

Report di Analisi Statica: Malware "notepad-classico.exe"

1. Introduzione

Il presente report documenta l'analisi statica di un file eseguibile sospetto denominato **notepad-classico.exe**. L'obiettivo dell'indagine è determinare la natura del file, identificare le tecniche di offuscamento e mimetismo, e mappare le funzionalità malevole secondo gli standard internazionali. Il sample è stato analizzato nella FlareVM per ricostruire la catena d'attacco originale in sicurezza.

2. Identificazione e Fingerprinting

Questa fase si concentra sull'intestazione del file Portable Executable (PE) per identificare modifiche sospette rispetto alla struttura standard di un'applicazione Windows legittima. Questo permette di stabilire l'identità digitale univoca del file tramite il calcolo degli hash crittografici. Per il sample **notepad-classico.exe**, sono stati rilevati i seguenti valori tramite il tool **HashMyFiles**:

The screenshot shows two windows. The top window is 'HashMyFiles' with a table of file details:

Filename	MD5	SHA-256	File Size	Modified Time	Created Time
notepad-classico.exe	8a00a5c59ac157754ca575d721bcf960	d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2	289,280	7/24/2025 3:26:46 PM	2/4/2026 9:42:56 AM

The bottom window is 'CFF Explorer VIII' showing the PE header structure of 'notepad-classico.exe'. The left pane shows sections like File Header, Nt Headers, and Import Directory. The right pane shows detailed memory dump information for sections like .text, .data, and .rsrc.

MD5: 8a00a5c59ac157754ca575d721bcf960

SHA-256:

d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2

2. Analisi della Struttura PE e Indicatori di Compromissione (IoC)

L'analisi tecnica condotta su **notepad-classico.exe** tramite **CFF Explorer** ha permesso di identificare profonde manipolazioni strutturali. Sebbene l'eseguibile si presenti come una versione dell'editor di testo Notepad, l'intestazione Portable Executable (PE) rivela anomalie critiche che ne confermano la natura di Trojan.

Indicatori di Compromissione (IoC) Strutturali

- Duplicazione e Iniezione di Sezioni:** L'evidenza principale della compromissione risiede nella tabella delle sezioni. Il file presenta **due sezioni denominate .text e due sezioni denominate .rsrc**. In un file PE legittimo, i nomi delle sezioni devono essere univoci; la duplicazione indica un'iniezione di codice (nella seconda sezione **.text**) e di risorse malevole (nella seconda sezione **.rsrc**) eseguita per aggiungere il payload Trojan senza rimuovere le funzionalità originali del programma.
- Analisi delle Dimensioni (Virtual Size):** La seconda sezione **.text** (associata al payload malevolo) presenta un *Virtual Size* di **0002B6AC**. Questa dimensione è significativamente superiore alla sezione **.text** originale (**00007748**), a conferma dell'inserimento di un carico di codice eseguibile complesso e voluminoso.
- Sezione .idata e Import Address Table:** È stata rilevata una sezione **.idata** (Import Data) con un *Virtual Size* di **0000113E**. Questa sezione è fondamentale per il funzionamento del malware, poiché contiene la Import Address Table (IAT) necessaria per mappare le funzioni esterne e le librerie di sistema richiamate dal payload durante l'esecuzione.

notepad-classico.exe					
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Add
Byte[8]	Dword	Dword	Dword	Dword	Dword
.text	00007748	00001000	00007800	00000400	00000000
.data	00001BA8	00009000	00000800	00007C00	00000000
.rsrc	00008DB4	0000B000	00008E00	00008400	00000000
.text	0002B6AC	00014000	0002B800	00011200	00000000
.idata	0000113E	00040000	00001200	0003CA00	00000000
.rsrc	00008DB0	00042000	00008E00	0003DC00	00000000

4. Analisi delle Dipendenze (Import Directory)

L'analisi della **Import Directory** permette di comprendere quali librerie di sistema (.dll) il programma richiama per interagire con il sistema operativo.

Questa analisi conferma che il malware tenta di mimetizzarsi come un'applicazione legittima utilizzando librerie di sistema standard, ma include moduli critici per attività di rete malevole.

- **Librerie di Supporto Legittimo:** Il file importa **KERNEL32.dll** (gestione memoria e processi), **USER32.dll** (interfaccia utente), **GDI32.dll** (grafica) e **COMDLG32.dll** (finestre di dialogo standard come "Apri/Salva").
- **Indicatore di Rete (C2):** La presenza di **WS2_32.dll** (Windows Socket Library) è un indicatore critico per un editor di testo, in quanto permette al malware di stabilire connessioni di rete per il controllo remoto.

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name
szAnsi	(nFunctions)	Dword	Dword	Dword	Dwo
comdlg32.dll	9	000400C8	00000000	FFFFFFF	0004
SHELL32.dll	4	000400F0	00000000	FFFFFFF	0004
WINSPOOL.DRV	3	00040104	00000000	FFFFFFF	0004
COMCTL32.dll	1	00040114	00000000	FFFFFFF	0004
msvcr.dll	22	0004011C	00000000	FFFFFFF	0004
ADVAPI32.dll	7	00040178	00000000	FFFFFFF	0004
KERNEL32.dll	57	00040198	00000000	FFFFFFF	0004
GDI32.dll	24	00040280	00000000	FFFFFFF	0004
USER32.dll	74	000402E4	00000000	FFFFFFF	0004

5. Mapping Tattiche e Tecniche MITRE ATT&CK®

Il comportamento analizzato è stato mappato secondo il framework internazionale MITRE ATT&CK® per categorizzare le fasi dell'attacco e le metodologie utilizzate dall'avversario. In base all'analisi statica e alle caratteristiche del payload rilevato, l'attacco segue questo schema operativo:

- **Initial Access:** Il file viene probabilmente distribuito come allegato email malevolo, sfruttando tecniche di social engineering per indurre l'utente all'apertura.
- **Execution :** L'attivazione del payload malevolo dipende interamente dall'esecuzione manuale del file da parte della vittima, infatti ha inizio solo se l'utente clicca direttamente sul file.
- **Defense Evasion:** Il malware usurpa l'identità di un processo di sistema fidato (`notepad.exe`) per ridurre i sospetti e mimetizzarsi tra i processi legittimi.
- **Defense Evasion:** L'inserimento di sezioni duplicate (`.text` e `.rsrc`) è una tecnica di offuscamento strutturale mirata a rendere più complessa l'analisi statica e l'individuazione del codice malevolo.
- **Command and Control:** La comunicazione con l'esterno avviene tramite una connessione TCP grezza per inviare e ricevere comandi direttamente dal server dell'attaccante.
- **Command and Control:** Il malware può avvolgere i propri comandi in protocolli personalizzati trasmessi sulla connessione TCP stabilita per esfiltrare dati o ricevere istruzioni.

La mappatura evidenzia come l'attacco, pur essendo tecnicamente accessibile tramite strumenti automatizzati come `msfvenom`, segua una catena di esecuzione rigorosa e ampiamente documentata. Questo sottolinea l'efficacia di una strategia di **difesa multilivello**, capace di interrompere l'attacco in una qualsiasi delle fasi della "Kill Chain", dal rilevamento del mimetismo strutturale alla prevenzione delle connessioni di rete verso server non autorizzati.

6. Conclusioni

L'analisi conferma che `notepad-classico.exe` agisce come un **Trojan**, mantenendo le funzioni legittime di Notepad per ingannare l'utente mentre nasconde un payload malevolo. È stato generato tramite `msfvenom` con un payload di tipo **Stageless**, che risulta più semplice da analizzare per la ricchezza di indicatori statici presenti nel codice.

La prova definitiva della natura malevola risiede nella presenza della stringa `ws2_32.dll` e delle funzioni di rete associate in un editor di testo, confermando che il file è stato progettato per fornire a un attaccante il controllo remoto del sistema vittima.