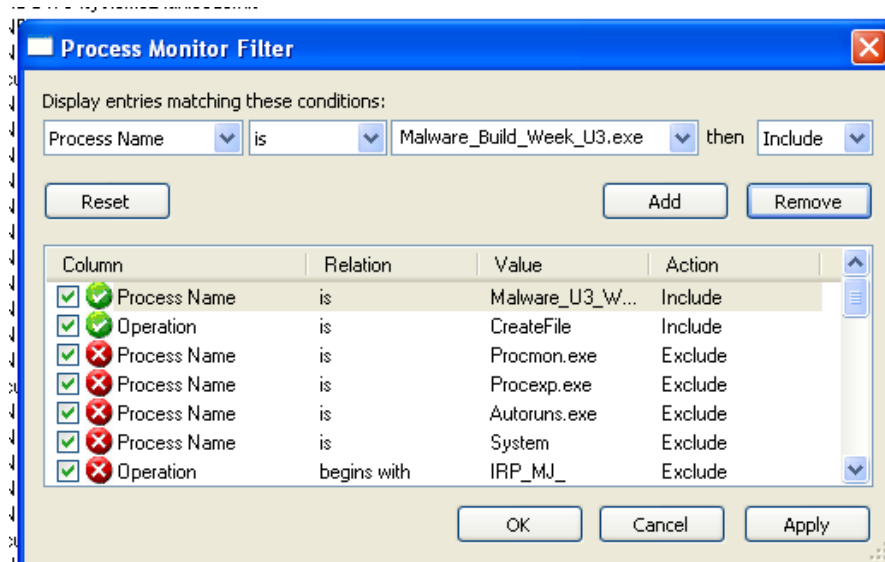


S10/L2

L'esercizio di oggi consiste nell'eseguire un'analisi dinamica basica.

Utilizzeremo come tools Process Monitor e RegShot.

Come prima cosa avviamo entrambi i tools, per facilitarci con l'analisi tramite Process Monitor andremo ad applicare i seguenti filtri:

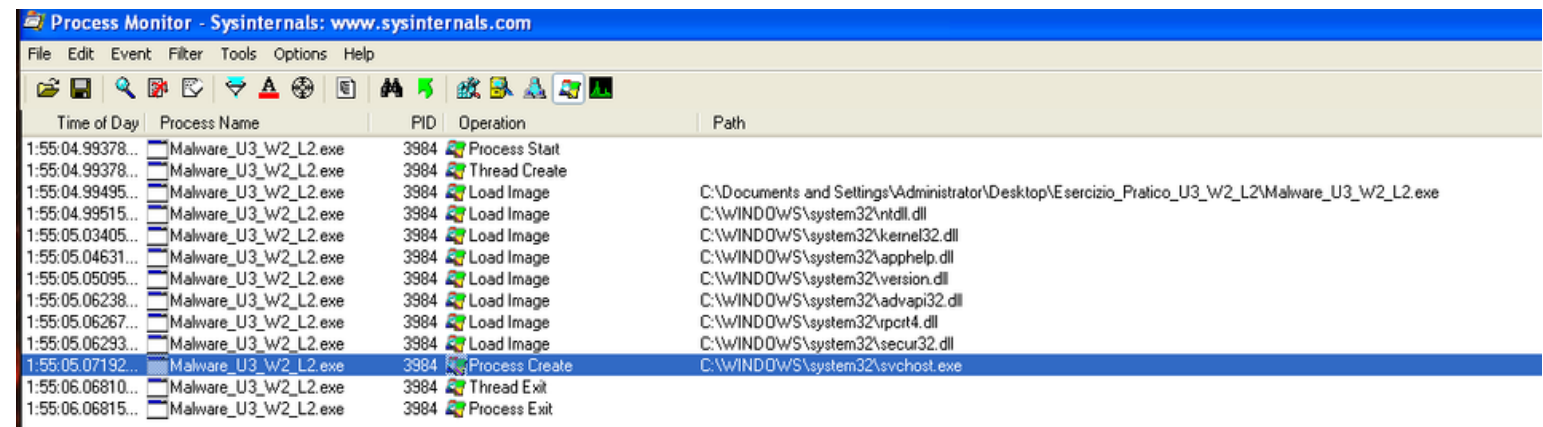


Possiamo notare immediatamente che la prima cosa che va a fare il malware è quella di creare un file con estensione .pf

Time of Day	Process Name	PID	Operation	Path
1:55:04.99544...	Malware_U3_W2_L2.exe	3984	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
1:55:04.99999...	Malware_U3_W2_L2.exe	3984	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf

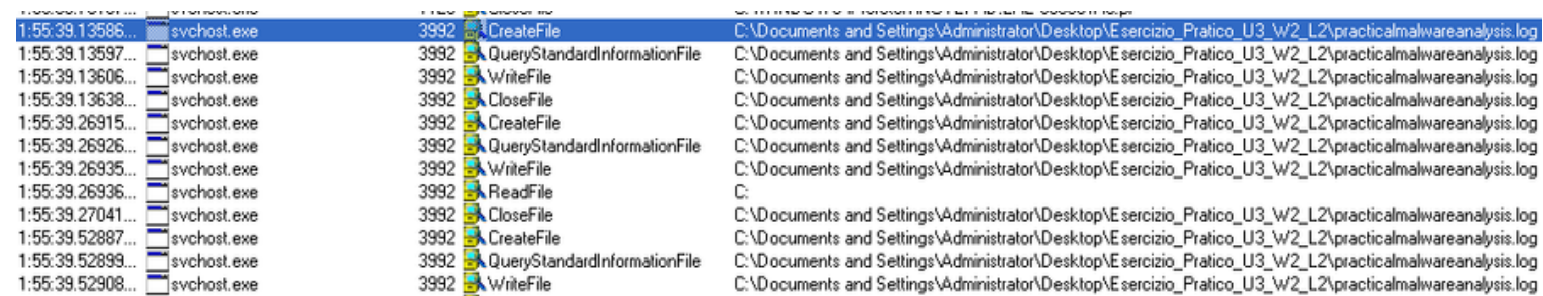
I file con estensione ".pf" sono spesso associati ai file Prefetch. Il sistema operativo Windows utilizza la tecnologia Prefetch per ottimizzare il caricamento delle applicazioni durante l'avvio.

Oltre alla creazione del file .pf , il malware ha creato anche il processo svchost.exe. Questo processo nativo di Windows è stato alterato.



Time of Day	Process Name	PID	Operation	Path
1:55:04.99378...	Malware_U3_W2_L2.exe	3984	Process Start	
1:55:04.99378...	Malware_U3_W2_L2.exe	3984	Thread Create	
1:55:04.99495...	Malware_U3_W2_L2.exe	3984	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
1:55:04.99515...	Malware_U3_W2_L2.exe	3984	Load Image	C:\WINDOWS\system32\ntdll.dll
1:55:05.03405...	Malware_U3_W2_L2.exe	3984	Load Image	C:\WINDOWS\system32\kernel32.dll
1:55:05.04631...	Malware_U3_W2_L2.exe	3984	Load Image	C:\WINDOWS\system32\apphelp.dll
1:55:05.05095...	Malware_U3_W2_L2.exe	3984	Load Image	C:\WINDOWS\system32\version.dll
1:55:05.06238...	Malware_U3_W2_L2.exe	3984	Load Image	C:\WINDOWS\system32\advapi32.dll
1:55:05.06267...	Malware_U3_W2_L2.exe	3984	Load Image	C:\WINDOWS\system32\iprt4.dll
1:55:05.06293...	Malware_U3_W2_L2.exe	3984	Load Image	C:\WINDOWS\system32\secur32.dll
1:55:05.07192...	Malware_U3_W2_L2.exe	3984	Process Create	C:\WINDOWS\system32\svchost.exe
1:55:06.06810...	Malware_U3_W2_L2.exe	3984	Thread Exit	
1:55:06.06815...	Malware_U3_W2_L2.exe	3984	Process Exit	

Se andiamo ad analizzare il processo svchost.exe possiamo notare che ha creato dei file di log nella cartella del Malware.



Time of Day	Process Name	PID	Operation	Path
1:55:39.13586...	svchost.exe	3992	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.13597...	svchost.exe	3992	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.13606...	svchost.exe	3992	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.13638...	svchost.exe	3992	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.26915...	svchost.exe	3992	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.26926...	svchost.exe	3992	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.26935...	svchost.exe	3992	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.26936...	svchost.exe	3992	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.27041...	svchost.exe	3992	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.52887...	svchost.exe	3992	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.52899...	svchost.exe	3992	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
1:55:39.52908...	svchost.exe	3992	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log

Spostandoci nella cartella del Malware e analizzando i file di log che crea possiamo presumere che abbiamo avviato un keylogger

