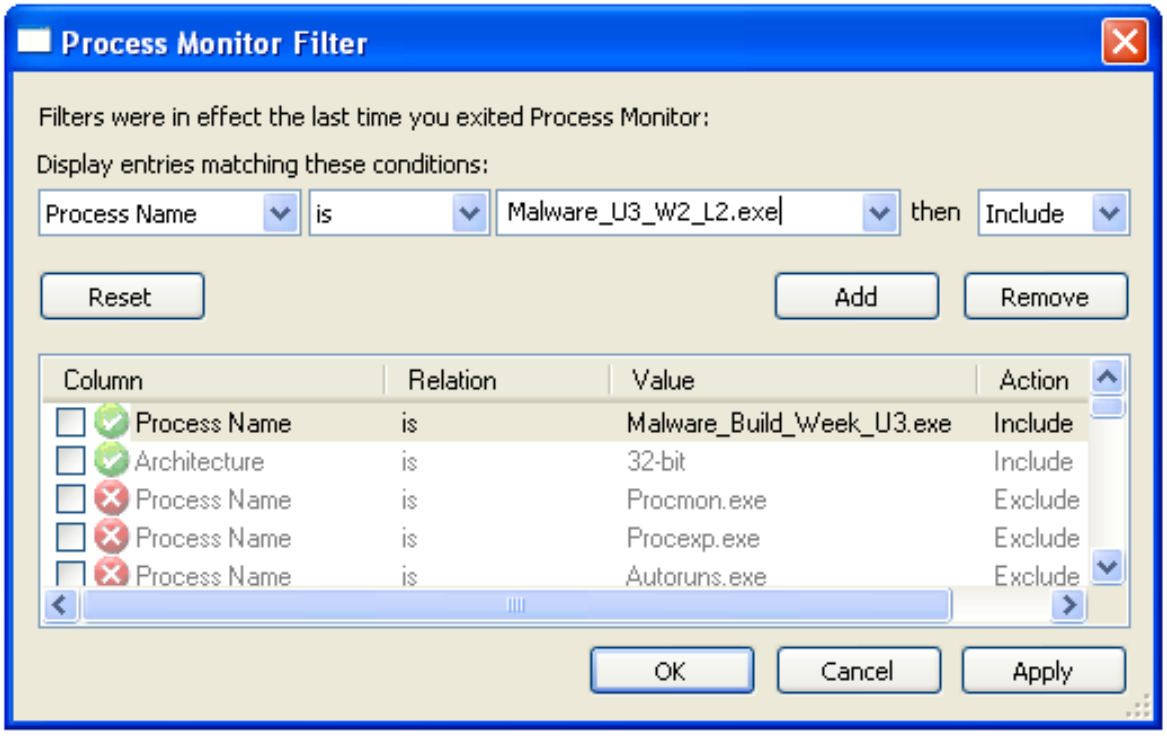
Analisi dinamica basica

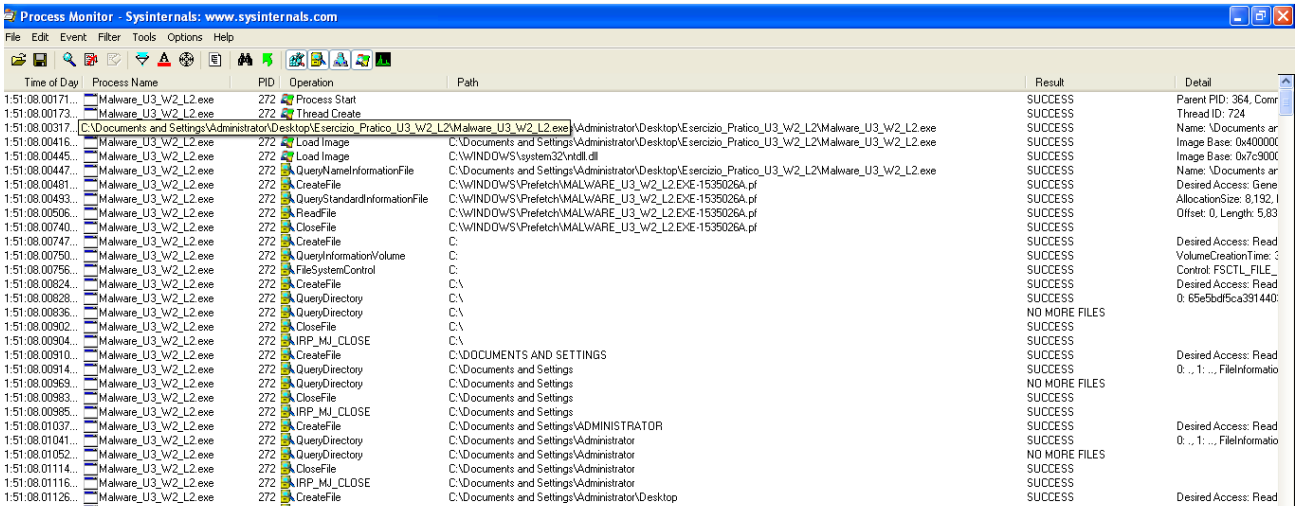
Identificare le azioni del malware sul file system con Process Monitor

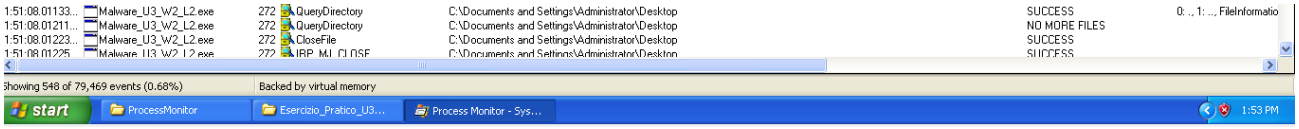
Dopo l'infarinatura effettuata con l'analisi statica basica, aggiungiamo un livello di dettaglio con l'analisi dinamica basica.

- Faccio partire **Procmon,** setto il filtro e faccio partire la cattura



- Avvio il malware
- Dopo circa 1 minuto stoppo la cattura





Appunti

Sappiamo che le ***operations*** *possibili su questo tool sono 5 e fanno visualizzare attività relative a:*

1. registri Windows, con cui posso controllare se il malware ha modificato chiavi di registro (variabili di configurazione dei sistemi Win). Alcuni malware lo fanno per essere avviati contemporaneamente rispetto all'avvio del sistema.

2. file system di Windows, con cui posso controllare ad esempio la creazione, l'eliminazione o la modifica di alcuni file.

3. flussi di rete, importanti per monitorare il traffico generato dal malware vs internet o vs la rete interna.

4. processi e ai thread, con cui posso identificare processi addizionali creati dal malware o per rendere se stesso non identificabile. Alcuni malware usano nomi piuttosto comuni (es: load image o create thread, create process) per caricare eseguibili e librerie.

5. tempi di: utilizzo del processore da parte di ogni processo; allocazione di memoria.

Nell'interfaccia generale ci sono:

Time di cattura

Process name

PID dei processi

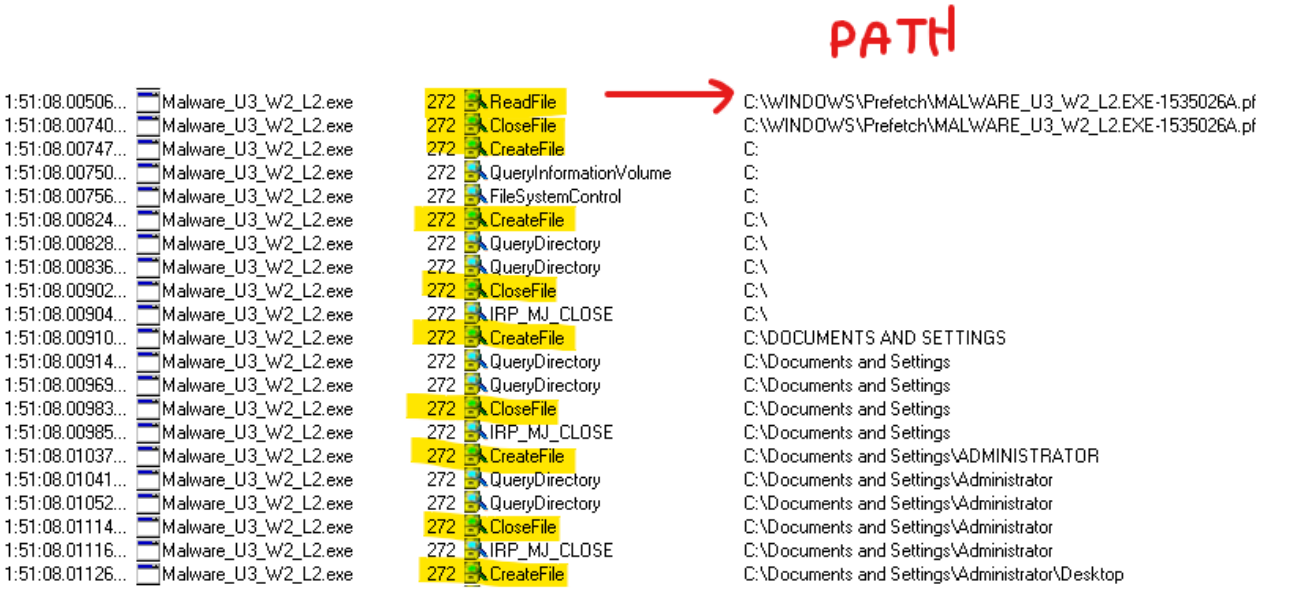
Operation effettuata *(ce ne sono una marea, per capire di cosa si tratta, si puo cercare online)*

Path (dove si sta concretizzando l'azione)

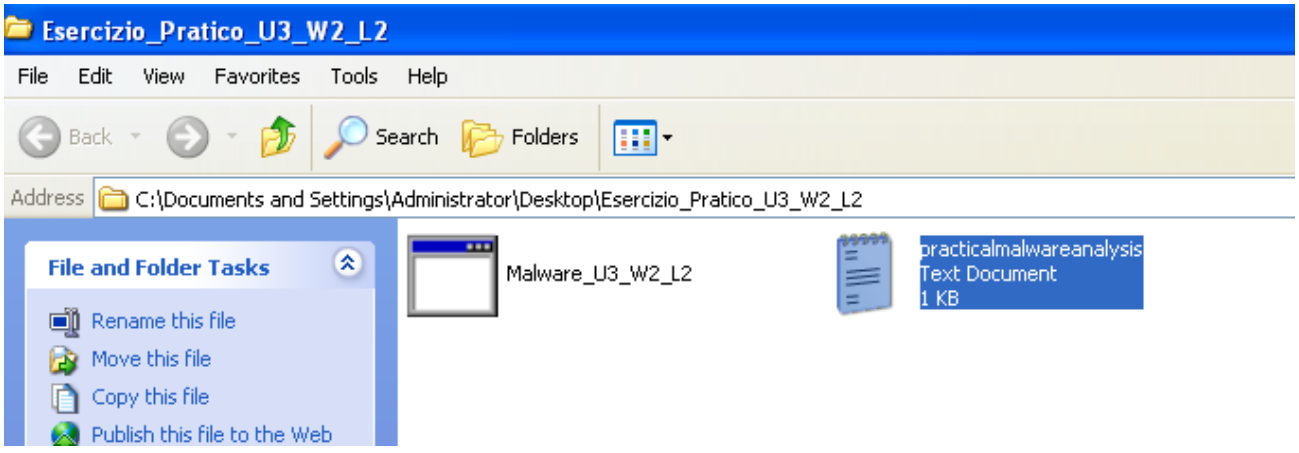
Result dell'azione dell'operazione

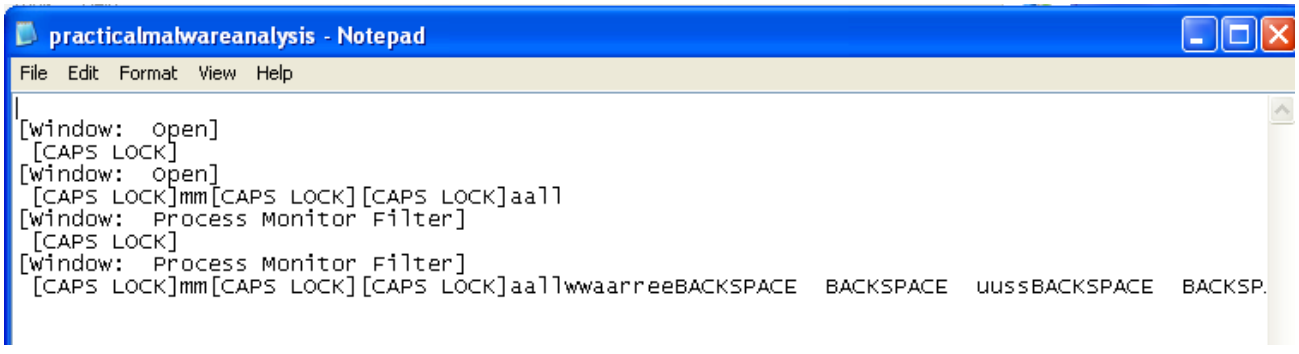
Detail della richiesta dell'operazione

- Ci accorgiamo immediatamente dal report di procmon che nella colonna operation ci sono funzioni come "Create file", "Read file", "Close file" e il loro path. Un esempio, di seguito:



- Nella cartella dove risiede il malware è stato creato un file .txt

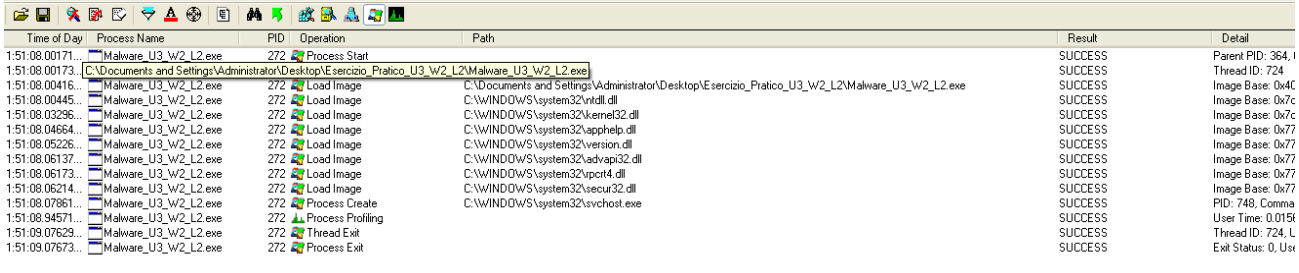




Soluzione: Il malware ha acquisito alcuni dei caratteri da tastiera: questo comportamento è tipico dei malware Keylogger

Identificare azioni del malware su processi e thread utilizzando Process Monitor

Ovviamente uso il filtro dei thread e dei processi



Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:51:08.00171...	Malware_U3_W2_L2.exe	272	Process Start		SUCCESS	Parent PID: 364,
1:51:08.00173...	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe				SUCCESS	Thread ID: 724
1:51:08.00416...	Malware_U3_W2_L2.exe	272	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x40
1:51:08.00445...	Malware_U3_W2_L2.exe	272	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c
1:51:08.03296...	Malware_U3_W2_L2.exe	272	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c
1:51:08.04664...	Malware_U3_W2_L2.exe	272	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77
1:51:08.05226...	Malware_U3_W2_L2.exe	272	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77
1:51:08.06137...	Malware_U3_W2_L2.exe	272	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77
1:51:08.06173...	Malware_U3_W2_L2.exe	272	Load Image	C:\WINDOWS\system32\vpcrt4.dll	SUCCESS	Image Base: 0x77
1:51:08.06214...	Malware_U3_W2_L2.exe	272	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77
1:51:08.07861...	Malware_U3_W2_L2.exe	272	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 748, Comma
1:51:08.94571...	Malware_U3_W2_L2.exe	272	Process Profiling		SUCCESS	User Time: 0.015
1:51:09.07629...	Malware_U3_W2_L2.exe	272	Thread Exit		SUCCESS	Thread ID: 724, L
1:51:09.07673...	Malware_U3_W2_L2.exe	272	Process Exit		SUCCESS	Exit Status: 0, Use

Ci sono alcune funzioni "Load Image" che importano librerie .dll, ma ci soffermiamo sulla funzione "process create": pare che il malware stia creando un processo "svchost.exe" (generalmente un processo valido di Windows). E' un comportamento tipico dei malware che tentano di nascondersi per eludere controlli antivirus.

Conclusioni finali

Alla luce delle nostre analisi, deduciamo che:
il malware, appena viene eseguito, cerca di camuffarsi creando un processo "svchost.exe". Poi lancia la sua principale funzionalità, un keylogger che salva i caratteri digitati dall'utente nel file "practicalmalwareanalysis" creato appositamente nella cartella dove si trova il file eseguibile.