

Report S11/L1

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.

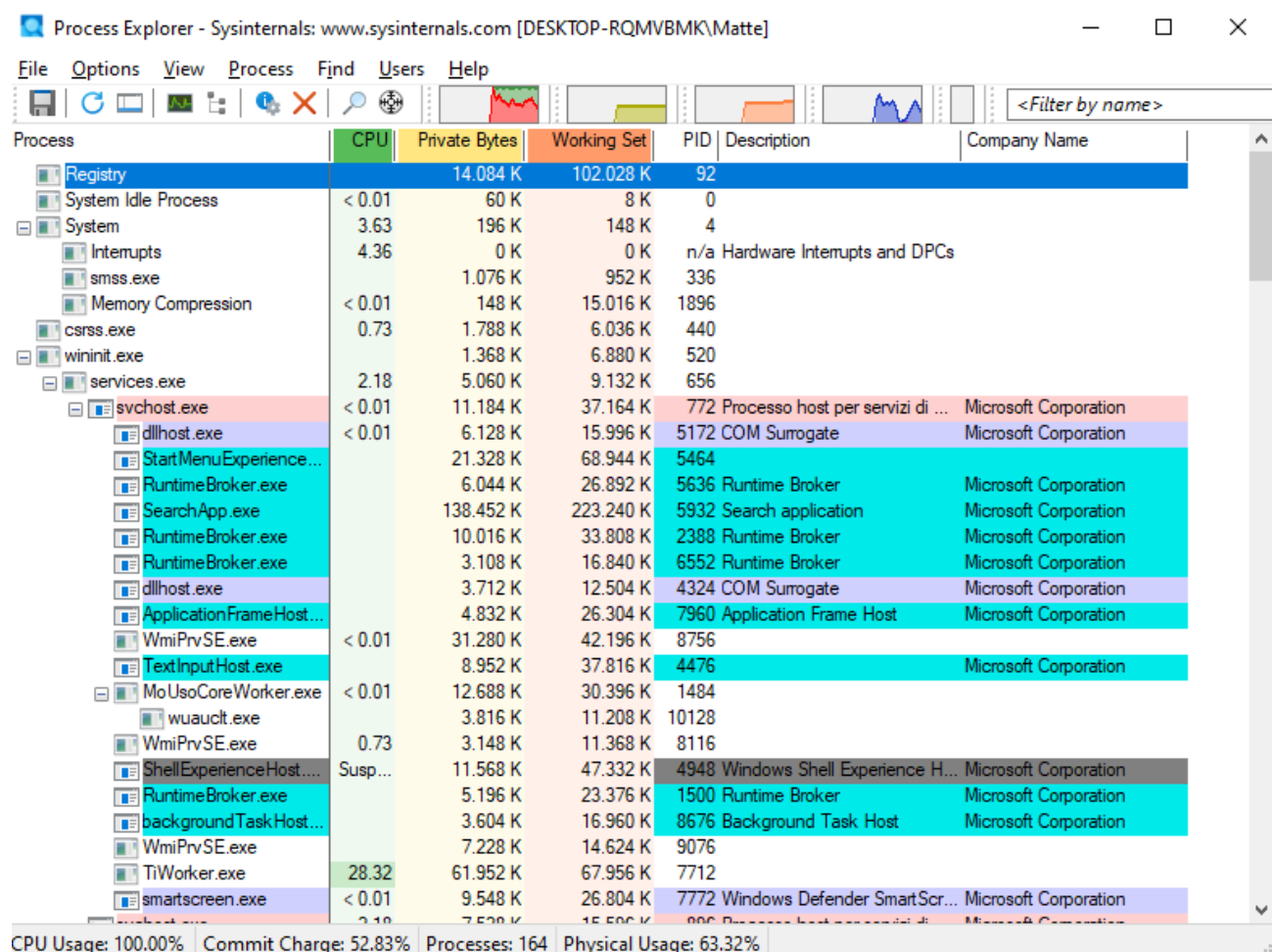
<https://itexamanswers.net/3-2-11-lab-exploring-processes-threads-handles-and-windows-registry-answers.html>

Svolgimento

Per questo laboratorio utilizzerò una VM con Windows 10 Pro.

Parte 1: Esplorazione dei processi

Vado sul sito precedentemente linkato, scarico SysInternals Suite, estraggo i file dalla cartella e apro il file procexp.exe.

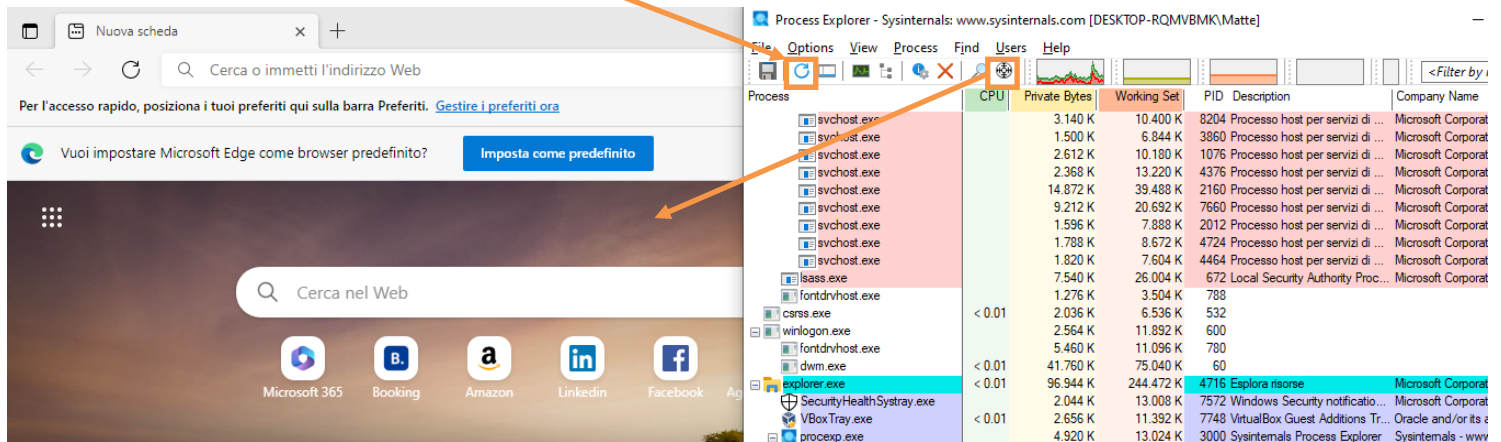


The screenshot shows the Process Explorer window from Sysinternals. The title bar reads 'Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-RQMVBK\Matte]'. The menu bar includes File, Options, View, Process, Find, Users, and Help. The toolbar contains icons for file operations and monitoring. The main window displays a list of processes with columns for CPU, Private Bytes, Working Set, PID, Description, and Company Name. The processes are listed in a tree view on the left, starting with Registry, System Idle Process, System, Interrupts, smss.exe, Memory Compression, csrss.exe, wininit.exe, services.exe, and svchost.exe. The svchost.exe process is expanded, showing several sub-processes including dllhost.exe, StartMenuExperienceHost.exe, RuntimeBroker.exe, SearchApp.exe, RuntimeBroker.exe, RuntimeBroker.exe, ApplicationFrameHost.exe, WmiPrvSE.exe, TextInputHost.exe, MoUsoCoreWorker.exe, wuauclt.exe, WmiPrvSE.exe, ShellExperienceHost.exe, RuntimeBroker.exe, BackgroundTaskHost.exe, WmiPrvSE.exe, TiWorker.exe, and smartscreen.exe. The status bar at the bottom shows CPU Usage: 100.00%, Commit Charge: 52.83%, Processes: 164, and Physical Usage: 63.32%.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		14.084 K	102.028 K	92		
System Idle Process	< 0.01	60 K	8 K	0		
System	3.63	196 K	148 K	4		
Interrupts	4.36	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1.076 K	952 K	336		
Memory Compression	< 0.01	148 K	15.016 K	1896		
csrss.exe	0.73	1.788 K	6.036 K	440		
wininit.exe		1.368 K	6.880 K	520		
services.exe	2.18	5.060 K	9.132 K	656		
svchost.exe	< 0.01	11.184 K	37.164 K	772	Processo host per servizi di ...	Microsoft Corporation
dllhost.exe	< 0.01	6.128 K	15.996 K	5172	COM Surrogate	Microsoft Corporation
StartMenuExperience...		21.328 K	68.944 K	5464		
RuntimeBroker.exe		6.044 K	26.892 K	5636	Runtime Broker	Microsoft Corporation
SearchApp.exe		138.452 K	223.240 K	5932	Search application	Microsoft Corporation
RuntimeBroker.exe		10.016 K	33.808 K	2388	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3.108 K	16.840 K	6552	Runtime Broker	Microsoft Corporation
dllhost.exe		3.712 K	12.504 K	4324	COM Surrogate	Microsoft Corporation
ApplicationFrameHost...		4.832 K	26.304 K	7960	Application Frame Host	Microsoft Corporation
WmiPrvSE.exe	< 0.01	31.280 K	42.196 K	8756		
TextInputHost.exe		8.952 K	37.816 K	4476		Microsoft Corporation
MoUsoCoreWorker.exe	< 0.01	12.688 K	30.396 K	1484		
wuauclt.exe		3.816 K	11.208 K	10128		
WmiPrvSE.exe	0.73	3.148 K	11.368 K	8116		
ShellExperienceHost...	Susp...	11.568 K	47.332 K	4948	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		5.196 K	23.376 K	1500	Runtime Broker	Microsoft Corporation
BackgroundTaskHost...		3.604 K	16.960 K	8676	Background Task Host	Microsoft Corporation
WmiPrvSE.exe		7.228 K	14.624 K	9076		
TiWorker.exe	28.32	61.952 K	67.956 K	7712		
smartscreen.exe	< 0.01	9.548 K	26.804 K	7772	Windows Defender SmartScr...	Microsoft Corporation

CPU Usage: 100.00% Commit Charge: 52.83% Processes: 164 Physical Usage: 63.32%

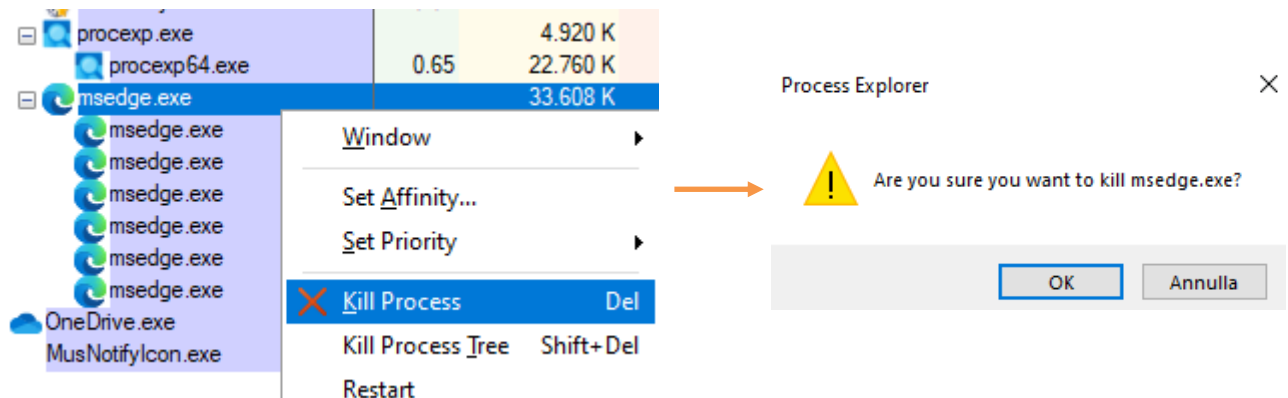
Apro il Browser Edge e aggiorno. Successivamente uso l'icona Find Windows Process e la trascina sulla scheda del Browser.



Verifico che il processo di Edge sia stato rilevato

explorer.exe	0.81	97.984 K	239.216 K	4716	Esplora risorse	Microsoft Corporat
SecurityHealthSystray.exe		1.936 K	12.948 K	7572	Windows Security notificatio...	Microsoft Corporat
VBoxTray.exe	< 0.01	2.656 K	11.392 K	7748	VirtualBox Guest Additions Tr...	Oracle and/or its a
procexp.exe		4.992 K	13.048 K	3000	Sysinternals Process Explorer	Sysinternals - www
procexp64.exe	5.66	22.760 K	52.204 K	5036	Sysinternals Process Explorer	Sysinternals - www
msedge.exe	< 0.01	33.500 K	113.688 K	9740	Microsoft Edge	Microsoft Corporat
msedge.exe		2.064 K	7.996 K	1300	Microsoft Edge	Microsoft Corporat
msedge.exe		21.892 K	62.024 K	3236	Microsoft Edge	Microsoft Corporat
msedge.exe		10.788 K	33.884 K	1100	Microsoft Edge	Microsoft Corporat
msedge.exe		145.752 K	236.948 K	9856	Microsoft Edge	Microsoft Corporat
msedge.exe		6.432 K	18.116 K	8840	Microsoft Edge	Microsoft Corporat
msedge.exe		12.624 K	27.988 K	4656	Microsoft Edge	Microsoft Corporat
OneDrive.exe		45.924 K	61.848 K	8668	Microsoft OneDrive	Microsoft Corporat
MusNotifIcon.exe		3.252 K	2.036 K	9188	MusNotifIcon.exe	Microsoft Corporat

Con il tasto destro del mouse clicco sul processo di Edge e seleziono Kill Process → Poi clicco su OK



In seguito alla conferma la finestra del Browser si chiude.

Avvio un altro processo tramite il Prompt dei Comandi e trascino l'icona Find Windows Process sulla scheda di CMD, mi appare così il processo su Process Explorer.

The screenshot shows the Process Explorer window with a list of processes. The 'cmd.exe' process is highlighted. Below the list, a command prompt window is open, showing the command 'C:\Users\Matte>' and the output of a 'ping' command.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		4.192 K	15.992 K	9888	Processo host per servizi di ...	Microsoft Corporation
lsass.exe		7.816 K	26.068 K	672	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1.276 K	3.180 K	788		
csrss.exe	1.02	2.028 K	6.500 K	532		
winlogon.exe		2.564 K	11.820 K	600		
fontdrvhost.exe		5.456 K	8.852 K	780		
dwm.exe	1.02	38.024 K	67.936 K	60		
explorer.exe	< 0.01	109.048 K	240.936 K	4716	Esplora risorse	Microsoft Corporation
SecurityHealthSystray.exe		1.908 K	12.924 K	7572	Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	< 0.01	2.656 K	11.284 K	7748	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
proceexp.exe		4.920 K	13.024 K	3000	Sysinternals Process Explorer	Sysinternals - www.sysinter...
proceexp64.exe	32.04	22.832 K	48.516 K	5036	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		2.040 K	4.148 K	3760	Processore dei comandi di ...	Microsoft Corporation
conhost.exe		9.428 K	20.228 K	9268	Host finestra console	Microsoft Corporation

CPU Usage: 92.06% Commit Charge: 43.99% Processes: 131 Physical Usage: 58.84%

Prompt dei comandi

```
Microsoft Windows [Versione 10.0.19045.3803]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\Matte>
```

Eseguo un ping e osservo cosa succede su Process Explorer

The screenshot shows the Process Explorer window with a list of processes. The 'PING.EXE' process is highlighted. Below the list, a command prompt window is open, showing the command 'C:\Users\Matte>ping 10.0.2.15' and the output of the 'ping' command.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
csrss.exe	1.23	2.032 K	6.484 K	532		
winlogon.exe		2.488 K	11.844 K	600		
fontdrvhost.exe		5.456 K	8.784 K	780		
dwm.exe	2.45	39.800 K	69.780 K	60		
explorer.exe	1.23	114.828 K	235.348 K	4716	Esplora risorse	Microsoft Corporation
SecurityHealthSystray.exe		1.908 K	12.896 K	7572	Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	< 0.01	2.656 K	11.296 K	7748	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
proceexp.exe		4.920 K	11.884 K	3000	Sysinternals Process Explorer	Sysinternals - www.sysinter...
proceexp64.exe	9.80	22.812 K	38.008 K	5036	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		2.212 K	4.552 K	3760	Processore dei comandi di ...	Microsoft Corporation
conhost.exe	2.45	9.452 K	22.248 K	9268	Host finestra console	Microsoft Corporation
PING.EXE	< 0.01	852 K	3.928 K	9124	Comando Ping TCP/IP	Microsoft Corporation
OneDrive.exe		45.924 K	60.108 K	8668	Microsoft OneDrive	Microsoft Corporation
MusNotifIcon.exe		3.224 K	1.988 K	9188	MusNotifIcon.exe	Microsoft Corporation

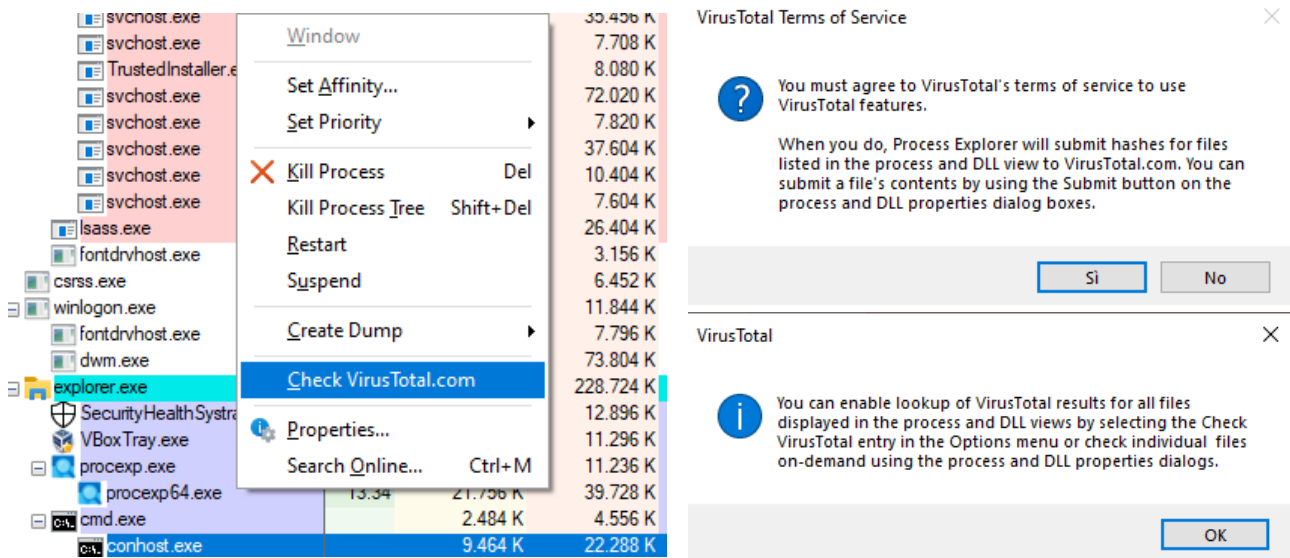
C:\Users\Matte>ping 10.0.2.15

```
Esecuzione di Ping 10.0.2.15 con 32 byte di dati:
Risposta da 10.0.2.15: byte=32 durata<1ms TTL=128
Risposta da 10.0.2.15: byte=32 durata<1ms TTL=128
Risposta da 10.0.2.15: byte=32 durata<1ms TTL=128
Risposta da 10.0.2.15: byte=32 durata<1ms TTL=128

Statistiche Ping per 10.0.2.15:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 0ms, Medio = 0ms
```

Sotto il processo figlio conhost.exe è uscito un'ulteriore processo chiamato PING.EXE.

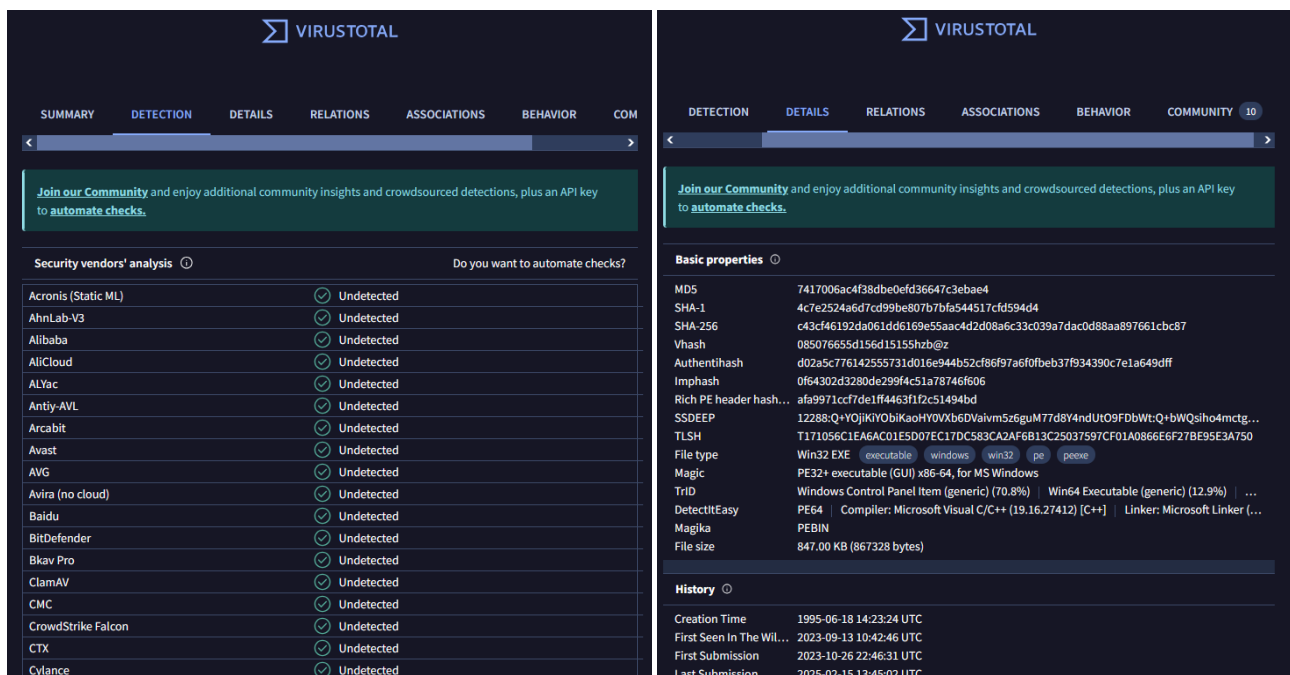
Per verificare la presenza di contenuti dannosi su un processo sospetto ci clicco sopra con il tasto destro del mouse e seleziono check VirusTotal.com e accetto i termini di servizio per avviarlo.



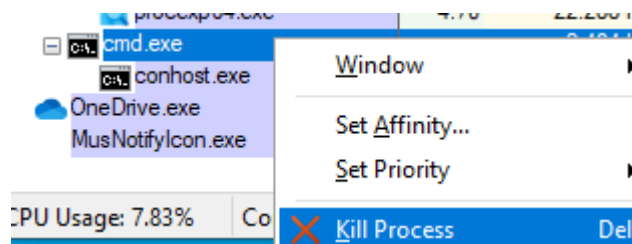
Sul processo analizzato è uscito il risultato della scansione di VirusTotal → 0/76

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
csrss.exe	0.50	2.032 K	6.416 K	532			
winlogon.exe		2.488 K	11.840 K	600			
fontdrvhost.exe		5.456 K	7.244 K	780			
dwm.exe	< 0.01	42.400 K	69.320 K	60			
explorer.exe	0.50	115.696 K	221.380 K	4716	Esplora risorse	Microsoft Corporation	
SecurityHealthSystray.exe		1.908 K	12.648 K	7572	Windows Security notificatio...	Microsoft Corporation	
VBoxTray.exe	< 0.01	2.656 K	10.976 K	7748	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates	
procexp.exe		4.920 K	10.960 K	3000	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp64.exe	3.00	22.284 K	41.620 K	5036	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		2.484 K	4.396 K	3760	Processore dei comandi di ...	Microsoft Corporation	
conhost.exe		9.488 K	22.116 K	9268	Host finestra console	Microsoft Corporation	0/76

Se faccio clic sopra il risultato ottenuto mi apre la pagina con tutti i risultati della scansione



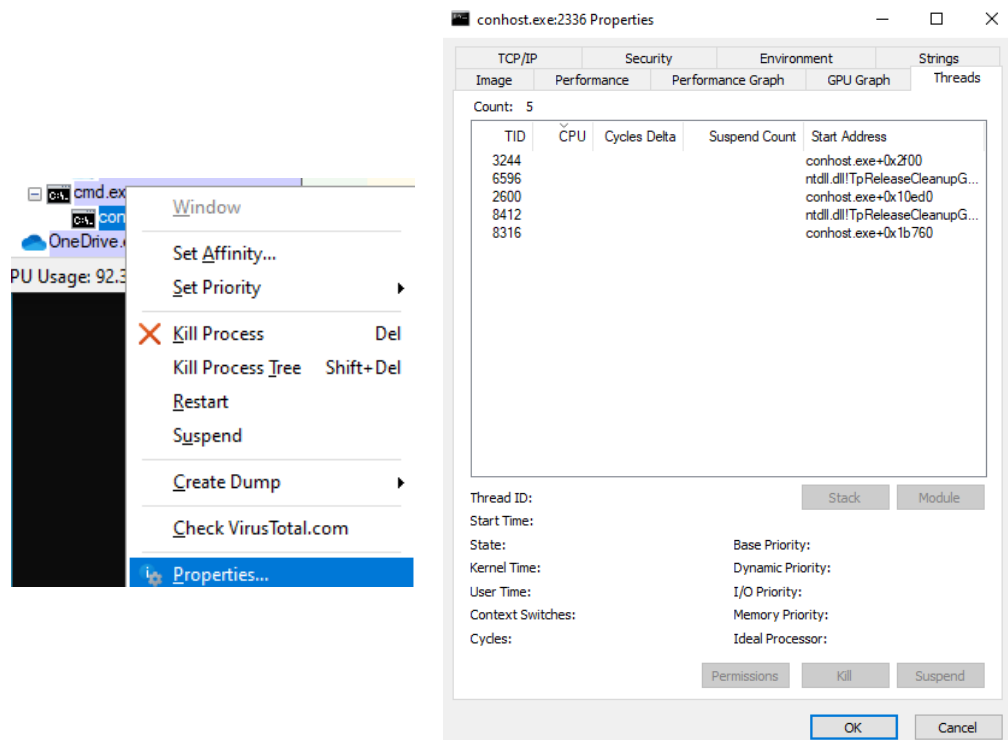
Per chiudere il processo faccio clic su cmd.exe e seleziono kill process, così facendo si chiuderà anche il processo figlio.



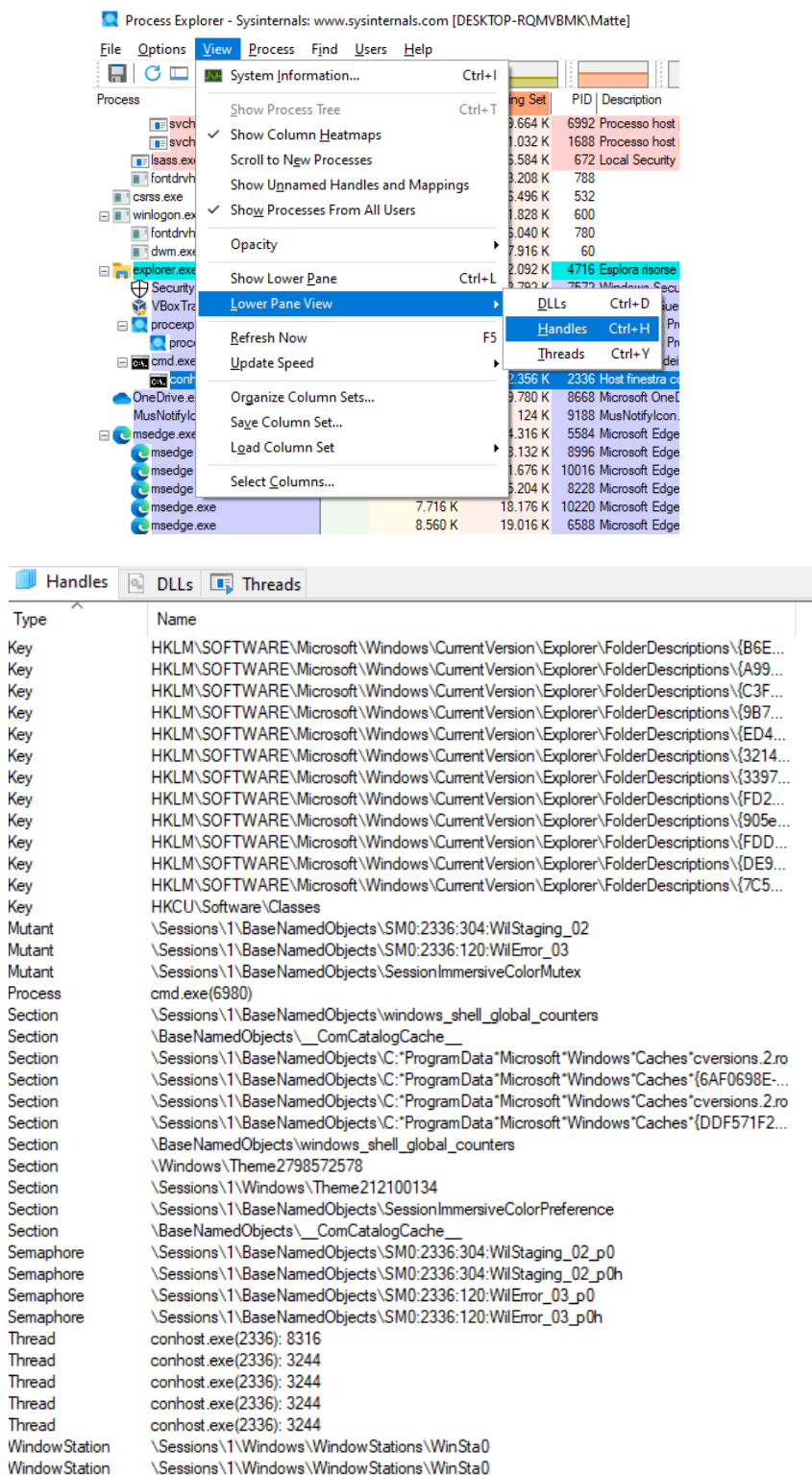
Parte 2: Esplorazione di thread e handle

Un thread è un'unità di esecuzione in un processo. Un handle è un riferimento astratto a blocchi di memoria o oggetti gestiti da un sistema operativo.

Inizio aprendo il prompt dei comandi, sul Process Explorer faccio clic destro su conhost.exe, seleziono Proprietà e poi mi sposto sulla scheda Thread per vedere appunto i thread attivi sul processo conhost.exe



Mentre per visualizzare gli Handle faccio clic su **View>Lower Pain View>Handles**

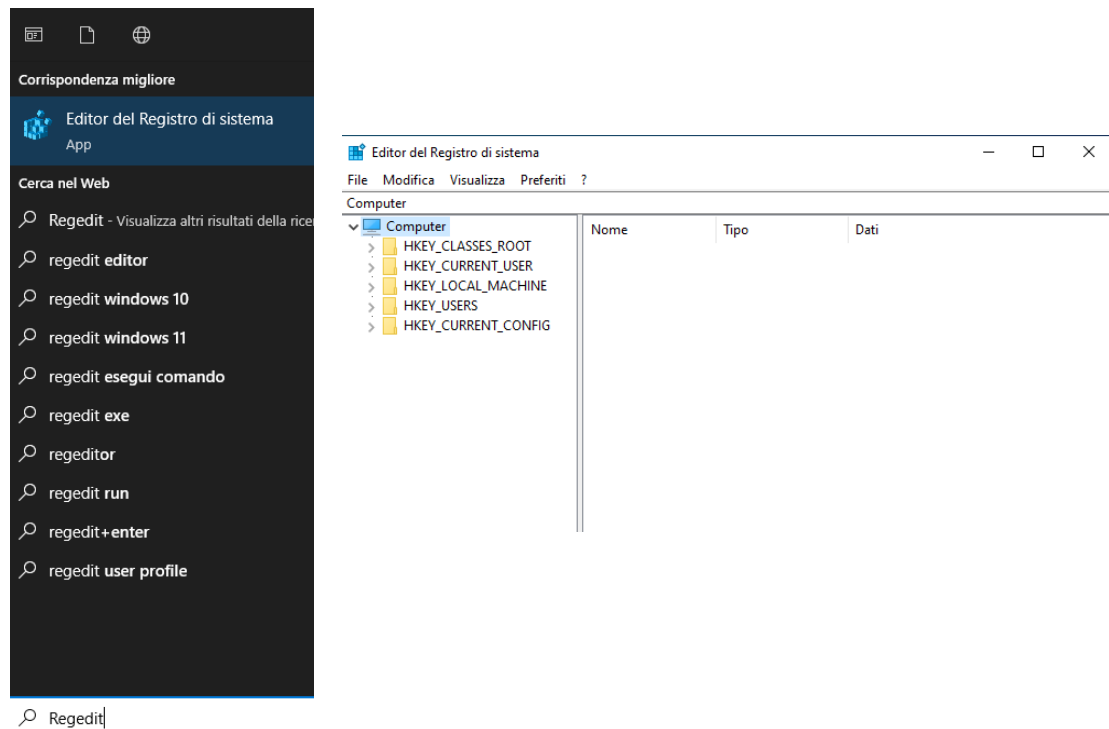


Come possiamo osservare gli handle puntano a file, chiavi di registro e thread.

Parte 3: Esplorazione del registro di Windows

Il Registro di sistema di Windows è un database gerarchico in cui sono archiviate la maggior parte delle impostazioni di configurazione dei sistemi operativi e dell'ambiente desktop.

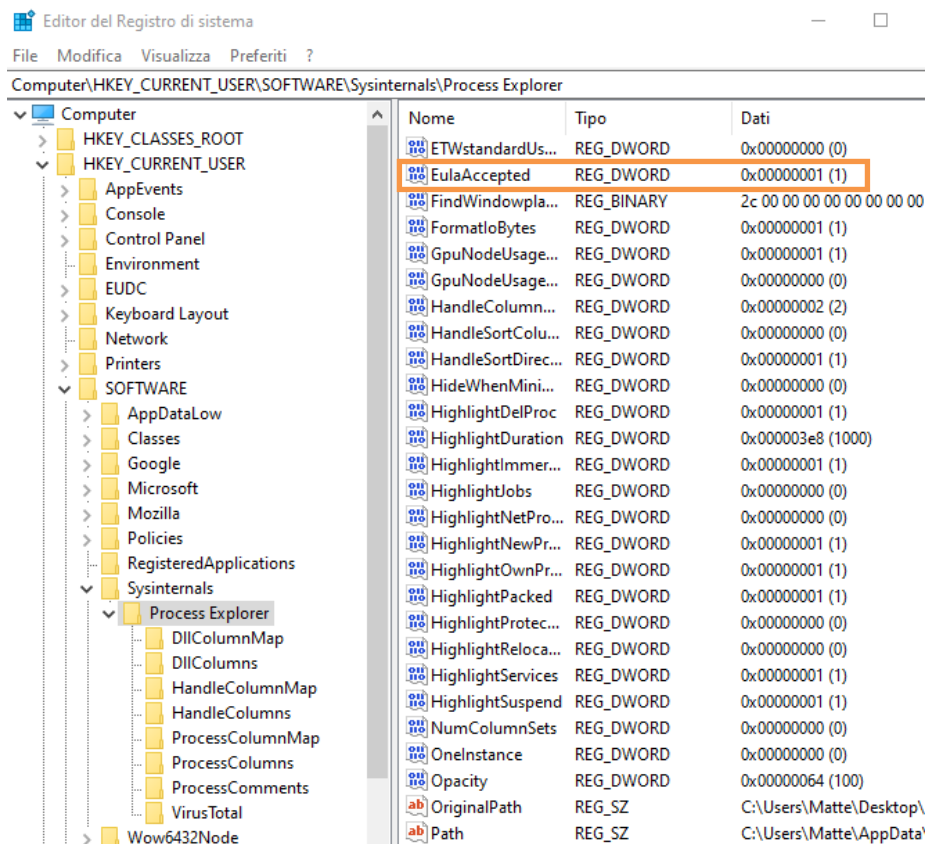
Per aprire il Registro di Windows faccio clic su Start>regedit>Editor del Registro di Sistema



- HKEY_CLASSES_ROOT è una sottochiave di HKEY_LOCAL_MACHINE\Software\.
Memorizza informazioni utilizzate dalle applicazioni registrate come l'associazione di estensioni di file, nonché dati di un identificatore programmatico (ProgID), ID di classe (CLSID) e ID di interfaccia (IID).
- HKEY_CURRENT_USER contiene le impostazioni e le configurazioni degli utenti attualmente connessi.
- HKEY_LOCAL_MACHINE memorizza le informazioni di configurazione specifiche del computer locale.
- HKEY_USERS contiene le impostazioni e le configurazioni per tutti gli utenti sul computer locale.
- HKEY_CURRENT_USER è una sottochiave di HKEY_USERS.
- HKEY_CURRENT_CONFIG memorizza le informazioni hardware utilizzate all'avvio del computer locale.

*In un passaggio precedente abbiamo accettato l'EULA per Process Explorer.

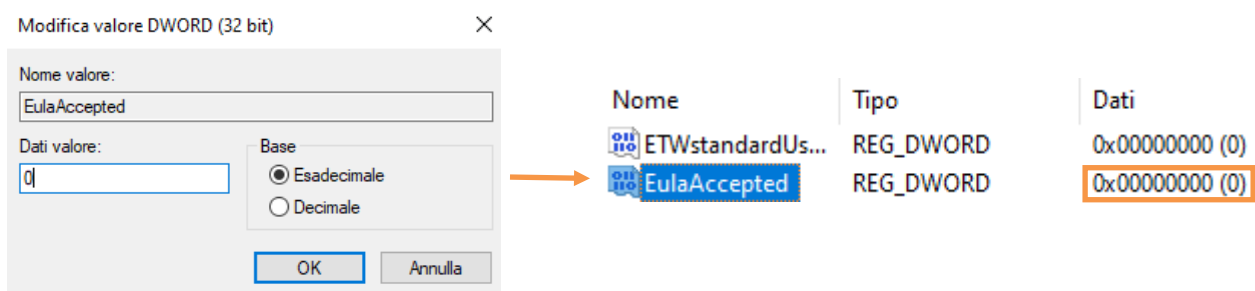
Faccio clic su **HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer** e individuo **EulaAccepted**



Attualmente il valore dati è impostato su 1, questo indica che l'EULA è stato accettato dall'utente.

Faccio doppio clic su EulaAccepted e cambio **1** in **0**. Il valore 0 indica che l'EULA non è stato accettato.

Faccio clic su **OK** per continuare.



Ora provo ad aprire nuovamente ProcessExplorer, all'avvio mi chiede nuovamente di accettare i termini di licenza.

