Report: Analisi di Processi, Thread, Handle e Registro di Windows

Questo report documenta un'esercitazione pratica volta all'esplorazione e alla manipolazione di processi, thread, handle e il Registro di Windows, utilizzando gli strumenti **Process Explorer** della suite Sysinternals e l'**Editor del Registro di sistema**. L'obiettivo è comprendere il comportamento del sistema operativo a un livello più granulare.

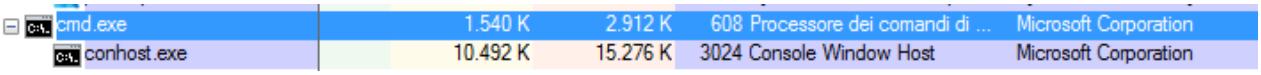
Parte 1: Esplorazione dei Processi

Terminazione del Processo Microsoft Edge

Durante l'esercitazione, si è tentato di terminare il processo associato a **Microsoft Edge** (specificatamente **Chrome.exe** come indicato nel log). Inizialmente, la terminazione del processo non è stata consentita, restituendo un errore di "Accesso negato". Questo indica che, anche con privilegi standard, alcuni processi critici o protetti non possono essere semplicemente terminati. Riavviando Process Explorer con privilegi di amministratore, si è tentata nuovamente la terminazione. Il log indica che anche come amministratore la terminazione non è riuscita per AvastBrowser.exe. Tuttavia, in un contesto generale, la terminazione forzata di un processo di browser web tramite Process Explorer solitamente causa la **chiusura immediata della finestra del browser**, interrompendo tutte le operazioni in corso e liberando le risorse occupate.

Avvio e Osservazione del Processo Prompt dei Comandi (cmd.exe)

1. **Avvio del Prompt dei Comandi:** È stato avviato un Prompt dei Comandi (cmd.exe). In Process Explorer, è stato identificato il processo cmd.exe.
2. **Processo Genitore e Figlio:** È stato osservato che cmd.exe ha **explorer.exe** come processo genitore. Inoltre, cmd.exe ha un processo figlio, **conhost.exe**. Quest'ultimo è responsabile della gestione dell'input/output della console.



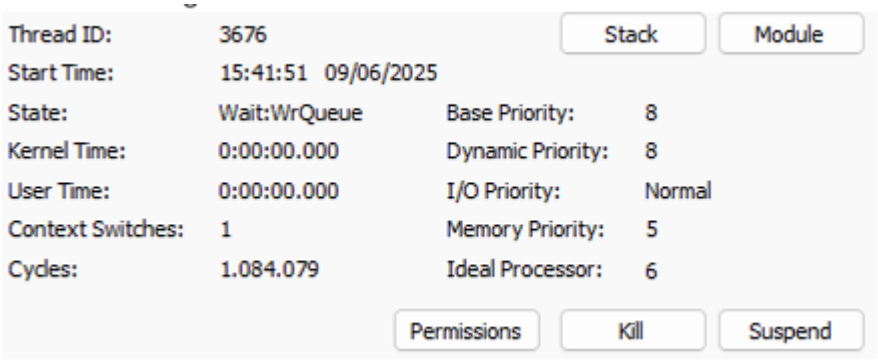
3. **Esecuzione del comando ping:** Un comando ping è stato eseguito all'interno del Prompt dei Comandi. Durante l'esecuzione del ping, un nuovo processo figlio, **PING.EXE**, è apparso temporaneamente sotto cmd.exe. Questo dimostra come i comandi esterni eseguiti dal prompt possano generare processi figli per la loro esecuzione.
4. **Analisi di conhost.exe con VirusTotal:** È stata eseguita una scansione del processo conhost.exe utilizzando l'integrazione VirusTotal di Process Explorer. I risultati hanno mostrato "0/77", indicando l'assenza di minacce note.
5. **Terminazione del Processo cmd.exe:** Il processo cmd.exe è stato terminato con successo. A seguito di questa azione, il processo figlio **conhost.exe** è stato **automaticamente terminato**. Questo comportamento è atteso, poiché i processi figli

dipendono dal loro genitore e vengono solitamente chiusi quando il genitore non è più in esecuzione.

Parte 2: Esplorazione di Thread e Handle

Esplorazione dei Thread

1. **Accesso ai Dettagli dei Thread:** È stato riaperto un Prompt dei Comandi e, in Process Explorer, sono state visualizzate le proprietà del processo conhost.exe, navigando alla scheda "Threads".
2. **Informazioni sui Thread:** La finestra delle proprietà ha fornito dettagli significativi per ciascun thread attivo all'interno del processo conhost.exe. Le informazioni disponibili includono:

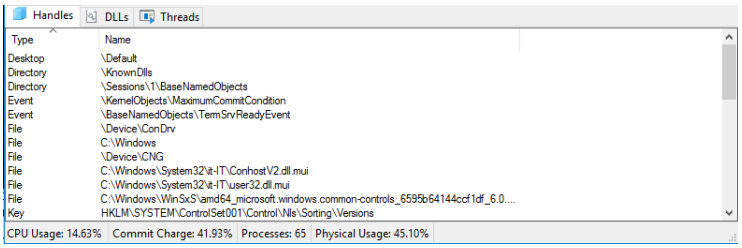


   - **Thread ID (TID):** Un identificatore univoco per ogni thread.
   - **Start Time:** L'ora e la data di avvio del thread.
   - **State:** Lo stato attuale del thread (ad esempio, Wait:WrQueue indica che il thread è in attesa).
   - **Kernel Time/User Time:** Il tempo di CPU speso dal thread in modalità kernel e utente, rispettivamente.
   - **Base Priority/Dynamic Priority:** Livelli di priorità del thread.
   - **Context Switches:** Il numero di volte in cui il thread ha scambiato il contesto di esecuzione con un altro thread.
   - **Cycles:** Il numero di cicli di clock della CPU dedicati all'esecuzione del thread.
   - **Memory Priority/I/O Priority:** Priorità relative alla memoria e alle operazioni di I/O.
   - **Ideal Processor:** Il processore ideale per l'esecuzione del thread.

Queste informazioni sono essenziali per il debugging, l'ottimizzazione delle prestazioni e l'analisi del comportamento di un'applicazione.

Esplorazione degli Handle

1. **Visualizzazione degli Handle:** In Process Explorer, è stata abilitata la "Lower Pane View" per visualizzare gli handle associati al processo conhost.exe.



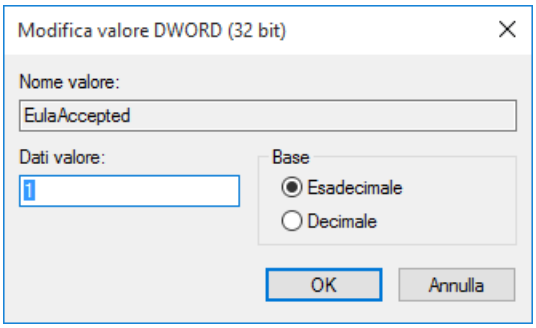
2. **Puntatori degli Handle:** Gli handle aperti da conhost.exe puntano a diversi tipi di oggetti del kernel, indicando le risorse con cui il processo interagisce. Tra gli oggetti identificati vi sono:
    - **ALPC Port:** Per la comunicazione interprocesso.
    - **Desktop, Directory:** Per l'interfaccia grafica e la gestione delle directory.
    - **Event:** Per la sincronizzazione tra thread o processi.
    - **File:** Riferimenti a file aperti, inclusi dispositivi e file di sistema (\Device\ConDrv, C:\Windows\, \Device\AvAswIDS_loc2, ecc.).
    - **Key:** Riferimenti a chiavi del Registro di Windows (HKLM, HKCU, HKCR, ecc.).
    - **Named Pipe:** Per la comunicazione tra processi.

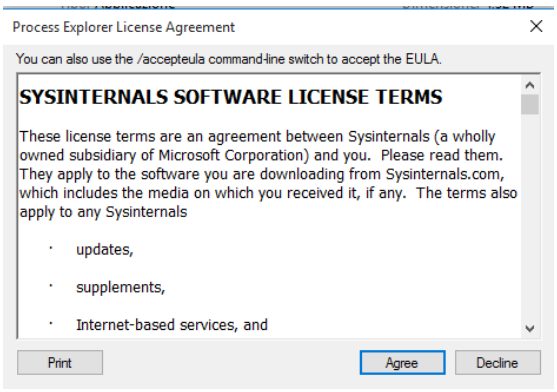
L'analisi degli handle fornisce una visione chiara delle interazioni di un processo con il sistema operativo e le sue risorse.

Parte 3: Esplorazione del Registro di Windows

Modifica della Chiave EulaAccepted

1. **Navigazione nel Registro di Windows:** Utilizzando l'Editor del Registro di sistema (regedit), è stata localizzata la chiave EulaAccepted per Process Explorer, situata in **Valore Iniziale:** Il valore iniziale della chiave EulaAccepted era 0x00000001 (1), indicando che l'Accordo di Licenza con l'Utente Finale (EULA) era stato accettato.
2. **Modifica del Valore:** Il valore della chiave è stato modificato da 1 a 0. Dopo la modifica, il valore nella colonna "Dati" è diventato 0x00000000 (0).





3. **Effetto della Modifica:** All'apertura successiva di Process Explorer, il programma ha nuovamente visualizzato la **finestra di dialogo dell'Accordo di Licenza con l'Utente Finale (EULA)**. Questo dimostra come le impostazioni di configurazione memorizzate nel Registro di Windows influenzino il comportamento delle applicazioni, e come la manipolazione di tali chiavi possa alterare la loro esperienza d'uso.