

ESERCIZIO S11 L1

ESERCIZIO 2: Esplorazione di Processi, Thread, Handle e Registro di Windows

Obiettivi

In questo laboratorio, esplorerai i processi, i thread e gli handle utilizzando Process Explorer della Suite SysInternals. Utilizzerai anche il Registro di Windows per modificare un'impostazione.

- Parte 1: Esplorazione dei Processi
- Parte 2: Esplorazione di Thread e Handle
- Parte 3: Esplorazione del Registro di Windows

SVOLGIMENTO

L'Esercizio 2 è focalizzato sull'esplorazione approfondita dei processi Windows utilizzando **Process Explorer** della **Suite SysInternals**. L'obiettivo è comprendere il funzionamento di *processi, thread, handle e del Registro di Windows*

Procedo inizialmente con lo scaricare **SysInternals Suite** dal sito Microsoft, estraendo tutti i file in una cartella dedicata. Avvio Process Explorer per la prima volta ed inizio l'esplorazione.

Prima Esplorazione dei Processi

Nell'immagine è presente l'interfaccia principale di **Process Explorer** che mostra tutti i processi attivi del sistema. Posso osservare processi evidenziati in colori diversi: quelli in verde acqua rappresentano processi dello stesso utente, mentre quelli in rosa sono processi di sistema. La struttura ad albero mostra come ogni processo derivi da un processo genitore (relazione parent-child tra i processi).

Process Explorer - SystemInfo\www.systeminfo.com [DESKTOP-GGGGQXAdmin]

FileOptionsViewProcessFindUsersHelp

Process

CPUPrivate BytesWorking SetPIDDescriptionCompany Name

Registry3.136 K57,828 K128

System Idle Process79.2960 K8 K0

System0.7640 K176 K4

Interrupts4.550 K0 Kn/aHardware Interrupts and DPCs

smss.exe1.116 K1,628 K476

Memory Compression128 K7,620 K3076

csrss.exe2,036 K7,082 K640

wininit.exe1,428 K8,768 K712

services.exe4,760 K11,464 K888

svchost.exe8,136 K33,340 K1000Host Process for Windows S...

lsass.exe81,112 K181,944 K5920

System Idle Process48,112 K120,044 K5920Windows Task Experience H...

System Idle Process5,328 K37,420 K6076Runtime Broker

RuntimeBroker.exe3,988 K28,440 K5200Runtime Broker

svchost.exe16,112 K62,720 K6272CDM Surrogate

svchost.exe4,696 K26,024 K5172Windows Defender SmartSc...

ApplicationFrameHost.exe5,396 K45,288 K7688Application Frame Host

RuntimeBroker.exe5,536 K27,752 K5824Runtime Broker

svchost.exe2,636 K12,664 K9032

svchost.exe5,232 K27,416 K7636Runtime Broker

svchost.exe22,668 K79,396 K6288

svchost.exe5,948 K15,644 K572Host Process for Windows S...

svchost.exe2,492 K11,268 K938Host Process for Windows S...

svchost.exe2,888 K12,176 K1136Host Process for Windows S...

svchost.exe2,264 K9,748 K1152Host Process for Windows S...

svchost.exe4,436 K20,912 K1160Host Process for Windows S...

svchost.exe2,508 K12,820 K1282Host Process for Windows S...

svchost.exe1,944 K14,712 K1332Host Process for Windows S...

svchost.exe1,676 K9,180 K1380Host Process for Windows S...

svchost.exe4,476 K10,220 K1596Host Process for Windows S...

svchost.exe7,768 K16,082 K1620Host Process for Windows S...

svchost.exe5,724 K19,252 K2872Host Process for Windows T...

svchost.exe5,032 K19,328 K1680Host Process for Windows S...

svchost.exe2,388 K13,528 K1676Host Process for Windows S...

svchost.exe1,656 K7,796 K1688Host Process for Windows S...

svchost.exe2,960 K25,248 K1884Host Process for Windows S...

svchost.exe5,552 K36,540 K4992Shell Infrastructure Host

svchost.exe8,808 K33,720 K8236StoreDesktopExtension

svchost.exe6,084 K29,216 K2640svchost.exe

svchost.exe3,068 K10,784 K2536Host Process for Windows S...

svchost.exe1,528 K8,836 K1308Host Process for Windows S...

svchost.exe2,496 K11,268 K2172Host Process for Windows S...

svchost.exe2,012 K9,552 K2212Host Process for Windows S...

svchost.exe299,292 K267,182 K2320Antimalware Service Execut...

svchost.exe10,176 K22,880 K2940Host Process for Windows S...

svchost.exe10,532 K24,988 K2844Host Process for Windows S...

svchost.exe2,124 K11,000 K2908Host Process for Windows S...

svchost.exe4,288 K14,080 K3056Microsoft Network Baseline I...

svchost.exe2,028 K8,808 K2884Windows Client Address S...

svchost.exe17,232 K22,696 K2082Host Process for Windows S...

svchost.exe62,672 K7,488 K2702Host Process for Windows S...

svchost.exe1,380 K7,372 K2696Host Process for Windows S...

svchost.exe2,064 K10,262 K2716Host Process for Windows S...

svchost.exe1,848 K10,544 K2900Host Process for Windows S...

svchost.exe1,816 K10,588 K3128Host Process for Windows S...

svchost.exe2,948 K16,760 K3212Host Process for Windows S...

svchost.exe1,548 K8,896 K3244Host Process for Windows S...

svchost.exe7,760 K30,968 K7528

svchost.exe1,952 K12,140 K3420Host Process for Windows S...

svchost.exe2,504 K13,244 K3432Host Process for Windows S...

svchost.exe2,880 K19,352 K3512Host Process for Windows S...

svchost.exe71,836 K63,348 K3540Host Process for Windows S...

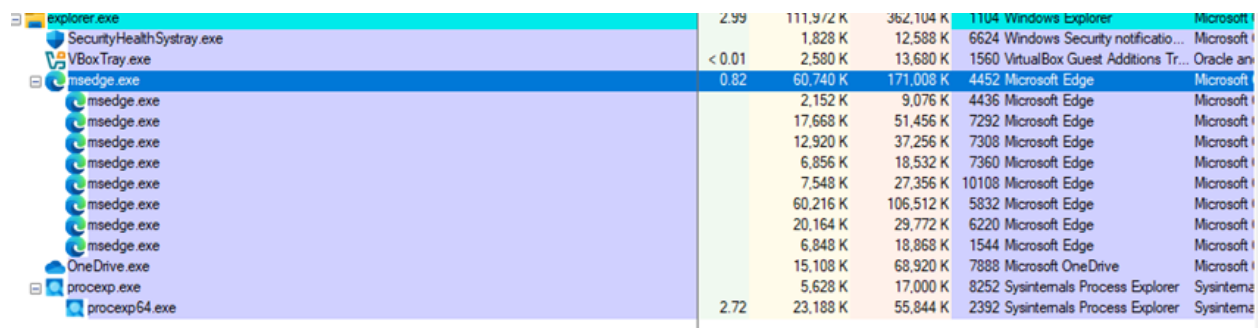
svchost.exe5,276 K20,240 K3684Spooler SubSystem App

Filter by name

Analisi di Microsoft Edge

Procedo ora utilizzando la funzione "*Find Window's Process*" per identificare il processo di Microsoft Edge. Trascino l'icona del mirino sulla finestra del browser e Process Explorer evidenzia automaticamente il processo corrispondente.

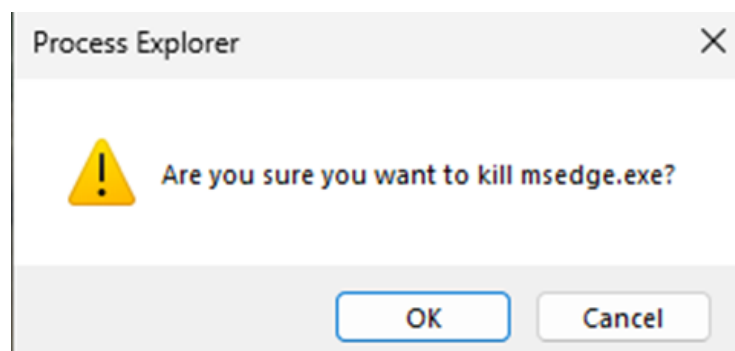
Nell'immagine successiva vedo come Process Explorer *abbia identificato diversi processi msedge.exe*, dimostrando l'*architettura multi-processo* di Edge. Ogni processo ha il proprio **PID** e utilizzo di risorse. Faccio clic destro su uno dei processi Edge per accedere al menu contestuale.



explorer.exe	2.99	111,9/2 K	362,104 K	1104 Windows Explorer	Microsoft
SecurityHealthSystray.exe		1,828 K	12,588 K	6624 Windows Security notificatio...	Microsoft
VBoxTray.exe	< 0.01	2,580 K	13,680 K	1560 VirtualBox Guest Additions Tr...	Oracle an
msedge.exe	0.82	60,740 K	171,008 K	4452 Microsoft Edge	Microsoft
msedge.exe		2,152 K	9,076 K	4436 Microsoft Edge	Microsoft
msedge.exe		17,668 K	51,456 K	7292 Microsoft Edge	Microsoft
msedge.exe		12,920 K	37,256 K	7308 Microsoft Edge	Microsoft
msedge.exe		6,856 K	18,532 K	7360 Microsoft Edge	Microsoft
msedge.exe		7,548 K	27,356 K	10108 Microsoft Edge	Microsoft
msedge.exe		60,216 K	106,512 K	5832 Microsoft Edge	Microsoft
msedge.exe		20,164 K	29,772 K	6220 Microsoft Edge	Microsoft
msedge.exe		6,848 K	18,868 K	1544 Microsoft Edge	Microsoft
OneDrive.exe		15,108 K	68,920 K	7888 Microsoft OneDrive	Microsoft
procexp.exe		5,628 K	17,000 K	8252 Sysinternals Process Explorer	Sysinterna
procexp64.exe	2.72	23,188 K	55,844 K	2392 Sysinternals Process Explorer	Sysinterna

Il menu contestuale mostra diverse opzioni, tra cui "**Kill Process**" che utilizzo per terminare il processo. Vedo anche altre opzioni utili come "**Check VirusTotal.com**" per verificare la sicurezza del processo.

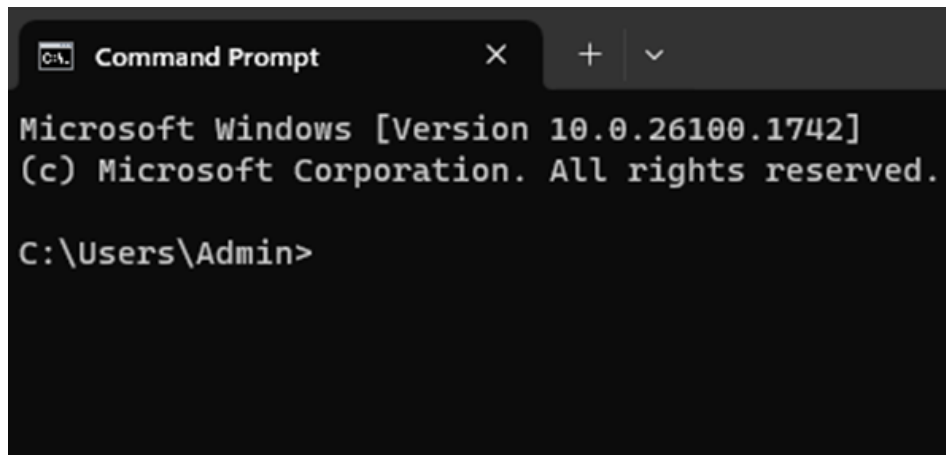
svchost.exe	2,864 K	15,432 K	1956 Host Process for Windows S...	Microsoft Corporation
MoUse	5,452 K	32,924 K	9360	
svchost.exe	6,128 K	24,672 K	6728 Host Process for Windows S...	Microsoft Corporation
svchost.exe	3,160 K	17,276 K	9640 Host Process for Windows S...	Microsoft Corporation
svchost.exe	3,040 K	13,668 K	6036 Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,804 K	15,864 K	10184 Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,692 K	8,680 K	8100 Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,940 K	11,140 K	8812 Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,680 K	9,408 K	6372 Host Process for Windows S...	Microsoft Corporation
lsass.exe	7,016 K	26,840 K	876 Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe	1,380 K	4,572 K	560	
csrss.exe	2,124 K	7,732 K	720	
winlogon.exe	2,788 K	13,660 K	784	
fontdrvhost.exe	3,352 K	8,336 K	520	
dwm.exe	83,084 K	156,940 K	1336	
explorer.exe	< 0.01	101,180 K	1104 Windows Explorer	Microsoft Corporation
SecurityHealth	< 0.01	1,768 K	6624 Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	< 0.01	2,584 K	1560 VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
msedge.exe	< 0.01	60,312 K	4452 Microsoft Edge	Microsoft Corporation



Esplorazione del Prompt dei Comandi

Procedo aprendo un prompt dei comandi per osservare la *creazione di nuovi processi e le loro relazioni*.

Vedo il prompt dei comandi appena aperto che mostra la versione di Windows e il path corrente. Questo genera il processo **cmd.exe** visibile in *Process Explorer*.



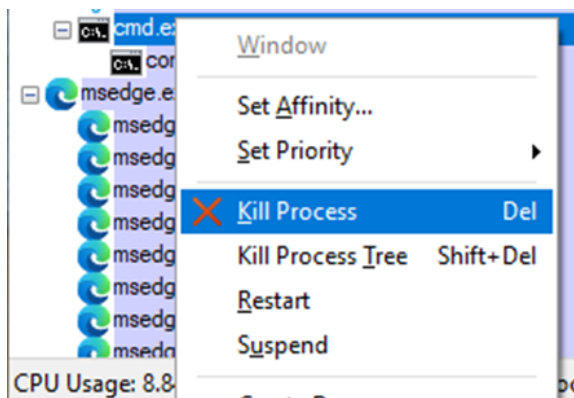
OpenConsole.exe		3,120 K	19,368 K	9304	
Windows Terminal.exe	1.82	21,536 K	87,944 K	9720	
RuntimeBroker.exe		2,424 K	13,856 K	2572	Runtime Broker Microsoft Corporation

Utilizzando nuovamente la funzione di ricerca, identifico il processo **cmd.exe** e il suo processo figlio **conhost.exe**.

Esecuzione Ping: Dopo aver avviato un comando ping, osservo come cambiano dinamicamente i valori di CPU e memoria per il processo **cmd.exe**, dimostrando l'attività in tempo reale. Il processo mostra un leggero aumento nell'utilizzo delle risorse durante l'esecuzione del comando.

Thread e Handle

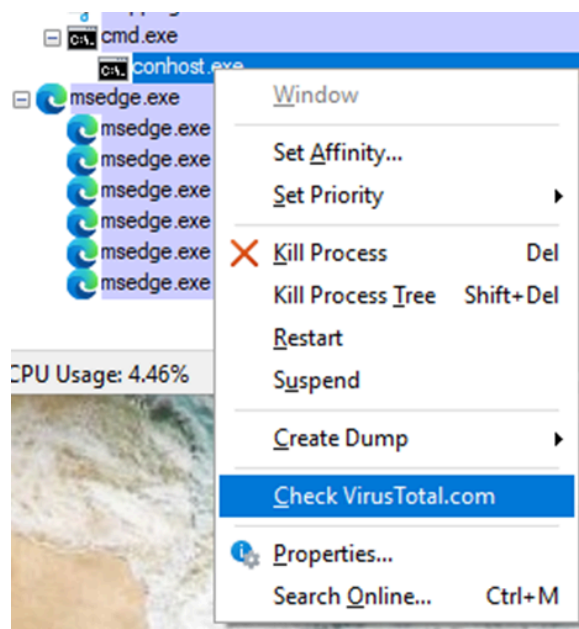
Procedo con la chiusura Kill process di **cmd.exe**.



Verrà chiuso automaticamente anche il processo figlio conhost.exe

Procedo ora con la verifica di sicurezza del processo conhost.exe utilizzando l'integrazione con VirusTotal.

Check VirusTotal: Faccio clic destro su conhost.exe e seleziono "Check VirusTotal.com" dal menu contestuale. Questa funzionalità permette di verificare se il file del processo è stato segnalato come malevolo da motori antivirus.



Risultati VirusTotal: All'avvio del check viene mandato l'hash del file al sito VirusTotal.

cmd.exe	1,988 K	5,616 K	9680 Windows Command Processor	Microsoft Corporation
conhost.exe	1,432 K	9,908 K	7248 Console Window Host	Microsoft Corporation

Nell'immagine vedo la finestra di Process Explorer con una nuova colonna "VirusTotal" che mostra lo stato della verifica. Cliccando sul link **0/77**, si apre automaticamente la pagina di VirusTotal nel browser che mostra il risultato completo: **0 detection su 77 motori antivirus**, confermando che conhost.exe è un processo completamente legittimo di Windows senza alcuna minaccia rilevata.

Process Name	Private Bytes	Working Set	Session ID	Company Name	VirusTotal
conhost.exe	1,404 K	9,892 K	7248	Console Window Host	Microsoft Corporation
msedge.exe	14.48	59,372 K	174,668 K	1628 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	2,176 K	9,944 K	3984 Microsoft Edge	Microsoft Corporation
msedge.exe	5.01	25,912 K	97,744 K	1572 Microsoft Edge	Microsoft Corporation
msedge.exe	2.78	13,312 K	38,152 K	10032 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	6,640 K	18,828 K	4904 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	85,880 K	125,408 K	9584 Microsoft Edge	Microsoft Corporation
msedge.exe	15.04	276,296 K	336,124 K	5784 Microsoft Edge	Microsoft Corporation
msedge.exe		9,652 K	20,976 K	6040 Microsoft Edge	Microsoft Corporation
msedge.exe	1.11	22,788 K	42,320 K	5708 Microsoft Edge	Microsoft Corporation

0 / 72

Community Score

No security vendors flagged this file as malicious

0eb777256a7336e65607eb7cc5772e37b7a4921c75f1979af42c3b23ca679b

CONHOST.EXE

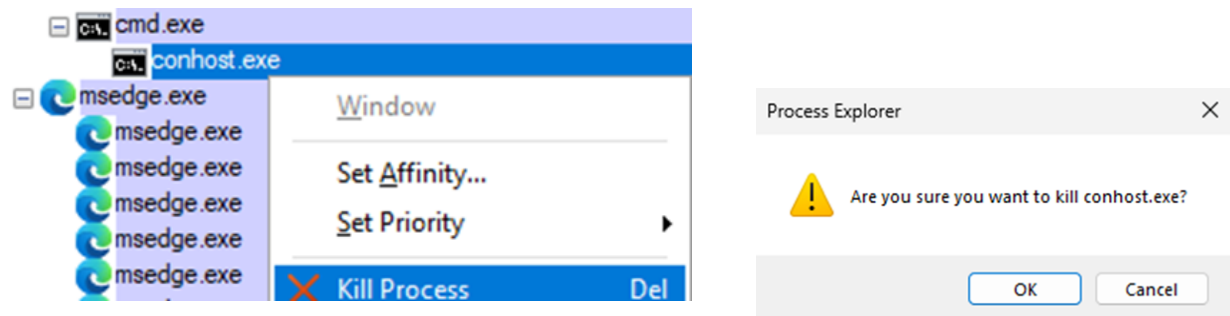
Size
1000.00 KB

Last Analysis Date
3 days ago

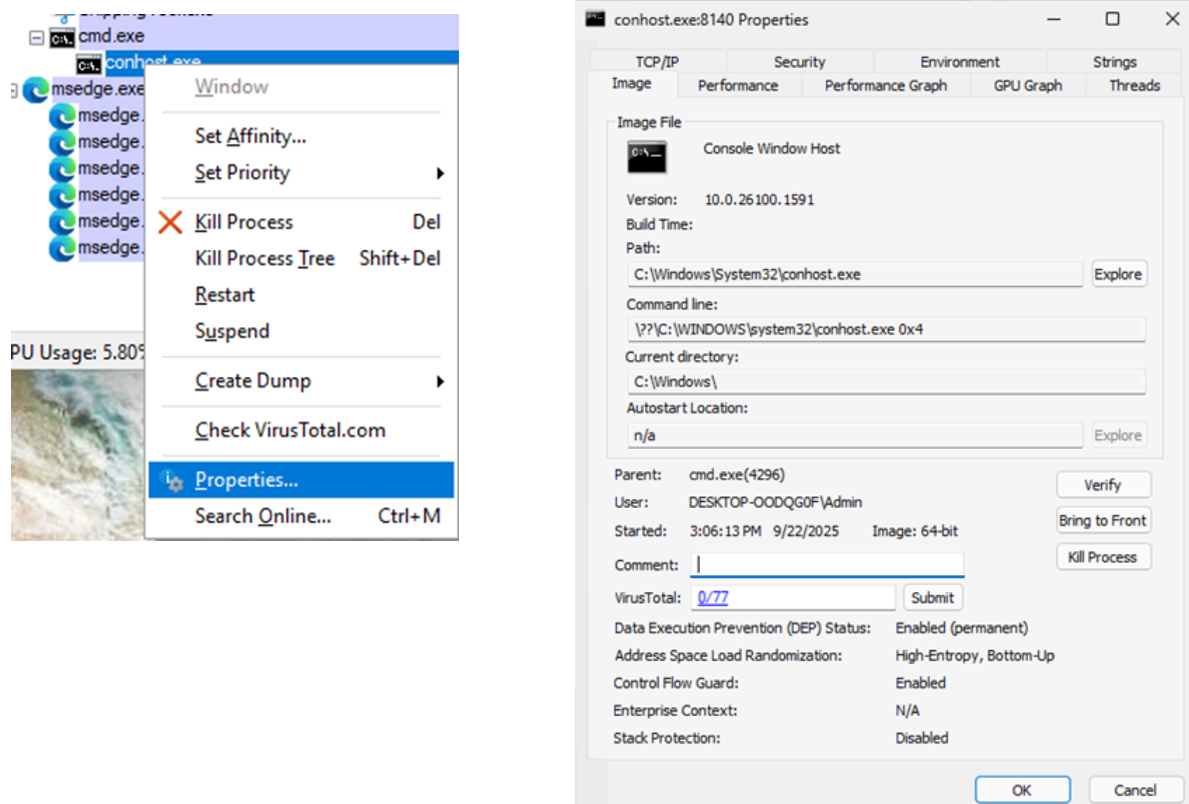
peexe 64bits known-distributor idle detect-debug-environment

Reanalyze Similar More

Kill Process di **conhost.exe**



Vado su proprietà di conhost.exe



In questa sezione Image possiamo vedere:

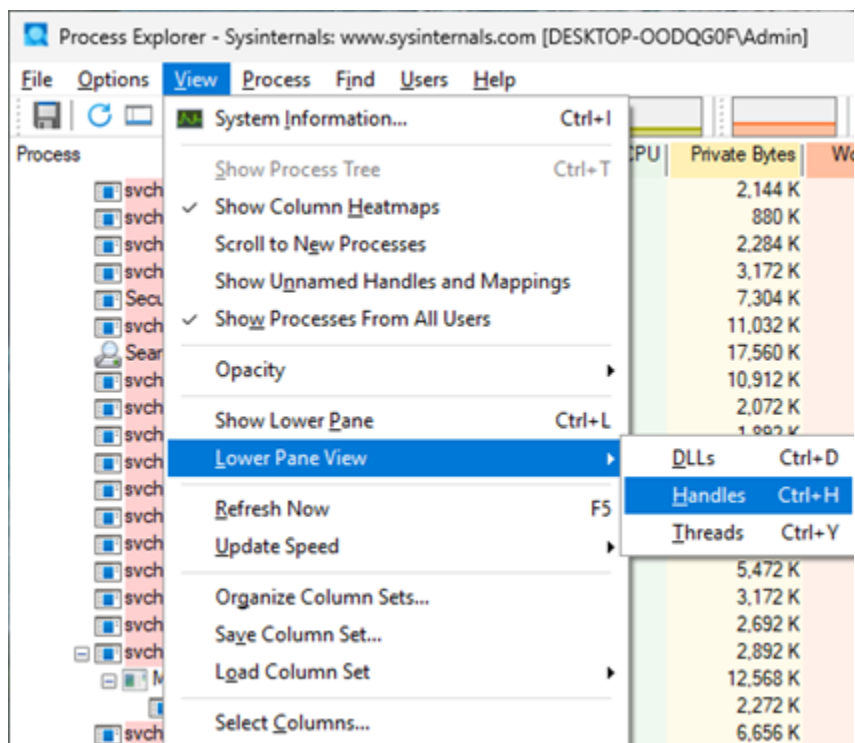
- **Image File:** conhost.exe (Console Window Host)
- **Version:** 10.0.26100.1591
- **Path:** C:\Windows\System32\conhost.exe (percorso completo del file eseguibile)
- **Command line:** Comando completo utilizzato per avviare il processo con parametri

Informazioni di Esecuzione:

- **Current directory:** C:\Windows\ (directory di lavoro corrente)
- **Parent:** cmd.exe (4296) - mostra chiaramente il processo genitore con PID
- **User:** DESKTOP-QQQQFVAdmin (utente proprietario del processo)
- **Started:** 3:06:13 PM 9/22/2025 (timestamp di avvio)
- **Image:** 64-bit (architettura del processo)

Accedere agli handles

Posso visualizzare gli handles tramite >>> View >>> Lower Pane View >>> Handles



Nell'immagine è possibile visualizzare gli handles associati al processo conhost.exe

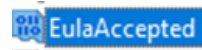
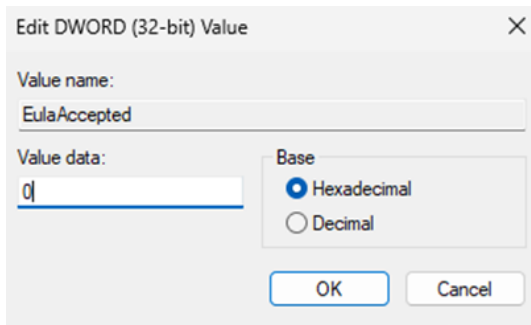
Handles		DLLs	Threads
Type	Name		
ALPC Port	\RPC Control\OLE1054757283E68D48E4659CB6B60D		
Desktop	\Default		
Directory	\KnownDlls		
Directory	\Sessions\1\1\BaseNamedObjects		
Event	\KernelObjects\MaximumCommitCondition		
File	\Device\ConDrv		
File	C:\Windows		
File	C:\Windows\System32\en-US\Conhost.exe.mui		
File	\Device\NCG		
File	\Device\NamedPipe\		
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions		
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft		
Key	HKCU		
Key	HKLM		
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options		
Key	HKLM\SOFTWARE\Microsoft\OLE		
Key	HKLM		
Key	HKCU\Software\Classes\Local Settings		
Key	HKCU\Software\Classes		
Key	HKCR\PackagedCom		
Key	HKCR\PackagedCom\ClassIndex		
Key	HKCU\Software\Classes\PackagedCom		
Key	HKCU\Software\Classes\PackagedCom\Package		
Key	HKCR\PackagedCom\Package		
Key	HKCU\Software\Classes		
Key	HKCU\Software\Classes		
Key	HKCR\PackagedCom\InterfaceIndex		
Mutant	\Sessions\1\1\BaseNamedObjects\SM0:3492:304\WlStaging_02		
Mutant	\Sessions\1\1\BaseNamedObjects\SM0:3492:120\WlError_03		
Section	\BaseNamedObjects__ComCatalogCache__		
Section	\BaseNamedObjects__ComCatalogCache__		
Semaphore	\Sessions\1\1\BaseNamedObjects\SM0:3492:304\WlStaging_02_p0		
Semaphore	\Sessions\1\1\BaseNamedObjects\SM0:3492:304\WlStaging_02_p0h		
Semaphore	\Sessions\1\1\BaseNamedObjects\SM0:3492:120\WlError_03_p0		
Semaphore	\Sessions\1\1\BaseNamedObjects\SM0:3492:120\WlError_03_p0h		
Thread	conhost.exe(3492): 8844		
Thread	conhost.exe(3492): 9772		
Thread	conhost.exe(3492): 9772		
WindowStation	\Sessions\1\1\Windows\WindowStations\WinSta0		
WindowStation	\Sessions\1\1\Windows\WindowStations\WinSta0		

Registro di Windows

Nell'ultima fase, procedo infine esplorando il registro Windows attraverso regedit, navigando tra i cinque hive principali. Modifico la chiave *EulaAccepted* di Process Explorer da **1 a 0**, dimostrando come il registro controlli il comportamento delle applicazioni.

Registry Editor			
File Edit View Favorites Help			
Computer\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer			
	Name	Type	Data
Computer			
HKEY_CLASSES_ROOT			
HKEY_CURRENT_USER			
AppEvents			
Console			
Control Panel			
Environment			
EUDC			
Keyboard Layout			
Microsoft			
Network			
Printers			
Software			
appdata\low			
ChangeTracker			
Classes			
Google			
Microsoft			
Policies			
RegisteredApplications			
Sysinternals			
Process Explorer			
DllColumnMap			
DllColumns			
HandleColumnMap			
HandleColumns			
ProcessColumnMap			
ProcessColumns			
ProcessComments			
VirusTotal			
Wow6432Node			
System			
ColorJobsDark		REG_DWORD	0x0000172d (5)
ColorNet		REG_DWORD	0x00a0ffff (105)
ColorNetDark		REG_DWORD	0x00005959 (22)
ColorNewProc		REG_DWORD	0x0046ff46 (46)
ColorNewProcDark		REG_DWORD	0x00004600 (17)
ColorOwn		REG_DWORD	0x00ffd0d0 (16)
ColorOwnDark		REG_DWORD	0x00640000 (6)
ColorPacked		REG_DWORD	0x00ff0080 (16)
ColorPackedDark		REG_DWORD	0x0037001c (3)
ColorProtected		REG_DWORD	0x008000ff (83)
ColorProtectedDark		REG_DWORD	0x001c0037 (1)
ColorRelocatedDlls		REG_DWORD	0x00a0ffff (105)
ColorRelocatedDllsDark		REG_DWORD	0x00005959 (22)
ColorServices		REG_DWORD	0x00d0d0ff (13)
ColorServicesDark		REG_DWORD	0x00000064 (1)
ColorSuspend		REG_DWORD	0x00808080 (84)
ColorSuspendDark		REG_DWORD	0x001b1b1b (1)
ConfirmKill		REG_DWORD	0x00000001 (1)
DbgHelpPath		REG_SZ	C:\WINDOWS\
DefaultDllPropPage		REG_DWORD	0x00000000 (0)
DefaultProcPropPage		REG_DWORD	0x00000006 (6)
DefaultSysInfoPage		REG_DWORD	0x00000000 (0)
Divider		REG_BINARY	29 5c 8f c2 f5 2
DllColumnCount		REG_DWORD	0x00000004 (4)
DllPropWindowplacement		REG_BINARY	2c 00 00 00 00
DllSortColumn		REG_DWORD	0x00000000 (0)
DllSortDirection		REG_DWORD	0x00000001 (1)
ETWStandardUserWarning		REG_DWORD	0x00000000 (0)
EulaAccepted		REG_DWORD	0x00000001 (1)

Cambio Valore EULA da 1 a 0 >>> da Vero a Falso



REG_DWORD

0x00000000 (0)

Domande

Cosa è successo alla finestra del browser web quando il processo è stato terminato?

La finestra del browser Microsoft Edge si è chiusa immediatamente e completamente quando il processo msedge.exe è stato terminato con "Kill Process". Questo dimostra che la terminazione forzata di un processo bypassa tutte le procedure di chiusura normale dell'applicazione, causando una chiusura istantanea senza possibilità di salvare dati

Cosa è successo durante il processo ping?

Durante l'esecuzione del comando ping, ho osservato variazioni dinamiche nell'utilizzo di CPU e memoria del processo cmd.exe in Process Explorer. Il processo ha mostrato un leggero aumento dell'attività delle risorse, dimostrando come Process Explorer possa monitorare in tempo reale l'attività dei processi durante l'esecuzione di comandi specifici.

Cosa è successo al processo figlio conhost.exe?

Al chiudersi del processo genitore cmd.exe si chiuderà automaticamente anche il processo figlio conhost.exe

Che tipo di informazioni sono disponibili nella finestra Proprietà?

Informazioni disponibili attraverso tutte le schede:

- Dettagli del file eseguibile e configurazione (**Image**)
- Monitoraggio prestazioni CPU e memoria (**Performance/Performance Graph**)
- Connessioni di rete attive (**TCP/IP**)
- Thread attivi e loro stati (**Threads**)
- Stringhe in memoria per analisi del comportamento (**Strings**)
- Variabili d'ambiente ereditate (**Environment**)

- *Contesto di sicurezza e privilegi (**Security**)*
- *Eventuale utilizzo GPU (**GPU Graph**)*

Esaminare gli handle. A cosa puntano gli handle?

Gli handle del processo conhost.exe puntano a diverse risorse di sistema

Qual è il valore per questa chiave di registro nella colonna Dati (Data)?

Una volta effettuato il cambio da 1 a 0 il valore per questa chiave è 0.

Quando apri Process Explorer, cosa vedi?

Posso vedere il License Agreement, perchè avendo cambiato il valore iniziale dell'EULA da 1 a 0, mi chiede di nuovo di accettare l'Agreement

