

## Laboratorio:

### Esplorazione di Processi, Thread, Handle e Registro di Windows

In questo laboratorio, completerai i seguenti obiettivi:

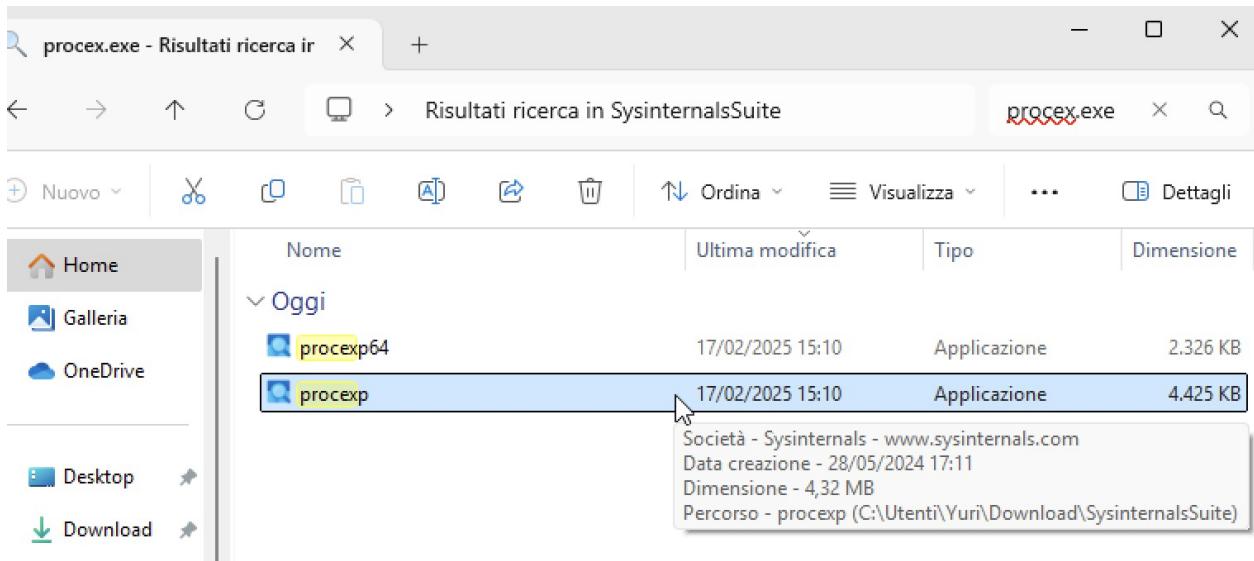
- Esplora i processi, i thread e gli handle utilizzando Process Explorer nella Sysinternals Suite.
- Utilizza il Registro di Windows per modificare un'impostazione.

Iniziamo cliccando sul link fornito, per poi trovarci di fronte alla schermata seguente

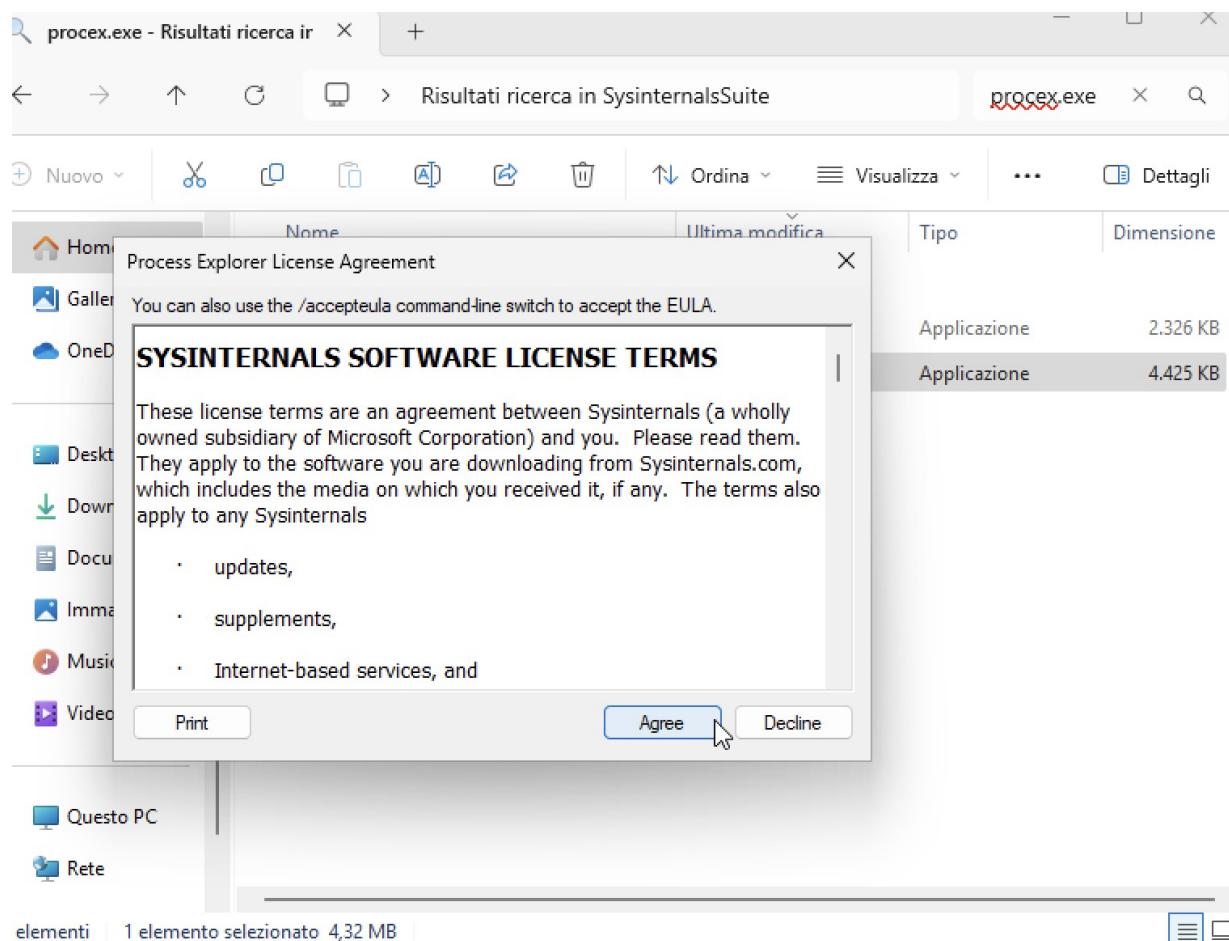
The screenshot shows a web browser window with the following details:

- Title Bar:** Sysinternals Suite - Sysinternals
- Address Bar:** learn.microsoft.com/it-it/sysinternals/downloads/sysinternals-suite
- Page Header:** Learn | Sysinternals | Download | Community | Risorse
- Notice:** ⓘ Parti di questo argomento potrebbero essere state tradotte automaticamente o con l'intelligenza artificiale.
- Left Sidebar (Download section):**
  - Home
  - Download
    - Download
    - > Utilità file e dischi
    - > Utilità di rete
    - > Utilità di processo
    - > Utilità di sicurezza
    - > Informazioni sul sistema
    - > Varie
  - Sysinternals Suite
  - Microsoft Store
- Page Content:**
  - Page Title:** Sysinternals Suite
  - Text:** Articolo • 16/12/2024 • 8 contributori
  - Text:** Da Mark Russinovich
  - Text:** Aggiornamento: 16 dicembre 2024
  - Links:**
    - Scaricare Sysinternals Suite (50,5 MB)
    - Scaricare Sysinternals Suite per Nano Server (9,5 MB)
    - Scaricare Sysinternals Suite per ARM64 (15 MB)
    - Installare Sysinternals Suite da Microsoft Store

Estraiamo tutto il file .zip e apriamo il programma con un doppio clic, come mostrato nella seguente immagine.



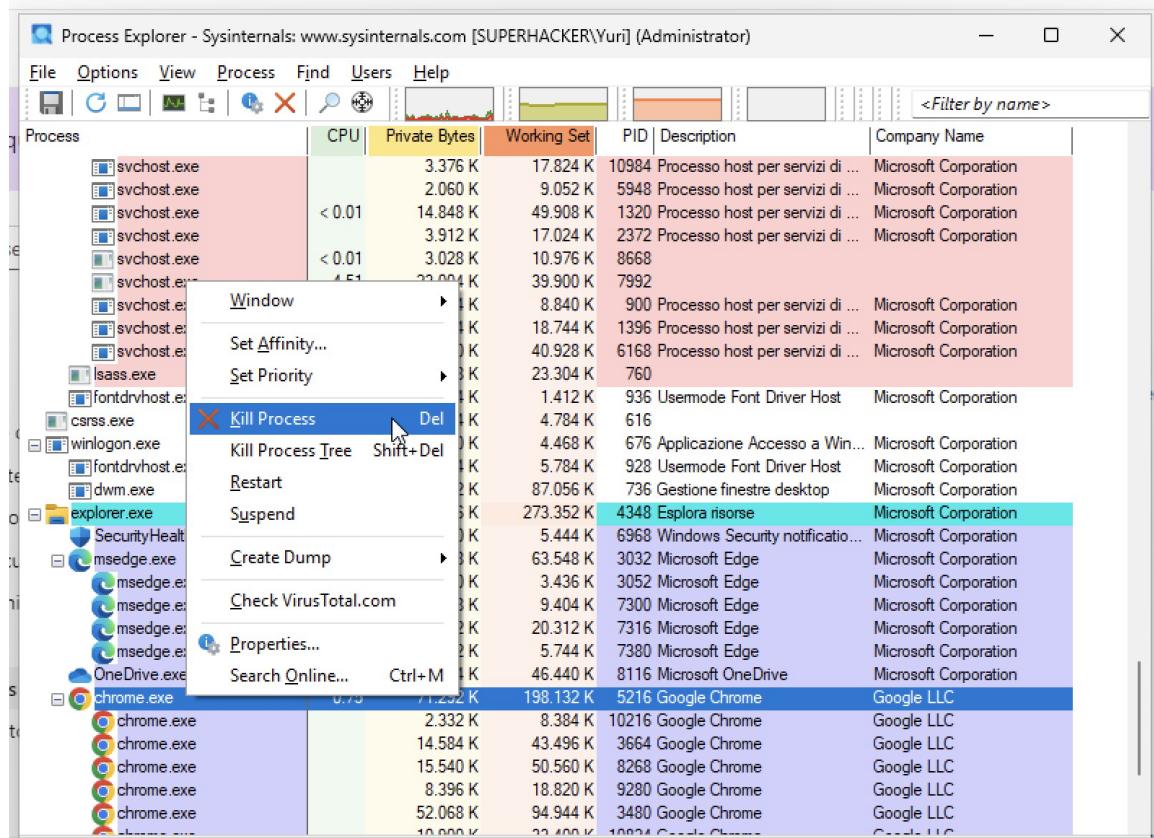
### Accettiamo l'EULA

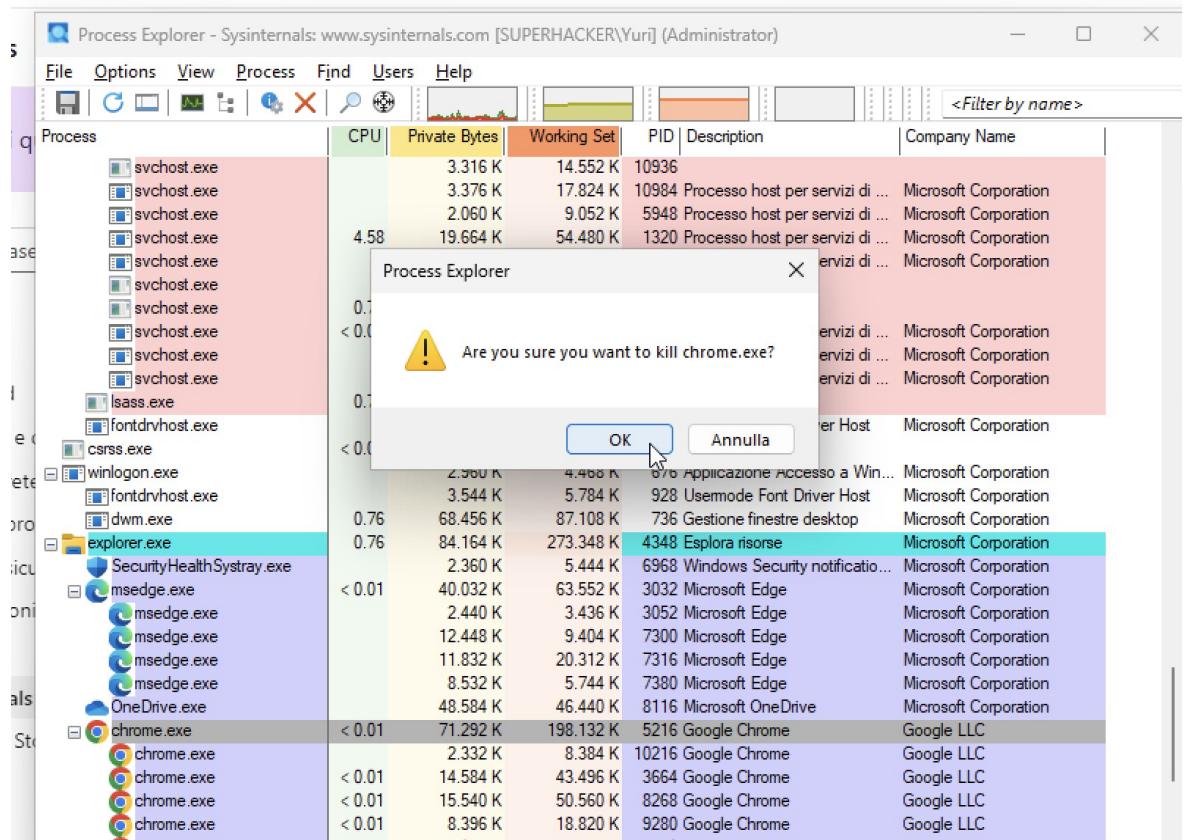


Process Explorer - Sysinternals: www.sysinternals.com [SUPERHACKER\Yuri] (Administrator)

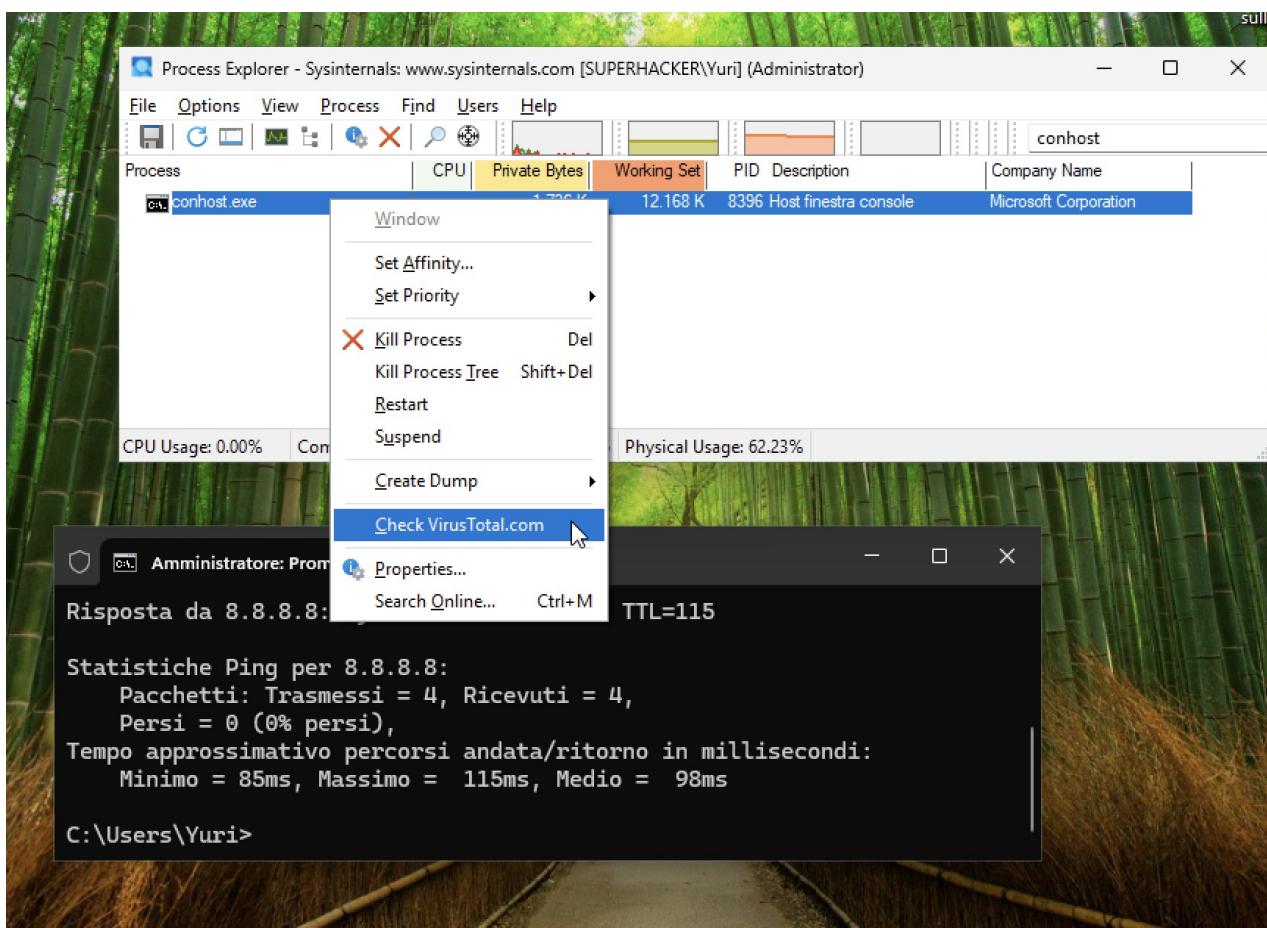
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		2.060 K	9.764 K	6476	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		27.288 K	59.924 K	10384	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		2.012 K	9.588 K	10728	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	2.956 K	14.444 K	10804	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		3.320 K	14.552 K	10936		
svchost.exe		3.376 K	17.824 K	10984	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		1.920 K	8.500 K	5948	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		12.648 K	47.756 K	1320	Processo host per servizi di Windows ...	Microsoft Corporation
svchost.exe		3.912 K	17.024 K	2372	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		3.028 K	10.976 K	8668		
svchost.exe	0.76	19.836 K	33.604 K	7992		
svchost.exe		< 0.01	1.888 K	8.828 K	900 Processo host per servizi di ...	Microsoft Corporation
svchost.exe		2.680 K	18.696 K	1396	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		6.092 K	40.992 K	6168	Processo host per servizi di ...	Microsoft Corporation
lsass.exe	< 0.01	9.028 K	23.228 K	760		
fontdrvhost.exe		1.584 K	1.412 K	936	Usermode Font Driver Host	Microsoft Corporation
csrss.exe	< 0.01	2.464 K	4.792 K	616		
winlogon.exe		2.960 K	4.468 K	676	Applicazione Accesso a Win...	Microsoft Corporation
fontdrvhost.exe		3.544 K	5.784 K	928	Usermode Font Driver Host	Microsoft Corporation
dwm.exe	1.52	68.576 K	86.160 K	736	Gestione finestre desktop	Microsoft Corporation
explorer.exe	< 0.01	85.996 K	274.668 K	4348	Esplora risorse	Microsoft Corporation
SecurityHealthSystray.exe		2.360 K	5.444 K	6968	Windows Security notificatio...	Microsoft Corporation
msedge.exe		40.028 K	63.248 K	3032	Microsoft Edge	Microsoft Corporation
msedge.exe		2.440 K	3.436 K	3052	Microsoft Edge	Microsoft Corporation
msedge.exe		12.448 K	9.404 K	7300	Microsoft Edge	Microsoft Corporation
msedge.exe		11.832 K	20.312 K	7316	Microsoft Edge	Microsoft Corporation
msedge.exe		8.532 K	5.744 K	7380	Microsoft Edge	Microsoft Corporation
OneDrive.exe		48.584 K	46.440 K	8116	Microsoft OneDrive	Microsoft Corporation
chrome.exe	< 0.01	71.308 K	198.116 K	5216	Google Chrome	Google LLC
chrome.exe		2.332 K	8.384 K	10216	Google Chrome	Google LLC

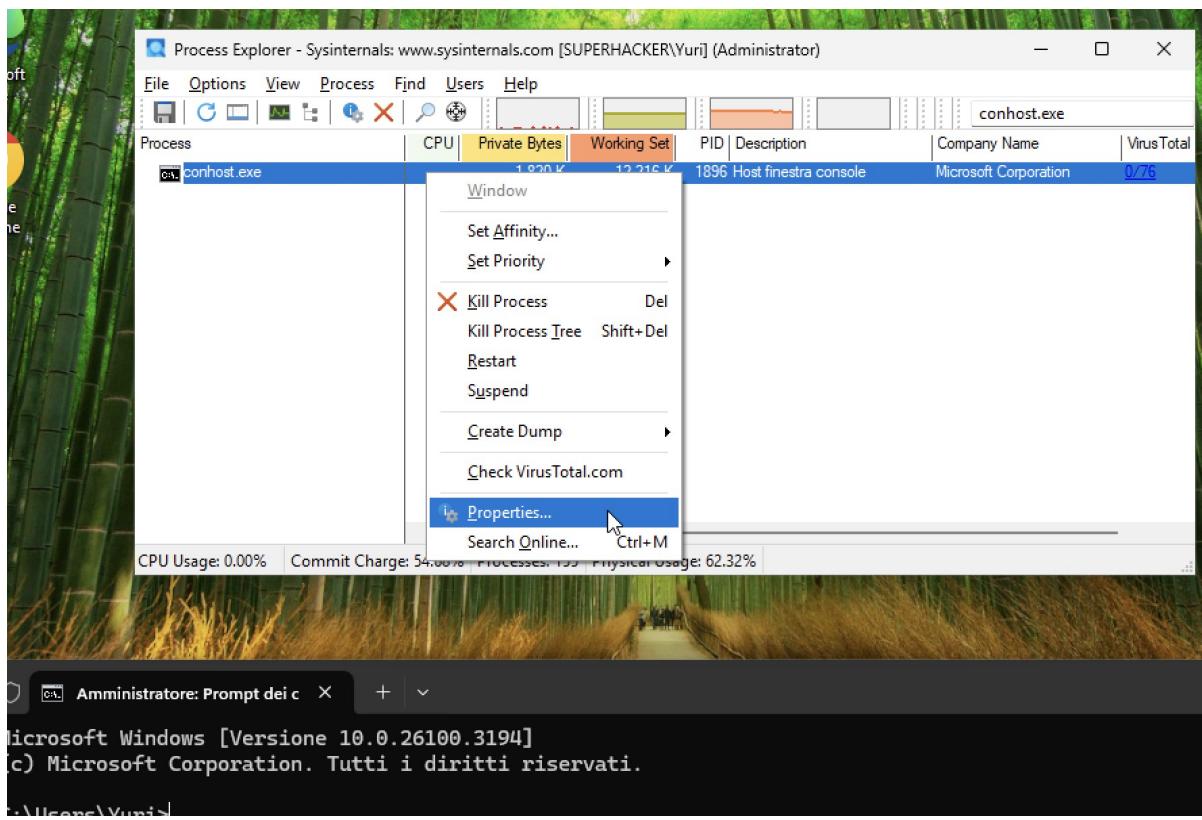
Trascinare il Trova Processo (oggetto nel quadrato rosso), sul processo di google chrome



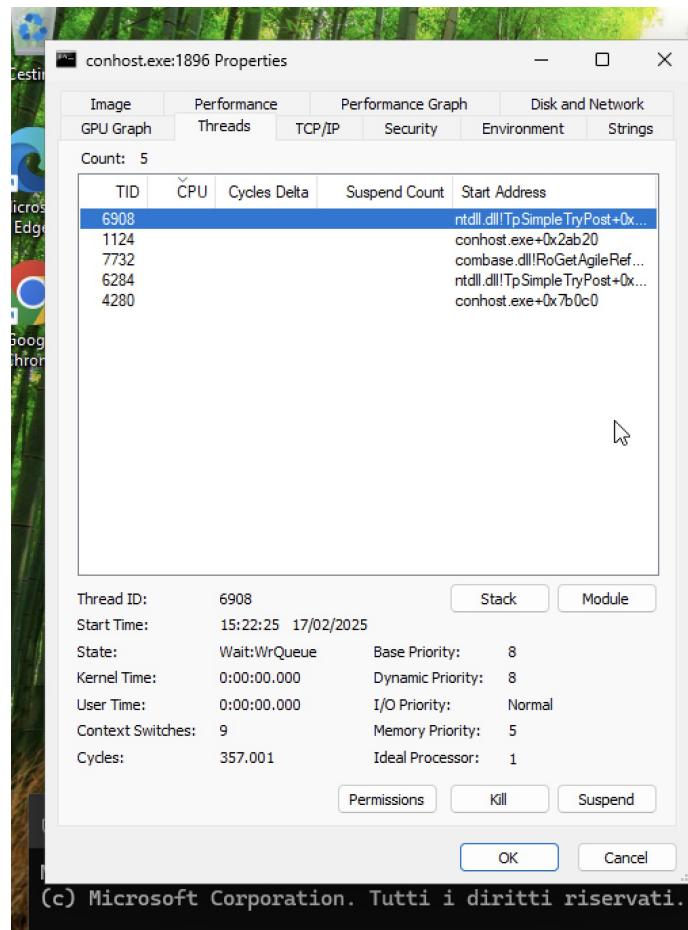


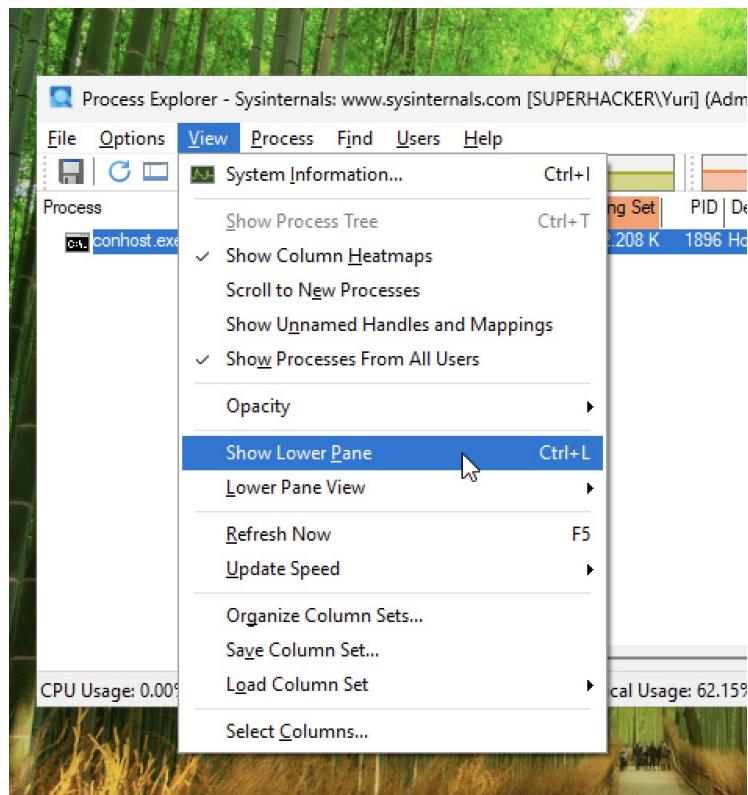
Di seguito, facciamo la scansione su virustotal



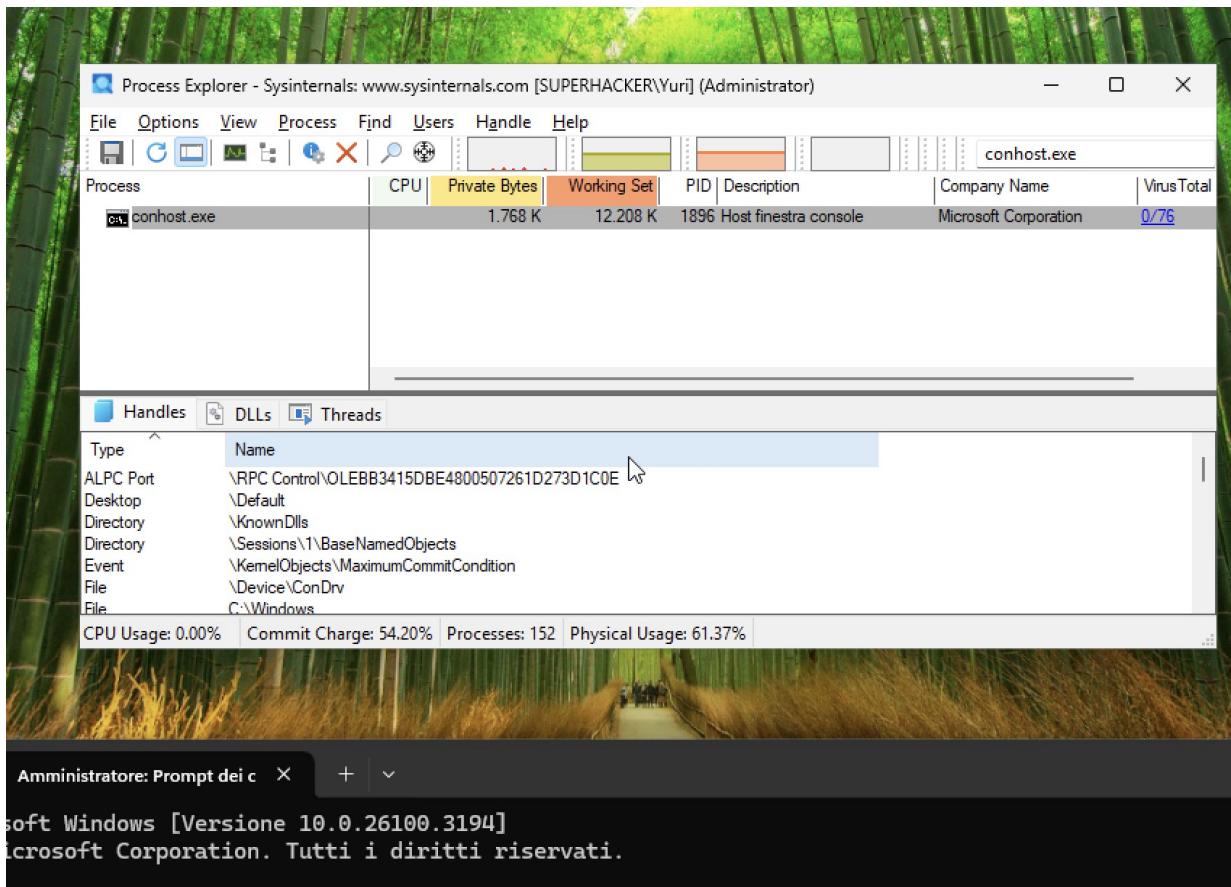


In questa schermata che ci appare, notiamo i threads





Ed infine qui ci compaiono i datteagli degli Handles



Per ultimare l'esercizio, ovvero modificare l'EULA, procediamo come segue nelle prossime schermate

