

Relazione di Analisi Malware:

notepad-classico.exe

S9L2

Traccia:

Rispondere ai seguenti quesiti facendo riferimento al file eseguibile notepad-classico.exe, presente nella cartella "Malware" della macchina virtuale "Windows 10 metasploitable".

- 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.

Facoltativo:

- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.
 - Analisi Dinamica: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.
-

1) Analisi statica: librerie importate

Dall'analisi effettuata tramite il tool PEStudio, sono state identificate le librerie dinamiche (DLL) importate dal file, le quali ci forniscono indicazioni sulle capacità del software.

Le principali librerie identificate sono:

- **KERNEL32.dll:** libreria fondamentale di Windows per la gestione della memoria, dei file e dei processi, la sua presenza è standard, ma nei malware viene usata per manipolare file o avviare altri processi.
- **USER32.dll & GDI32.dll:** gestiscono l'interfaccia utente (finestre, input mouse/tastiera) e la grafica, indicano che il programma ha una GUI (Interfaccia Grafica) visibile.
- **ADVAPI32.dll (Advanced Windows 32 base API):** permette l'accesso al Registro di Sistema e alla gestione dei servizi/permessi, questa libreria è spesso utilizzata dai malware per garantire la persistenza (avviarsi automaticamente) o modificare le impostazioni di sicurezza.
- **SHELL32.dll:** consente l'esecuzione di comandi shell, spesso usata per lanciare altri eseguibili o aprire risorse esterne.
- **WINSPOOL.DRV:** driver per la gestione della stampa, talvolta sfruttato per tecniche di iniezione o persistenza meno comuni.

library (9)	flag (0)	type	imports (201)	description
comdlg32.dll	-	Implicit	9	Common Dialogs Library
SHELL32.dll	-	Implicit	4	Windows Shell Library
WINSPOOL.DRV	-	Implicit	3	Windows Spooler Driver
COMCTL32.dll	-	Implicit	1	Common Controls Library
msvcrt.dll	-	Implicit	22	Microsoft C Runtime Library
ADVAPI32.dll	-	Implicit	7	Advanced Windows 32 Base API
KERNEL32.dll	-	Implicit	57	Windows NT BASE API Client
GDI32.dll	-	Implicit	24	GDI Client Library
USER32.dll	-	Implicit	74	Multi-User Windows USER API Client Library

2) Analisi statica: sezioni del file

L'analisi degli header del file eseguibile ha rivelato la struttura interna delle sezioni.

Sono state rilevate le seguenti sezioni, con una **anomalia critica**:

- **.text, .data, .rsrc**: sezioni standard che contengono rispettivamente il codice eseguibile, i dati e le risorse (icone, stringhe).
- **Sezione .text duplicata (sospetta)**: è stata individuata una seconda sezione **.text** (o con caratteristiche anomale) che presenta permessi sia di **scrittura** che di **esecuzione** (Flag **RWX** o *Writable + Executable*).
 - **Analisi**: nei programmi legittimi, il codice non è mai scrivibile per motivi di sicurezza, questa configurazione è un forte indicatore che il malware è **"packed" (compresso)** o utilizza codice auto-modificante per nascondere il suo vero payload agli antivirus durante l'analisi statica.

property	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]
name	.text	.data	.rsrc	.text
section > sha256	181352B212CAF80C7A8FEAF...	87CBB581163F3AABE623127...	5E074AE0754BC823C26E8C3...	0033E40D79E7586AED87
entropy	6.214	1.149	5.421	6.428
file > ratio (99.65%)	10.62 %	0.71 %	12.57 %	61.59 %
raw-address (begin)	0x0000400	0x00007C00	0x00008400	0x00011200
raw-address (end)	0x00007C00	0x00008400	0x00011200	0x0003CA00
raw-size (288256 bytes)	0x00007800 (30720 bytes)	0x00000800 (2048 bytes)	0x00008E00 (36352 bytes)	0x0002B800 (178176 byt
virtual-address (begin)	0x00001000	0x00009000	0x0000B000	0x00014000
virtual-address (end)	0x00008748	0x0000ABA8	0x00013DB4	0x0003F6AC
virtual-size (292414 bytes)	0x00007748 (30536 bytes)	0x00001BA8 (7080 bytes)	0x00008DB4 (36276 bytes)	0x0002B6AC (177836 by
characteristics	0x60000020	0xC0000040	0x40000040	0xE0000020
write	-	x	-	x
execute	x	-	-	x
share	-	-	-	-
self-modifying	-	-	-	x
virtual	-	-	-	-
items				
directory > import	-	-	-	-
directory > resource	-	-	-	-
directory > relocation	-	-	-	0x0003F698
directory > import-address	0x00001000	-	-	-
manifest	-	-	-	-
version	-	-	-	-
base-of-code	0x00001000	-	-	-
base-of-data	-	0x00009000	-	-
entry-point > location	-	-	-	0x00014000

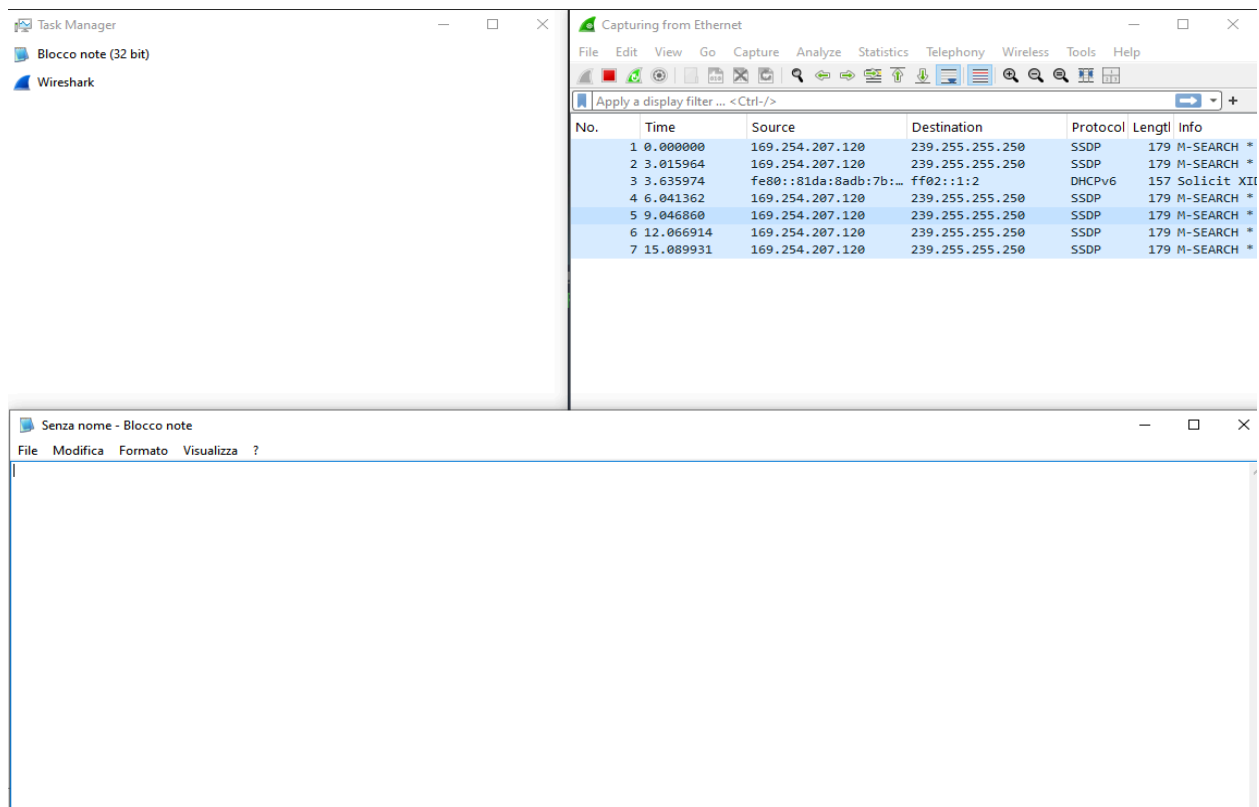
3) Analisi dinamica

Il file è stato eseguito in un ambiente controllato e isolato dalla rete (rete interna) per osservarne il comportamento in tempo reale.

Osservazioni:

- **Esecuzione:** al doppio clic sul file **notepad-classico.exe**, si è aperta immediatamente una finestra legittima del "Blocco Note" di Windows.
- **Processi:** strumenti di monitoraggio (Task Manager/Process Hacker) hanno mostrato che il processo rimane attivo.
- **Traffico di rete:** l'analisi con Wireshark ha mostrato traffico di background locale, ma l'isolamento della rete ha prevenuto connessioni verso server di comando e controllo (C2).

Deduzione: il comportamento osservato è tipico di un attacco "**Decoy**", il malware lancia un'applicazione innocua (il vero Blocco Note) per non destare sospetti nell'utente, mentre il codice malevolo viene verosimilmente iniettato in memoria o eseguito in background.



4) Considerazioni finali

In conclusione, l'analisi condotta permette di classificare **notepad-classico.exe** come un file malevolo, presumibilmente un **Trojan**.

Gli elementi probatori sono:

- La presenza di sezioni con permessi anomali (RWX) che indicano tecniche di offuscamento/packing.
- L'importazione di API sensibili per la manipolazione del registro e della shell.
- Il comportamento ingannevole all'esecuzione, che maschera l'attività malevola dietro l'apertura di un software legittimo.