REPORT S11/L1

Lo scopo di questo laboratorio è quello di andare ad esplorare i ***processi***, i ***thread*** e gli ***handles*** utilizzando ***Process Explorer*** della ***Suite Sysinternals***. Modificare poi un impostazione modificando un valore nel registro di windows.

SOLUZIONE

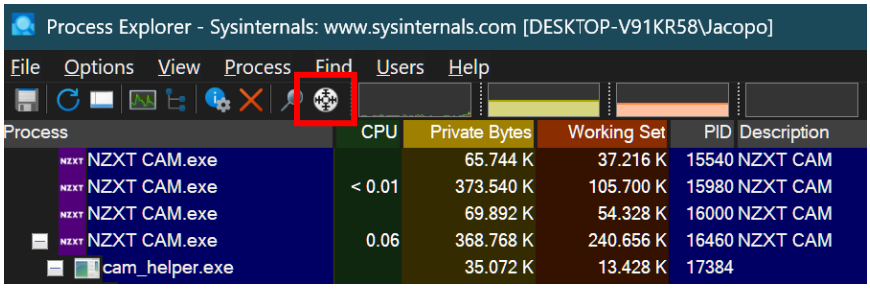
Un ***processo*** è un' istanza di esecuzione di un programma, ha un proprio spazio di indirizzamento (memoria isolata dagli altri processi). Ogni processo puo aveere piu thread che eseguono codice in maniera simultanea.

Un ***thread*** è l' unità di esecuzione all' interno di un processo, tutti i thread di un processo condividono le stesse risorse e la stessa memoria. Questi permettono il ***multithreading***, ovvero l' esecuzoine concorrente all' interno di un processo.

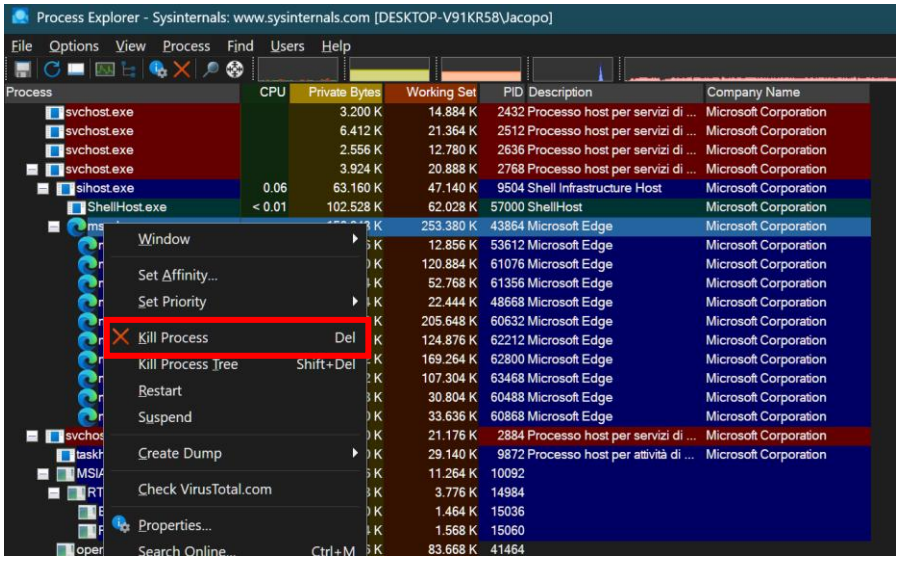
Un ***Handle*** è un identificatore (numero o puntatore), usato dal sistema operativo per riferirsi ad un oggetto, come un processo, un thread, un file aperto, una finestra. Permettono ai programmi di poter accedere alle risorse del sistema senza conoscere dettagli. In windows gli ***Handle*** sono gestiti dal ***Kernel***.

Il primo passo è quello di procedere con l' esplorazione dei processi, come già detto un processo è l' istanza di esecuzione di un programma. Lo farò attraverso il ***Process Explorer di Sysinternals***.

Procedo quindi attraverso lo strumento "***Drag over window***" per andare ad individuare un processo trascinando il cursore su una finestra aperta, nello specifico lo farò sulla sessione aperta di ***Microsoft Edge***.

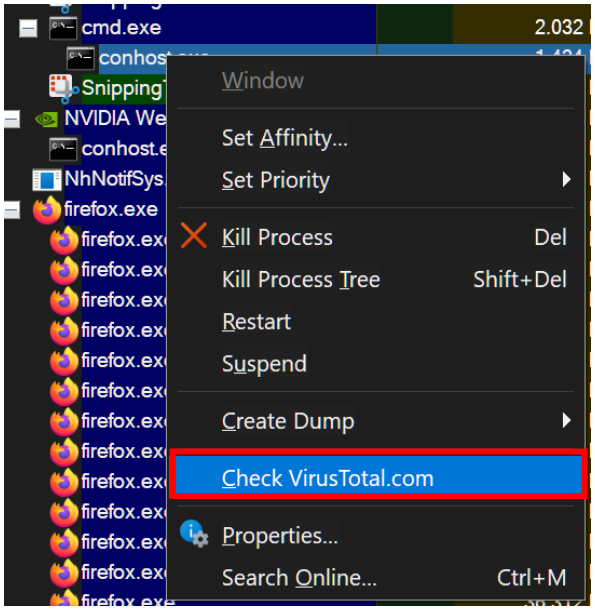


A questo punto avrò individuato il procsso interessato, procederò andando a terminarlo facendo ***ClickDestro*** e ***Kill Process***, il risultato sarà ovviamente la chiusura della sessione ***Microsoft Edge***.



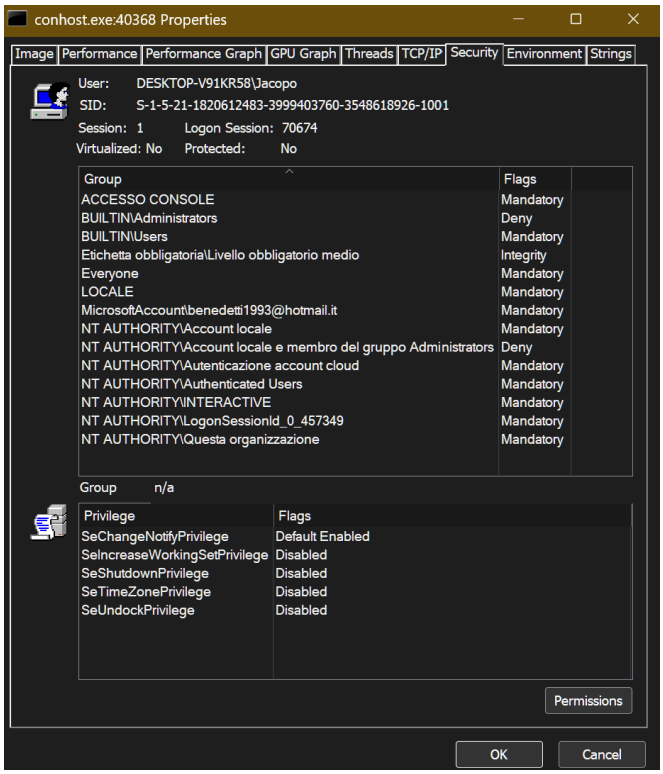
A questo punto provo con un un nuovo processo, avvio il ***Prompt dei Comandi*** e con lo strumento ***Drag to window*** lo vado ad evidenziare la sessione, faccio poi un comando ping e posso vedere come sotto il processo in questione venga avviato un processo figlio "***PING.EXE***".

Vado ora a fare un controllo su "virustotal.com" del proesso figlio "***cohost.exe***" e vado poi a killarlo come visto in precedenza.



Passo ora all' esplorazione dei ***thread*** e degli ***handle***, faccio click destro su "***cohost.exe***" e poi su prorpietà, vado quindi su Threads per visualizzare i thread attivi per il processo "***cohost.exe***".

Da qui si ha accesso ad una serie di info come le variabili, i permessi e le info relative alla sicurezza, le info sulle performance e le ***printable strings*** (sequenze di caratteri leggibili nella memoria di un processo).



Nel process explorer vado ora ad analizzare gli handles associati, click **View** > seleziono **Lower Pane View** > **Handles,** da qui posso vedere a cosa puntano gli handles del processo figlio cohost.exe, nello specifico puntano a file e chiavi di registro.

Type	Name
ALPC Port	\RPC Control\OLE5EC2D2C2152E04BC73FA914228BA
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackit-IT_26100.18.37.0_ne...
File	\Device\CNG
File	\Device\NamedPipe\
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKCU
Key	HKCU\Software\Classes\Local Settings
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKLM
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom
Key	HKCR\PackagedCom\ClassIndex
Key	HKCU\Software\Classes\PackagedCom