CYBER OPS GIORNO 1

ESERIZIO 10/12:

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

Parte 1: Esplorazione dei processi

In questa parte esplorerai i processi. I processi sono programmi o applicazioni in esecuzione. Esplorerai i processi utilizzando Process Explorer nella Windows SysInternals Suite. Inoltre, avvierai e osserverai un nuovo processo.

Passaggio 1: Scarica Windows SysInternals Suite.

a. Vai al seguente link per scaricare Windows SysInternals Suite:

https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

b. Una volta completato il download, estrarre i file dalla cartella.

c. Lasciare aperto il browser web per i passaggi successivi.

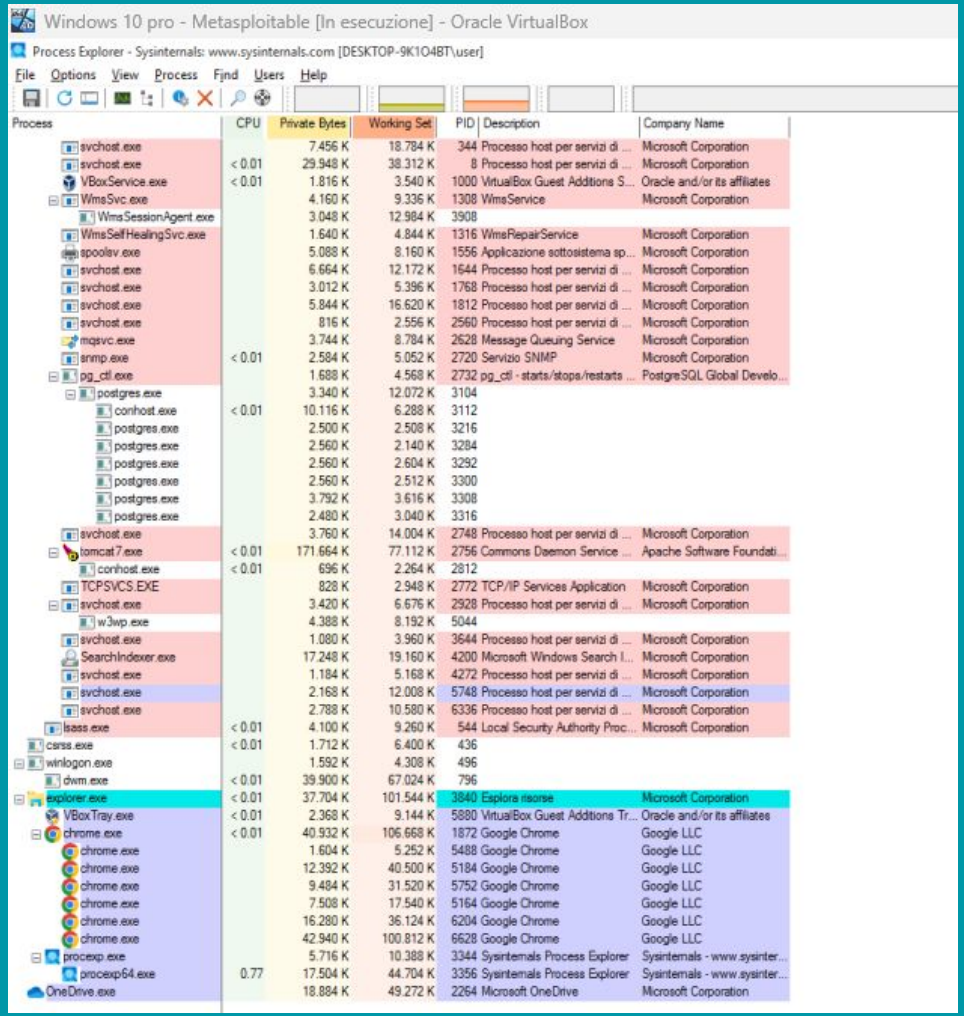
Fase 2: esplorare un processo attivo.

a. Passare alla cartella SysinternalsSuite con tutti i file estratti.

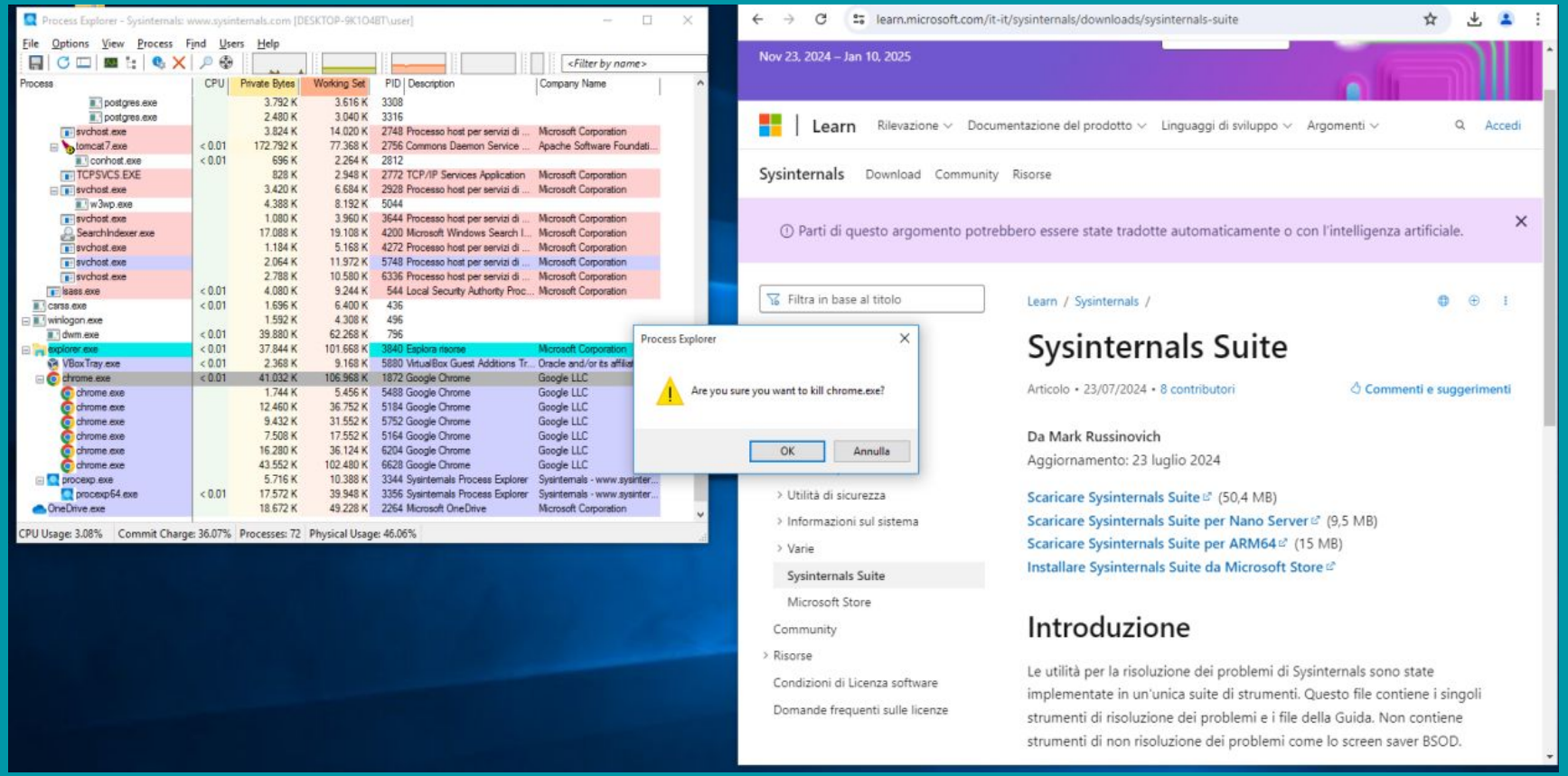
b. Aprire **procexp.exe** . Accettare il Contratto di licenza di Process Explorer quando richiesto.

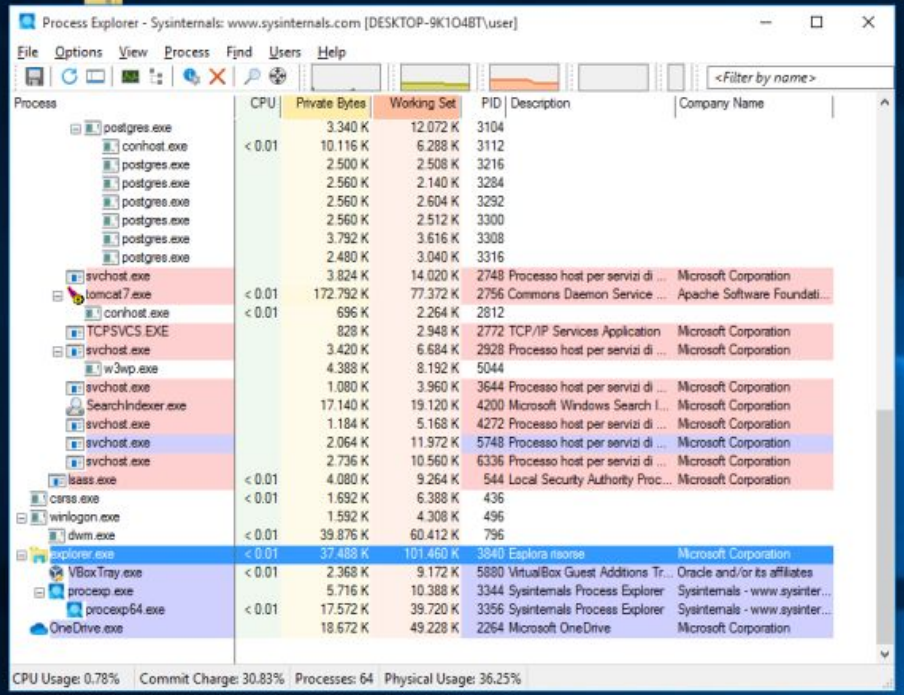
c. Process Explorer visualizza un elenco dei processi attualmente attivi.

d. Per individuare il processo del browser Web, trascinare l' icona **Processo della finestra Trova** nella finestra del browser Web aperta.


Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
svchost.exe 7.456 K 18.784 K 344 Processo host per servizi di ... Microsoft Corporation
svchost.exe < 0.01 29.948 K 38.312 K 8 Processo host per servizi di ... Microsoft Corporation
VBoxService.exe < 0.01 1.816 K 3.540 K 1000 VirtualBox Guest Additions S... Oracle and/or its affiliates
WmiSvc.exe 4.160 K 9.336 K 1308 WmiService Microsoft Corporation
WmiSessionAgent.exe 3.048 K 12.984 K 3908
WmiSelfHealingSvc.exe 1.640 K 4.844 K 1316 WmiRepairService Microsoft Corporation
spoolsv.exe 5.088 K 8.160 K 1556 Applicazione sottosistema sp... Microsoft Corporation
svchost.exe 6.664 K 12.172 K 1644 Processo host per servizi di ... Microsoft Corporation
svchost.exe 3.012 K 5.396 K 1768 Processo host per servizi di ... Microsoft Corporation
svchost.exe 5.844 K 16.620 K 1812 Processo host per servizi di ... Microsoft Corporation
svchost.exe 816 K 2.556 K 2560 Processo host per servizi di ... Microsoft Corporation
mqsvc.exe 3.744 K 8.784 K 2628 Message Queuing Service Microsoft Corporation
snmp.exe < 0.01 2.584 K 5.052 K 2720 Servizio SNMP Microsoft Corporation
pg_ctl.exe 1.688 K 4.568 K 2732 pg_ctl - starts/stops/restarts ... PostgreSQL Global Develo...
postgres.exe 3.340 K 12.072 K 3104
conhost.exe < 0.01 10.116 K 6.288 K 3112
postgres.exe 2.500 K 2.508 K 3216
postgres.exe 2.560 K 2.140 K 3284
postgres.exe 2.560 K 2.604 K 3292
postgres.exe 2.560 K 2.512 K 3300
postgres.exe 3.792 K 3.616 K 3308
postgres.exe 2.480 K 3.040 K 3316
svchost.exe 3.760 K 14.004 K 2748 Processo host per servizi di ... Microsoft Corporation
tomcat7.exe < 0.01 171.664 K 77.112 K 2756 Commons Daemon Service ... Apache Software Foundati...
conhost.exe < 0.01 696 K 2.264 K 2812
TCPSVCS.EXE 828 K 2.948 K 2772 TCP/IP Services Application Microsoft Corporation
svchost.exe 3.420 K 6.676 K 2928 Processo host per servizi di ... Microsoft Corporation
w3wp.exe 4.388 K 8.192 K 5044
svchost.exe 1.080 K 3.960 K 3644 Processo host per servizi di ... Microsoft Corporation
SearchIndexer.exe 17.248 K 19.160 K 4200 Microsoft Windows Search I... Microsoft Corporation
svchost.exe 1.184 K 5.168 K 4272 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.168 K 12.008 K 5748 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.788 K 10.580 K 6336 Processo host per servizi di ... Microsoft Corporation
lsass.exe < 0.01 4.100 K 9.260 K 544 Local Security Authority Proc... Microsoft Corporation
csrss.exe < 0.01 1.712 K 6.400 K 436
winlogon.exe 1.592 K 4.308 K 496
dwm.exe < 0.01 39.900 K 67.024 K 796
explorer.exe < 0.01 37.704 K 101.544 K 3840 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.368 K 9.144 K 5880 VirtualBox Guest Additions Tr... Oracle and/or its affiliates
chrome.exe < 0.01 40.932 K 106.668 K 1872 Google Chrome Google LLC
chrome.exe 1.604 K 5.252 K 5488 Google Chrome Google LLC
chrome.exe 12.392 K 40.500 K 5184 Google Chrome Google LLC
chrome.exe 9.484 K 31.520 K 5752 Google Chrome Google LLC
chrome.exe 7.508 K 17.540 K 5164 Google Chrome Google LLC
chrome.exe 16.280 K 36.124 K 6204 Google Chrome Google LLC
chrome.exe 42.940 K 100.812 K 6628 Google Chrome Google LLC
procexp.exe 5.716 K 10.388 K 3344 Sysinternals Process Explorer Sysinternals - www.sysinter...
procexp64.exe 0.77 17.504 K 44.704 K 3356 Sysinternals Process Explorer Sysinternals - www.sysinter...
OneDrive.exe 18.884 K 49.272 K 2264 Microsoft OneDrive Microsoft Corporation

Il processo può essere terminato in Process Explorer. Fai clic con il pulsante destro del mouse sul processo selezionato e seleziona **Kill Process** . Fai clic su **OK** per continuare




Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]
File Options View Process Find Users Help
<Filter by name>
Process CPU Private Bytes Working Set PID Description Company Name
postgres.exe 3.340 K 12.072 K 3104
conhost.exe < 0.01 10.116 K 6.288 K 3112
postgres.exe 2.500 K 2.508 K 3216
postgres.exe 2.560 K 2.140 K 3284
postgres.exe 2.560 K 2.604 K 3292
postgres.exe 2.560 K 2.512 K 3300
postgres.exe 3.792 K 3.616 K 3308
postgres.exe 2.480 K 3.040 K 3316
svchost.exe 3.824 K 14.020 K 2748 Processo host per servizi di ... Microsoft Corporation
tomcat7.exe < 0.01 172.792 K 77.372 K 2756 Commons Daemon Service ... Apache Software Foundati...
conhost.exe < 0.01 696 K 2.264 K 2812
TCPSVCS.EXE 828 K 2.948 K 2772 TCP/IP Services Application Microsoft Corporation
svchost.exe 3.420 K 6.684 K 2928 Processo host per servizi di ... Microsoft Corporation
w3wp.exe 4.388 K 8.192 K 5044
svchost.exe 1.080 K 3.960 K 3644 Processo host per servizi di ... Microsoft Corporation
SearchIndexer.exe 17.140 K 19.120 K 4200 Microsoft Windows Search I... Microsoft Corporation
svchost.exe 1.184 K 5.168 K 4272 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.064 K 11.972 K 5748 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.736 K 10.560 K 6336 Processo host per servizi di ... Microsoft Corporation
lsass.exe < 0.01 4.080 K 9.264 K 544 Local Security Authority Proc... Microsoft Corporation
csrss.exe < 0.01 1.692 K 6.388 K 436
winlogon.exe 1.592 K 4.308 K 496
dwm.exe < 0.01 39.876 K 60.412 K 796
explorer.exe < 0.01 37.488 K 101.460 K 3840 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.368 K 9.172 K 5880 VirtualBox Guest Additions Tr... Oracle and/or its affiliates
procexp.exe 5.716 K 10.388 K 3344 Sysinternals Process Explorer Sysinternals - www.sysinter...
procexp64.exe < 0.01 17.572 K 39.720 K 3356 Sysinternals Process Explorer Sysinternals - www.sysinter...
OneDrive.exe 18.672 K 49.228 K 2264 Microsoft OneDrive Microsoft Corporation
CPU Usage: 0.78% Commit Charge: 30.83% Processes: 64 Physical Usage: 36.25%

Passaggio 3: avviare un altro processo.

a. Aprire un Prompt dei comandi. (**Start** > cerca **Prompt dei comandi** > seleziona **Prompt dei comandi**)

b. Trascinare l' icona **del processo della finestra Trova** nella finestra del Prompt dei comandi e individuare il processo del Prompt dei comandi evidenziato in Process Explorer.

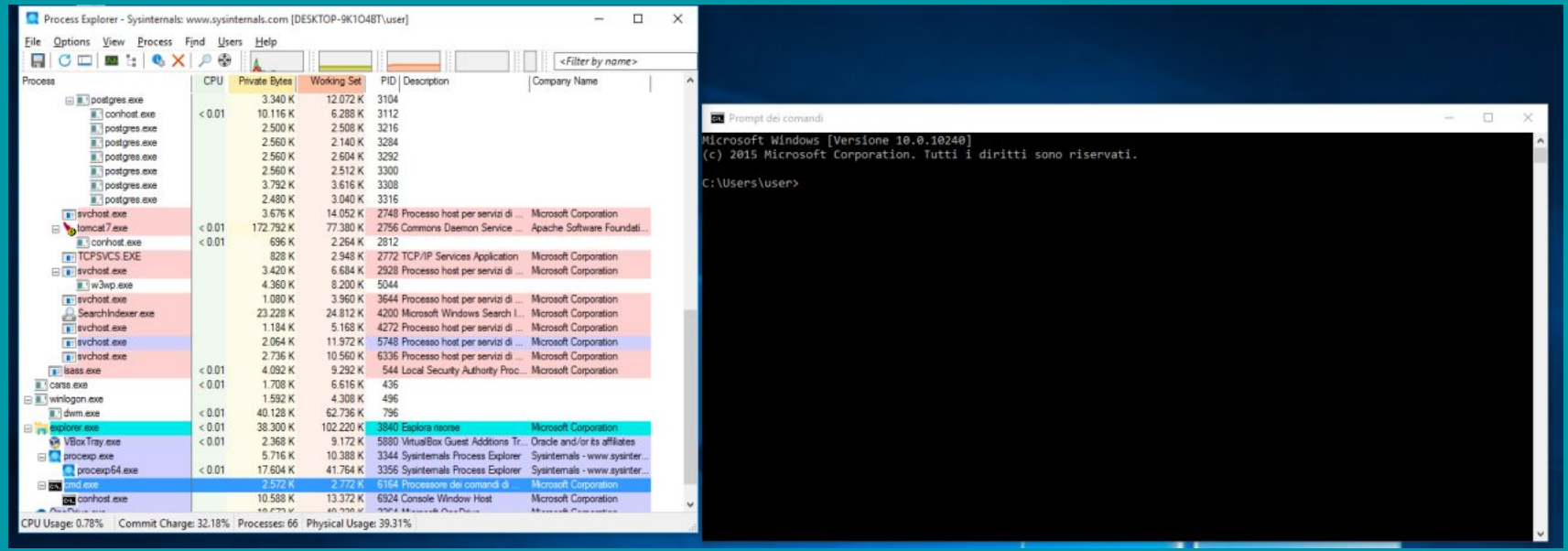
c. Il processo per il Prompt dei comandi è cmd.exe. Il suo processo padre è explorer.exe. Il cmd.exe ha un processo figlio, conhost.exe.

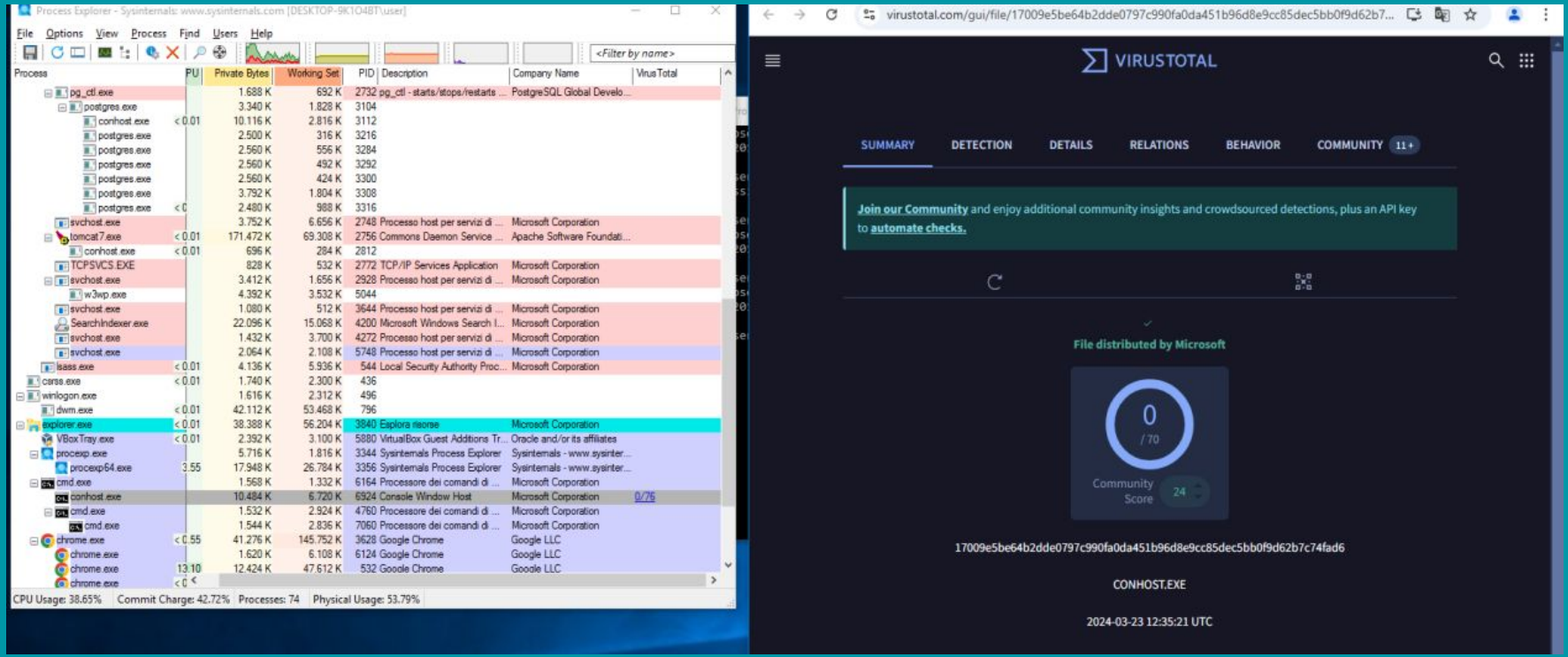
Mentre esamini l'elenco dei processi attivi, scopri che il processo figlio conhost.exe potrebbe essere sospetto. Per verificare la presenza di contenuti dannosi, fai clic con il pulsante destro del mouse **su conhost.exe** e seleziona **Controlla VirusTotal** . Quando richiesto, fai clic su **Sì** per accettare i Termini di servizio di VirusTotal. Quindi fai clic su **OK** per il prompt successivo.

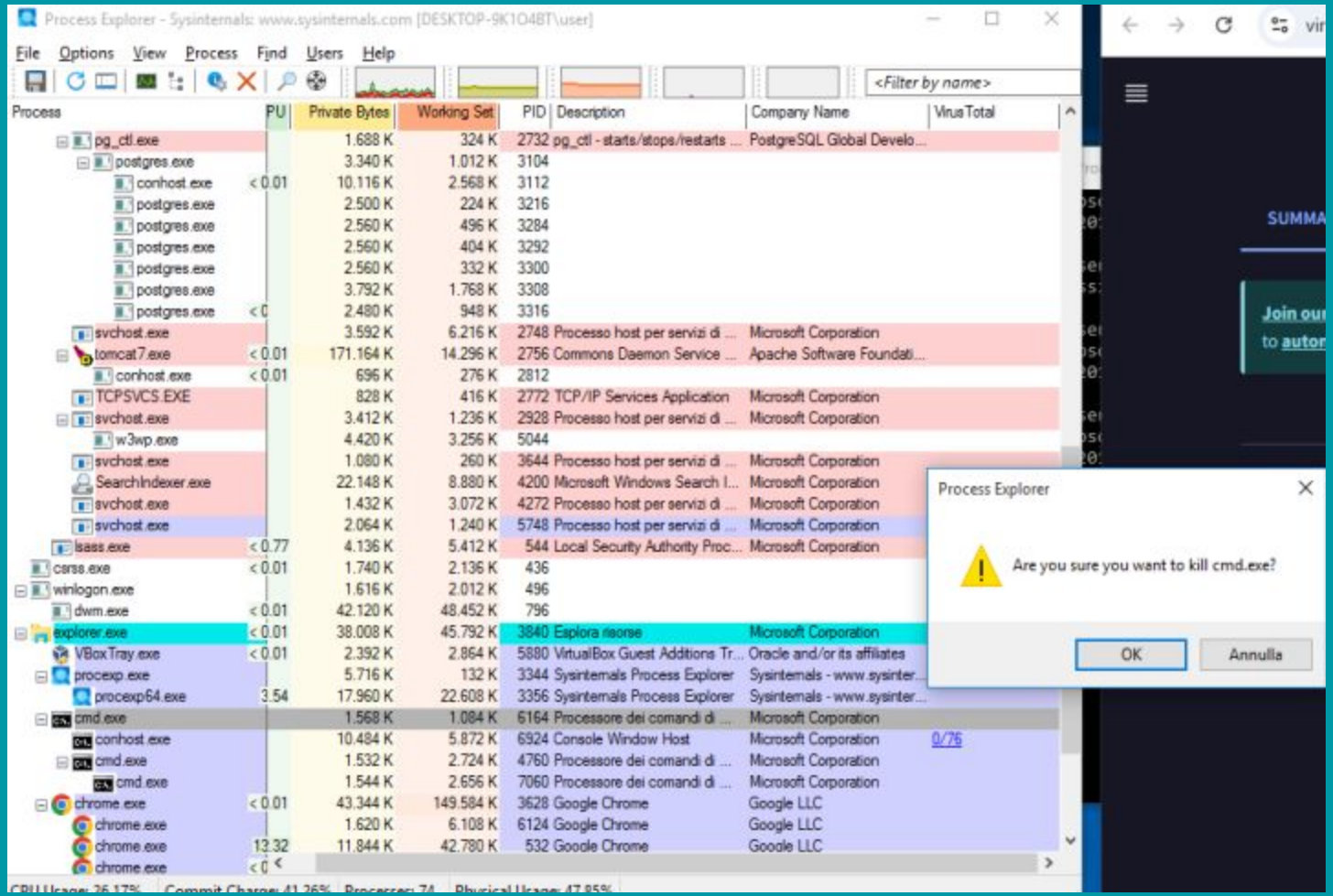
f. Espandi la finestra Process Explorer o scorri verso destra finché non vedi la colonna VirusTotal. Fai clic sul collegamento sotto la colonna VirusTotal. Il browser Web predefinito si apre con i risultati relativi al contenuto dannoso di conhost.exe.

g. Fare clic con il pulsante destro del mouse sul processo cmd.exe e selezionare **Termina processo** .

Fare clic con il pulsante destro del mouse sul processo cmd.exe e selezionare **Termina processo**


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]
File Options View Process Find Users Help
<Filter by name>
Process CPU Private Bytes Working Set PID Description Company Name
postgres.exe 3.340 K 12.072 K 3104
conhost.exe < 0.01 10.116 K 6.288 K 3112
postgres.exe 2.500 K 2.508 K 3216
postgres.exe 2.560 K 2.140 K 3284
postgres.exe 2.560 K 2.604 K 3292
postgres.exe 2.560 K 2.512 K 3300
postgres.exe 3.792 K 3.616 K 3308
postgres.exe 2.480 K 3.040 K 3316
svchost.exe 3.676 K 14.052 K 2748 Processo host per servizi di ... Microsoft Corporation
tomcat7.exe < 0.01 172.792 K 77.380 K 2756 Commons Daemon Service ... Apache Software Foundati...
conhost.exe < 0.01 696 K 2.264 K 2812
TCPSVCS.EXE 828 K 2.948 K 2772 TCP/IP Services Application Microsoft Corporation
svchost.exe 3.420 K 6.684 K 2928 Processo host per servizi di ... Microsoft Corporation
w3wp.exe 4.360 K 8.200 K 5044
svchost.exe 1.080 K 3.960 K 3644 Processo host per servizi di ... Microsoft Corporation
SearchIndexer.exe 23.228 K 24.812 K 4200 Microsoft Windows Search I... Microsoft Corporation
svchost.exe 1.184 K 5.168 K 4272 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.064 K 11.972 K 5748 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.736 K 10.560 K 6336 Processo host per servizi di ... Microsoft Corporation
lsass.exe < 0.01 4.092 K 9.292 K 544 Local Security Authority Proc... Microsoft Corporation
csrss.exe < 0.01 1.708 K 6.616 K 436
winlogon.exe 1.592 K 4.308 K 496
dwm.exe < 0.01 40.128 K 62.736 K 796
explorer.exe < 0.01 38.300 K 102.220 K 3840 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.368 K 9.172 K 5880 VirtualBox Guest Additions Tr... Oracle and/or its affiliates
procexp.exe 5.716 K 10.388 K 3344 Sysinternals Process Explorer Sysinternals - www.sysinter...
procexp64.exe < 0.01 17.604 K 41.764 K 3356 Sysinternals Process Explorer Sysinternals - www.sysinter...
cmd.exe 2.572 K 2.772 K 6164 Processore dei comandi di Microsoft Corporation
conhost.exe 10.588 K 13.372 K 6924 Console Window Host Microsoft Corporation
CPU Usage: 0.78% Commit Charge: 32.18% Processes: 66 Physical Usage: 39.31%
Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.
C:\Users\user>


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]
File Options View Process Find Users Help
<Filter by name>
Process PU Private Bytes Working Set PID Description Company Name VirusTotal
pg_ctl.exe 1.688 K 692 K 2732 pg_ctl - starts/stops/restarts ... PostgreSQL Global Develo...
postgres.exe 3.340 K 1.828 K 3104
conhost.exe < 0.01 10.116 K 2.816 K 3112
postgres.exe 2.500 K 316 K 3216
postgres.exe 2.560 K 556 K 3284
postgres.exe 2.560 K 492 K 3292
postgres.exe 2.560 K 424 K 3300
postgres.exe 3.792 K 1.804 K 3308
postgres.exe 2.480 K 988 K 3316
svchost.exe 3.752 K 6.656 K 2748 Processo host per servizi di ... Microsoft Corporation
tomcat7.exe < 0.01 171.472 K 69.308 K 2756 Commons Daemon Service ... Apache Software Foundati...
conhost.exe < 0.01 696 K 284 K 2812
TCPSVCS.EXE 828 K 532 K 2772 TCP/IP Services Application Microsoft Corporation
svchost.exe 3.412 K 1.656 K 2928 Processo host per servizi di ... Microsoft Corporation
w3wp.exe 4.392 K 3.532 K 5044
svchost.exe 1.080 K 512 K 3644 Processo host per servizi di ... Microsoft Corporation
SearchIndexer.exe 22.096 K 15.068 K 4200 Microsoft Windows Search I... Microsoft Corporation
svchost.exe 1.432 K 3.700 K 4272 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.064 K 2.108 K 5748 Processo host per servizi di ... Microsoft Corporation
lsass.exe < 0.01 4.136 K 5.936 K 544 Local Security Authority Proc... Microsoft Corporation
csrss.exe < 0.01 1.740 K 2.300 K 436
winlogon.exe 1.616 K 2.312 K 496
dwm.exe < 0.01 42.112 K 53.468 K 796
explorer.exe < 0.01 38.388 K 56.204 K 3840 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.392 K 3.100 K 5880 VirtualBox Guest Additions Tr... Oracle and/or its affiliates
procexp.exe 5.716 K 1.816 K 3344 Sysinternals Process Explorer Sysinternals - www.sysinter...
procexp64.exe 3.55 17.948 K 26.784 K 3356 Sysinternals Process Explorer Sysinternals - www.sysinter...
cmd.exe 1.568 K 1.332 K 6164 Processore dei comandi di ... Microsoft Corporation
conhost.exe 10.484 K 6.720 K 6924 Console Window Host Microsoft Corporation 0/76
cmd.exe 1.532 K 2.924 K 4760 Processore dei comandi di ... Microsoft Corporation
cmd.exe 1.544 K 2.836 K 7060 Processore dei comandi di ... Microsoft Corporation
chrome.exe < 0.55 41.276 K 145.752 K 3628 Google Chrome Google LLC
chrome.exe 1.620 K 6.108 K 6124 Google Chrome Google LLC
chrome.exe 13.10 12.424 K 47.612 K 532 Google Chrome Google LLC
chrome.exe
CPU Usage: 38.65% Commit Charge: 42.72% Processes: 74 Physical Usage: 53.79%
virustotal.com/gui/file/17009e5be64b2dde0797c990fa0da451b96d8e9cc85dec5bb0f9d62b7...
VIRUSTOTAL
SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 11+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
File distributed by Microsoft
0
/ 70
Community Score 24
17009e5be64b2dde0797c990fa0da451b96d8e9cc85dec5bb0f9d62b7c74fad6
CONHOST.EXE
2024-03-23 12:35:21 UTC


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O48T\user]
File Options View Process Find Users Help
<Filter by name>
Process PU Private Bytes Working Set PID Description Company Name VirusTotal
pg_ctl.exe 1.688 K 324 K 2732 pg_ctl - starts/stops/restarts ... PostgreSQL Global Develo...
postgres.exe 3.340 K 1.012 K 3104
conhost.exe < 0.01 10.116 K 2.568 K 3112
postgres.exe 2.500 K 224 K 3216
postgres.exe 2.560 K 496 K 3284
postgres.exe 2.560 K 404 K 3292
postgres.exe 2.560 K 332 K 3300
postgres.exe 3.792 K 1.768 K 3308
postgres.exe < 0 2.480 K 948 K 3316
svchost.exe 3.592 K 6.216 K 2748 Processo host per servizi di ... Microsoft Corporation
tomcat7.exe < 0.01 171.164 K 14.296 K 2756 Commons Daemon Service ... Apache Software Foundati...
conhost.exe < 0.01 696 K 276 K 2812
TCPSVCS.EXE 828 K 416 K 2772 TCP/IP Services Application Microsoft Corporation
svchost.exe 3.412 K 1.236 K 2928 Processo host per servizi di ... Microsoft Corporation
w3wp.exe 4.420 K 3.256 K 5044
svchost.exe 1.080 K 260 K 3644 Processo host per servizi di ... Microsoft Corporation
SearchIndexer.exe 22.148 K 8.880 K 4200 Microsoft Windows Search I... Microsoft Corporation
svchost.exe 1.432 K 3.072 K 4272 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.064 K 1.240 K 5748 Processo host per servizi di ... Microsoft Corporation
lsass.exe < 0.77 4.136 K 5.412 K 544 Local Security Authority Proc... Microsoft Corporation
csrss.exe < 0.01 1.740 K 2.136 K 436
winlogon.exe 1.616 K 2.012 K 496
dwm.exe < 0.01 42.120 K 48.452 K 796
explorer.exe < 0.01 38.008 K 45.792 K 3840 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.392 K 2.864 K 5880 VirtualBox Guest Additions Tr... Oracle and/or its affiliates
procexp.exe 5.716 K 132 K 3344 Sysinternals Process Explorer Sysinternals - www.sysinter...
procexp64.exe 3.54 17.960 K 22.608 K 3356 Sysinternals Process Explorer Sysinternals - www.sysinter...
cmd.exe 1.568 K 1.084 K 6164 Processore dei comandi di ... Microsoft Corporation
conhost.exe 10.484 K 5.872 K 6924 Console Window Host Microsoft Corporation 0/76
cmd.exe 1.532 K 2.724 K 4760 Processore dei comandi di ... Microsoft Corporation
cmd.exe 1.544 K 2.656 K 7060 Processore dei comandi di ... Microsoft Corporation
chrome.exe < 0.01 43.344 K 149.584 K 3628 Google Chrome Google LLC
chrome.exe 1.620 K 6.108 K 6124 Google Chrome Google LLC
chrome.exe 13.32 11.844 K 42.780 K 532 Google Chrome Google LLC
chrome.exe < 0
Process Explorer
Are you sure you want to kill cmd.exe?
OK
Annulla
SUMMA
Join our
to autor

Fase 1: Esplora i thread.

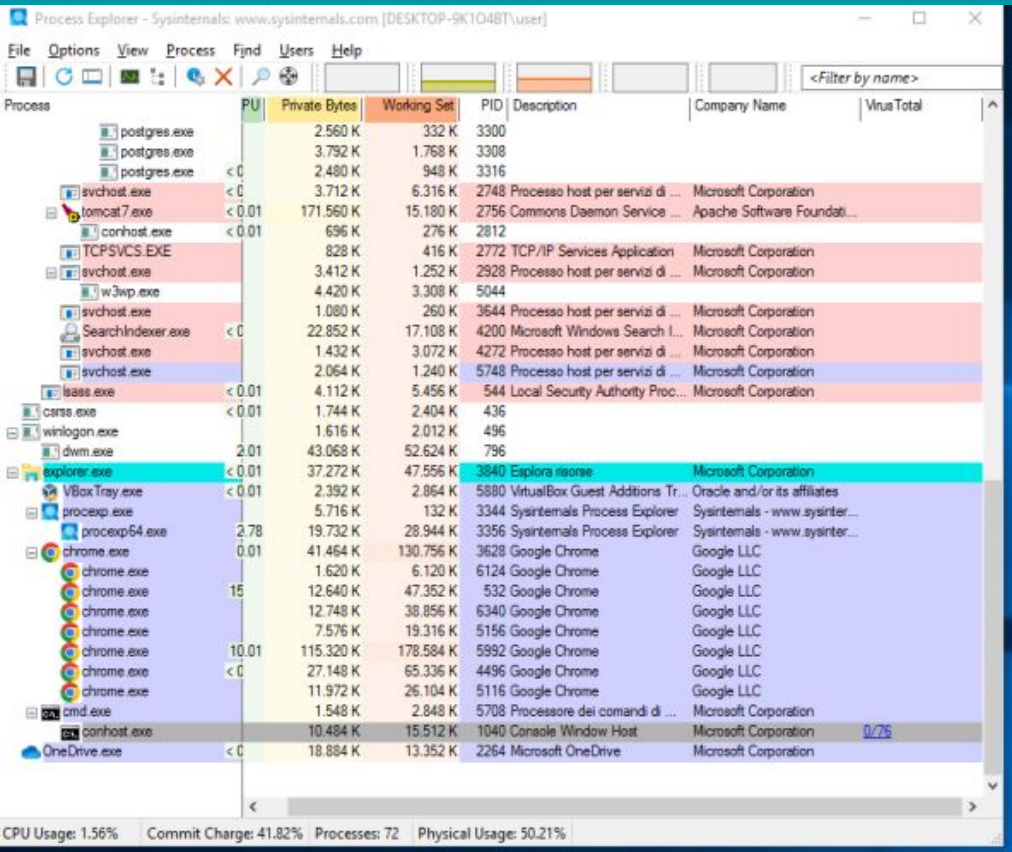
a. Aprire un prompt dei comandi.

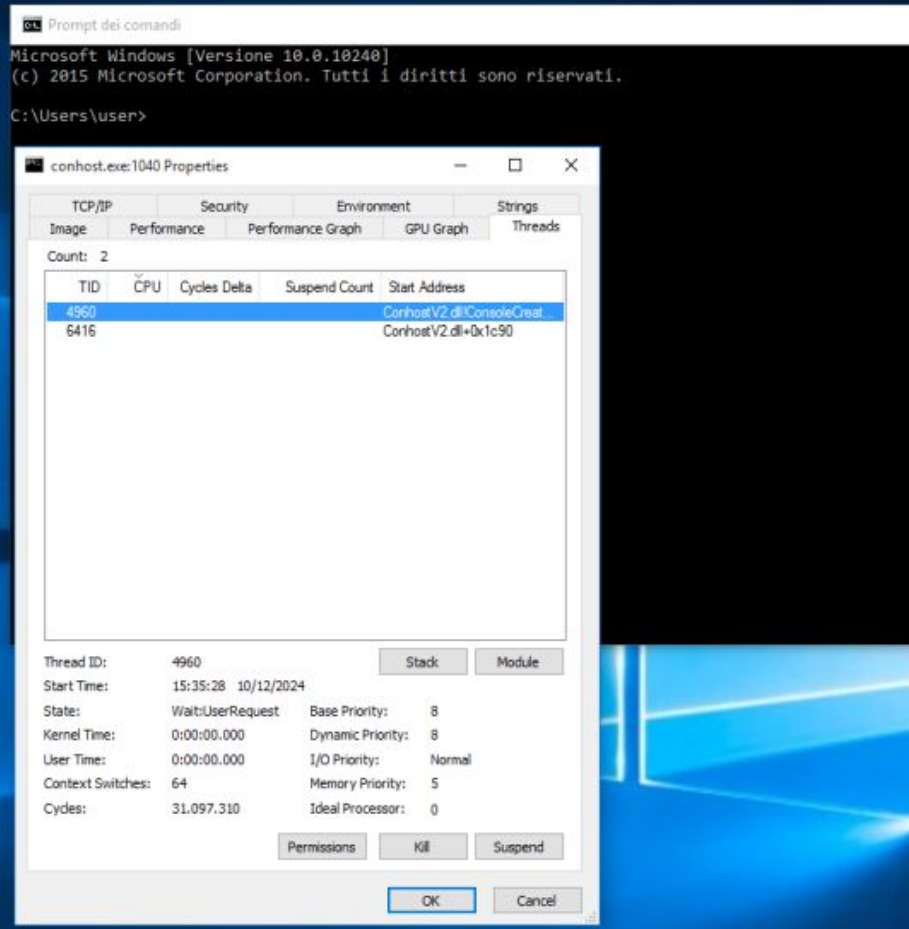
b. Nella finestra Process Explorer, fai clic con il pulsante destro del mouse su conhost.exe e seleziona **Proprietà…..** Fai clic sulla scheda **Thread** per visualizzare i thread attivi per il processo conhost.exe. Fai clic su **OK** per continuare se richiesto da una finestra di dialogo di avviso.

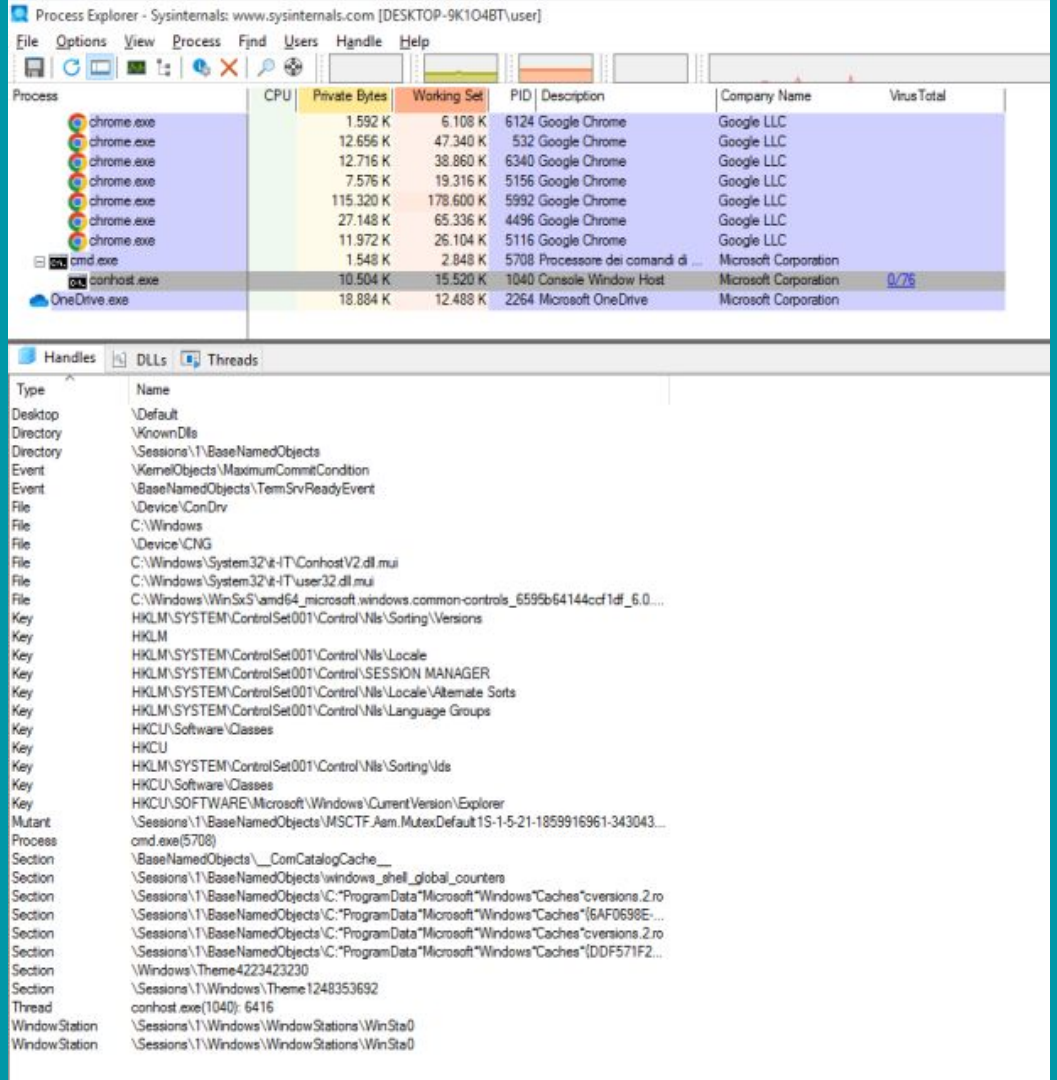
c. Esaminare i dettagli del thread

Fase 2: Esplora le maniglie.

a. In Process Explorer, fare clic su **Visualizza** > selezionare **Visualizzazione riquadro inferiore** > **Handle** per visualizzare gli handle associati al processo conhost.exe.


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]
File Options View Process Find Users Help
<Filter by name>
Process PU Private Bytes Working Set PID Description Company Name VirusTotal
postgres.exe 2.560 K 332 K 3300
postgres.exe 3.792 K 1.768 K 3308
postgres.exe < 0 2.480 K 948 K 3316
svchost.exe < 0 3.712 K 6.316 K 2748 Processo host per servizi di ... Microsoft Corporation
tomcat7.exe < 0.01 171.560 K 15.180 K 2756 Commons Daemon Service ... Apache Software Foundati...
conhost.exe < 0.01 696 K 276 K 2812
TCPSVCS.EXE 828 K 416 K 2772 TCP/IP Services Application Microsoft Corporation
svchost.exe 3.412 K 1.252 K 2928 Processo host per servizi di ... Microsoft Corporation
w3wp.exe 4.420 K 3.308 K 5044
svchost.exe 1.080 K 260 K 3644 Processo host per servizi di ... Microsoft Corporation
SearchIndexer.exe < 0 22.852 K 17.108 K 4200 Microsoft Windows Search I... Microsoft Corporation
svchost.exe 1.432 K 3.072 K 4272 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.064 K 1.240 K 5748 Processo host per servizi di ... Microsoft Corporation
lsass.exe < 0.01 4.112 K 5.456 K 544 Local Security Authority Proc... Microsoft Corporation
csrss.exe < 0.01 1.744 K 2.404 K 436
winlogon.exe 1.616 K 2.012 K 496
dwm.exe 2.01 43.068 K 52.624 K 796
explorer.exe < 0.01 37.272 K 47.556 K 3840 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.392 K 2.864 K 5880 VirtualBox Guest Additions Tr... Oracle and/or its affiliates
procexp.exe 5.716 K 132 K 3344 Sysinternals Process Explorer Sysinternals - www.sysinter...
procexp64.exe 2.78 19.732 K 28.944 K 3356 Sysinternals Process Explorer Sysinternals - www.sysinter...
chrome.exe 0.01 41.464 K 130.756 K 3628 Google Chrome Google LLC
chrome.exe 1.620 K 6.120 K 6124 Google Chrome Google LLC
chrome.exe 15 12.640 K 47.352 K 532 Google Chrome Google LLC
chrome.exe 12.748 K 38.856 K 6340 Google Chrome Google LLC
chrome.exe 7.576 K 19.316 K 5156 Google Chrome Google LLC
chrome.exe 10.01 115.320 K 178.584 K 5992 Google Chrome Google LLC
chrome.exe < 0 27.148 K 65.336 K 4496 Google Chrome Google LLC
chrome.exe 11.972 K 26.104 K 5116 Google Chrome Google LLC
cmd.exe 1.548 K 2.848 K 5708 Processore dei comandi di ... Microsoft Corporation
conhost.exe 10.484 K 15.512 K 1040 Console Window Host Microsoft Corporation 0/76
OneDrive.exe < 0 18.884 K 13.352 K 2264 Microsoft OneDrive Microsoft Corporation
CPU Usage: 1.56% Commit Charge: 41.82% Processes: 72 Physical Usage: 50.21%


Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.
C:\Users\user>
conhost.exe:1040 Properties
TCP/IP Security Environment Strings
Image Performance Performance Graph GPU Graph Threads
Count: 2
TID CPU Cycles Delta Suspend Count Start Address
4960 ConhostV2.dll!ConsoleCreat...
6416 ConhostV2.dll+0x1c90
Thread ID: 4960 Stack Module
Start Time: 15:35:28 10/12/2024
State: Wait:UserRequest Base Priority: 8
Kernel Time: 0:00:00.000 Dynamic Priority: 8
User Time: 0:00:00.000 I/O Priority: Normal
Context Switches: 64 Memory Priority: 5
Cycles: 31.097.310 Ideal Processor: 0
Permissions Kill Suspend
OK Cancel


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]
File Options View Process Find Users Handle Help
Process CPU Private Bytes Working Set PID Description Company Name VirusTotal
chrome.exe 1.592 K 6.108 K 6124 Google Chrome Google LLC
chrome.exe 12.656 K 47.340 K 532 Google Chrome Google LLC
chrome.exe 12.716 K 38.860 K 6340 Google Chrome Google LLC
chrome.exe 7.576 K 19.316 K 5156 Google Chrome Google LLC
chrome.exe 115.320 K 178.600 K 5992 Google Chrome Google LLC
chrome.exe 27.148 K 65.336 K 4496 Google Chrome Google LLC
chrome.exe 11.972 K 26.104 K 5116 Google Chrome Google LLC
cmd.exe 1.548 K 2.848 K 5708 Processore dei comandi di ... Microsoft Corporation
conhost.exe 10.504 K 15.520 K 1040 Console Window Host Microsoft Corporation 0/76
OneDrive.exe 18.884 K 12.488 K 2264 Microsoft OneDrive Microsoft Corporation
Handles DLLs Threads
Type Name
Desktop \Default
Directory \KnownDlls
Directory \Sessions\1\BaseNamedObjects
Event \KernelObjects\MaximumCommitCondition
Event \BaseNamedObjects\TermSrvReadyEvent
File \Device\ConDrv
File C:\Windows
File \Device\CNG
File C:\Windows\System32\it-IT\ConhostV2.dll.mui
File C:\Windows\System32\it-IT\user32.dll.mui
File C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0....
Key HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key HKLM
Key HKLM\SYSTEM\ControlSet001\Control\Nls\Locale
Key HKLM\SYSTEM\ControlSet001\Control\SESSION MANAGER
Key HKLM\SYSTEM\ControlSet001\Control\Nls\Locale\Alternate Sorts
Key HKLM\SYSTEM\ControlSet001\Control\Nls\Language Groups
Key HKCU\Software\Classes
Key HKCU
Key HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
Key HKCU\Software\Classes
Key HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Mutant \Sessions\1\BaseNamedObjects\MSCTF.Asm.MutexDefault1S-1-5-21-1859916961-343043...
Process cmd.exe(5708)
Section \BaseNamedObjects__ComCatalogCache__
Section \Sessions\1\BaseNamedObjects\windows_shell_global_counters
Section \Sessions\1\BaseNamedObjects\C:"ProgramData"Microsoft"Windows"Caches"cversions.2.ro
Section \Sessions\1\BaseNamedObjects\C:"ProgramData"Microsoft"Windows"Caches"{6AF0698E-...
Section \Sessions\1\BaseNamedObjects\C:"ProgramData"Microsoft"Windows"Caches"cversions.2.ro
Section \Sessions\1\BaseNamedObjects\C:"ProgramData"Microsoft"Windows"Caches"{DDF571F2...
Section \Windows\Theme4223423230
Section \Sessions\1\Windows\Theme1248353692
Thread conhost.exe(1040): 6416
WindowStation \Sessions\1\Windows\WindowStations\WinSta0
WindowStation \Sessions\1\Windows\WindowStations\WinSta0

Parte 3: Esplorazione del registro di Windows

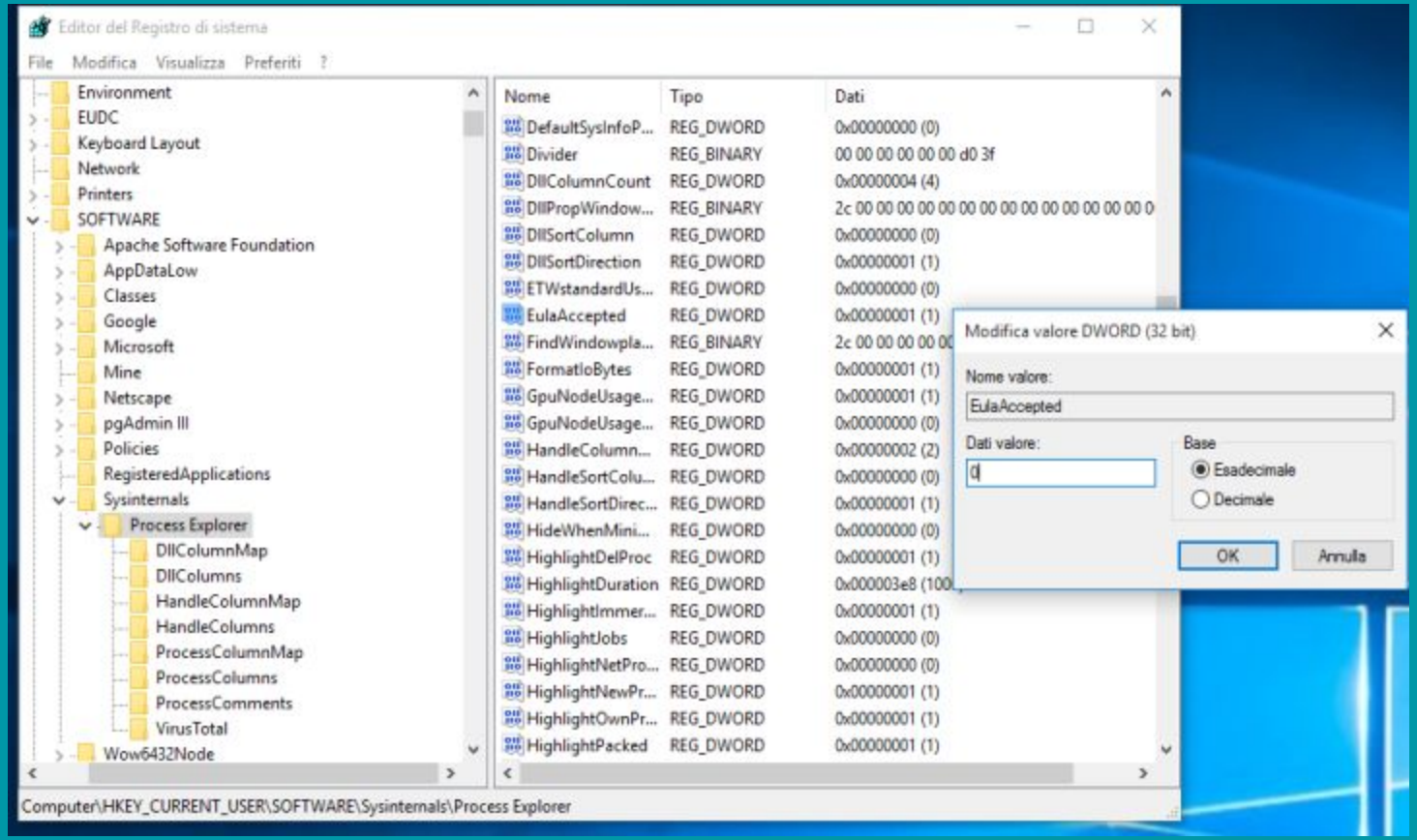
Il Registro di sistema di Windows è un database gerarchico in cui sono archiviate la maggior parte delle impostazioni di configurazione dei sistemi operativi e dell'ambiente desktop.

a. Per accedere al Registro di sistema di Windows, fai clic su **Start** > Cerca **regedit** e seleziona **Editor del Registro di sistema** . Fai clic su **Sì** quando ti viene chiesto di consentire a questa app di apportare modifiche.

Fai clic per selezionare Process Explorer in **HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer** . Scorri verso il basso per individuare la chiave **EulaAccepted** . Attualmente, il valore per la chiave di registro EulaAccepted è 0x00000001(1).

c. Fare doppio clic sulla chiave di registro **EulaAccepted** . Attualmente il valore dati è impostato su 1. Il valore 1 indica che l'EULA è stato accettato dall'utente.

d. Cambia **1** in **0** per i dati del valore. Il valore 0 indica che l'EULA non è stato accettato. Fai clic su **OK** per continuare.


Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
Environment
EUDC
Keyboard Layout
Network
Printers
SOFTWARE
Apache Software Foundation
AppDataLow
Classes
Google
Microsoft
Mine
Netscape
pgAdmin III
Policies
RegisteredApplications
Sysinternals
Process Explorer
DllColumnMap
DllColumns
HandleColumnMap
HandleColumns
ProcessColumnMap
ProcessColumns
ProcessComments
VirusTotal
Wow6432Node
Nome Tipo Dati
DefaultSysInfoP... REG_DWORD 0x00000000 (0)
Divider REG_BINARY 00 00 00 00 00 00 d0 3f
DllColumnCount REG_DWORD 0x00000004 (4)
DllPropWindow... REG_BINARY 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
DllSortColumn REG_DWORD 0x00000000 (0)
DllSortDirection REG_DWORD 0x00000001 (1)
ETWstandardUs... REG_DWORD 0x00000000 (0)
EulaAccepted REG_DWORD 0x00000001 (1)
FindWindowpla... REG_BINARY 2c 00 00 00 00 00
FormatIoBytes REG_DWORD 0x00000001 (1)
GpuNodeUsage... REG_DWORD 0x00000001 (1)
GpuNodeUsage... REG_DWORD 0x00000000 (0)
HandleColumn... REG_DWORD 0x00000002 (2)
HandleSortColu... REG_DWORD 0x00000000 (0)
HandleSortDirec... REG_DWORD 0x00000001 (1)
HideWhenMini... REG_DWORD 0x00000000 (0)
HighlightDelProc REG_DWORD 0x00000001 (1)
HighlightDuration REG_DWORD 0x000003e8 (100
HighlightImmer... REG_DWORD 0x00000001 (1)
HighlightJobs REG_DWORD 0x00000000 (0)
HighlightNetPro... REG_DWORD 0x00000000 (0)
HighlightNewPr... REG_DWORD 0x00000001 (1)
HighlightOwnPr... REG_DWORD 0x00000001 (1)
HighlightPacked REG_DWORD 0x00000001 (1)
Computer\HKEY_CURRENT_USER\SOFTWARE\Sysinternals\Process Explorer
Modifica valore DWORD (32 bit)
Nome valore:
EulaAccepted
Dati valore:
0
Base
Esadecimale
Decimale
OK
Annulla