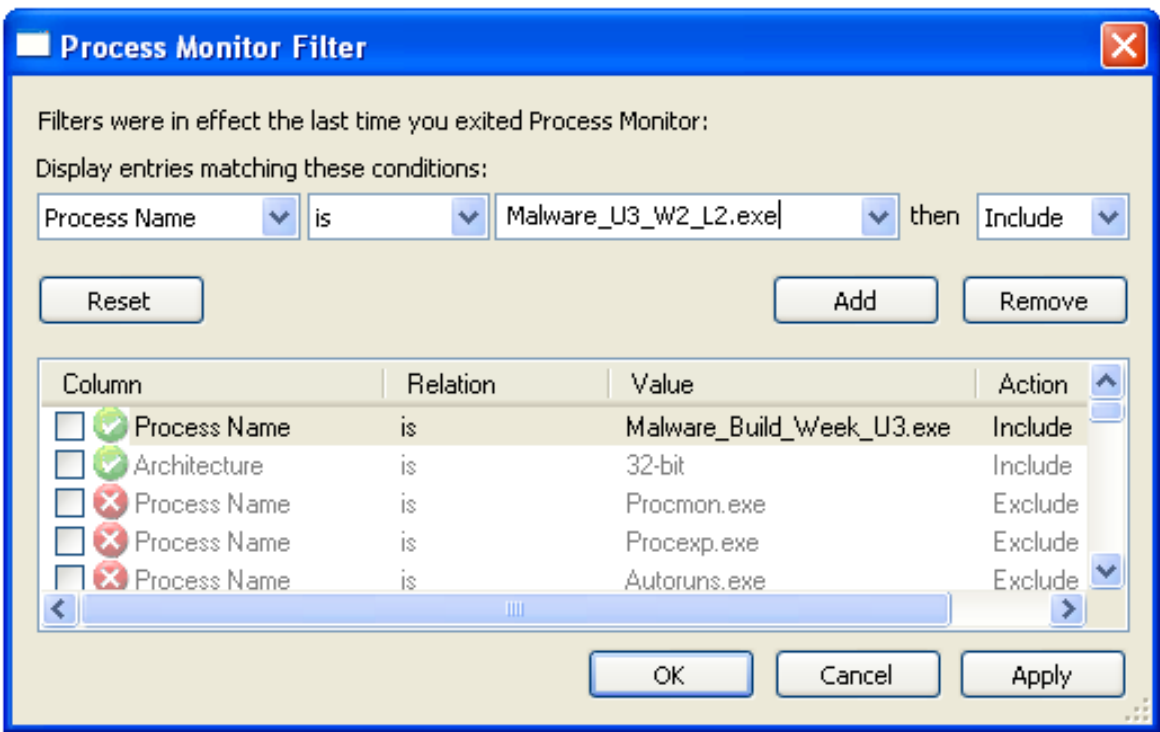


Analisi dinamica basica

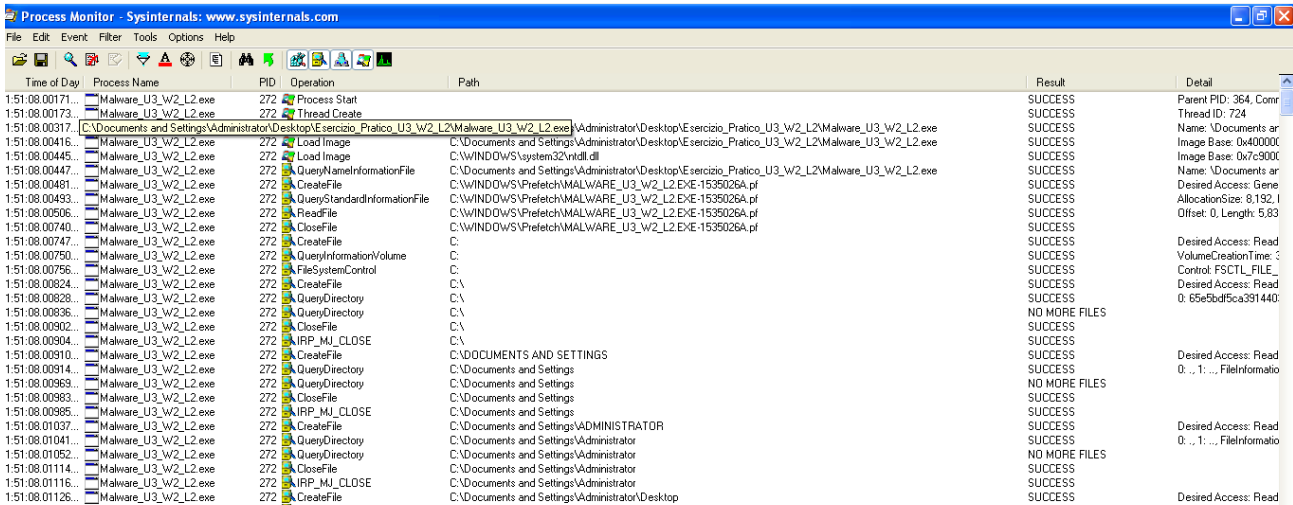
Identificare le azioni del malware sul file system con Process Monitor

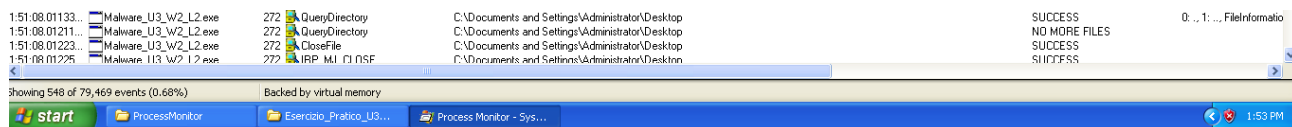
Dopo l'infarinatura effettuata con l'analisi statica basica, aggiungiamo un livello di dettaglio con l'analisi dinamica basica.

- 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 aggiuntivi 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 può cercare online)

Path (dove si sta concretizzando l'azione)

Result dell'azione dell'operazione

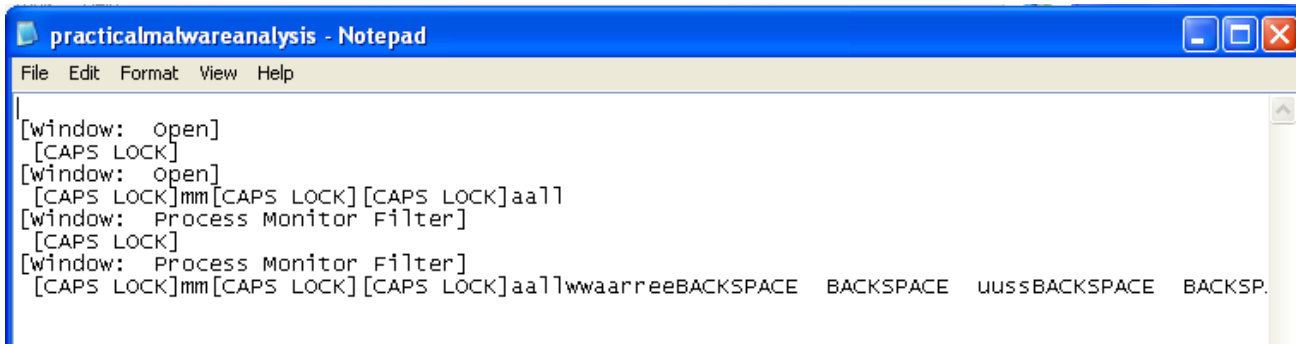
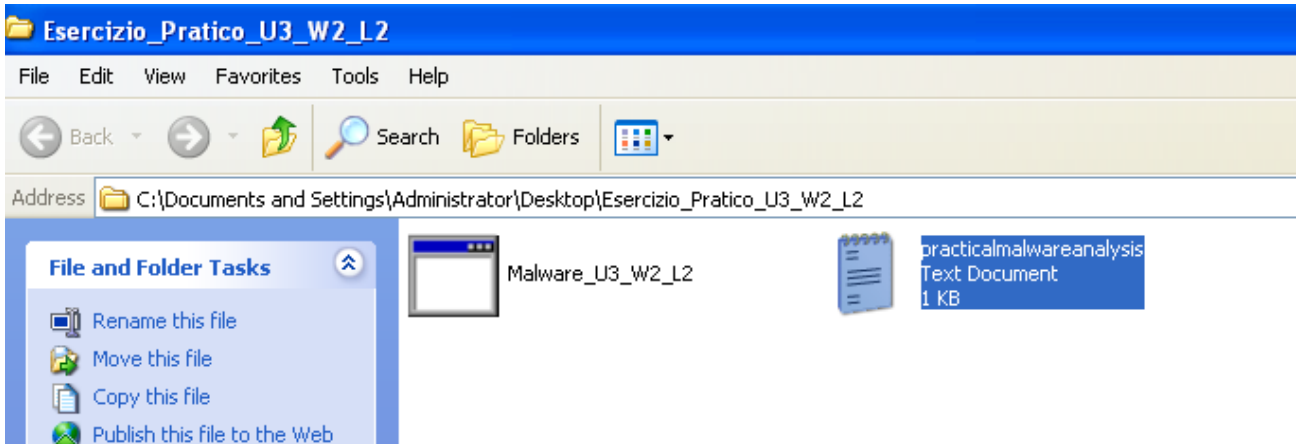
Detail della richiesta dell'operazione

- 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:

PATH

1:51:08.00506...	Malware_U3_W2_L2.exe	272	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
1:51:08.00740...	Malware_U3_W2_L2.exe	272	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
1:51:08.00747...	Malware_U3_W2_L2.exe	272	CreateFile	C:\
1:51:08.00750...	Malware_U3_W2_L2.exe	272	QueryInformationVolume	C:\
1:51:08.00756...	Malware_U3_W2_L2.exe	272	FileSystemControl	C:\
1:51:08.00824...	Malware_U3_W2_L2.exe	272	CreateFile	C:\
1:51:08.00828...	Malware_U3_W2_L2.exe	272	QueryDirectory	C:\
1:51:08.00836...	Malware_U3_W2_L2.exe	272	QueryDirectory	C:\
1:51:08.00902...	Malware_U3_W2_L2.exe	272	CloseFile	C:\
1:51:08.00904...	Malware_U3_W2_L2.exe	272	IRP_MJ_CLOSE	C:\
1:51:08.00910...	Malware_U3_W2_L2.exe	272	CreateFile	C:\DOCUMENTS AND SETTINGS
1:51:08.00914...	Malware_U3_W2_L2.exe	272	QueryDirectory	C:\Documents and Settings
1:51:08.00969...	Malware_U3_W2_L2.exe	272	QueryDirectory	C:\Documents and Settings
1:51:08.00983...	Malware_U3_W2_L2.exe	272	CloseFile	C:\Documents and Settings
1:51:08.00985...	Malware_U3_W2_L2.exe	272	IRP_MJ_CLOSE	C:\Documents and Settings
1:51:08.01037...	Malware_U3_W2_L2.exe	272	CreateFile	C:\Documents and Settings\ADMINISTRATOR
1:51:08.01041...	Malware_U3_W2_L2.exe	272	QueryDirectory	C:\Documents and Settings\Administrator
1:51:08.01052...	Malware_U3_W2_L2.exe	272	QueryDirectory	C:\Documents and Settings\Administrator
1:51:08.01114...	Malware_U3_W2_L2.exe	272	CloseFile	C:\Documents and Settings\Administrator
1:51:08.01116...	Malware_U3_W2_L2.exe	272	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator
1:51:08.01126...	Malware_U3_W2_L2.exe	272	CreateFile	C:\Documents and Settings\Administrator\Desktop

- 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	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Parent PID: 364, 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: 0x4C...
1:51:08.00445...	Malware_U3_W2_L2.exe	272	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7C...
1:51:08.00396...	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\user32.dll	SUCCESS	Image Base: 0x77...
1:51:08.06214...	Malware_U3_W2_L2.exe	272	Load Image	C:\WINDOWS\system32\user32.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, Us...

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.

Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000

Load Image
Process Create
Process Profiling
Thread Exit
Process Exit

C:\WINDOWS\system32\svchost.exe

SUCCESS
SUCCESS
SUCCESS
SUCCESS
SUCCESS

Image base: 0x771e0000, Image size: 0x11000
PID: 748, Command line: "C:\WINDOWS\system32\svchost.exe"
User Time: 0.0156250 seconds, Kernel Time: 0.0468750 seconds,
Thread ID: 724, User Time: 0.0000000, Kernel Time: 0.0468750
Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0468750

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.