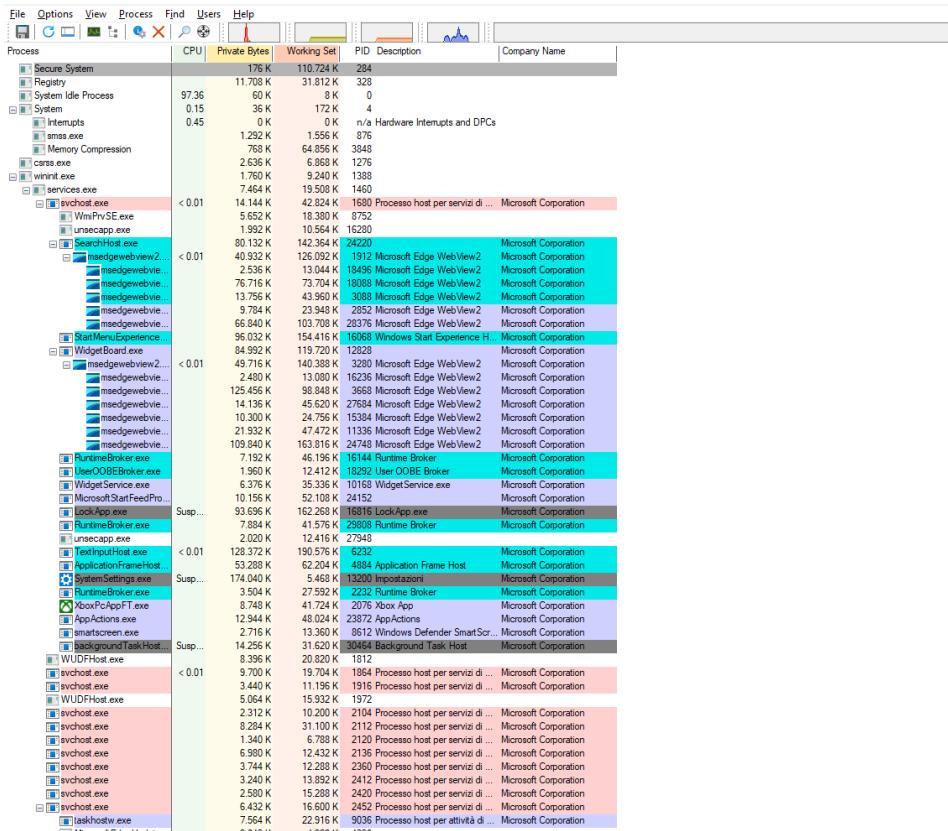


Thread, Handle e Registro di Windows

Executive Summary

Il presente report documenta le fasi esplorazione dei processi, thread, handle e Registro Windows

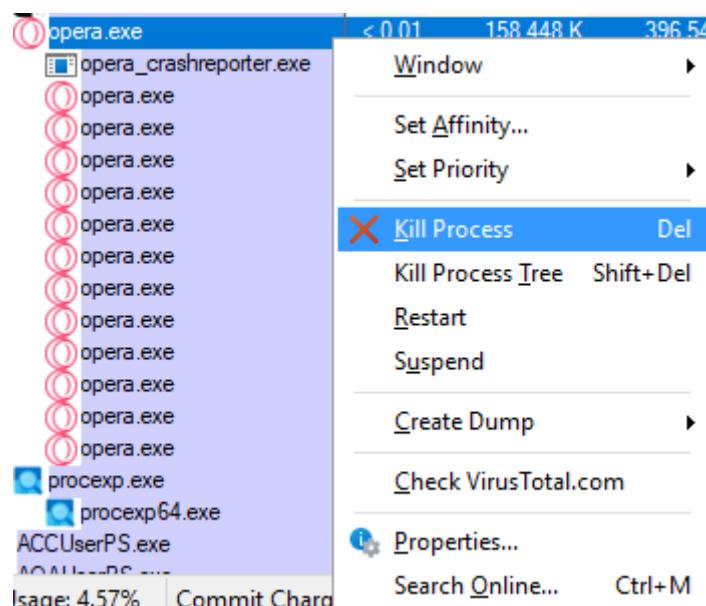
Fase1 – Esplorazione processi



*Fig. 1 Pagina principale procexp

opera.exe	0.08	158.828 K	396.756 K	21000	Opera GX Internet Browser	Opera Software
opera_crashreporter.exe		2.580 K	13.832 K	25928	Opera GX crash-reporter	Opera Software
opera.exe	< 0.01	284.736 K	267.072 K	21452	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	17.888 K	51.392 K	15844	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	10.944 K	24.716 K	20684	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	26.760 K	119.712 K	29512	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	67.544 K	187.732 K	25744	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	79.616 K	244.508 K	15200	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	37.404 K	138.880 K	22052	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	108.828 K	228.092 K	18372	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	8.868 K	25.604 K	25320	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	211.516 K	273.356 K	15848	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	15.896 K	37.504 K	27324	Opera GX Internet Browser	Opera Software
opera.exe	< 0.01	26.256 K	54.464 K	20928	Opera GX Internet Browser	Opera Software

*Fig.2 Processo browser



*Fig.3 Terminazione processo browser

	procexp64.exe	0.07	55.996 K	93.428 K	16424	Sysinternals Process Explorer
	SnippingTool.exe	0.97	14.460 K	53.160 K	18804	Sysinternals - www.sysintern...
	ACCUserPS.exe		2.880 K	19.308 K	21280	
	AQAUserPS.exe	< 0.01	6.640 K	43.464 K	10296	
	msedgewebview2.exe	Susp...	41.280 K	123.828 K	19728	Microsoft Edge WebView2
	msedgewebview2.exe		2.528 K	12.844 K	10504	Microsoft Edge WebView2
	msedgewebview2.exe	Susp...	62.860 K	68.536 K	26972	Microsoft Edge WebView2
	msedgewebview2.exe	Susp...	12.968 K	43.180 K	16304	Microsoft Edge WebView2
	msedgewebview2.exe	Susp...	8.836 K	22.688 K	15628	Microsoft Edge WebView2
	msedgewebview2.exe	Susp...	79.356 K	121.016 K	28260	Microsoft Edge WebView2

*Fig.4 Processo browser post-kill

- Cosa è successo alla finestra del browser web quando il processo è stato terminato?

Tutti i processi attivi del browser vengono interrotti con conseguenza l'arresto del browser.

 cmd.exe	2.032 K	5.876 K	27968 Processore dei comandi di ...	Microsoft Corporation
 conhost.exe	1.628 K	11.260 K	9816 Host finestra console	Microsoft Corporation

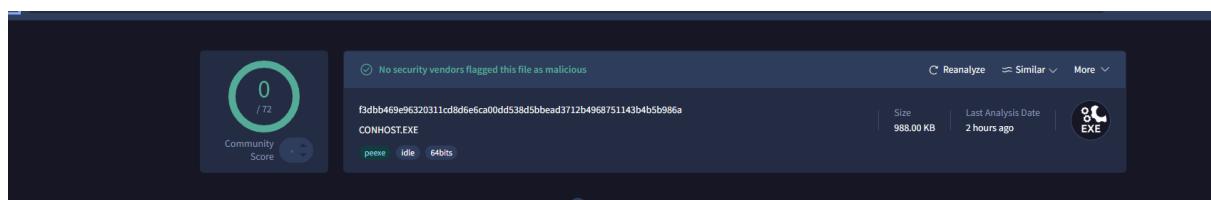
*Fig.5 Processi prompt comandi

 cmd.exe	3.240 K	6.368 K	27968 Processore dei comandi di ...	Microsoft Corporation
 conhost.exe	1.556 K	11.232 K	9816 Host finestra console	Microsoft Corporation
 PING.EXE	984 K	5.908 K	17472 Comando Ping TCP/IP	Microsoft Corporation

*Fig.6 Processo PING.EXE

- Cosa è successo durante il processo ping?

Durante la fase di ping, viene rivelato un processo chiamato PING.EXE.



*Fig.7 Scansione conhost.exe

 cmd.exe	2.028 K	5.876 K	21372 Processore dei comandi di ...	Microsoft Corporation
 conhost.exe	1.488 K	11.132 K	21048 Host finestra console	Microsoft Corporation 0/72
 msedge.exe	0.43	76.972 K	206.324 K	27208 Microsoft Edge
 msedge.exe		2.592 K	10.136 K	18444 Microsoft Edge
 msedge.exe	0.14	17.068 K	47.344 K	23344 Microsoft Edge
 msedge.exe	0.21	143.380 K	94.128 K	20348 Microsoft Edge
 msedge.exe		8.836 K	19.408 K	13712 Microsoft Edge
 msedge.exe	< 0.01	72.428 K	104.364 K	19464 Microsoft Edge
 msedge.exe	0.07	372.404 K	381.260 K	21436 Microsoft Edge
 msedge.exe	< 0.01	7.948 K	16.224 K	22196 Microsoft Edge

*Fig.8 Scansione conhost.exe

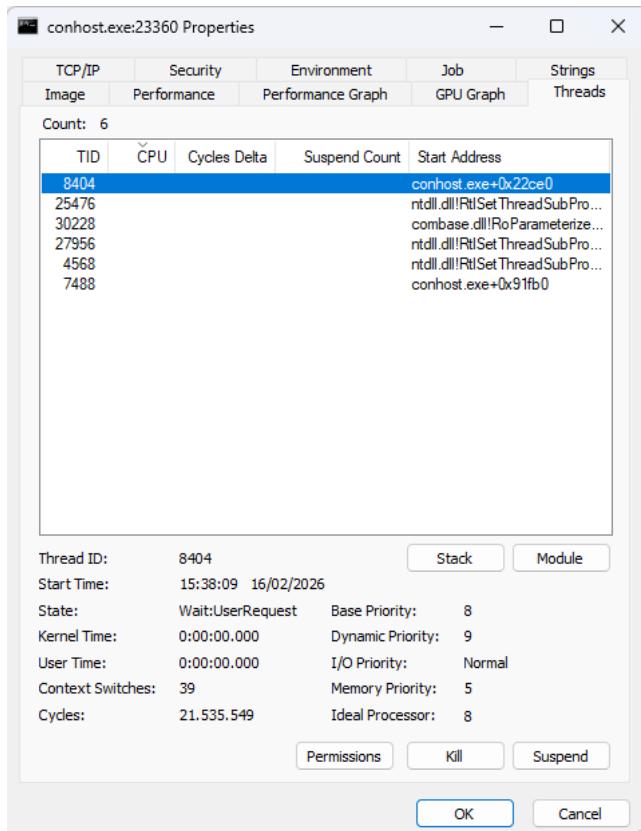
 opera.exe	0.0 /	156.684 K	379.236 K	30184 Opera GX Internet Browser	Opera Software
 procexp.exe		6.144 K	15.840 K	7472 Sysinternals Process Explorer	Sysinternals - www.sysinter...
 procexp64.exe	0.22	56.948 K	95.188 K	5084 Sysinternals Process Explorer	Sysinternals - www.sysinter...
 ACCUserPS.exe		2.880 K	19.308 K	21280	
 AQAUserPS.exe	< 0.01	6.608 K	43.488 K	10296	
 msedgewebview2.exe	Susp...	41.280 K	123.828 K	19728 Microsoft Edge WebView2	Microsoft Corporation

*Fig.9 Processo prompt comandi post-kill

- Cosa è successo al processo figlio conhost.exe?

Terminando il processo **cmd.exe**, anche il processo figlio **conhost.exe** viene interrotto automaticamente.

Fase2 - Esplorazione di Thread e Handle

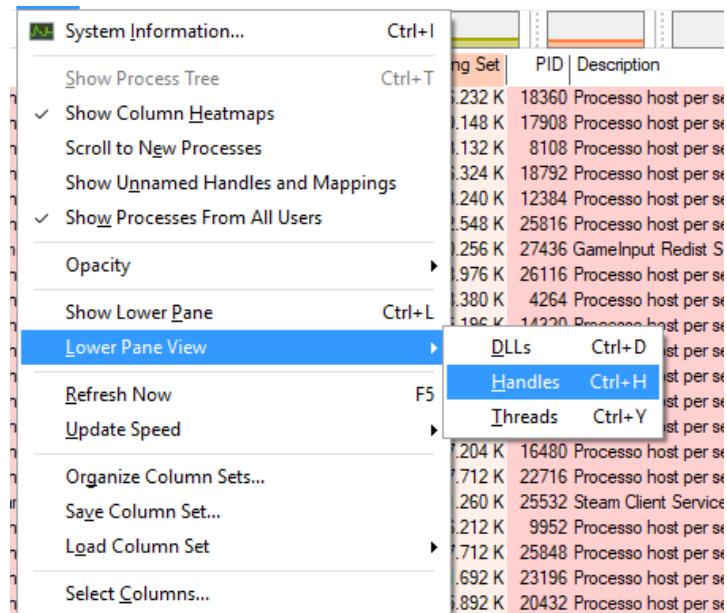


*Fig. 10 Proprietà processo conhost.exe

- **Che tipo di informazioni sono disponibili nella finestra Proprietà?**

È possibile ricavare informazioni come:

- **TID:** L'identificativo univoco assegnato dal sistema operativo a quel singolo thread.
- **CPU:** Indica la capacità di calcolo del processore che sta assorbendo il thread.
- **Cycles Delta:** Rappresenta la variazione dei cicli di clock consumati dal thread.
- **Suspend Count:** Indica quante volte il thread è stato messo in pausa.
- **Start Address:** L'indirizzo di memoria che ha dato inizio al thread.



*Fig.11 Conhost.exe handles

Type	Name
ALPC Port	\RPC Control\OLE8C5EA95B4715B440125E5A294E88
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\3\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	C:\Program Files\Windows Apps\Microsoft.LanguageExperiencePackit-IT_26100.156.249.0...
File	\Device\VCNG
File	\Device\NamedPipe\
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKCU
Key	HKLM
Key	HKCR\PackagedCom\Package
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU\Software\Classes\Local Settings
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom
Key	HKCR\PackagedCom\ClassIndex
Key	HKCU\Software\Classes\PackagedCom
Key	HKCU\Software\Classes\PackagedCom\Package
Key	HKCU\Software\Classes
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom\InterfaceIndex
Mutant	\Sessions\3\BaseNamedObjects\SM0:23360:304:WiStaging_02

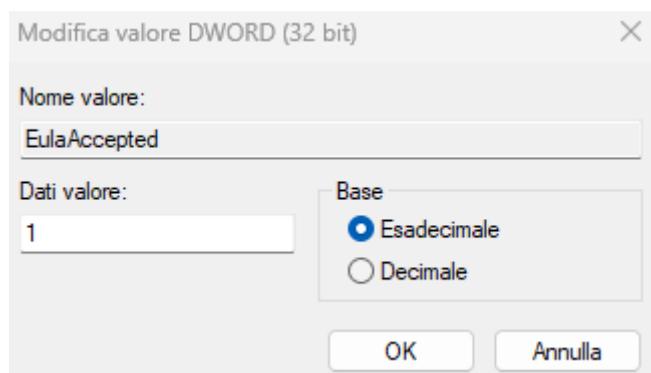
*Fig.12 Conhost.exe handles

- **Esaminare gli handle. A cosa puntano gli handle?**

Gi handles puntano alle directory **KnowDlls** e **BaseNamedObjects** e alle diverse chiavi di registro

Fase3 – Esplorazione del Registro di Windows

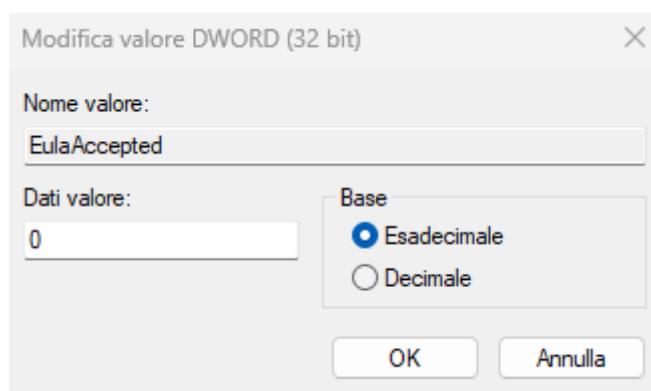
*Fig. 13 Chiave Eula



*Fig. 14 Valore chiave attuale (1)

- Qual è il valore per questa chiave di registro nella colonna Dati (Data)?

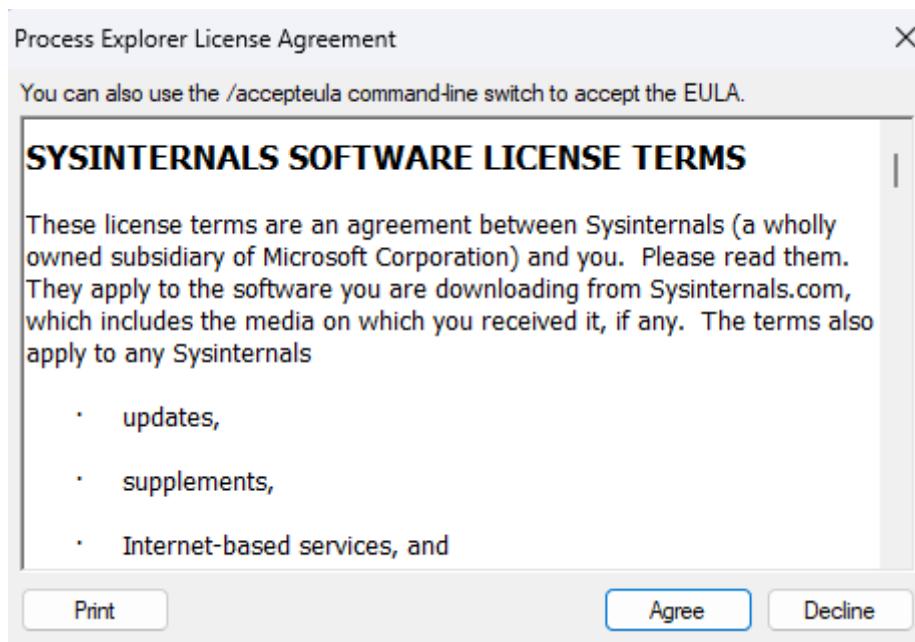
Il valore della chiave EULA è attualmente 1, ciò significa che l'agreement è stato accettato.



*Fig. 15 Modifica valore chiave (0)

	EulaAccepted	REG_DWORD	0x00000000 (0)
--	--------------	-----------	----------------

*Fig. 16 Valore chiave attuale post modifica



*Fig. 17 Verifica modifica (Reset Eula)

- **Quando apri Process Explorer, cosa vedi?**

Alla riapertura di Process Explorer, verrà chiesto nuovamente di accettare l'EULA poichè il valore della chiave è stata modificata a 0

Conclusione

Il report ha dimostrato le diverse fasi di **esplorazione e gestione di processi, thread e handle**, evidenziando come l'interazione con il **Registro di Windows** possa influenzare il comportamento di determinati software.