Report 16/02/2026 Cristiano Samuel Processi,

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

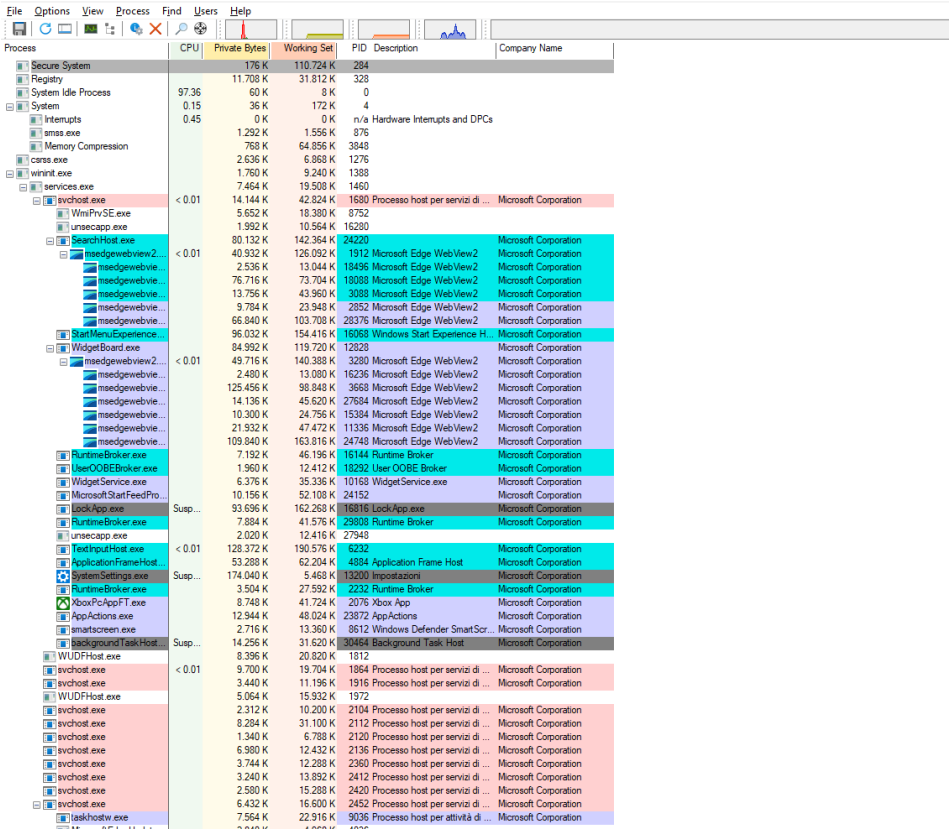
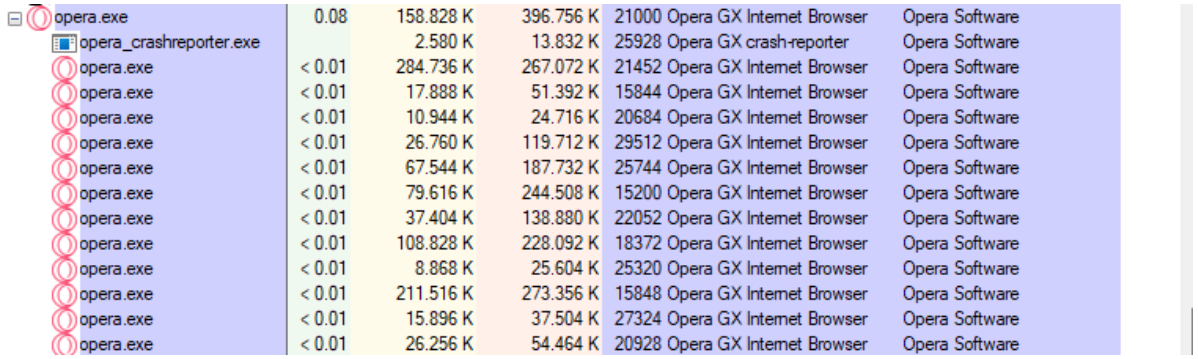


Fig.1 Pagina principale procexp



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

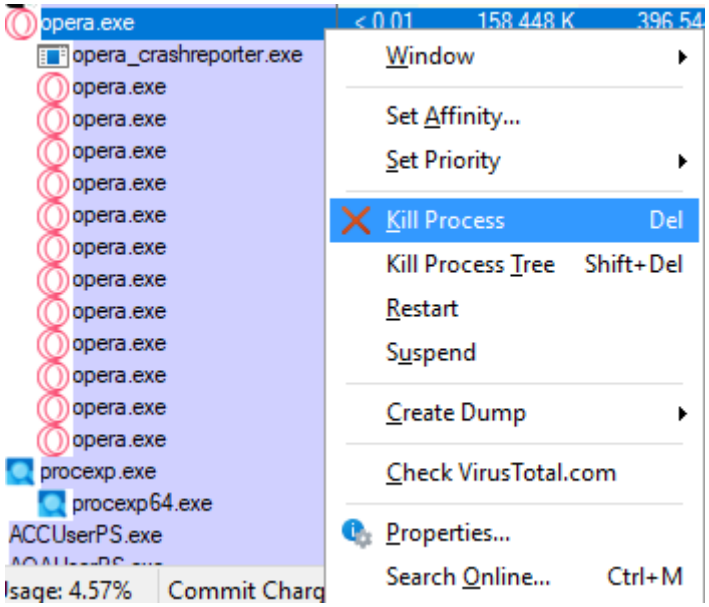
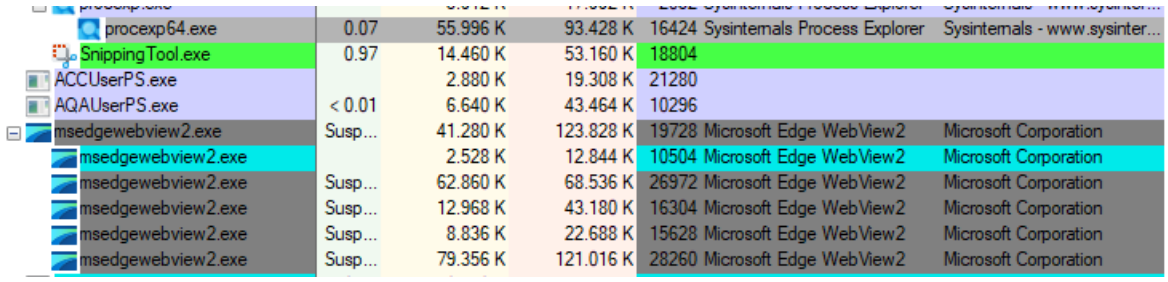


*Fig.3 Terminazione processo browser



procexp64.exe	0.07	55.996 K	93.428 K	16424 Sysinternals Process Explorer	Sysinternals - www.sysinter...
SnippingTool.exe	0.97	14.460 K	53.160 K	18804	
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	Microsoft Corporation
msedgewebview2.exe		2.528 K	12.844 K	10504 Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe	Susp...	62.860 K	68.536 K	26972 Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe	Susp...	12.968 K	43.180 K	16304 Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe	Susp...	8.836 K	22.688 K	15628 Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe	Susp...	79.356 K	121.016 K	28260 Microsoft Edge WebView2	Microsoft Corporation

*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.

*Fig.5 Processi prompt comandi

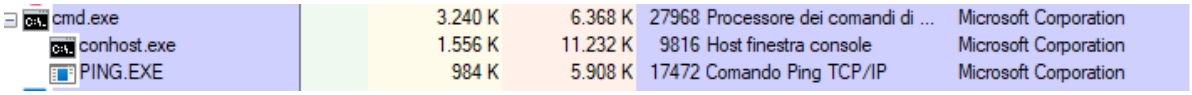


*Fig.6 Processo PING.EXE

- **Cosa è successo durante il processo ping?**

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

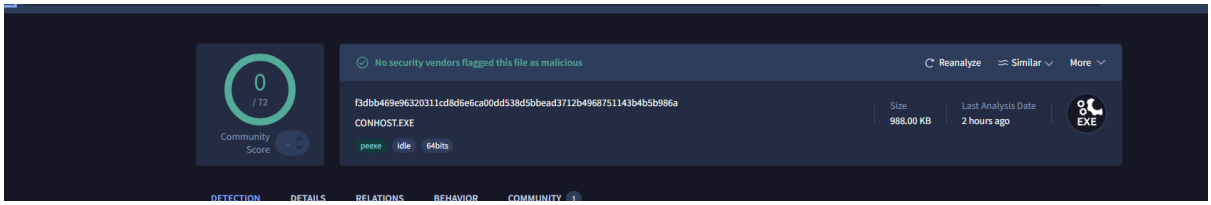


*Fig.7 Scansione conhost.exe

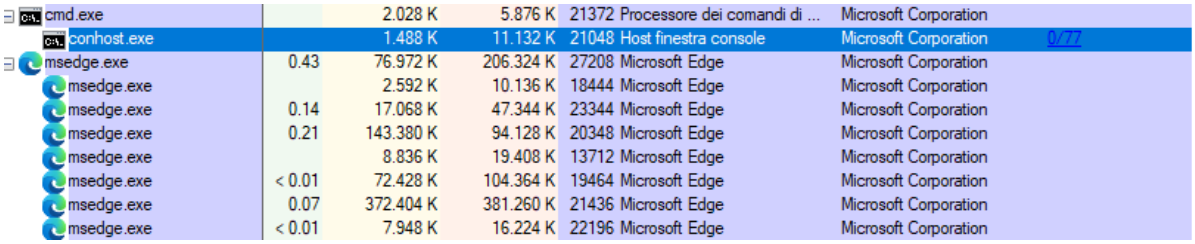


*Fig.8 Scansione conhost.exe

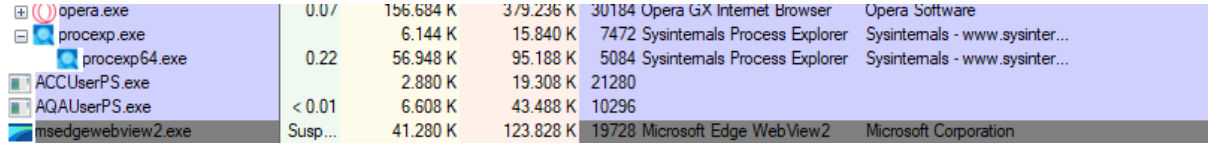


*Fig.9 Processo prompt comandi post-kill

- **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

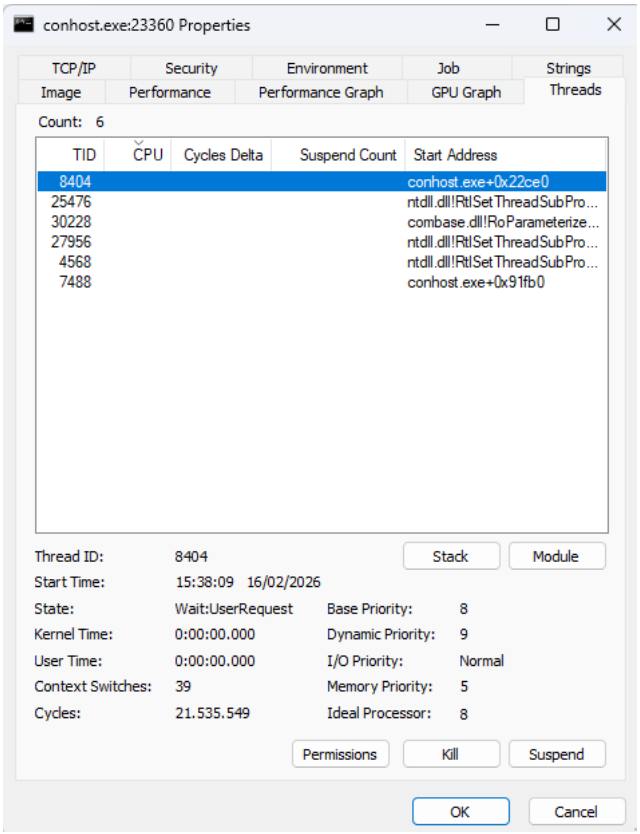


Fig.10 Proprietà processo conhost.exe

- **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.

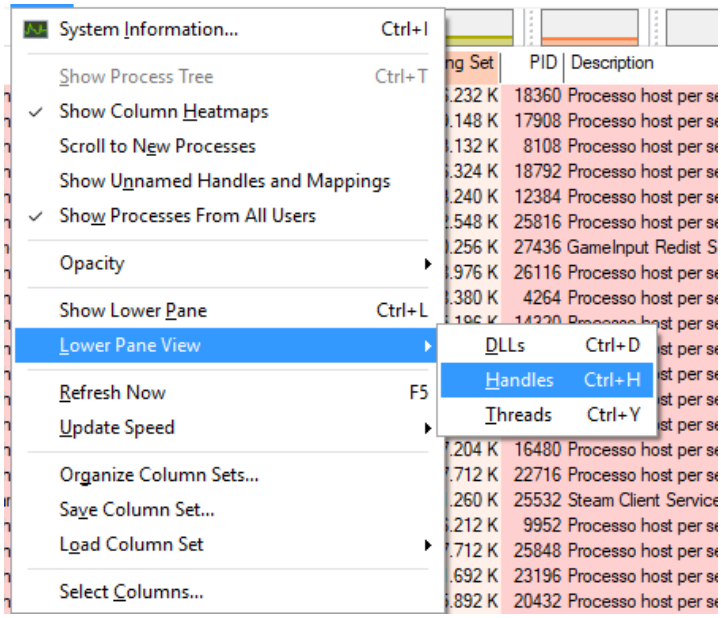


Fig.11 Conhost.exe handles

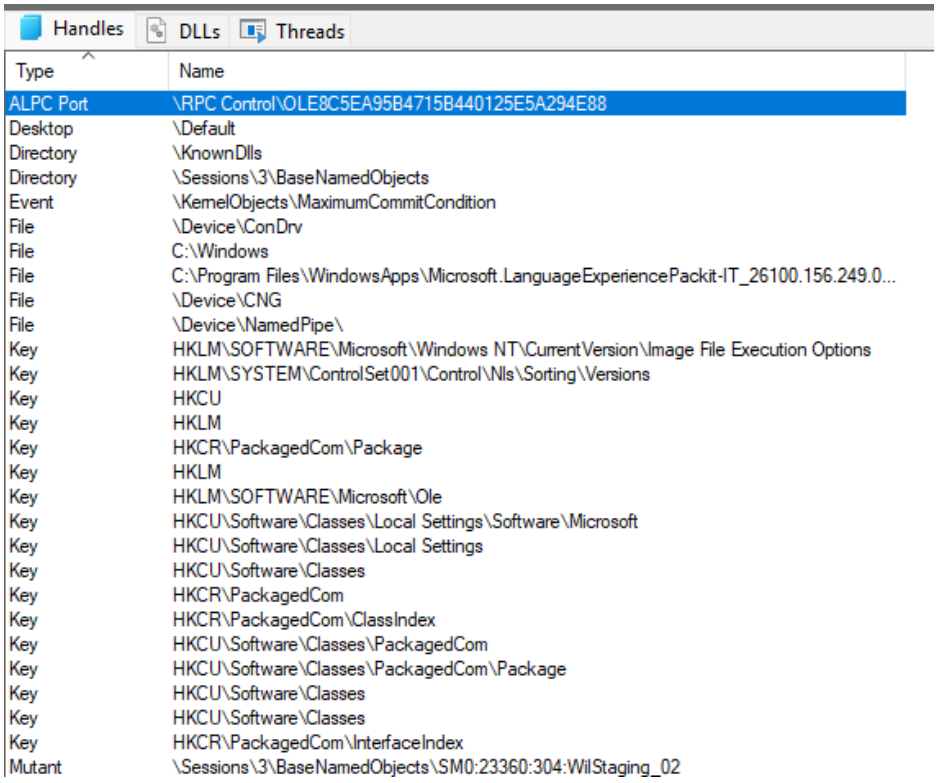


Fig.12 Conhost.exe handles

- **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

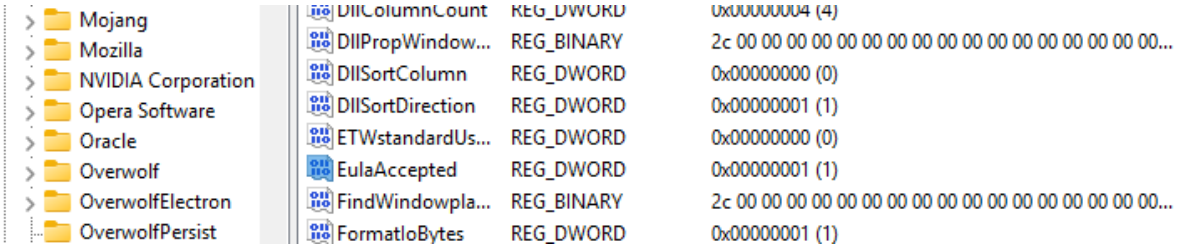


Fig.13 Chiave Eula

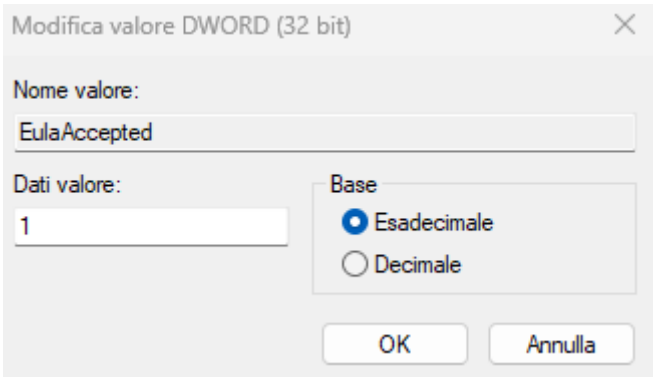


Fig.14 Valore chiave attuale (1)

- **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.

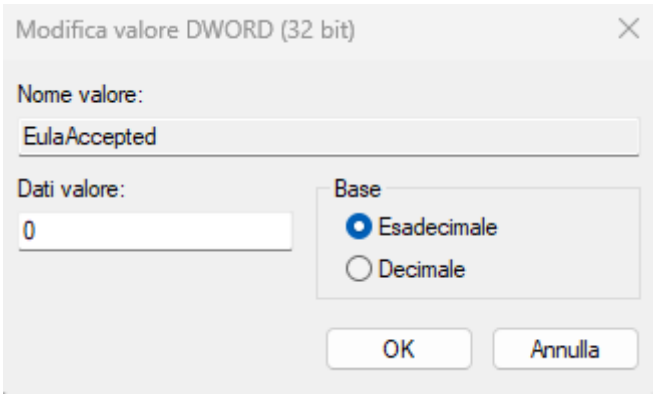


Fig.15 Modifica valore chiave (0)

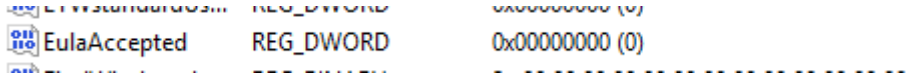


*Fig.16 Valore chiave attuale post modfica

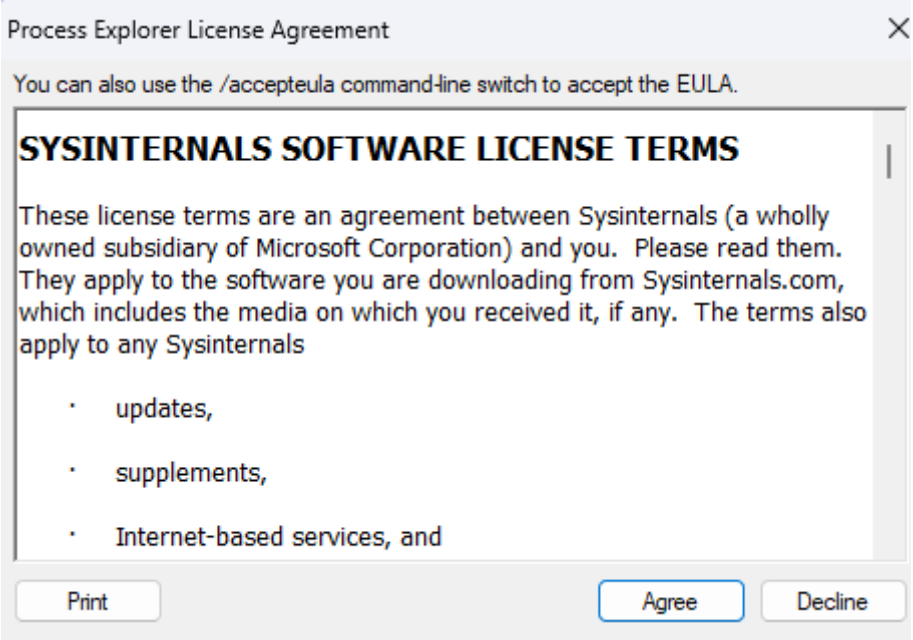


*Fig.17 Verifica modifica (Reset Eula)

- **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.