

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

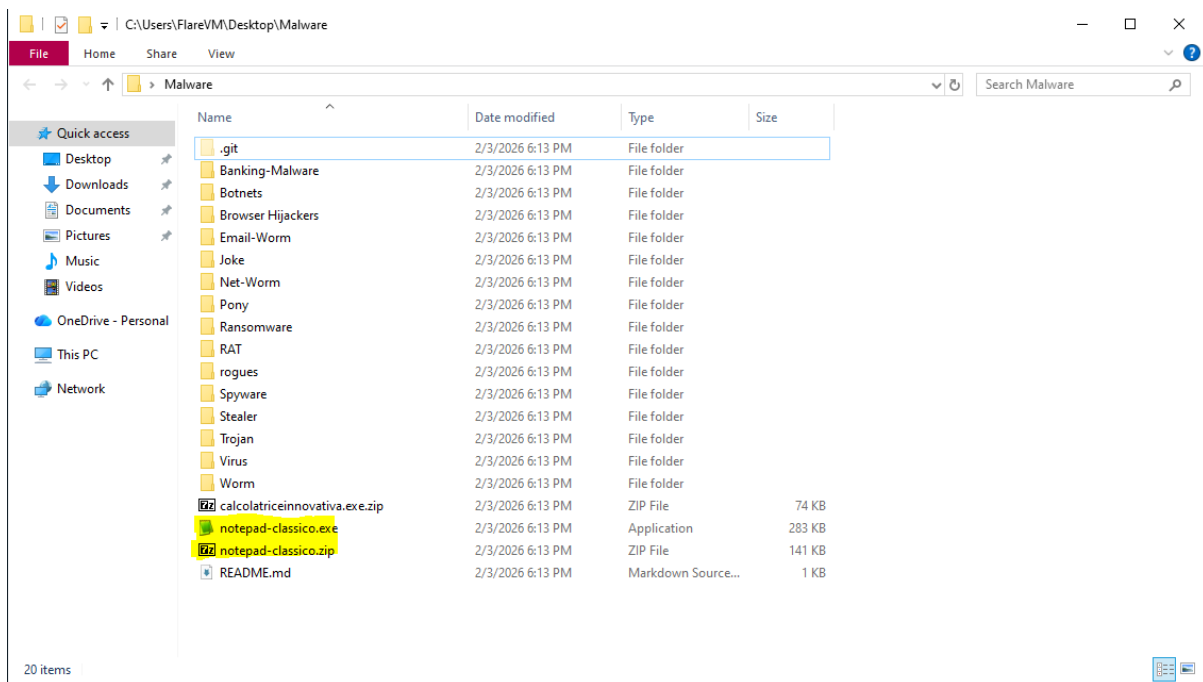
Per completare l'analisi, ho utilizzato i seguenti strumenti, scelti per la loro efficacia nel parsing degli header dei file eseguibili Windows:

- **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):

File Settings ?

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

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.

File Settings ?

notepad-classico.exe

File: notepad-classico.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]**
 - Import Directory
 - Resource Directory
 - Relocation Directory
 - Address Converter
 - Dependency Walker
 - Hex Editor
 - Identifier
 - Import Address
 - Quick Disassembler
 - Rebuilder
 - Resource Editor
 - UPX Utility

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

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Ascii

```

00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ . . . . .yy.
00000001 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00000002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000003 00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00
00000004 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
00000005 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F
00000006 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
00000007 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00
00000008 EC 95 5B A1 A8 E4 35 F2 A8 E4 35 F2 A8 E4 35 F2
00000009 6B EB 3A F2 A9 E4 35 F2 6B EB 55 F2 A9 E4 35 F2
0000000A 6B EB 68 F2 BB E4 35 F2 A8 E4 34 F2 63 E4 35 F2
0000000B 6B EB 6B F2 A9 E4 35 F2 6B EB 6A F2 BF E4 35 F2
0000000C 6B EB 6F F2 A9 E4 35 F2 52 69 63 68 A8 E4 35 F2
0000000D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000E 50 45 00 00 4C 01 06 00 87 52 02 48 00 00 00 00
0000000F 00 00 00 00 E0 00 0F 01 0E 01 01 00 00 40 03 00
00000010 00 60 01 00 00 00 00 00 00 00 00 00 10 00 00 00
00000011 00 90 00 00 00 00 00 01 00 10 00 00 00 02 00 00
  
```

Ecco le sezioni identificate e la loro descrizione tecnica:

1. .text

- Descrizione:** Questa sezione contiene il codice eseguibile vero e proprio del programma (le istruzioni CPU). È solitamente marcata come "eseguibile" e "sola lettura".
- Analisi:** Se la dimensione "Raw Size" (su disco) è molto inferiore alla "Virtual Size" (in memoria), potrebbe indicare che il malware è "packato" (compressato/offuscato) per evadere gli antivirus.

2. .data

- Descrizione:** Contiene le variabili globali e statiche inizializzate del programma. Qui vengono salvati i dati che il programma usa durante l'esecuzione.
- 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.