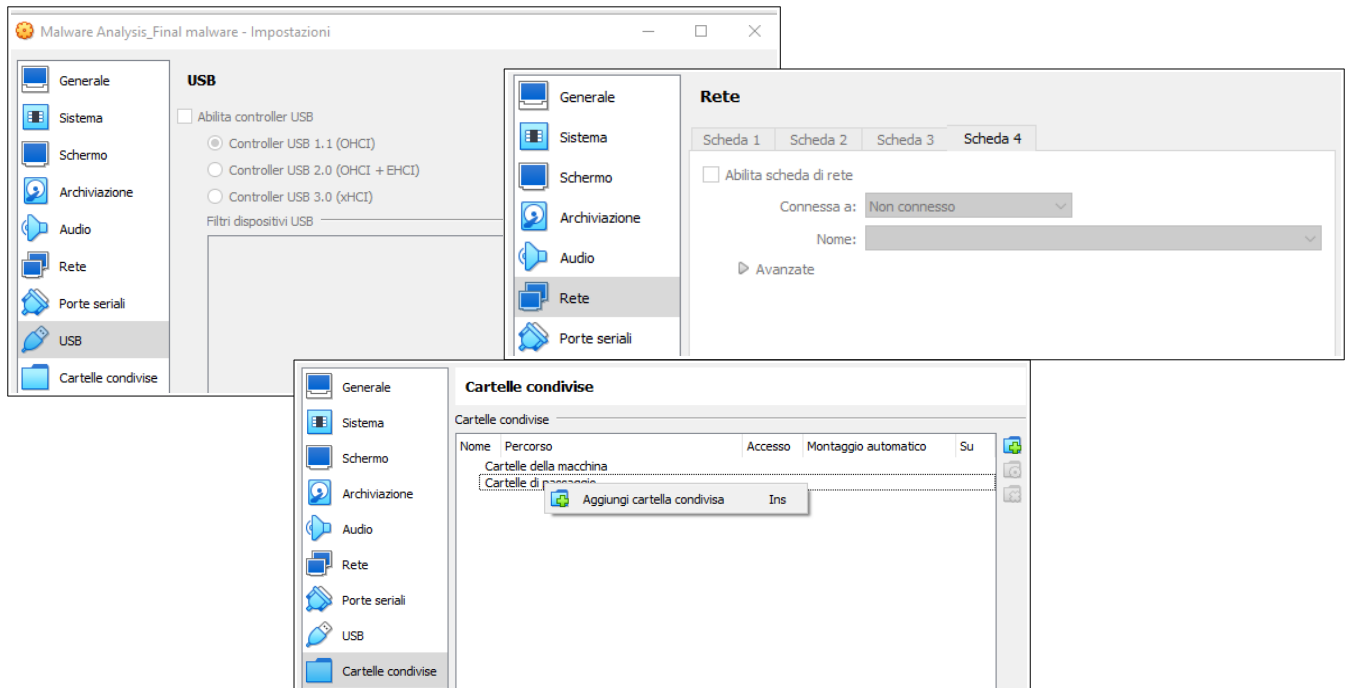


Analisi Dinamica Basica

Obiettivo: Effettuare un'analisi dinamica basica di un Malware su Windows XP 32 bit.

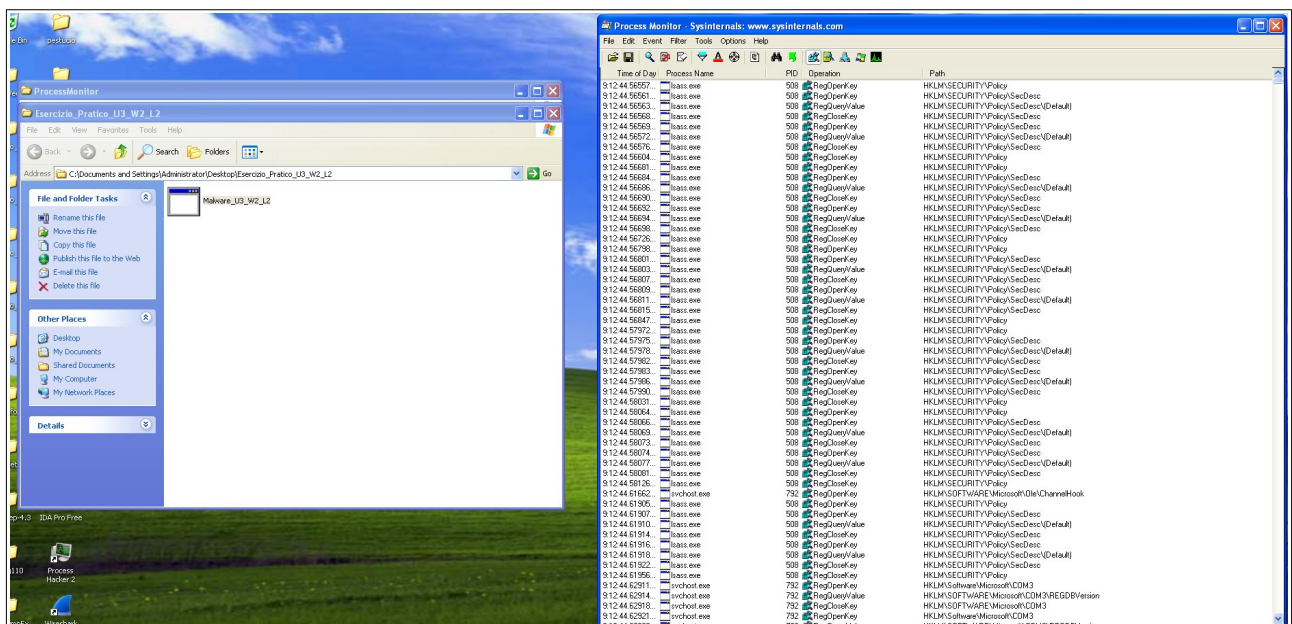
1) Macchina Offline

Prima di iniziare mi sono assicurato che la macchina virtuale fosse completamente *offline* e senza alcun collegamento con la macchina **Host Principale** controllando **Scheda di Rete Disattiva**, **Porte USB disattivate** e **Cartelle Condivise non collegate**.



2) Avvio ProcMon e Malware

La traccia chiede di utilizzare il tool **Process Monitor** per analizzare il comportamento del **Malware**. Per cominciare ho avviato il tool per poi cliccare sul file .exe che la traccia chiede.



1:15:14.14203.	Malware_U3_W2_L2.exe	1496	C:\Process Start	SUCCESS
1:15:14.14204.	Malware_U3_W2_L2.exe	1496	C:\Thread Create	SUCCESS
1:15:14.14384.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS
1:15:14.14414.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS
1:15:14.14440.	Malware_U3_W2_L2.exe	1496	C:\WINDOWS\system32\cmd.dll	SUCCESS
1:15:14.14444.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS
1:15:14.14475.	Malware_U3_W2_L2.exe	1496	C:\WINDOWS\system32\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
1:15:14.14480.	Malware_U3_W2_L2.exe	1496	C:\WINDOWS\system32\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
1:15:14.14505.	Malware_U3_W2_L2.exe	1496	C:\WINDOWS\system32\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
1:15:14.14902.	Malware_U3_W2_L2.exe	1496	C:\CloseFile	
1:15:14.14908.	Malware_U3_W2_L2.exe	1496	C:\CreateFile	
1:15:14.14913.	Malware_U3_W2_L2.exe	1496	C:\QueryInformationVolume	
1:15:14.14920.	Malware_U3_W2_L2.exe	1496	C:\FileSystemControl	
1:15:14.15406.	Malware_U3_W2_L2.exe	1496	C:\CreateFile	
1:15:14.15411.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	
1:15:14.15422.	Malware_U3_W2_L2.exe	1496	C:\CloseFile	
1:15:14.15581.	Malware_U3_W2_L2.exe	1496	C:\CloseFile	
1:15:14.15934.	Malware_U3_W2_L2.exe	1496	C:\DOCUMENTS AND SETTINGS	
1:15:14.15938.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings	
1:15:14.15948.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings	
1:15:14.16138.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings	
1:15:14.16151.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings	
1:15:14.16155.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings	
1:15:14.16399.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings	
1:15:14.16411.	Malware_U3_W2_L2.exe	1496	C:\CloseFile	
1:15:14.16737.	Malware_U3_W2_L2.exe	1496	C:\CreateFile	
1:15:14.16747.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	
1:15:14.16764.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	
1:15:14.17159.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings	
1:15:14.17185.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings	
1:15:14.17206.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings	
1:15:14.17463.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE
1:15:14.17479.	Malware_U3_W2_L2.exe	1496	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
1:15:14.17637.	Malware_U3_W2_L2.exe	1496	C:\CreateFile	SUCCESS
1:15:14.17707.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	SUCCESS
1:15:14.17727.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	NO MORE
1:15:14.17936.	Malware_U3_W2_L2.exe	1496	C:\CloseFile	SUCCESS
1:15:14.17961.	Malware_U3_W2_L2.exe	1496	C:\CreateFile	SUCCESS
1:15:14.17976.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	SUCCESS
1:15:14.18271.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	SUCCESS
1:15:14.18280.	Malware_U3_W2_L2.exe	1496	C:\CloseFile	NO MORE
1:15:14.18417.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	SUCCESS
1:15:14.18435.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	SUCCESS
1:15:14.18471.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	SUCCESS
1:15:14.18643.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	SUCCESS
1:15:14.18678.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	SUCCESS
1:15:14.19204.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	SUCCESS
1:15:14.19332.	Malware_U3_W2_L2.exe	1496	C:\QueryDirectory	NO MORE
1:15:14.19352.	Malware_U3_W2_L2.exe	1496	C:\CloseFile	SUCCESS
1:15:14.19497.	Malware_U3_W2_L2.exe	1496	C:\CreateFile	SUCCESS
1:15:14.19518.	Malware_U3_W2_L2.exe	1496	C:\CreateFileMapping	SUCCESS
1:15:14.19520.	Malware_U3_W2_L2.exe	1496	C:\QueryStandarInformationFile	SUCCESS
1:15:14.19524.	Malware_U3_W2_L2.exe	1496	C:\CreateFileMapping	SUCCESS
1:15:14.19554.	Malware_U3_W2_L2.exe	1496	C:\CreateFile	SUCCESS

3) Eventi di Registro

[illegible]

- **Elencare** le Chiavi di Registro in una Directory (**RegEnumKey**);
- **Aprire** le Chiavi sopracitate, o tentare almeno di aprirle (**RegOpenKey**);
- **Interrogare** le Chiavi stesse per ottenerne i valori specifici (**RegQueryValue**).

Permettere ad un Malware di leggere le **Chiavi di Registro** è molto pericoloso; potrebbe ottenere l'accesso ad informazioni sensibili o compromettere le impostazioni di sicurezza del Sistema.

4) File System

Il secondo *switch* mostra invece attività relative ai **File System** di **Windows**.

[illegible]

Nella prima parte dell'analisi il Malware crea o importa le librerie di cui ha bisogno per funzionare e per interagire col Sistema Operativo (**kernel32**), con i Registri (**advapi32.dll**), con la gestione delle Operazioni di sicurezza (**secur32.dll**) e altre.

15:14:23.05	Malware_U3_V2_L2_en	1496	C:\Windows\System32\cmd.exe	Read Attributes: Disposition: Open; Options: Non-Destructive File; Attributes: N; ShowMetadata: Read; SyncType: SyncTypeCreateNew, PageProtection: PAGE_READWRITE	SUCCESS	Desired Access: ReadDataList; Read Attributes: Disposition: Open; Options: Non-Destructive File; Attributes: N; ShowMetadata: Read; SyncType: SyncTypeCreateNew, PageProtection: PAGE_READWRITE
15:14:23.05	Malware_U3_V2_L2_en	1498	C:\Windows\System32\cmd.exe	Allocate 5148; EndOfFile: 51472; NumberLinks: 1; DeletePending: False; Directory: False	SUCCESS	Allocation: 5148; EndOfFile: 51472; NumberLinks: 1; DeletePending: False; Directory: False
15:14:23.67	Malware_U3_V2_L2_en	1499	C:\Windows\System32\cmd.exe	SyncType: SyncType	SUCCESS	SyncType: SyncType
15:14:23.67	Malware_U3_V2_L2_en	1500	C:\Windows\System32\cmd.exe	Desired Access: ReadDataList; Read Attributes: Disposition: Open; Options: Non-Destructive File; Attributes: N; ShowMetadata: Read; SyncType: SyncTypeCreateNew, PageProtection: PAGE_READWRITE	SUCCESS	Desired Access: ReadDataList; Read Attributes: Disposition: Open; Options: Non-Destructive File; Attributes: N; ShowMetadata: Read; SyncType: SyncTypeCreateNew, PageProtection: PAGE_READWRITE
15:14:23.67	Malware_U3_V2_L2_en	1501	C:\Windows\System32\cmd.exe	Allocate 59520; EndOfFile: 59470; NumberLinks: 1; DeletePending: False; Directory: False	SUCCESS	Allocation: 59520; EndOfFile: 59470; NumberLinks: 1; DeletePending: False; Directory: False
15:14:23.67	Malware_U3_V2_L2_en	1502	C:\Windows\System32\cmd.exe	SyncType: SyncType	SUCCESS	SyncType: SyncType
15:14:23.67	Malware_U3_V2_L2_en	1503	C:\Windows\System32\cmd.exe	Desired Access: ReadDataList; Read Attributes: Disposition: Open; Options: Non-Destructive File; Attributes: N; ShowMetadata: Read; SyncType: SyncTypeCreateNew, PageProtection: PAGE_READWRITE	SUCCESS	Desired Access: ReadDataList; Read Attributes: Disposition: Open; Options: Non-Destructive File; Attributes: N; ShowMetadata: Read; SyncType: SyncTypeCreateNew, PageProtection: PAGE_READWRITE
15:14:23.67	Malware_U3_V2_L2_en	1504	C:\Windows\System32\cmd.exe	Allocate 97344; EndOfFile: 96320; NumberLinks: 1; DeletePending: False; Directory: False	SUCCESS	Allocation: 97344; EndOfFile: 96320; NumberLinks: 1; DeletePending: False; Directory: False
15:14:23.67	Malware_U3_V2_L2_en	1505	C:\Windows\System32\cmd.exe	SyncType: SyncType	SUCCESS	SyncType: SyncType

Nella seconda parte dell'analisi invece il **Malware** crea e "killa" il processo **svchost.exe**, probabilmente per mascherare le modifiche che vuole effettuare al Sistema o sfruttare il processo legittimo per eseguire il proprio codice malevolo.

[illegible]

5) Flussi di Rete

Il terzo *switch* elenca le attività che vengono svolte sulla Rete da parte del **Malware**; nell'analisi effettuata non ci sono attività di questo tipo.

The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains icons for file operations, search, and process management. The main display area shows a list of events. The columns are Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The events listed are all related to svchost.exe and involve UDP network operations.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
9:13:31.20869...	svchost.exe	904	UDP Receive	239.255.255.250:1900 -> localhost:1028	SUCCESS	Length: 133
9:13:31.20870...	svchost.exe	828	UDP Send	localhost:1028 -> 239.255.255.250:1900	SUCCESS	Length: 133
9:13:34.20865...	svchost.exe	828	UDP Receive	239.255.255.250:1900 -> localhost:1028	SUCCESS	Length: 133
9:13:34.20867...	svchost.exe	828	UDP Send	localhost:1028 -> 239.255.255.250:1900	SUCCESS	Length: 133
9:13:37.20872...	svchost.exe	904	UDP Receive	239.255.255.250:1900 -> localhost:1028	SUCCESS	Length: 133
9:13:37.20873...	svchost.exe	828	UDP Send	localhost:1028 -> 239.255.255.250:1900	SUCCESS	Length: 133
9:13:40.20864...	svchost.exe	828	UDP Receive	localhost:1028 -> localhost:1028	SUCCESS	Length: 1
9:13:40.20865...	svchost.exe	828	UDP Send	localhost:1028 -> localhost:1028	SUCCESS	Length: 1

6) Processi e Thread

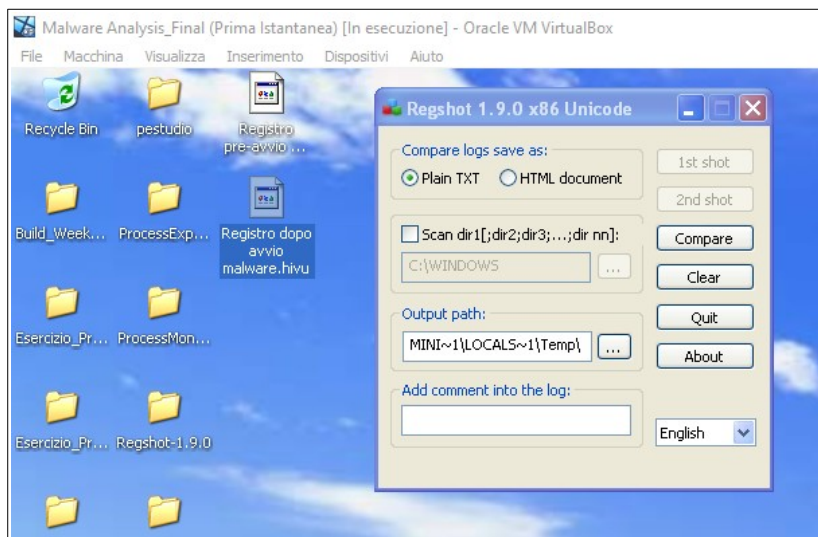
Il quarto *switch* mostra le attività relative ai **Processi e Thread** che il **Malware** avvia o meno.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:54:14.003	Malware_U3_W2_L2.exe	1496	Process Start		SUCCESS	Parent PID: 248, Command Line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe"
11:54:14.004	Malware_U3_W2_L2.exe	1496	SUCCESS		SUCCESS	Thread ID: 168
11:54:14.014	Malware_U3_W2_L2.exe	1496	Thread Create	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x0000
11:54:14.040	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\user32.dll	SUCCESS	Image Base: 0x780000, Image Size: 0x40000
11:54:15.057	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\ole32.dll	SUCCESS	Image Base: 0x780000, Image Size: 0x40000
11:54:15.076	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\gdi32.dll	SUCCESS	Image Base: 0x780000, Image Size: 0x20000
11:54:15.276	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\user32.dll	SUCCESS	Image Base: 0x780000, Image Size: 0x40000
11:54:15.282	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\advapi32.dll	SUCCESS	Image Base: 0x780000, Image Size: 0x40000
11:54:15.301	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\user32.dll	SUCCESS	Image Base: 0x780000, Image Size: 0x40000
11:54:15.301	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\advapi32.dll	SUCCESS	Image Base: 0x780000, Image Size: 0x40000
11:54:15.310	Malware_U3_W2_L2.exe	1496	Process Create		SUCCESS	Parent PID: 1496, Command Line: "C:\WINDOWS\System32\cmd.exe"
11:54:15.310	Malware_U3_W2_L2.exe	1496	Process Create		SUCCESS	Parent PID: 1496, Command Line: "C:\WINDOWS\System32\cmd.exe"
11:54:15.325	Malware_U3_W2_L2.exe	1496	Process Exit		SUCCESS	Exit Status: 0, CPU Time: 0.000000s, Private Bytes: 274,432, Peak Private Bytes: 307,200, Working Set: 16,896, User Time: 0.000000s, System Time: 0.000000s

Si possono notare i caricamenti delle varie librerie (alcune viste prima) e la creazione del processo **svchost.exe** sopracitato dal momento che viene avviato per poi “killarsi” automaticamente.

7) Modifiche del Registro

Grazie al tool **Regshot** si possono creare delle *Istantanee* pre e dopo l'avviamento di un **Malware** per poterle confrontare e osservare le modifiche che vengono eseguite sulle **Chiavi di Registro**.



Salvando il 1st (*pre-avvio Malware*) e 2nd shot (*post avvio Malware*) possiamo grazie al tool confrontarli in un file di testo che potremo successivamente salvare dove vogliamo.



Ci sono stati da come leggiamo *30 modifiche* alle **Chiavi di Registro** con relativi **Path**.

8) Conclusioni

Alla luce dei risultati della scansione con **Process Monitor** e con **Regshot** posso supporre che questo **Malware** crei una serie di Processi **svchost.exe** per poi “killarli”. Ogni processo creato probabilmente apporta ognuno delle modifiche al **Registro di Sistema** e poi si chiude per non farsi scoprire dal **Sistema**.