

# Rapporto di Analisi Statica: notepad-classico.exe

**Data Analisi:** 3 Febbraio 2026

**Strumenti utilizzati:** pestudio 9.61 (Ambiente FLARE-VM)

**Hash SHA256:**

D2E6C9F9273663F3218BC07CBFB3B6F599FBCE7A4BA986F9BBFF77E3603988F2

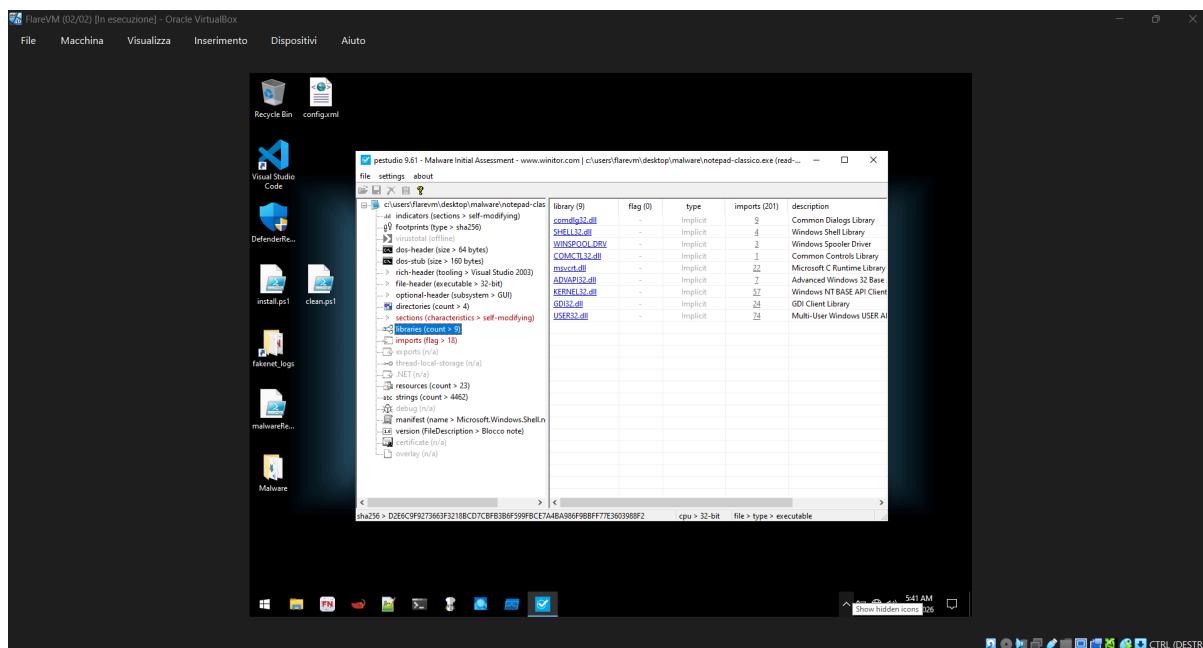
## 1) Introduzione

Il file analizzato si presenta come un editor di testo legittimo (Notepad), ma l'analisi della struttura PE (Portable Executable) rivela diverse anomalie critiche. La presenza di sezioni auto-modificanti e un entry-point spostato suggeriscono fortemente che il file sia un **Malware Packato** o che contenga uno **Shellcode** iniettato.

## 2) Analisi delle Librerie (Importazioni)

Il file importa **9 librerie** di sistema (DLL) in modo implicito, che forniscono le seguenti capacità potenziali:

- **Persistenza e Sistema:** *ADVAPI32.dll* (gestione registro/servizi) e *KERNEL32.dll* (gestione processi/memoria).
- **Interazione Utente:** *USER32.dll* (finestre/input tastiera) e *COMDLG32.dll* (finestre di dialogo).
- **Esecuzione Comandi:** *SHELL32.dll*, utilizzata per lanciare altri processi o manipolare file tramite la shell di Windows.



### 3) Analisi delle Sezioni (Anomalie Strutturali)

La tabella delle sezioni mostra una configurazione non standard per un binario Windows originale:

- **Sezioni Duplicare:** Sono presenti più sezioni con lo stesso nome (due `.text` e due `.rsrc`), indicando una manipolazione post-compilazione.
- **Caratteristica "Self-Modifying":** La sezione `section[3]` (denominata `.text`) possiede i flag di Scrittura ed Esecuzione simultanei. Questo è un indicatore primario di codice che si decompresse o si decripta in memoria durante l'esecuzione.
- **Entropia Elevata:** La `section[3]` presenta un'entropia di **6.214**, valore superiore alla norma per il codice sorgente standard, indicando dati compressi o offuscati.
- **Entry Point Sospetto:** L'esecuzione del programma non inizia nella sezione di codice originale, ma in `section[3]` all'indirizzo virtuale `0x00014000`.

The screenshot captures a Windows desktop environment where a virtual machine named "FlareVM (02/02)" is running under Oracle VM VirtualBox. The active application window is titled "FlareVM (02/02) [in esecuzione] - Oracle VirtualBox". It features a standard Windows menu bar with "File", "Macchina", "Visualizza", "Inserimento", "Dispositivi", and "Aiuto".

Below the menu bar, there's a command prompt or terminal area displaying the path "c:\users\flarevm\Desktop\malware\notepad-classic.exe" and some initial assessment results from VirusTotal.

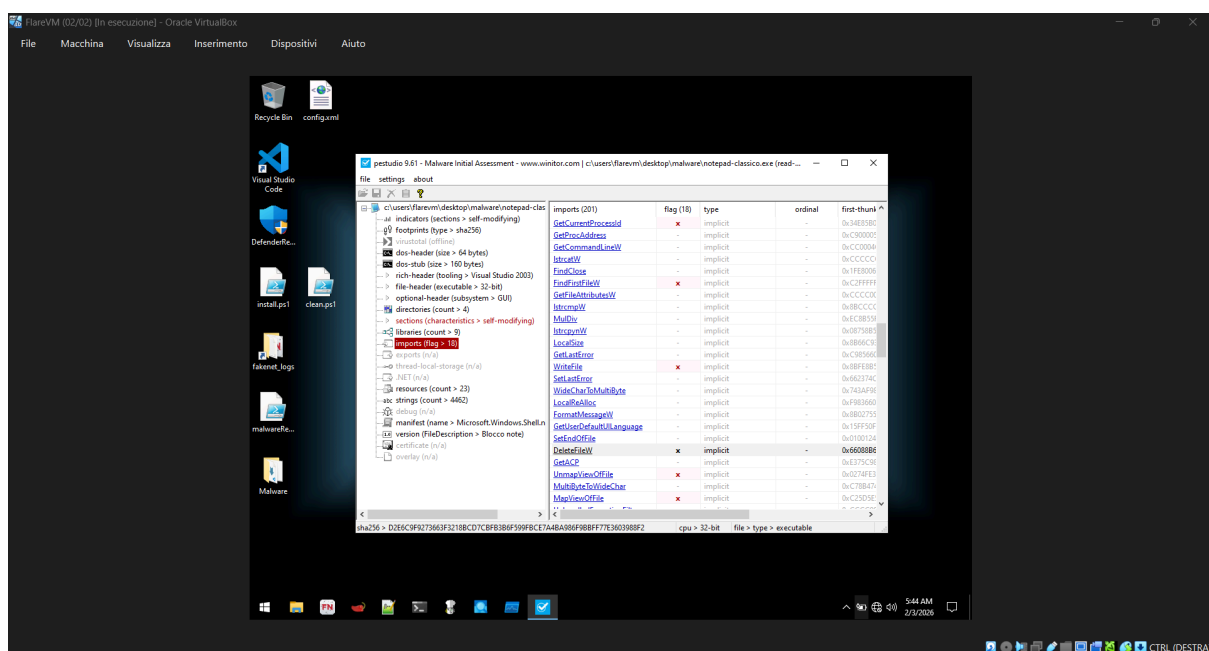
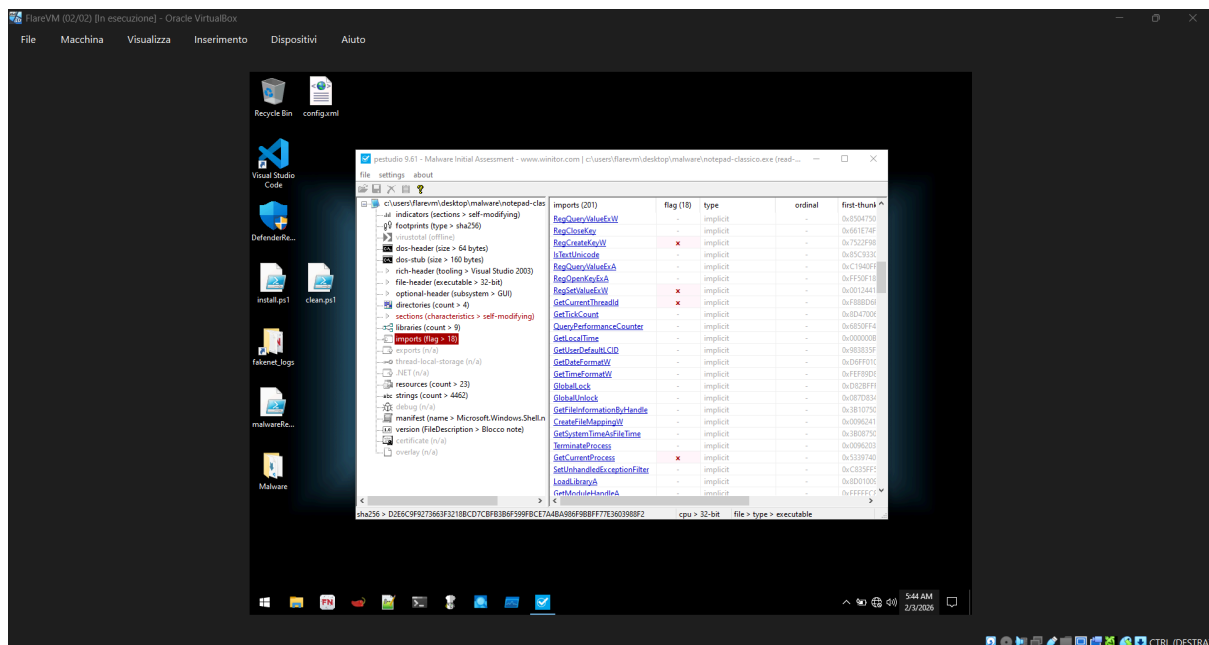
The main workspace is divided into two panes. The left pane shows a tree view of the file's metadata, including sections like "file-header", "optional-header", "resources", and "manifest". The right pane displays a detailed table of characteristics and items related to the file.

The table has columns for "property", "value", and "section". It lists various file properties such as "name", "md5", "entropy", "file size", "raw-address", "virtual-address", "characteristics", "items", and "entry-point". Each row provides specific details about these properties, often including hex values and offsets.

At the bottom of the window, a status bar provides additional context: "cpu ~ 32-bit", "file ~ type ~ executable", "subsystem ~ GUI", and "entry-point ~ 0x0014000".

#### 4) Indicatori di Compromissione (IoC)

- **Flag di Alert:** pestudio segnala oltre **18 importazioni critiche** (flag > 18) e più di **23 risorse** incluse nel file.
- **Mascheramento:** Il file utilizza metadati descrittivi ("Blocco note") per apparire come un componente di sistema legittimo.

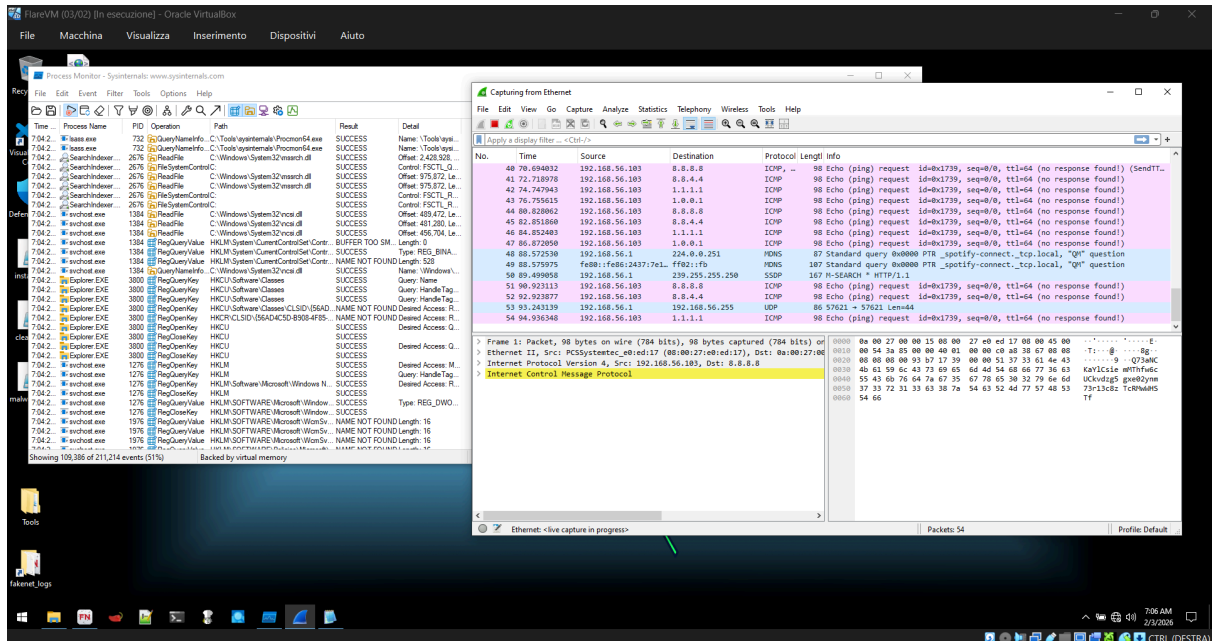


## 5) Conclusioni e Raccomandazioni

Il file è classificabile come **altamente sospetto**. La tecnica di self-modification rilevata indica che l'analisi statica non è sufficiente per vedere il carico pagante (payload) finale, poiché questo viene "scompattato" solo all'avvio.

## Prossimi passi suggeriti:

- **Analisi Dinamica:** Con Wireshark, abbiamo identificato il blocco note che prova ad andare su Internet pingando Cloudflare e Google.



- **Analisi delle Stringhe:** Esaminare la sezione "strings" di pestudio per cercare indirizzi IP, domini C2 o comandi PowerShell nascosti.