

Analisi malware dinamica basica

Richiesta: Configurare la macchina per l’analisi dinamica, eseguire il malware L2 presente nella VM win7.

Rispondere ai seguenti quesiti:

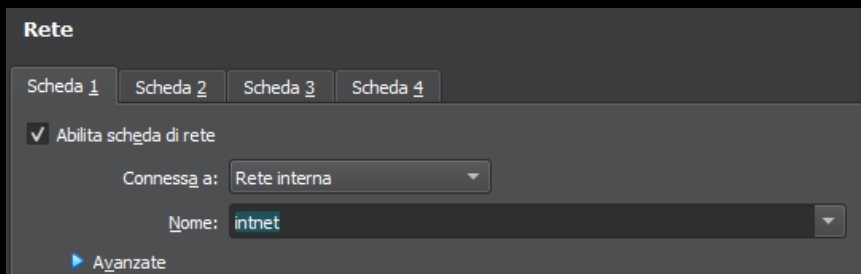
- 1. Identificare azioni del malware sul file system utilizzando process monitor
- 2. Identificare azioni del malware su processi e thread utilizzando process monitor
- 3. Modifiche del registro dopo il malware (le differenze)

Configurazione macchina

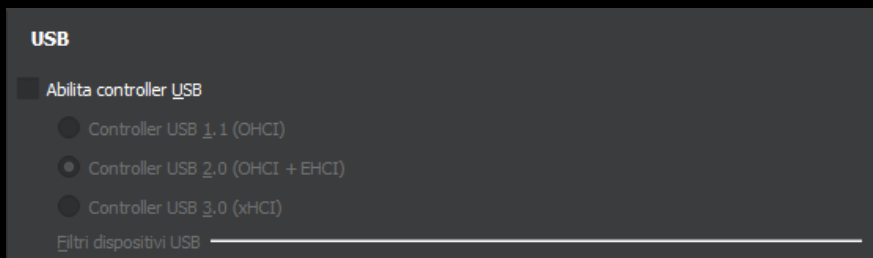
Prima di eseguire il malware, assicuriamoci di settare l’ambiente di test in maniera adeguata.

Procediamo attraverso le seguenti pratiche:

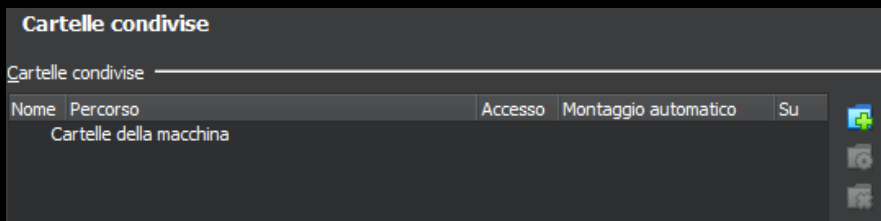
- 1. Configurazione scheda di rete: Impostiamo la macchina virtuale su rete interna, in modo da non comunicare con l’host reale.



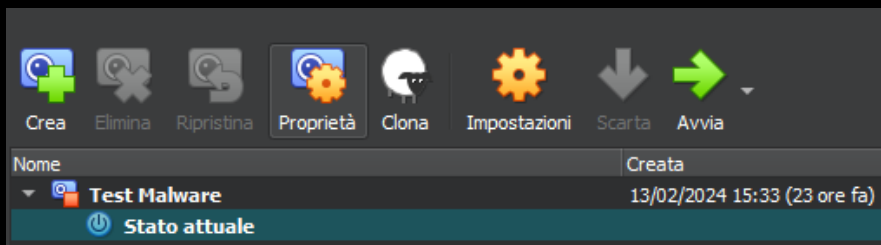
- 2. Disabilitare la possibilità di rilevare chiavette USB connesse alla macchina fisica.



- 3. Non condividere cartelle tra host e guest.



- 4. Creare delle istantanee prima dell’esecuzione del malware.



Esecuzione Malware

Una volta configurata la macchina virtuale, procediamo a lanciare il malware. Per l’analisi del malware utilizzeremo Process Monitor e Regshot.

Process Monitor: Tool avanzato per windows, permette di monitorare processi e thread attivi, l’attività di rete, l’accesso ai file e le chiamate di sistema effettuato su un sistema operativo.

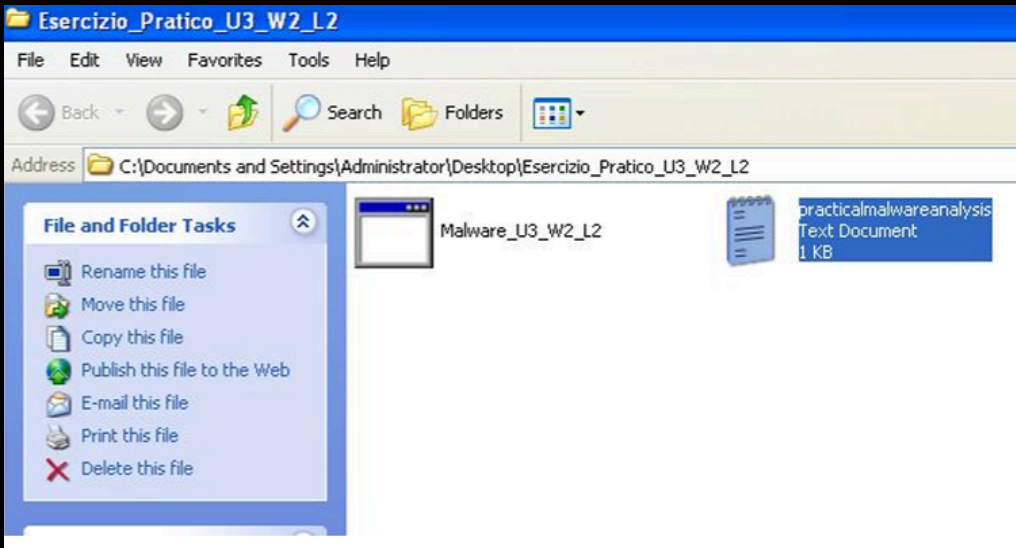
Regshot: Tool che permette di salvare un’istantanea delle chiave di registro, in modo da poter analizzare le differenze pre e post esecuzione malware.

Avviamo il malware e osserviamone le azioni attraverso Process Monitor. Inseriamo il filtro per mostrare solo le attività del malware.

2:32:44.31538	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\	NO MORE FILES	
2:32:44.31543	Malware_U3_W2_L2.exe	3180	CloseFile	C:\	SUCCESS	
2:32:44.31599	Malware_U3_W2_L2.exe	3180	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute
2:32:44.31601	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: ..., FileInformationClass: FileNameInformation, 3: All Users, 4: Default User, 5: LocalService, 6: NetworkService
2:32:44.31645	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
2:32:44.31649	Malware_U3_W2_L2.exe	3180	CloseFile	C:\Documents and Settings	SUCCESS	
2:32:44.31656	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute
2:32:44.31711	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0: ., 1: ..., FileInformationClass: FileNameInformation, 3: Cookies, 4: Default User, 5: LocalService, 6: NetworkService, 10 Non-Alert, Open For Backup, Attribute
2:32:44.31716	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
2:32:44.31720	Malware_U3_W2_L2.exe	3180	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
2:32:44.31829	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute
2:32:44.31835	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	0: ., 1: ..., FileInformationClass: FileNameInformation, 3: OFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio, 6: Esercizio_Pratico_U3_W2_L1, 7: Esercizio_Pratico_U3_W2_L2
2:32:44.31851	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
2:32:44.31864	Malware_U3_W2_L2.exe	3180	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
2:32:44.31872	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute
2:32:44.31883	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	0: ., 1: ..., FileInformationClass: FileNameInformation
2:32:44.31891	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
2:32:44.31898	Malware_U3_W2_L2.exe	3180	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
2:32:44.31911	Malware_U3_W2_L2.exe	3180	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute
2:32:44.31917	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1: ..., FileInformationClass: FileNameInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16.bmp, 8: bootstat.dat, 9: clock.avi

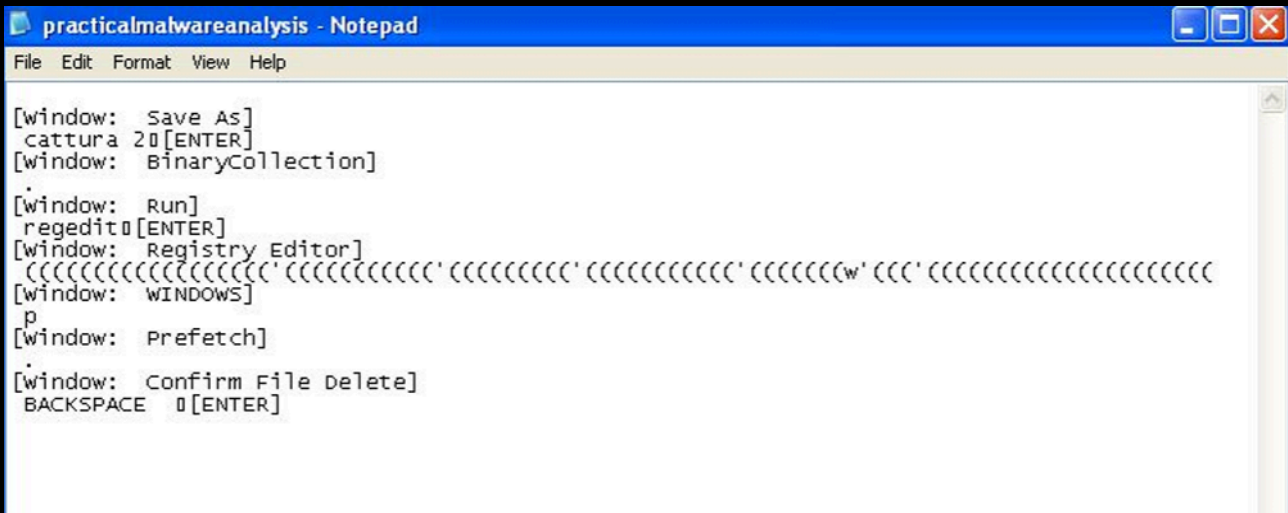
Notiamo che il malware nella sezione “operations” esegue azioni come create file, read file, close file, associate al path di corrispondenza. In particolare, l’azione evidenziata è molto curiosa, ci fa capire che esso ha creato un file.txt nella cartella dove risiede il malware.

Verifichiamo:



Il file.txt è stato effettivamente creato con successo (practicalmalwareanalysis).

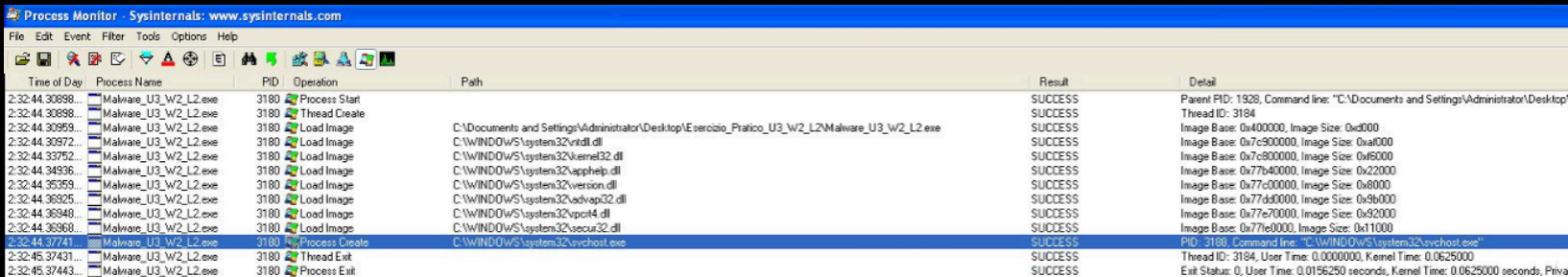
Osserviamone il contenuto:



Dalla lettura del file possiamo facilmente dedurre che si tratti di un **Keylogger**, un malware capace di registrare le digitazioni da parte della tua tastiera. Un malware reale avrebbe inviato i dati contenuti nel file direttamente ad una destinazione malevola, un possibile attaccante.

Identificazione processi e thread

Utilizzando Process Monitor, possiamo filtrare i processi e i thread avviati dal malware.



Notiamo come il malware utilizzi l’operazione load image per caricare l’esecuzione e le librerie necessarie per il funzionamento.

Troviamo Process Create che serve per creare un processo, in particolar modo possiamo osservare come crei un processo legittimo di windows “svchost.exe” in modo da camuffarsi come processo valido, per poi auto eliminarsi, in modo tale da rendere molto più difficile l’individuazione.