Esercizio di Pratica S11L1 -Esplorazione di Processi, Thread, Handle e Registro di Windows

Sergio Falcone

INTRODUZIONE

In questa parte, esplorerai i processi. I processi sono programmi o applicazioni in esecuzione. Esplorerai i processi utilizzando Process Explorer nella Suite SysInternals di Windows. Avvierai e osserverai anche un nuovo processo.

1. Esplorare un processo attivo (**Microsoft Edge**).
   Il processo di Microsoft Edge può essere terminato in Process Explorer
   Cosa è successo alla finestra del browser web quando il processo è stato terminato?

2. Avviare un altro processo (**cmd.exe**)
   Avviare un **ping** al prompt e osservare i cambiamenti sotto il processo cmd.exe.
   Cosa è successo durante il processo ping?

3. Il processo figlio conhost.exe potrebbe essere sospetto. Selezionare **Check VirusTotal.**

4. Sul processo cmd.exe, selezionare **Kill Process**.
   Cosa è successo al processo figlio conhost.exe?

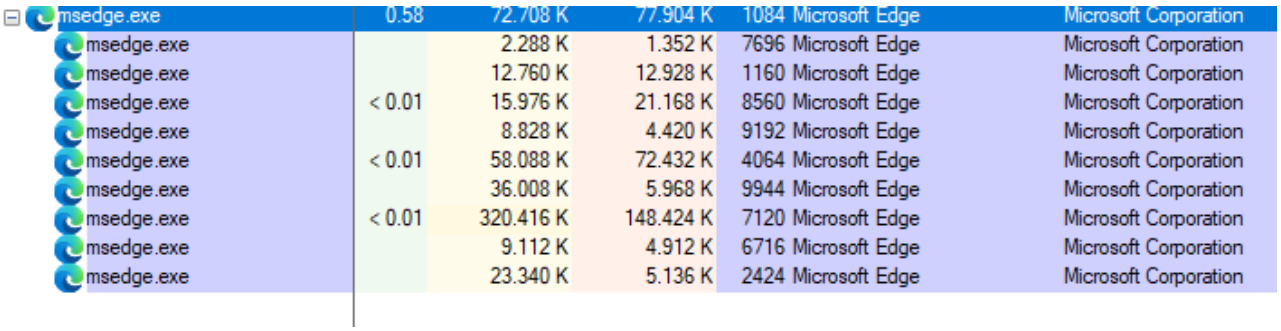
5. Esplorazione di **Thread** e **Handle** (**chhost.exe**)
   Esaminare i dettagli del thread.
   Che tipo di informazioni sono disponibili nella finestra Proprietà?
   Esplorare gli handle.
   A cosa puntano gli handle?

6. Esplorazione del Registro di Windows
   In **HKEY_CURRENT_USER**, individuare la chiave **EulaAccepted** e cambiare il valore 1 in 0
   Qual è il valore per questa chiave di registro nella colonna Dati (Data)?

7. Aprire la cartella **SysInternalsSuite** > Aprire **procexp.exe**.
   Quando apri Process Explorer, cosa vedi?

ESECUZIONE

1. Estratto e avviato **Process Explorer(procexp.exe)** il quale mostra un elenco dei processi attualmente attivi, si è localizzato il processo del browser web trascinando l'icona **Find Window's Process**

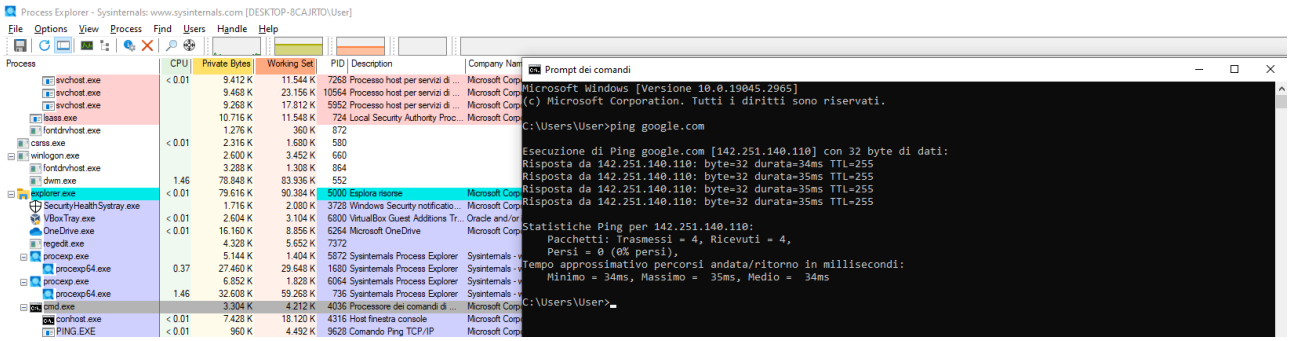


msedge.exe	0.58	72.708 K	77.904 K	1084 Microsoft Edge	Microsoft Corporation
msedge.exe		2.288 K	1.352 K	7696 Microsoft Edge	Microsoft Corporation
msedge.exe		12.760 K	12.928 K	1160 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	15.976 K	21.168 K	8560 Microsoft Edge	Microsoft Corporation
msedge.exe		8.828 K	4.420 K	9192 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	58.088 K	72.432 K	4064 Microsoft Edge	Microsoft Corporation
msedge.exe		36.008 K	5.968 K	9944 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	320.416 K	148.424 K	7120 Microsoft Edge	Microsoft Corporation
msedge.exe		9.112 K	4.912 K	6716 Microsoft Edge	Microsoft Corporation
msedge.exe		23.340 K	5.136 K	2424 Microsoft Edge	Microsoft Corporation

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

- Terminato il processo (**Kill Process**) la finestra del browser si è chiusa.

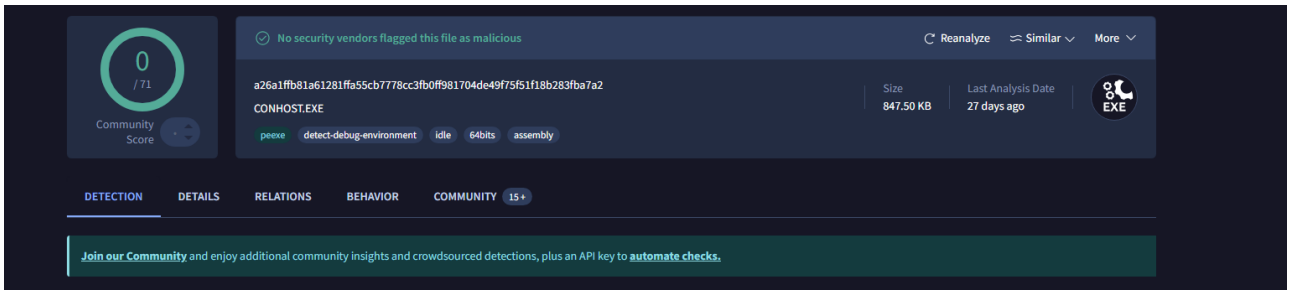
2. Si è avviato il Prompt dei Comandi (**cmd.exe**) e si è effettuato il **ping** verso google.com (**ping google.com**)



Cosa è successo durante il processo ping?

- Durante il processo di ping si è creato il processo temporaneo **PING.EXE**, il quale è sparito una volta terminato il processo di ping

3. Con il tasto destro su **conhost.exe** si è effettuato il check con **VirusTotal**



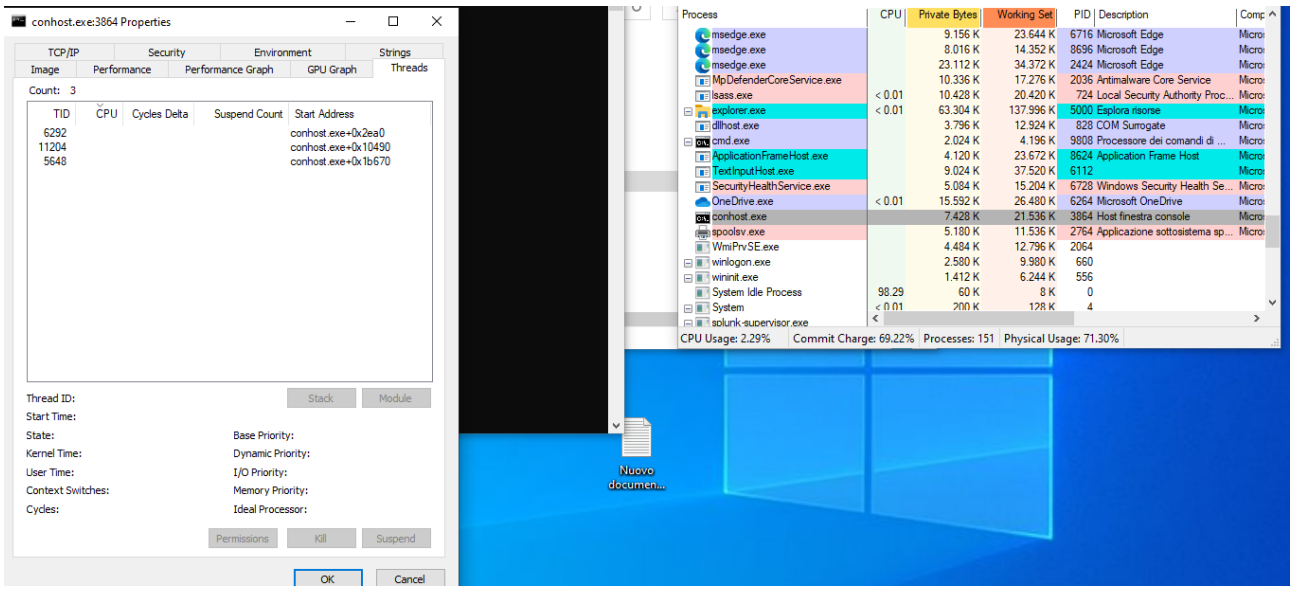
- Process Explorer calcola l'**hash** di **conhost.exe** e invia l'**hash** a **VirusTotal,** il browser mostra il report (0/70)

4. Si seleziona **Kill Process** su **cmd.exe**

   Cosa è successo al processo figlio conhost.exe?

   - Entrambi i processi si sono illuminati e chiuso il processo **cmd.exe** si è chiuso anche il processo **conhost.exe**

5. Vengono esaminati i dettagli del **thread.**
   I thread sono le unità di esecuzione all'interno di un processo. Più thread possono appartenere allo stesso processo e condividono memoria e risorse, ma ciascun thread ha il proprio flusso di esecuzione e stack

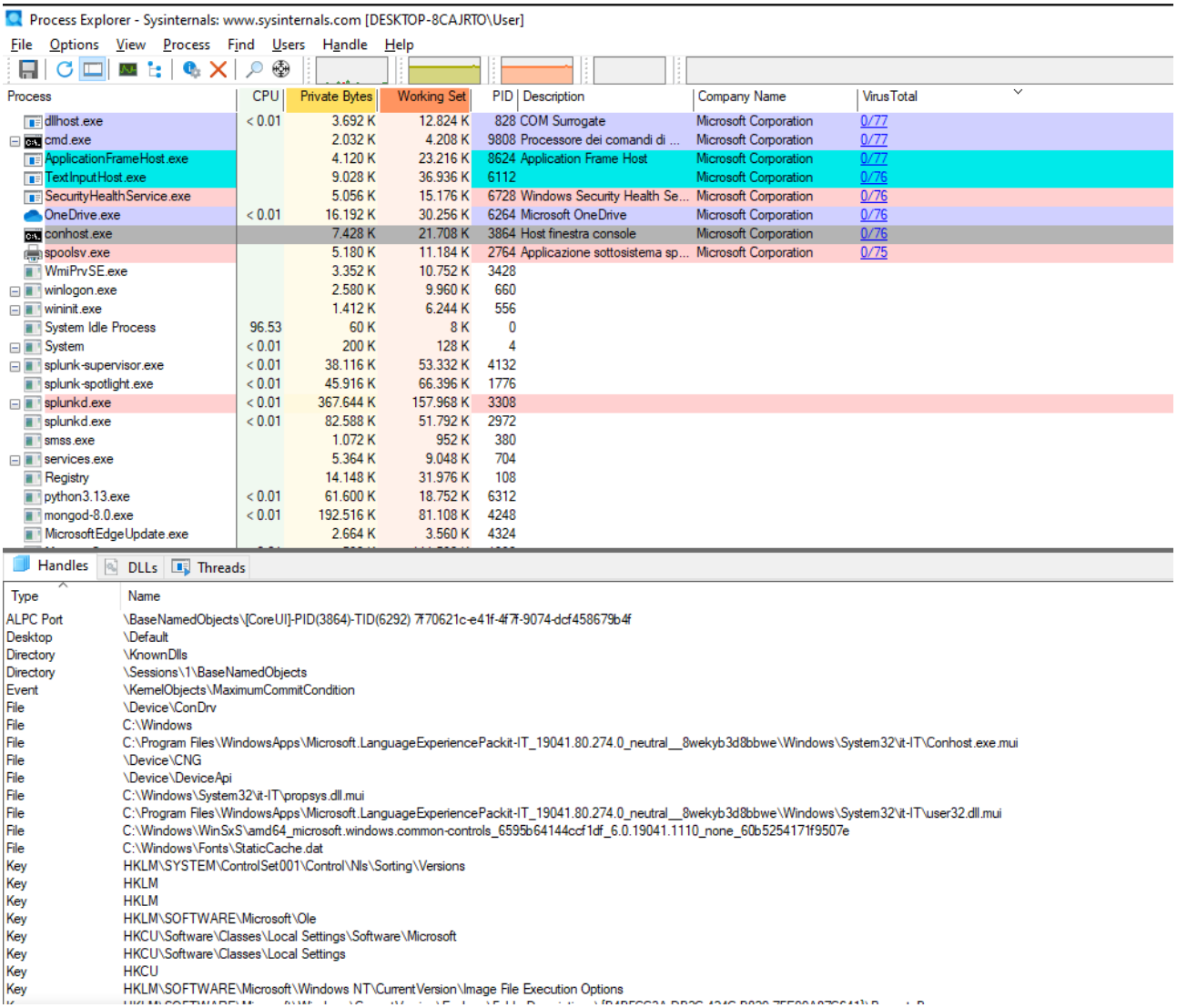


Che tipo di informazioni sono disponibili nella finestra Proprietà?

- Nella finestra delle Proprietà, nella sezione Threads sono disponibili Thread ID (TID) e Start Address, CPU cioè l'utilizzo di risorse e lo stato dei threads. Queste informazioni permettono di analizzare il

comportamento del processo, il carico di lavoro dei singoli thread e l'interazione con il sistema operativo.

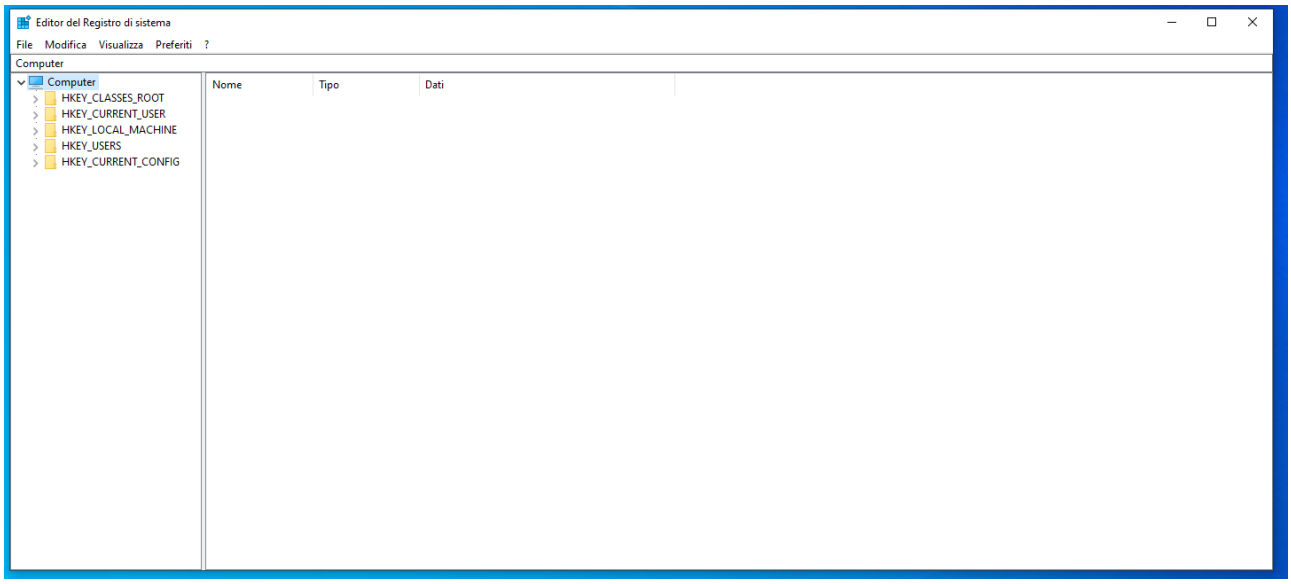
Si esplorano gli Handles.
Un handle è un riferimento astratto creato dal sistema operativo per accedere a risorse interne e permette al processo di interagire con risorse senza conoscere direttamente gli indirizzi fisici o la struttura interna dell'oggetto.

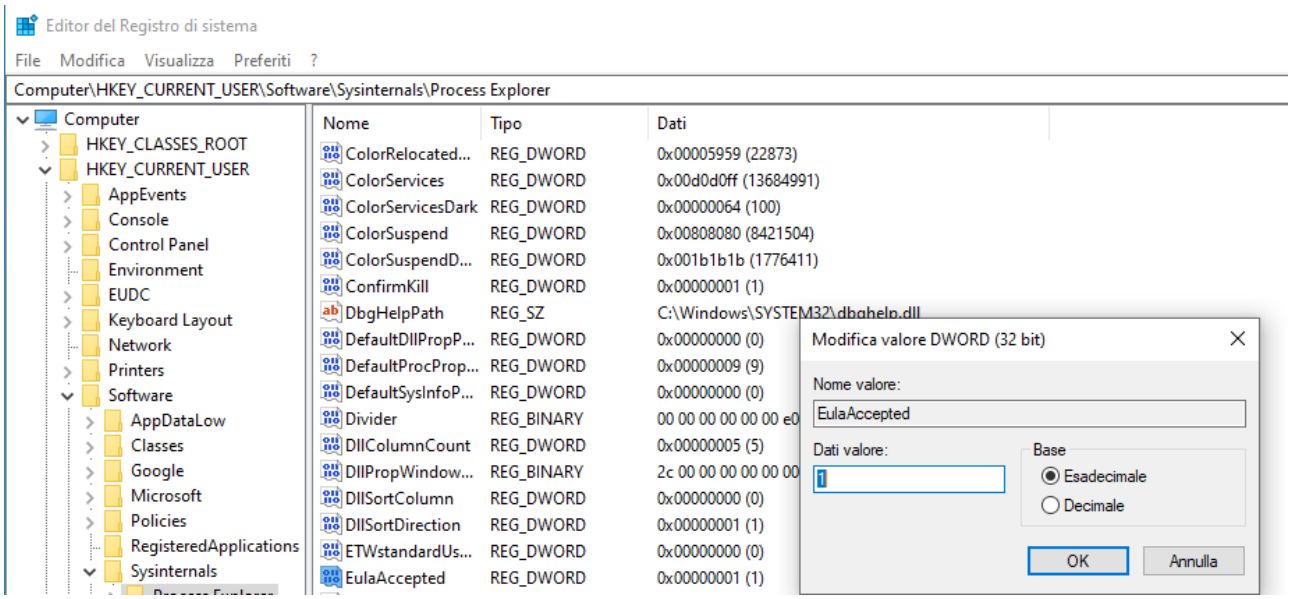


A cosa puntano gli handle?

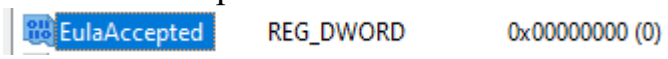
- Gli Handle puntano a risorse gestite dal sistema operativo come file, chiavi di registro, sezioni di memoria e threads

6. Si accede al registro di Window attraverso **Regedit**.
   In **HKEY_CURRENT_USER** si seleziona Process Explorer e si individua la chiave **EulaAccepted**





Il valore 1 indica che l'EULA è stato accettato dall'utente.
Si modifica il parametro da 1 a 0

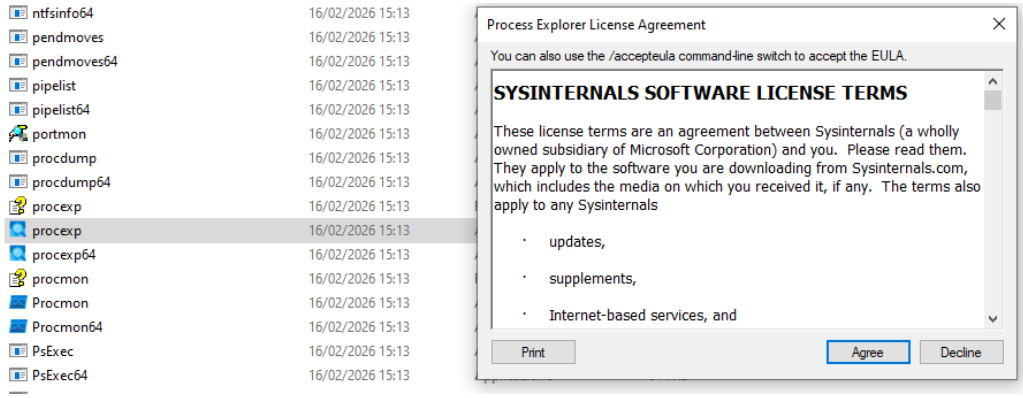


Qual è il valore per questa chiave di registro nella colonna Dati (Data)?

- Il valore del registro nella colonna Data si modifica **da 0x00000000(1)** a **0x000000000 (0)**

Quando apri Process Explorer, cosa vedi?

- Quando si riapre Process Explorer ricompare la sezione per accettare i termini di utilizzo.


ntfsinfo64 16/02/2026 15:13
pendmoves 16/02/2026 15:13
pendmoves64 16/02/2026 15:13
pipelist 16/02/2026 15:13
pipelist64 16/02/2026 15:13
portmon 16/02/2026 15:13
procdump 16/02/2026 15:13
procdump64 16/02/2026 15:13
procexp 16/02/2026 15:13
procexp 16/02/2026 15:13
procexp64 16/02/2026 15:13
procmon 16/02/2026 15:13
Procmon 16/02/2026 15:13
Procmon64 16/02/2026 15:13
PsExec 16/02/2026 15:13
PsExec64 16/02/2026 15:13
Process Explorer License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
updates,
supplements,
Internet-based services, and
Print
Agree
Decline