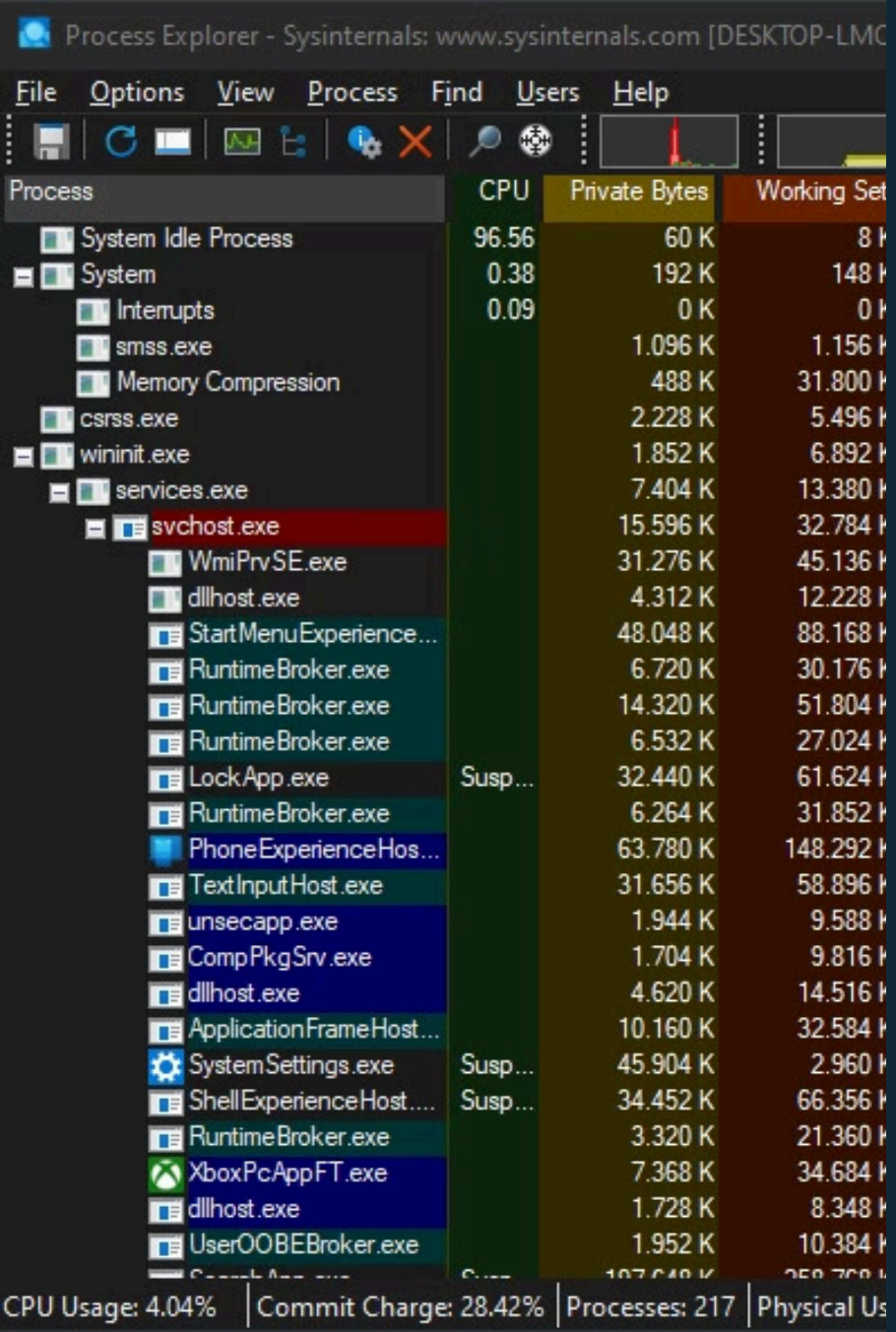
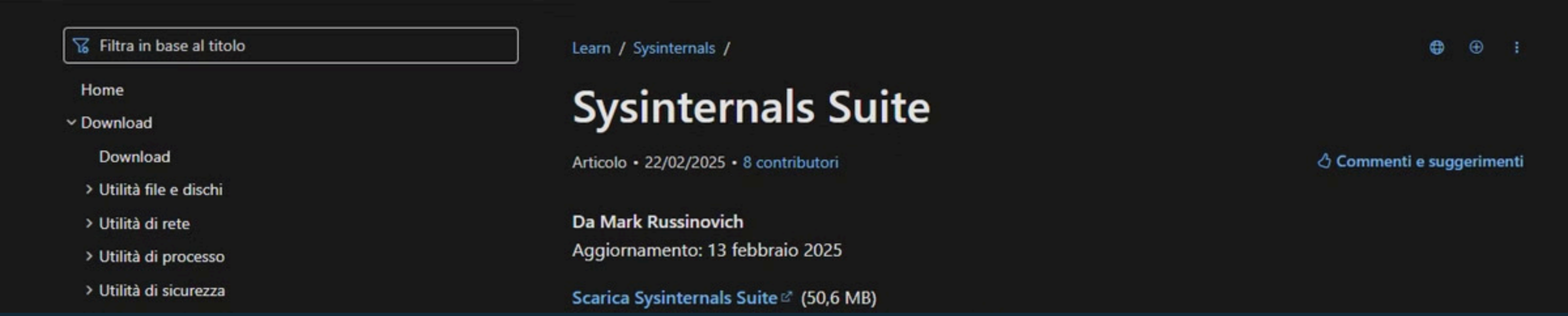


Esplorazione di Processi e Registro di Windows con Sysinternals

Nell'esercizio di oggi andremo a vedere concetti fondamentali del sistema operativo Windows, quali processi, thread e handle, e l'interazione con il Registro di Windows. L'obiettivo è stato quello di utilizzare strumenti avanzati per visualizzare e comprendere meglio le attività in esecuzione sul sistema.

Lo strumento principale impiegato è stato Process Explorer, parte della rinomata Sysinternals Suite, che fornisce una vista gerarchica e dettagliata dei processi attivi, superando le capacità del Task Manager standard di Windows.



Metodologia e Strumenti

Acquisizione Strumenti

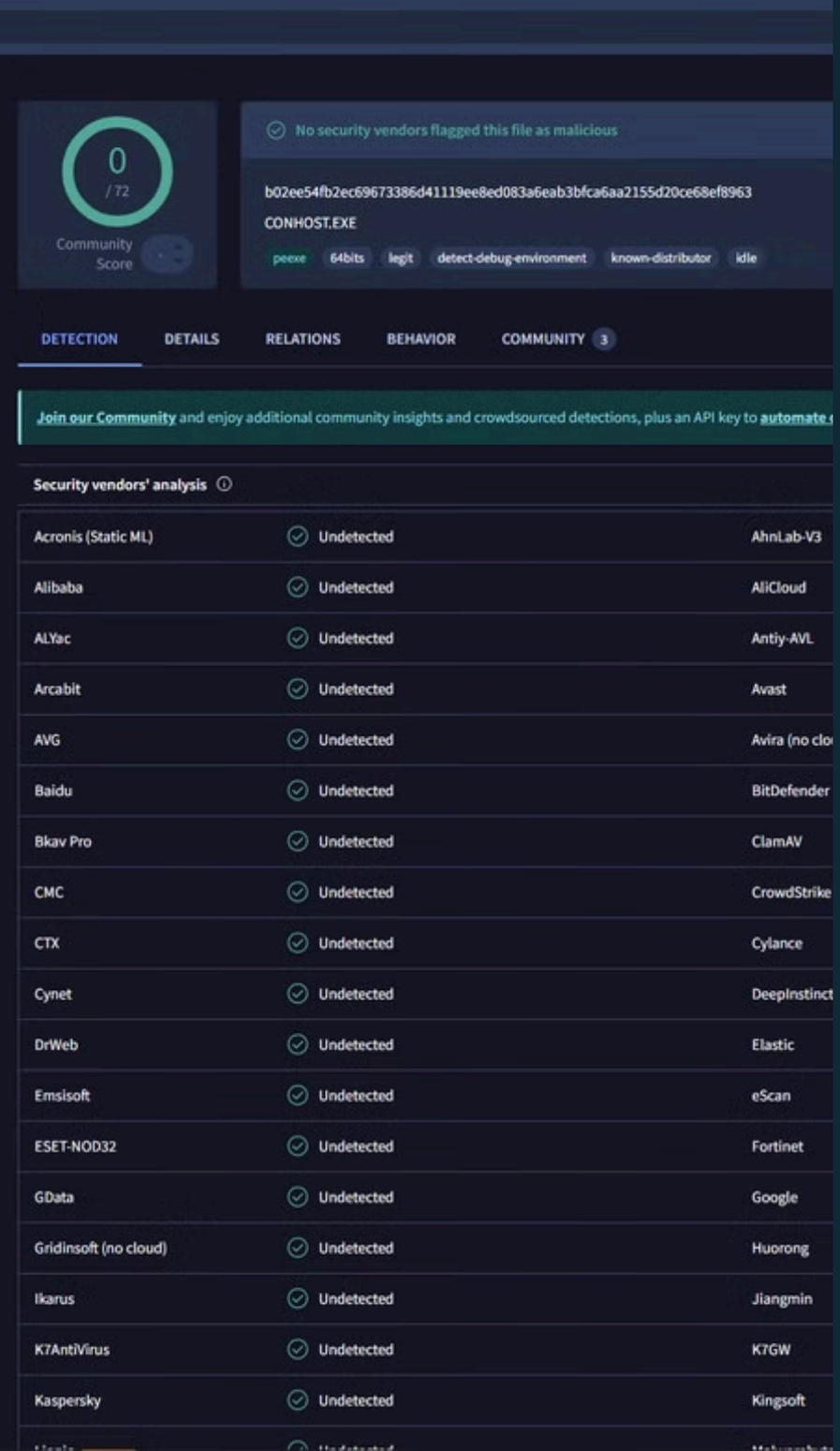
È stata scaricata la Sysinternals Suite dal sito ufficiale Microsoft TechNet, contenente una collezione completa di utilità per l'analisi avanzata del sistema Windows.

Estrazione e Avvio

Dopo il download, l'archivio .zip è stato decompresso e l'eseguibile procexp.exe (Process Explorer) è stato avviato per iniziare l'analisi del sistema.

Utilizzo Avanzato

Process Explorer è stato utilizzato per esplorare i processi attivi e le loro relazioni gerarchiche, fornendo informazioni dettagliate non disponibili negli strumenti standard.



Analisi dei Processi con Process Explorer

Identificazione dei Processi

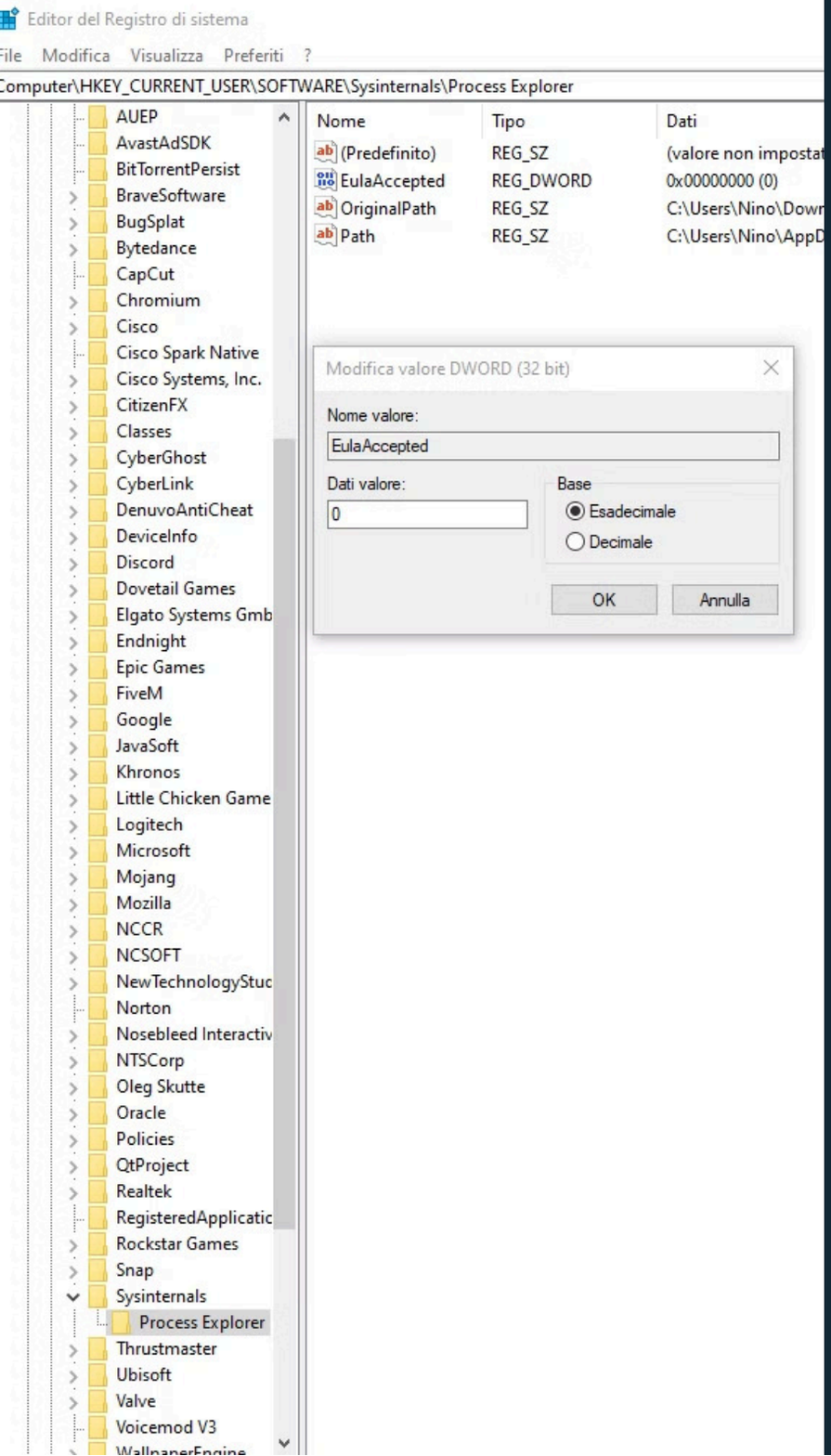
Utilizzo della funzionalità "Find Window's Process" (icona a forma di mirino) per identificare il processo associato a una finestra del Prompt dei Comandi (cmd.exe).

Osservazione della Creazione di Processi Figlio

Esecuzione del comando ping google.com all'interno del Prompt dei Comandi, con conseguente visualizzazione di PING.EXE come processo figlio di cmd.exe.

Verifica di Sicurezza Integrata

Utilizzo dell'integrazione con VirusTotal per verificare la reputazione dei processi tramite l'invio dell'hash del file eseguibile ai server di VirusTotal.



Interazione con il Registro di Windows

1 Accesso al Registro

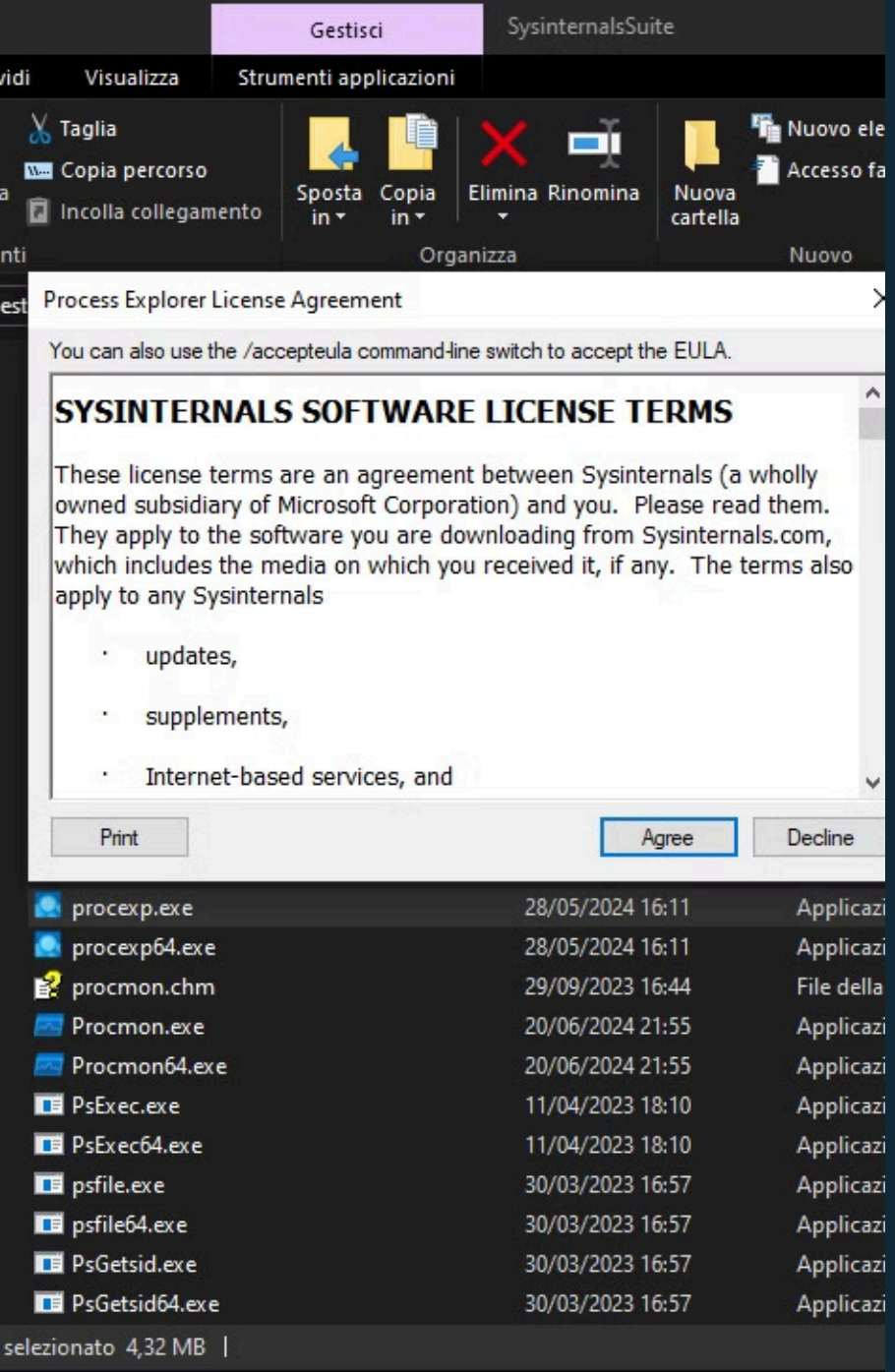
Avvio dell'Editor del Registro di Windows (regedit.exe) per accedere alla struttura gerarchica delle chiavi di registro del sistema.

2 Navigazione e Modifica

Navigazione all'interno dell'hive HKEY_CURRENT_USER fino alla sottochiave utilizzata da Process Explorer. Modifica del valore DWORD "EulaAccepted" da 1 a 0.

3 Verifica dell'Effetto

Riavvio di Process Explorer per confermare che la modifica ha causato la ricomparsa della finestra di dialogo per l'accettazione dell'EULA.



Conclusioni

Comprensione Avanzata dei Processi

Process Explorer si è rivelato efficace per ottenere una comprensione più profonda della gestione dei processi in Windows, incluse le relazioni gerarchiche padre-figlio.

Integrazione con Strumenti di Sicurezza

L'integrazione con VirusTotal dimostra il valore di Process Explorer nell'analisi di sicurezza e nell'identificazione di potenziali minacce.

Importanza del Registro di Windows

L'esplorazione del Registro ha confermato il suo ruolo centrale nella memorizzazione delle configurazioni, dimostrando come la modifica diretta dei suoi valori influenzi il comportamento del software.