft) e le sue dipendenze sono del tutto coerenti con quelle del legittimo programma **Blocco Note (Notepad.exe)** di una vecchia versione di Windows, probabilmente Windows XP. Le librerie importate sono quelle standard per un'applicazione di testo con interfaccia grafica e non includono funzioni sospette comunemente associate a malware (es. connessioni di rete nascoste, modifica di file di sistema, registrazione della tastiera).

In conclusione, si tratta molto probabilmente di una versione autentica e non dannosa del Blocco Note, utilizzata come campione per un'esercitazione di analisi.

FACOLTATIVO

Nonostante il file analizzato sia effettivamente un Malware, dall'analisi statica basica effettuata con il supporto dell' AI, non risultano presenti evidenze che permettano di riconoscere il malware.

Per avere riscontri differenti ho effettuato l'analisi con diversi modelli (Chat GPT, Deepseek) ma con gli stessi risultati.

Sarà quindi necessario effettuare analisi di tipo differente per analizzare le sezioni malevole del file.