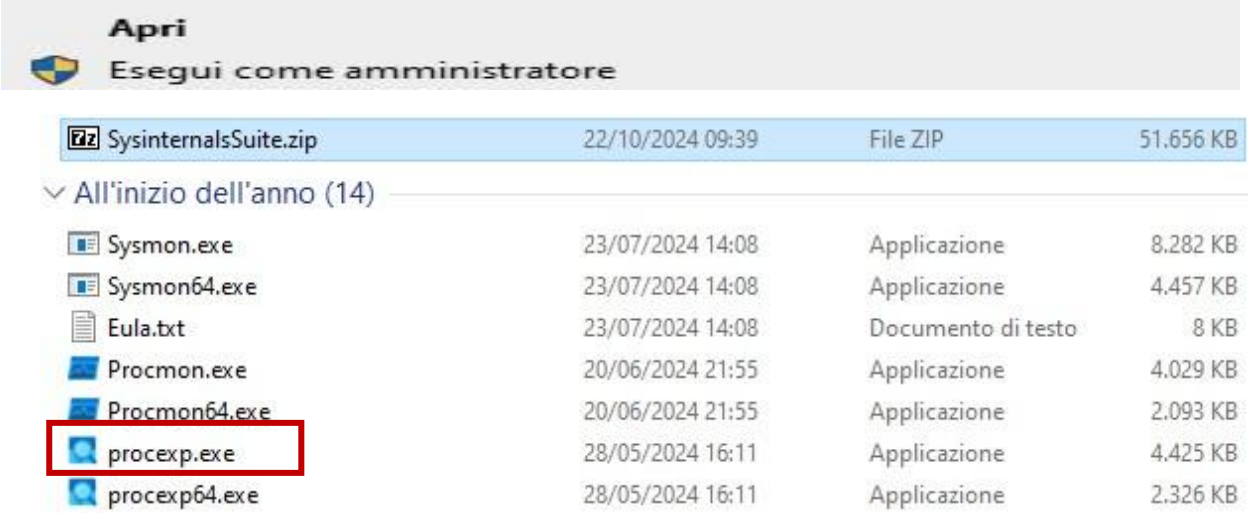
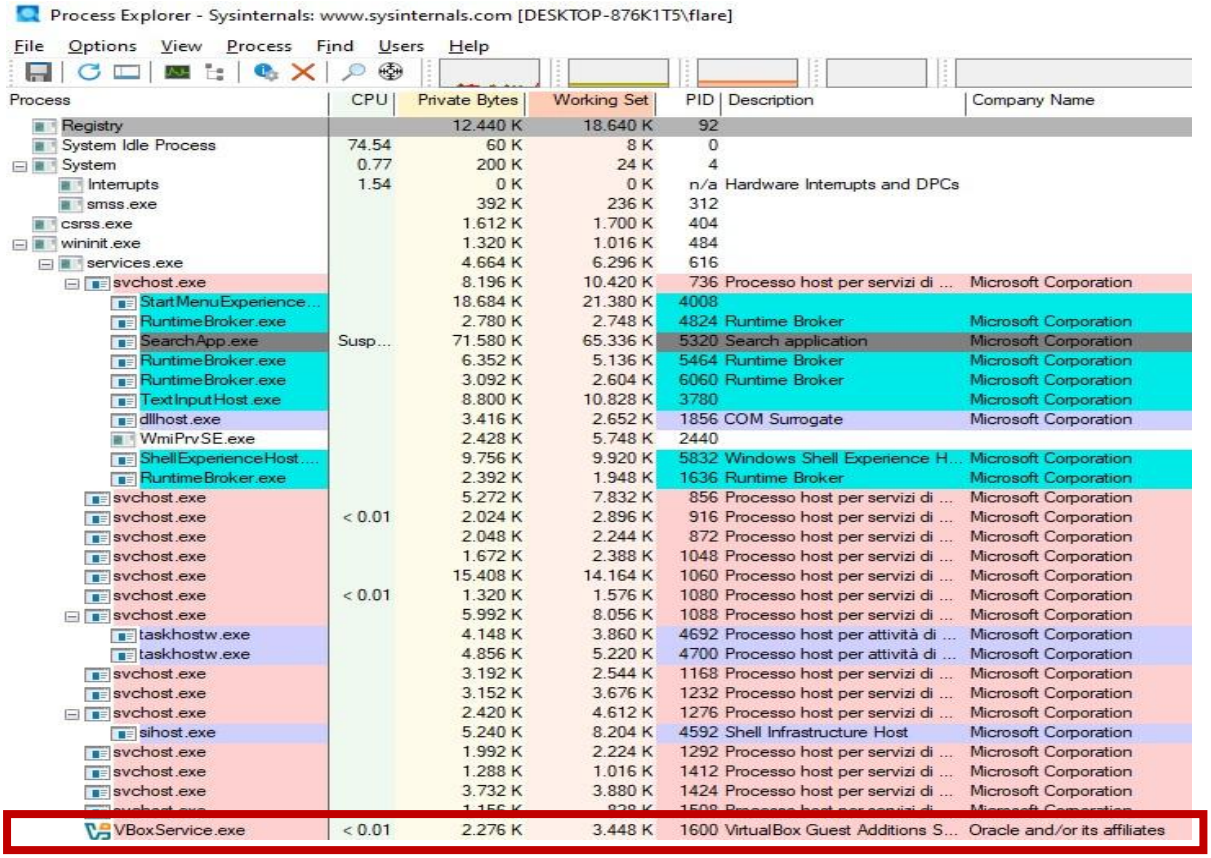
Relazione Processi – Threads – Handle e Registro di Windows

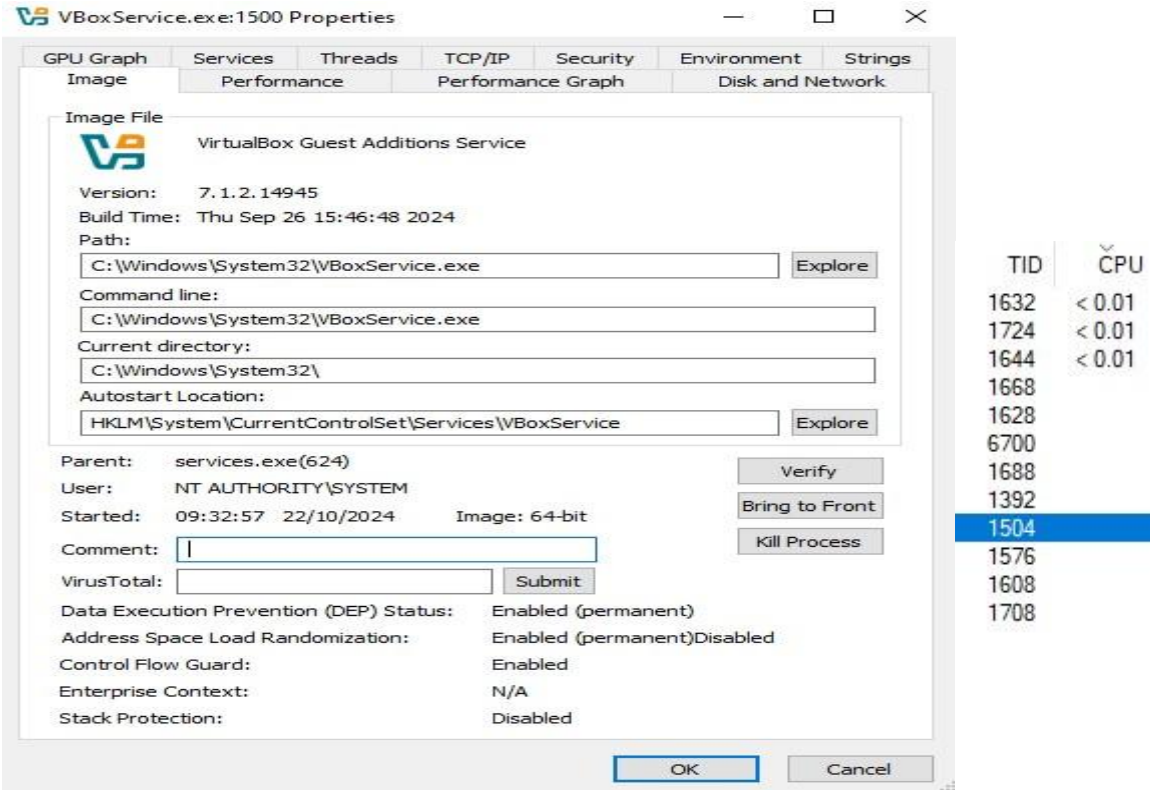
Nella seguente immagine dopo aver scaricato **SysinternalsSuite.zip** sulla macchina Windows, estraggo i file zippati, e come da immagine seguente, ho vari programmi (exe), eseguibili.
Il programma che utilizzerò per svolgere le operazioni richieste è procexp.exe, che devo eseguire con i privilegi **amministratore**

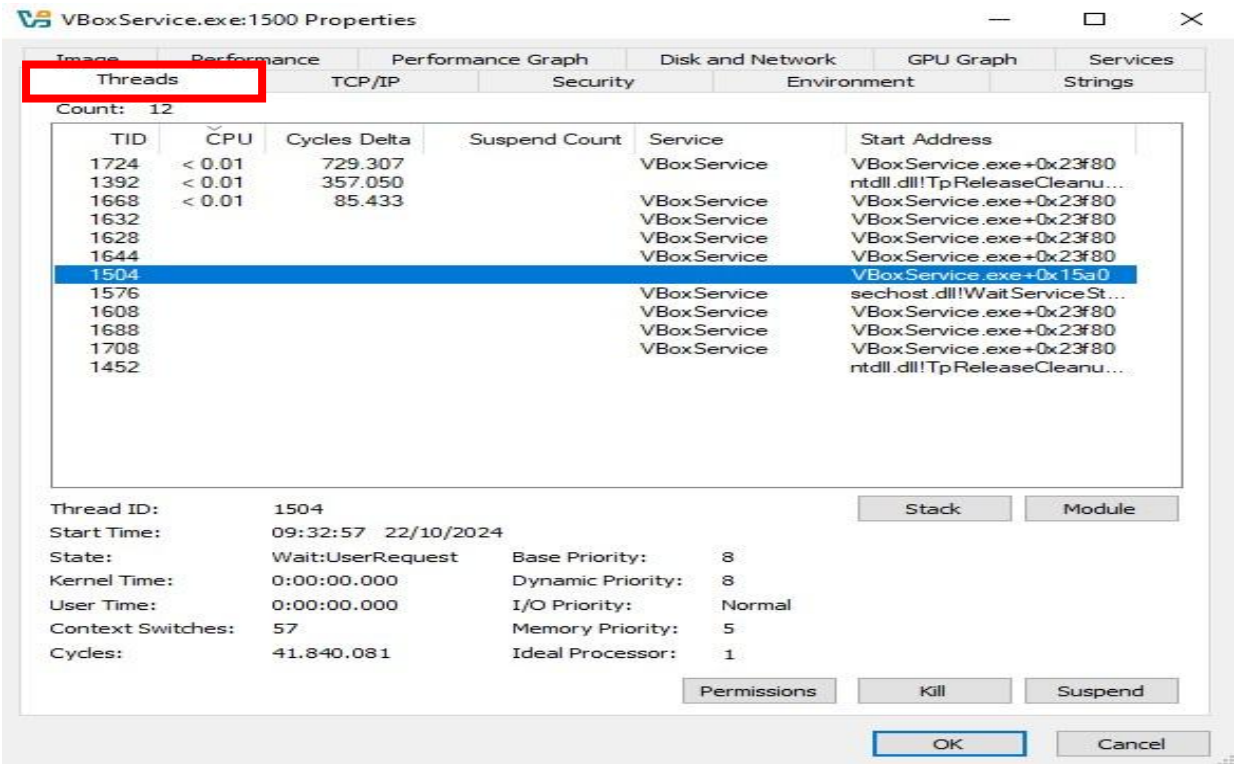


Nel passaggio successivo, dopo aver estratto i file dalla cartella **SysinternalsSuite.zip**, clicco sul file eseguibile **procexp.exe**, dove vedrò i vari processi in corso del mio sistema operativo

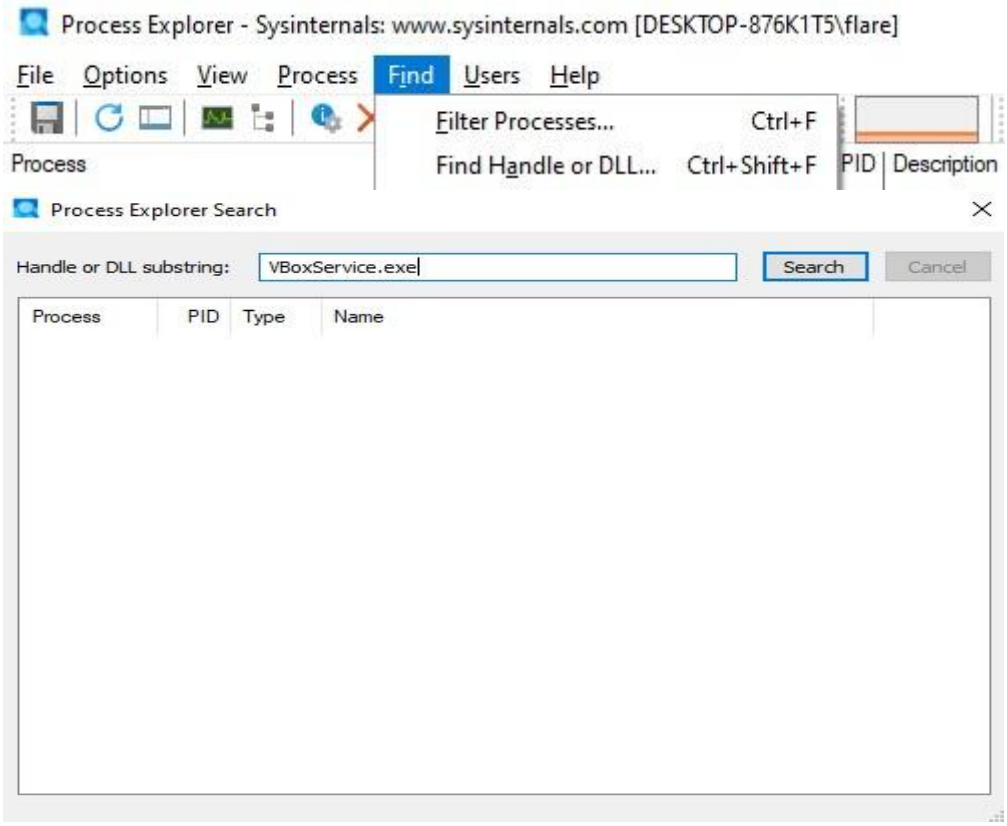


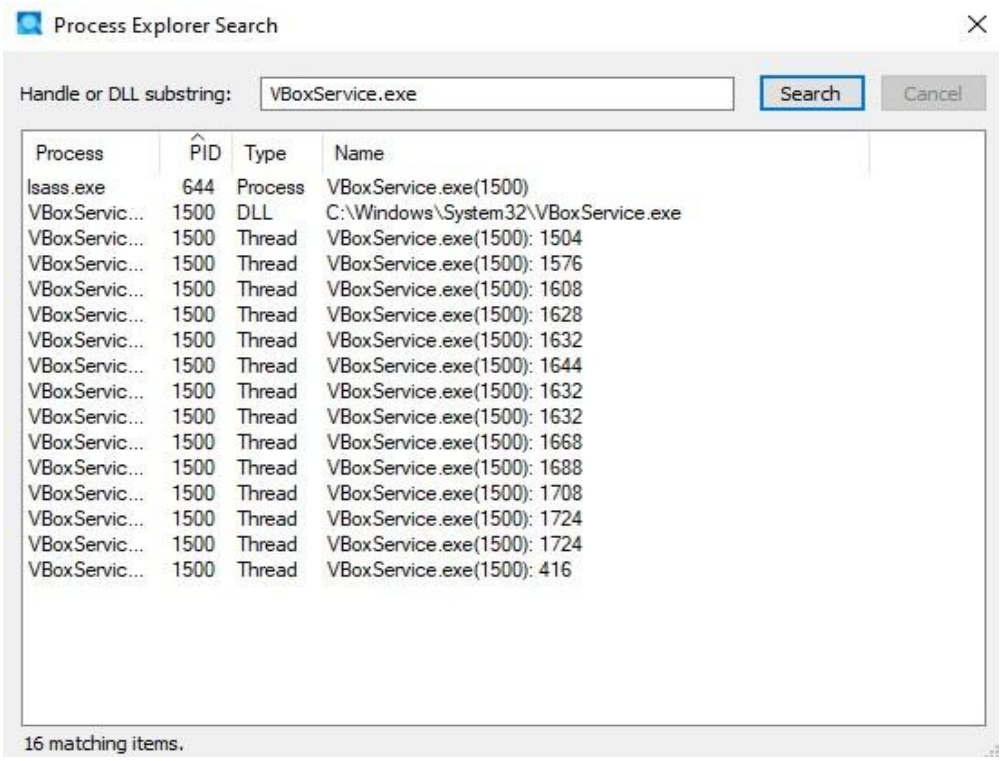
Dopo aver individuato il file da analizzare nella lista dei processi, in questo caso, **VboxService.exe**, come già illustrato in precedenza, con il tasto destro, clicco su **Properties**, in cui vedo il **Path** (**percorsi del programma**), e nello specifico, nelle prossime immagini e passaggi, lavorerò sulla parte evidenziata in rosso, ma ora vado nella scheda Threads, per visualizzare sia il **TID**, che identifica l'**ID del processo** ed il tempo della **CPU** che impiega, utilizza ogni **Threads**



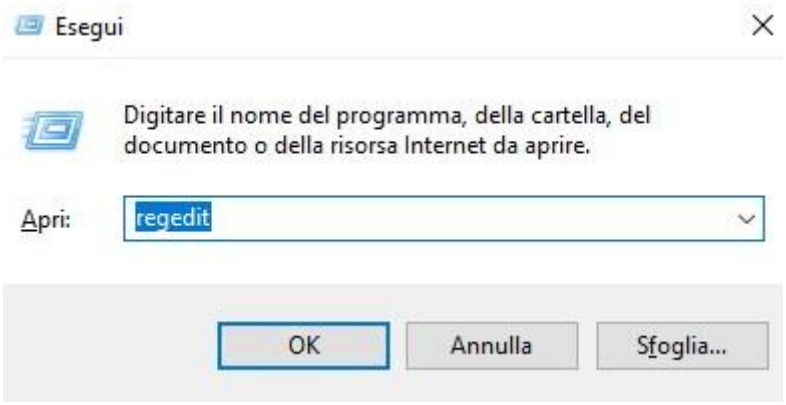


Nel passaggio illustrato di seguito, sempre, all'interno del programma **procexp.exe**, vado in alto a sinistra sulla scheda **Find**, e clicco su Handle or DLL (**Dynamic Link Libraries**), dove posso cercare il programma specifico che voglio modificare o visualizzare, in questo caso e come illustrato e descritto in precedenza, **VBoxService.exe,** per aprire in modalità rapida la scheda **Find**, all'interno di **procexp.exe**, posso utilizzare il comando e combinazione di tasti **Ctrl + F**:



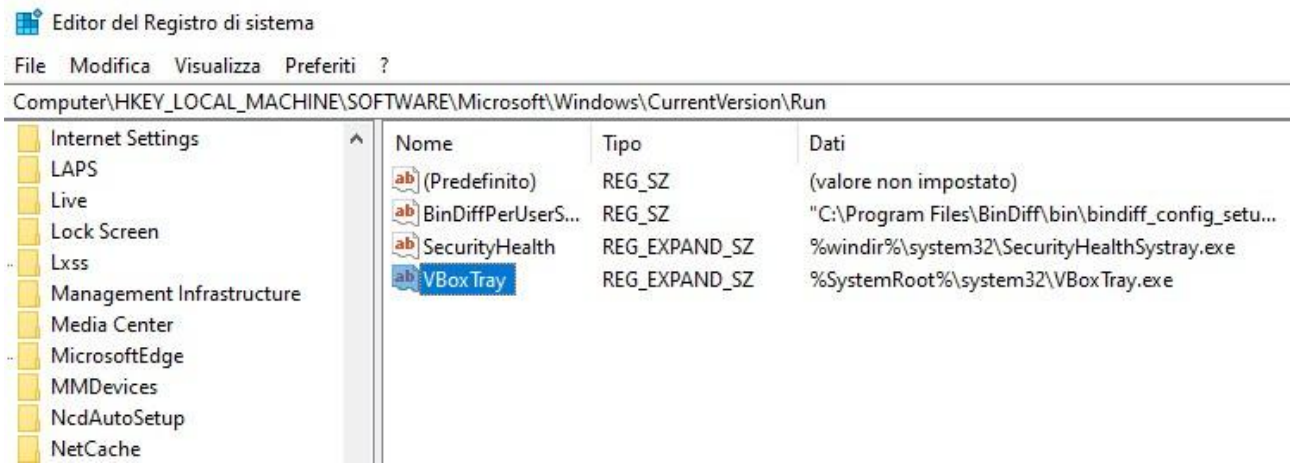


Nel prossimo passaggio con la combinazione tasti **Windows + R**, scrivo all'interno della stringa di ricerca **regedit** (**Editor del Registro di Sistema di Windows**), nel quale posso andare a modificare o configurare le impostazioni del mio Sistema Operativo (Windows):

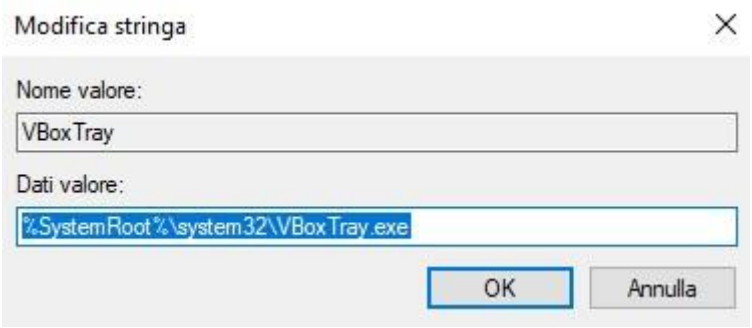


Nella prossima immagine e passaggio, all'interno dell'Editor del Registro di Sistema, in alto, posso notare il percorso:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- **HKEY_LOCAL_MACHINE:** è la radice del Registro di Windows, contenente le informazioni per le configurazioni, applicabili all'interno del computer e relative configurazioni anche per gli Users
- **SOFTWARE\Microsoft\Windows\CurrentVersion\Run**: è la chiave che identifica il file o i file che si avviano nella fase di avvio del Sistema Operativo (Windows)

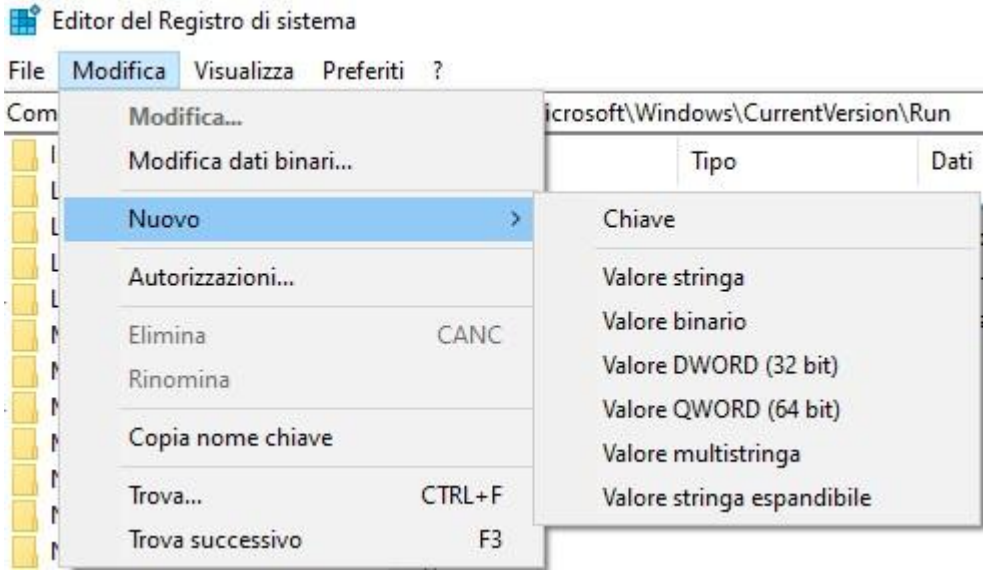


Dopo aver individuato nell'Editor del Registro di Sistema di Windows, VBoxTray clicco due volte sul file **VBoxTray**, per visualizzare il valore del programma, in fase di avvio di Windows:

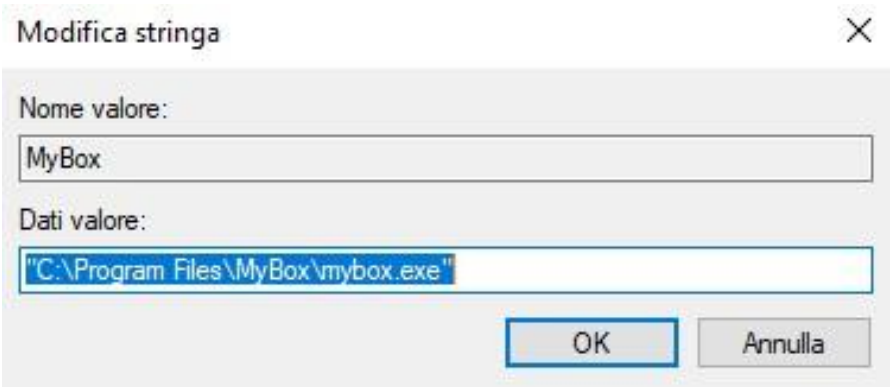


Dopo che ho visualizzato il percorso di **VboxTray** e verificato che il programma si avvia all'avvio della macchina Windows, ho cliccato su **Modifica**, successivamente su **Nuovo** e poi **Valore stringa** in cui ho creato u nuovo valore (exe), chiamato **MyBox** che si avvierà durante l'avvio di Windows, nella stringa Dati valore, come da immagine seguente, il percorso del programma è:

- **C:\Program Files\MyBox\mybox.exe**



Dopo aver creato il programma e dato un nome al valore **MyBox**, clicco su **OK** e per rendere le modifiche e configurazioni, eseguibili, all'avvio di Windows, riavvio la macchina



Dopo aver riavviato la macchina Windows, torno sull'Editor del Registro di Sistema di Windows e controllo se il valore configurato e programma, che si avviano all'avvio di Windows:

Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
BinDiffPerUserS...	REG_SZ	"C:\Program Files\BinDiff\bin\bindiff_config_setu...
MyBox	REG_SZ	"C:\Program Files\MyBox\mybox.exe"
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
VBoxTray	REG_EXPAND_SZ	%SystemRoot%\system32\VBoxTray.exe

Per verificare che **MyBox** si avii correttamente, all'avio di Windows, verifico il tutto, con il comando **Ctrl + Shift + Esc**, che aprirà il **Task Manager**, nella scheda Avvio, verifico che il programma **MyBox**, si sia avviato: