

ESERCIZIO 2: Esplorazione di Processi, Thread, Handle e Registro di Windows

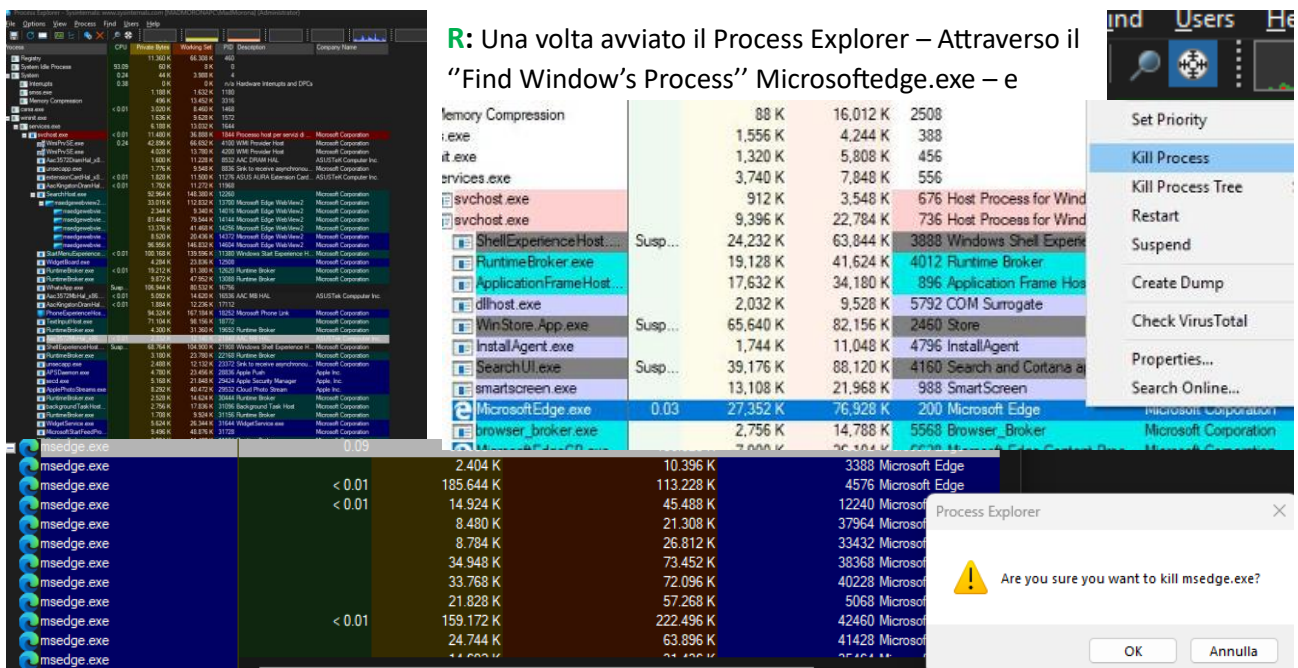
Rispondiamo alle seguenti domande:

1. Il processo di Microsoft Edge può essere terminato in Process Explorer.

Fare clic con il pulsante destro del mouse sul processo selezionato e selezionare Kill Process (Termina Processo). Fare clic su OK per continuare.

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

R: Una volta avviato il Process Explorer – Attraverso il “Find Window’s Process” Microsoftedge.exe – e



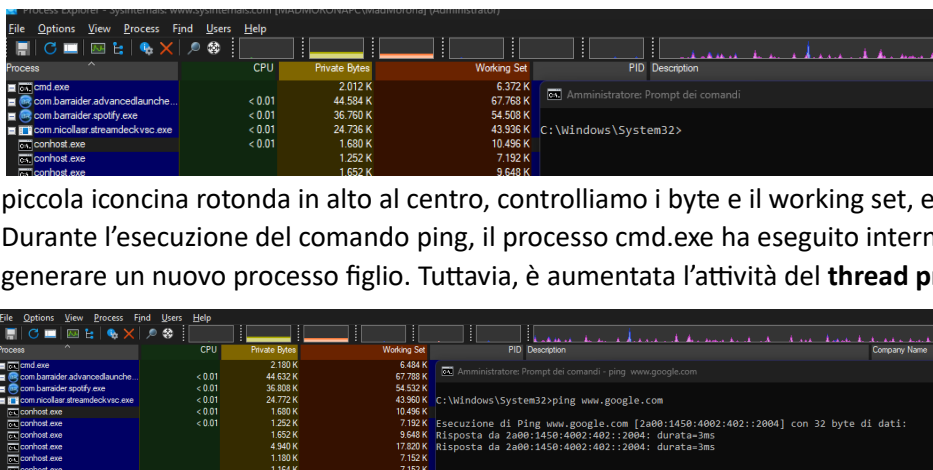
The screenshot shows the Process Explorer window with the 'Find Window's Process' button clicked. The list of processes includes several instances of 'msedge.exe'. A right-click context menu is open over the 'msedge.exe' processes, showing options like 'Set Priority', 'Kill Process', 'Kill Process Tree', 'Restart', 'Suspend', 'Create Dump', 'Check VirusTotal', 'Properties...', and 'Search Online...'. A confirmation dialog box is displayed in the foreground, asking 'Are you sure you want to kill msedge.exe?' with 'OK' and 'Annulla' buttons.

Killiamo il processo. Ovviamente una volta killato il processo, windows Explorer verrà “terminato”. Quindi la risposta alla domanda è che terminando il processo la finestra viene di colpo chiusa.

2. **Avviare un altro processo**

Cosa è successo durante il processo ping?

R: Una volta trovato il processo interessato sempre con il “Find Window’s process” la



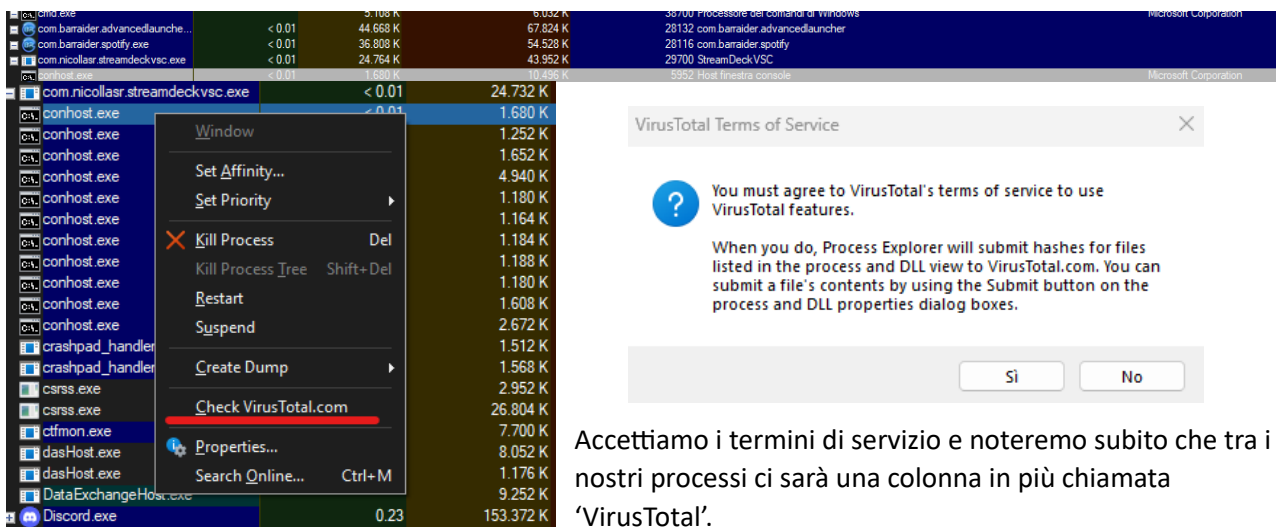
The screenshot shows the Process Explorer window with the 'Find Window's Process' button clicked. The list of processes includes 'cmd.exe' and 'conhost.exe'. A right-click context menu is open over the 'cmd.exe' process, showing options like 'Set Priority', 'Kill Process', 'Kill Process Tree', 'Restart', 'Suspend', 'Create Dump', 'Check VirusTotal', 'Properties...', and 'Search Online...'. A confirmation dialog box is displayed in the foreground, asking 'Are you sure you want to kill cmd.exe?' with 'OK' and 'Annulla' buttons.

piccola iconcina rotonda in alto al centro, controlliamo i byte e il working set, e avviamo subito dopo il ping. Durante l'esecuzione del comando ping, il processo cmd.exe ha eseguito internamente l'utility ping senza generare un nuovo processo figlio. Tuttavia, è aumentata l'attività del **thread principale** del cmd.exe, e

anche conhost.exe ha mostrato un leggero aumento di attività per visualizzare i risultati del comando nella finestra.

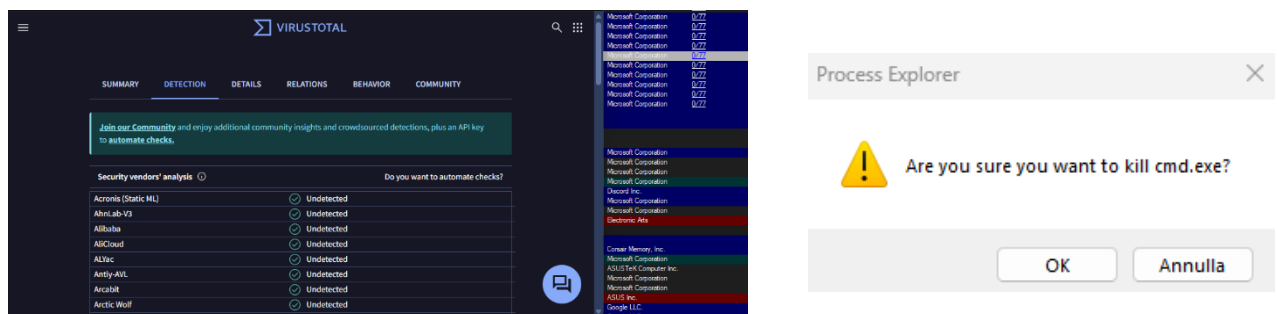
3. Cosa è successo al processo figlio conhost.exe?

R: Trovato il processo conhost.exe figlio di **cmd.exe** – facciamolo analizzare da VirusTotal, con click destro sul processo → Check VirusTotal.com.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
conhost.exe		1.652 K	9.648 K	24880	Host finestra console	Microsoft Corporation	0/77
conhost.exe		4.940 K	17.824 K	28252	Host finestra console	Microsoft Corporation	0/77
conhost.exe		1.180 K	7.152 K	28124	Host finestra console	Microsoft Corporation	0/77
conhost.exe		1.164 K	7.152 K	28156	Host finestra console	Microsoft Corporation	0/77
conhost.exe		1.184 K	7.052 K	29040	Host finestra console	Microsoft Corporation	0/77
conhost.exe		1.188 K	7.208 K	1892	Host finestra console	Microsoft Corporation	0/77
conhost.exe		1.180 K	7.040 K	29728	Host finestra console	Microsoft Corporation	0/77
conhost.exe		1.608 K	9.692 K	7156	Host finestra console	Microsoft Corporation	0/77
conhost.exe		2.672 K	21.524 K	40840	Host finestra console	Microsoft Corporation	0/77

Clicchiamo sul numero sottostante alla dicitura VirusTotal quindi su 0/77, e si aprirà una pagina browser indirizzata proprio sul sito di VirusTotal. Una volta ispezionato, killiamo il processo.

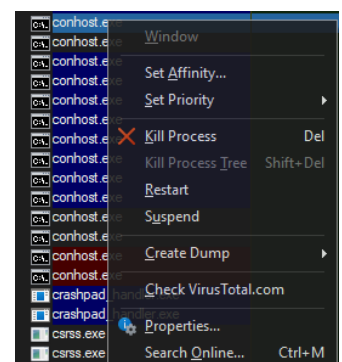


Per rispondere alla domanda: Quando il processo cmd.exe è stato terminato, anche il suo processo figlio conhost.exe è stato automaticamente chiuso. Questo accade perché conhost.exe è strettamente legato a cmd.exe e serve per gestire l'interfaccia grafica del prompt. Una volta che il processo principale viene chiuso, conhost.exe non ha più utilità e viene terminato anch'esso.

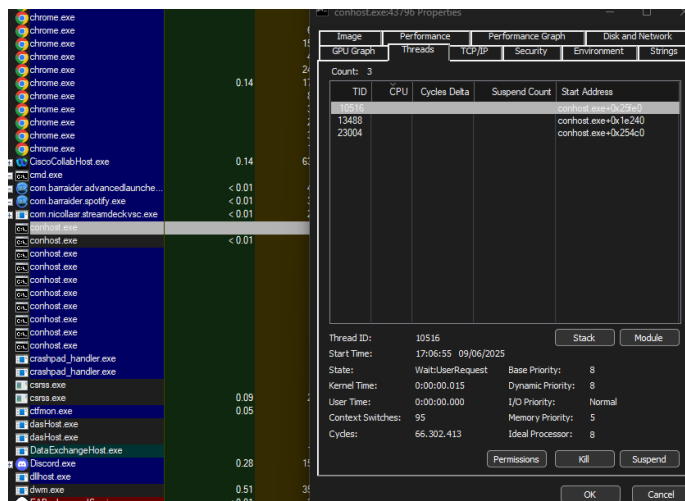
4. Esplorazione di Thread e Handle

Che tipo di informazioni sono disponibili nella finestra Proprietà?

Una volta avviato il prompt dei comandi, prendiamo il processo figlio conhost.exe → click destro → Properties → e poi andiamo nella sezione



Threads, aprirà un messaggio di avviso per i permessi, clickiamo su OK e continuiamo.

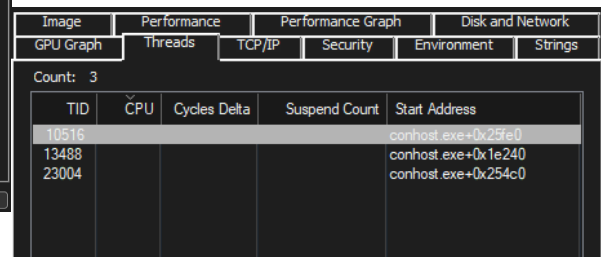


- **Campi disponibili ma non popolati:** utilizzo della CPU, conteggio dei cicli (Cycles Delta) e numero di sospensioni (Suspend Count), che in questo caso risultano vuoti.

Queste informazioni permettono di monitorare i thread attivi e identificare comportamenti sospetti o anomali a livello di esecuzione del processo.

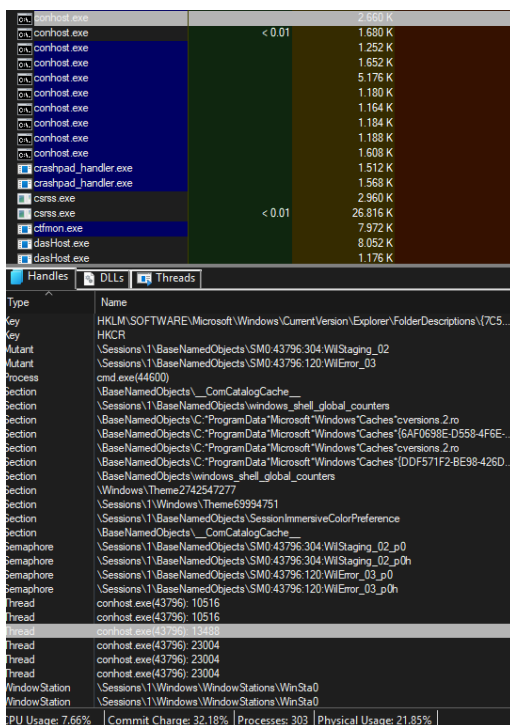
R: All'interno della scheda Threads sono visibili i seguenti dati per ogni thread attivo:

- **TID (Thread ID):** l'identificatore univoco del thread, ad esempio 10516, 13488 e 23004.
- **Start Address:** l'indirizzo (con offset) da cui è stato avviato ciascun thread all'interno del modulo conhost.exe, ad esempio conhost.exe+0x25fe0.



5. Esaminare gli handle. A cosa puntano gli handle?

Esaminiamo ora gli handles. In alto a sinistra clickiamo su → View → Lower Pane View → Handles



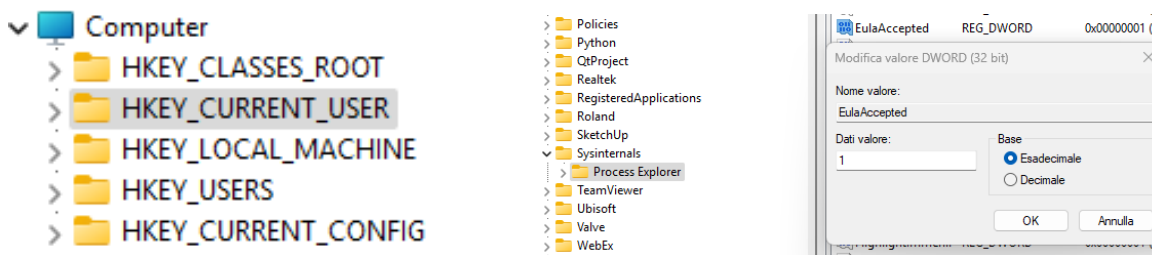
R: Gli handle del processo conhost.exe puntano a diversi tipi di oggetti gestiti dal sistema operativo Windows, tra cui:

- **Chiavi del Registro di sistema**, come HKLM\SOFTWARE\...
- **File di cache** e altri file di sistema aperti
- **Oggetti di sincronizzazione** come mutex (Mutant), eventi (Event) e semafori (Semaphore)
- **Thread** interni del processo stesso
- **Processi esterni**, ad esempio il processo cmd.exe
- **Sezioni di memoria condivisa**
- **WindowStation**, che rappresenta il contesto grafico del processo

Questi handle sono essenziali per permettere al processo conhost.exe di comunicare con il sistema operativo e con altri processi in modo sicuro ed efficiente.

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

Su start cerchiamo 'Regedit' e avviamolo come amministratore, l'editor del registro di cinque 'Hive'



Clicchiamo su HKEY_CURRENT_USER → Software → Sysinternals → Process Explorer → EulaAccepted → doppio click, e vediamo che il valore è impostato su 1, cambiamolo impostandolo su 0 e rispondiamo alla domanda.

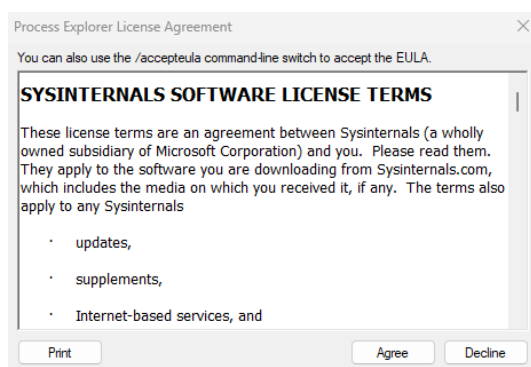
R: 0x00000001 (1) è il formato standard con cui il Registro di Windows mostra i valori DWORD:

- 0x00000001 è la rappresentazione esadecimale.
- (1) è la rappresentazione decimale.

Quando il valore viene modificato a 0, apparirà così: 0x00000000 (0), ovvero quando è a 1 – l'utente ha accettato l'EULA, quando è a 0 l'utente non ha ancora accettato l'EULA.

7. Quando apri Process Explorer, cosa vedi?

R: Una volta impostata l'Eula a 0 – riapriamo Process Explorer, e ci richiederà appunto di accettare di nuovo gli accordi di licenza.



Questo comportamento conferma che Process Explorer utilizza la chiave di registro EulaAccepted per memorizzare se l'utente ha accettato i termini di licenza. Modificando il valore a 0, forziamo il programma a richiederne nuovamente

EulaAccepted **REG_DWORD** **0x00000001 (1)**

l'accettazione. Una volta accettati, il valore torna automaticamente a 1. Ciò dimostra come il Registro di sistema venga utilizzato dalle applicazioni per gestire e salvare configurazioni e preferenze utente.