S11-L1
Cisco CyberOps

Emanuele Benedetti | 17 febbraio 2025

Consegna

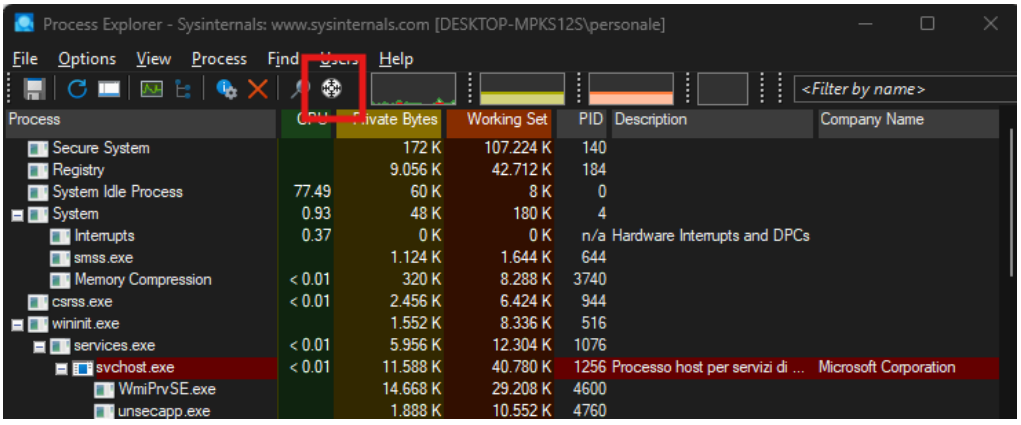
In questo laboratorio incentrato sull'esplorazione di processi, thread, handle e registri di Windows vengono approfonditi i seguenti obiettivi:

- Verifica i processi, i thread e gli handle utilizzando Process Explorer nella Sysinternals Suite
- Utilizza il Registro di Windows per modificare un'impostazione

Il laboratorio è basato sulla seguente esercitazione: https://itexamanswers.net/3-2-11-lab-exploring-processes-threads-handles-and-windows-registry-answers.html

Svolgimento

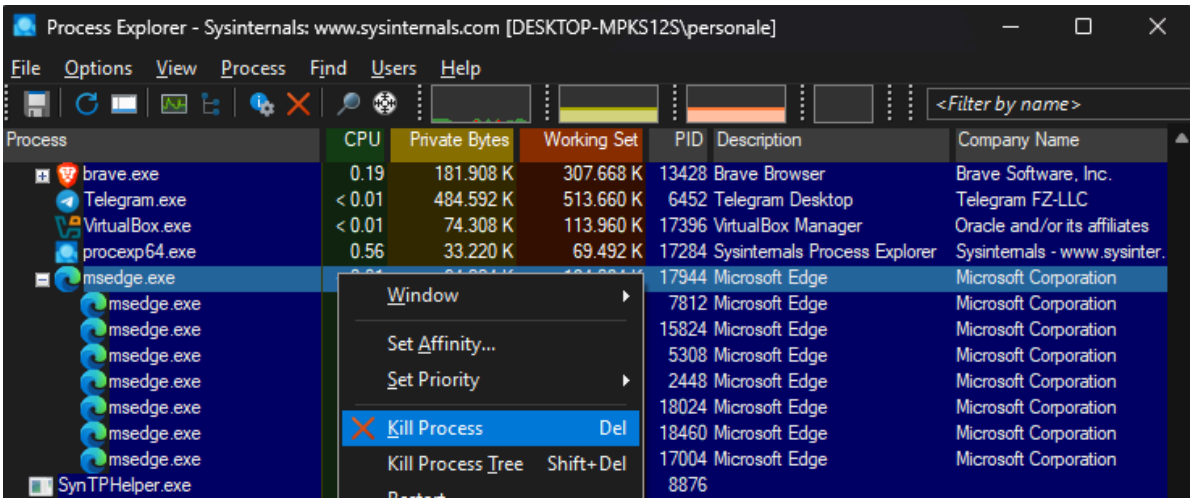
Ho iniziato l'esercitazione scaricando la Sysinternals Suite di Microsoft. Dopo aver estratto il file scaricato, ho avviato il programma *procexp.exe* ed accettato la licenza.



Il programma *Process Explorer* mostra la lista dei processi attivi.

Apriamo una finestra del browser (in questo caso *Edge*) e cerchiamo il processo avviato trascinando il tasto *Find Window's Process*, evidenziato nell'immagine precedente, sul browser.

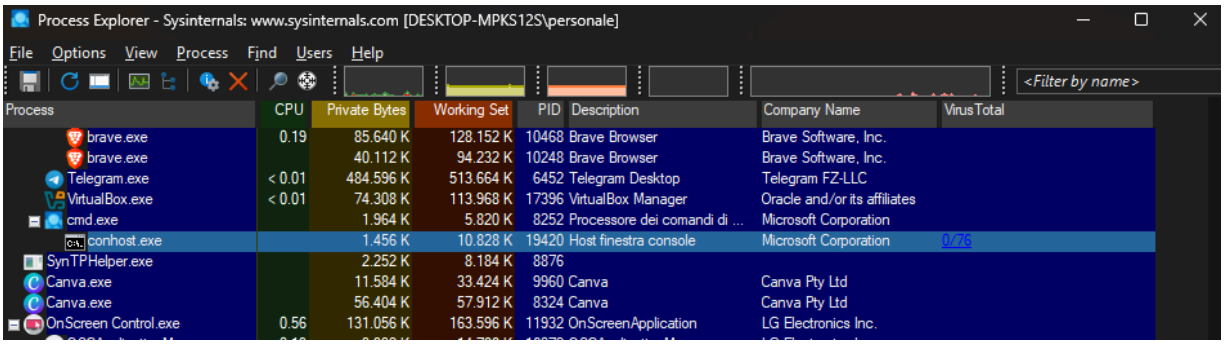
Identificato il processo, lo terminiamo con *Click destro* > *Kill Process*



Terminando il processo il programma *Edge* viene chiuso.

Apriamo ora un *Command Prompt* e cerchiamo nuovamente il relativo processo. In questo caso il processo è chiamato *cmd.exe* ed ha un processo figlio chiamato *conhost.exe*.

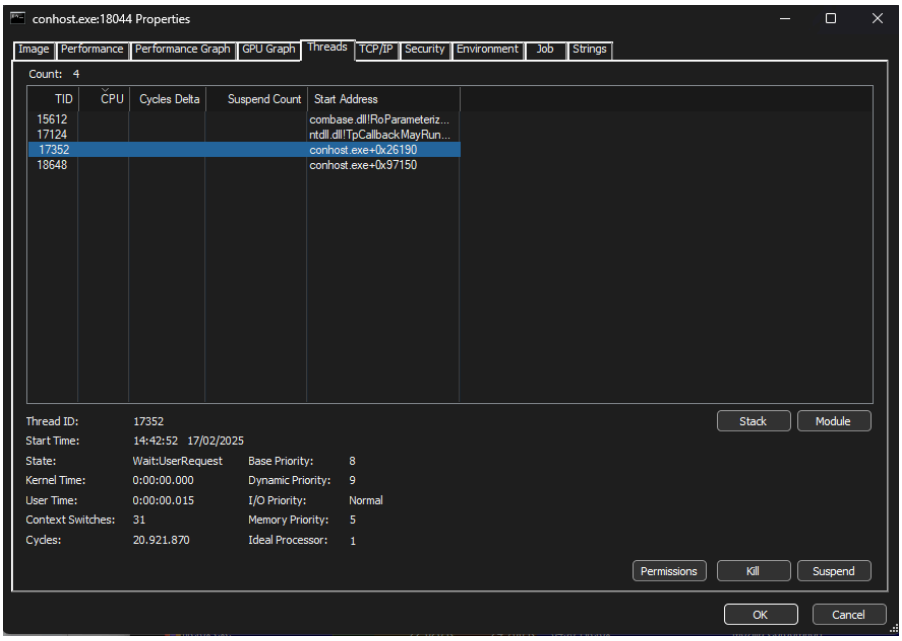
Per verificare l'attendibilità di quest'ultimo possiamo controllarlo con *Click destro* > *Check VirusTotal.com*



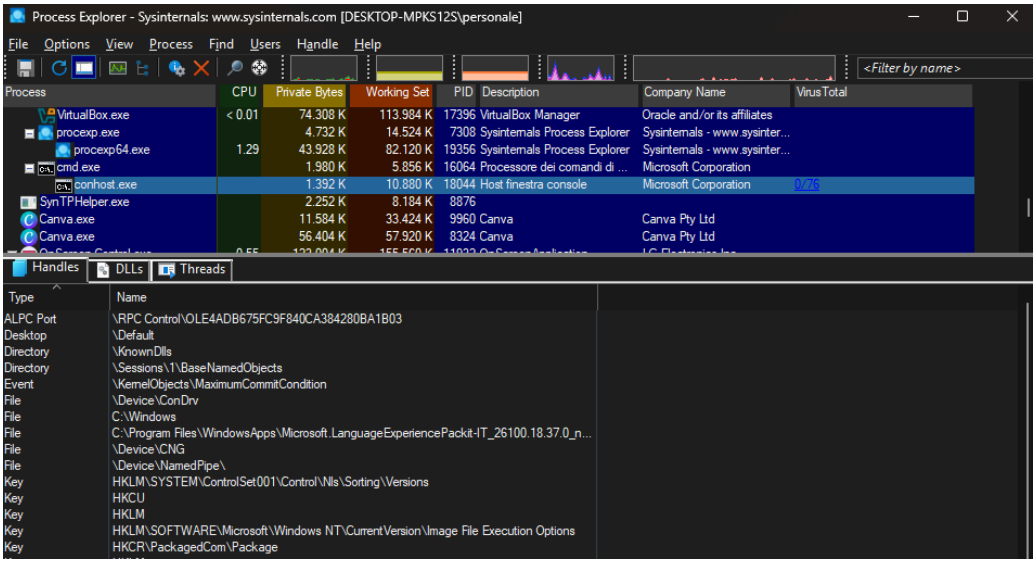
L'ultima colonna a destra mostra il risultato della scansione con VirusTotal indicando che l'hash del processo non viene identificato come sospetto o malevolo.

Chiudendo il processo *cmd.exe* viene terminato anche il processo figlio.

Riaprendo il processo e controllando le proprietà di *conhost.exe* possiamo verificare nel dettaglio le informazioni sui thread.



È inoltre possibile verificare gli handles andando su *View* > *Lowe pane view* > *Handles*

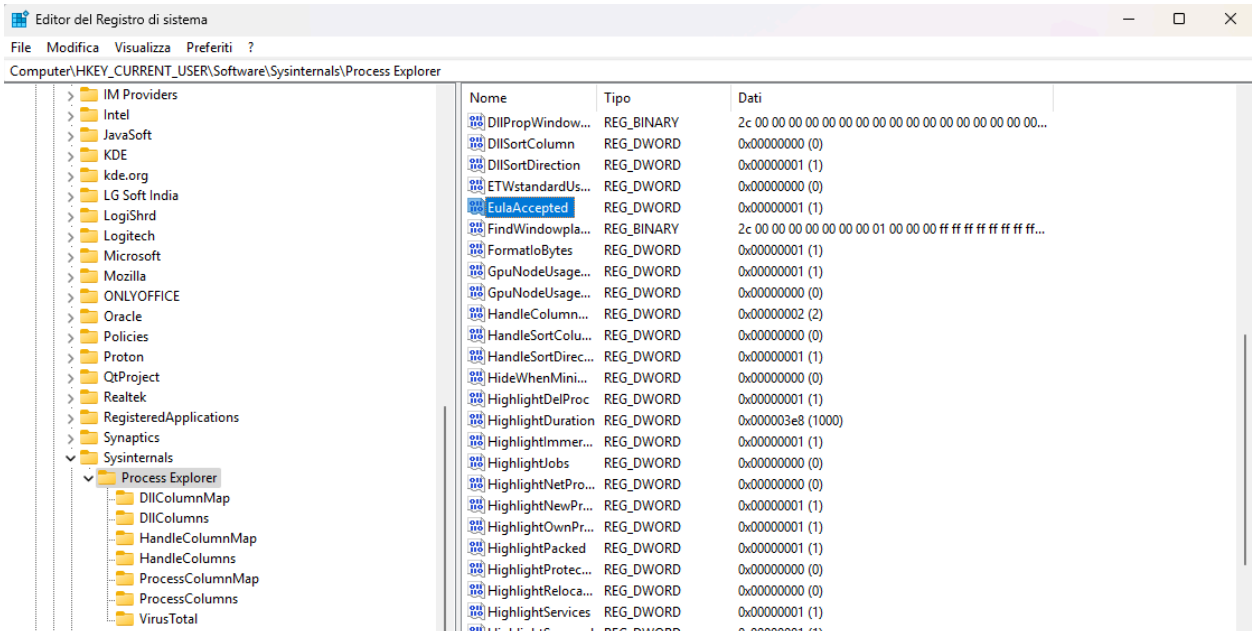


Nell'immagine è possibile apprezzare gli handles associati al processo *conhost.exe*.

Nell'ultima fase del laboratorio mi sono dedicato ai registri di Windows.

Per visualizzare i registri si può ricercare l'editor tramite *Start* > *regedit* > *Editor del Registro di sistema*.

Tramite l'applicazione possiamo modificare i valori dei registri. Ad esempio nella schermata che segue viene visualizzato il valore dell'Eula accettata durante l'esecuzione delle fasi precedenti del programma *Process Monitor*.



Concludiamo il laboratorio modificando il valore della chiave, cliccando due volte su *EulaAccepted* e cambiando il valore da *1* (accepted) a *0* (not accepted).