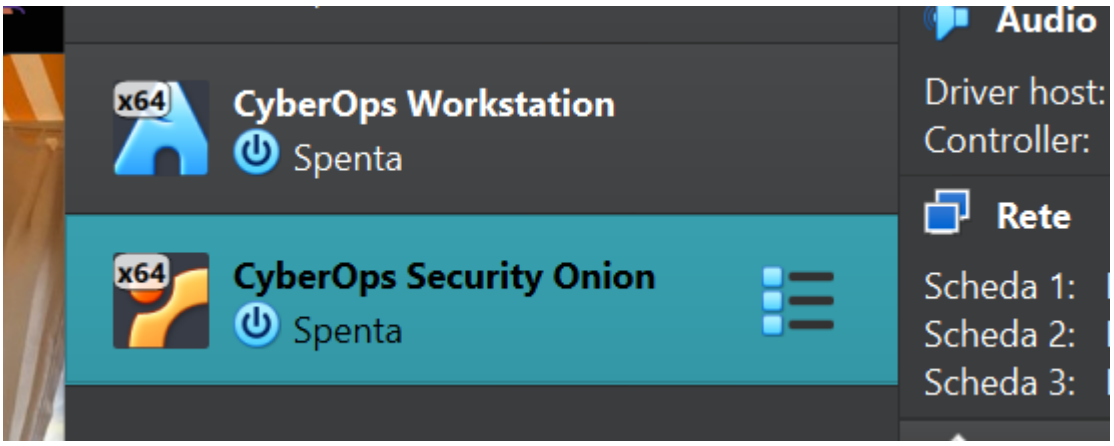
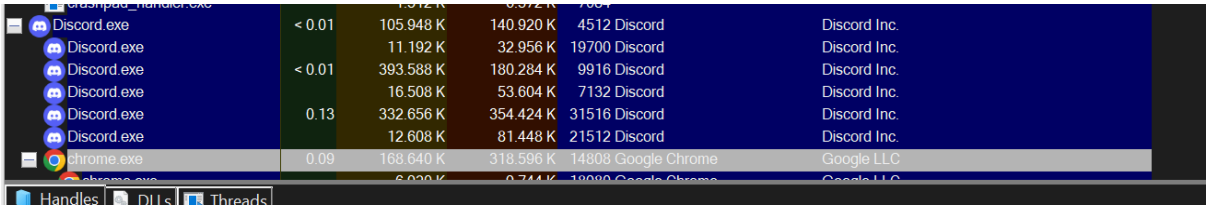
Esercizio S11L2 - CyberOps Workstation, Onion, ProcExp64.exe & RegEdit

Prova di installazione CyberOps Workstation e Onion:

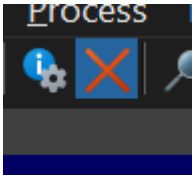


Esercizi su procexp64.exe:

Individuazione con drag & drop di servizi all'interno di procexp



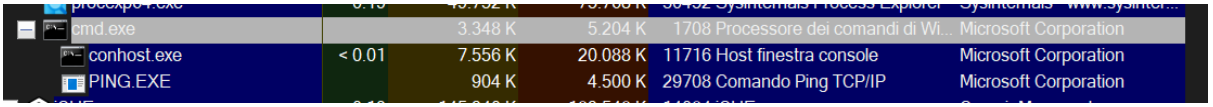
Dimostrazione di kill process da comando



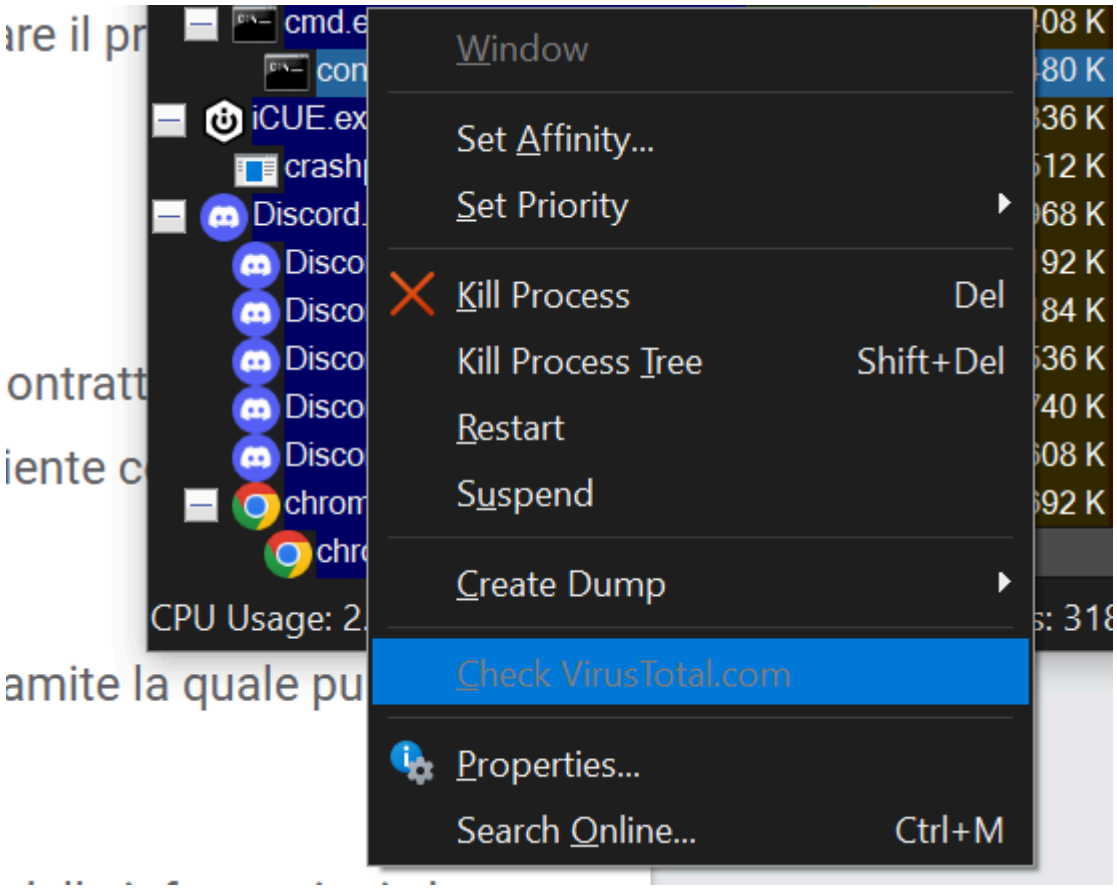
Esplorazione di creazione di nuovi sottoprocessi in tempo reale attraverso un ping da cmd.exe:

```
C:\Users\uomos>ping 192.168.1.250

Esecuzione di Ping 192.168.1.250 con 32 byte di dati:
Risposta da 192.168.1.196: Host di destinazione non raggiungibile.
Risposta da 192.168.1.196: Host di destinazione non raggiungibile.
Risposta da 192.168.1.196: Host di destinazione non raggiungibile.
Risposta da 192.168.1.196: Host di destinazione non raggiungibile.

Statistiche Ping per 192.168.1.250:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
```

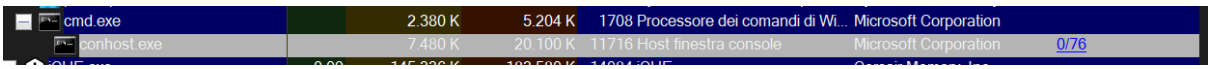
Visibilità di PING.EXE che rappresenta il ping comandato:



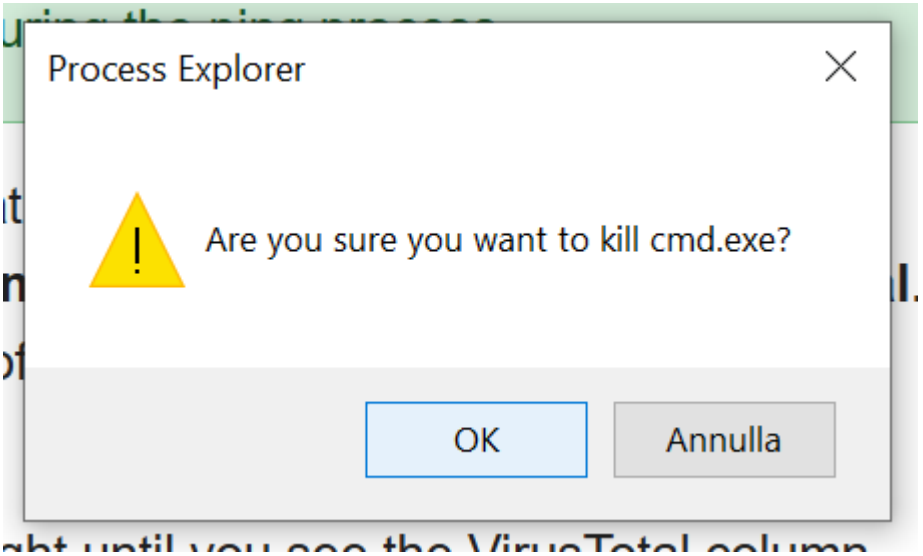
Check da VirusTotal.com per sicurezza e vulnerabilità dei singoli servizi:



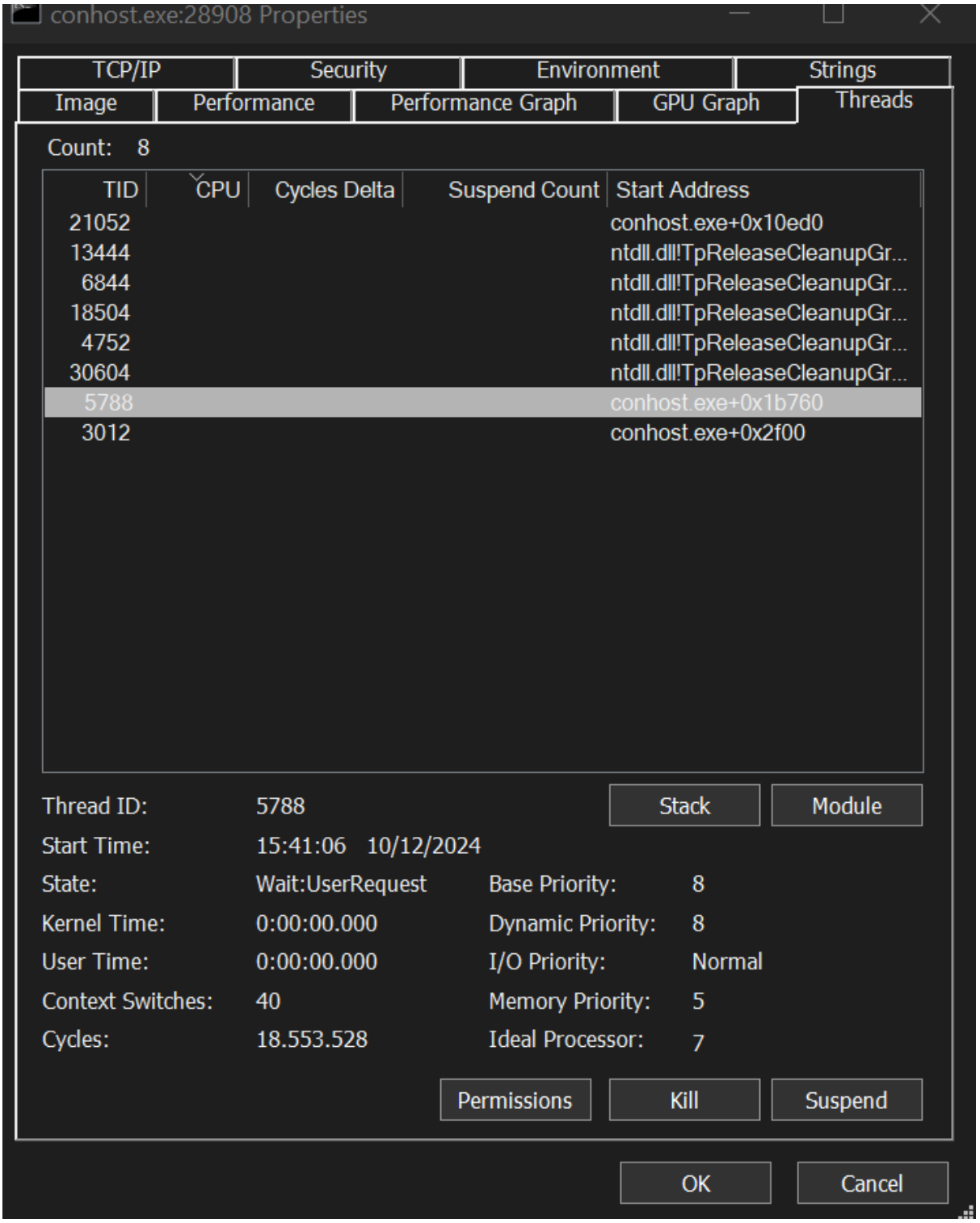
Risultato su conhost.exe, 0/76:



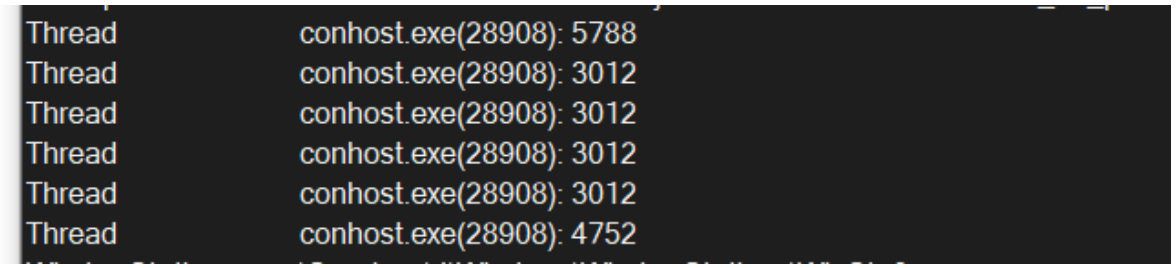
Kill di processo cmd.exe per dimostrazione di chiusura anche dei sottoprocessi uccidendo il processo madre:

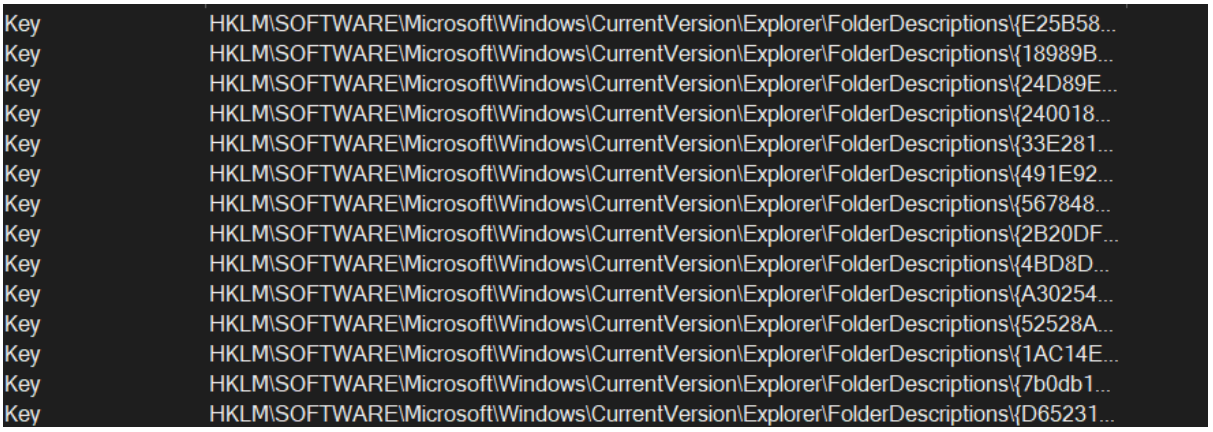


Visibilità dei Threads da procexp64.exe esplorando le proprietà del processo:



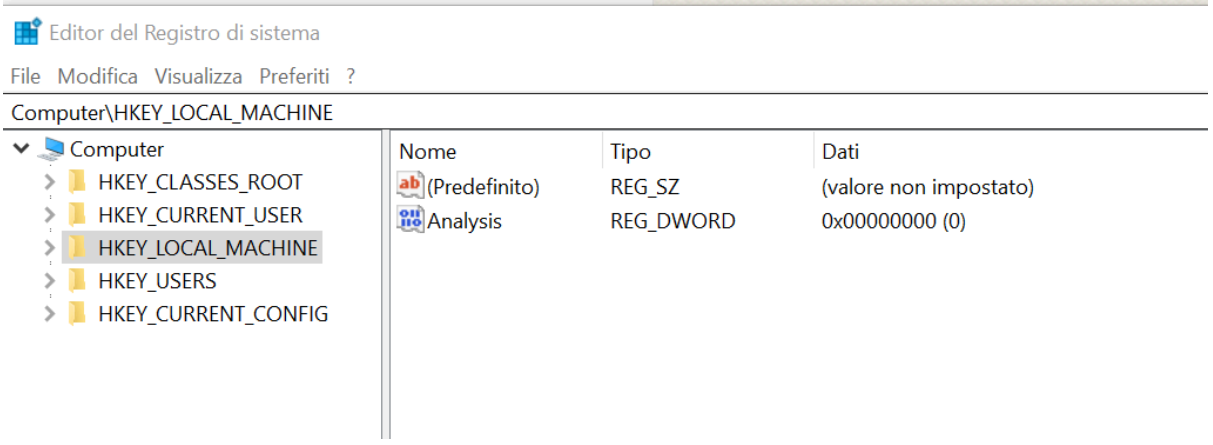
Visibilità delle handles; chiavi di registro e i threads visualizzati poco fa:



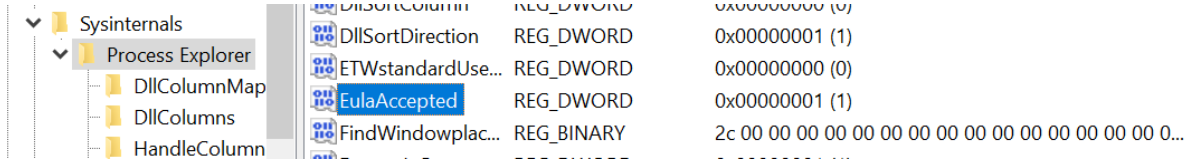


Esercizi su regedit:

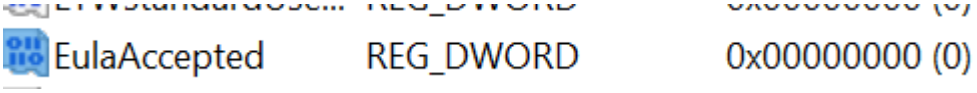
Visibilità delle chiavi dei 5 macrogruppi di chiavi di sistema:
Ub



Individuazione di procexp all'interno delle chiavi del registro, in particolare la stringa che segnala che i termini di utilizzo sono stati accettati (valore 1):



Modifica del valore 1 in valore 0, per riprodurre nuovamente la richiesta di accettazione:



Dimostrazione della ricomparsa della richiesta di accettazione dei termini di utilizzo: