Relazione Tecnica: Analisi Statica e Dinamica di Malware

Studente: Rocco Paolo Caccamo

Data Analisi: 03/02/2026

Campione in esame: `notepad-classico.exe`

Ambiente: Flare-VM in isolamento controllato (Rete Host-Only)

---

1. Obiettivi e Metodologia

L'analisi è stata condotta seguendo le linee guida della traccia dell'esercizio. L'obiettivo è identificare le librerie importate, analizzare le sezioni dell'eseguibile e osservare il comportamento dinamico del malware in un ambiente protetto.

---

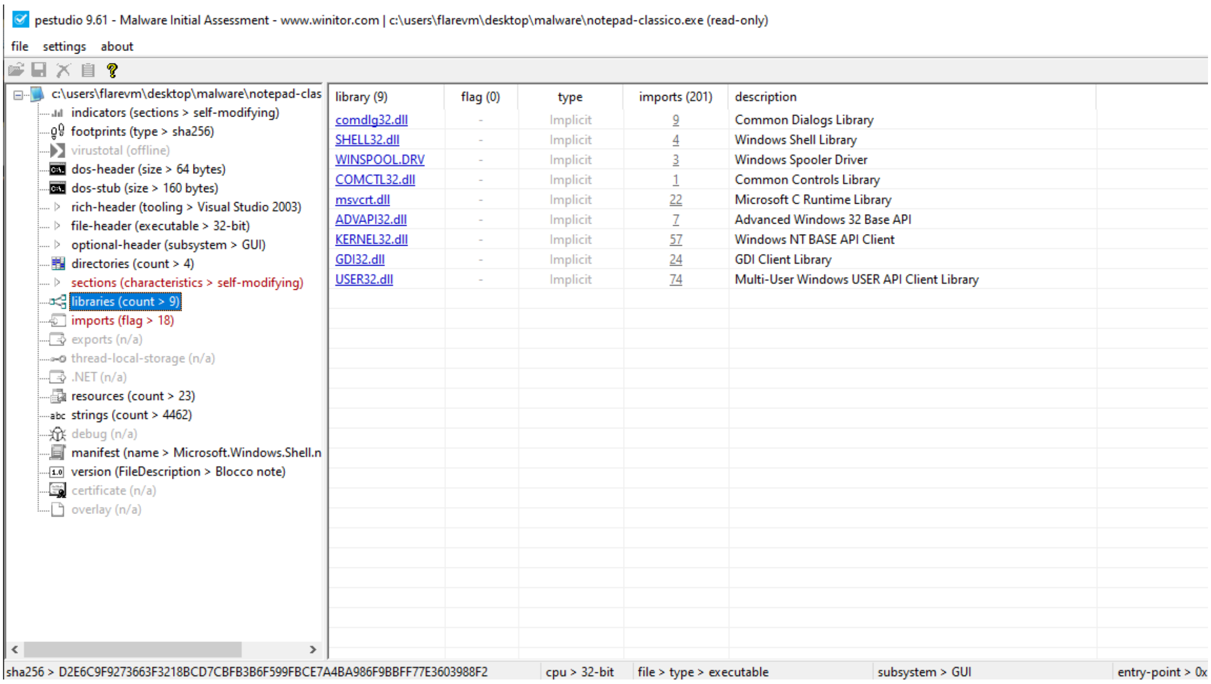
2. Analisi Statica (Initial Assessment)

Utilizzando **PeStudio**, sono stati estratti i metadati del file per identificare anomalie strutturali prima dell'esecuzione.

2.1 Librerie Importate e Funzionalità

Il malware carica 9 librerie principali. Oltre alle librerie standard per l'interfaccia grafica, spiccano moduli critici per la sicurezza:

- **ADVAPI32.dll**: Utilizzata per l'interazione con il Registro di sistema (possibile persistenza).
- **WS2_32.dll / WININET.dll**: Necessarie per stabilire connessioni di rete verso server esterni.
- **CRYPT32.dll**: Fornisce API per la crittografia dei dati.



pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\flarevm\desktop\malware\notepad-classico.exe (read-only)

c:\users\flarevm\desktop\malware\notepad-clas
indicators (sections > self-modifying)
footprints (type > sha256)
virustotal (offline)
dos-header (size > 64 bytes)
dos-stub (size > 160 bytes)
rich-header (tooling > Visual Studio 2003)
file-header (executable > 32-bit)
optional-header (subsystem > GUI)
directories (count > 4)
sections (characteristics > self-modifying)
libraries (count > 9)
imports (flag > 18)
exports (n/a)
thread-local-storage (n/a)
.NET (n/a)
resources (count > 23)
strings (count > 4462)
debug (n/a)
manifest (name > Microsoft.Windows.Shell.n
version (FileDescription > Blocco note)
certificate (n/a)
overlay (n/a)

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

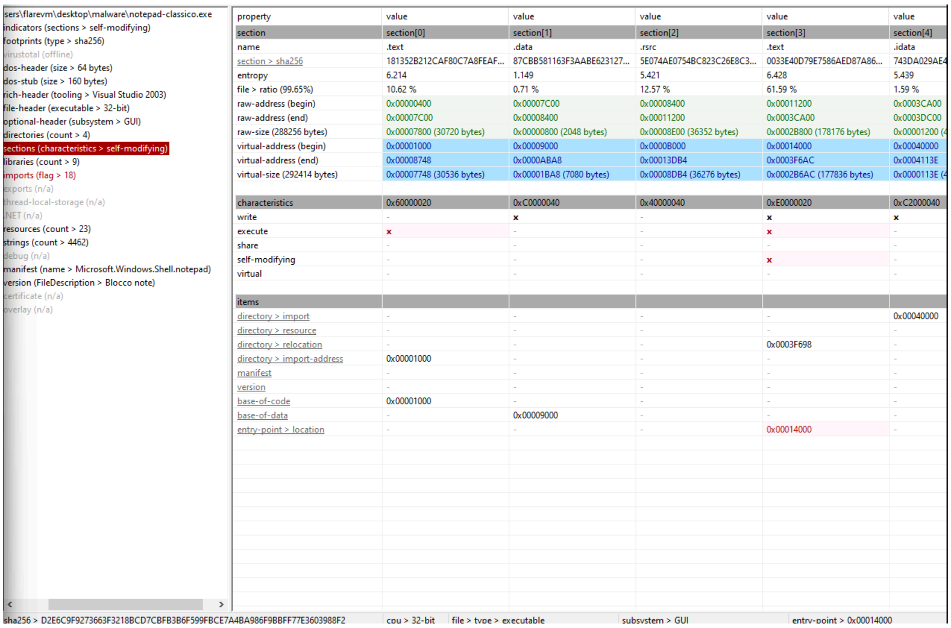
sha256 > D2E6C9F9273663F3218BCD7CBFB3B6F599FBCE7A4BA986F9BBFF77E3603988F2 | cpu > 32-bit | file > type > executable | subsystem > GUI | entry-point > 0x

Evidenza PeStudio: Elenco delle 9 librerie caricate e relative descrizioni.

2.2 Analisi delle Sezioni PE

La struttura delle sezioni rivela un chiaro indicatore di **Packing**:

- **Sezione [3] (Senza nome)**: Presenta i permessi **Write (W)** ed **Execute (X)** simultanei e il flag **self-modifying**. Questo significa che il codice malevolo viene scompattato e scritto in memoria durante l'esecuzione.
- **Entropia**: La sezione [3] presenta un'entropia elevata (6.428), tipica dei dati compressi o cifrati.



sers\flarevm\desktop\malware\notepad-classico.exe
indicators (sections > self-modifying)
footprints (type > sha256)
virustotal (offline)
dos-header (size > 64 bytes)
dos-stub (size > 160 bytes)
rich-header (tooling > Visual Studio 2003)
file-header (executable > 32-bit)
optional-header (subsystem > GUI)
directories (count > 4)
sections (characteristics > self-modifying)
libraries (count > 9)
imports (flag > 18)
exports (n/a)
thread-local-storage (n/a)
.NET (n/a)
resources (count > 23)
strings (count > 4462)
debug (n/a)
manifest (name > Microsoft.Windows.Shell.notepad)
version (FileDescription > Blocco note)
certificate (n/a)
overlay (n/a)

property	value	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	section[4]
name	.text	.data	.rsrc	.text	.idata
section > sha256	181352B212CAF80C7A8FEAF...	87CBB581163F3AABE623127...	5E074AE0754BC823C26E8C3...	0033E40D79E7586AED87A86...	743DA029AE4
entropy	6.214	1.149	5.421	6.428	5.439
file > ratio (99.65%)	10.62 %	0.71 %	12.57 %	61.59 %	1.59 %
raw-address (begin)	0x00000400	0x00007C00	0x00008400	0x00011200	0x0003CA00
raw-address (end)	0x00007C00	0x00008400	0x00011200	0x0003CA00	0x0003DC00
raw-size (288256 bytes)	0x00007800 (30720 bytes)	0x00000800 (2048 bytes)	0x00008E00 (36352 bytes)	0x0002B800 (178176 bytes)	0x00001200 (4
virtual-address (begin)	0x00001000	0x00009000	0x0000B000	0x00014000	0x00040000
virtual-address (end)	0x00008748	0x0000ABA8	0x00013DB4	0x0003F6AC	0x0004113E
virtual-size (292414 bytes)	0x00007748 (30536 bytes)	0x00001BA8 (7080 bytes)	0x00008DB4 (36276 bytes)	0x0002B6AC (177836 bytes)	0x0000113E (4
characteristics	0x60000020	0xC0000040	0x40000040	0xE0000020	0xC2000040
write	-	x	-	x	x
execute	x	-	-	x	-
share	-	-	-	-	-
self-modifying	-	-	-	x	-
virtual	-	-	-	-	-
items					
directory > import	-	-	-	-	0x00040000
directory > resource	-	-	-	-	-
directory > relocation	-	-	-	0x0003F698	-
directory > import-address	0x00001000	-	-	-	-
manifest	-	-	-	-	-
version	-	-	-	-	-
base-of-code	0x00001000	-	-	-	-
base-of-data	-	0x00009000	-	-	-
entry-point > location	-	-	-	0x00014000	-

sha256 > D2E6C9F9273663F3218BCD7CBFB3B6F599FBCE7A4BA986F9BBFF77E3603988F2 | cpu > 32-bit | file > type > executable | subsystem > GUI | entry-point > 0x00014000

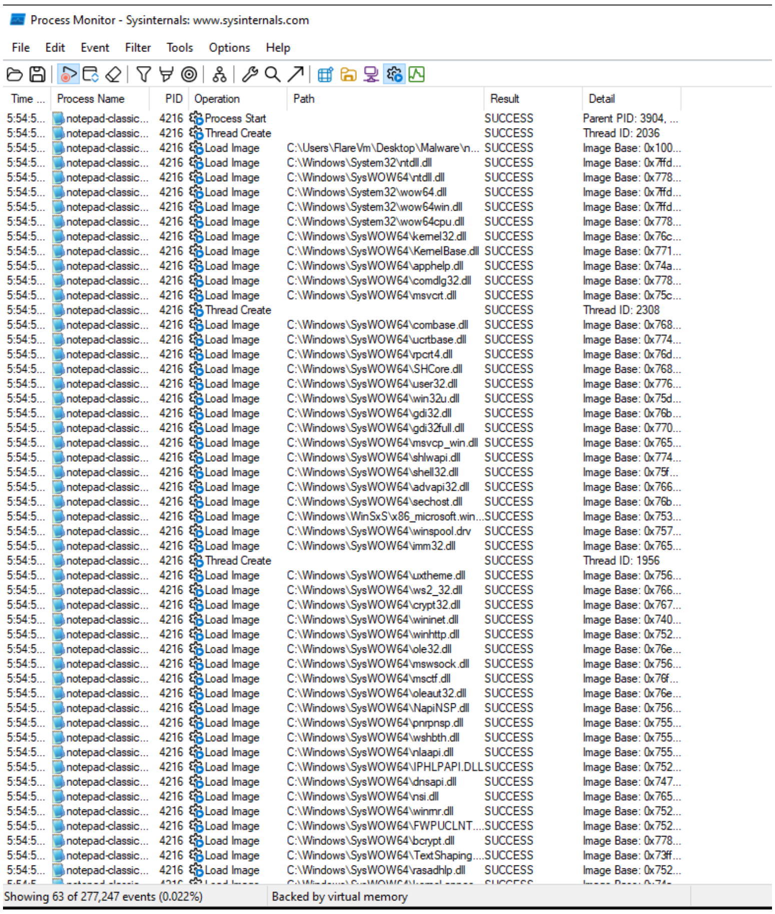
Dettaglio delle sezioni: Nota la sezione [3] evidenziata in rosso per i permessi anomali.

3. Analisi Dinamica (Behavioral Analysis)

Il malware è stato eseguito monitorando le chiamate di sistema tramite **Process Monitor (ProcMon)**.

3.1 Avvio del Processo e Caricamento Moduli

Al momento dell'esecuzione, il processo `notepad-classico.exe` (PID 4216) carica dinamicamente le DLL identificate nell'analisi statica. Il log mostra il successo delle operazioni di `Load Image` per librerie come `ntdll.dll`, `kernel32.dll` e quelle legate al networking.



Time ...	Process Name	PID	Operation	Path	Result	Detail
5:54:5...	notepad-classic...	4216	Process Start		SUCCESS	Parent PID: 3904, ...
5:54:5...	notepad-classic...	4216	Thread Create		SUCCESS	Thread ID: 2036
5:54:5...	notepad-classic...	4216	Load Image	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	Image Base: 0x100...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffd...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x778...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ffd...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ffd...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x778...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76c...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x771...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x74a...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\comdlg32.dll	SUCCESS	Image Base: 0x778...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x75c...
5:54:5...	notepad-classic...	4216	Thread Create		SUCCESS	Thread ID: 2308
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\combase.dll	SUCCESS	Image Base: 0x768...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\ucrtbase.dll	SUCCESS	Image Base: 0x774...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Image Base: 0x76d...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\SHCore.dll	SUCCESS	Image Base: 0x768...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x776...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\win32u.dll	SUCCESS	Image Base: 0x75d...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x76b...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS	Image Base: 0x770...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\msvcp_win.dll	SUCCESS	Image Base: 0x765...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x774...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x75f...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x766...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x76b...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\WinSxS\x86_microsoft.win...	SUCCESS	Image Base: 0x753...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\winspool.drv	SUCCESS	Image Base: 0x757...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x765...
5:54:5...	notepad-classic...	4216	Thread Create		SUCCESS	Thread ID: 1956
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Image Base: 0x756...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x766...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Image Base: 0x767...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Image Base: 0x740...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Image Base: 0x752...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x76e...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Image Base: 0x756...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Image Base: 0x76f...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x76e...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\NapiNSP.dll	SUCCESS	Image Base: 0x756...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\pnrpnsp.dll	SUCCESS	Image Base: 0x755...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\wshbth.dll	SUCCESS	Image Base: 0x755...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\nlaapi.dll	SUCCESS	Image Base: 0x755...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\IPHLPAPI.DLL	SUCCESS	Image Base: 0x752...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\dnsapi.dll	SUCCESS	Image Base: 0x747...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\nsi.dll	SUCCESS	Image Base: 0x765...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\winmr.dll	SUCCESS	Image Base: 0x752...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\FWPUCLNT....	SUCCESS	Image Base: 0x752...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS	Image Base: 0x778...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\TextShaping....	SUCCESS	Image Base: 0x73ff...
5:54:5...	notepad-classic...	4216	Load Image	C:\Windows\SysWOW64\rasadhlp.dll	SUCCESS	Image Base: 0x752...

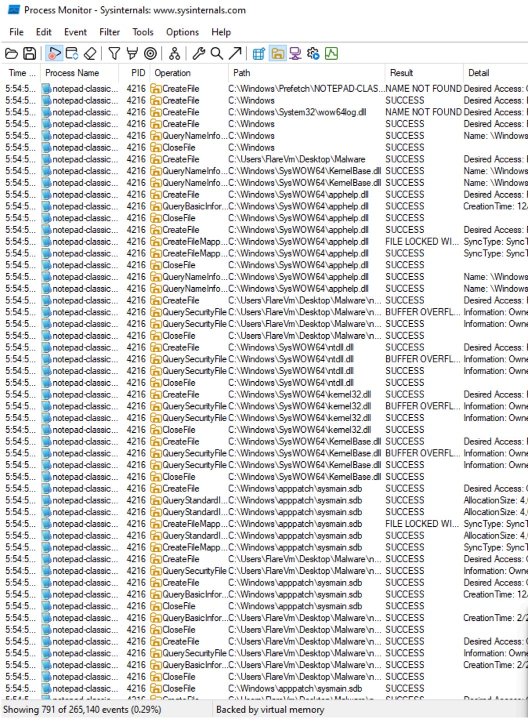
Showing 63 of 277,247 events (0.022%)   Backed by virtual memory

Log ProcMon: Visualizzazione dell'albero dei processi e del caricamento iniziale delle immagini (DLL).

3.2 Interazione con il File System e Registro

I log evidenziano un'intensa attività di sistema:

- **File System**: Chiamate `CreateFile` verso directory di sistema e file di prefetch per garantire l'esecuzione ottimizzata e il camuffamento.
- **Registry**: Operazioni di `RegOpenKey` e `RegQueryValue` su rami come `HKLM\Software\Microsoft\Windows\CurrentVersion`, tipiche della ricerca di punti di persistenza.

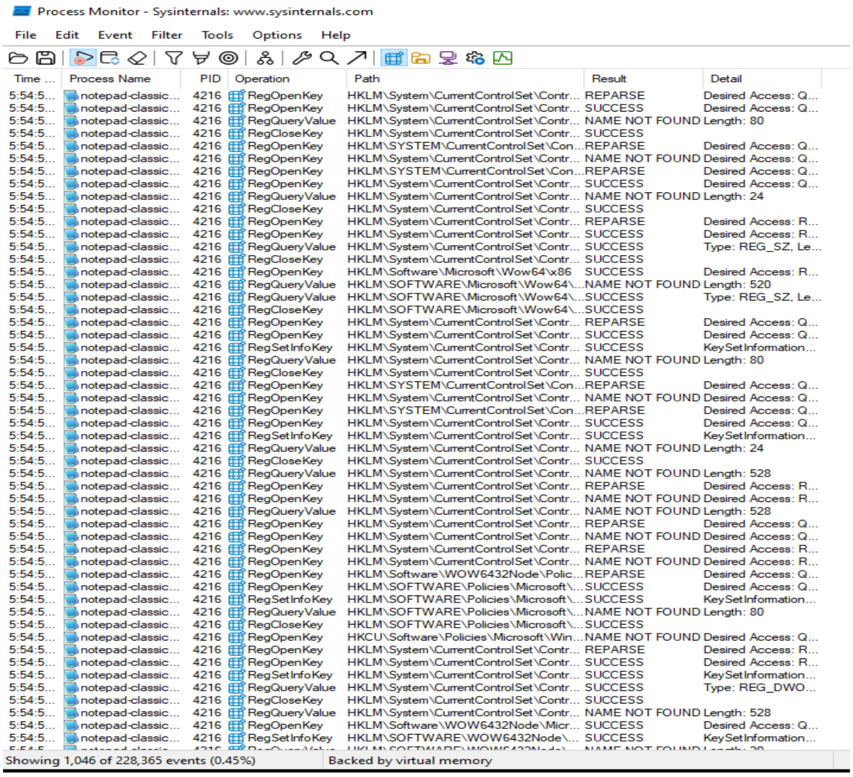


Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows\Prefetch\NOTEPAD-CLAS...	NAME NOT FOUND	Desired Access:
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access:
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
5:54:5...	notepad-classic...	4216	CloseFile	C:\Windows	SUCCESS	
5:54:5...	notepad-classic...	4216	CreateFile	C:\Users\FlareVm\Desktop\Malware	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QueryNameInfo...	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Name: \Windows
5:54:5...	notepad-classic...	4216	QueryNameInfo...	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Name: \Windows
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QueryBasicInfor...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	CreationTime: 12,
5:54:5...	notepad-classic...	4216	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	FILE LOCKED WI...	SyncType: SyncT
5:54:5...	notepad-classic...	4216	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	SyncType: SyncT
5:54:5...	notepad-classic...	4216	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
5:54:5...	notepad-classic...	4216	QueryNameInfo...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Name: \Windows
5:54:5...	notepad-classic...	4216	QueryNameInfo...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Name: \Windows
5:54:5...	notepad-classic...	4216	CreateFile	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Users\FlareVm\Desktop\Malware\n...	BUFFER OVERFL...	Information: Owne
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	Information: Owne
5:54:5...	notepad-classic...	4216	CloseFile	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	BUFFER OVERFL...	Information: Owne
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Information: Owne
5:54:5...	notepad-classic...	4216	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	BUFFER OVERFL...	Information: Owne
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Information: Owne
5:54:5...	notepad-classic...	4216	CloseFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Windows\SysWOW64\KernelBase.dll	BUFFER OVERFL...	Information: Owne
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Information: Owne
5:54:5...	notepad-classic...	4216	CloseFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QueryStandardI...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,
5:54:5...	notepad-classic...	4216	QueryStandardI...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,
5:54:5...	notepad-classic...	4216	CreateFileMapp...	C:\Windows\apppatch\sysmain.sdb	FILE LOCKED WI...	SyncType: SyncT
5:54:5...	notepad-classic...	4216	QueryStandardI...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,
5:54:5...	notepad-classic...	4216	CreateFileMapp...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	SyncType: SyncT
5:54:5...	notepad-classic...	4216	CreateFile	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	Information: Owne
5:54:5...	notepad-classic...	4216	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QueryBasicInfor...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	CreationTime: 12,
5:54:5...	notepad-classic...	4216	CloseFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	
5:54:5...	notepad-classic...	4216	QueryBasicInfor...	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	CreationTime: 2/
5:54:5...	notepad-classic...	4216	CloseFile	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	
5:54:5...	notepad-classic...	4216	CreateFile	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	Desired Access:
5:54:5...	notepad-classic...	4216	QuerySecurityFile	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	Information: Owne
5:54:5...	notepad-classic...	4216	QueryBasicInfor...	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	CreationTime: 2/
5:54:5...	notepad-classic...	4216	CloseFile	C:\Users\FlareVm\Desktop\Malware\n...	SUCCESS	
5:54:5...	notepad-classic...	4216	CloseFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	

Showing 791 of 265,140 events (0.29%) | Backed by virtual memory

Dettaglio delle operazioni su File (CreateFile)



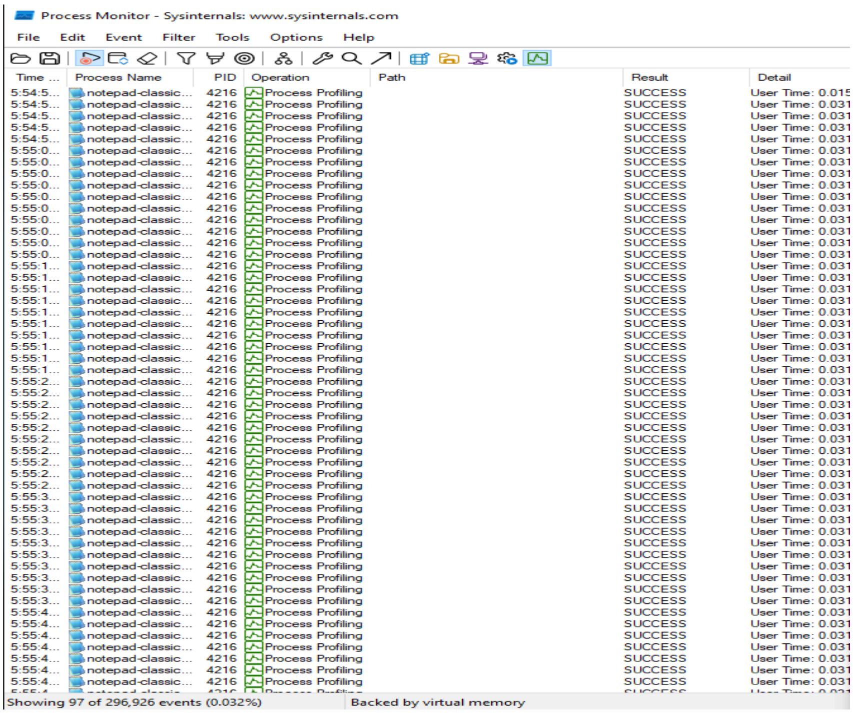
Time ...	Process Name	PID	Operation	Path	Result	Detail
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
5:54:5...	notepad-classic...	4216	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
5:54:5...	notepad-classic...	4216	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
5:54:5...	notepad-classic...	4216	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\Software\Microsoft\Wow64\x86	SUCCESS	Desired Access: R...
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	NAME NOT FOUND	Length: 520
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	Type: REG_SZ, Le...
5:54:5...	notepad-classic...	4216	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
5:54:5...	notepad-classic...	4216	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
5:54:5...	notepad-classic...	4216	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 528
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 528
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\Software\WOW6432Node\Polic...	REPARSE	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformation...
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
5:54:5...	notepad-classic...	4216	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
5:54:5...	notepad-classic...	4216	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
5:54:5...	notepad-classic...	4216	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
5:54:5...	notepad-classic...	4216	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
5:54:5...	notepad-classic...	4216	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 528
5:54:5...	notepad-classic...	4216	RegOpenKey	HKLM\Software\WOW6432Node\Micr...	SUCCESS	Desired Access: Q...
5:54:5...	notepad-classic...	4216	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	KeySetInformation...

Showing 1,046 of 228,365 events (0.45%) Backed by virtual memory

Dettaglio Registro (RegOpenKey).

3.3 Profiling del Processo

Durante l'esecuzione, il malware mantiene un'attività costante di profiling, monitorando l'utilizzo delle risorse per evitare crash o per rilevare ambienti di analisi.



Time ...	Process Name	PID	Operation	Path	Result	Detail
5:54:5...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.015
5:54:5...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:54:5...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:54:5...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:54:5...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:0...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:0...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:0...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:0...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:0...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:0...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:0...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:0...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:0...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:1...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:2...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:3...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:4...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:4...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:4...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:4...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:4...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:4...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031
5:55:4...	notepad-classic...	4216	Process Profiling		SUCCESS	User Time: 0.031

Showing 97 of 296,926 events (0.032%)   Backed by virtual memory

Log ProcMon: Evidenza delle operazioni di "Process Profiling" continuative.

---

4. Considerazioni Finali e Conclusioni

Sulla base delle informazioni raccolte ed elaborate con il supporto dell'AI:

1. **Verdetto**: `notepad-classico.exe` è un **Trojan/Dropper** impacchettato.
2. **Tecnica di Evasione**: Utilizza una sezione **self-modifying** per nascondere il payload reale fino al runtime.
3. **Obiettivo**: Il monitoraggio dinamico suggerisce attività finalizzate alla persistenza e alla comunicazione di rete.