26/03/2024

ANALISI DINAMICA BASICA

Prepared by:
Manuel Buonanno

Organized by:
EPICODE

Indice

Traccia

Configurare la macchina virtuale per l'analisi dinamica (il malware sarà effettivamente eseguito). 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:

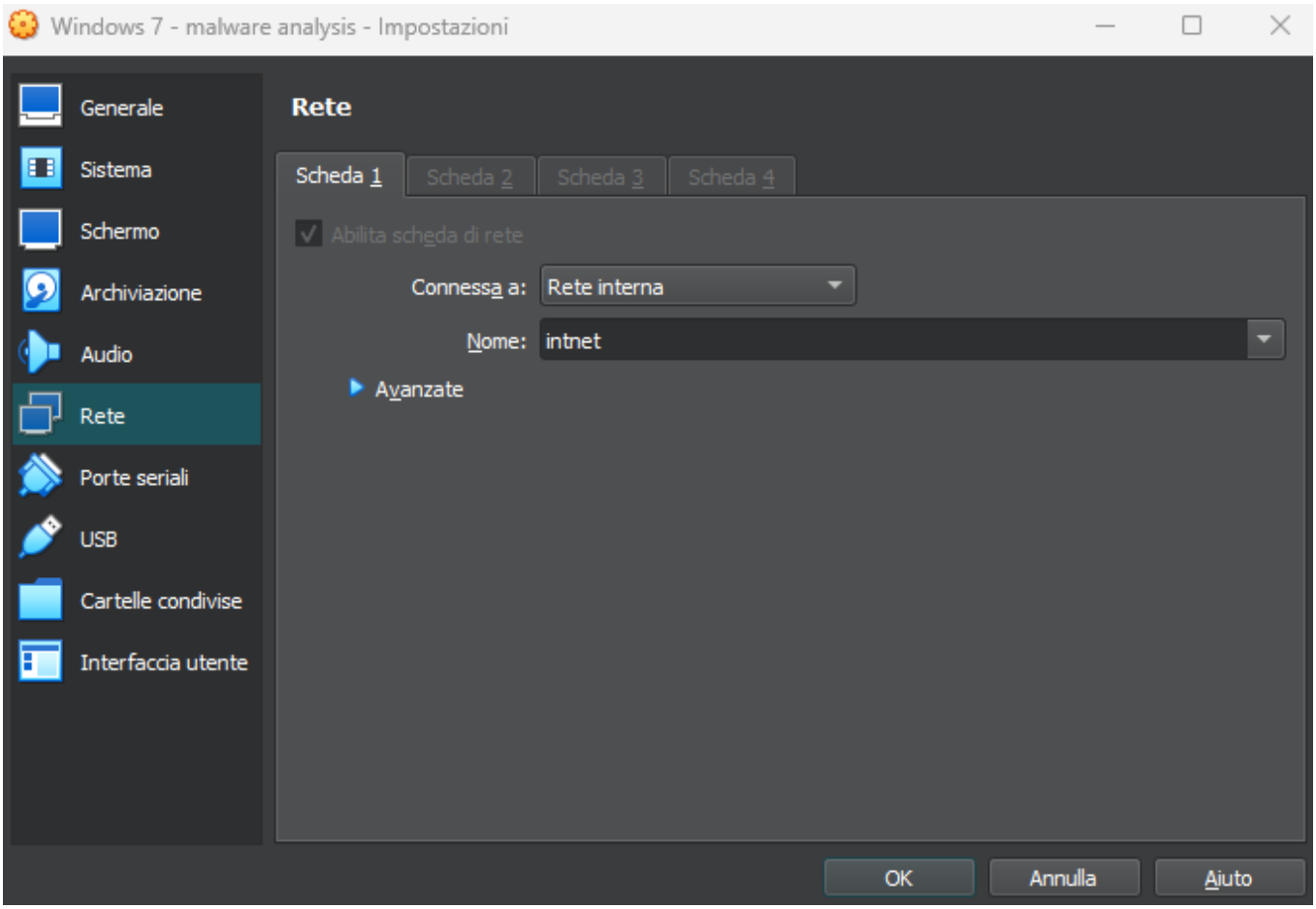
- Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon) .
- Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor .
- Modifiche del registro dopo il malware (le differenze) .
- Provare a profilare il malware in base alla correlazione 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). Creare istantanea da Virtualbox della macchina Windows 7 prima di avviare il malware per poter ripristinare in caso di problemi (o al limite fare il clone).

Configurazione macchina: rete

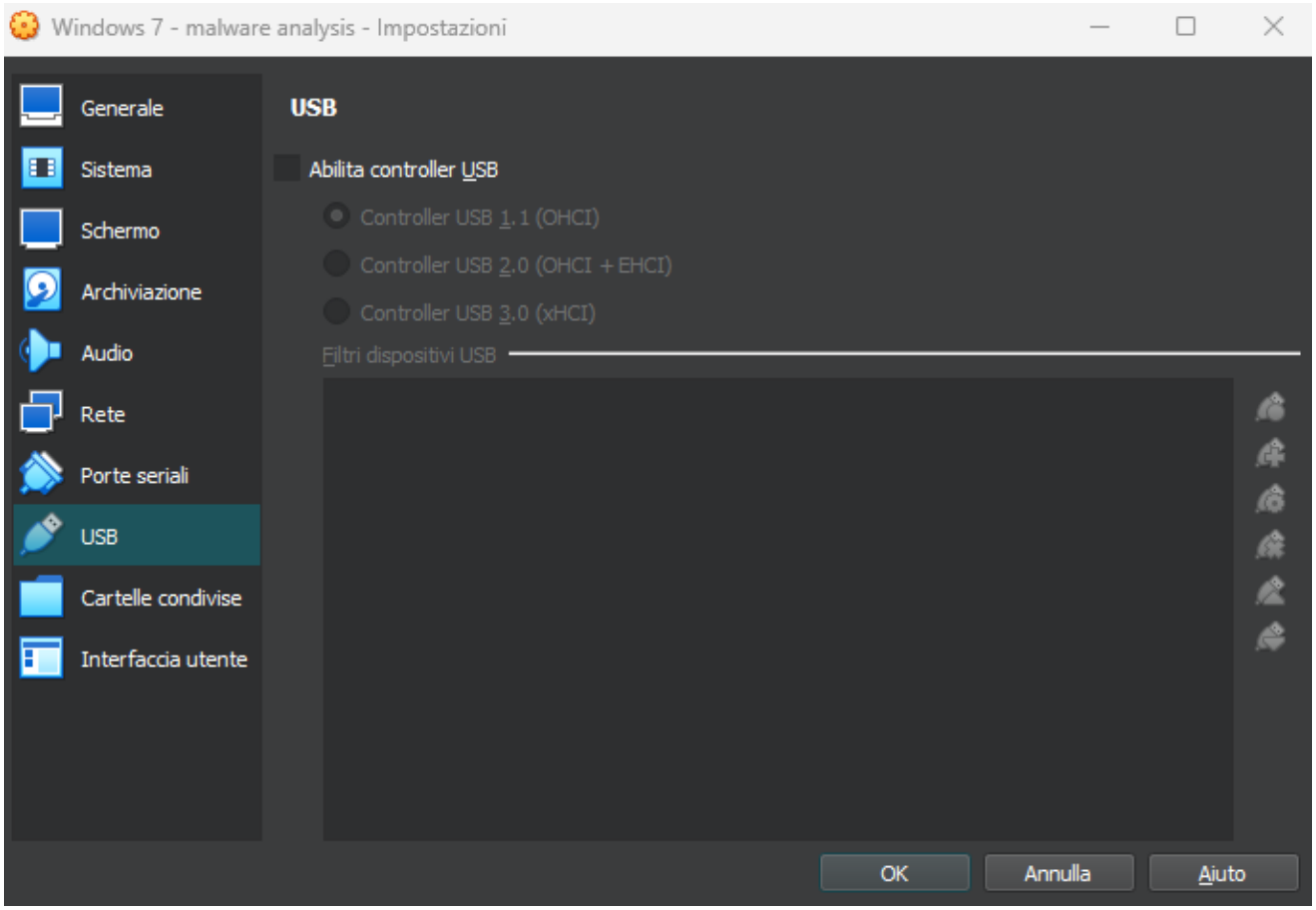
Prima di eseguire un ananlisi dinamica dobbiamo adottare delle pratiche per rendere sicuro il nostro ambiente.

1. Configurazione schede di rete: l'ambiente di test non deve avere accesso diretto ad Internet e preferibilmente nemmeno accesso ad altre macchine sulla rete. La configurazione ideale è: Eliminare le interfacce di rete durante l'analisi statica;
2. Abilitare un'interfaccia di rete interna (su VirtualBox viene chiamata «rete interna») per l'analisi dinamica. Questa impostazione è necessaria per monitorare il traffico che genera potenzialmente il malware.



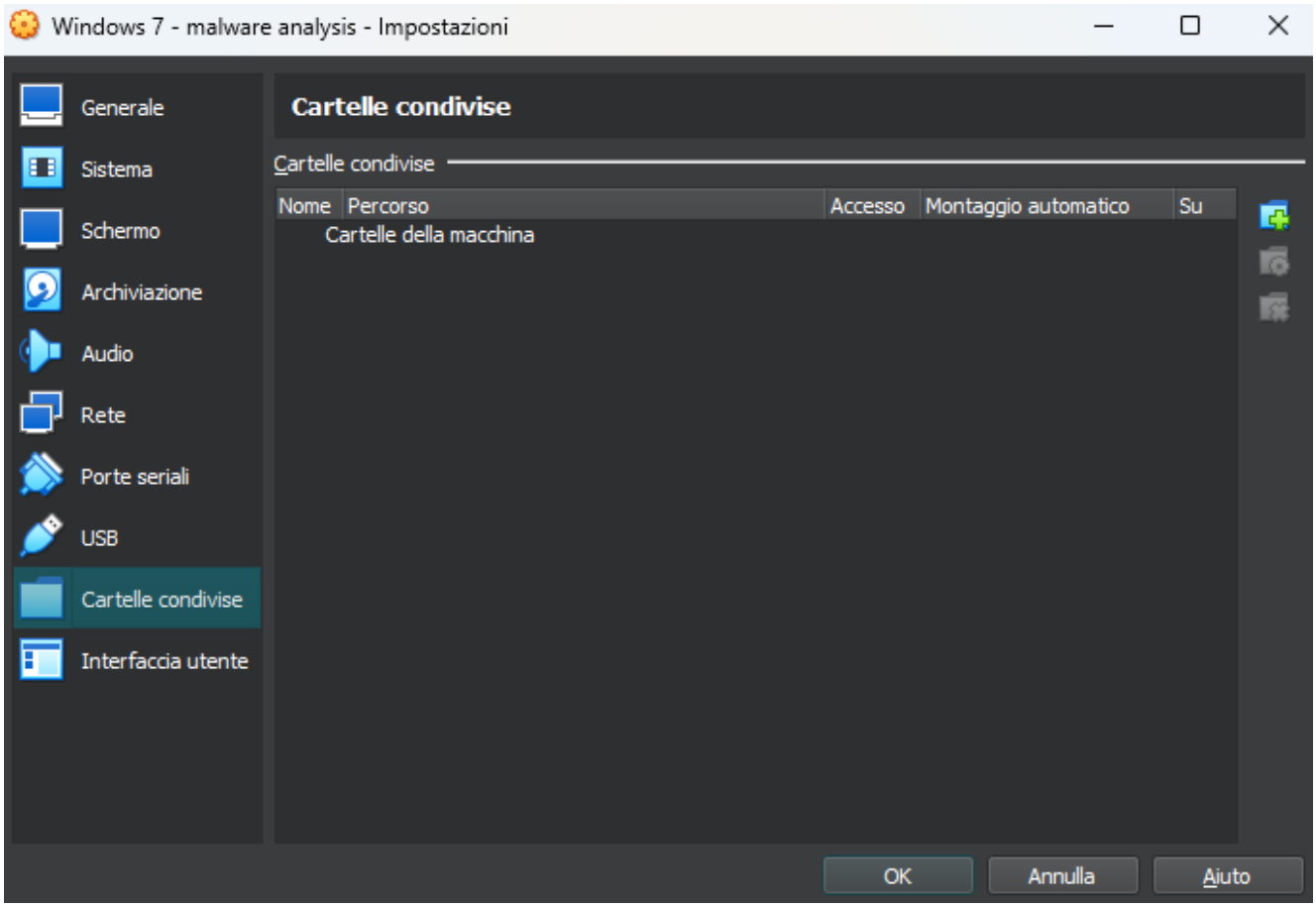
Configurazione macchina: USB

- Dispositivi USB: quando un dispositivo USB viene collegato alla macchina fisica, esso può essere riconosciuto anche dall'ambiente di test. Al fine di evitare questo comportamento, è buona pratica non abilitare o disabilitare il controller USB. Infatti, il malware potrebbe utilizzare il dispositivo USB per propagarsi poi sulla vostra macchina fisica. La figura di fianco mostra l'impostazione in VirtualBox, «abilita controller USB» NON deve essere abilitato.



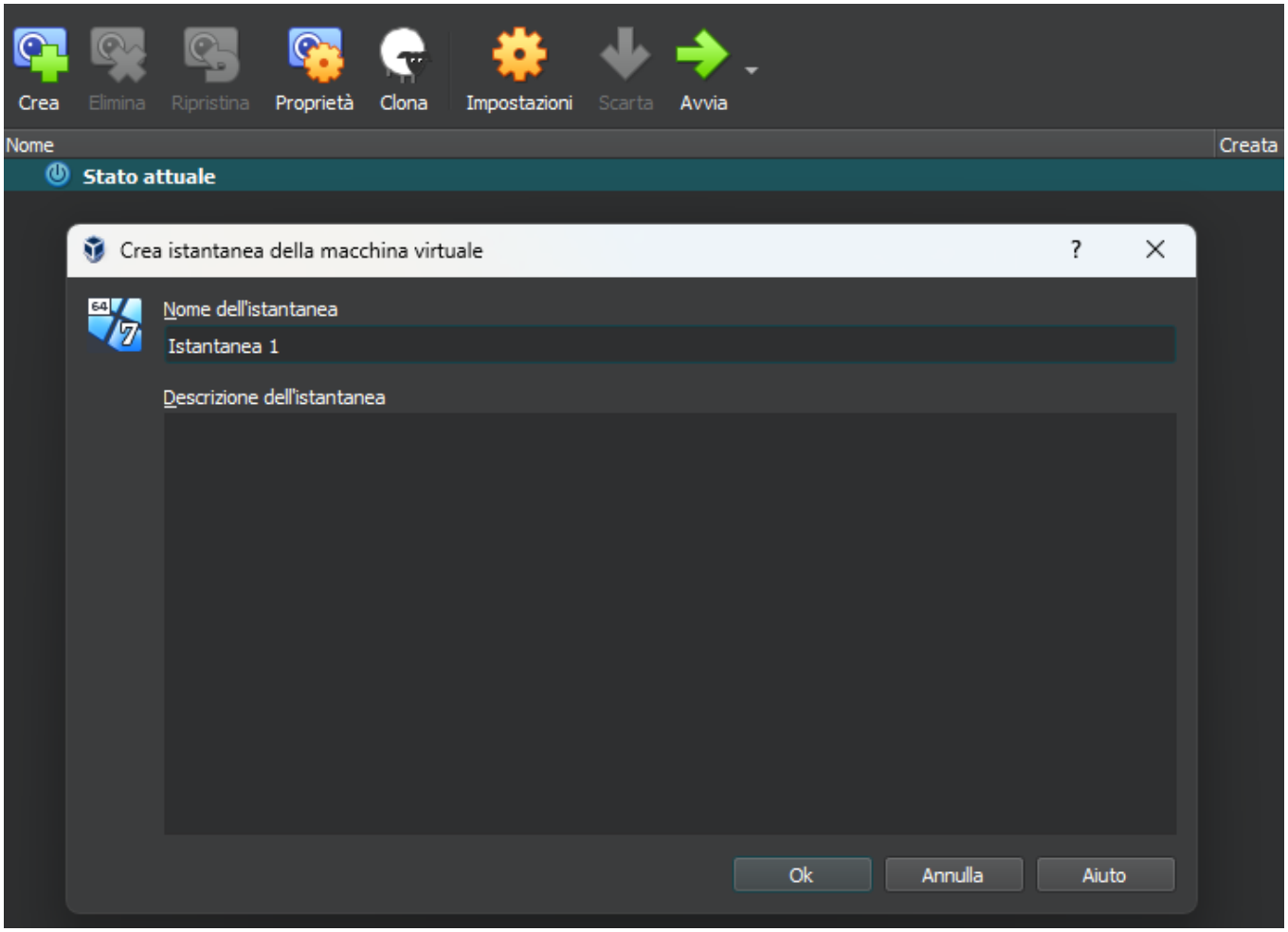
Configurazione macchina: cartelle condivise

- Cartelle condivise: stesso discorso può essere per le cartelle condivise tra la vostra macchina reale ed il laboratorio virtuale. Potrebbero essere utilizzate dal malware per propagarsi al di fuori del laboratorio causando danni alla vostra macchina e alle macchine sulla vostra rete domestica. Di conseguenza, è consigliato non condividere cartelle tra host e guest.



Configurazione macchina: istantanee

- Creare delle istantanee: Una buona pratica è creare delle istantanee della macchina virtuale nel suo stato iniziale, prima di iniziare tutte le analisi, in modo tale da ripristinarlo qualora ce ne fosse bisogno. Per creare un'istantanea, cliccate su «crea» (1), poi su OK (2) dopo aver inserito un nome ed una descrizione facoltativa.

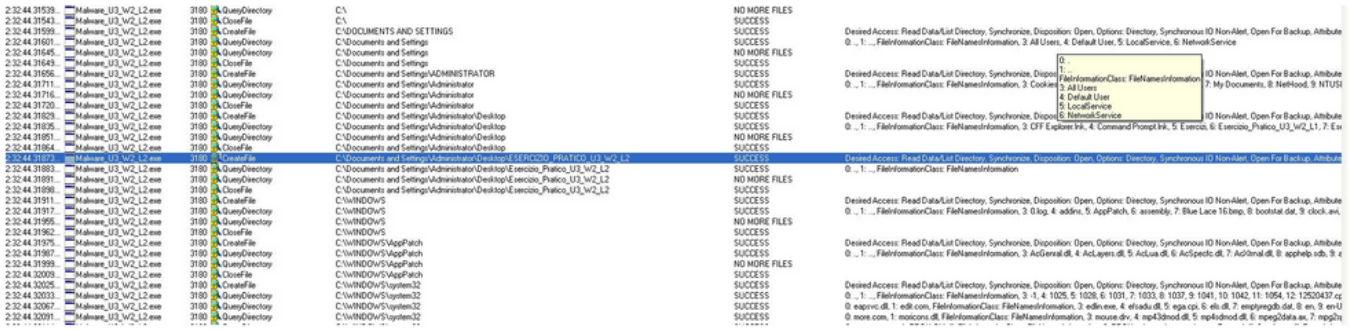


Se l'ambiente virtuale dovesse risultare compromesso, potete ripristinare l'istantanea cliccando sull'icona «ripristina» dopo averla selezionata dalla lista. Assicuratevi quindi di avviare la macchina avendo cura di selezionare «stato attuale» dalla lista.

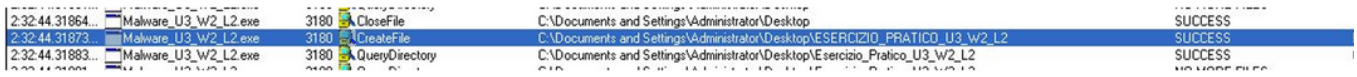
Avvio malware

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. (Il programma è stato installato su win7 ma ha una comptabilità migliore con winXP).

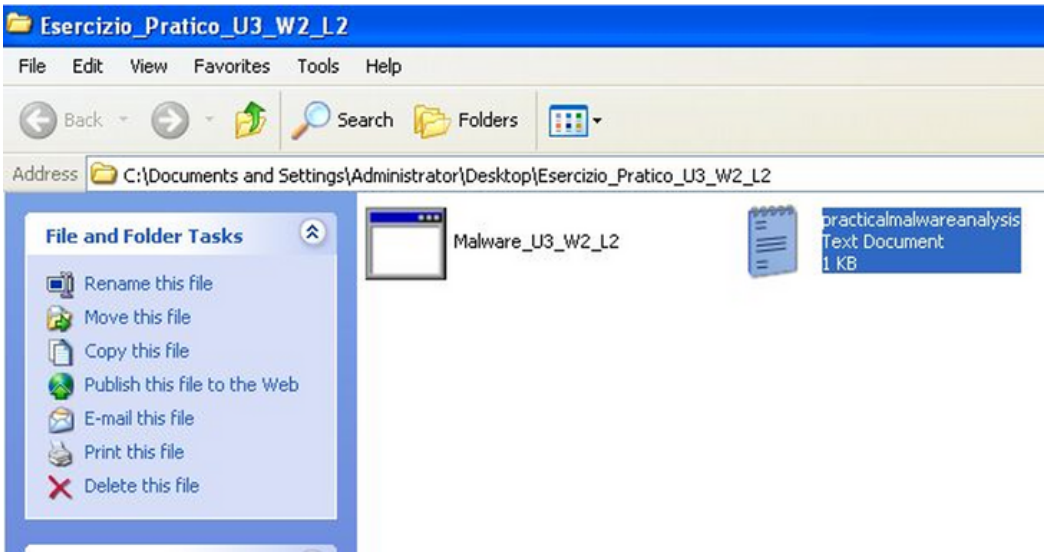
Inseriamo il filtro come visto in teoria per mostrare solo le attività del processo con nome «Malware_U3_W2_L2.exe. Vediamo subito dal report di procmon che ci sono delle funzioni riportate nella colonna «operation» molto interessanti come «Create File», «Read file» e «Close File» con rispettivo path.



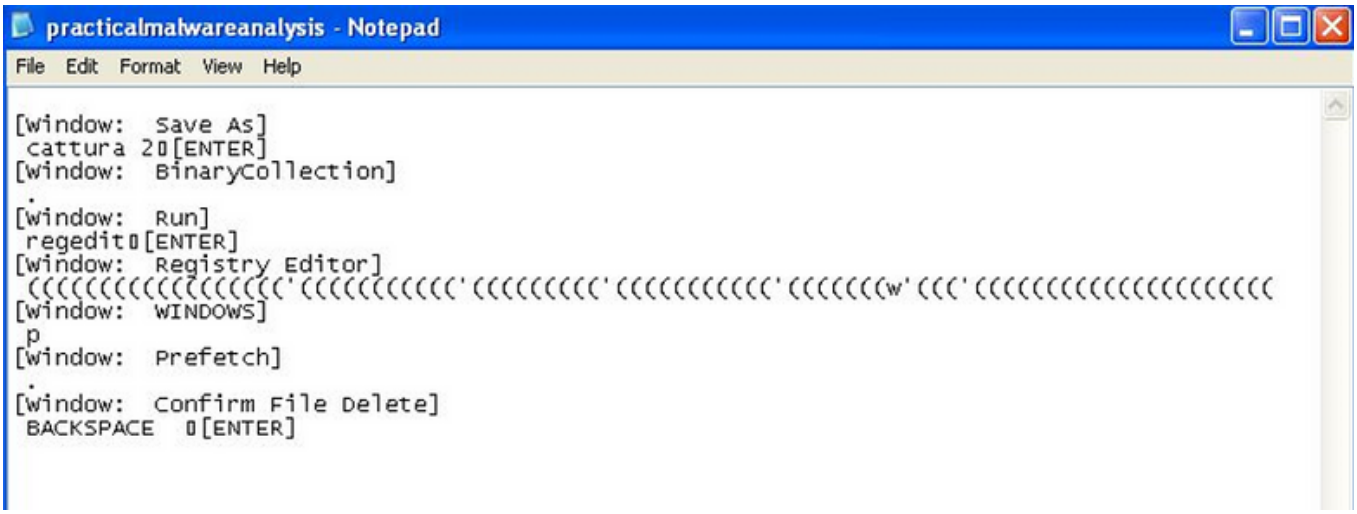
Procmon ci indica che è stato creato un file .txt nella cartella dove risiede il Malware.



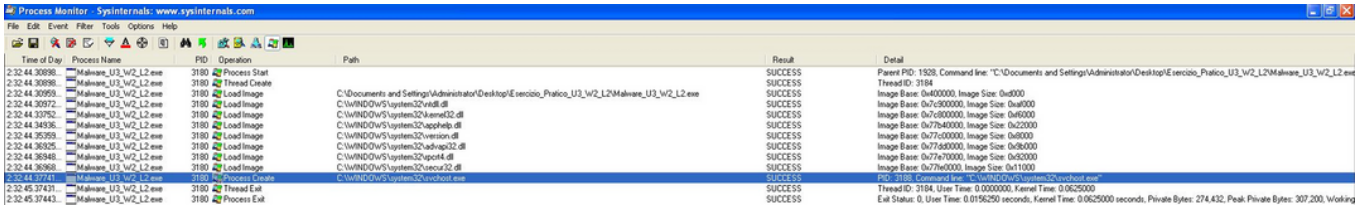
Apriamo la cartella sul desktop dove risiede l'eseguibile del malware per confermare che in effetti il malware ha creato un file denominato «practicalmalwareanalysis»



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.



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

Conclusioni

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.