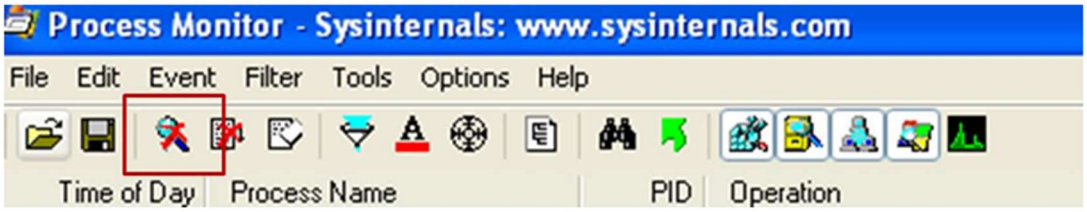
Soluzione – Identificare azioni su File system del Malware

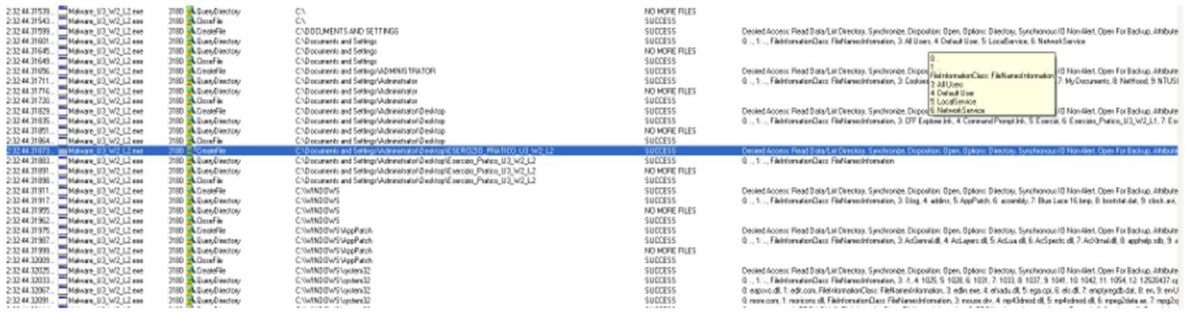
Per prima cosa, facciamo partire Procmon prima di eseguire il malware, successivamente avviamo il malware e dopo un lasso di tempo di circa 1 minuto stoppiamo la cattura Procmon, cliccando sull'icona a forma di lente nel rettangolo rosso in figura. Attenzione, quando come in figura c'è una «X» rossa 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.

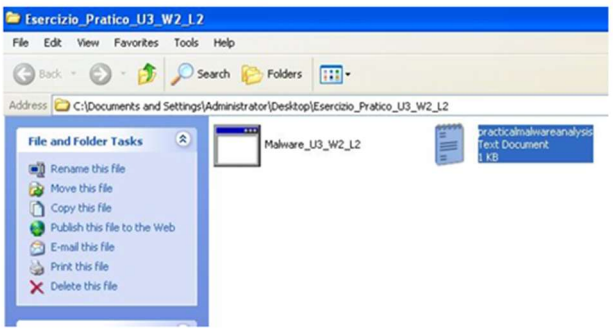
Vediamo subito dal report di procmon che ci sono delle funzioni riportate nella colonna «operation» molto interessanti come «**Create File**», «**Read file**» e «**Close File**» con rispettivo path.



Soluzione – Identificare azioni su File system del Malware

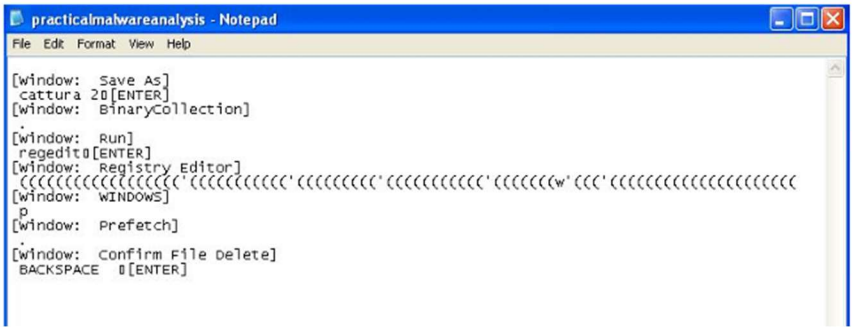
Molto interessante è la riga riportata sotto - Procmon ci indica che è stato creato un file .txt nella cartella dove risiede il Malware.

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.**

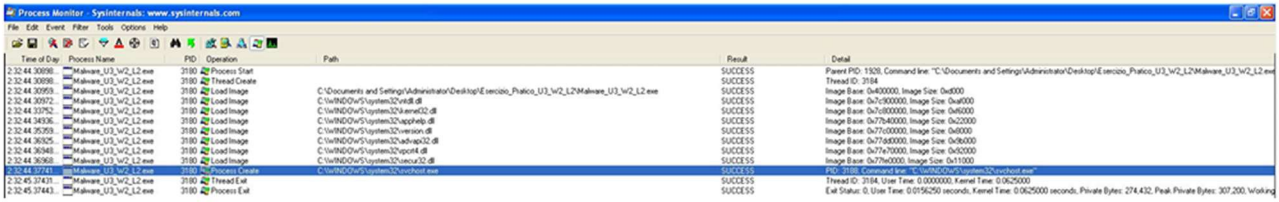


Soluzione – Identificare azioni su Processi e Thread

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.



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.