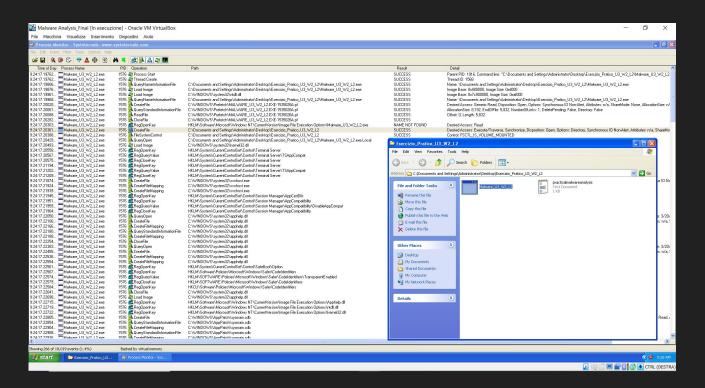
Analisi Malware 2

Azioni del malware sul file system



Apro il programma Process Monitor e lo metto in ascolto cliccando sulla lente in alto a Sx (non deve avere la X). Alla fine della scansione noto che il malware ha creato un file di testo nella cartella dove si trovava il suo eseguibile

Azioni del malware sul file system

```
d
[Window: Esercizio_Pratico_U3_W2_L2]
dffffrrrrvvvvbbbbjjjjhhhhffffaaaassssddddeeeerrrreeeevvvvgggggggghhhhgggghhhh
```

Questo è il contenuto del file di testo creato dal malware, questo comportamento è piuttosto solito dei malware Keylogger.

Azioni del malware su processi e thread

9:24:17.26785	Malware_U3_W2_L2.exe 1	1576 KRegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\svchost.exe	NAME NOT FOUND	Desired Access: Read
		1576 🗟 CreateFile	C:\WINDOWS\system32\svchost.exe.Manifest	NAME NOT FOUND	Desired Access: Generic Read/Execute, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes; n/a, ShareMc
9.24:17.26874	Malware_U3_W2_L2.exe 1	1576 Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1572, Command line: "C:\WINDOWS\system32\svchost.exe"
			C:\WINDOWS\system32\svchost.exe	SUCCESS	
		1576 A. Process Profiling			User Time: 0.0156250 seconds, Kernel Time: 0.0468750 seconds, Private Bytes: 282,624, Working Set: 1,056,768
		1576 🌌 Thread Exit			Thread ID: 1568, User Time: 0.0000000, Kernel Time: 0.0625000
		1576 ar Process Exit			Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0468750 seconds, Private Bytes: 274,432, Peak Private Bytes: 307,200, World
9:24:18.26873	Malware_U3_W2_L2.exe 1	1576 🔜 CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	The state of the s

Sono presenti funzioni come Load Image che viene utilizzata per l'esecuzione del malware e caricare le librerie (.dll) necessarie, e poi vediamo Process Create che serve per creare un processo.

Profilazione del malware

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.