Windows SysInternals Suite

Introduzione

La gestione e l’analisi dei processi e delle risorse di sistema sono fondamentali per il monitoraggio, la sicurezza e il debugging di un sistema operativo. In questo contesto, la **Windows SysInternals Suite** si rivela uno strumento indispensabile, offrendo funzionalità avanzate per il controllo dei processi, la verifica delle minacce e l’analisi delle risorse. Questa relazione illustra un'esplorazione dettagliata di SysInternals Suite, focalizzandosi su **Process Explorer**, uno strumento per il monitoraggio dei processi, e su altre funzionalità correlate come l’analisi di thread, handle e registro di sistema.

L’obiettivo principale è stato acquisire competenze pratiche nella gestione avanzata del sistema operativo Windows, approfondendo il funzionamento interno di processi e risorse.

Introduzione alla suite SysInternals e gestione dei processi

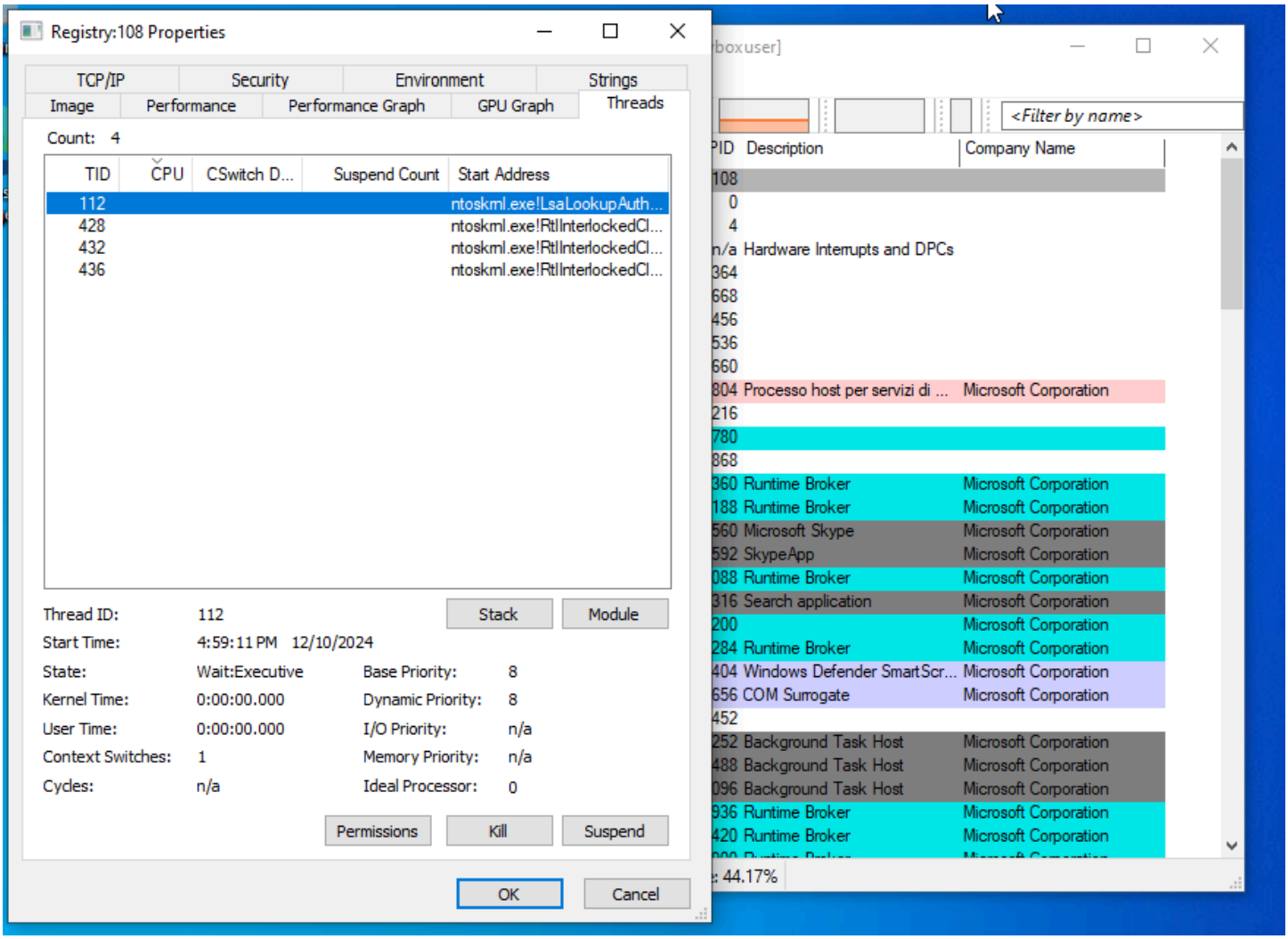
Obiettivo: Familiarizzare con la gestione dei processi attivi tramite Process Explorer.

Passaggio 1: Download e configurazione

- Abbiamo scaricato e configurato la **SysInternals Suite**, una raccolta di strumenti progettati per monitorare, analizzare e gestire processi e risorse di sistema. L'apertura di **Process Explorer (procexp.exe)** ci consente di analizzare in dettaglio i processi attivi.

Fase 2: Esplorazione di un processo attivo

1. **Avvio di Process Explorer**:
   - Process Explorer elenca i processi attivi, organizzati in una struttura gerarchica che mostra la relazione tra processi padre e figli. Questo ci permette di comprendere come i processi interagiscono tra loro.
2. **Individuazione e terminazione di un processo**:
   - Con l’icona "Trova processo", abbiamo individuato il processo del browser web (ad esempio Microsoft Edge) direttamente dalla finestra del browser.
   - Terminando il processo tramite "Kill Process", abbiamo osservato che la finestra del browser si è chiusa immediatamente, confermando che il processo è strettamente collegato all'interfaccia visibile.



Passaggio 3: Avvio e analisi di un nuovo processo

1. **Monitoraggio dei processi padre e figlio**:
   - Avviando un Prompt dei comandi (cmd.exe), abbiamo osservato i processi correlati:
     - **explorer.exe** (processo padre).
     - **cmd.exe** (processo attivo).
     - **conhost.exe** (processo figlio).
   - Durante un comando **ping**, è stato generato un ulteriore processo figlio, **ping.exe**, evidenziando la gerarchia e l'interazione dinamica tra processi.
2. **Verifica di sicurezza con VirusTotal**:
   - Il processo **conhost.exe** è stato verificato con **VirusTotal** per esaminare potenziali minacce, dimostrando come Process Explorer integri strumenti di sicurezza.
3. **Dipendenza dei processi figli dai processi padre**:
   - Quando abbiamo terminato il processo cmd.exe, anche conhost.exe si è interrotto. Questo ci ha mostrato che i processi figli non possono esistere senza il processo genitore.

Esplorazione di thread e handle

Obiettivo: Analizzare gli elementi interni dei processi, come thread e handle.

Fase 1: Esame dei thread

- Un **thread** è l'unità base di esecuzione all'interno di un processo. Ogni processo può avere uno o più thread attivi.
- Tramite la finestra **Proprietà**di conhost.exe in Process Explorer, abbiamo osservato:
  - Informazioni su variabili ambientali, dati di sicurezza e prestazioni.
  - Dettagli tecnici relativi ai thread attivi.

Fase 2: Esame degli handle

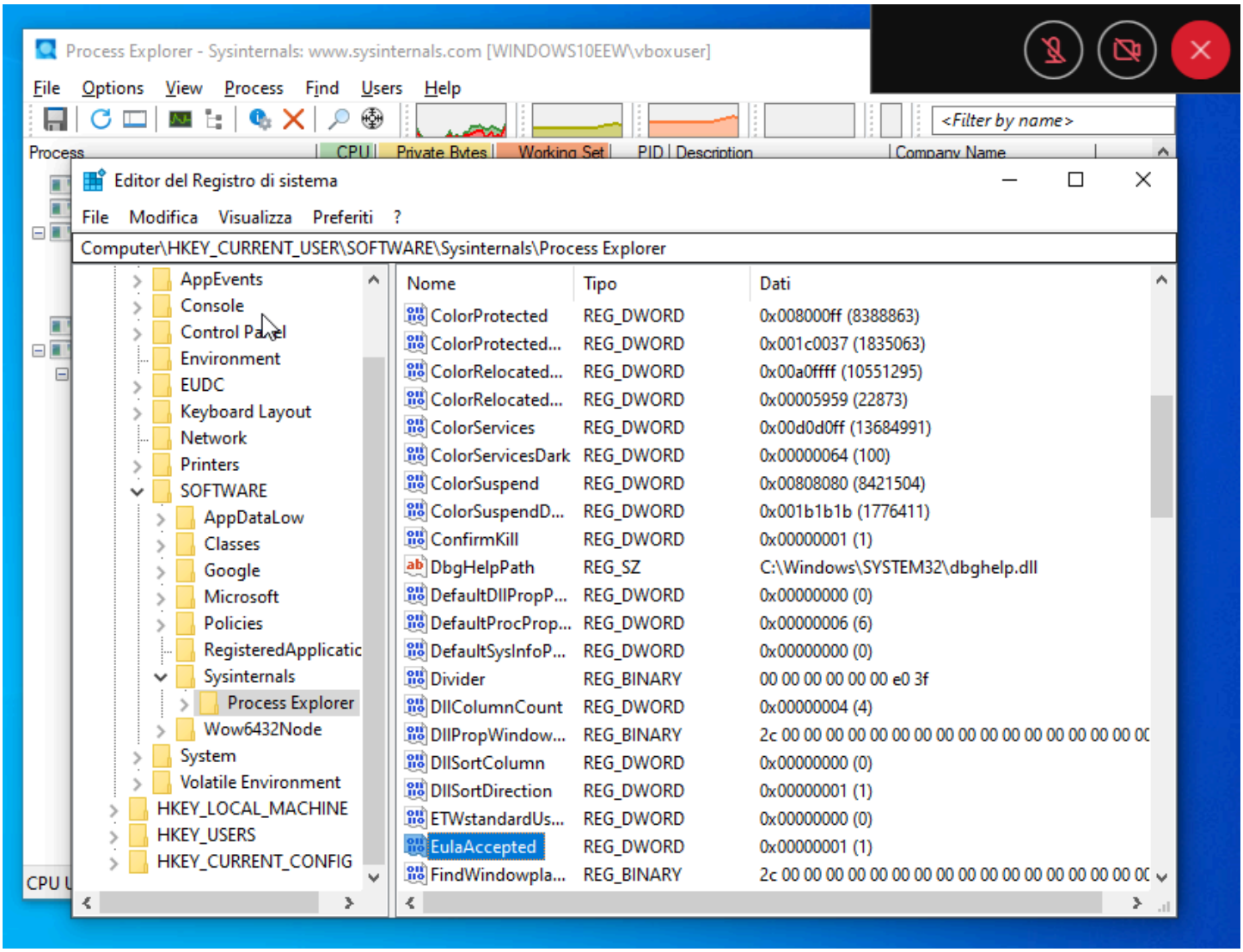
- Gli **handle** sono riferimenti utilizzati dai processi per accedere a risorse di sistema come file, chiavi di registro e oggetti.
- Attivando la visualizzazione degli handle, abbiamo osservato che essi puntano a risorse come:
  - File aperti.
  - Chiavi di registro specifiche.
  - Thread associati al processo.

Esplorazione del registro di sistema

Obiettivo: Comprendere la struttura del registro di sistema e modificare una chiave per osservare i risultati.

Esplorazione del registro di Windows

1. Il **registro di sistema** è un database che memorizza le impostazioni di configurazione del sistema operativo e delle applicazioni. È organizzato in cinque hive principali:
   - **HKEY_CLASSES_ROOT**: Gestisce associazioni di file e identificatori di classe.
   - **HKEY_CURRENT_USER**: Contiene configurazioni specifiche dell'utente connesso.
   - **HKEY_LOCAL_MACHINE**: Archivia impostazioni del computer locale.
   - **HKEY_USERS**: Raccoglie configurazioni di tutti gli utenti.
   - **HKEY_CURRENT_CONFIG**: Salva informazioni hardware utilizzate all'avvio.

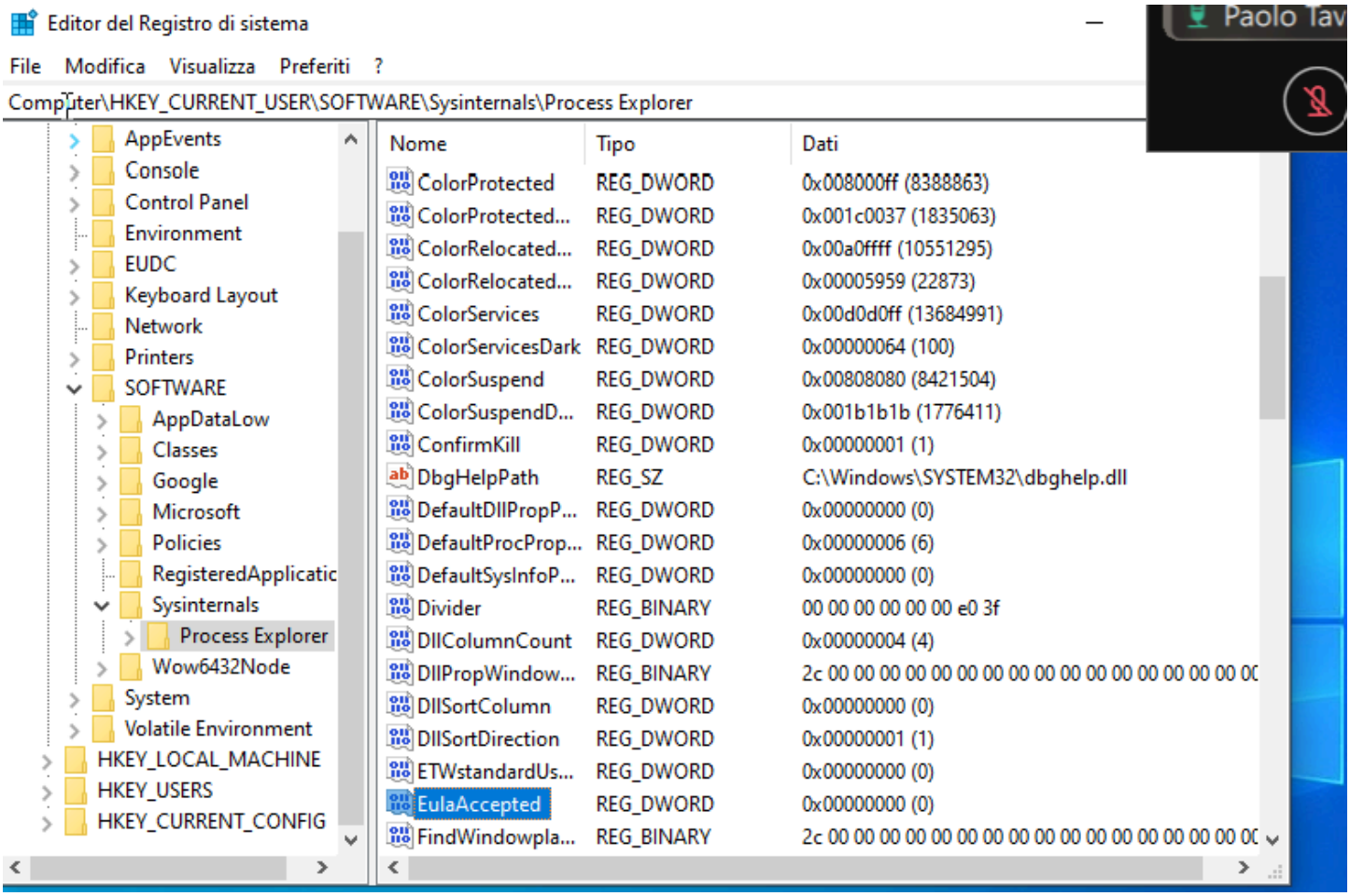


1. Qui si trova la chiave **EulaAccepted**, che determina se l'utente ha accettato il contratto di licenza.

Modifica della chiave di registro

- Il valore originale di **EulaAccepted** era **0x00000001(1)**, indicando che il contratto di licenza era stato accettato.
- Abbiamo cambiato il valore a **0x00000000(0)**, disattivando l'accettazione. Questo ha portato al ripristino della finestra del contratto di licenza alla successiva apertura di Process Explorer.

Risultato: La modifica dimostra come il registro controlli il comportamento delle applicazioni e come le modifiche possano influenzare direttamente il sistema.


Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
Computer\HKEY_CURRENT_USER\SOFTWARE\Sysinternals\Process Explorer
AppEvents
Console
Control Panel
Environment
EUDC
Keyboard Layout
Network
Printers
SOFTWARE
AppDataLow
Classes
Google
Microsoft
Policies
RegisteredApplicatic
Sysinternals
Process Explorer
Wow6432Node
System
Volatile Environment
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
Nome
Tipo
Dati
ColorProtected REG_DWORD 0x008000ff (8388863)
ColorProtected... REG_DWORD 0x001c0037 (1835063)
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 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 00 00 00 00 00 0
Paolo Tav