Report S10-L2
Analisi dinamica basica

Sommario

Traccia: 1
Svolgimento 2
1.Identificazione Azioni su File system da parte del Malware 2
Avvio del tool 2
Esecuzione Malware 3
Filtro 3
Selezione icona "show file system activity" 4
Analisi report di procmon 4
Conferma creazione di un file 5
Malware Keylogger 5
2.Identificazione azioni su Processi e Thread da parte del malware 5
3.Conclusioni finali – Profilazione del malware 6

Traccia:

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Suggerimento

Per quanto riguarda le attività dal malware sul file system, soffermatevi con particolare interesse sulle chiamate alla funzione **Create File** su path noti (ad esempio il path dove è presente l'eseguibile del malware).

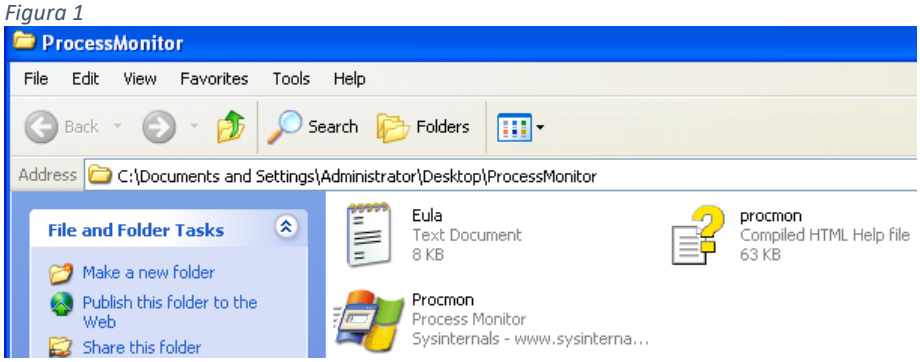
Svolgimento

Nell'ambito della **analisi dinamica basica**, che comprende tutte quelle attività di analisi che presuppongono l'esecuzione dei malware in un ambiente dedicato, è utilizzato molto il 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.
È un tool molto utilizzato per monitorare eventuali processi o attività create dal malware in esecuzione su un sistema.

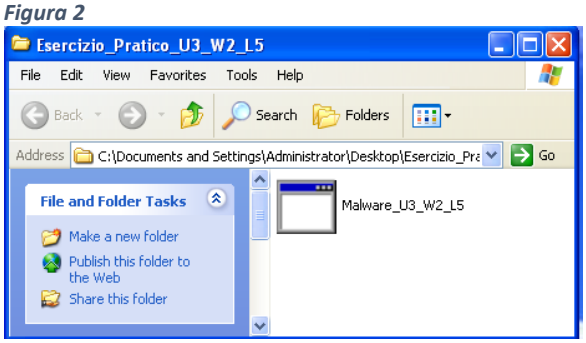
Il tool è installato di default sulla macchina virtuale dedicata per l'analisi dei malware (Malware Analysis_Final) e può essere avviato facendo doppio click sull'icona del file eseguibile, **procmon,** all'interno della cartella «ProcessMonitor» sul desktop.

Figura 1



Invece, **l'eseguibile del malware**, chiamato "**Malware_U3_W2_L2**", si trova nella cartella del desktop "Esercizio_pratico_U3_W2_L2".

Figura 2



1. Identificazione Azioni su File system da parte del Malware

Avvio del tool

Per prima cosa, si avvia il tool (**figura 3**) cliccando sull'icona della lente di ingrandimento (l'icona della lente rossa in figura si ha quando il monitoraggio è in atto e, cliccandola si ferma il monitoraggio). Al momento non è presente alcuna informazione perché il filtro applicato esclude tutti gli eventi relativi al sistema operativo della macchina. Per vederli, invece, basta andare su "Filter", e cliccare "Reset Filter".
La **figura 4** riporta i filtri iniziali, presentati di default dal tool, che si possono applicare.
Come si può notare non è presente il filtro relativo all'eseguibile del Malware, "**Malware_U3_W2_L2**". Questa è la ragione per si è chiusa questa finestra per avviare direttamente il tool.

Figura 3

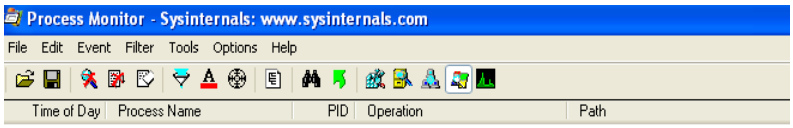
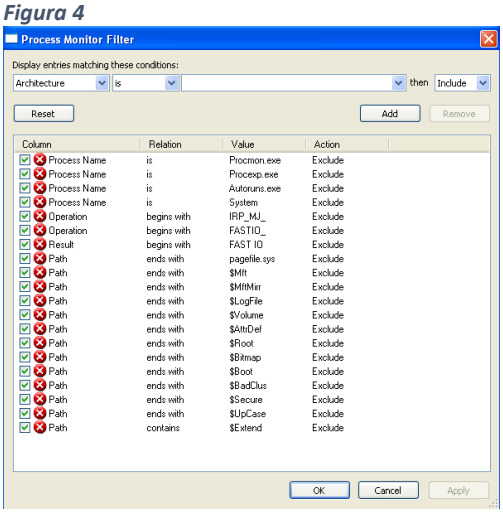


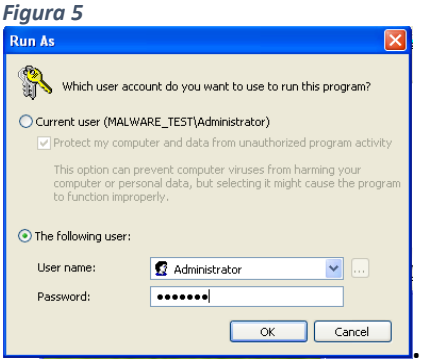
Figura 4



Esecuzione Malware

In secondo luogo, si procede ad **eseguire il file del malware.** Per l'efficacia del tool è necessario eseguire il malware nel seguente modo: cliccare con il tasto destro su "Malware_U3_W2_L2**",** scegliere **"run as"** e selezionare l'opzione **"the following user",** come in **figura 5,** poi si può cliccare sull'icona del file per eseguirlo.
N.B. Potrebbe essere necessario seguire il percorso inverso per far comparire l'eseguibile come opzione nel filtro del tool (prima run as e poi avvio tool e cliccare di nuovo su malware per eseguirlo e catturarlo)

Figura 5

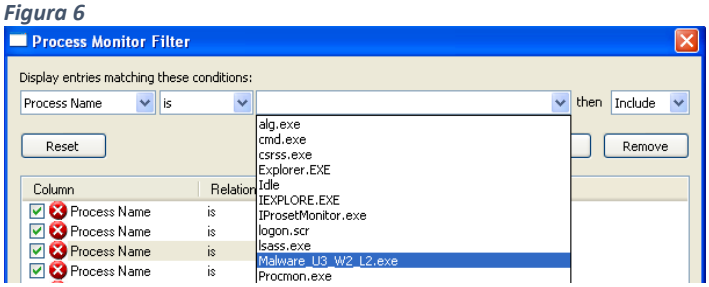


Filtro

Tornando su Procmon, si deve impostare **il malware in esecuzione come filtro,** in modo da visualizzare le azioni che questo esegue sul sistema della macchina.

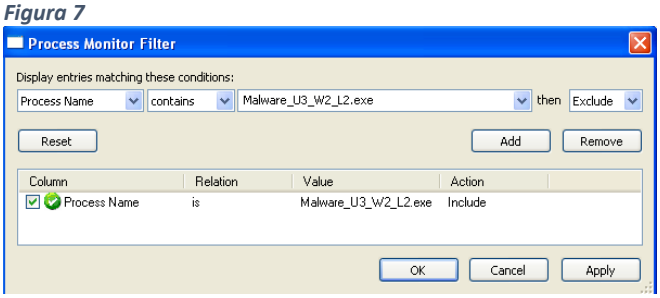
Si clicca sulla tab **"Filter"** e si seleziona nuovamente **"filter"**, dove apparirà nuovamente la finestra mostrata in figura 4.
A questo punto**,** si ricerca il malware attraverso il **"Process Name"** e cercando tra le opzioni, il tool percepisce il malware come attivo **(figura 6).** È anche possibile ricercare scrivendo direttamente nel campo.

Figura 6



Una volta selezionato l'eseguibile del malware, si clicca su **add (Figura 7), apply e OK (figura 7).**
N.B Le altre opzioni di processi presenti devono essere rimossi con doppio click su ciascuna.

Figura 7



Selezione icona "show file system activity"

Una volta inserito il filtro, la schermata della cattura fatta dal tool restituirà solo le **azioni compiute dal Malware come processo sul sistema della macchina.**
Dal momento che nella traccia viene richiesto di visualizzare specificatamente le **azioni del malware sul file system**, si devono escludere dalla cattura tutti gli eventi o attività che non attengono al file system, cliccando e dese-lezionando le icone in **figura 8.**
Si lascia, invece, selezionata la **seconda icona da sinistra** che mostra le attività del file system.
Le icone, quindi, sono utilizzate per filtrare gli eventi di una determinata categoria.

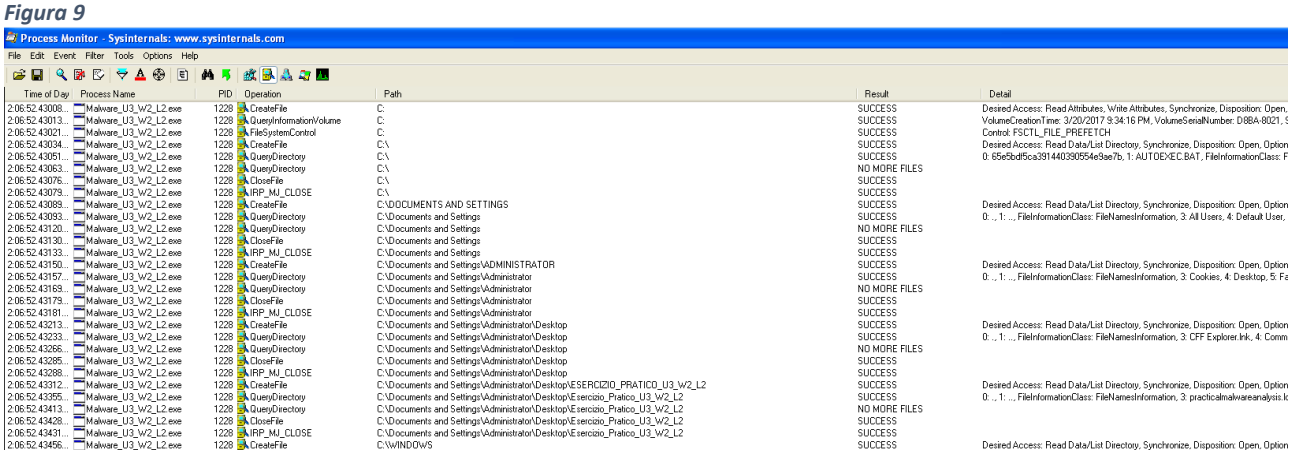
Figura 8

Analisi report di procmon

Dalla schermata del tool, è possibile capire subito che il malware ha interagito con il file system del sistema operativo file system evidenziate dalla presenza di funzioni come «**Create File**», «**Read file**» e «**Close File**» con rispettivo path (**Figura 9**).

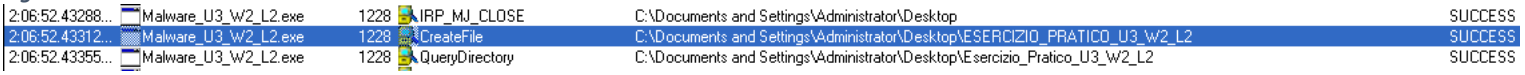
Le azioni specifiche sono identificate attraverso le **funzioni** elencate, ovvero "**Create File**" (Creare File), "**Read File**" (Leggere File) e "**Close File**" (Chiudere File).
Queste funzioni indicano che **il malware ha eseguito operazioni di creazione di file, lettura di file esistenti e chiusura di file precedentemente aperti**.
La presenza di un percorso (**path**) associato a ciascuna di queste operazioni fornisce informazioni dettagliate sul **luogo in cui sono avvenute tali azioni nel sistema di file**.
Analizzando questi percorsi, è possibile ottenere una comprensione più approfondita di quali file sono stati coinvolti e potenzialmente quali sezioni del sistema sono state interessate dal malware.

Figura 9



In particolare, Procmon mostra che il malware ha **creato un file** nella cartella del desktop, “Esercizio_pratico_U3_W2_L2”, in cui si trova il malware.

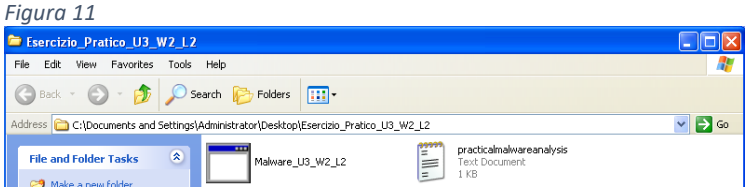
Figura 10



Conferma creazione di un file

Quindi, aprendo la cartella suddetta, si può confermare che in effetti il malware ha creato un **file di testo** (text o .txt) denominato «**practicalmalwareanalysis**».

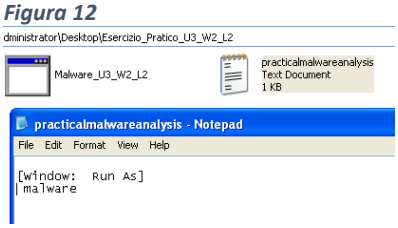
Figura 11



Malware Keylogger

Aprendo il file, si può vedere che riporta alcuni **caratteri da tastiera** utilizzati durante l’esecuzione del malware. Questo comportamento è tipico dei **Keylogger,** un tipo di malware che registra e memorizza le sequenze di tasti digitati su una tastiera di un dispositivo infetto.

Figura 12

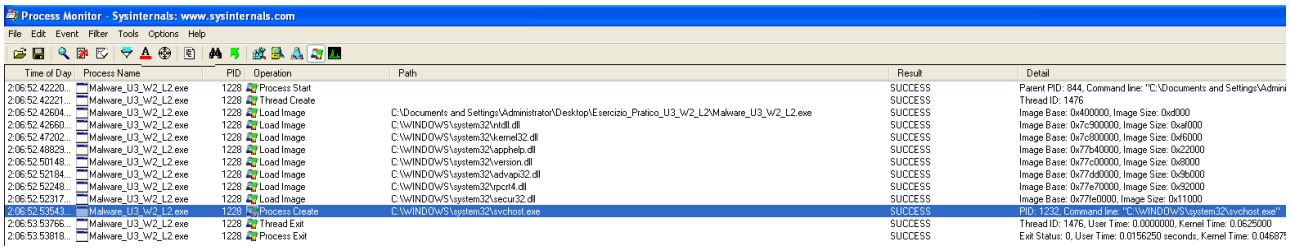


2. Identificazione azioni su Processi e Thread da parte del malware

Sempre con la stessa cattura, cliccando sull’icona precedente e sulla quart’ultima (che mostra i processi e i thread), si filtrano solo gli eventi dei processi e threas.

Innanzitutto, si possono notare funzioni come **Load Image** che viene utilizzata per «caricare» il malware per l’esecuzione e le librerie (.dll) a ciò necessarie.
In altri termini, Load Image" è una funzione fondamentale per inizializzare il malware in quanto consente al malware di caricare se se stesso e tutte le risorse necessarie per la sua esecuzione,.
In sintesi, grazie a questa funzione, il malware ha la possibilità di caricare e inizializzare sia se stesso che le librerie (.dll) richieste nel processo di esecuzione.

Poi, si nota una funzione «**Process Create**» che serve per creare un processo.
Sembra che il 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.



3. Conclusioni finali – Profilazione del malware

Le informazioni raccolte sulle azioni compiute dal malware, interagendo con il file system e i processi e thread, consentono di tentare una breve profilazione del malware.
In particolare, si ipotizza che, una volta in esecuzione, il malware cerchi di celare la propria presenza nascondendosi “dietro” un processo legittimo, detto “svchost.exe”, generato dal malware stesso.
Successivamente, sembra avviare la sua funzione principale, consistente in un keylogger atto a registrare i caratteri digitati dall'utente.
Tali informazioni vengono poi memorizzate in un file chiamato «practicalmalwareanalysis», appositamente creato nella stessa directory dell'eseguibile.