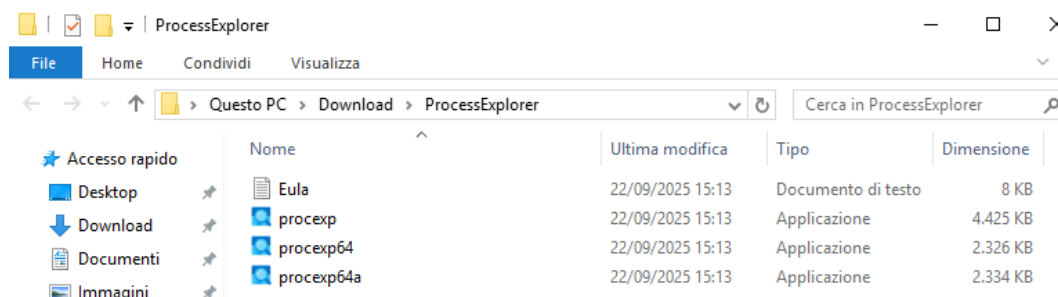


Report Laboratorio - Cisco CyberOps Giorno 1

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.

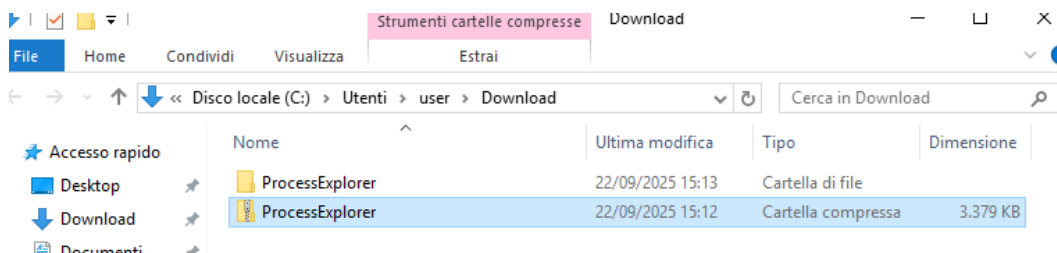
1. Avvio di Process Explorer

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
proccxp.exe		4.072 K	10.740 K	5980 Sysinternals Process Explorer	Sysinternals - www.sysinter...
proccxp64.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.

Process	CPU	Private Bytes	Working Set	PID	Description
TCPVCS.EXE		848 K	3.800 K	2492	TCP/IP Services
snmp.exe		2 K	6.080 K	2576	Servizio SNMP
svchost.e		2 K	14.024 K	2668	Processo host per
tomcat7.e		0 K	25.956 K	2696	Commons Daemon
conho		6 K	3.364 K	2752	Console Window
svchost.e		2 K	6.980 K	2744	Processo host per
SearchIn		6 K	18.648 K	3740	Microsoft Window
Search		2 K	6.588 K	1556	Microsoft Window
Search		2 K	5.952 K	5976	Microsoft Window
Search		2 K	6.600 K	5964	Microsoft Window
svchost.e		2 K	11.428 K	1824	Processo host per
lsass.exe		6 K	9.472 K	556	Local Security Aut
csrss.exe		2 K	5.972 K	448	
winlogon.exe		0 K	6.492 K	504	Applicazione Acco
dwm.exe		8 K	53.996 K	860	Gestione finestre c
explorer.exe		0 K	103.632 K	3140	Esplora risorse
VBoxTray.exe		2 K	9.092 K	5444	VirtualBox Guest /
chrome.exe		6 K	137.436 K	1752	Google Chrome
chrome.exe		6 K	5.960 K	4220	Google Chrome
chrome.exe	2.27	100.596 K	106.424 K	3728	Google Chrome
chrome.exe		13.512 K	38.312 K	4224	Google Chrome
chrome.exe		7.764 K	18.816 K	5680	Google Chrome
chrome.exe		68.264 K	120.892 K	5288	Google Chrome

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.

The screenshot shows a Windows Command Prompt window with the following text:

```

C:\Windows\system32>ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con:
Tempo approssimativo percorsi
Minimo = 20ms, Massimo =
Risposta da 8.8.8.8: byte=32 d
Risposta da 8.8.8.8: byte=32 d
Risposta da 8.8.8.8: byte=32 d
Risposta da 8.8.8.8: byte=32 d
Risposta da 8.8.8.8: byte=32 d
Risposta da 8.8.8.8: byte=32 d
Risposta da 8.8.8.8: byte=32 d
Risposta da 8.8.8.8: byte=32 d
Risposta da 8.8.8.8: byte=32 d
Risposta da 8.8.8.8: byte=32 d

```

Overlaid on the Command Prompt is the Windows Task Manager window, showing the 'Processes' tab. The 'PING EXE' process is highlighted in blue. Below it, the 'Handles' tab is selected, showing a list of loaded DLLs:

Name	Description	Company Name	Path
{6AF0698E-D558-4...			C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-D...
{DDF571F2-BE98-4...			C:\ProgramData\Microsoft\Windows\Caches\{DDF571F2-...
advapi32.dll	API Windows 32 Base avanzato	Microsoft Corporation	C:\Windows\System32\advapi32.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll
combase.dll	Microsoft COM per Windows	Microsoft Corporation	C:\Windows\System32\combase.dll
comctl32.dll	Libreria di controlli per le azioni dell'...	Microsoft Corporation	C:\Windows\WinSxS\amd64_microsoft.windows.common-c...

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.

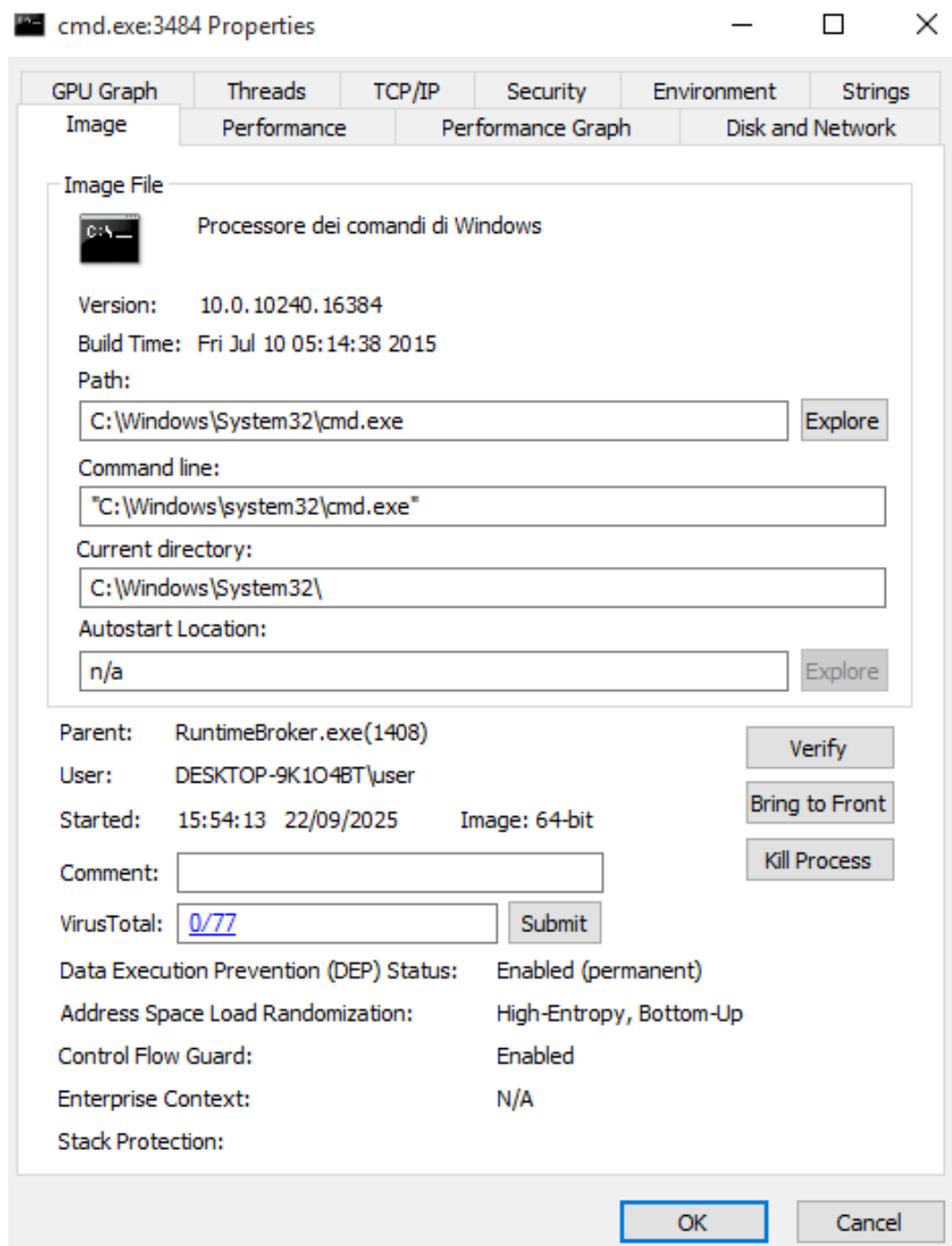
The screenshot shows the VirusTotal web interface. The top navigation bar includes links for SUMMARY, DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (11+). Below the navigation bar, there is a green banner that reads: "Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks."

The main content area shows a file analysis result. At the top, it says "File distributed by Microsoft" with a green checkmark. Below this, there is a large circular progress indicator showing "0 / 72". At the bottom, it displays the "Community Score" as "24".

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
cryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\cryptprimitives.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.

Thread ID:	3708	Stack	Module
Start Time:	15:54:13 22/09/2025		
State:	Wait:Executive	Base Priority:	8
Kernel Time:	0:00:00.046	Dynamic Priority:	12
User Time:	0:00:00.000	I/O Priority:	Normal
Context Switches:	66	Memory Priority:	5
Cycles:	32.063.552	Ideal Processor:	0
		Permissions	Kill Suspend

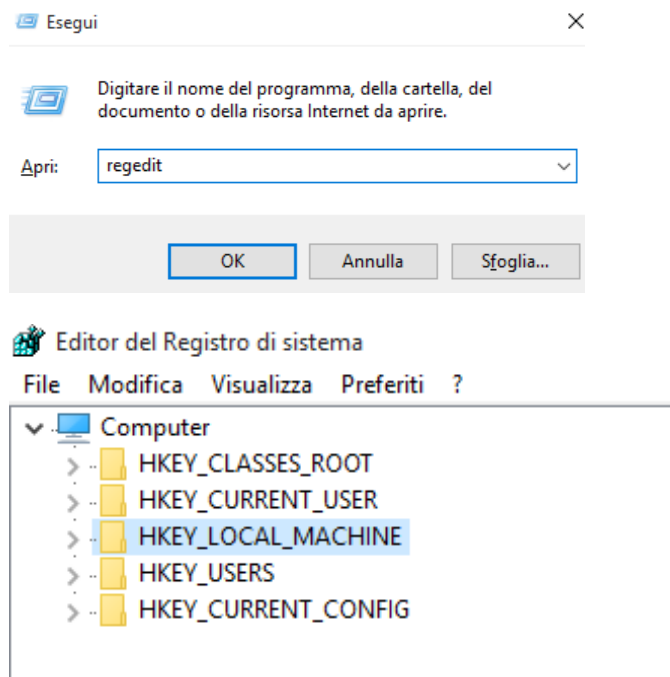
10. Analisi dei Thread

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.

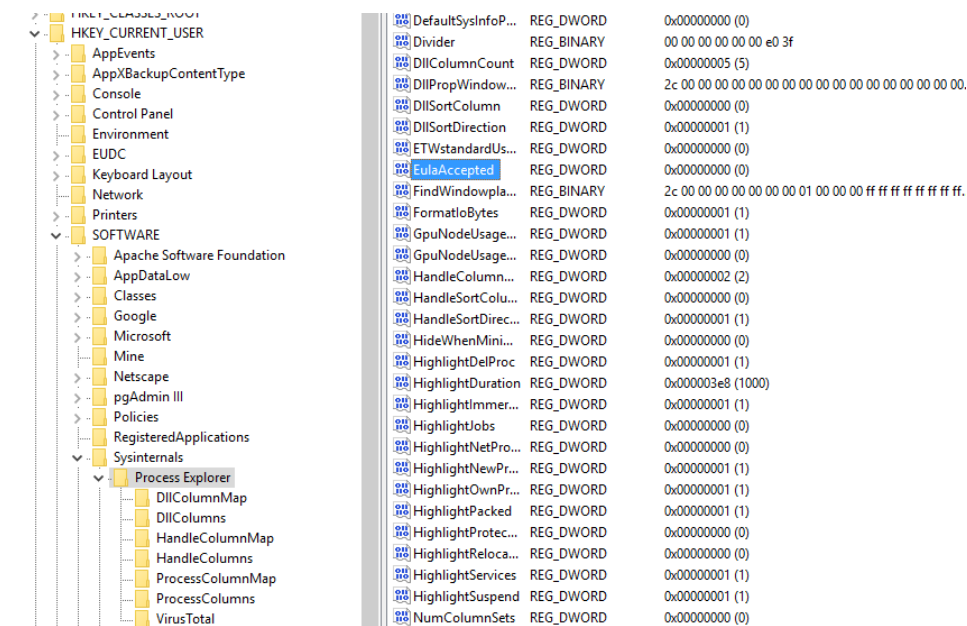
Type	Name
file	C:\Windows\System32\it-IT\user32.dll.mui
file	C:\Windows\System32\it-IT\ConhostV1.dll.mui
key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
key	HKLM
key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
key	HKLM\SYSTEM\ControlSet001\Control\SESSION MANAGER
key	HKU\DEFAULT\Control Panel\International
key	HKLM\SYSTEM\ControlSet001\Control\Nls\Locale
key	HKLM\SYSTEM\ControlSet001\Control\Nls\Locale\Alternate Sorts
key	HKLM\SYSTEM\ControlSet001\Control\Nls\Language Groups
process	tomcat7.exe(2696)
WindowStation	\Windows\WindowStations\Service-0x0-3e75
WindowStation	\Windows\WindowStations\Service-0x0-3e75

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.



Modifica valore DWORD (32 bit) ✕

Nome valore:
EulaAccepted

Dati valore:
0

Base
☒ Esadecimale
☐ Decimale

OK Annulla

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.