

**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](mailto:mynameisimone@gmail.com)

Linkedin: <https://www.linkedin.com/in/simone-giordano-91290652/>

## Sommario

<b>Analisi dinamica notepad-classixo.exe con Procmon .....</b>	<b>3</b>
<b>Considerazioni finali sul malware.....</b>	<b>9</b>
<b>Analisi con Cuckoo .....</b>	<b>10</b>

# 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.

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 7:58:23.96	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 66, Length: 8,192. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 7:58:24.04	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 447, Length: 8,192. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 7:58:24.12	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 123, Length: 8,192. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:01:55.51	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 123,954. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:03:21.19	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 361,472. Length: 20,490. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:03:21.27	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 123,954. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:05:46.90	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 107,522. Length: 16,384. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:06:08.11	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 168,960. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:07:58.49	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 156,672. Length: 12,288. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:08:00.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 107,232. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:13:37.67	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 87,040. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:14:22.19	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 183,440. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:15:25.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,631,232. Length: 16,384. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:17:00.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 123,954. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:17:57.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,721,344. Length: 16,384. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:18:06.62	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,795,072. Length: 16,384. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:18:10.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,693,276. Length: 20,490. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:21:10.05	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,655,808. Length: 16,384. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:22:01.02	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,655,892. Length: 28,672. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:23:14.75	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 592,656. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:23:20.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,619,444. Length: 12,288. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:25:54.94	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,619,444. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:26:17.20	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\TextInputFramework.dll	SUCCESS	Offset: 247,712. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:27:00.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Measuring.dll	SUCCESS	Offset: 201,712. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:28:41.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 291,840. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:31:19.08	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,693,276. Length: 16,384. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:32:23.03	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,693,276. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:32:24.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,693,276. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:34:01.09	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\TextInputFramework.dll	SUCCESS	Offset: 291,840. Length: 28,672. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:35:56.81	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 592,656. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:37:52.87	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,619,444. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:38:00.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,619,444. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:41:09.60	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\TextInputFramework.dll	SUCCESS	Offset: 422,912. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:41:58.90	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\TextInputFramework.dll	SUCCESS	Offset: 132,096. Length: 16,384. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:42:00.00	notepad-classico.exe	5900	[CreateFile]	C:\Windows\SystemResources\USER32.dll\mun	NAME NOT FOUND	OpenFile, Access: Read, Share: None, Synchronization: Deposit Open, Options: Synchronous, Non-Directory File, Attributes: ...
12/21/09 8:42:00.00	notepad-classico.exe	5900	[CreateFile]	C:\Windows\SystemResources\USER32.dll\mun	NAME NOT FOUND	OpenFile, Access: Read, Share: None, Synchronization: Deposit Open, Options: Synchronous, Non-Directory File, Attributes: ...
12/21/09 8:42:53.93	notepad-classico.exe	5900	[ReadFile]	C:\Windows\WinSxS\amd64_microsoft-windows-common-controls_6599b54144cd1f_5.0.19041.1110_none_a8625c1898757984	SUCCESS	Offset: 320,512. Length: 4,096. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:43:04.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\WinSxS\amd64_microsoft-windows-common-controls_6599b54144cd1f_5.0.19041.1110_none_a8625c1898757984	SUCCESS	Offset: 287,744. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:43:04.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\WinSxS\amd64_microsoft-windows-common-controls_6599b54144cd1f_5.0.19041.1110_none_a8625c1898757984	SUCCESS	Offset: 701,440. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:43:04.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\WinSxS\amd64_microsoft-windows-common-controls_6599b54144cd1f_5.0.19041.1110_none_a8625c1898757984	SUCCESS	Offset: 230,400. Length: 12,288. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:43:54.44	notepad-classico.exe	5900	[ReadFile]	C:\Windows\WinSxS\amd64_microsoft-windows-common-controls_6599b54144cd1f_5.0.19041.1110_none_a8625c1898757984	SUCCESS	Offset: 351,320. Length: 8,192. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:44:00.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\WinSxS\amd64_microsoft-windows-common-controls_6599b54144cd1f_5.0.19041.1110_none_a8625c1898757984	SUCCESS	Offset: 1,233,120. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:44:18.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 717,824. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:44:19.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 775,168. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:44:20.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\Core\Components.dll	SUCCESS	Offset: 1,233,120. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:44:20.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\g32.dll	SUCCESS	Offset: 290,816. Length: 16,384. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:45:07.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\lutherne.dll	SUCCESS	Offset: 316,416. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:45:09.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\lutherne.dll	SUCCESS	Offset: 312,320. Length: 4,096. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:45:09.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\lutherne.dll	SUCCESS	Offset: 312,320. Length: 4,096. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:45:10.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\lutherne.dll	SUCCESS	Offset: 254,976. Length: 24,576. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:45:10.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\lutherne.dll	SUCCESS	Offset: 517,120. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:45:10.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\lutherne.dll	SUCCESS	Offset: 230,400. Length: 12,288. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:45:10.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\lutherne.dll	SUCCESS	Offset: 417,440. Length: 32,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal
12/21/09 8:45:10.00	notepad-classico.exe	5900	[ReadFile]	C:\Windows\SysWOW64\lutherne.dll	SUCCESS	Offset: 311,768. I/O Rags. Non-cached. Paging I/O. Synchronous Paging I/O. Priority: Normal

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\SystemResources\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:

- scrittura (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
- apprendo 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
<b>Time of Day</b> <b>Process Name</b> <b>PID</b> <b>Operation</b> <b>Path</b> <b>Result</b> <b>Detail</b>						
12:21:09.1800252	[notepad-classico.exe]	5900	Thread Create	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS	Thread ID: 648 Image Base: 0x76080000, Image Size: 0x5000
12:21:09.1802622	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\msvcp_vin.dll	SUCCESS	Image Base: 0x76250000, Image Size: 0x7000
12:21:09.1805957	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x75200000, Image Size: 0x45000
12:21:09.1815577	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\shell_32.dll	SUCCESS	Image Base: 0x74e80000, Image Size: 0x56000
12:21:09.1830841	[notepad-classico.exe]	5900	Thread Create	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Thread ID: 2140 Image Base: 0x76900000, Image Size: 0x7000
12:21:09.1831589	[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\Win32\Microsoft.Windows.Common-Controls_6595b64144cc1df_6_0.19041.1110_none_a8625c1886757984...	SUCCESS	Image Base: 0x74a40000, Image Size: 0x210000
12:21:09.1898534	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\win32pspool.dll	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
12:21:09.2274462	[notepad-classico.exe]	5900	Thread Create	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Thread ID: 540 Image Base: 0x749f0000, Image Size: 0x72000
12:21:09.2316100	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\ienv2_32.dll	SUCCESS	Image Base: 0x76150000, Image Size: 0x30000
12:21:09.2329111	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Image Base: 0x75980000, Image Size: 0x100000
12:21:09.2391605	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\winmin.dll	SUCCESS	Image Base: 0x73440000, Image Size: 0x456200
12:21:09.2425008	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Image Base: 0x741d0000, Image Size: 0x40000
12:21:09.2464149	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\msacfl.dll	SUCCESS	Image Base: 0x762d0000, Image Size: 0x40000
12:21:09.2542418	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x762c0000, Image Size: 0x60000
12:21:09.2726711	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x75b00000, Image Size: 0x30000
12:21:09.3108093	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Image Base: 0x74d90000, Image Size: 0x20000
12:21:09.3233341	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\TextShaping.dll	SUCCESS	Image Base: 0x738d0000, Image Size: 0x40000
12:21:09.3326552	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\NapiNSP.dll	SUCCESS	Image Base: 0x74080000, Image Size: 0x10000
12:21:09.3431039	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\prmpnp.dll	SUCCESS	Image Base: 0x74060000, Image Size: 0x16000
12:21:09.3460037	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\drapi.dll	SUCCESS	Image Base: 0x73c50000, Image Size: 0x10000
12:21:09.3471715	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\IPHLPAPI.DLL	SUCCESS	Image Base: 0x73f10000, Image Size: 0x10000
12:21:09.3526396	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\vtapi.dll	SUCCESS	Image Base: 0x75540000, Image Size: 0x20000
12:21:09.3562540	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\vtapi.dll	SUCCESS	Image Base: 0x74d040000, Image Size: 0x10000
12:21:09.3640431	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\vtapi.dll	SUCCESS	Image Base: 0x74d040000, Image Size: 0x10000
12:21:09.3679182	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Image Base: 0x72e90000, Image Size: 0x10000
12:21:09.3744153	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\FWFLCLNT.DLL	SUCCESS	Image Base: 0x73af0000, Image Size: 0x59000
12:21:09.3766151	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS	Image Base: 0x75400000, Image Size: 0x19000
12:21:09.3945827	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\asdhlp.dll	SUCCESS	Image Base: 0x73ea0000, Image Size: 0x8000
12:21:09.5790167	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\kernel_apcore.dll	SUCCESS	Image Base: 0x743d4000, Image Size: 0x4000
12:21:09.5814783	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\bcryptimitives.dll	SUCCESS	Image Base: 0x75600000, Image Size: 0x9000
12:21:09.6676809	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\TextInputFramework.dll	SUCCESS	Image Base: 0x73a30000, Image Size: 0xb000
12:21:09.6876787	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\CoreMessaging.dll	SUCCESS	Image Base: 0x73990000, Image Size: 0x9000
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\vtmarta.dll	SUCCESS	Image Base: 0x73e70000, Image Size: 0x29000
12:21:09.7235535	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Image Base: 0x73060000, Image Size: 0xd8000
12:21:09.7241154	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Image Base: 0x74270000, Image Size: 0xdb000
12:21:09.72419152	[notepad-classico.exe]	5900	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Image Base: 0x74270000, Image Size: 0xdb000
12:21:09.3355476	[notepad-classico.exe]	5900	Thread Create	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Thread ID: 4056 Image Base: 0x74270000, Image Size: 0xdb000
12:21:09.3365982	[notepad-classico.exe]	5900	Thread Create	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Thread ID: 4340 Image Base: 0x74270000, Image Size: 0xdb000
12:22:09.1984882	[notepad-classico.exe]	5900	Thread Exit		SUCCESS	Thread ID: 3234, User Time: 0.0000000, Kernel Time: 0.0156250
12:22:09.1985631	[notepad-classico.exe]	5900	Thread Exit		SUCCESS	Thread ID: 548, 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
12:22:09.19953	[notepad-classico.exe]	5900	Thread Exit		SUCCESS	Thread ID: 4340, User Time: 0.0000000, Kernel Time: 0.0000000
12:22:09.19953	[notepad-classico.exe]	5900	Thread Exit		SUCCESS	Thread ID: 4056, User Time: 0.0000000, Kernel Time: 0.0000000
12:22:23.3587321	[notepad-classico.exe]	5900	Thread Exit		SUCCESS	Thread ID: 4056, User Time: 0.0000000, Kernel Time: 0.0000000
12:22:23.3590653	[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: 4056, User Time: 0.0000000, Kernel Time: 0.0000000
12:27:51.1446350	[notepad-classico.exe]	5900	Thread Exit		SUCCESS	Thread ID: 4056, User Time: 0.0000000, Kernel Time: 0.0000000
12:31.09.24626171	[notepad-classico.exe]	5900	Thread Create		SUCCESS	Thread ID: 5416, User Time: 0.0000000, Kernel Time: 0.0000000
12:32.19.2455011	[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.

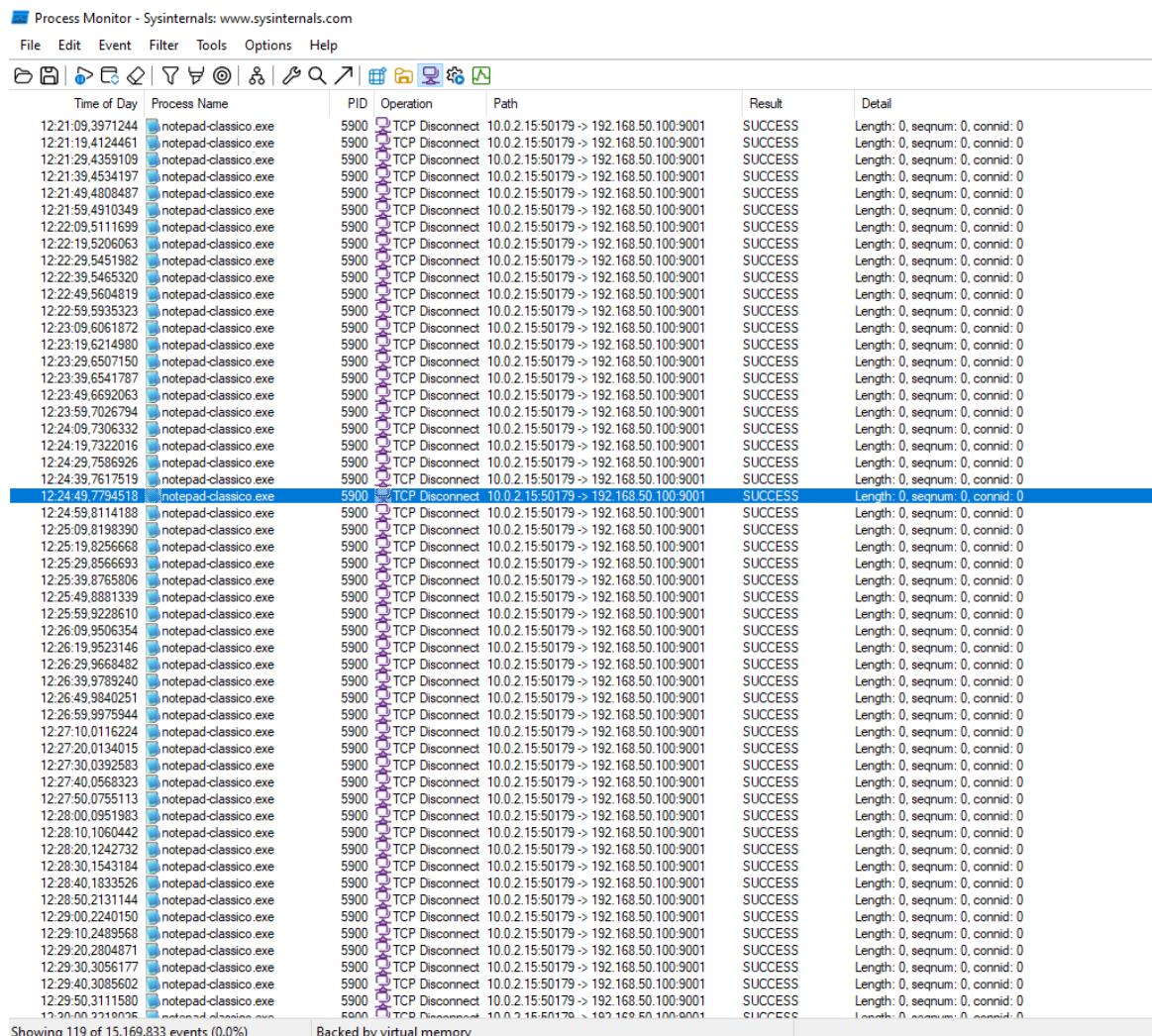
# Considerazioni finali sul malware

**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/9msmlrh6lf3?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.



The screenshot shows a table of network events from Process Monitor. The columns are: Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The table lists numerous entries where 'notepad-classico.exe' is performing TCP Disconnect operations to various external IP addresses (e.g., 192.168.50.100) on port 9001. All operations result in SUCCESS with a length of 0 and sequence number 0. The last event in the list is highlighted with a blue bar.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
12-21-09.3971244	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-21-19.4124461	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-21-29.4359105	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-21-39.4534197	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-21-49.4808487	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-21-59.4910349	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-22-09.5111695	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-22-19.5206063	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-22-29.5451982	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-22-39.5465320	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-22-49.5604819	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-22-59.5933523	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-23-09.6061872	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-23-19.6214980	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-23-29.6507150	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-23-39.6541787	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-23-39.6692063	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-23-59.7026794	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-24-09.7306332	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-24-19.7322016	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-24-29.7586926	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-24-39.7617519	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-24-49.7734518	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-24-59.8114188	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-25-09.8198390	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-25-19.0256663	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-25-29.0566693	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-25-39.0785806	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-25-49.0881339	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-25-59.9228610	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-26-09.9506354	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-26-19.9523146	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-26-29.9668482	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-26-39.9789240	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-26-49.9840251	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-26-59.9975944	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-27-10.0116224	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-27-20.0134015	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-27-30.0325823	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-27-40.0568323	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-27-50.0755113	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-28-00.0951983	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-28-10.1060442	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-28-20.1242732	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-28-30.1543184	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-28-40.1833526	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-28-50.2131144	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-29-00.2240150	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-29-10.2489568	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-29-20.2804871	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-29-30.3056177	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-29-40.3085602	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-29-50.3111580	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0
12-30-00.2218025	notepad-classico.exe	5900	TCP Disconnect	10.0.2.15:50179 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum: 0, connid: 0

# Analisi con Cuckoo

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

## Vista generale

**Summary**

**File notepad-classico.exe**

Summary	<a href="#">Download</a>   <a href="#">Resubmit sample</a>   <a href="#">Download yara</a>
Size	282.5KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	8a00a5c59ac157754ca575d721bcf960
SHA1	c31e260630d6553e2000f8e5f8dc270c751780d9
SHA256	d2ec9c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e360398bf2
SHA512	Show SHA512
CRC32	97668313
ssdeep	None
Yara	<ul style="list-style-type: none"><li>CrowdStrike_CSIT_16018_03 - Metasploit payload loader</li><li>DebuggerCheck_QueryInfo - (no description)</li><li>anti_dbg - Checks if being debugged</li><li>inject_thread - Code injection with CreateRemoteThread in a remote process</li><li>network_http - Communications over HTTP</li><li>network_dns - Communications use DNS</li><li>network_dga - Communication using dga</li><li>escalate_priv - Escalade privileges</li><li>screenshot - Take screenshot</li><li>win_mutex - Create or check mutex</li></ul>

**Score**  
This file is very suspicious, with a score of 10 out of 10!

Please notice: The scoring system is currently still in development and should be considered an alpha feature.

**Feedback**  
Expecting different results? Send us this analysis and we will inspect it.  
[Click here](#)

## Analisi comportamentale

Le attività di rete sono le stesse rilevate da Procmon.

**Process tree**

**notepad-classico.exe** PID 2736  
C:\Users\Administrator\AppData\Local\Temp\notepad-classico.exe

**Process contents**

**notepad-classico.exe**

PID 2736  
Parent PID 1892

**Time & API** **Arguments** **Status** **Return** **Repe**

WSAStartup	wVersionRequested: 514	1	0	0
socket	protocol: 6 type: 1 socket: 296 af: 2	1	296	0
gethostbyname	hostname: 192.168.50.100	1	12011672	0
connect	ip_address: 192.168.50.100 socket: 296 port: 9001	4294967295	0	