Rapporto

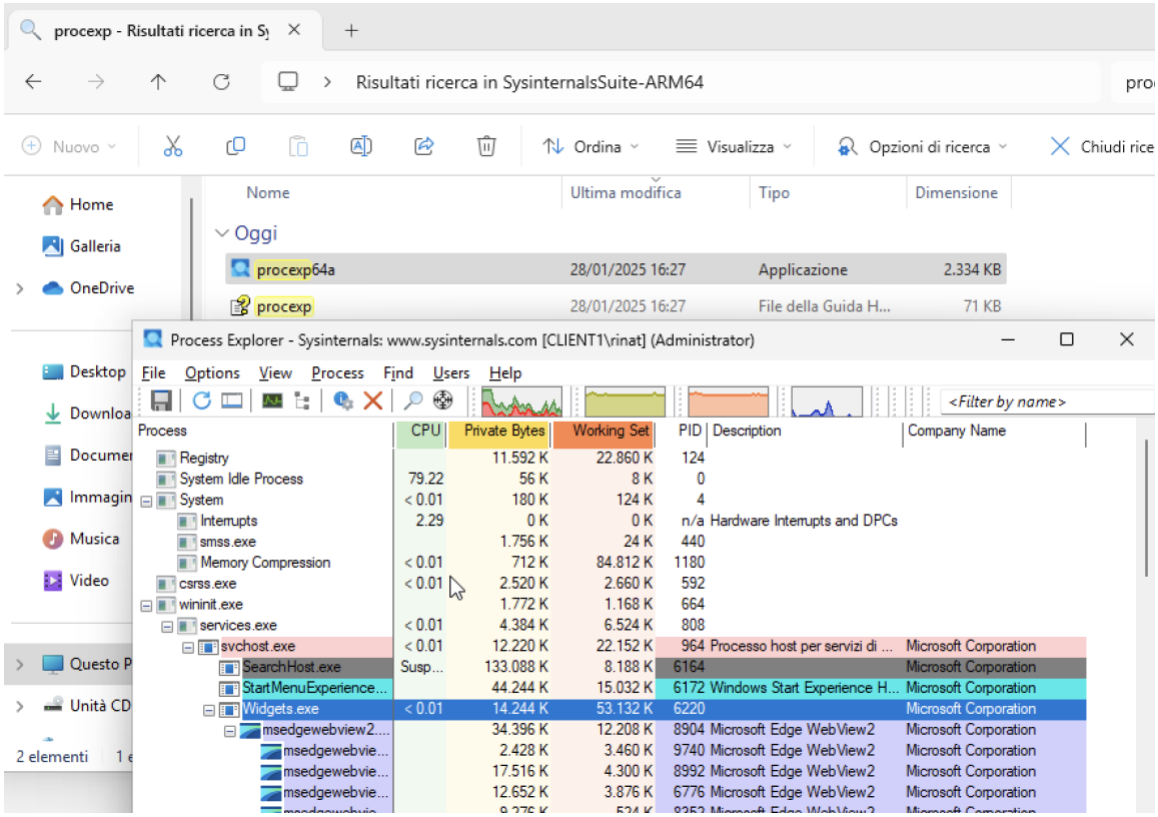
Configurazione delle macchine virtuali:

Ho configurato le VM, di seguito le prove:

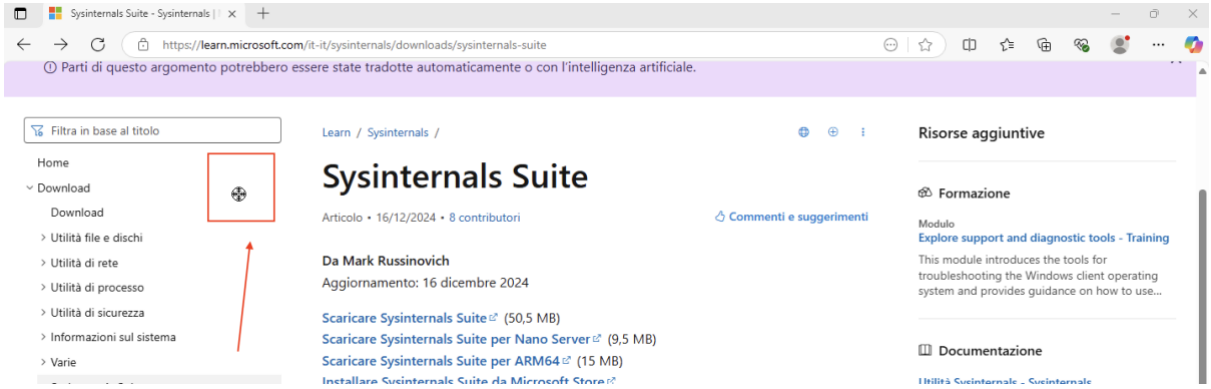
Esplorazione di Processi, Thread, Handle e Registro di Windows

Esplorazione dei processi

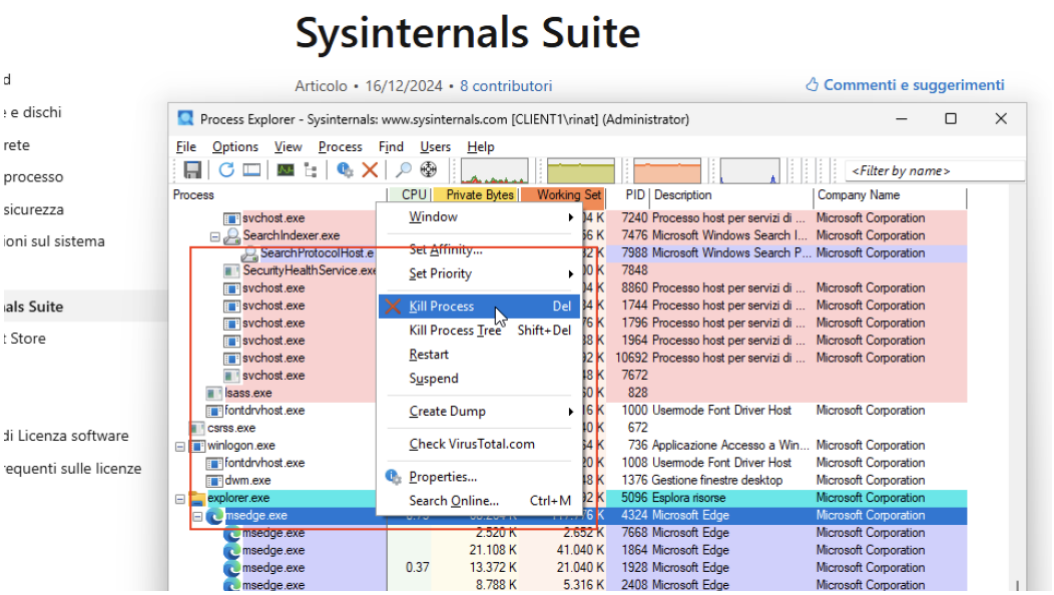
Dopo aver scaricato il file, l'ho decompresso e ho inserito il file eseguibile di procexp64a:

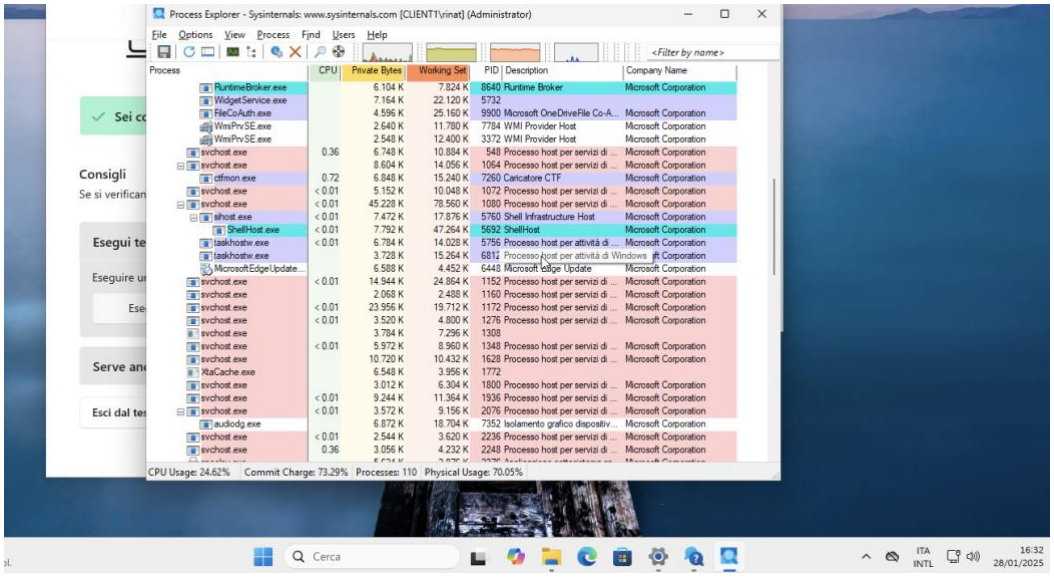


Ho quindi trascinato l'icona del processo di Windows sulla pagina web:

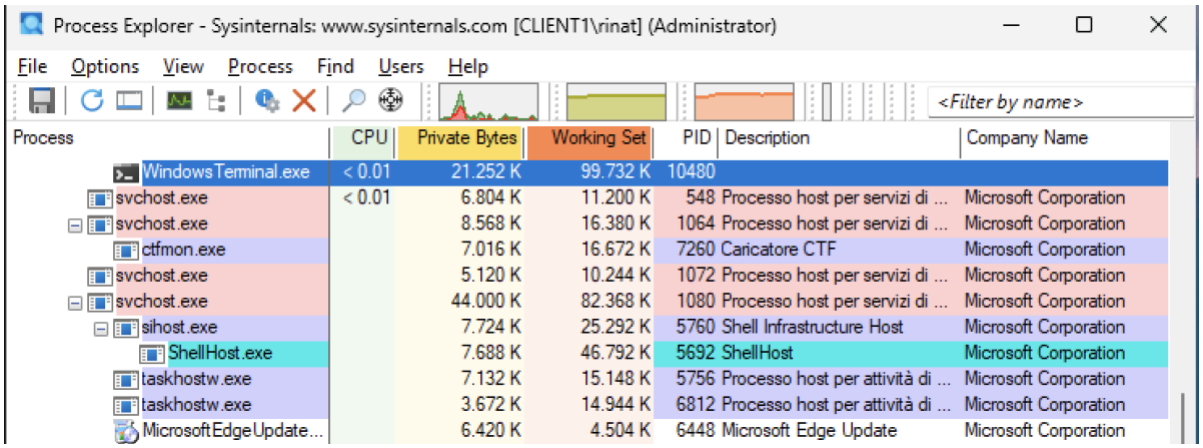


Poi ho ucciso il processo. La pagina web è stata immediatamente chiusa:

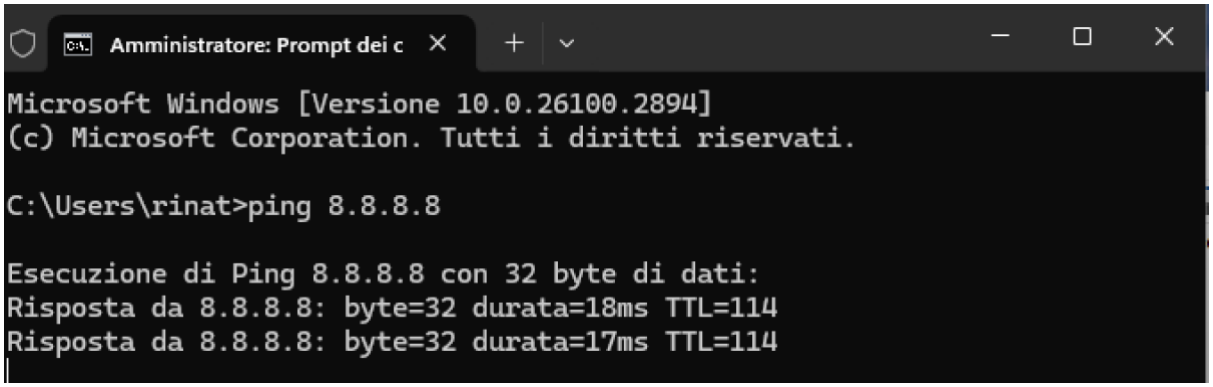


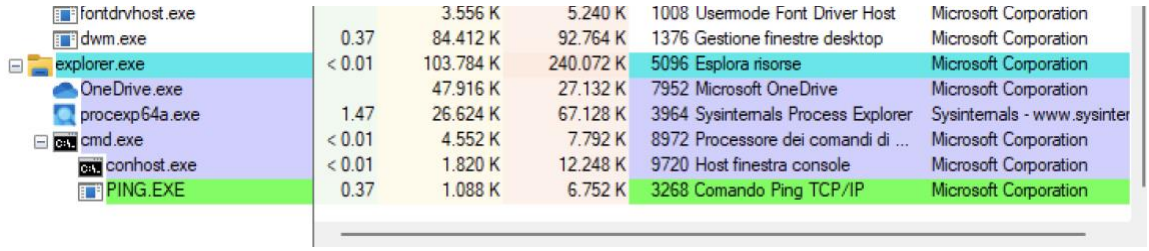


Poi ho aperto cmd e l'ho trovato:



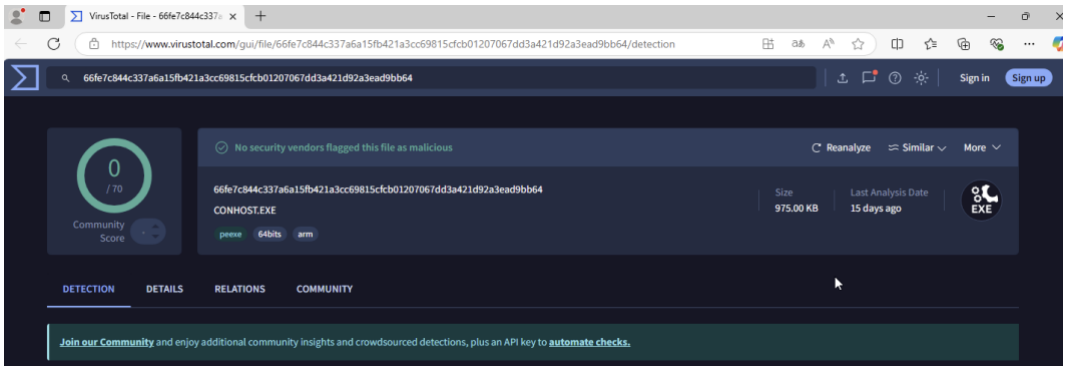
Si chiama Windows Terminal.exe. Di seguito ho trovato cmd sotto il processo padre Explorer. Quando faccio ping, viene creato un altro processo figlio sotto cmd:





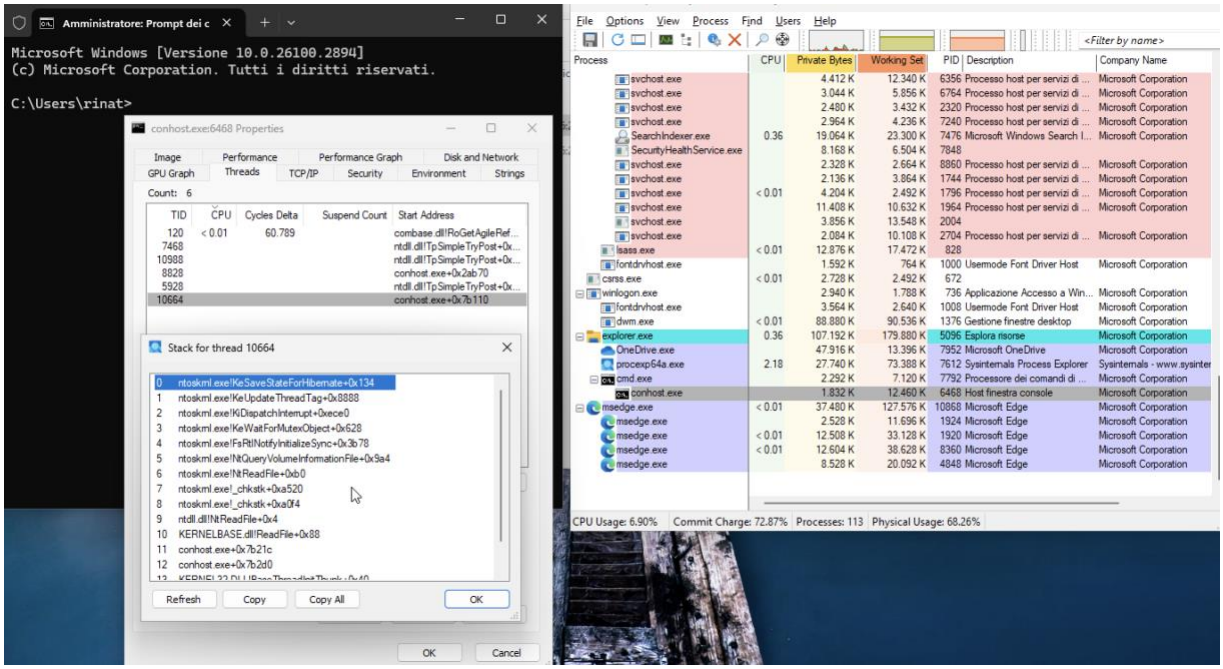
Quando clicco su controlla virustotal per conhost.exe, si nota un cambiamento visibile:

Quando clicco sul numero, si apre una nuova pagina web con la scansione Virustotal:ù



Esplorazione di thread e gli handle

Ho fatto clic con il pulsante destro del mouse su conhost.exe e ho selezionato Proprietà….. Quindi ho fatto clic sulla scheda Thread per visualizzare i thread attivi per il processo conhost.exe:

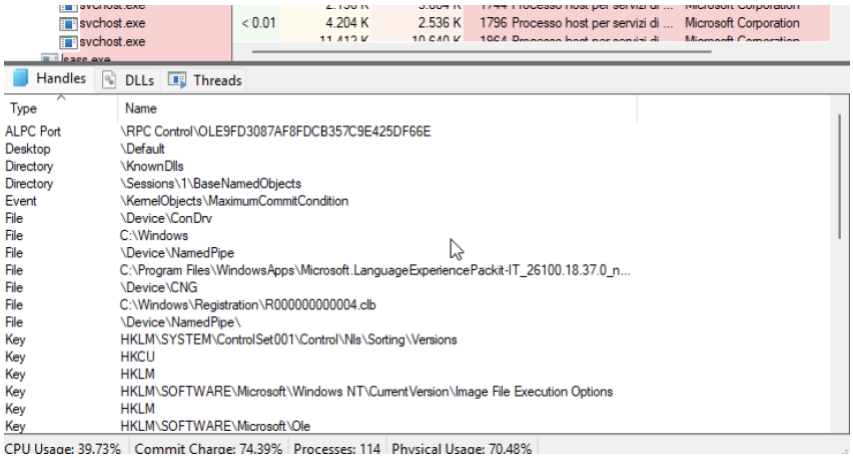


Queste chiamate di funzione e indirizzi di memoria dal kernel di Windows (ntoskrnl.exe) e dalle librerie di sistema (ntdll.dll, KERNELBASE.dll, KERNEL32.DLL) in genere compaiono nei crash dump o nelle tracce dello stack. Indicano funzioni di sistema come la gestione dei thread, le operazioni sui file e la gestione della memoria. Punti chiave:

- ntoskrnl.exe gestisce la gestione dei thread, lo stato del sistema e gli interrupt.
- ntdll.dll e KERNELBASE.dll gestiscono le operazioni sui file.
- conhost.exe gestisce le operazioni della console.
- KERNEL32.DLL gestisce processi e thread.
- Gli offset di funzione (ad esempio, +0x134) mostrano le posizioni delle operazioni.

Ciò aiuta a diagnosticare crash correlati alla gestione dei file, alla memoria o ai thread.

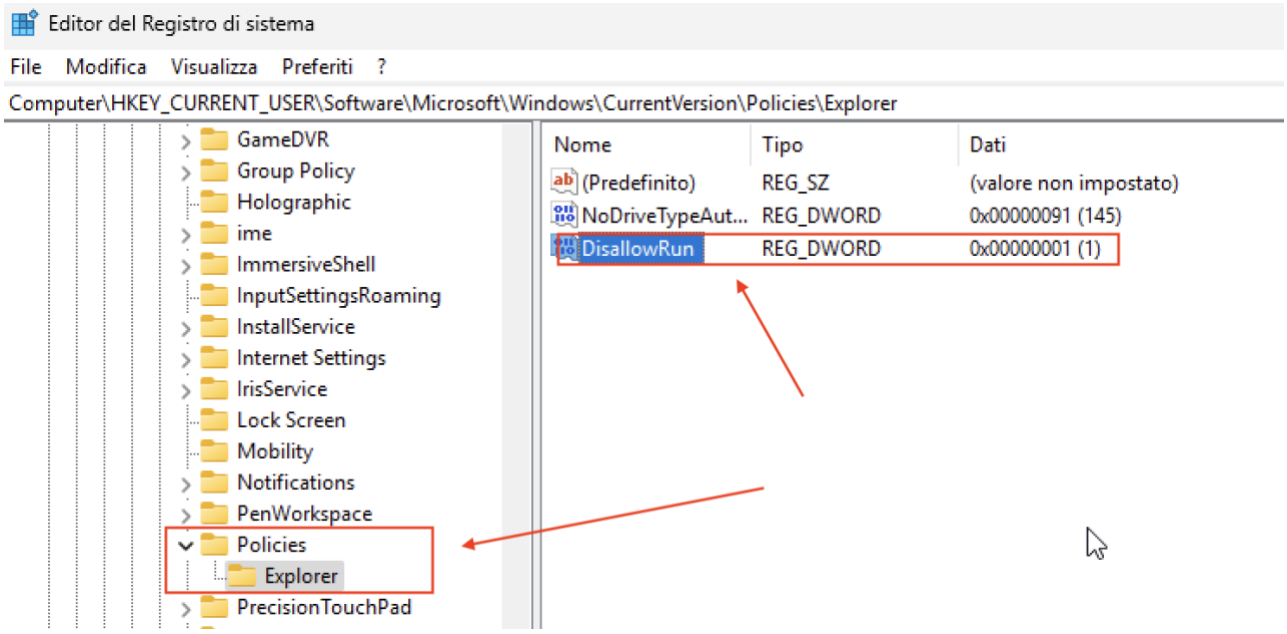
Quindi in Process Explorer, fatto clic su Visualizza > seleziona Visualizzazione riquadro inferiore > Handle per visualizzare gli handle associati al processo conhost.exe:

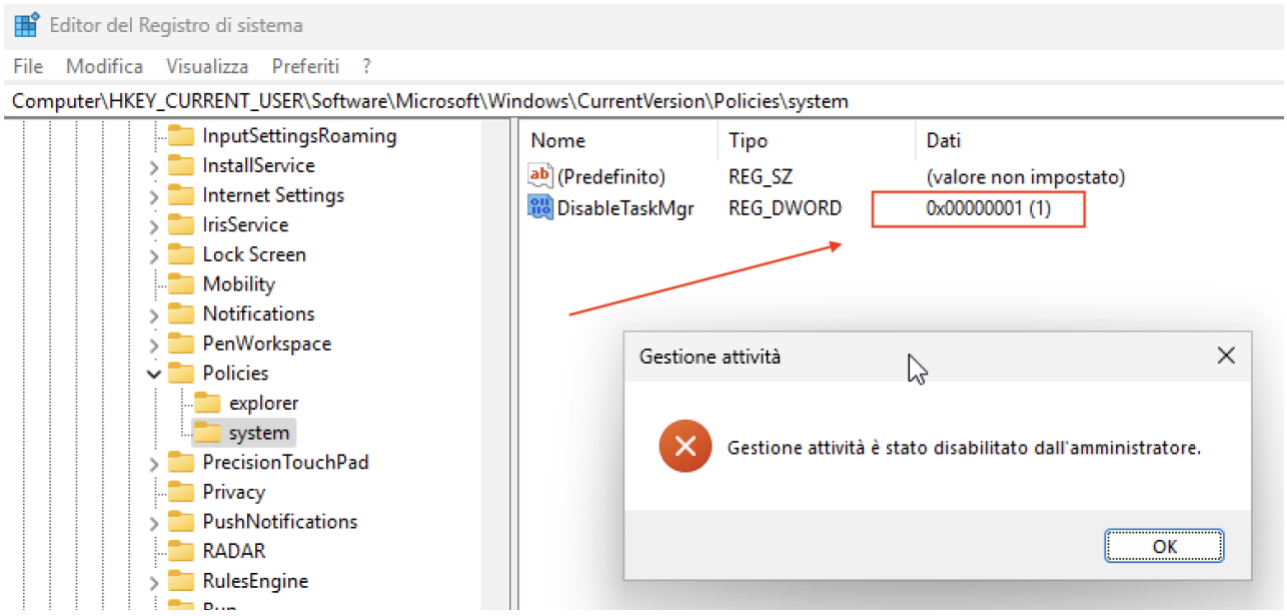


Gli handle puntano a file, chiavi di registro e thread.

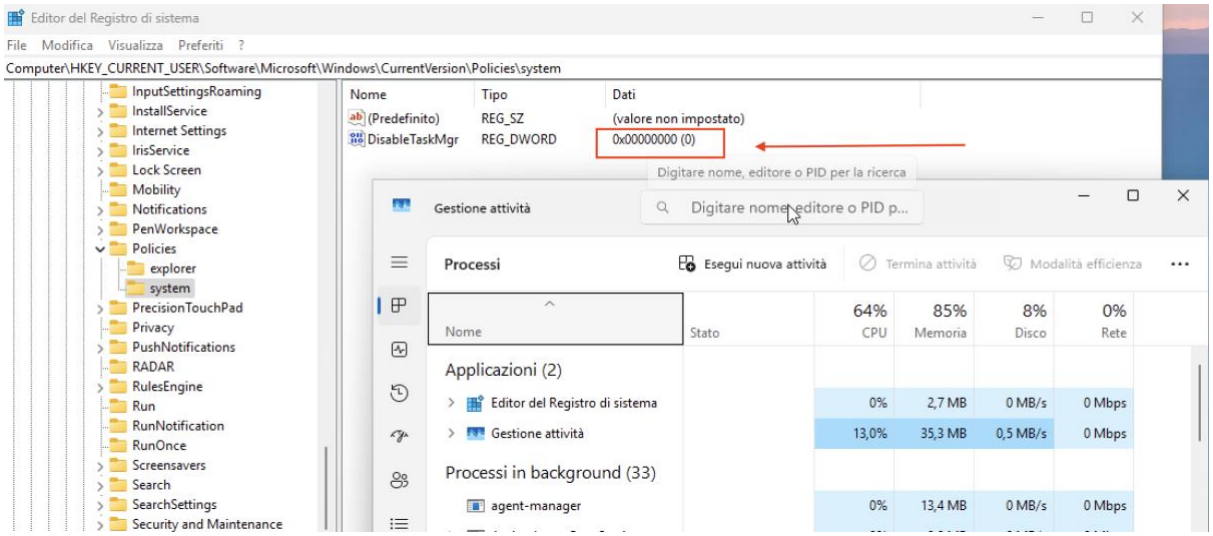
Utilizza il Registro di Windows per modificare un'impostazione

Sono entrato nell'Editor del Registro di sistema di Windows, ho seguito il seguente percorso per creare una nuova chiave per disabilitare l'accesso al Task Manager: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\. Ho creato la chiave Sytem, e poi ho creato DWORD 32 BIT al suo interno. Per disabilitare l'accesso, ho scritto lì 1:





Come è visibile, l'accesso è negato. Quindi lo abilito di nuovo scrivendo 0:


Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\system
InputSettingsRoaming
InstallService
Internet Settings
IrisService
Lock Screen
Mobility
Notifications
PenWorkspace
Policies
explorer
system
PrecisionTouchPad
Privacy
PushNotifications
RADAR
RulesEngine
Run
RunNotification
RunOnce
Screensavers
Search
SearchSettings
Security and Maintenance
Nome
Tipo
Dati
(Predefinito)
REG_SZ
(valore non impostato)
DisableTaskMgr
REG_DWORD
0x00000000 (0)
Digitare nome, editore o PID per la ricerca
Gestione attività
Digitare nome, editore o PID p...
Processi
Esegui nuova attività
Termina attività
Modalità efficienza
Nome
Stato
64%
CPU
85%
Memoria
8%
Disco
0%
Rete
Applicazioni (2)
Editor del Registro di sistema
0%
2,7 MB
0 MB/s
0 Mbps
Gestione attività
13,0%
35,3 MB
0,5 MB/s
0 Mbps
Processi in background (33)
agent-manager
0%
13,4 MB
0 MB/s
0 Mbps