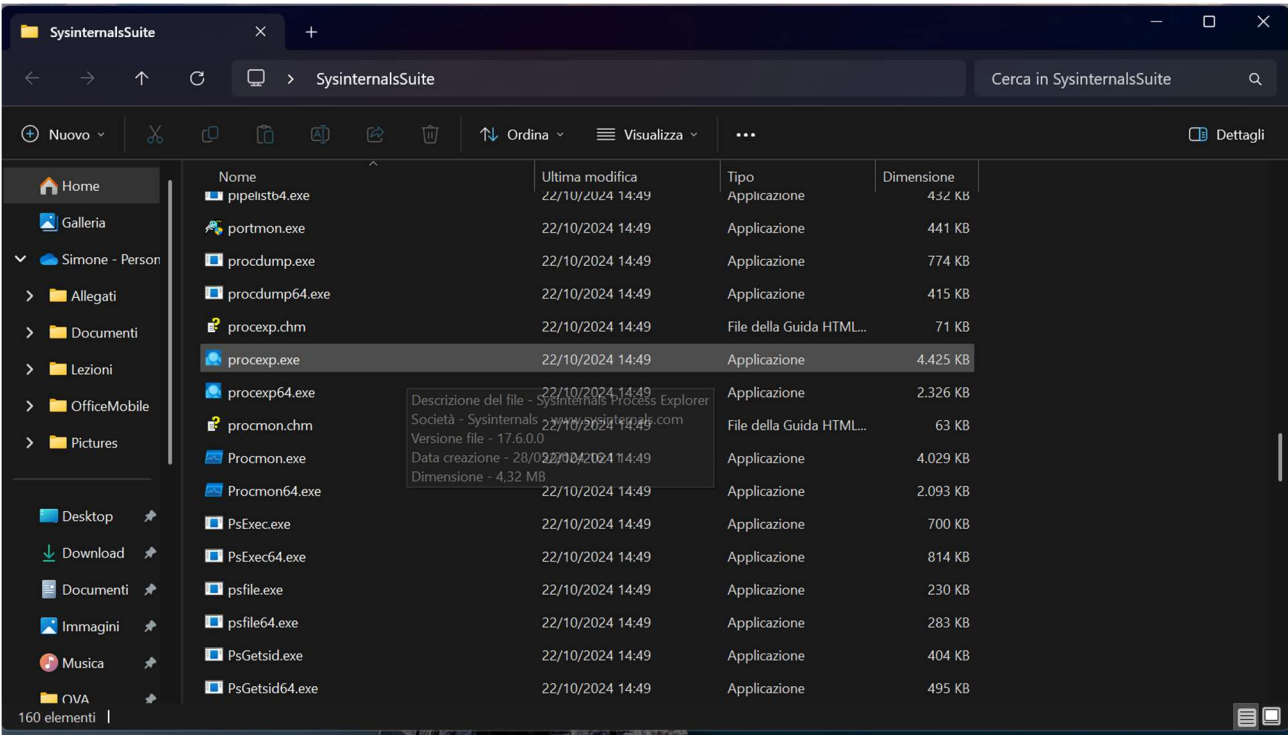
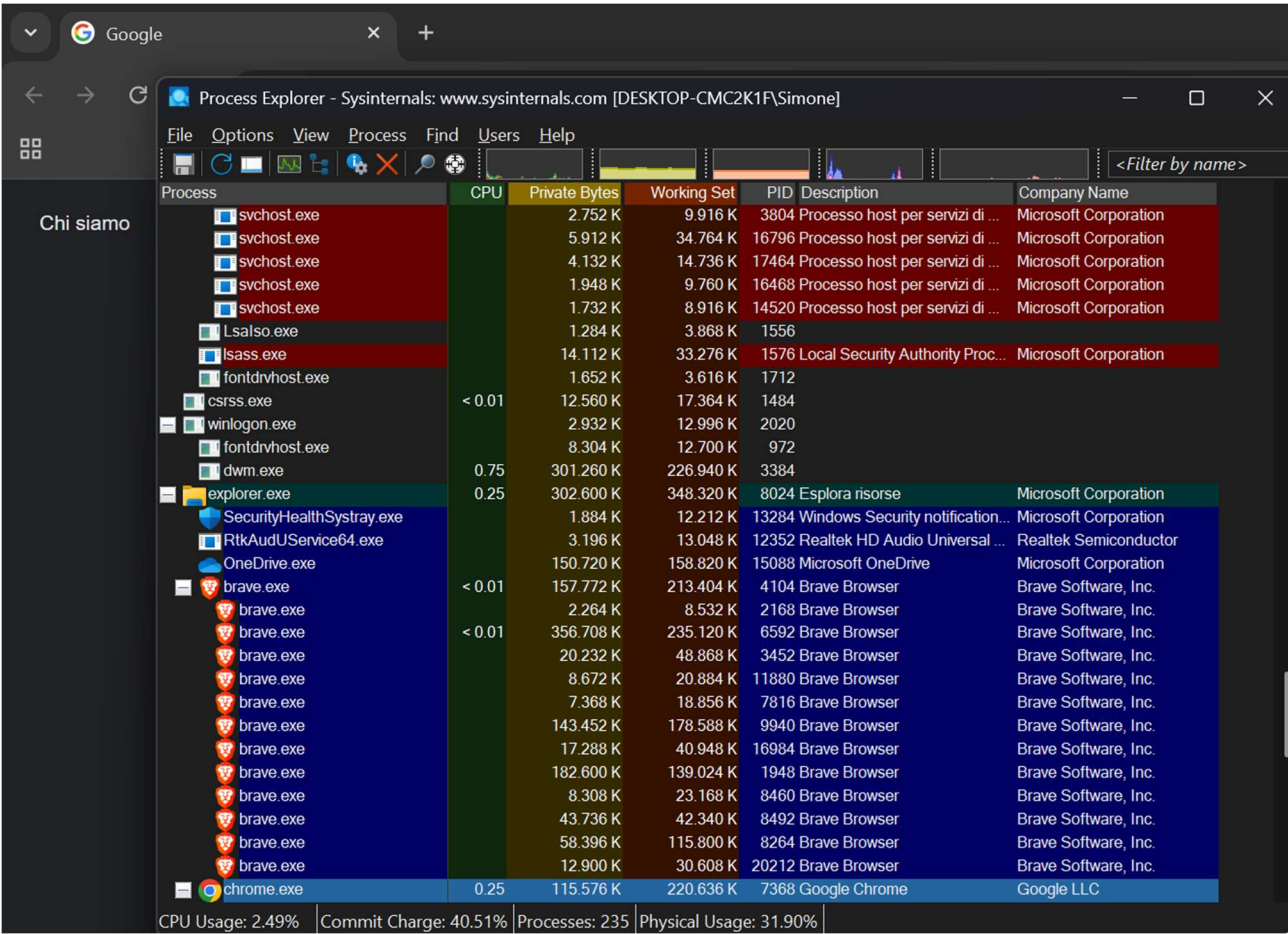


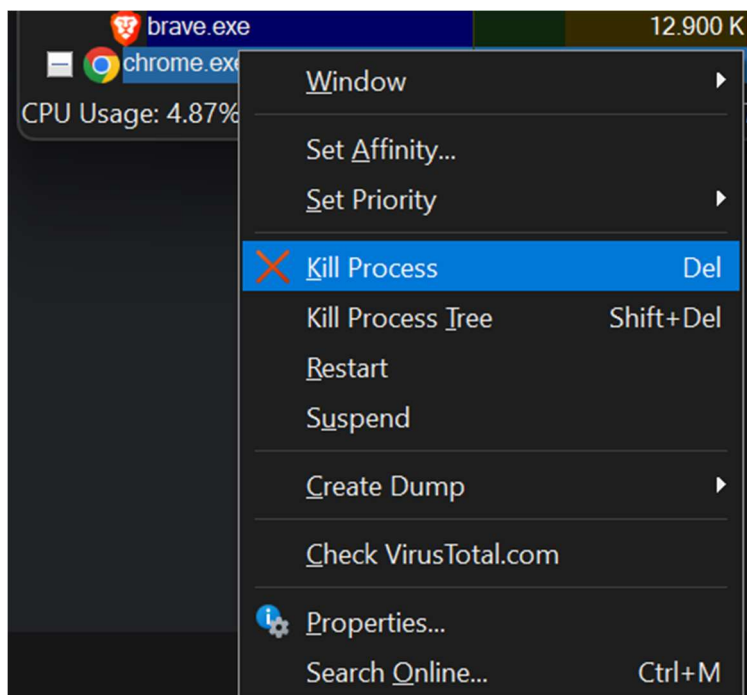
Parte 1 = Eseguiamo procexp.exe



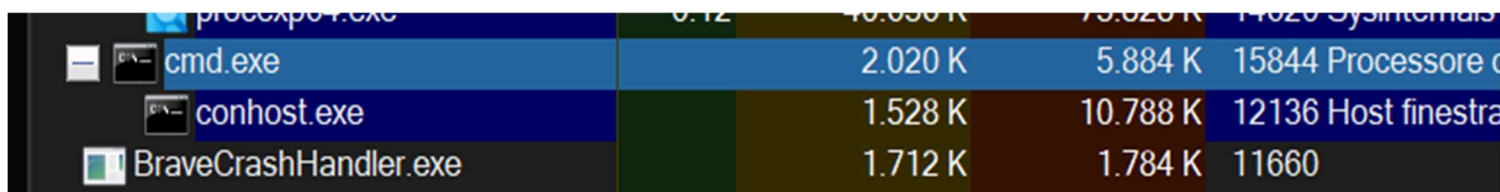
Tramite il tasto di ricerca cerchiamo il processo di chrome:



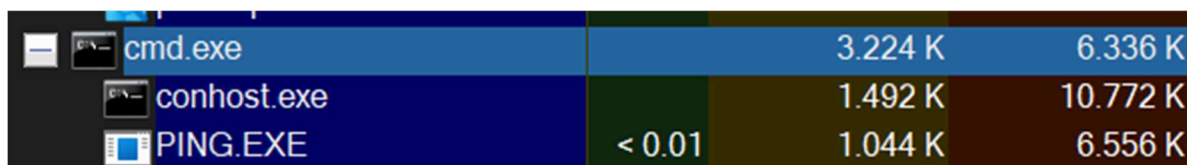
Usando Kill process lo chiudiamo:



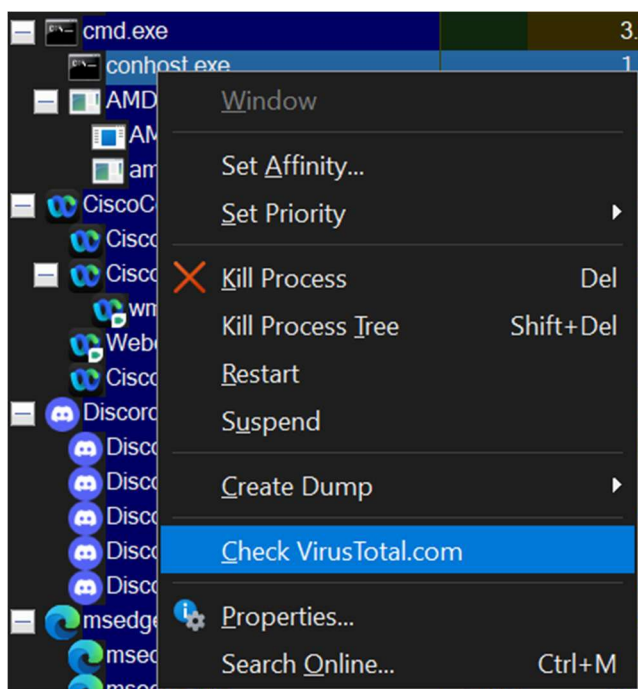
Tramite explorer, apriamo cmd:



Ed eseguiamo un ping:



Facciamo un controllo con virustotal su conhost.exe:



Il risultato compare nella colonna di destra:

OneDrive.exe		152.024 K	161.048 K	15088 Microsoft OneDrive	Microsoft Corporation
brave.exe	< 0.01	157.676 K	212.276 K	4104 Brave Browser	Brave Software, Inc.
brave.exe		2.264 K	8.532 K	2168 Brave Browser	Brave Software, Inc.
brave.exe	< 0.01	348.780 K	229.180 K	6592 Brave Browser	Brave Software, Inc.
brave.exe		20.116 K	48.812 K	3452 Brave Browser	Brave Software, Inc.
brave.exe		8.672 K	20.884 K	11880 Brave Browser	Brave Software, Inc.
brave.exe		7.364 K	18.852 K	7816 Brave Browser	Brave Software, Inc.
brave.exe		143.556 K	178.628 K	9940 Brave Browser	Brave Software, Inc.
brave.exe		17.288 K	40.948 K	16984 Brave Browser	Brave Software, Inc.
brave.exe		182.720 K	139.120 K	1948 Brave Browser	Brave Software, Inc.
brave.exe		8.308 K	23.168 K	8460 Brave Browser	Brave Software, Inc.
brave.exe		43.736 K	42.340 K	8492 Brave Browser	Brave Software, Inc.
brave.exe		57.660 K	110.880 K	8264 Brave Browser	Brave Software, Inc.
brave.exe		13.024 K	30.768 K	20212 Brave Browser	Brave Software, Inc.
WINWORD.EXE	< 0.01	233.512 K	320.436 K	5744 Microsoft Word	Microsoft Corporation
ai.exe	< 0.01	22.920 K	40.520 K	19152 Artificial Intelligence (AI) Host...	Microsoft Corporation
proccxp.exe		6.236 K	14.500 K	1852 Sysinternals Process Explorer	Sysinternals - www.sysinter...
proccxp64.exe	0.25	40.980 K	80.048 K	14620 Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		4.120 K	6.276 K	15844 Processore dei comandi di Wi...	Microsoft Corporation
conhost.exe		1.536 K	10.824 K	12136 Host finestra console	Microsoft Corporation

0/77

Chiudiamo il processo cmd e tutti i sottoprocessi a lui collegati:

cmd.exe	3.920 K	17.676 K
conhost.exe		6.752 K
AMDRSS		31.780 K
AMDRS		59.932 K
amdow.		1.860 K
CiscoCollab		404.008 K
CiscoColla		2.264 K
CiscoColla		750.724 K
wmlhos		20.416 K

Parte 2 = Apriamo un prompt dei comandi, su conhost.exe facciamo tasto destro – proprietà e andiamo su thread:

conhost.exe:11568 Properties				
TCP/IP		Security		Environment
Image		Performance		Performance Graph
		GPU Graph		Strings
Threads				
Count: 4				
TID	CPU	Cycles Delta	Suspend Count	Start Address
4692				conhost.exe+0x26190
10460				combase.dll!RoParameterize...
16796				ntdll.dll!TpCallbackMayRunLo...
18892				conhost.exe+0x97240
Thread ID: 4692				
Start Time: 15:03:42 22/10/2024				
State: Wait:UserRequest				
Base Priority: 8				
Kernel Time: 0:00:00.000				
Dynamic Priority: 9				
User Time: 0:00:00.015				
I/O Priority: Normal				
Context Switches: 30				
Memory Priority: 5				
Cycles: 20.192.686				
Ideal Processor: 8				
Permissions				
Kill				
Suspend				
OK				
Cancel				

Poi, in alto facciamo view – lower panel view – handles

ViewProcessFindUsersHelp

System Information...Ctrl+I

Show Process TreeCtrl+T

✓ Show Column Heatmaps

Scroll to New Processes

Show Unnamed Handles and Mappings

✓ Show Processes From All Users

Opacity

Show Lower PaneCtrl+L

Lower Pane View

Refresh NowF5

Update Speed

Organize Column Sets...

Save Column Set...

Load Column Set

Select Columns...

7460Processo host per serv

3016Processo host per serv

1556

1576Local Security Authority

1712

1484

2020

972

3384

8024Esplora risorse

DLLsCtrl+D

HandlesCtrl+H

ThreadsCtrl+Y

2768Brave Browser

6592Brave Browser

3452Brave Browser

1880Brave Browser

7816Brave Browser

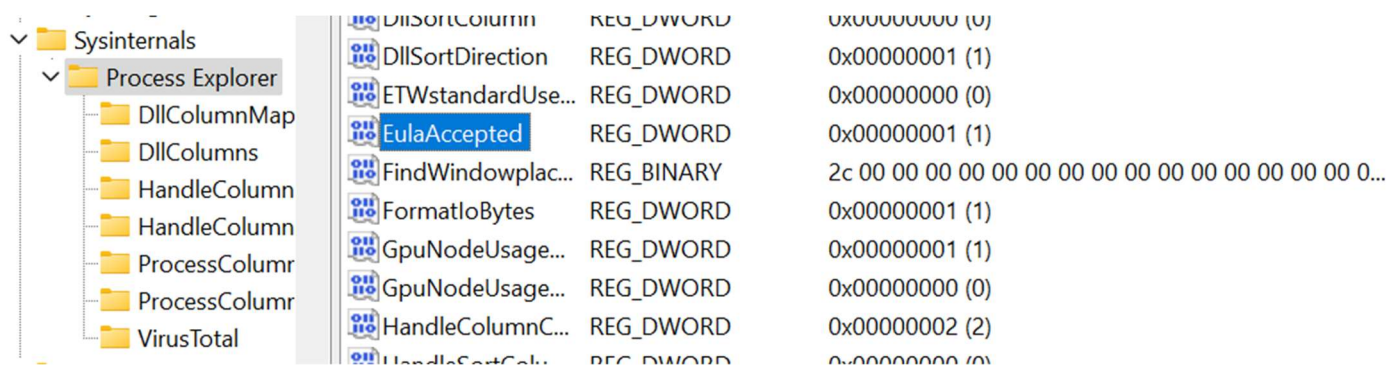
9940Brave Browser

6984Brave Browser

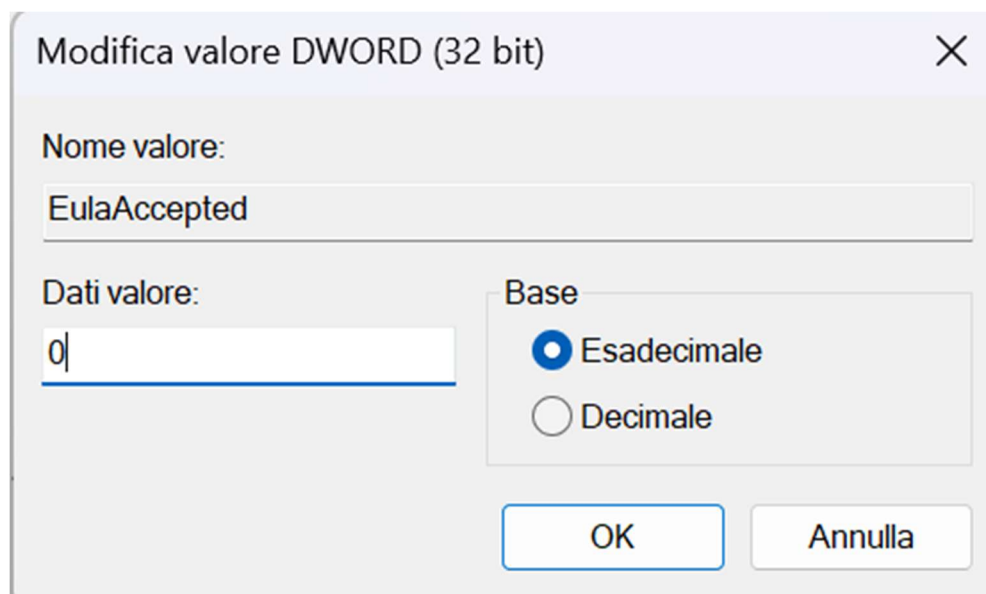
1040Brave Browser

Handles		
Type	Name	
ALPC Port	\RPC Control\OLE90DBFFA7679B7BC2630570E0EF95	
ALPC Port	\BaseNamedObjects\{CoreUI}-PID(2660)-TID(19244) d6534f19-c9a7-4bf2-b566-fddae79969...	
ALPC Port	\BaseNamedObjects\{CoreUI}-PID(2660)-TID(2300) 9c400ee6-9ca2-410f-86e8-7e0fdae297cd	
ALPC Port	\BaseNamedObjects\{CoreUI}-PID(2660)-TID(14632) a638a877-7d71-47f2-8f58-c10754f274...	
ALPC Port	\BaseNamedObjects\{CoreUI}-PID(2660)-TID(2300) 25575ff1-5a57-4026-9382-7f2787b6da59	
ALPC Port	\BaseNamedObjects\{CoreUI}-PID(2660)-TID(14632) ac8f98b9-11d0-4a4d-854a-78d3115be...	
ALPC Port	\BaseNamedObjects\{CoreUI}-PID(2660)-TID(14632) 345994c8-59b9-4b05-88f6-e1852e252...	
Desktop	\Default	
Directory	\KnownDlls	
Directory	\Sessions\1\BaseNamedObjects	
Event	\KernelObjects\MaximumCommitCondition	
Event	\Sessions\1\BaseNamedObjects\HasDeferredAnimationOperations.2660.19244	
Event	\Sessions\1\BaseNamedObjects\AMDSetsHookE_A64	
Event	\Sessions\1\BaseNamedObjects\HasAnimations.2660.19244	
Event	\Sessions\1\BaseNamedObjects\AnimationsComplete.2660.19244	
Event	\Sessions\1\BaseNamedObjects\HasDeferredAnimationOperations.2660.19244	
Event	\Sessions\1\BaseNamedObjects\DeferredAnimationOperationsComplete.2660.19244	
Event	\Sessions\1\BaseNamedObjects\RootVisualReset.2660.19244	
Event	\Sessions\1\BaseNamedObjects\ImageDecodingIdle.2660.19244	
Event	\Sessions\1\BaseNamedObjects\FontDownloadsIdle.2660.19244	
Event	\Sessions\1\BaseNamedObjects\PopupMenuCommandInvoked.2660.19244	
Event	\Sessions\1\BaseNamedObjects\HasBuildTreeWorks.2660.19244	
Event	\Sessions\1\BaseNamedObjects\BuildTreeServiceDrained.2660.19244	

Parte 3) Nei registri di sistema cerchiamo EulaAccepted sotto HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer



Cambiamo il valore in 0:



Riaprendo procexp.exe dovremo riaccettare di nuovo l'EULA

