



Malware analysis

S10

Team





GIORNO 2

L2

Analisi Dinamica Basica



Traccia giorno 2

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:

01

Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)

02

Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor

03

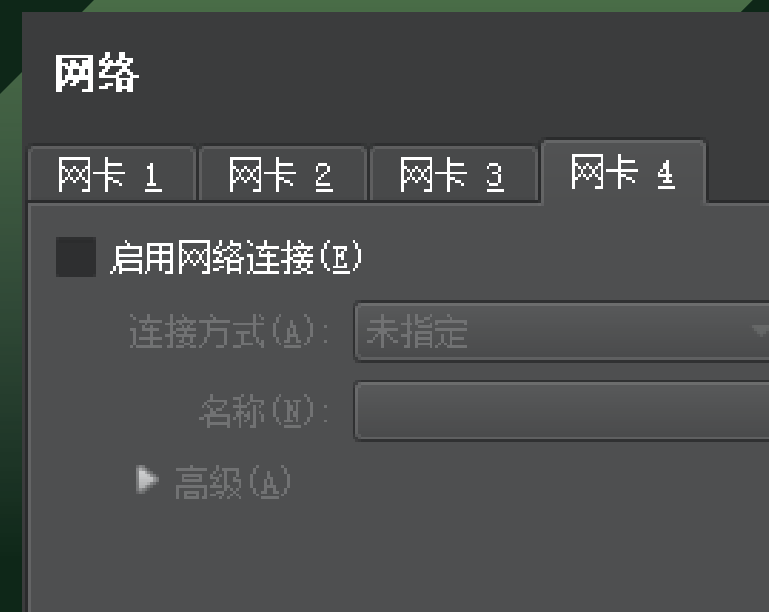
Modifiche del registro dopo il malware (le differenze)

04

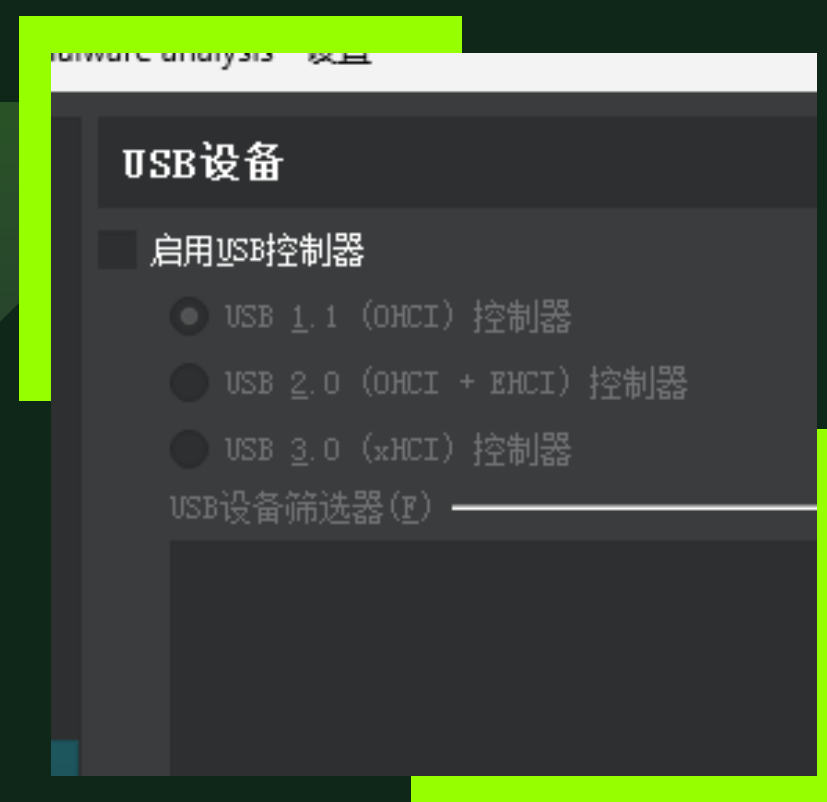
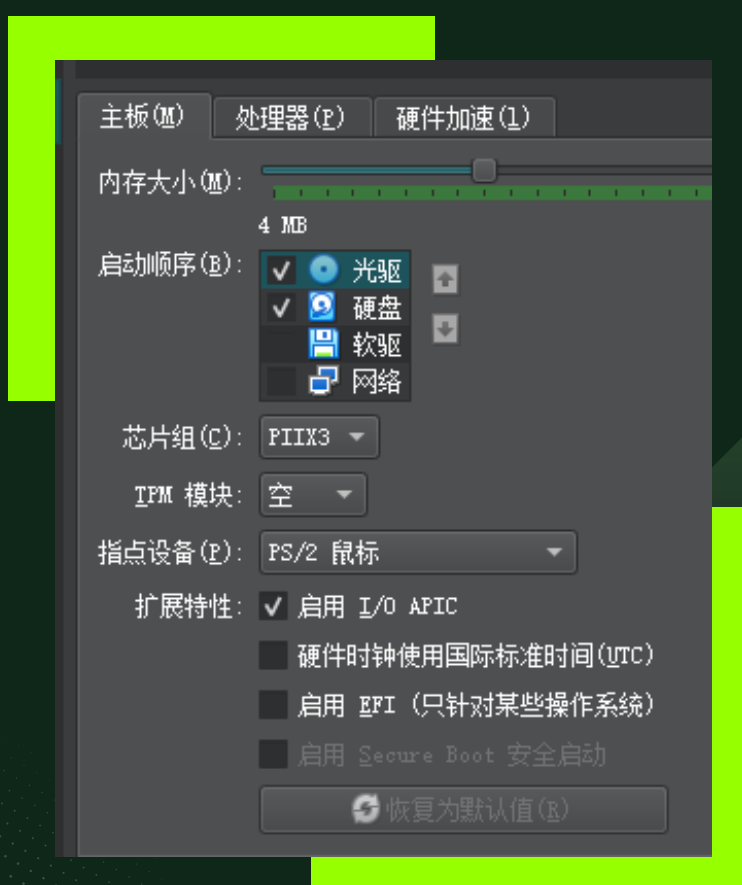
Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Configurazione macchina virtuale

In “rete” disabilitiamo tutte le interfacce di rete:

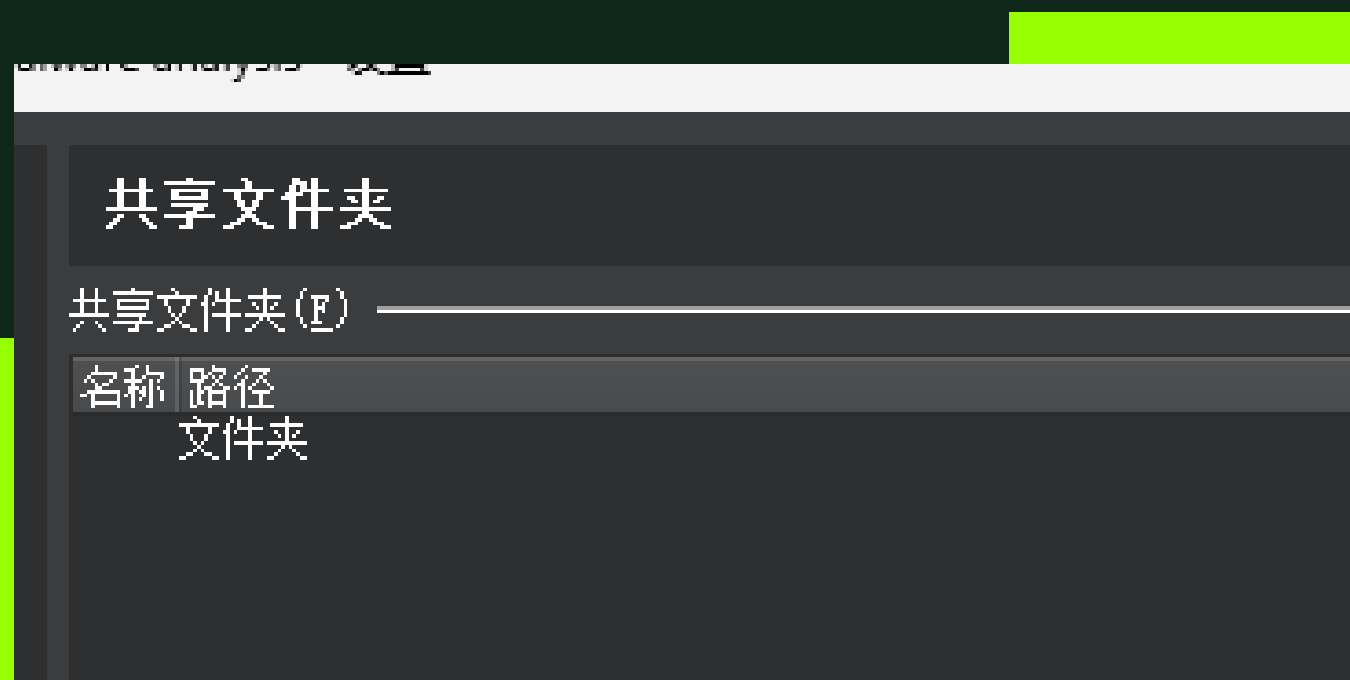
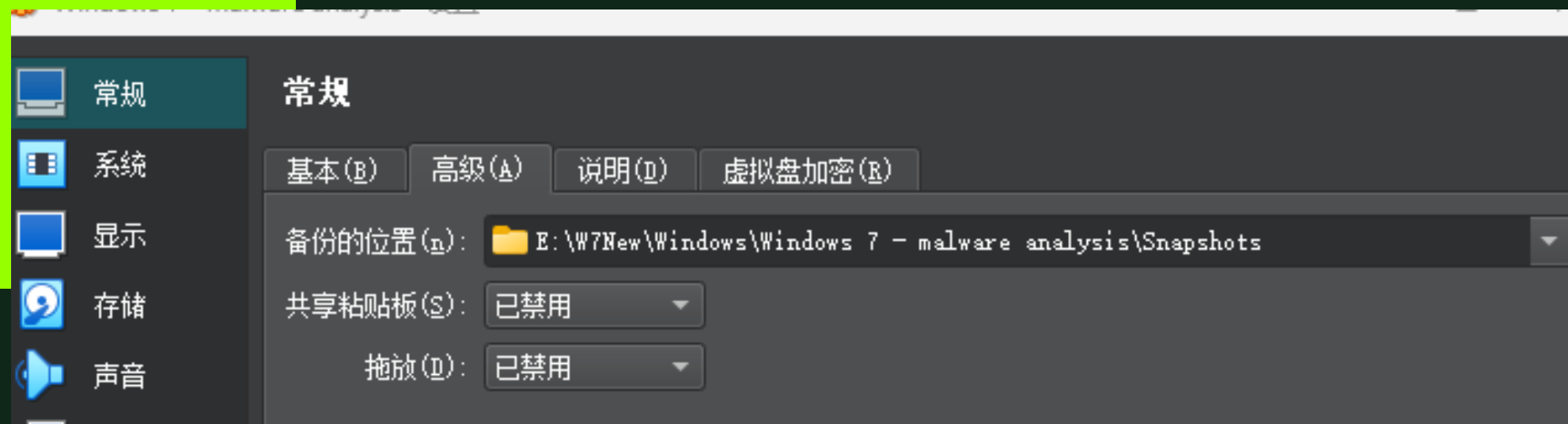


In “Sistema” disattiviamo il Floppy per poi disabilitare il controller USB in “Porte” > “USB”:




Configurazione macchina virtuale

In “Generale” > “Avanzate” disabilitare “appunti condivisi” e “trascina e rilascia”:



Configurazione macchina virtuale

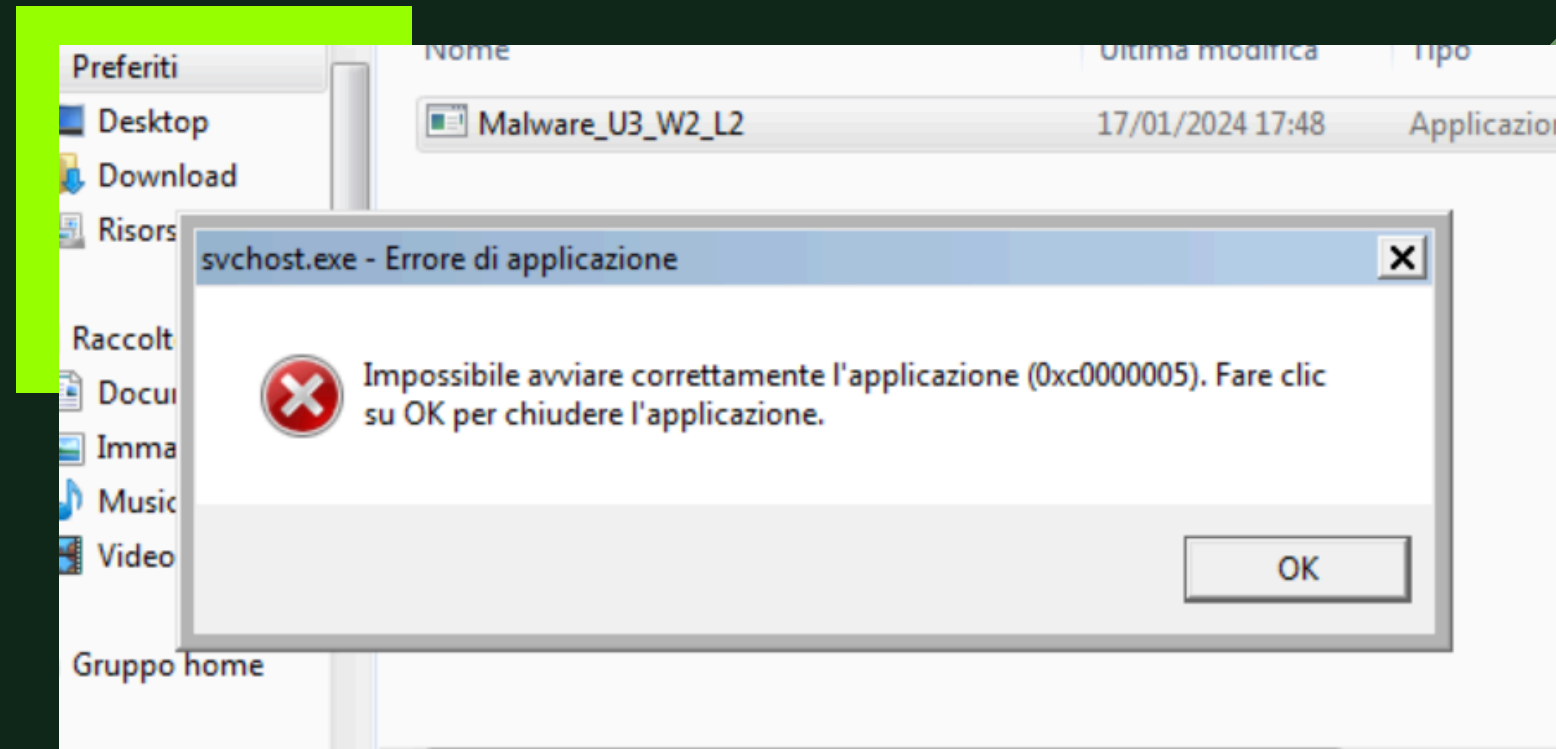
In  > “Istantanee” > “Crea”, creiamo un’istantanea della VM.

Questa operazione serve per avere un backup dello stato attuale della macchina in caso dopo l’esecuzione del malware questa venga compromessa.



Esecuzione del malware

Provando ad eseguire il Malware, il sistema ci restituisce il seguente errore:



Dopo svariate ricerche abbiamo appurato che il Malware è eseguibile su Windows XP e non su Windows 7. A questo punto abbiamo cercato un modo per copiare i file contenenti il malware da Windows 7 a Windows XP e lo abbiamo fatto creando un disco fisso VDI vuoto su VirtualBox. abbiamo montato il disco vuoto su Windows 7 e abbiamo copiato su di esso i dati di nostro interesse, dopodiché abbiamo montato lo stesso disco (che a questo punto contiene i dati) su WindowsXP.



Zhongshi Liu



Mara Dello Russo



Mario Marsicano



Luca Lenzi




Giovanni Sannino



Andre Vinicius

TEAM ALBA

THANK YOU

An abstract geometric design featuring two overlapping parallelograms. The top parallelogram is a vibrant yellow-green, while the bottom one is a darker, muted green. They are positioned diagonally across the right side of the frame. The background is a dark navy blue, accented with a fine, light-green dot pattern in the corners.