



CONSEGNA S10-L2

analisi dinamica basica



Traccia:

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.

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:

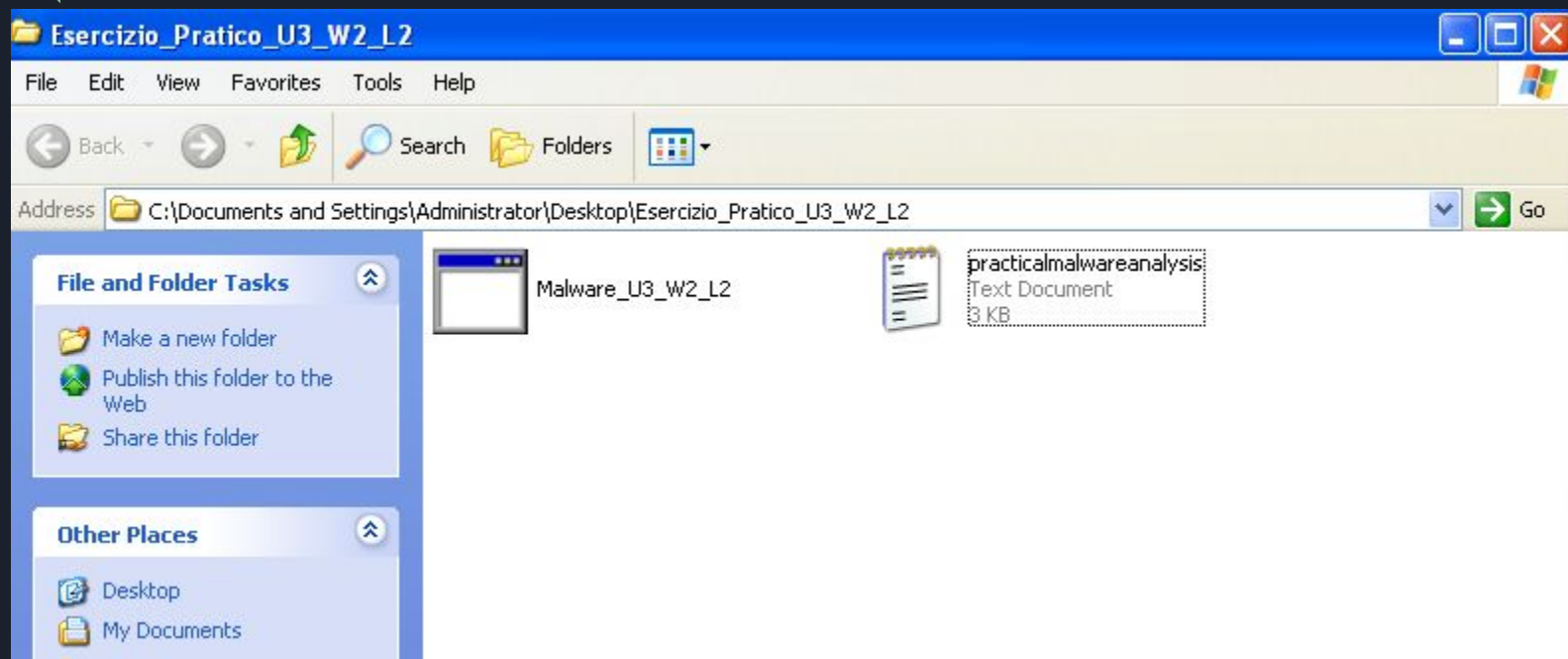
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Per prima cosa andiamo ad analizzare le azioni del malware che agiscono

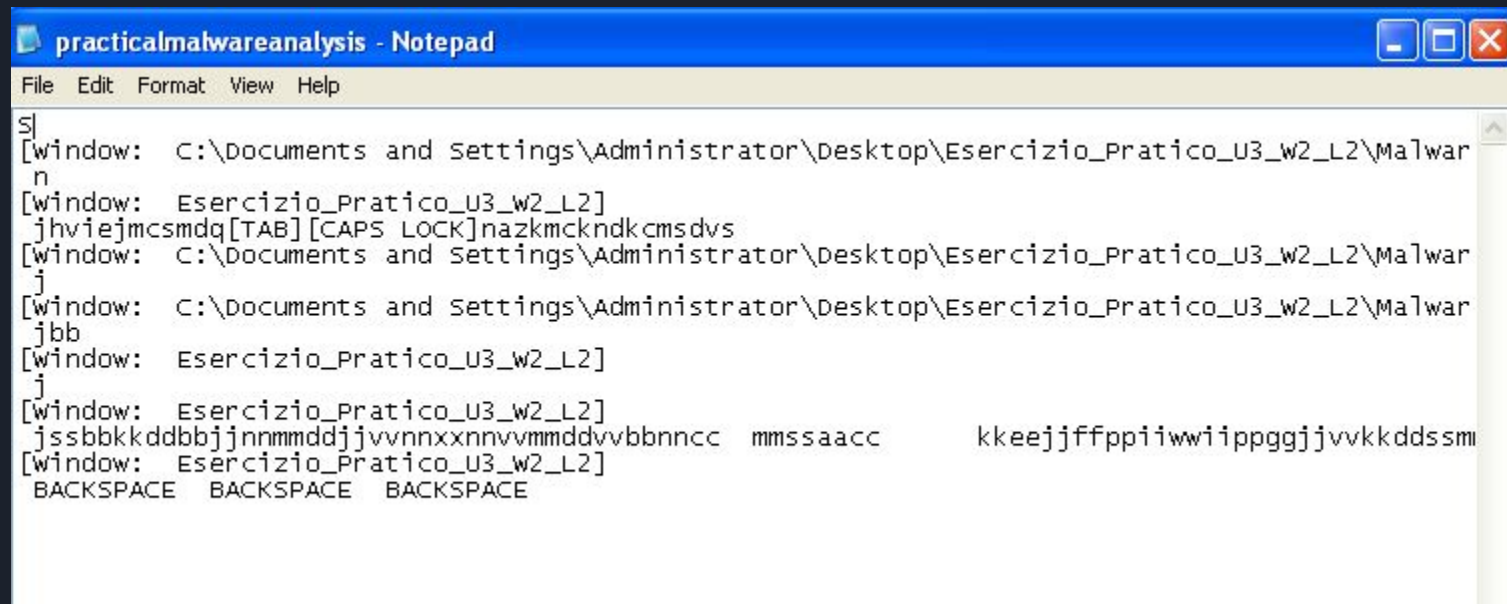
sul file system, per fare ciò utilizziamo ProcMon, un tool che ci permette di monitorare i processi in esecuzione sulla macchina:

[illegible]

Analizzando i processi ci siamo accorti di un processo che crea un file di testo chiamato practicalmalwareanalysis nella cartella dove risiede il malware.

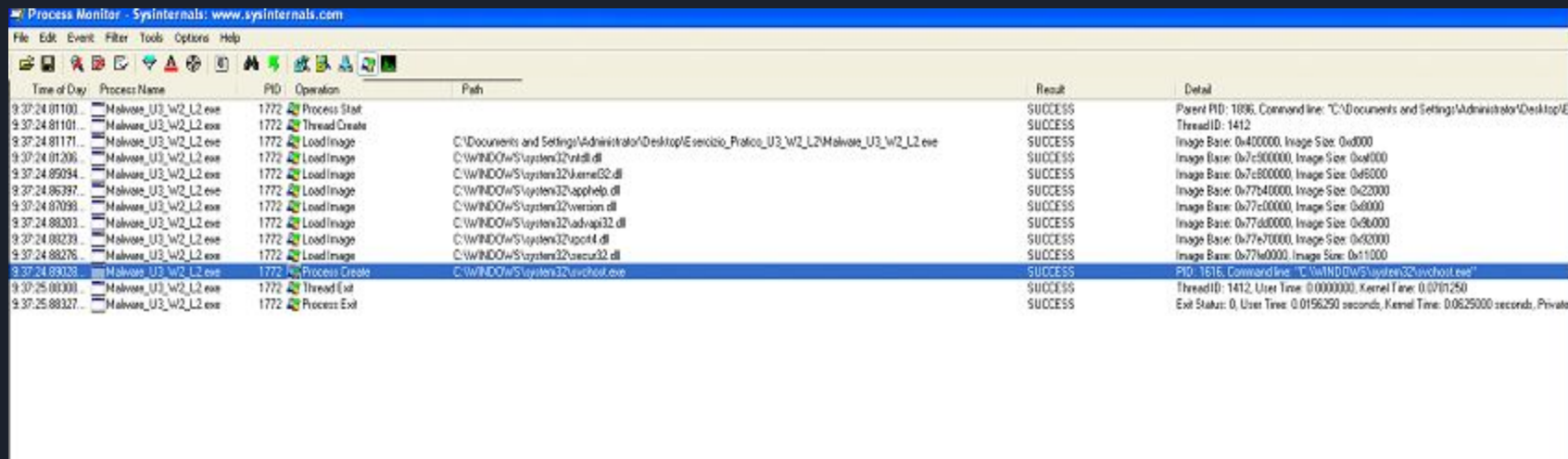


Apriamo il file per notare che contiene alcuni dei nostri caratteri inseriti da tastiera, questo è un tipico comportamento dei Key Logger



```
practicalmalwareanalysis - Notepad
File Edit Format View Help
S[
[window: C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_w2_L2\Malwar
n
[window: Esercizio_Pratico_U3_w2_L2]
jhviejmcsmdq[TAB][CAPS LOCK]nazkmckndkcmsdvs
[window: C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_w2_L2\Malwar
j
[window: C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_w2_L2\Malwar
jbb
[window: Esercizio_Pratico_U3_w2_L2]
j
[window: Esercizio_Pratico_U3_w2_L2]
jssbbkkddbbjjnnmmddjjvvnnxxnnvvmmddvvbbnncc mmssaacc kkeejfffppiiwwiippgggjjvvkkddssm
[window: Esercizio_Pratico_U3_w2_L2]
BACKSPACE BACKSPACE BACKSPACE
```

Utilizzando la cattura precedente di ProcMon e cliccando sull'icona "Processi e Thread" andiamo a filtrare i processi che appartengono a quella categoria.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
9:37:24.01100	Malware_U3_W2_L2.exe	1772	Process Start		SUCCESS	Parent PID: 1086, Command line: "C:\Documents and Settings\Administrato\Desktop\E
9:37:24.81101	Malware_U3_W2_L2.exe	1772	Thread Create		SUCCESS	ThreadID: 1412
9:37:24.81171	Malware_U3_W2_L2.exe	1772	Load Image	C:\Documents and Settings\Administrato\Desktop\Esercizio_Platco_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x0000
9:37:24.01206	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0x0af000
9:37:24.89094	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0x4f6000
9:37:24.86397	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
9:37:24.87093	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x6000
9:37:24.88203	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d00000, Image Size: 0x86000
9:37:24.88239	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x50000
9:37:24.88276	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x77f00000, Image Size: 0x11000
9:37:24.89038	Malware_U3_W2_L2.exe	1772	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1616, Command line: "C:\WINDOWS\system32\svchost.exe"
9:37:25.00300	Malware_U3_W2_L2.exe	1772	Thread Exit		SUCCESS	ThreadID: 1412, User Time: 0.0000000, Kernel Time: 0.0701250
9:37:25.88327	Malware_U3_W2_L2.exe	1772	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0196250 seconds, Kernel Time: 0.0625000 seconds, Private

Abbiamo notato che il malware crea un processo chiamato Svchost.exe, che è il nome di un processo generalmente valido di Windows xp.
Il malware cerca di camuffarsi chiamandosi Svchost, poi esegue la sua funzione principale di Key Logger salvando tutti i caratteri digitati dall'utente in un file chiamato `praticalmalwareanalysis`.