

Esplorazione di Processi, Thread, Handle e Registro di Windows

Obiettivi

L'attività aveva come scopo quello di analizzare e comprendere il funzionamento di processi, thread, handle e del Registro di Windows utilizzando lo strumento Process Explorer della suite Sysinternals. L'esercizio è stato suddiviso in tre parti:

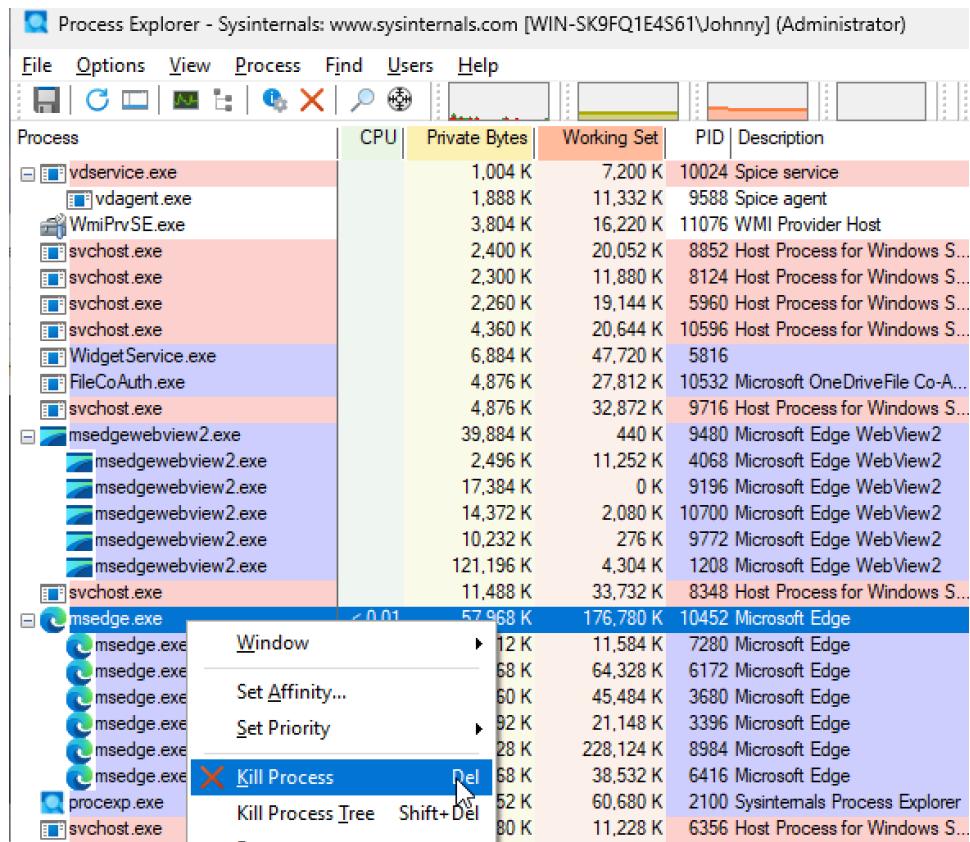
1. Esplorazione dei Processi
2. Esplorazione di Thread e Handle
3. Esplorazione del Registro di Windows

Parte 1 – Esplorazione dei Processi

Dopo aver scaricato e avviato Process Explorer, è stato possibile visualizzare l'elenco dei processi in esecuzione sul sistema. Ogni processo era corredata da informazioni come memoria utilizzata (Private Bytes, Working Set), descrizione e società sviluppatrice.

Come prova pratica, è stato selezionato il processo Microsoft Edge (msedge.exe) e successivamente è stato effettuato il comando Kill Process. L'effetto immediato osservato è stata la chiusura forzata della finestra del browser, confermando che l'interruzione del processo principale termina anche l'applicazione associata.

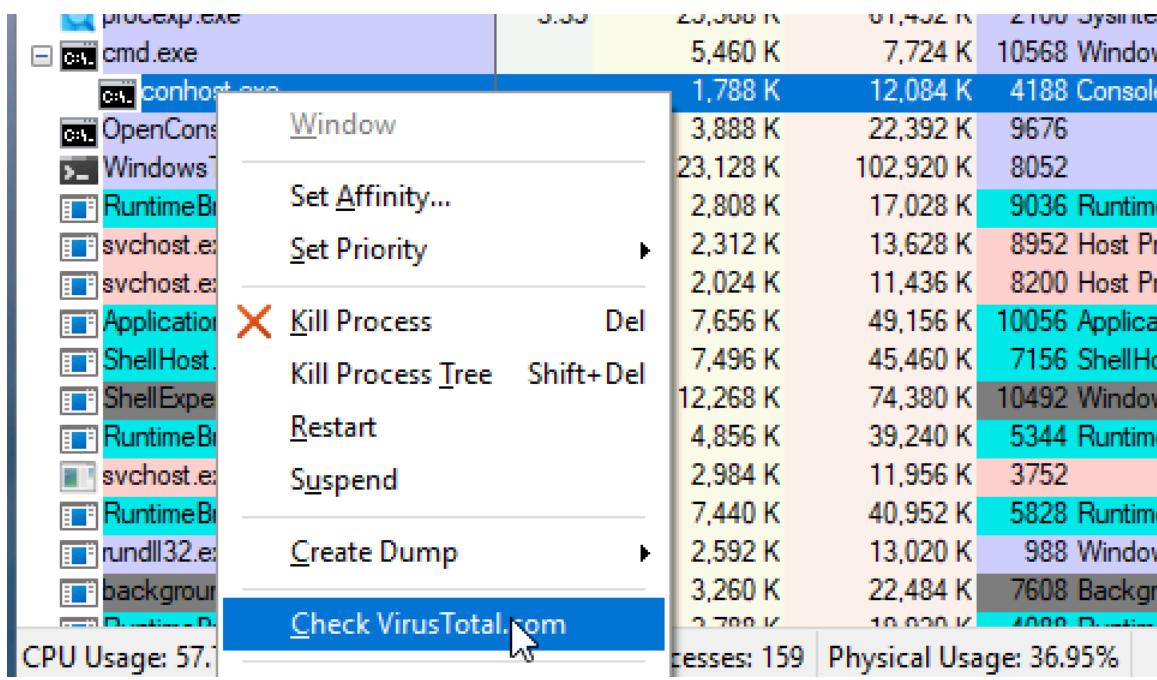
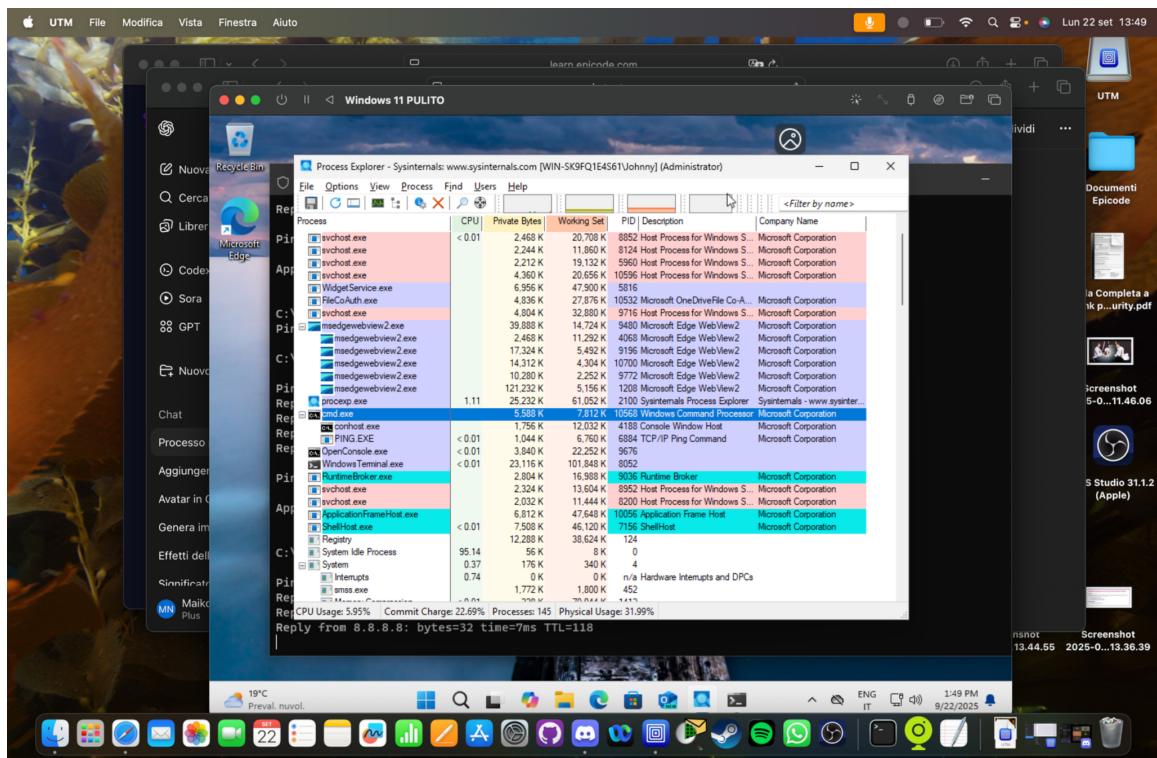
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
vdservice.exe	< 0.01	1,008 K	7,204 K	10024	Spice service	Red Hat Inc.
vdagent.exe	< 0.01	1,856 K	11,312 K	9588	Spice agent	Red Hat Inc.
WmiPrvSE.exe		3,708 K	16,128 K	11076	WMI Provider Host	Microsoft Corporation
svchost.exe		2,296 K	19,984 K	8852	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,140 K	11,812 K	8124	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,260 K	19,108 K	5960	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,308 K	20,592 K	10596	Host Process for Windows S...	Microsoft Corporation
WidgetService.exe		7,048 K	48,040 K	5816		
FileCoAuth.exe		4,868 K	27,804 K	10532	Microsoft OneDriveFile Co-A...	Microsoft Corporation
svchost.exe		4,968 K	32,940 K	9716	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		3,316 K	15,480 K	1988	WMI Provider Host	Microsoft Corporation
msedgewebview2.exe		39,716 K	8,632 K	9480	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2,428 K	11,212 K	4068	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		17,752 K	224 K	9196	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		14,672 K	3,120 K	10700	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		10,976 K	624 K	9772	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		106,128 K	3,572 K	1208	Microsoft Edge WebView2	Microsoft Corporation
svchost.exe	< 0.01	10,888 K	32,176 K	8348	Host Process for Windows S...	Microsoft Corporation
msedge.exe	< 0.01	48,216 K	149,412 K	10452	Microsoft Edge	Microsoft Corporation
msedge.exe		2,512 K	11,584 K	7280	Microsoft Edge	Microsoft Corporation
msedge.exe		13,552 K	33,740 K	6172	Microsoft Edge	Microsoft Corporation
msedge.exe		13,632 K	43,728 K	3680	Microsoft Edge	Microsoft Corporation
msedge.exe		9,288 K	21,136 K	3396	Microsoft Edge	Microsoft Corporation
msedge.exe		107,588 K	158,176 K	8984	Microsoft Edge	Microsoft Corporation
msedge.exe		19,880 K	38,480 K	6416	Microsoft Edge	Microsoft Corporation
procexp.exe	1.51	25,216 K	60,496 K	2100	Sysinternals Process Explorer	Sysinternals - www.sysinter...
WmiPrvSE.exe		3,800 K	16,796 K	7856	WMI Provider Host	Microsoft Corporation

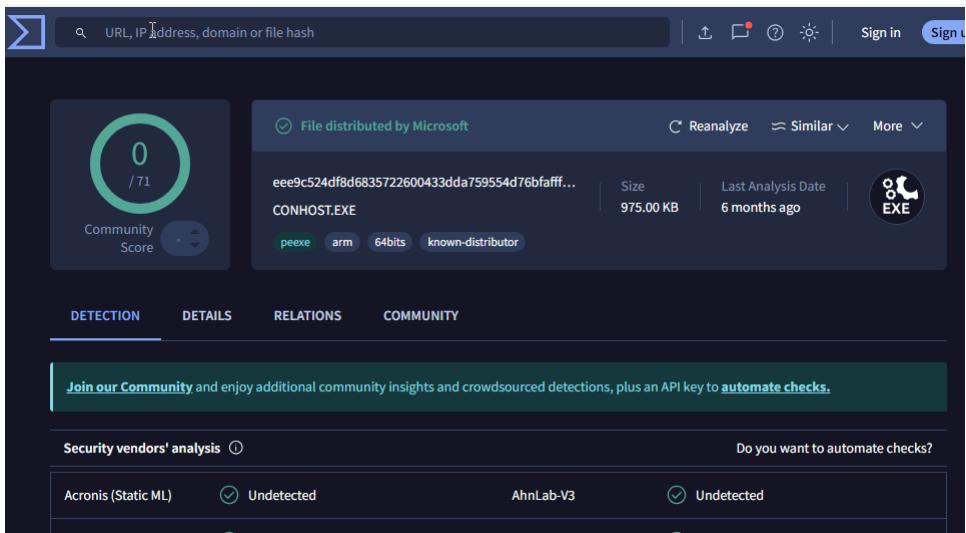


Parte 2 – Esplorazione di Thread e Handle

In questa fase è stato aperto il Prompt dei Comandi (cmd.exe). Dall’analisi in Process Explorer, si è visto che cmd.exe ha come processo figlio conhost.exe. Avviando il comando PING dal prompt, è comparso il processo temporaneo ping.exe. Terminata l’operazione di ping, questo processo si è chiuso automaticamente.

È stata inoltre verificata la sicurezza di conhost.exe inviando il suo hash a VirusTotal, che ha confermato l’assenza di codice malevolo. Infine, eseguendo Kill Process su conhost.exe, si è notato che anche la finestra del Prompt dei Comandi si è chiusa, dimostrando la relazione di dipendenza tra processo padre e figlio.

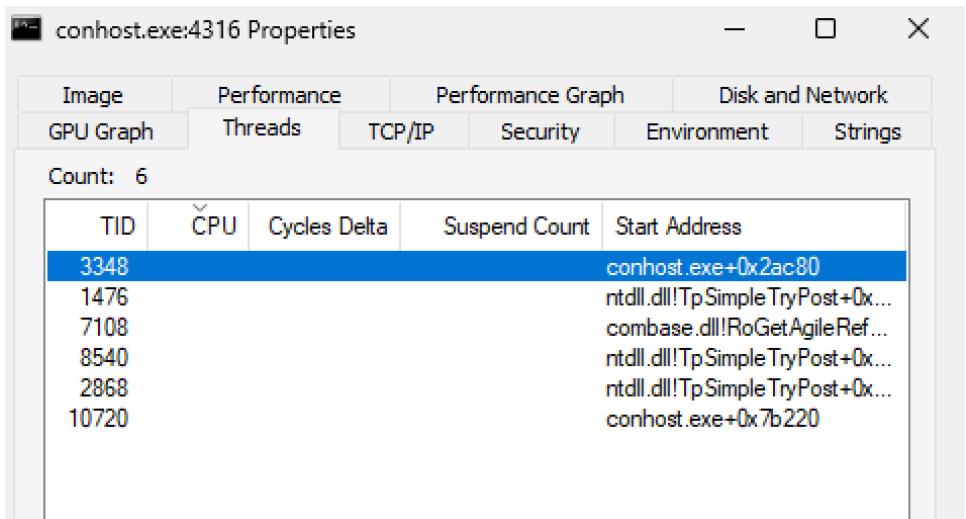
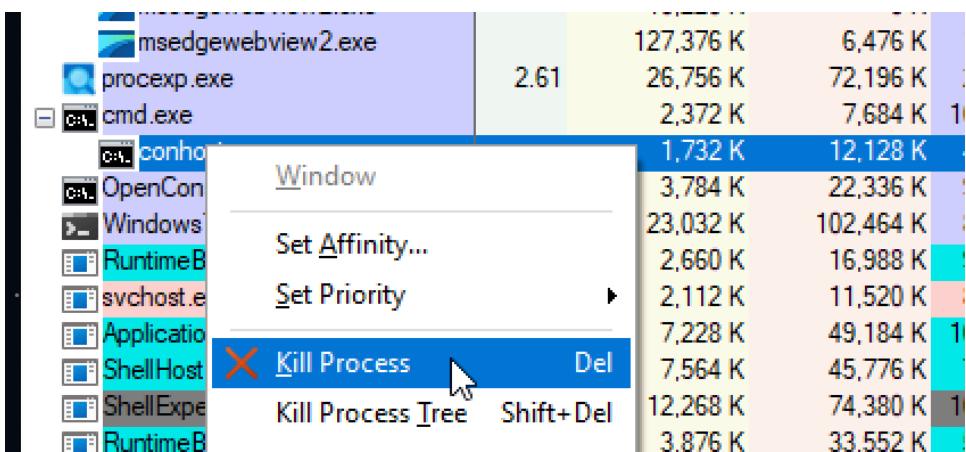




Screenshot of the VirusShare analysis page for the file CONHOST.EXE. The file is identified as "File distributed by Microsoft". Key details shown include:

- Community Score: 0 / 71
- File Hash: eee9c524df8d6835722600433dda759554d76bfaff...
- Type: EXE
- Size: 975.00 KB
- Last Analysis Date: 6 months ago

The interface includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A message encourages joining the community for additional insights and API keys. Below the main details, there's a section for security vendor analysis showing results from Acronis (Undetected) and AhnLab-V3 (Undetected).



Screenshot of the "conhost.exe:4316 Properties" window in Process Hacker.

Performance Tab Data:

TID	CPU	Cycles Delta	Suspend Count	Start Address
3348				conhost.exe+0x2ac80
1476				ntdll.dll!TpSimpleTryPost+0x...
7108				combase.dll!RoGetAgileRef...
8540				ntdll.dll!TpSimpleTryPost+0x...
2868				ntdll.dll!TpSimpleTryPost+0x...
10720				conhost.exe+0x7b220

Process Explorer - Sysinternals: www.sysinternals.com [WIN-SK9FQ1E4S61Johnny] (Administrator)

File Options View Process Find Users Help

Process

- svchost.exe
- svchost.exe
- svchost.exe
- WidgetServ
- FileCoAuth.
- svchost.exe
- msedgeweb
- msedge
- msedge
- msedge
- msedge
- procesp.exe
- Application
- ShellHost.e
- ShellExperi
- RuntimeBro
- audiogd.exe
- msedge.exe
- msedge
- msedge
- msedge.exe
- msedge.exe
- msedge.exe
- msedge.exe
- cmd.exe
- conhost.exe
- OpenConsole.exe

View

- System Information... Ctrl+I
- Show Process Tree Ctrl+T
- Show Column Heatmaps
- Scroll to New Processes
- Show Unnamed Handles and Mappings
- Show Processes From All Users
- Opacity
- Show Lower Pane Ctrl+L
- Lower Pane View**
- Refresh Now F5
- Update Speed
- Organize Column Sets...
- Save Column Set...
- Load Column Set
- Select Columns...

Session	PID	Description
832 K	8124	Host Process for Windows S
116 K	5960	Host Process for Windows S
620 K	10596	Host Process for Windows S
644 K	5816	
848 K	10532	Microsoft OneDrive File Co-A
856 K	9716	Host Process for Windows S
796 K	9480	Microsoft Edge WebView2
316 K	4068	Microsoft Edge WebView2
480 K	9196	Microsoft Edge WebView2
1002 K	10700	Microsoft Edge WebView2
736 K	7156	ShellHost
380 K	10492	Windows Shell Experience Host
216 K	5344	Runtime Broker
788 K	3956	Windows Audio Device Graph Host
280 K	3692	Microsoft Edge
588 K	10628	Microsoft Edge
940 K	5140	Microsoft Edge
14,620 K	44,876	Microsoft Edge
9,256 K	21,424	Microsoft Edge
87,328 K	138,972	Microsoft Edge
17,552 K	36,332	Microsoft Edge
5,380 K	7,160	10140 Windows Command Process
1,800 K	12,108	4316 Console Window Host

Process Explorer - Sysinternals: www.sysinternals.com [WIN-SK9FQ1E4S61Johnny] (Administrator)

File Options View Process Find Users Handle Help

Handles

Type	Name
ALPC Port	\RPC Control\OLE23B3D442489348dff0A899FA821E
Desktop	\Default
Directory	\KnownDls
Directory	\Sessions\2\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	C:\Windows\System32\en-US\Conhost.exe.mui
File	\Device\CNG
File	C:\Windows\Registration\R000000000004.cib
File	\Device\NamedPipe
File	\Device\NamedPipe\
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKCU
Key	HKLM
Key	HKCR\PackagedCom\InterfaceIndex
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
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
Mutant	\Sessions\2\BaseNamedObjects\SM0:4316:304\WlStaging_02
Mutant	\Sessions\2\BaseNamedObjects\SM0:4316:120\WlError_03
Process	<Access is denied.>
Section	\BaseNamedObjects_\ComCatalogCache_
Section	\BaseNamedObjects_\ComCatalogCache_
Semaphore	\Sessions\2\BaseNamedObjects\SM0:4316:304\WlStaging_02_p0h
Semaphore	\Sessions\2\BaseNamedObjects\SM0:4316:304\WlStaging_02_p0h
Semaphore	\Sessions\2\BaseNamedObjects\SM0:4316:120\WlError_03_p0
Semaphore	\Sessions\2\BaseNamedObjects\SM0:4316:120\WlError_03_p0h
Thread	conhost.exe(4316): 10720
Thread	conhost.exe(4316): 3348
Thread	conhost.exe(4316): 3348
WindowStation	\Sessions\2\Windows\WindowStations\WinSta0
WindowStation	\Sessions\2\Windows\WindowStations\WinSta0

CPU Usage: 1.83% Commit Charge: 24.66% Processes: 149 Physical Usage: 35.21%

19°C Preval. nuvol.

Search

ENG IT 2:05 PM 9/22/2025

Analisi dei Thread

(La più piccola unità di esecuzione che un sistema operativo può gestire)

Esplorando la sezione thread di conhost.exe sono stati visualizzati i thread attivi:

- Alcuni con start address interni a conhost.exe → eseguono funzioni native del processo, responsabili delle funzioni interne del programma.
- Altri basati su librerie come ntdll.dll e combase.dll → gestiscono funzionalità del sistema operativo (eseguono codice di librerie di sistema e non codice scritto dal programma in esecuzione).

Analisi degli Handle

Nella vista Handle si è osservato che conhost.exe possiede riferimenti a varie risorse:

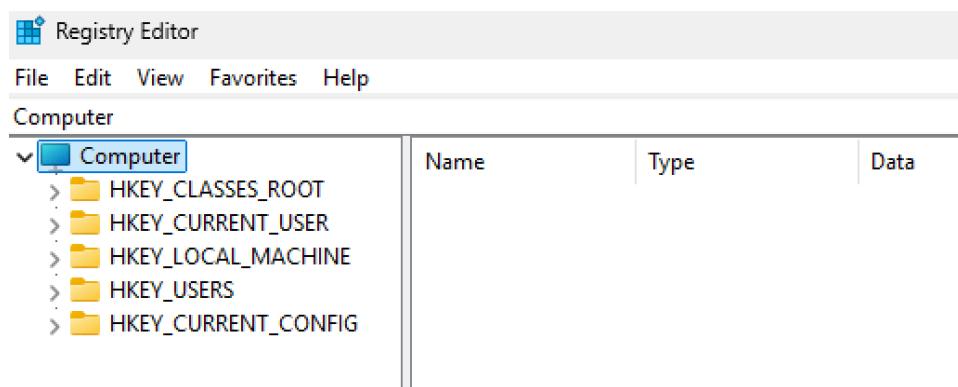
- File system
- Chiavi di registro
- Named Pipe (comunicazione tra servizi di sistema ed applicazioni)
- Mutex e Semaphore (sincronizzazione e gestione ordine dei threads)
- Oggetti grafici (WindowStation, Desktop)

Parte 3 – Esplorazione del Registro di Windows

L'ultima parte ha riguardato il Registro di Windows. In particolare, si è analizzata la chiave:

HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer\EulaAccepted

Il valore di default era 1, che indica che l'utente ha già accettato la licenza d'uso (EULA). Modificando il valore in 0 e riaprendo Process Explorer, il programma ha comunque funzionato, il sistema ha automaticamente riportato il valore della chiave a 1, in quanto l'accettazione della licenza è un requisito indispensabile.



Registry Editor

File Edit View Favorites Help

Computer\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer

Software

Name	Type	Data
DbgHelpPath	REG_SZ	C:\WINDOWS\SYS
DefaultDIIPropP...	REG_DWORD	0x00000000 (0)
DefaultProcProp...	REG_DWORD	0x00000006 (6)
DefaultSysInfoP...	REG_DWORD	0x00000000 (0)
Divider	REG_BINARY	7b 14 ae 47 e1 7a 8
DIIColumnCount	REG_DWORD	0x00000004 (4)
DIIPropWindow...	REG_BINARY	2c 00 00 00 00 00 0
DIISortColumn	REG_DWORD	0x00000000 (0)
DIISortDirection	REG_DWORD	0x00000001 (1)
ETWstandardUs...	REG_DWORD	0x00000000 (0)
EulaAccepted	REG_DWORD	0x00000001 (1)
FindWindowpla...	REG_BINARY	2c 00 00 00 00 00 0
FindWindowpla...	REG_DWORD	0x00000001 (1)

Process Explorer

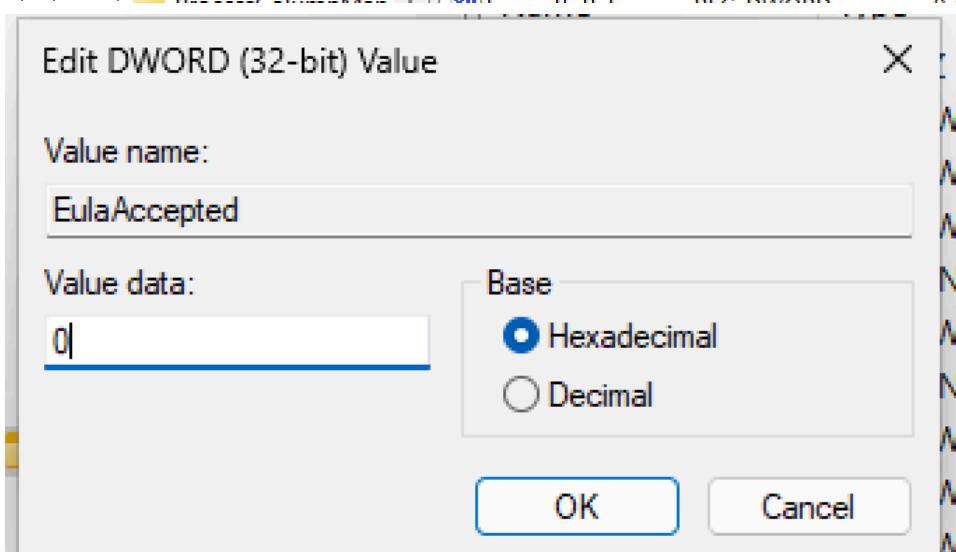
EulaAccepted

Value name: EulaAccepted

Value data: 0

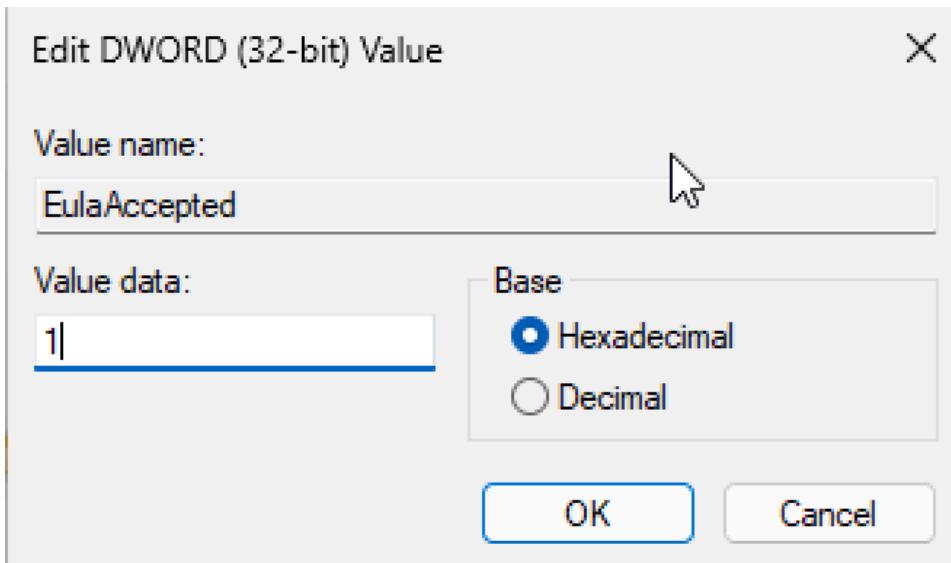
Base: Hexadecimal

OK Cancel



Process Explorer - Sysinternals: www.sysinternals.com [WIN-SK9FQ1E4S61\Johnny] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
vdservice.exe	< 0.01	1,008 K	7,204 K	10024	Spice service	Red Hat Inc.
vdagent.exe	< 0.01	1,856 K	11,312 K	9588	Spice agent	Red Hat Inc.
WmiPrvSE.exe		3,708 K	16,128 K	11076	WMI Provider Host	Microsoft Corporation
svchost.exe		2,296 K	19,984 K	8852	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,140 K	11,812 K	8124	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,260 K	19,108 K	5960	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,308 K	20,592 K	10596	Host Process for Windows S...	Microsoft Corporation
WidgetService.exe		7,048 K	48,040 K	5816		
FileCoAuth.exe		4,868 K	27,804 K	10532	Microsoft OneDrive File Co-A...	Microsoft Corporation
svchost.exe		4,968 K	32,940 K	9716	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		3,316 K	15,480 K	1988	WMI Provider Host	Microsoft Corporation
msedgewebview2.exe		39,716 K	8,632 K	9480	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2,428 K	11,212 K	4068	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		17,752 K	224 K	9196	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		14,672 K	3,120 K	10700	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		10,976 K	624 K	9772	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		106,128 K	3,572 K	1208	Microsoft Edge WebView2	Microsoft Corporation
svchost.exe	< 0.01	10,888 K	32,176 K	8348	Host Process for Windows S...	Microsoft Corporation
msedge.exe	< 0.01	48,216 K	149,412 K	10452	Microsoft Edge	Microsoft Corporation
msedge.exe		2,512 K	11,584 K	7280	Microsoft Edge	Microsoft Corporation
msedge.exe		13,552 K	33,740 K	6172	Microsoft Edge	Microsoft Corporation
msedge.exe		13,632 K	43,728 K	3680	Microsoft Edge	Microsoft Corporation
msedge.exe		9,288 K	21,136 K	3396	Microsoft Edge	Microsoft Corporation
msedge.exe		107,588 K	158,176 K	8984	Microsoft Edge	Microsoft Corporation
msedge.exe		19,880 K	38,480 K	6416	Microsoft Edge	Microsoft Corporation
procexp.exe	1.51	25,216 K	60,496 K	2100	Sysinternals Process Explorer	Sysinternals - www.sysinter...
WmiPrvSE.exe		3,800 K	16,796 K	7856	WMI Provider Host	Microsoft Corporation



Approfondimento: Differenza tra Processi, Thread e Handle

- Processo → contenitore che racchiude codice, dati e risorse necessarie a un programma in esecuzione.
- Thread → unità di esecuzione all'interno di un processo, permette esecuzioni parallele.
- Handle → riferimento univoco a una risorsa (file, chiavi di registro, oggetti grafici, meccanismi di sincronizzazione).

Conclusioni

L'esercizio ha permesso di comprendere meglio come Windows gestisca i processi e le loro relazioni, e come strumenti avanzati come Process Explorer consentano di:

- Analizzare i processi attivi e le risorse utilizzate.
- Verificare la sicurezza dei processi tramite integrazione con VirusTotal.
- Comprendere la gerarchia padre-figlio tra processi.
- Esplorare i thread interni e gli handle collegati a ogni processo.
- Modificare e monitorare impostazioni nel Registro di Windows.

Questa attività fornisce una base importante per l'amministrazione di sistema e l'analisi di sicurezza, mostrando come diagnosticare anomalie e comprendere il funzionamento interno del sistema operativo.