

# Malware Analysis Basica Dinamica

L'analisi dinamica di base è il secondo passo da effettuare quando si approccia l'analisi di un malware.

Essa può supportare e confermare le teorie e la profilazione ipotizzata circa il malware durante l'analisi statica, oppure può smentire eventuali teorie iniziali.

I tool sono lo strumento che un malware analyst ha a disposizione per correlare le informazioni provenienti da diverse fonti come i processi, la memoria, le chiavi di registro, ed il traffico di rete per profilare il comportamento di un malware.

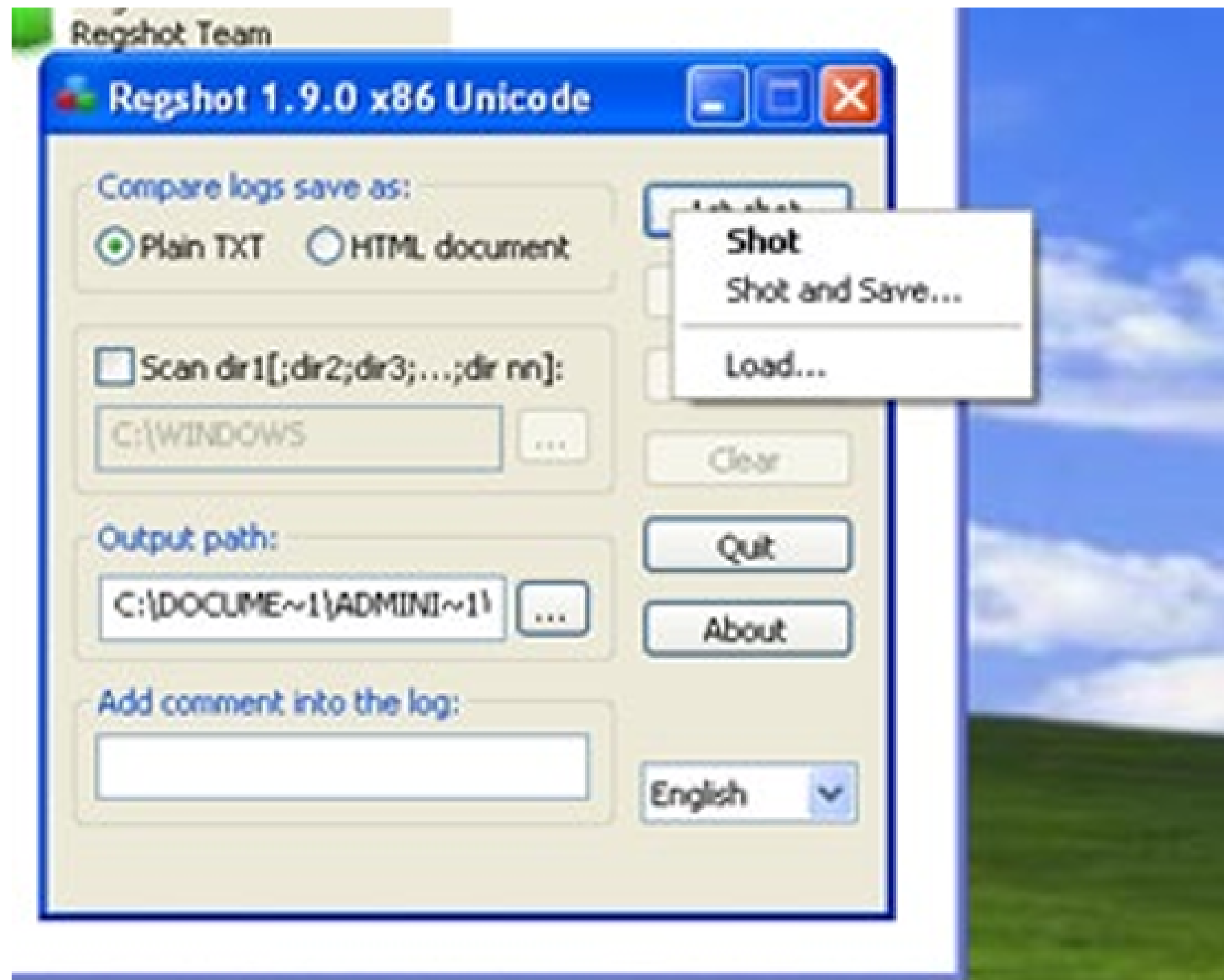
Andiamo nello specifico a definire questi elementi molto importanti per una corretta analisi, ovvero:

- Processi
- Chiavi di registro
- Traffico di rete
- File System

- Registri: gli eventi catturati permettono di controllare se il malware ha modificato eventuali chiavi di registro. Le chiavi di registro sono le variabili di configurazione dei sistemi Windows e i valori delle chiavi rappresentano tutto ciò che viene caricato all'avvio del sistema. Spesso capita di incontrare malware che modificano le chiavi di registro al fine di essere avviati automaticamente appena avviato il sistema.
- File System: gli eventi di questa categoria permettono di monitorare e controllare tutte le interazioni tra il malware e il file system come ad esempio: la creazione di un nuovo file, l'eliminazione di un file, la modifica di un file e così via. Generalmente queste attività sono supportate da «operation» quali Create File, Read File, Close File e così via.
- Rete: le attività di questa categoria sono particolarmente importanti per monitorare il traffico generato dal malware verso internet e verso la rete interna. La maggior parte dei malware presenta attività di rete abbastanza marcate, che vanno dall'invio di file verso web server remoti, alla connessione verso domini infetti, fino alla creazione di backdoor.

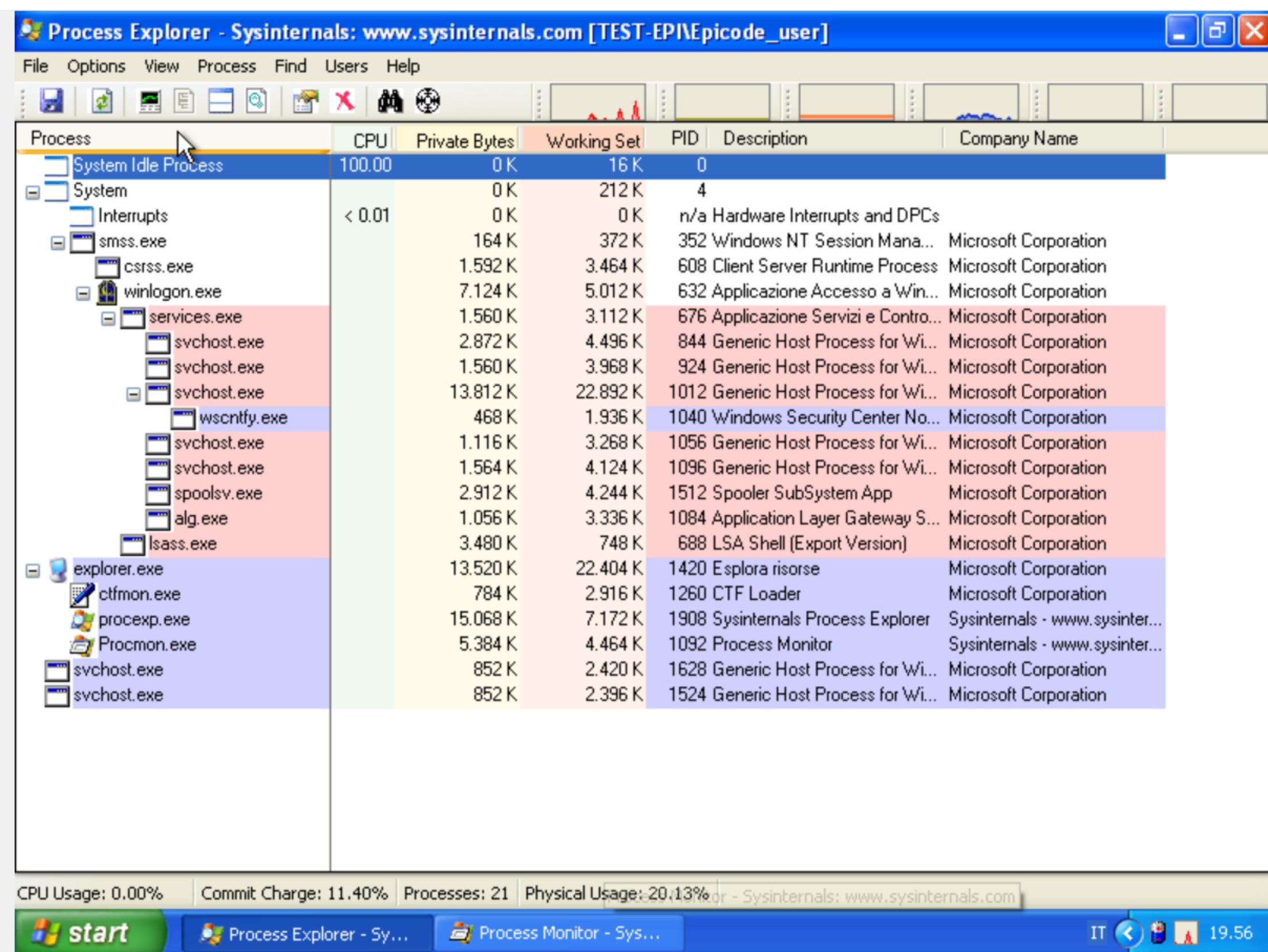
- Processi: gli eventi di questa categoria aiutano ad identificare eventuali processi addizionali creati dal malware per propagarsi sul sistema o per rendere se stesso non identificabile. Alcuni malware infatti, tendono a creare nuovi processi con nomi piuttosto comuni oppure apparentemente innocui in modo tale da non destare sospetto sui sistemi vittima. Le funzioni sfruttate dai malware più comuni sono «LoadImage» per caricare eseguibili e librerie per esecuzione in memoria e attività sui processi e Thread come Create Process, Create Thread che appunto servono per creare nuovi processi o thread all'interno di processi.

Una volta chiarite tutte queste informazioni possiamo partire con l'analisi basica dinamica, la prima cosa che andiamo a fare è un'istantanea sullo stato delle chiavi di registro del sistema; in modo da poterla confrontare alla fine del processo con una seconda istantanea catturata dopo aver lanciato il malware così da poter avere una tangibile constatazione delle modifiche apportate.



Tra i tool che andremo a utilizzare c'è anche ProcessExplorer, un tool che permette l'analisi dettagliata di tutti i processi in esecuzione su un sistema.

Come detto ci permette di avere una chiara panoramica sui processi attivi e ci restituisce altre preziose informazioni quali : Il nome del processo, la CPU utilizzata, il PID del processo, La descrizione del processo in esecuzione e il nome della compagnia. Tutte queste informazioni lette correttamente portano all'individuazione del malware, o quanto meno si restringe il campo



Process Explorer - Sysinternals: www.sysinternals.com [TEST-EPINEpicode\_user]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	100.00	0 K	16 K	0		
System	< 0.01	0 K	212 K	4		
Interrupts		0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		164 K	372 K	352	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1.592 K	3.464 K	608	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		7.124 K	5.012 K	632	Applicazione Accesso a Win...	Microsoft Corporation
services.exe		1.560 K	3.112 K	676	Applicazione Servizi e Contro...	Microsoft Corporation
svchost.exe		2.872 K	4.496 K	844	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1.560 K	3.968 K	924	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13.812 K	22.892 K	1012	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		468 K	1.936 K	1040	Windows Security Center No...	Microsoft Corporation
svchost.exe		1.116 K	3.268 K	1056	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1.564 K	4.124 K	1096	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		2.912 K	4.244 K	1512	Spooler SubSystem App	Microsoft Corporation
alg.exe		1.056 K	3.336 K	1084	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3.480 K	748 K	688	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe		13.520 K	22.404 K	1420	Esplora risorse	Microsoft Corporation
ctfmon.exe		784 K	2.916 K	1260	CTF Loader	Microsoft Corporation
procexp.exe		15.068 K	7.172 K	1908	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon.exe		5.384 K	4.464 K	1092	Process Monitor	Sysinternals - www.sysinter...
svchost.exe		852 K	2.420 K	1628	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		852 K	2.396 K	1524	Generic Host Process for Wi...	Microsoft Corporation

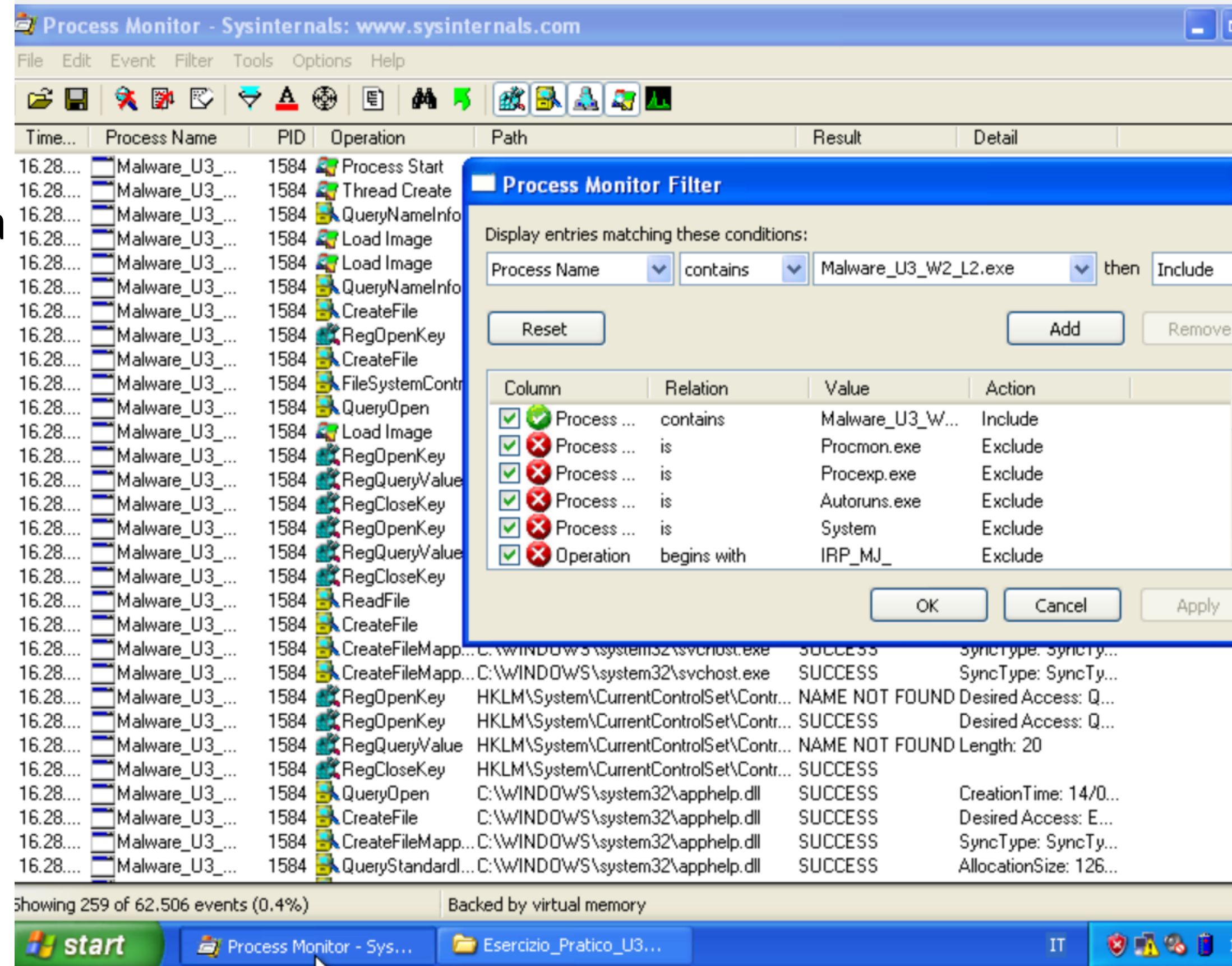
CPU Usage: 0.00% Commit Charge: 11.40% Processes: 21 Physical Usage: 20.13% Sysinternals: www.sysinternals.com



Ciò che ci resta da fare è lanciare il malware nel nostro sistema chiuso, dargli un breve lasso di tempo in modo da attivarsi ed eseguire la seconda istantanea alle chiavi di registro. Queste infatti saranno state modificate dal malware e potremo quindi indagare.

La fase successiva richiede l'utilizzo del tool Process Monitor.

Process Monitor, o «procmon», è un tool avanzato per Windows che permette di monitorare i processi ed i thread attivi, l'attività di rete, l'accesso ai file e le chiamate di sistema effettuate su un sistema operativo. Una funzione davvero utile di questo tool è quella di applicare filtri alle informazioni visualizzate in modo da ridurre il campo in modo considerevole.



Quello che sono andato a fare è stato restringere il campo a tutti quei processi i quali avevano lo stesso nome di processo del nostro malware. Successivamente ho effettuato un'altra scrematura dei risultati analizzando tra i risultati solo le modifiche ai processi e thread, notando che ha creato un nuovo processo chiamato "svchost.exe" con PID: 1628, fornendoci ulteriori elementi da indagare per comprendere meglio il comportamento del nostro malware. Successivamente controlliamo invece le richieste di accesso alle chiavi e le operazioni compiute dal nostro malware. Ho notato ad un certo punto che accedeva a un file e scriveva dati, sono risalito al path del file in questione e all'interno c'erano tutti i tasti da me digitati fino a quel momento. Abbiamo quindi compreso la natura del malware, si tratta di un keylogger. Un'ulteriore controlla da effettuare è sulle possibili connessioni che tenta il malware. Analizzando questo punto, non sono state riscontrate tracce.