Zurigo 10.12.2024

Laboratorio:
Cyber Security & Ethical Hacking Cisco CyberOps
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.

Il laboratorio si è concentrato sull'esplorazione di concetti fondamentali della sicurezza informatica: processi, thread, handle e il registro di Windows. Utilizzando Process Explorer, un potente strumento della suite Sysinternals, abbiamo approfondito il funzionamento interno del sistema operativo, acquisendo conoscenze essenziali per la comprensione e l'analisi di potenziali minacce.

Obiettivi

- **Esplorazione di Processi, Thread e Handle:** Abbiamo utilizzato Process Explorer per visualizzare e analizzare i processi in esecuzione, i loro thread associati e gli handle utilizzati per accedere alle risorse di sistema.
- **Modifica di un'impostazione tramite il Registro di Windows:** Abbiamo modificato un valore nel registro di Windows per osservare l'impatto sulla configurazione del sistema.

Procedimento

1. Process Explorer:

- **Avvio e Interfaccia:** Abbiamo avviato Process Explorer e familiarizzato con la sua interfaccia, identificando le colonne principali (nome processo, PID, CPU, memoria, descrizione, ecc.).
- **Analisi dei Processi:** Abbiamo esaminato i processi in esecuzione, filtrando per nome, PID o altri criteri. Abbiamo osservato lo stato dei processi (in esecuzione, in pausa, terminato), la loro gerarchia e le risorse consumate.
- **Thread:** Abbiamo analizzato i thread associati a ciascun processo, identificando il thread principale e i thread secondari. Abbiamo osservato come i thread condividono le risorse del processo.
- **Handle:** Abbiamo esaminato gli handle utilizzati dai processi per accedere a risorse come file, registri, porte di rete, ecc. Abbiamo compreso l'importanza degli handle nella sicurezza informatica.

2. Registro di Windows:

- **Navigazione:** Abbiamo utilizzato l'Editor del Registro di sistema per navigare tra le chiavi e i valori.

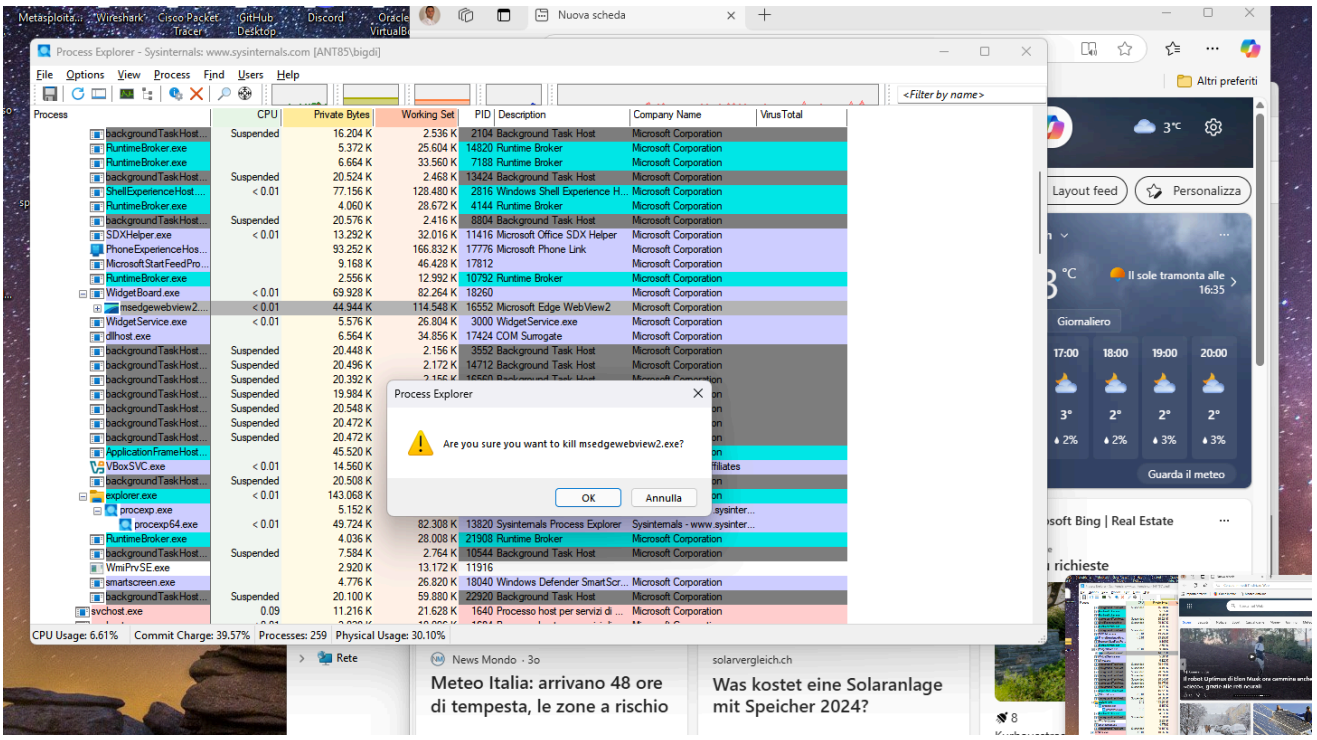
- **Modifica di un'impostazione:** Abbiamo identificato la chiave del registro relativa all'impostazione che volevamo modificare e abbiamo modificato il valore corrispondente.
- **Osservazione degli effetti:** Abbiamo riavviato il sistema o l'applicazione interessata per osservare gli effetti della modifica apportata al registro.

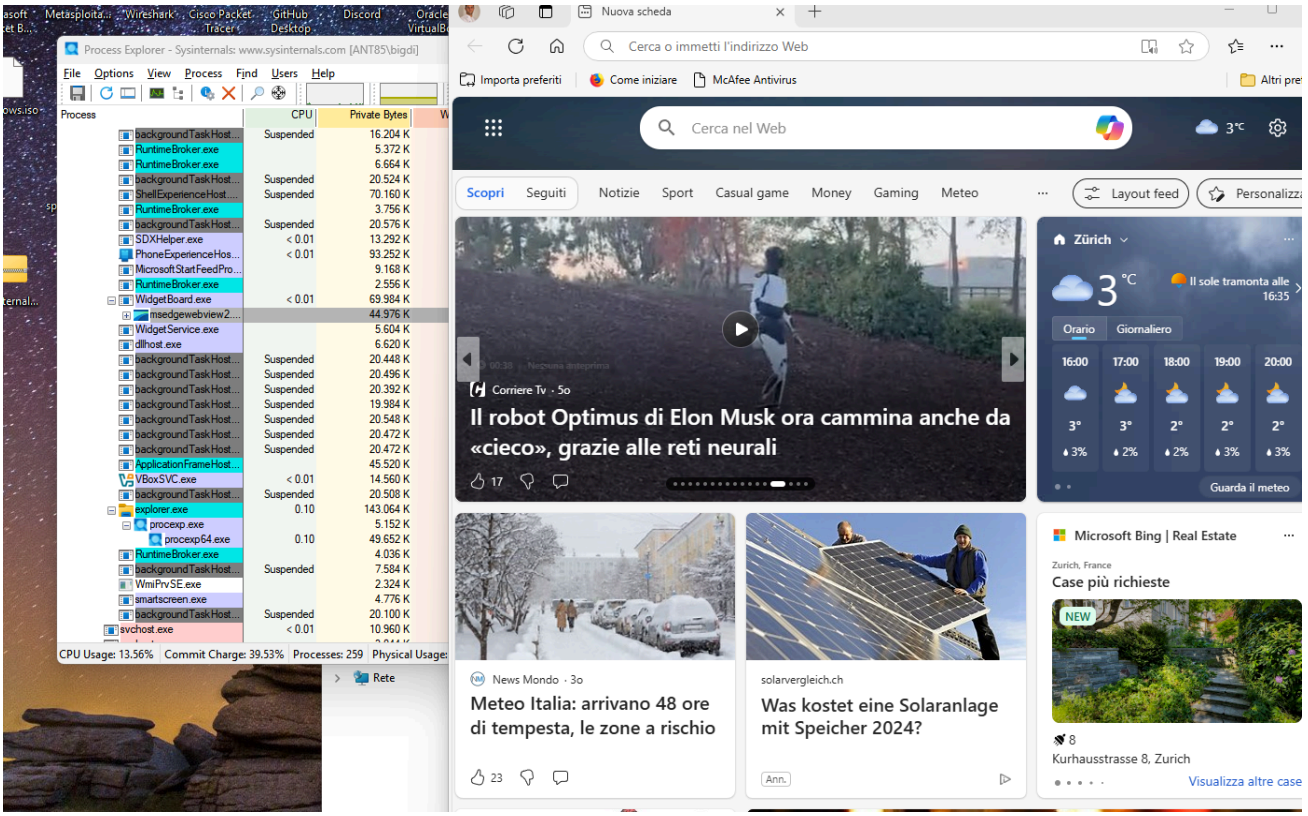
Risultati

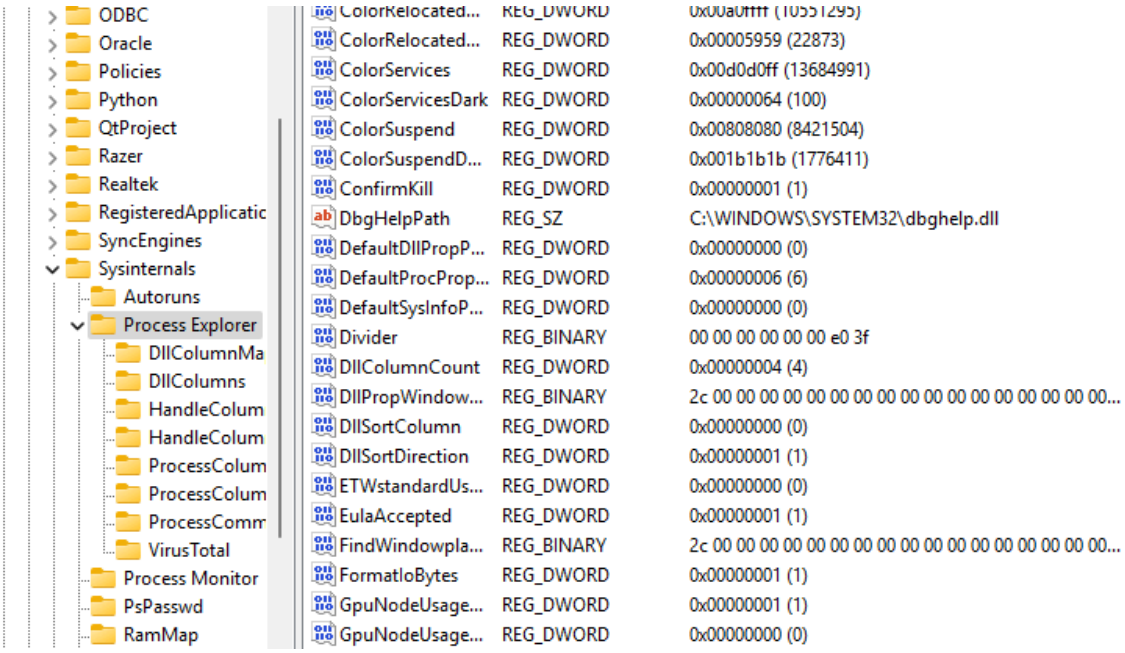
- **Processi:** Abbiamo acquisito una comprensione approfondita di come i processi vengono gestiti dal sistema operativo e di come interagiscono tra loro.
- **Thread:** Abbiamo compreso il ruolo dei thread nell'esecuzione concorrente di attività all'interno di un processo.
- **Handle:** Abbiamo compreso l'importanza degli handle nella sicurezza informatica e come possono essere utilizzati dagli attacchi per ottenere privilegi elevati.
- **Registro di Windows:** Abbiamo imparato a navigare nel registro di Windows e a modificare le impostazioni di sistema.

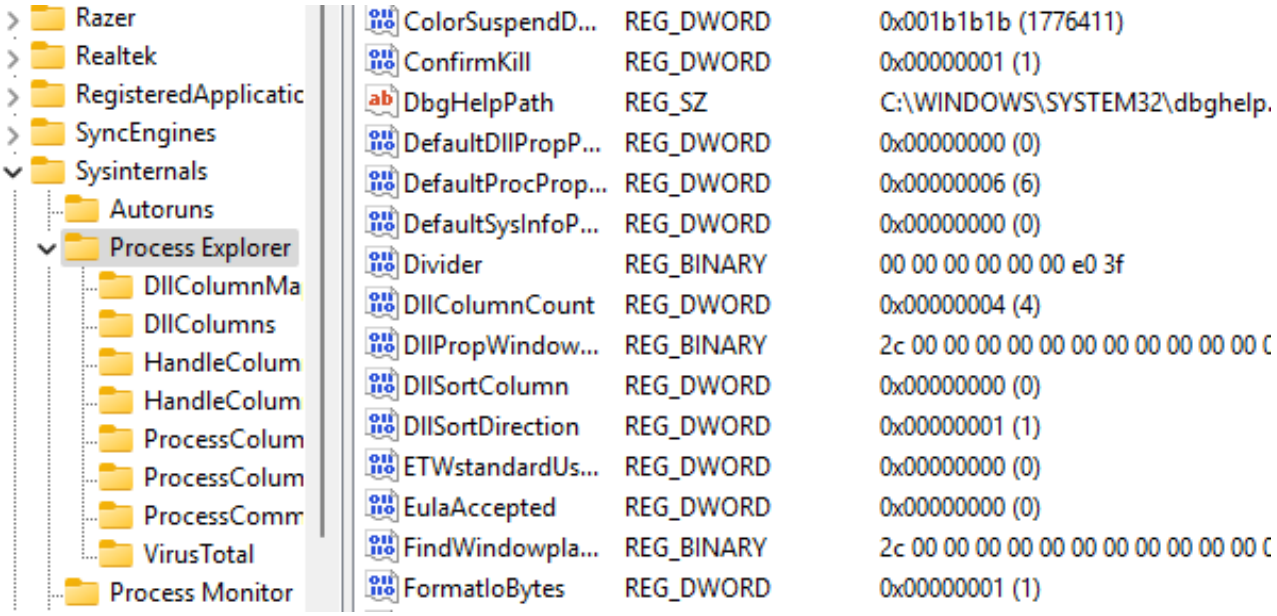
Conclusioni

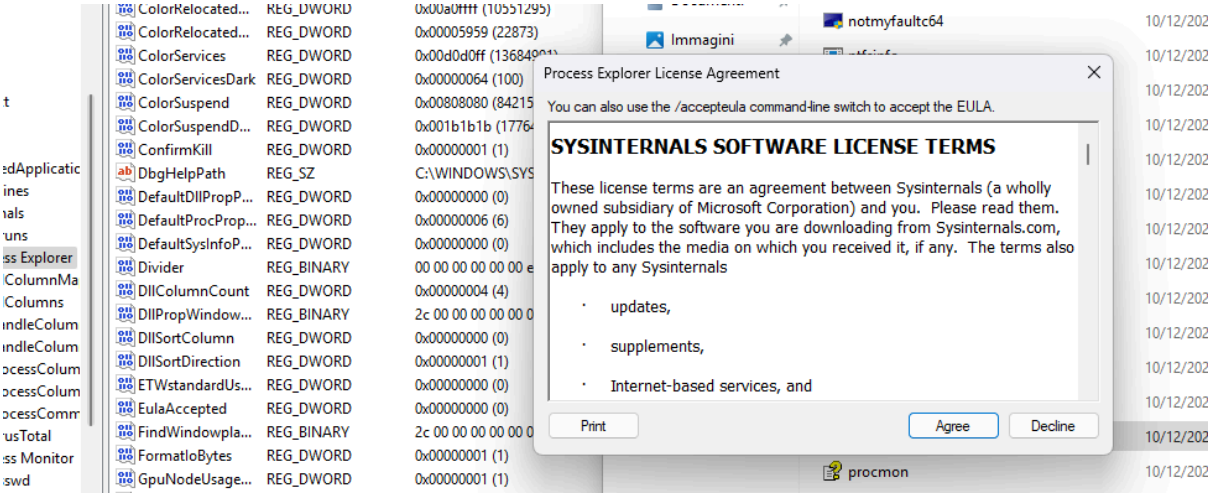
Questo laboratorio ci ha fornito una solida base per comprendere i meccanismi fondamentali del sistema operativo e le loro implicazioni in termini di sicurezza informatica. Le conoscenze acquisite sono essenziali per un analista della sicurezza per identificare e mitigare le minacce che sfruttano vulnerabilità a livello di sistema operativo.

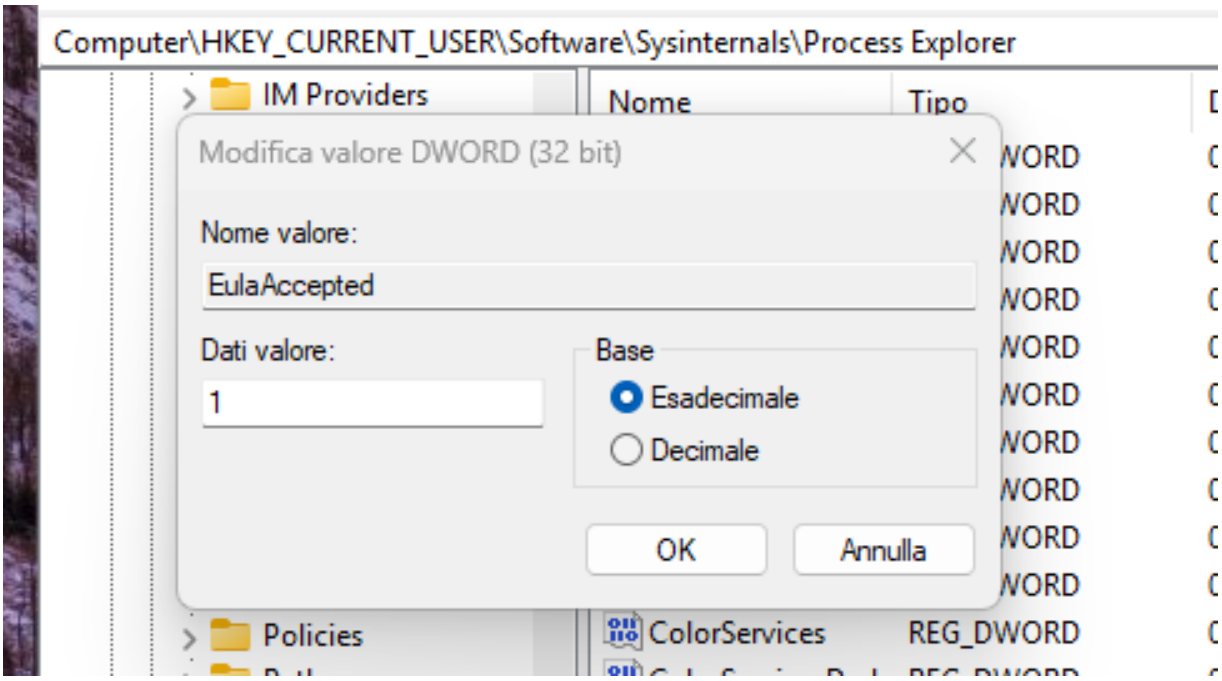

Process Explorer - Sysinternals: www.sysinternals.com [ANT85\bigdi]
Process Explorer
Are you sure you want to kill msedgewebview2.exe?
OK
Annulla
Nuova scheda
Altri preferiti
Layout feed
Personalizza
Il sole tramonta alle 16:35
Giornaliero
Guarda il meteo
News Mondo · 3o
Meteo Italia: arrivano 48 ore di tempesta, le zone a rischio
solarvergleich.ch
Was kostet eine Solaranlage mit Speicher 2024?


Process Explorer - Sysinternals: www.sysinternals.com [ANT85\bigdi]
Nuova scheda
Cerca o immetti l'indirizzo Web
Cerca nel Web
Scopri
Seguiti
Notizie
Sport
Casual game
Money
Gaming
Meteo
Layout feed
Personalizza
Corriere Tv · 5o
Il robot Optimus di Elon Musk ora cammina anche da «cieco», grazie alle reti neurali
Zürich
Il sole tramonta alle 16:35
Orario
Giornaliero
Guarda il meteo
News Mondo · 3o
Meteo Italia: arrivano 48 ore di tempesta, le zone a rischio
solarvergleich.ch
Was kostet eine Solaranlage mit Speicher 2024?
Microsoft Bing | Real Estate
Case più richieste
Kurhausstrasse 8, Zurich
Visualizza altre case


ODBC
Oracle
Policies
Python
QtProject
Razer
Realtek
RegisteredApplicatic
SyncEngines
Sysinternals
Autoruns
Process Explorer
DllColumnMa
DllColumns
HandleColum
HandleColum
ProcessColum
ProcessColum
ProcessComm
VirusTotal
Process Monitor
PsPasswd
RamMap
ColorRelocated... REG_DWORD 0x00a0ffff (10551295)
ColorRelocated... REG_DWORD 0x00005959 (22873)
ColorServices REG_DWORD 0x00d0d0ff (13684991)
ColorServicesDark REG_DWORD 0x00000064 (100)
ColorSuspend REG_DWORD 0x00808080 (8421504)
ColorSuspendD... REG_DWORD 0x001b1b1b (1776411)
ConfirmKill REG_DWORD 0x00000001 (1)
DbgHelpPath REG_SZ C:\WINDOWS\SYSTEM32\dbghelp.dll
DefaultDllPropP... REG_DWORD 0x00000000 (0)
DefaultProcProp... REG_DWORD 0x00000006 (6)
DefaultSysInfoP... REG_DWORD 0x00000000 (0)
Divider REG_BINARY 00 00 00 00 00 00 e0 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 00...
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 00 00 00 00 00 00 00 00 00 00 00...
FormatIoBytes REG_DWORD 0x00000001 (1)
GpuNodeUsage... REG_DWORD 0x00000001 (1)
GpuNodeUsage... REG_DWORD 0x00000000 (0)


Razer
Realtek
RegisteredApplicatic
SyncEngines
Sysinternals
Autoruns
Process Explorer
DllColumnMa
DllColumns
HandleColum
HandleColum
ProcessColum
ProcessColum
ProcessComm
VirusTotal
Process Monitor
ColorSuspendD... REG_DWORD 0x001b1b1b (1776411)
ConfirmKill REG_DWORD 0x00000001 (1)
DbgHelpPath REG_SZ C:\WINDOWS\SYSTEM32\dbghelp.
DefaultDllPropP... REG_DWORD 0x00000000 (0)
DefaultProcProp... REG_DWORD 0x00000006 (6)
DefaultSysInfoP... REG_DWORD 0x00000000 (0)
Divider REG_BINARY 00 00 00 00 00 00 e0 3f
DllColumnCount REG_DWORD 0x00000004 (4)
DllPropWindow... REG_BINARY 2c 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 0x00000000 (0)
FindWindowpla... REG_BINARY 2c 00 00 00 00 00 00 00 00 00 00 00 0
FormatIoBytes REG_DWORD 0x00000001 (1)


ColorRelocated... REG_DWORD 0x00a0ffff (10551295)
ColorRelocated... REG_DWORD 0x00005959 (22873)
ColorServices REG_DWORD 0x00d0d0ff (13684991)
ColorServicesDark REG_DWORD 0x00000064 (100)
ColorSuspend REG_DWORD 0x00808080 (8421504)
ColorSuspendD... REG_DWORD 0x001b1b1b (1776411)
ConfirmKill REG_DWORD 0x00000001 (1)
DbgHelpPath REG_SZ C:\WINDOWS\SYS
DefaultDllPropP... REG_DWORD 0x00000000 (0)
DefaultProcProp... REG_DWORD 0x00000006 (6)
DefaultSysInfoP... REG_DWORD 0x00000000 (0)
Divider REG_BINARY 00 00 00 00 00 00 e
DllColumnCount REG_DWORD 0x00000004 (4)
DllPropWindow... REG_BINARY 2c 00 00 00 00 00 0
DllSortColumn REG_DWORD 0x00000000 (0)
DllSortDirection REG_DWORD 0x00000001 (1)
ETWstandardUs... REG_DWORD 0x00000000 (0)
EulaAccepted REG_DWORD 0x00000000 (0)
FindWindowpla... REG_BINARY 2c 00 00 00 00 00 0
FormatIoBytes REG_DWORD 0x00000001 (1)
GpuNodeUsage... REG_DWORD 0x00000001 (1)
Immagini
notmyfaultc64
procmon
10/12/202
Process Explorer License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
updates,
supplements,
Internet-based services, and
Print
Agree
Decline


Computer\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer
IM Providers
Nome
Tipo
Modifica valore DWORD (32 bit)
Nome valore:
EulaAccepted
Dati valore:
1
Base
Esadecimale
Decimale
OK
Annulla
Policies
ColorServices
REG_DWORD