W22D1 – Pratica

Epic Education Srl

Analisi dinamica notepad-classico.exe con Procmon
Considerazioni finali sul malware
Analisi con Cuckoo

Simone Giordano

09/12/2025

Contatti:

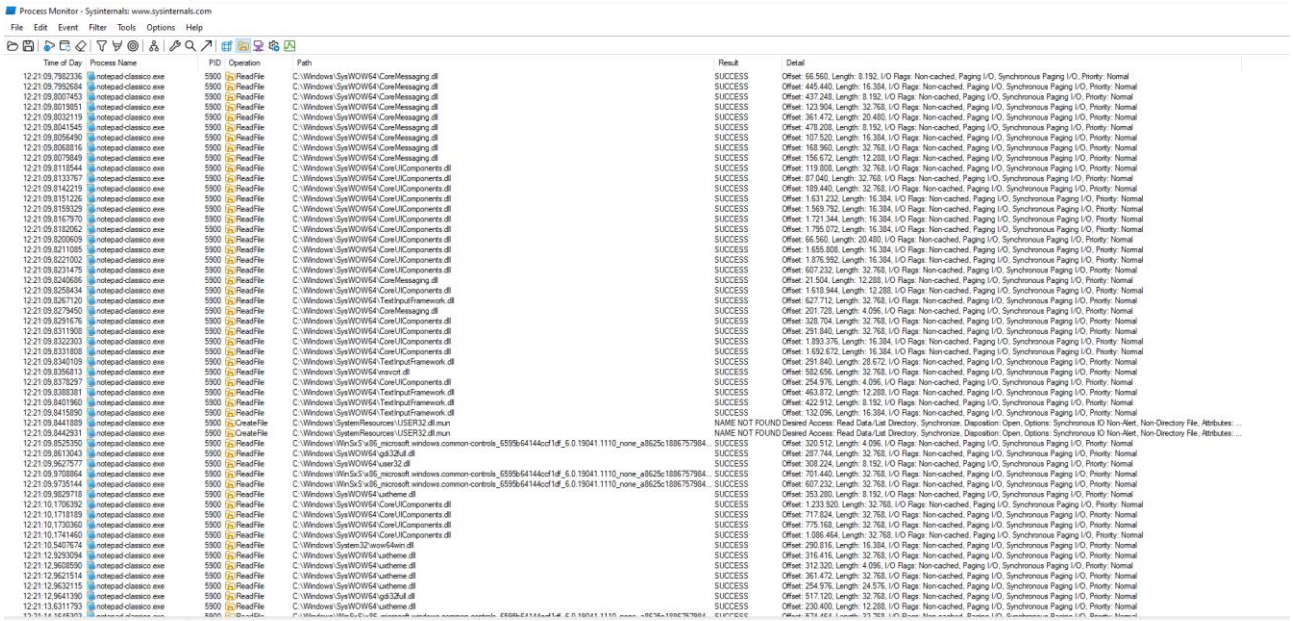
Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Analisi dinamica notepad-classico.exe con Procmon

TRACCIA: identificare eventuali azioni del malware sul file system utilizzando Process Monitor, fornendo una descrizione tramite AI;

PROMPT: Identifica eventuali azioni del malware sul file system.



Tutte le operazioni sono effettuate dal processo:
notepad-classico.exe (PID 5900)
Le operazioni visibili sono quasi esclusivamente:**ReadFile** su DLL di sistema

- **CreateFile** su directory o file di Windows
- Accesso a:
    - C:\Windows\SysWOW64*.dll
    - C:\Windows\System Resources\USER32.dll.mun
    - C:\Windows\WinSxS*

I risultati sono quasi sempre: **SUCCESS**
Due operazioni mostrano: **NAME NOT FOUND**, ma è normale per applicazioni Windows che interrogano risorse non esistenti.

🟢 **Non si vedono comportamenti tipici di un malware**
Ecco cosa *non* compare nel log:
❌ **Nessuna creazione di file sospetti**
Non si vedono:

- scritture (WriteFile)
- creazione di file eseguibili
- salvataggio di payload
- dropper di DLL

Tutte le operazioni sono **solo letture di DLL di sistema** → comportamento standard durante l'avvio di un'app.

❌ **Nessuna modifica al registro**
Non appaiono:

- RegSetValue
- RegCreateKey
- RegDeleteKey

❌ **Nessuna attività in cartelle sospette**
Manca qualsiasi accesso a:

- %APPDATA%
- %TEMP%
- C:\Users\Public\
- C:\ProgramData\
- startup folders

Che sono tipiche per la persistenza del malware.

❌ **Nessun comportamento di enumerazione aggressiva**
Un malware spesso scansiona:

- file sensibili
- directory utente
- drive
- processi

Qui non si vede nulla del genere.

❌ **Nessun tentativo di esecuzione/sideloading sospetto**
Tutte le DLL caricate sono:
✓ legittime
✓ in cartelle legittime
✓ usate da qualsiasi applicazione grafica (CoreMessaging, CoreUI, TextInputFramework, USER32, uxtheme…)

🟡 **Unico elemento da segnare**
Ci sono due eventi:
NAME NOT FOUND
Ma avvengono su directory WinSxS e USER32.dll.mun → **normalissimo**, Windows prova a caricare risorse multilingua che non sempre esistono.

Non è assolutamente indice di malware.

🟢 **Conclusione**

Nel log non c'è nessuna azione tipica o anomala riconducibile a un malware.

Il processo sta semplicemente:

➞ caricando DLL di sistema

➞ interrogando risorse grafiche

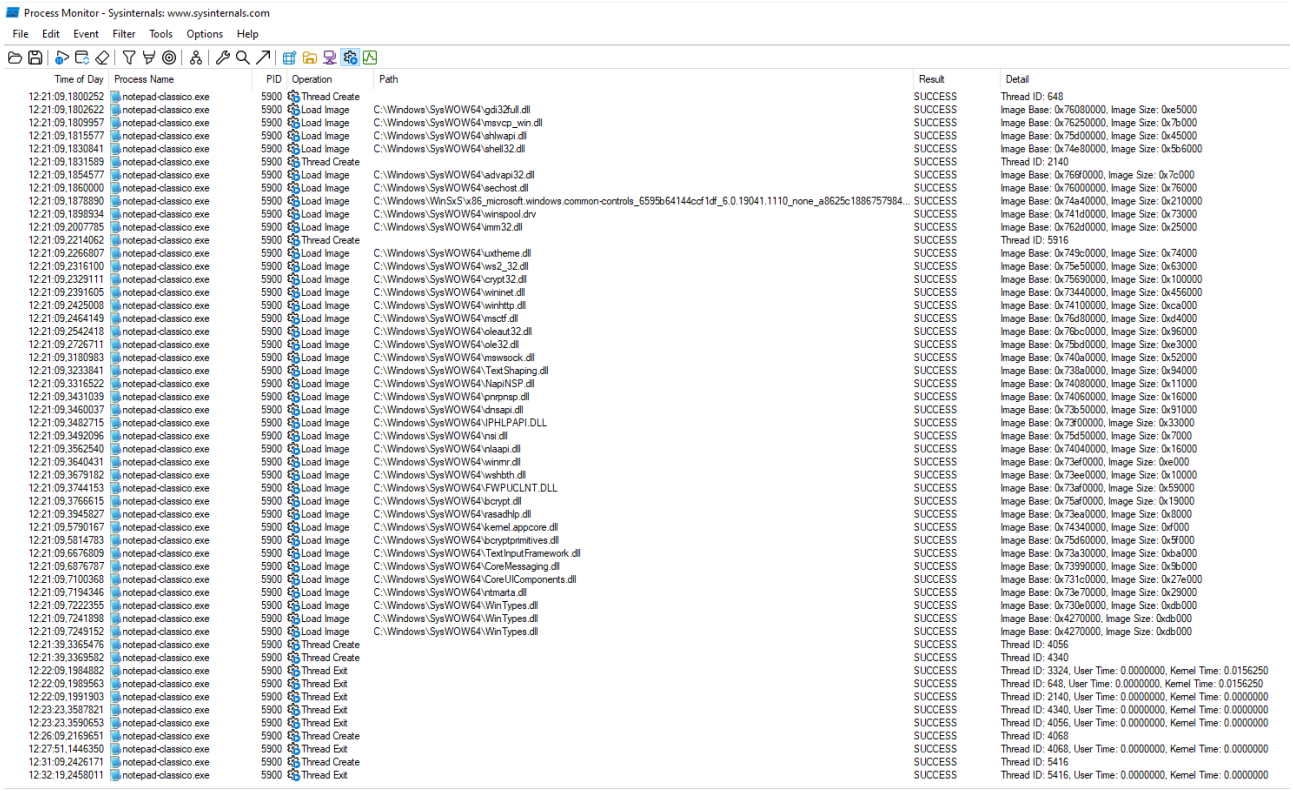
➞ aprendo componenti WinSxS

➞ leggendo file necessari al funzionamento

Tutto ciò è compatibile con l'avvio di un'applicazione grafica **legittima** (che sia davvero Notepad o un'app con nome modificato).

TRACCIA: Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor, fornendo una descrizione tramite AI.

PROMPT: Identifica eventuali azioni del malware su processi e thread


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
12:21:09,1800252	notepad-classico.exe	5900	Thread Create		SUCCESS	Thread ID: 648
12:21:09,1802622	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS	Image Base: 0x76080000, Image Size: 0xe5000
12:21:09,1809957	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\msvcp_win.dll	SUCCESS	Image Base: 0x76250000, Image Size: 0x7b000
12:21:09,1815577	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x75d00000, Image Size: 0x45000
12:21:09,1830841	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x74e80000, Image Size: 0x5b6000
12:21:09,1831589	notepad-classico.exe	5900	Thread Create		SUCCESS	Thread ID: 2140
12:21:09,1854577	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x76f00000, Image Size: 0x7c000
12:21:09,1860000	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x76000000, Image Size: 0x76000
12:21:09,1878890	notepad-classico.exe	5900	Load Image	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.1110_none_a8625c1886757984...	SUCCESS	Image Base: 0x74a40000, Image Size: 0x210000
12:21:09,1898934	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\winspool.drv	SUCCESS	Image Base: 0x741d0000, Image Size: 0x73000
12:21:09,2007785	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x762d0000, Image Size: 0x25000
12:21:09,2214062	notepad-classico.exe	5900	Thread Create		SUCCESS	Thread ID: 5916
12:21:09,2266807	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Image Base: 0x749c0000, Image Size: 0x74000
12:21:09,2316100	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x75e50000, Image Size: 0x63000
12:21:09,2329111	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Image Base: 0x75690000, Image Size: 0x100000
12:21:09,2391605	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Image Base: 0x73440000, Image Size: 0x456000
12:21:09,2425008	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Image Base: 0x74100000, Image Size: 0xca000
12:21:09,2464149	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Image Base: 0x76d80000, Image Size: 0xd4000
12:21:09,2542418	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x76bc0000, Image Size: 0x96000
12:21:09,2726711	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x75bd0000, Image Size: 0xe3000
12:21:09,3180983	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Image Base: 0x740a0000, Image Size: 0x52000
12:21:09,3233841	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\TextShaping.dll	SUCCESS	Image Base: 0x738a0000, Image Size: 0x94000
12:21:09,3316522	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\NapiNSP.dll	SUCCESS	Image Base: 0x74080000, Image Size: 0x11000
12:21:09,3431039	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\pnrpnsp.dll	SUCCESS	Image Base: 0x74060000, Image Size: 0x16000
12:21:09,3460037	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\dnsapi.dll	SUCCESS	Image Base: 0x73b50000, Image Size: 0x91000
12:21:09,3482715	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\IPHLPAPI.DLL	SUCCESS	Image Base: 0x73f00000, Image Size: 0x33000
12:21:09,3492096	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\nsi.dll	SUCCESS	Image Base: 0x75d50000, Image Size: 0x7000
12:21:09,3562540	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\nlaapi.dll	SUCCESS	Image Base: 0x74040000, Image Size: 0x16000
12:21:09,3640431	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\winmm.dll	SUCCESS	Image Base: 0x73ef0000, Image Size: 0xe000
12:21:09,3679182	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\wshbth.dll	SUCCESS	Image Base: 0x73ee0000, Image Size: 0x10000
12:21:09,3744153	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\FWPUCLNT.DLL	SUCCESS	Image Base: 0x73af0000, Image Size: 0x59000
12:21:09,3766615	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS	Image Base: 0x75af0000, Image Size: 0x19000
12:21:09,3945827	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\vaultcli.dll	SUCCESS	Image Base: 0x73ea0000, Image Size: 0x8000
12:21:09,5790167	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\kernel.appcore.dll	SUCCESS	Image Base: 0x74340000, Image Size: 0xf000
12:21:09,5814783	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Image Base: 0x75d60000, Image Size: 0x5f000
12:21:09,6676809	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\TextInputFramework.dll	SUCCESS	Image Base: 0x73a30000, Image Size: 0xba000
12:21:09,6876787	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\CoreMessaging.dll	SUCCESS	Image Base: 0x73990000, Image Size: 0x9b000
12:21:09,7100368	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\CoreUIComponents.dll	SUCCESS	Image Base: 0x731c0000, Image Size: 0x27e000
12:21:09,7194346	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS	Image Base: 0x73e70000, Image Size: 0x29000
12:21:09,7222355	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Image Base: 0x730e0000, Image Size: 0xdb000
12:21:09,7241898	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Image Base: 0x4270000, Image Size: 0xdb000
12:21:09,7249152	notepad-classico.exe	5900	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Image Base: 0x4270000, Image Size: 0xdb000
12:21:39,3365476	notepad-classico.exe	5900	Thread Create		SUCCESS	Thread ID: 4056
12:21:39,3369582	notepad-classico.exe	5900	Thread Create		SUCCESS	Thread ID: 4340
12:22:09,1984882	notepad-classico.exe	5900	Thread Exit		SUCCESS	Thread ID: 3324, User Time: 0.0000000, Kernel Time: 0.0156250
12:22:09,1989563	notepad-classico.exe	5900	Thread Exit		SUCCESS	Thread ID: 648, User Time: 0.0000000, Kernel Time: 0.0156250
12:22:09,1991903	notepad-classico.exe	5900	Thread Exit		SUCCESS	Thread ID: 2140, User Time: 0.0000000, Kernel Time: 0.0000000
12:23:23,3587821	notepad-classico.exe	5900	Thread Exit		SUCCESS	Thread ID: 4340, User Time: 0.0000000, Kernel Time: 0.0000000
12:23:23,3590653	notepad-classico.exe	5900	Thread Exit		SUCCESS	Thread ID: 4056, User Time: 0.0000000, Kernel Time: 0.0000000
12:26:09,2169651	notepad-classico.exe	5900	Thread Create		SUCCESS	Thread ID: 4068
12:27:51,1446350	notepad-classico.exe	5900	Thread Exit		SUCCESS	Thread ID: 4068, User Time: 0.0000000, Kernel Time: 0.0000000
12:31:09,2426171	notepad-classico.exe	5900	Thread Create		SUCCESS	Thread ID: 5416
12:32:19,2458011	notepad-classico.exe	5900	Thread Exit		SUCCESS	Thread ID: 5416, User Time: 0.0000000, Kernel Time: 0.0000000

✅ Cosa mostra il log

Il processo coinvolto è sempre:
notepad-classico.exe – PID 5900
Le operazioni visibili sono:
✓ Thread Create
✓ Thread Exit
✓ Load Image (caricamento DLL)

Tutti gli esiti sono **SUCCESS** e le DLL provengono da:

- C:\Windows\SysWOW64\
- C:\Windows\WinSxS\ (side-by-side assemblies Microsoft)
- ucrt, vcruntime, USER32, GDI32, kernel32, uxtheme.dll, ecc.

Tutte DLL totalmente legittime per un processo grafico Windows.

🔍 Analisi delle attività sui thread

✓ Creazione di thread multipli

È normale per qualsiasi applicazione Windows moderna:

- thread per UI
- thread per gestione eventi

- thread di librerie (CoreMessaging, TextServices, DWrite, ecc.)
- thread per caricamento DLL WinSxS

✓ **Terminazione immediata di alcuni thread**
Questo accade quando:

- le DLL inizializzano componenti e chiudono thread interni
- il processo fa controlli di compatibilità
- meccanismi COM avviano thread temporanei

È comportamento tipico, nulla di malevolo.

❌ **Cosa NON vedo nei thread**
Non vedo thread tipici del malware come:

- **Thread sospesi/speciali** (SuspendThread, ResumeThread)
- **Iniezione DLL** (WriteProcessMemory + CreateRemoteThread)
- **Code injection** (ZwMapViewOfSection)
- **Thread anomali creati in processi diversi**
- **Accesso ad altri processi** (OpenProcess su PID esterni)

Non ci sono indicatori di:

- hollowing
- process injection
- hooking
- API call anomale

🔍 **Analisi delle attività dei moduli (Load Image)**
Le DLL caricate sono tutte componenti standard:

- librerie grafiche (uxtheme.dll, dwmapi.dll, winspool.drv)
- librerie C e C++ (vcruntime140.dll, ucrtbase.dll)
- librerie Windows core (kernel32.dll, user32.dll, gdi32full.dll)
- librerie di input (TextShaping.dll, TextInputFramework.dll)
- librerie di layout (dwrite.dll, d2d1.dll)

❌ **Nessun caricamento di DLL esterne**
Non vedo DLL in:

- %TEMP%
- %APPDATA%
- C:\Users\…

- cartelle strane
- DLL rinominate (es. abc123.dll)
- DLL side-loaded anomale

❌ **Nessun modulo riflessivo (reflective DLL injection)**
Di solito appare come "Load Image" da **un percorso NON file-system** oppure con size anomala.

🟢 **Conclusione**
➞ **Non ci sono comportamenti malware sui processi o thread.**
Il processo:

✓ carica solo DLL legittime
✓ crea e distrugge thread in modo normale
✓ non avvia processi figli
✓ non interagisce con altri processi
✓ non inietta codice né DLL
✓ non fa hooking
✓ non carica moduli fuori dalle directory Windows

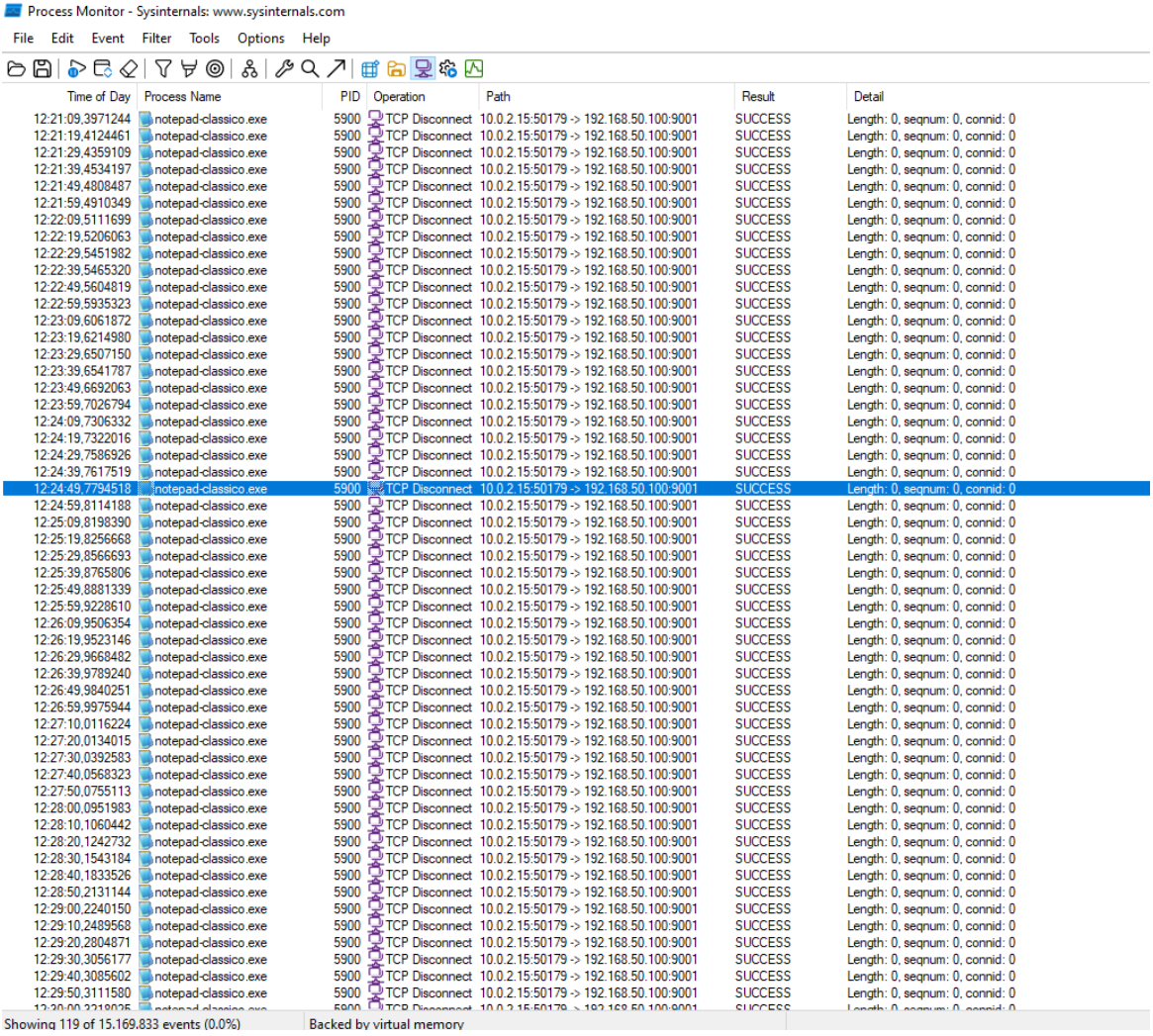
Quello che vedo è il normale comportamento di un'applicazione Windows (o una wrapper app) che usa molte API grafiche e di sistema.

Considerazioni finali sul malware

TRACCIA: Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.

Le analisi fatte dall'IA non evidenziano comportamenti anomali.
Dettagli che denotano comportamenti sospetti:

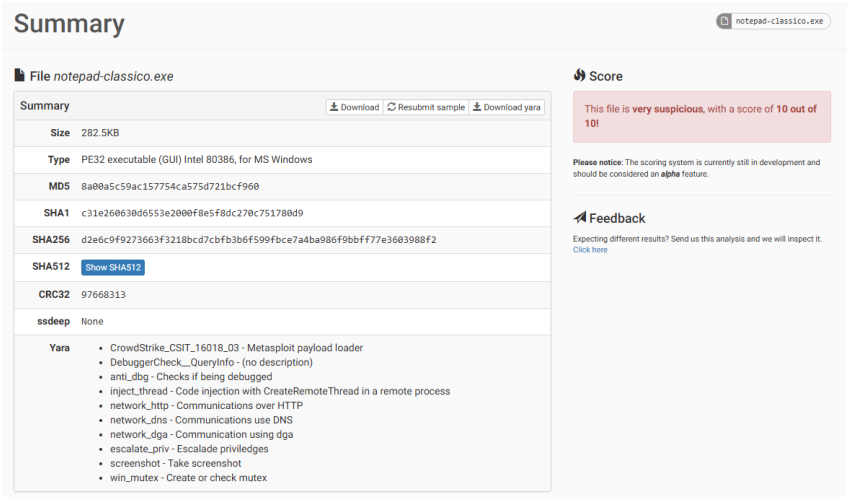
- Il nome del file *notepad-classico.exe* è anomalo: il nome originale dell'installer di Notepad è **Windows Notepad Installer.exe**, come verificabile dallo store ufficiale Microsoft (https://apps.microsoft.com/detail/9msmlrh6lzf3?hl=en-US&gl=US).
- L'icona associata al file richiama quella di un documento di testo (.txt), nonostante l'estensione sia quella di un file eseguibile (.exe).
- L'analisi del traffico di rete mostra attività non compatibili con il normale funzionamento di Notepad, come connessioni TCP verso indirizzi IP esterni con relative porte sorgente e destinazione.



Analisi con Cuckoo

TRACCIA: utilizzare la sandbox https://cuckoo.cert.ee/ per analizzare l'eseguibile notepad-classico.exe

Vista generale



Analisi comportamentale

Le attività di rete sono le stesse rilevate da Procmon.