



26/03/2024

Analisi dinamica basica

Prepared by:
Manuel Buonanno

Organized by:



Indice

1) Traccia.....	3
1.1) Configurazione macchina base.....	4
1.2) Configurazione macchina base usb.....	5
1.3) Configurazione macchina base cartelle condivise.....	6
1.4) Configurazione macchina base istantanee.....	7
2) Avvio malware.....	8
2.1) practicalmalwareanalysis.....	9
2.2) svchost.exe.....	10
3) Conclusioni.....	11

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.

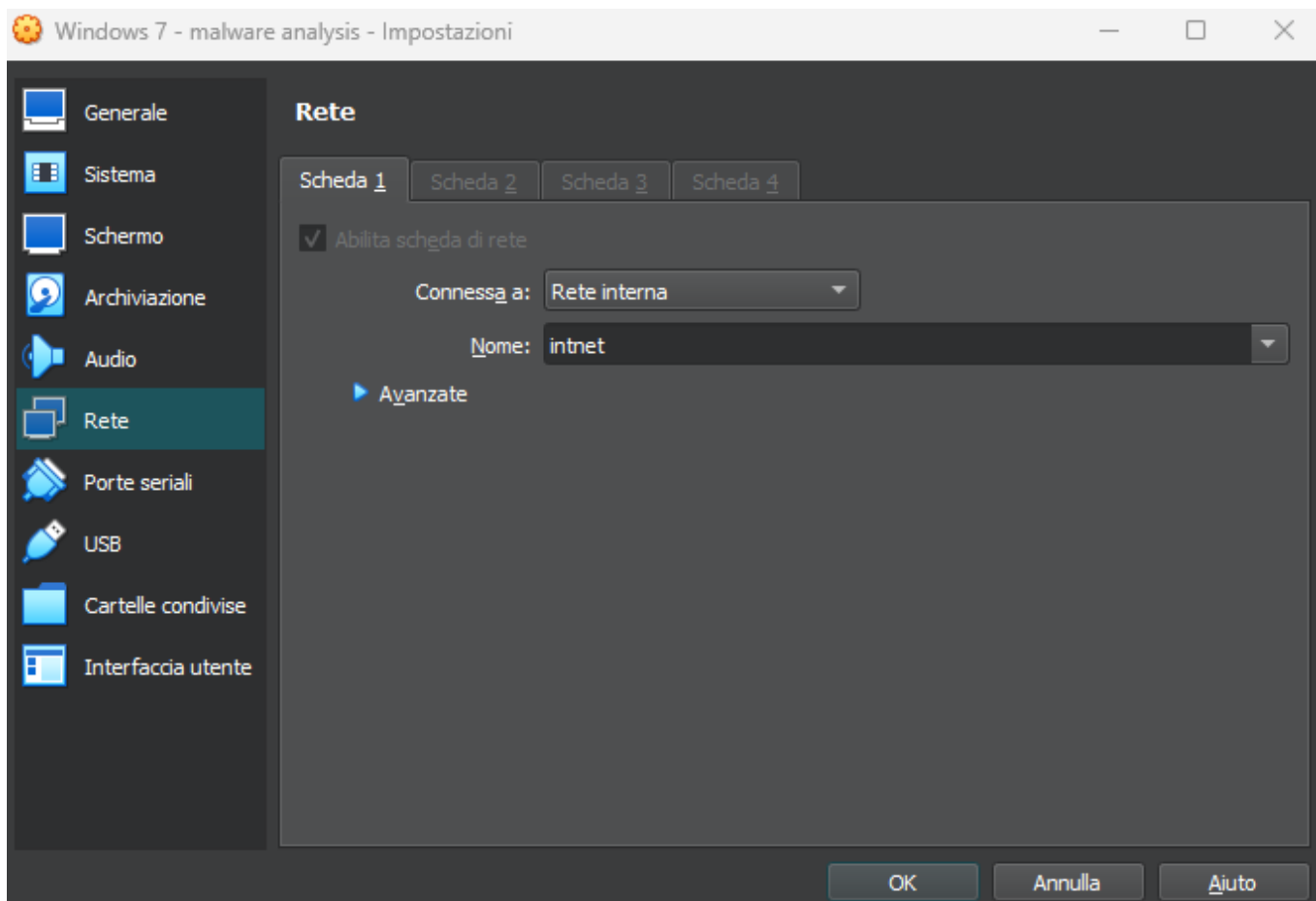
Suggerimento:

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

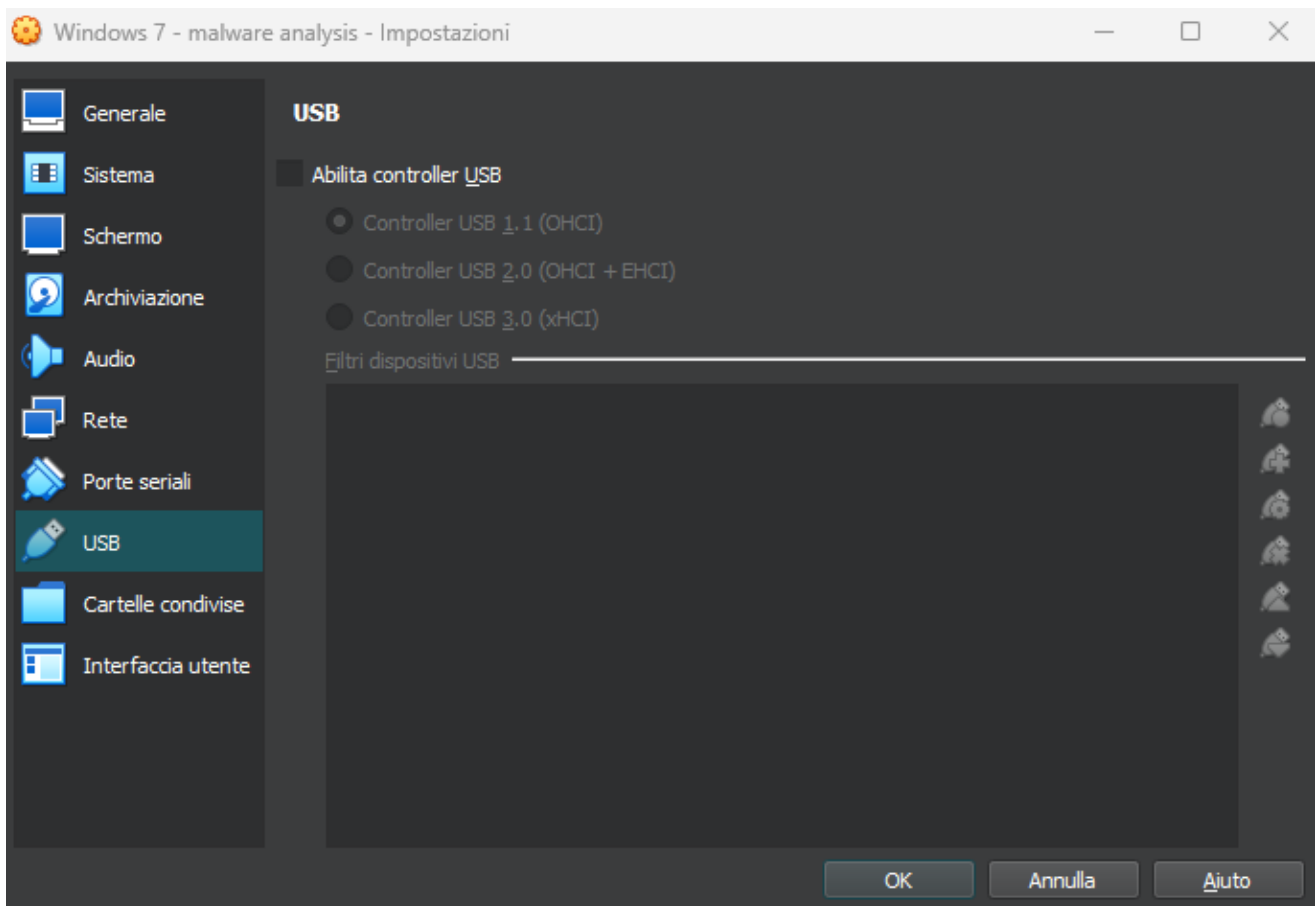
Prima di eseguire un'analisi dinamica dobbiamo adottare delle pratiche per rendere sicuro il nostro ambiente.

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.



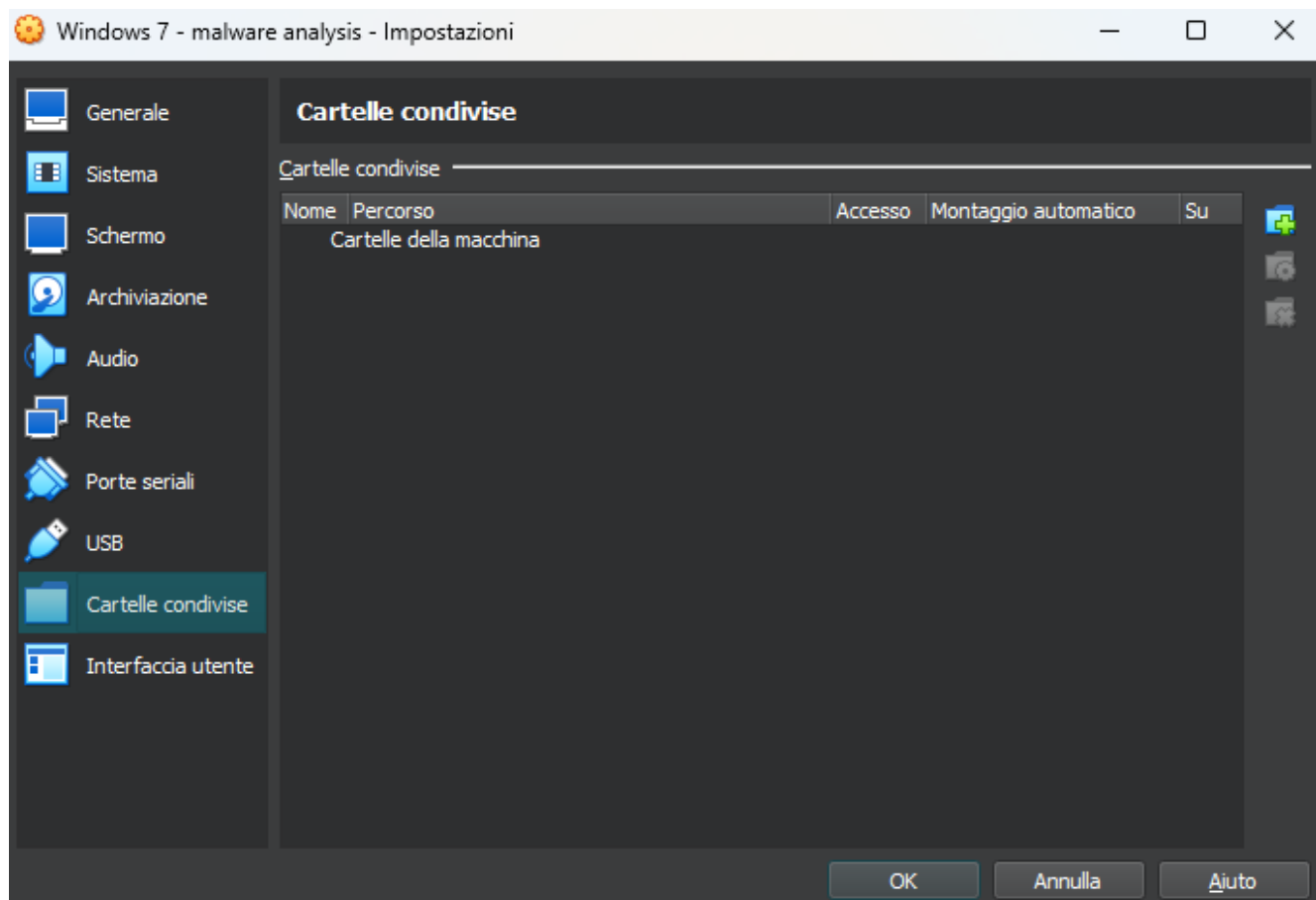
Configurazione macchina: USB

- 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.



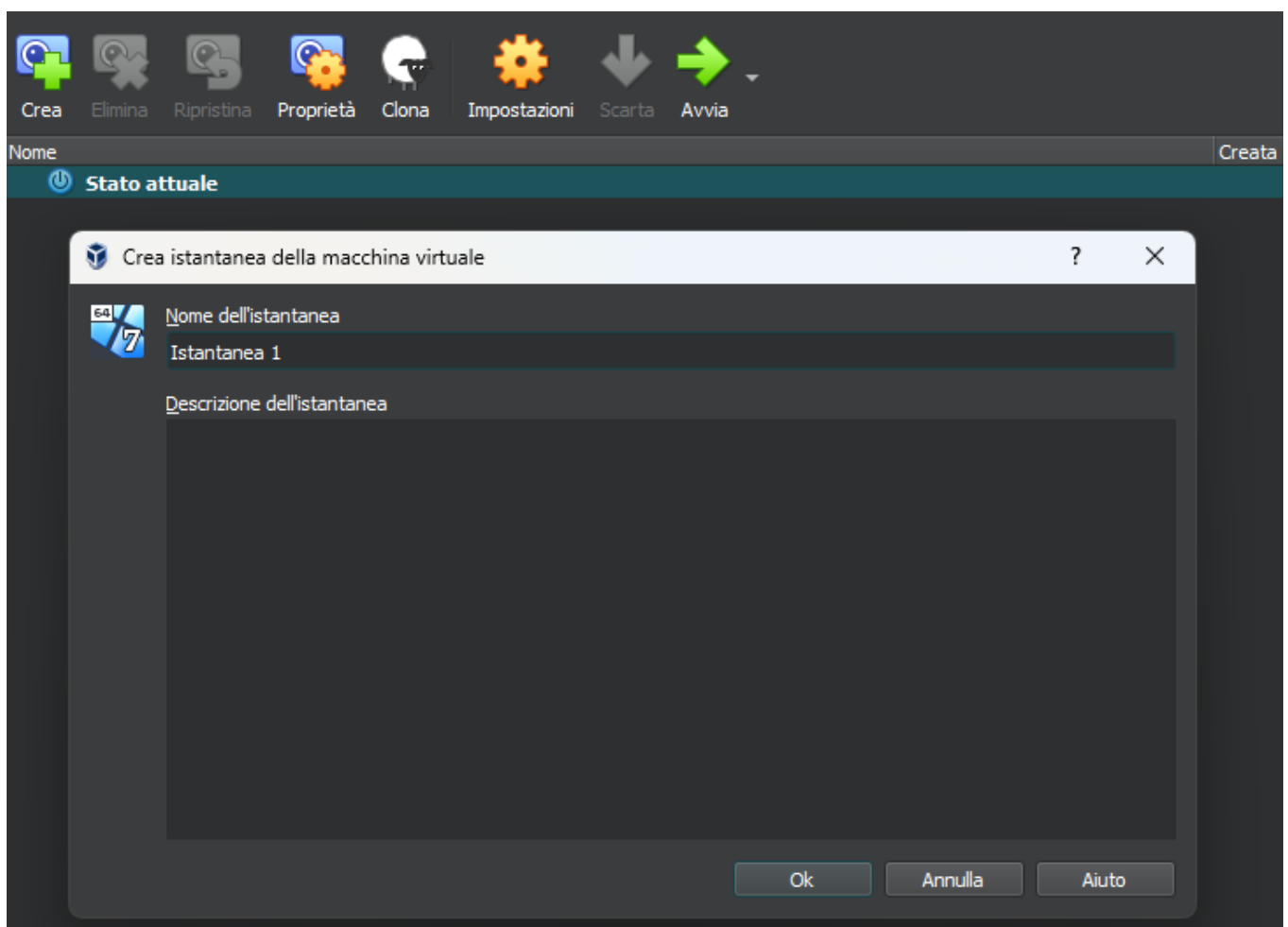
Configurazione macchina: cartelle condivise

- 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'istananea, cliccate su «crea» (1), poi su OK (2) dopo aver inserito un nome ed una descrizione facoltativa.

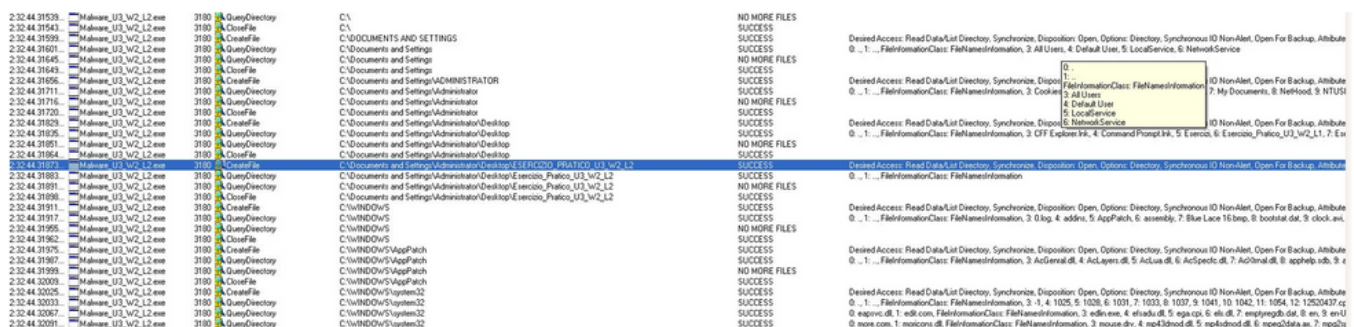


Se l'ambiente virtuale dovesse risultare compromesso, potete ripristinare l'istananea cliccando sull'icona «ripristina» dopo averla selezionata dalla lista. Assicuratevi quindi di avviare la macchina avendo cura di selezionare «stato attuale» dalla lista.

Avvio malware

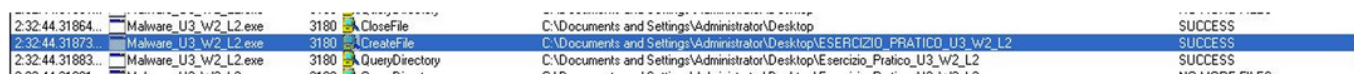
Per prima cosa, facciamo partire Procmon prima di eseguire il malware, successivamente avviamo il malware e dopo un lasso di tempo di circa 1 minuto stoppiamo la cattura Procmon, cliccando sull'icona a forma di lente nel rettangolo rosso in figura. (Il programma è stato installato su win7 ma ha una comptabilità 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.



2:32:44.31539...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\	NO MORE FILES
2:32:44.31543...	Malware_U3_W2_L2.exe	3180	CloseFile	C:\	SUCCESS
2:32:44.31559...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS
2:32:44.31601...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings	SUCCESS
2:32:44.31645...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings	NO MORE FILES
2:32:44.31643...	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
2:32:44.31711...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS
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
2:32:44.31825...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS
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
2:32:44.31883...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	NO MORE FILES
2:32:44.31891...	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
2:32:44.31917...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS	SUCCESS
2:32:44.31955...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS	NO MORE FILES
2:32:44.31962...	Malware_U3_W2_L2.exe	3180	CloseFile	C:\WINDOWS	SUCCESS
2:32:44.31975...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\SoftwarePatch	SUCCESS
2:32:44.31987...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\WINDOWS\SoftwarePatch	SUCCESS
2:32:44.31999...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\SoftwarePatch	NO MORE FILES
2:32:44.32003...	Malware_U3_W2_L2.exe	3180	CloseFile	C:\WINDOWS\SoftwarePatch	SUCCESS
2:32:44.32025...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\WINDOWS\System32	SUCCESS
2:32:44.32033...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\System32	SUCCESS
2:32:44.32057...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\System32	SUCCESS
2:32:44.32091...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\System32	SUCCESS

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



2:32:44.31864...	Malware_U3_W2_L2.exe	3180	CloseFile	C:\documents and Settings\Administrator\Desktop	SUCCESS
2:32:44.31873...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS
2:32:44.31883...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS

The screenshot shows a Windows XP desktop environment. A File Explorer window is open, displaying the contents of a folder named 'Esercizio_Pratico_U3_W2_L2' located on the desktop. The address bar shows the full path: 'C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2'. The main view shows a single file named 'Malware_U3_W2_L2' with a document icon. A right-click context menu is open over the file, providing options such as 'Rename this file', 'Move this file', 'Copy this file', 'Publish this file to the Web', 'E-mail this file', 'Print this file', and 'Delete this file'. The taskbar at the bottom includes the Start button, a system clock showing 11:58 AM, and a single application icon.

```

[window: Save As]
cattura 20[ENTER]
[window: BinaryCollection]
.
[window: Run]
regedit0[ENTER]
[window: Registry Editor]
((((((((((((((((('((((((((((((((((('((((((((((((((((('((((((((w'((( '((((((((((((((((((((
[window: WINDOWS]
p
[window: Prefetch]
.
[window: Confirm File Delete]
BACKSPACE 0[ENTER]

```

Time of Day	Process Name	PID	Operation	Path	Result	Detail
2:22:44.30898	Malware_U3_v2_L2.exe	3180	Process Start		SUCCESS	Parent PID: 1938. Command line: "C:\Documents and Settings\Administrator\Desktop\E\exercio_Phatico_U3_v2_L2\Malware_U3_v2_L2.exe"
2:22:44.30908	Malware_U3_v2_L2.exe	3180	Thread Create		SUCCESS	Thread ID: 3188
2:22:44.30959	Malware_U3_v2_L2.exe	3180	Load Image	C:\Documents and Settings\Administrator\Desktop\E\exercio_Phatico_U3_v2_L2\Malware_U3_v2_L2.exe	SUCCESS	Image Base: 0x400000. Image Size: 0x4000
2:22:44.30972	Malware_U3_v2_L2.exe	3180	Load Image	C:\WINDOWS\system32\kernel.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x8000
2:22:44.31012	Malware_U3_v2_L2.exe	3180	Load Image	C:\WINDOWS\system32\kernel.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x8000
2:22:44.34936	Malware_U3_v2_L2.exe	3180	Load Image	C:\WINDOWS\system32\api-ms-win-base.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x2000
2:22:44.34950	Malware_U3_v2_L2.exe	3180	Load Image	C:\WINDOWS\system32\api-ms-win-base.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x2000
2:22:44.36025	Malware_U3_v2_L2.exe	3180	Load Image	C:\WINDOWS\system32\api-ms-win-base.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x2000
2:22:44.36848	Malware_U3_v2_L2.exe	3180	Load Image	C:\WINDOWS\system32\api-ms-win-base.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x2000
2:22:44.36862	Malware_U3_v2_L2.exe	3180	Load Image	C:\WINDOWS\system32\api-ms-win-base.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x2000
2:22:44.37241	Malware_U3_v2_L2.exe	3180	Process Create	C:\WINDOWS\system32\api-ms-win-base.dll	SUCCESS	Process ID: 3188. Command line: "C:\Documents and Settings\Administrator\Desktop\E\exercio_Phatico_U3_v2_L2\Malware_U3_v2_L2.exe"
2:22:45.37471	Malware_U3_v2_L2.exe	3180	Thread Exit		PROCESS_EXIT	Thread ID: 3188. User Time: 0.000000. Kernel Time: 0.000000
2:22:45.37483	Malware_U3_v2_L2.exe	3180	Process Exit		PROCESS_EXIT	Process ID: 3188. User Time: 0.000000. Kernel Time: 0.000000. Private Bytes: 274,432. Peak Private Bytes: 307,200. Working Set: 1,024. Peak Working Set: 1,024.

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.

