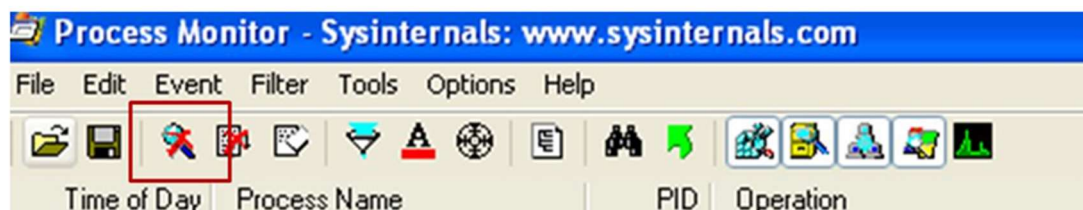


Soluzione – Identificare azioni su File system del Malware

Per prima cosa, facciamo partire Procmon prima di eseguire il malware, successivamente avviamo il malware e dopo un lasso di tempo di circa 1 minuto stoppiamo la cattura Procmon, cliccando sull'icona a forma di lente nel rettangolo rosso in figura. Attenzione, quando come in figura c'è una «X» rossa sull'icona vuole dire che la cattura è bloccata e procmon non sta monitorando gli eventi. Quando la «X» rossa non è presente, allora la cattura è in corso.



Soluzione – Identificare azioni su File system del Malware

Inseriamo il filtro come visto in teoria per mostrare solo le attività del processo con nome «Malware_U3_W2_L2.exe».

Vediamo subito dal report di procmon che ci sono delle funzioni riportate nella colonna «operation» molto interessanti come «Create File», «Read file» e «Close File» con rispettivo path.

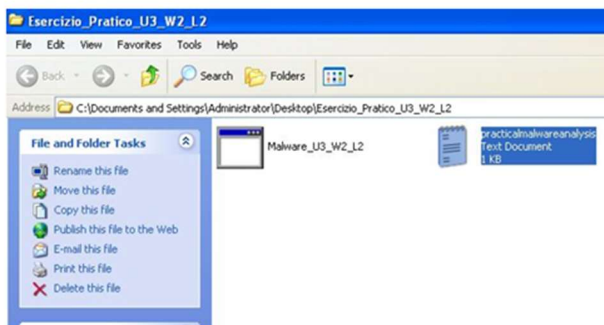
2:32:44.31559	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\	NO MORE FILES	
2:32:44.31563	Malware_U3_W2_L2.exe	2100	CreateFile	C:\	SUCCESS	
2:32:44.31598	Malware_U3_W2_L2.exe	2100	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31607	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings	SUCCESS	
2:32:44.31645	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings	SUCCESS	
2:32:44.31656	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31711	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	
2:32:44.31716	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
2:32:44.31726	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31829	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31836	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
2:32:44.31871	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
2:32:44.31874	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31904	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31908	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31983	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	
2:32:44.31991	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	NO MORE FILES	
2:32:44.31998	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31981	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31917	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	
2:32:44.31925	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	NO MORE FILES	
2:32:44.31962	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31975	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.31987	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	
2:32:44.31999	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	NO MORE FILES	
2:32:44.32003	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.32025	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	Desired Access: Read Data/Lat Directory; Synchronize; Disposition: Open; Options: Directory; Synchronization: Non-Alert; Open For Backup; Attributes: 0; ...; FileInformationClass: FileInformation; 3: All Users; 4: Default User; 5: Local Service; 6: Network Service
2:32:44.32033	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	
2:32:44.32067	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	
2:32:44.32091	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Exercise_Pratico_U3_W2_L2	SUCCESS	

Soluzione – Identificare azioni su File system del Malware

Molto interessante è la riga riportata sotto - Procmon ci indica che è stato creato un file .txt nella cartella dove risiede il Malware.

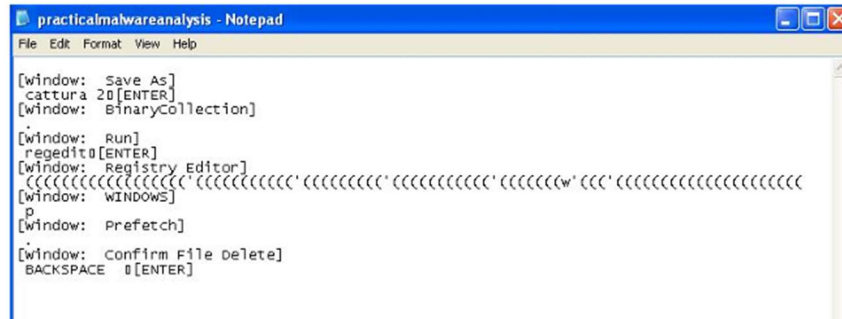
2:32:44.31864	Malware_U3_W2_L2.exe	3180	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
2:32:44.31873	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS	
2:32:44.31883	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS	

Apriamo la cartella sul desktop dove risiede l'eseguibile del malware per confermare che in effetti il malware ha creato un file denominato «practicalmalwareanalysis»



Soluzione – Identificare azioni su File system del Malware

Apriamo il file (il contenuto del vostro file potrebbe essere diverso) per notare che il file ha acquisito alcuni dei caratteri da tastiera utilizzati durante l'esecuzione del malware – questo comportamento è piuttosto solito dei malware **Keylogger**.



Soluzione – Identificare azioni su Processi e Thread

Utilizzando la medesima cattura di Procmon, utilizziamo le icone per filtrare sugli eventi riguardanti **processi e thread**.

Vediamo alcune funzioni molto interessanti come Load Image che viene utilizzata per «caricare» per l'esecuzione il malware e le librerie (.dll) necessarie, e poi vediamo «Process Create» che serve per creare un processo.

Sembra che il nostro malware stia creando un processo chiamato «svchost.exe» che generalmente è un processo valido di Windows. Questo è un altro comportamento frequente dei malware, cercare di camuffare la loro esecuzione sotto un processo con un nome valido per eludere eventuali antivirus / anti malware.

[illegible]

Soluzione – conclusioni finali

Possiamo ipotizzare quindi che il nostro malware quando viene eseguito cerca prima di camuffarsi creando un nuovo processo chiamato «svchost.exe», poi lancia la sua principale funzionalità ovvero un keylogger che salva i caratteri digitati dall'utente nel file «practicalmalwareanalysis» creato appositamente nella cartella dove si trova l'eseguibile.

