

Rapporto di Analisi Statica: notepad-classico.exe

Data Analisi: 3 Febbraio 2026

Strumenti utilizzati: pestudio 9.61 (Ambiente FLARE-VM)

Hash SHA256:

D2E6C9F9273663F3218BC07CBFB3B6F599FBCE7A4BA986F9BBFF77E3603988F2

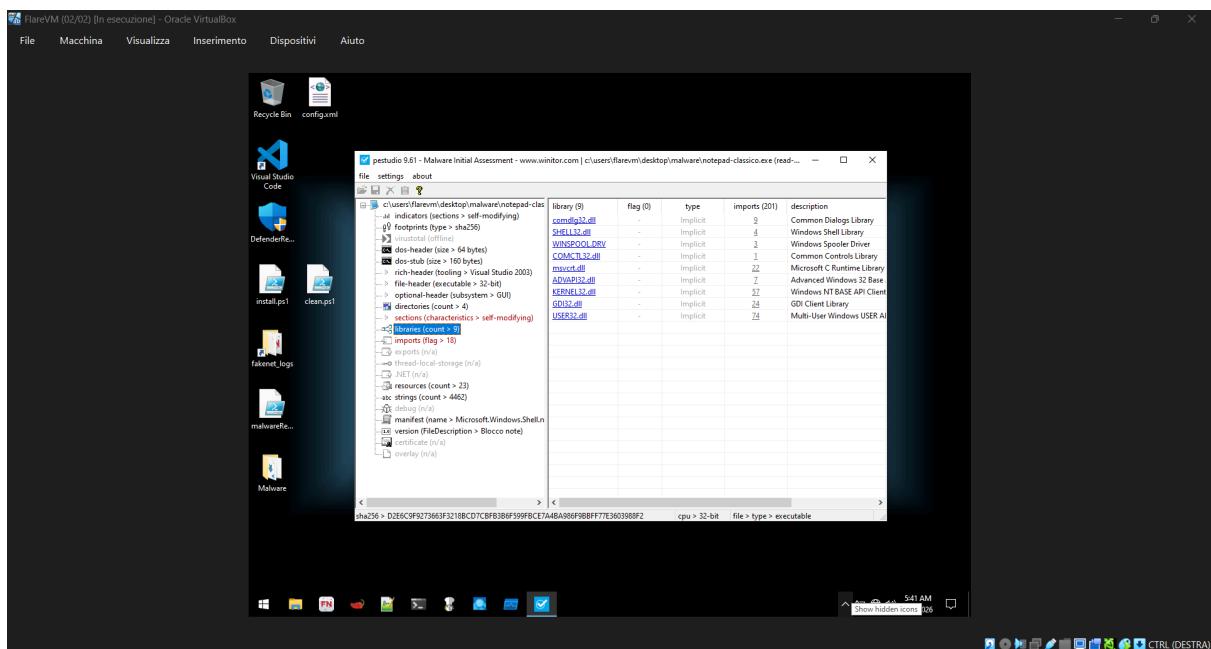
1) Introduzione

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:

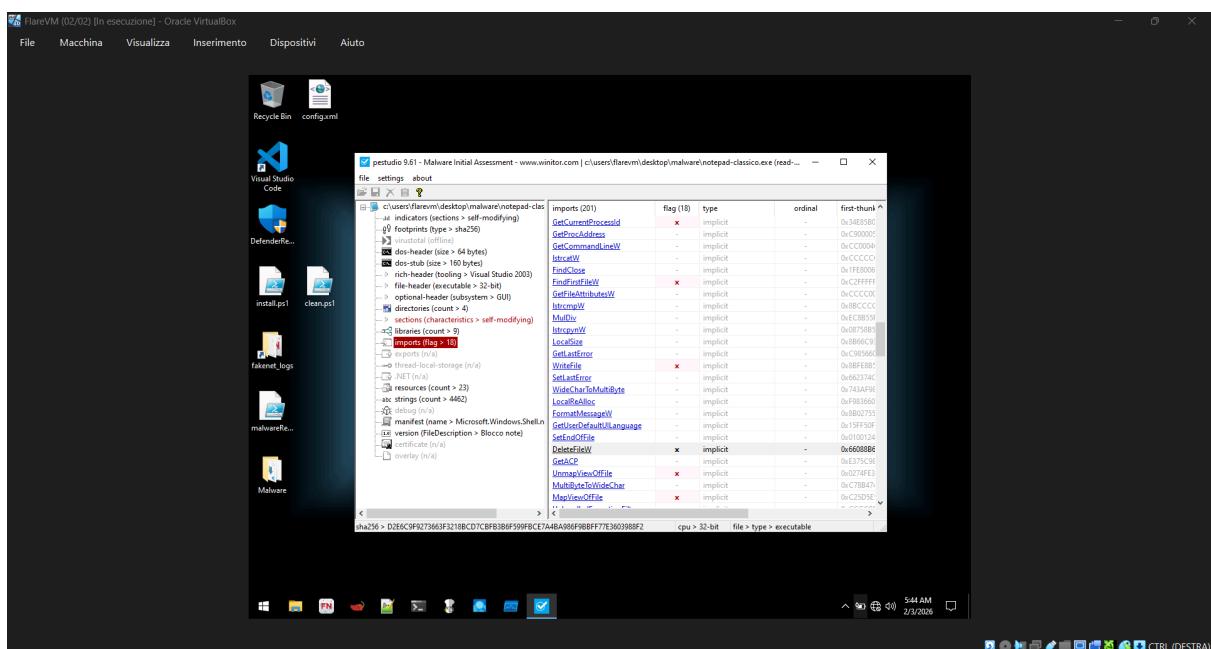
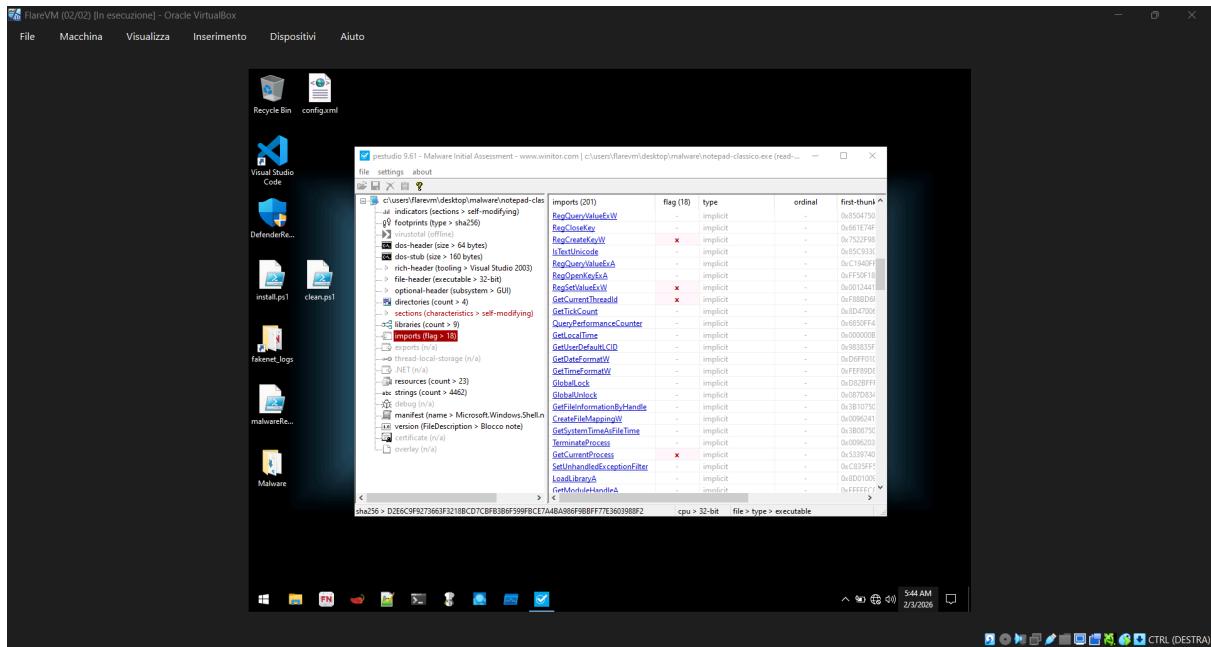
- **Sezioni Duplicate:** Sono presenti più sezioni con lo stesso nome (due `.text` e due `.rsrc`), indicando una manipolazione post-compilazione.
- **Caratteristica "Self-Modifying":** La sezione `section[3]` (denominata `.text`) possiede i flag di Scrittura ed Esecuzione simultanei. Questo è un indicatore primario di codice che si decomprime 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 shows the FlareVM interface with the following details:

- Title Bar:** FlareVM (02/02) [In esecuzione] - Oracle VirtualBox
- File Menu:** File, Macchina, Visualizza, Inserimento, Dispositivi, Aiuto
- Toolbar:** Includes icons for file operations (Open, Save, Print, etc.)
- Central Window:** Displays the file path: c:\users\flarevm\desktop\malware\notepad-clas... and the checked option "per tutto 9.61 - Malware Initial Assessment - www.wiinror.com | c:\users\flarevm\desktop\malware\notepad-classico.exe (read-only)".
- Left Sidebar:** Shows a tree view of the file structure, including:
 - Indicators (sections > self-modifying)
 - Footprints (type > sha256)
 - dos-header (size > 64 bytes)
 - dos-stub (size > 160 bytes)
 - file-refs (99.6%)
 - rich-header (tooling > Visual Studio 2003)
 - file-header (executable > 32-bit)
 - internal-header (filesystem > GZIP)
 - sections (characteristics > self-modifying)
 - libraries (count > 9)
 - imports (flag > 18)
 - exports (n/a)
 - resource storage (n/a)
 - NET (n/a)
 - resources (count > 23)
 - sec strings (count > 4462)
 - manifest (name > Microsoft.Windows.Shell
 - version (FileDescription > Blocco netd)
 - certificate (n/a)
 - overlay (n/a)
- Table View:** A large table showing section details across seven columns: property, value, value, value, value, value, value, section[0], section[1], section[2], section[3], section[4], section[5]. Key data points include:
 - name: .text, .rsrc, .text, .rsrc, .text, .rsrc
 - entropy: 6.214, 1.149, 5.421, 6.428, 5.439, 5.407
 - file-size: 10.35, 0.17%, 127.76, 61.59 %, 1.37%, 127.76
 - raw-address: (begin) 0x00000400, 0x00000C00, 0x00000400, 0x0001200, 0x0003CA00, 0x0003DC00
 - raw-size: (begin) 0x00007800 (30720 bytes), 0x00000000 (2048 bytes), 0x00003E00 (36352 bytes), 0x0002B800 (178176 bytes), 0x00001200 (4608 bytes), 0x00008E00 (36352 bytes)
 - virtual-address: (begin) 0x00010000, 0x00090000, 0x00098000, 0x00014000, 0x00040000, 0x00042000
 - virtual-size: (begin) 0x00007A80 (302414 bytes), 0x00001BA8 (7080 bytes), 0x00008D80 (36276 bytes), 0x0002B8AC (177836 bytes), 0x0000113E (4114 bytes), 0x00008D80 (36272 bytes)
- Bottom Status Bar:** Shows CPU: 32-bit, File: type > executable, Subsystem: GUI, Entry-point: 0x00014000. It also displays system status icons (Wi-Fi, battery, etc.) and a taskbar with various application icons.

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.

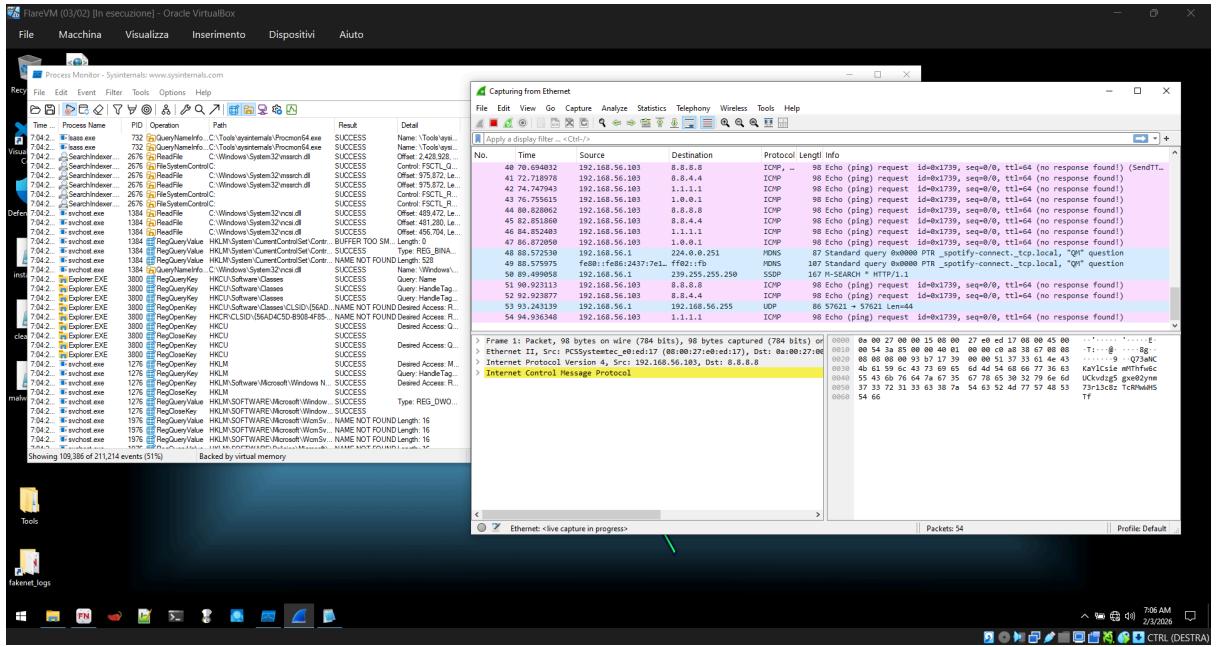


5) Conclusioni e Raccomandazioni

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.