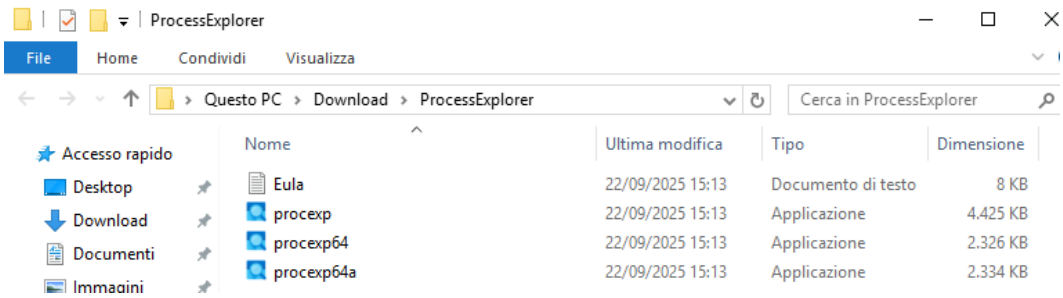
Report Laboratorio - Cisco CyberOps Giorno 1

Questo report documenta in dettaglio i passaggi e i risultati ottenuti durante il laboratorio pratico su Windows, utilizzando Process Explorer (Sysinternals) e l'Editor del Registro di sistema. L'obiettivo è stato comprendere come analizzare i processi, verificare dipendenze e risorse utilizzate, controllare la reputazione con VirusTotal e osservare come i valori nel registro influenzano il comportamento delle applicazioni.

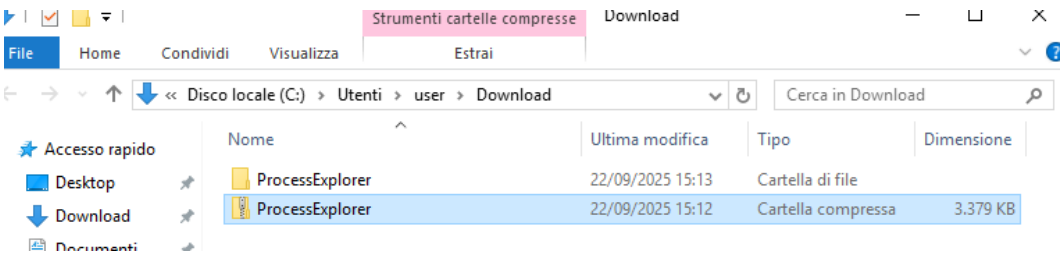
1. Avvio di Process Explorer

Dopo aver scaricato ed estratto la cartella ProcessExplorer.zip, è stato avviato il programma procexp.exe con privilegi amministrativi. La schermata iniziale mostra tutti i processi attivi nel sistema in tempo reale, con informazioni su CPU, memoria utilizzata (Private Bytes, Working Set), PID e società sviluppatrice. Questo permette di avere una panoramica immediata dello stato del sistema.



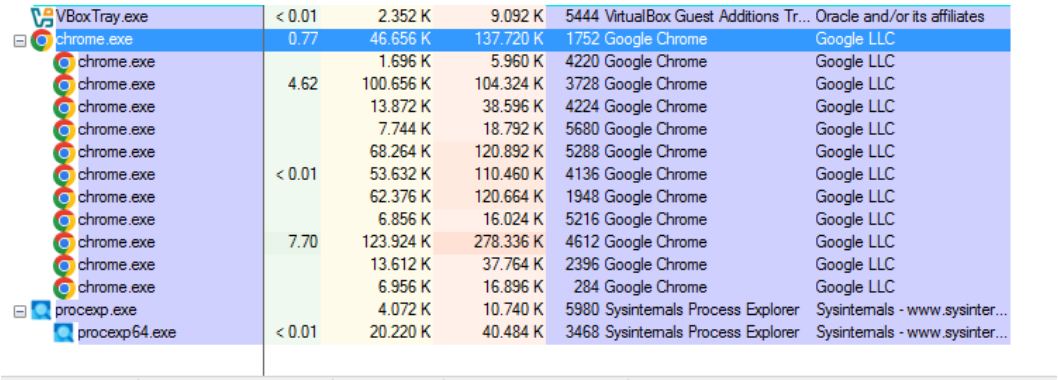
2. Analisi dei processi principali

È stato possibile osservare i processi fondamentali di Windows, come csrss.exe, lsass.exe, winlogon.exe ed explorer.exe. Questi processi sono critici: ad esempio, lsass.exe gestisce la sicurezza e l'autenticazione, mentre explorer.exe è l'interfaccia grafica. Vederli correttamente in esecuzione indica che il sistema funziona normalmente.



3. Analisi Handle e Threads

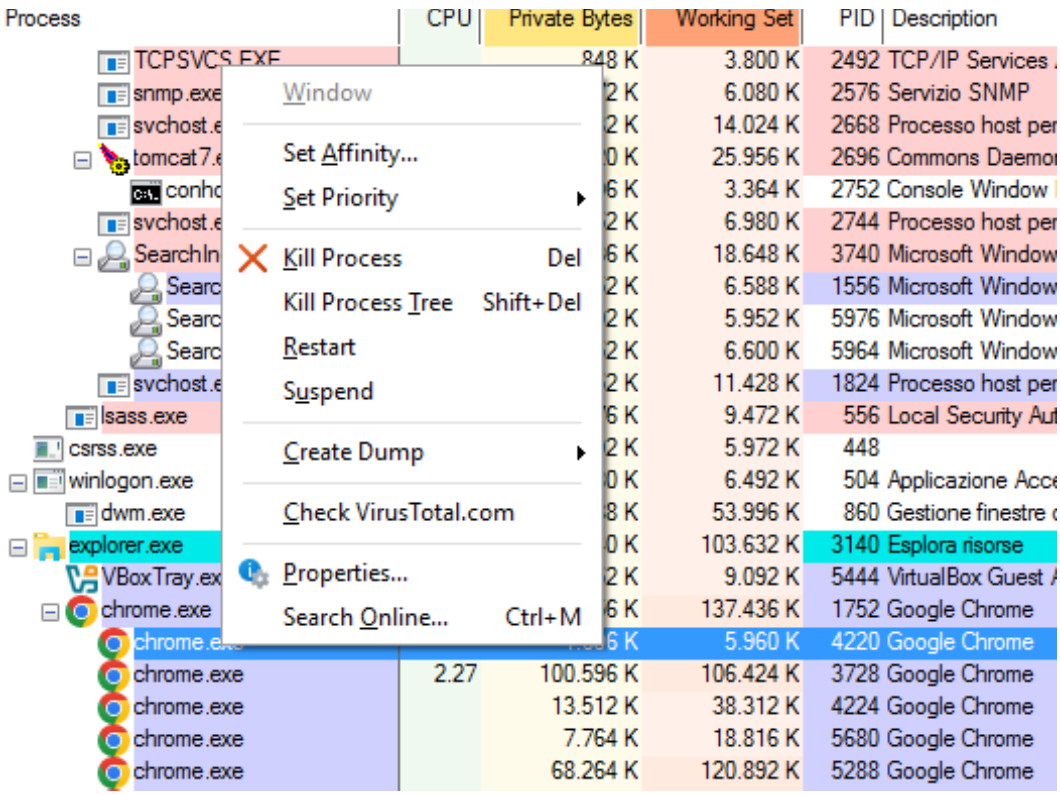
Sono stati analizzati gli Handle aperti del processo conhost.exe. Gli handle rappresentano risorse a cui il processo accede: file, chiavi di registro, mutex, socket. Questa analisi consente di capire con quali componenti del sistema il processo interagisce. Se un malware fosse in esecuzione, potrebbe mantenere handle sospetti verso file nascosti o chiavi anomale.



VBoxTray.exe	< 0.01	2.352 K	9.092 K	5444 VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
chrome.exe	0.77	46.656 K	137.720 K	1752 Google Chrome	Google LLC
chrome.exe		1.696 K	5.960 K	4220 Google Chrome	Google LLC
chrome.exe	4.62	100.656 K	104.324 K	3728 Google Chrome	Google LLC
chrome.exe		13.872 K	38.596 K	4224 Google Chrome	Google LLC
chrome.exe		7.744 K	18.792 K	5680 Google Chrome	Google LLC
chrome.exe		68.264 K	120.892 K	5288 Google Chrome	Google LLC
chrome.exe	< 0.01	53.632 K	110.460 K	4136 Google Chrome	Google LLC
chrome.exe		62.376 K	120.664 K	1948 Google Chrome	Google LLC
chrome.exe		6.856 K	16.024 K	5216 Google Chrome	Google LLC
chrome.exe	7.70	123.924 K	278.336 K	4612 Google Chrome	Google LLC
chrome.exe		13.612 K	37.764 K	2396 Google Chrome	Google LLC
chrome.exe		6.956 K	16.896 K	284 Google Chrome	Google LLC
procexp.exe		4.072 K	10.740 K	5980 Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	< 0.01	20.220 K	40.484 K	3468 Sysinternals Process Explorer	Sysinternals - www.sysinter...

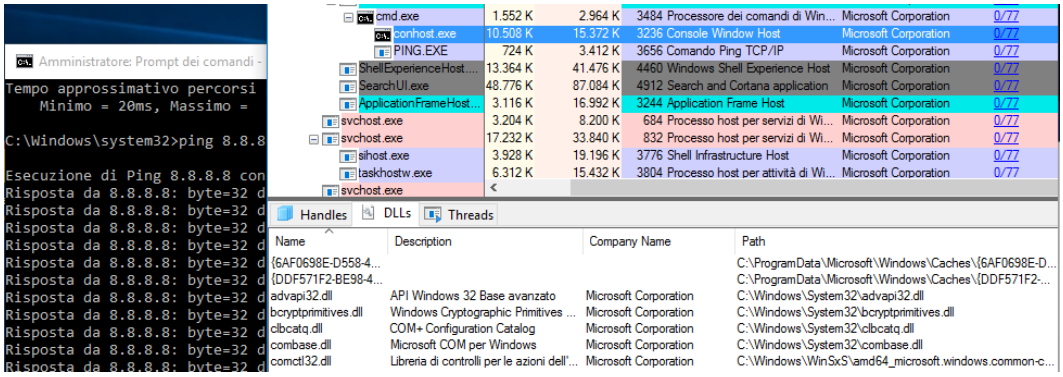
4. Analisi dei processi di Chrome

Avviando Google Chrome, in Process Explorer sono comparsi numerosi processi chrome.exe. Ogni scheda e funzionalità del browser viene gestita da un processo separato. Questo approccio aumenta la stabilità e la sicurezza: se una scheda va in crash, non blocca l'intero browser.



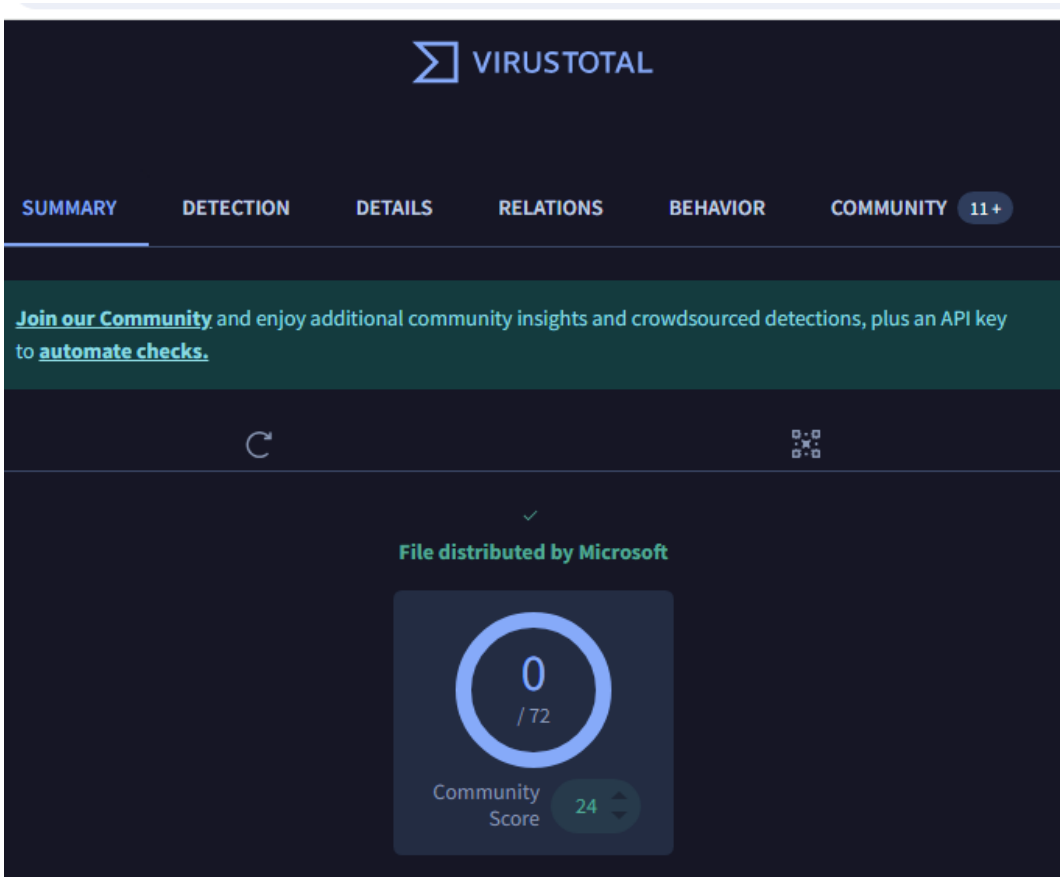
5. Terminazione di un processo

Selezionando explorer.exe e usando la funzione Kill Process, l'interfaccia grafica di Windows viene chiusa. Questo dimostra l'importanza dei processi critici e come l'interruzione forzata di un processo padre possa avere conseguenze evidenti sull'usabilità del sistema.



6. Prompt dei comandi e ping

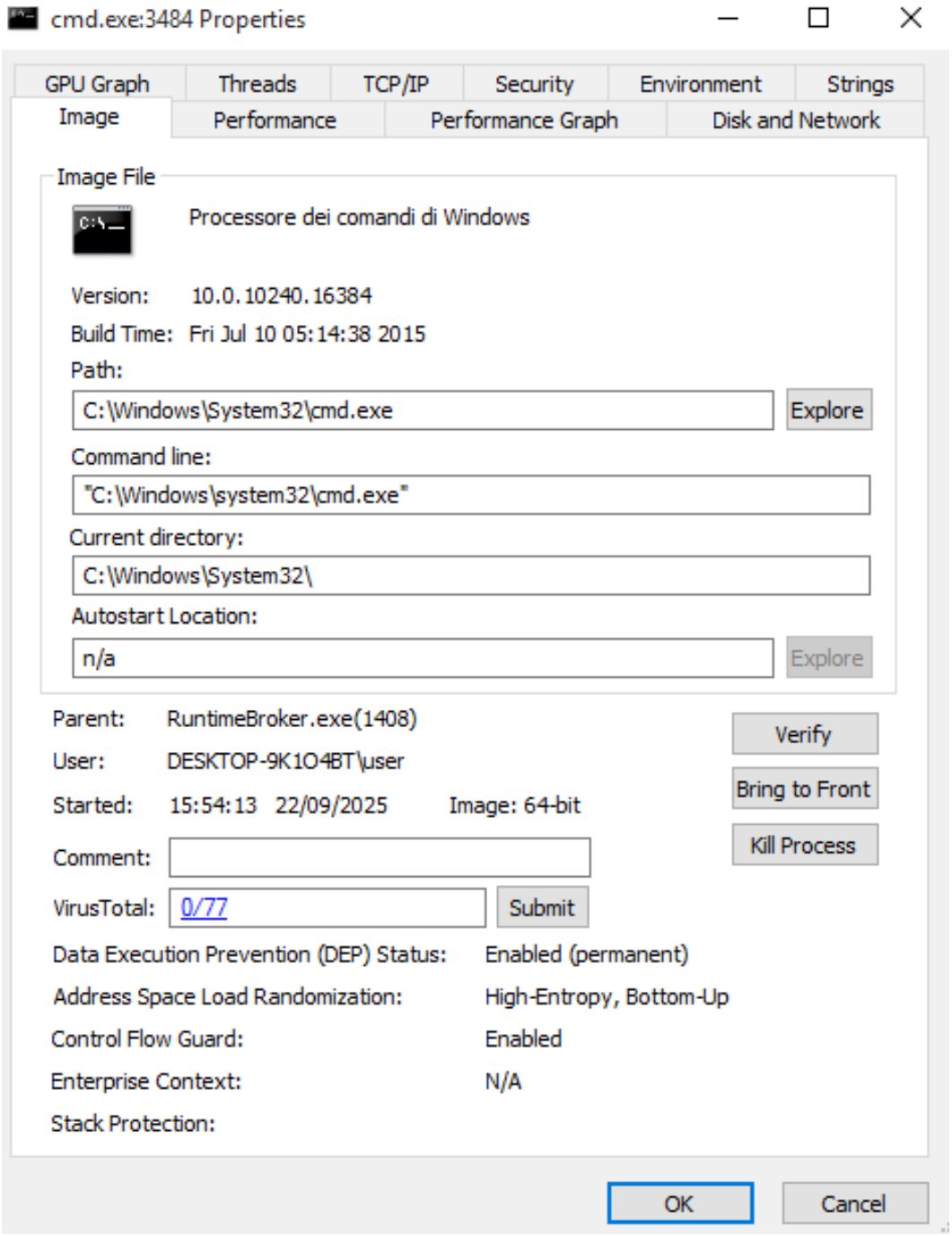
Avviando cmd.exe e lanciando un ping verso 8.8.8.8, in Process Explorer è comparso il processo ping.exe come figlio di cmd.exe. Questo conferma la relazione gerarchica padre-figlio tra processi. Monitorare questa gerarchia è utile in analisi forense: se un programma sospetto genera processi anomali, può essere un segnale di compromissione.



7. Verifica con VirusTotal

Process Explorer permette di verificare i file in esecuzione tramite VirusTotal. Il file analizzato è risultato pulito (0/72), indicando che nessun motore antivirus lo ha classificato

come malevolo. Questa funzione è preziosa per controllare rapidamente la reputazione di un binario senza uscire dall'analisi.



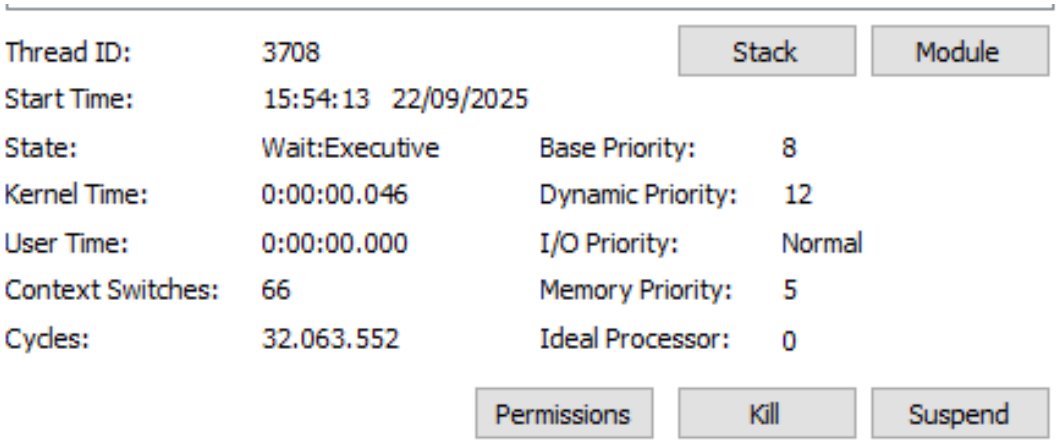
8. Proprietà dettagliate di un processo

Le proprietà di cmd.exe mostrano informazioni sul percorso del file, argomenti di avvio, processo padre, e tecniche di sicurezza attive come Data Execution Prevention (DEP) e Address Space Layout Randomization (ASLR). Il controllo VirusTotal conferma nuovamente la legittimità del file.

Name	Description	Company Name	Path	Virus
advapi32.dll	API Windows 32 Base avanzato	Microsoft Corporation	C:\Windows\System32\advapi32.dll	0/77
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll	0/77
chrome.exe	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe	0/77
chrome_elf.dll	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\126.0.6478.1...	0/79
combase.dll	Microsoft COM per Windows	Microsoft Corporation	C:\Windows\System32\combase.dll	0/77
CrashpadMetrics-ac...			C:\Users\user\AppData\Local\Google\Chrome\User Data\...	0/79
dwmapi.dll	API di Gestione finestre desktop Mi...	Microsoft Corporation	C:\Windows\System32\dwmapi.dll	0/77
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll	0/77
imm32.dll	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	C:\Windows\System32\imm32.dll	0/77
kernel32.dll	DLL client di Windows NT BASE A...	Microsoft Corporation	C:\Windows\System32\kernel32.dll	0/77
KernelBase.dll	DLL client di Windows NT BASE A...	Microsoft Corporation	C:\Windows\System32\KernelBase.dll	0/77
locale.nls			C:\Windows\System32\locale.nls	0/72

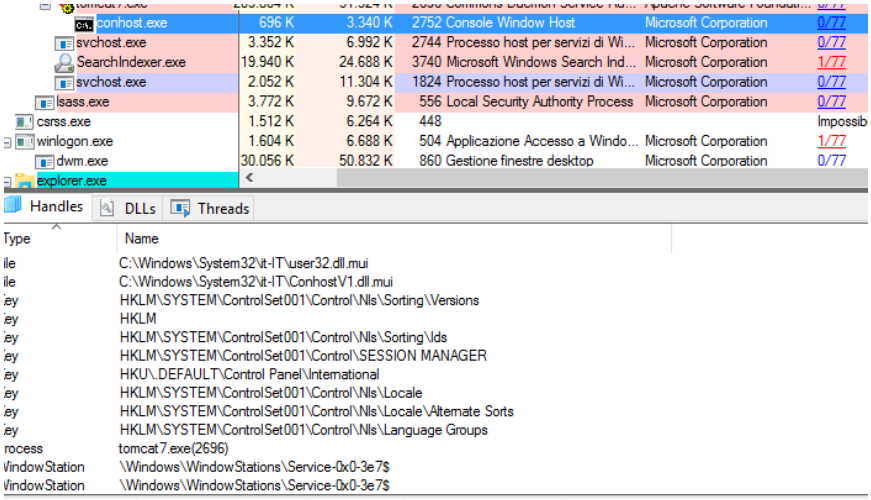
9. Analisi delle DLL caricate

Per un processo selezionato è stata visualizzata la lista delle DLL caricate in memoria. Queste librerie forniscono funzionalità aggiuntive ai processi. Analizzare le DLL è utile per individuare eventuali moduli sospetti o iniettati da malware.



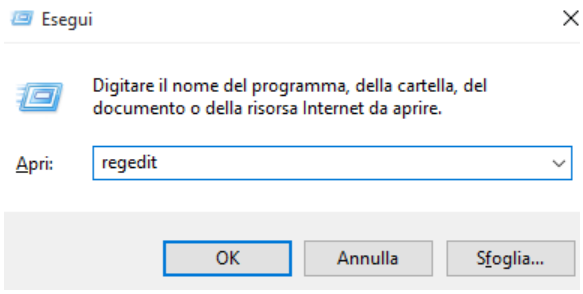
10. Analisi dei Thread

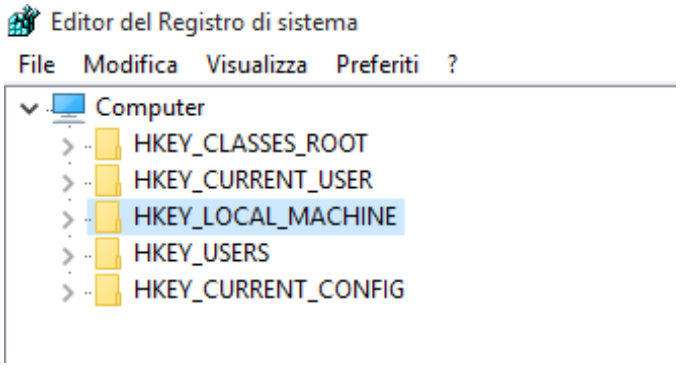
Ogni processo può avere più thread in esecuzione. Nella scheda Threads vengono mostrati ID, stato, priorità e consumo risorse. Queste informazioni aiutano a capire se un processo sta svolgendo attività intensive o anomale.



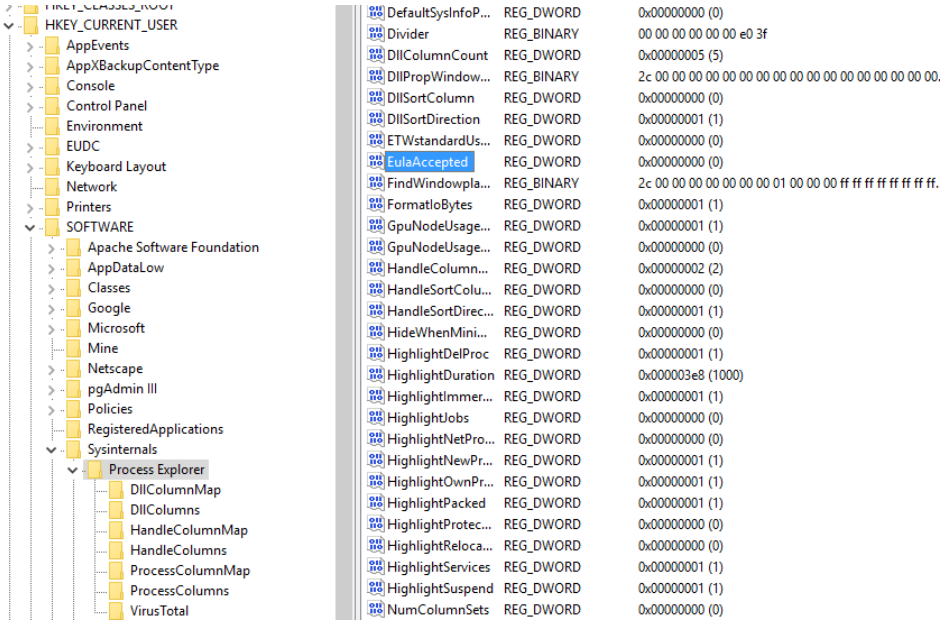
11. Analisi del Registro di sistema

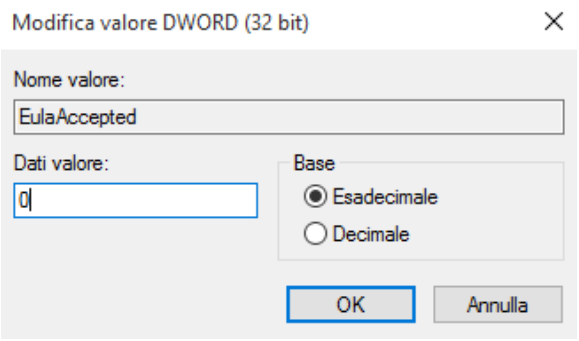
Il laboratorio ha previsto anche l'esplorazione del Registro di sistema, la banca dati di configurazione di Windows. È stato aperto l'editor regedit e individuate le principali hive: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG.





Navigando in HKCU\Software\Sysinternals\Process Explorer, è stato trovato il valore EulaAccepted. Questo valore indica se l'utente ha accettato la licenza del programma. Modificandolo da 1 a 0, al riavvio di Process Explorer compare nuovamente la finestra di accettazione.





Conclusioni

Il laboratorio ha permesso di acquisire competenze pratiche fondamentali per un analista SOC: riconoscere processi legittimi e sospetti, verificare relazioni padre-figlio, analizzare thread e handle, controllare la reputazione dei file con VirusTotal e comprendere il ruolo del Registro di sistema nel comportamento delle applicazioni. Questi strumenti sono essenziali per attività di triage e investigazione forense in ambito Cybersecurity.