

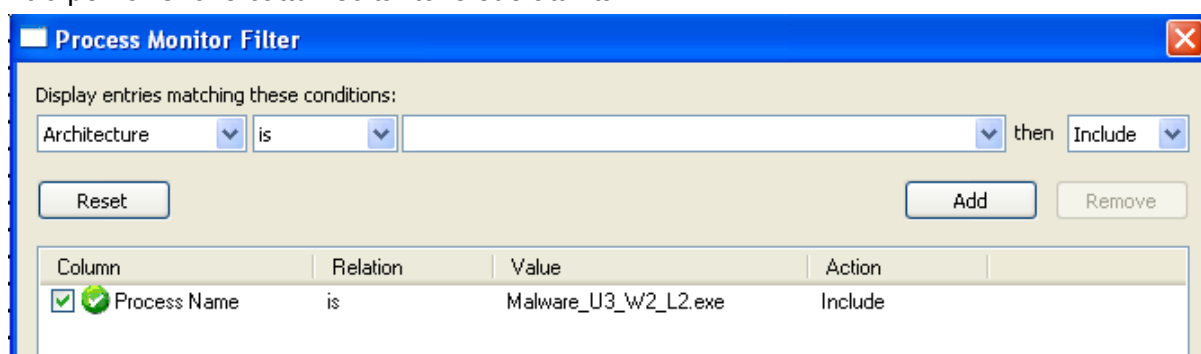
CONSEGNA S10/L2

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 facciamo partire Procmon prima di eseguire il malware e ne impostiamo il filtro per far sì che catturi soltanto le sue attività.



Lanciamo la cattura e successivamente apriamo l'eseguibile del malware.

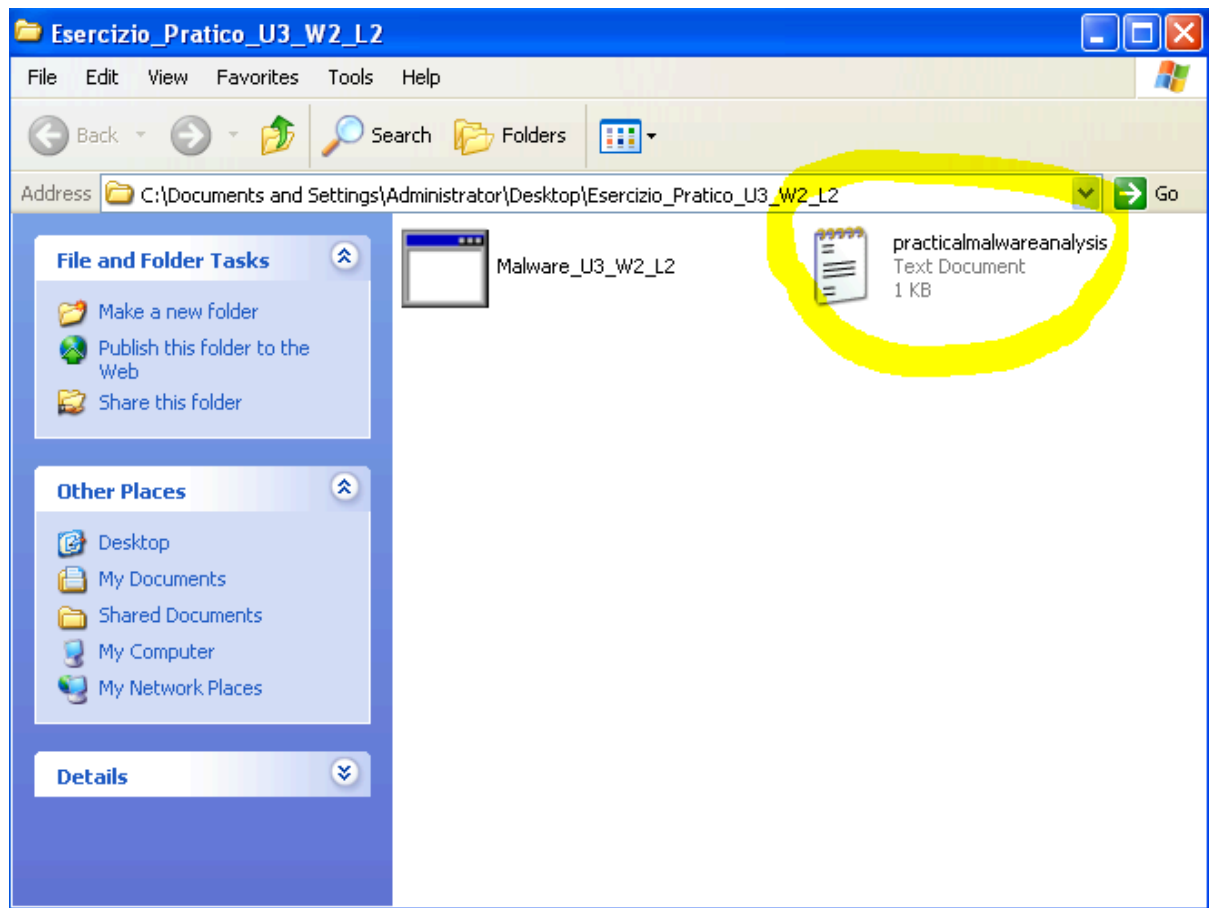
Process Monitor - Sysinternals: www.sysinternals.com					
Time of Day	Process Name	PID	Operation	Path	Result
13.42.37.6121	Malware_U3_W2_L2.exe	984	Process Start		SUCCESS
13.42.37.6123	Malware_U3_W2_L2.exe	984	Thread Create		SUCCESS
13.42.37.6125	Malware_U3_W2_L2.exe	984	QueryNameInforma...	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwa...	SUCCESS
13.42.37.6127	Malware_U3_W2_L2.exe	984	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwa...	SUCCESS
13.42.37.6129	Malware_U3_W2_L2.exe	984	Load Image	C:\WINDOWS\system32\cmd.dll	SUCCESS
13.42.37.6130	Malware_U3_W2_L2.exe	984	QueryNameInforma...	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwa...	SUCCESS
13.42.37.6131	Malware_U3_W2_L2.exe	984	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
13.42.37.6132	Malware_U3_W2_L2.exe	984	QueryStandardInfo...	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
13.42.37.6133	Malware_U3_W2_L2.exe	984	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
13.42.37.6135	Malware_U3_W2_L2.exe	984	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
13.42.37.6136	Malware_U3_W2_L2.exe	984	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\M...	NAME NOT FOUND
13.42.37.6138	Malware_U3_W2_L2.exe	984	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
13.42.37.6139	Malware_U3_W2_L2.exe	984	FileSystemControl	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
13.42.37.6145	Malware_U3_W2_L2.exe	984	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwa...	NAME NOT FOUND
13.42.37.6146	Malware_U3_W2_L2.exe	984	Load Image	C:\WINDOWS\system32\lsasrv.dll	SUCCESS
13.42.37.6151	Malware_U3_W2_L2.exe	984	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
13.42.37.6152	Malware_U3_W2_L2.exe	984	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
13.42.37.6152	Malware_U3_W2_L2.exe	984	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
13.42.37.6173	Malware_U3_W2_L2.exe	984	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
13.42.37.6181	Malware_U3_W2_L2.exe	984	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
13.42.37.6181	Malware_U3_W2_L2.exe	984	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
13.42.37.6187	Malware_U3_W2_L2.exe	984	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6189	Malware_U3_W2_L2.exe	984	CreateFileMapping	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6189	Malware_U3_W2_L2.exe	984	FASTIO_ACQUIR...	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6189	Malware_U3_W2_L2.exe	984	FASTIO_RELEASE...	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6189	Malware_U3_W2_L2.exe	984	FASTIO_RELEASE...	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6190	Malware_U3_W2_L2.exe	984	FASTIO_RELEASE...	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6190	Malware_U3_W2_L2.exe	984	FASTIO_RELEASE...	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6190	Malware_U3_W2_L2.exe	984	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls	NAME NOT FOUND
13.42.37.6191	Malware_U3_W2_L2.exe	984	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility	SUCCESS
13.42.37.6191	Malware_U3_W2_L2.exe	984	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility\DisableApp...	NAME NOT FOUND
13.42.37.6192	Malware_U3_W2_L2.exe	984	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility	SUCCESS
13.42.37.6198	Malware_U3_W2_L2.exe	984	QueryOpen	C:\WINDOWS\system32\apphelp.dll	SUCCESS
13.42.37.6198	Malware_U3_W2_L2.exe	984	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS
13.42.37.6199	Malware_U3_W2_L2.exe	984	CreateFileMapping	C:\WINDOWS\system32\apphelp.dll	SUCCESS
13.42.37.6199	Malware_U3_W2_L2.exe	984	FASTIO_RELEASE...	C:\WINDOWS\system32\apphelp.dll	SUCCESS
13.42.37.6200	Malware_U3_W2_L2.exe	984	FASTIO_RELEASE...	C:\WINDOWS\system32\apphelp.dll	SUCCESS
13.42.37.6200	Malware_U3_W2_L2.exe	984	FASTIO_RELEASE...	C:\WINDOWS\system32\apphelp.dll	SUCCESS

Notiamo subito nella colonna “operation” funzioni sospette quali “create file”, “read file” e “close file”.

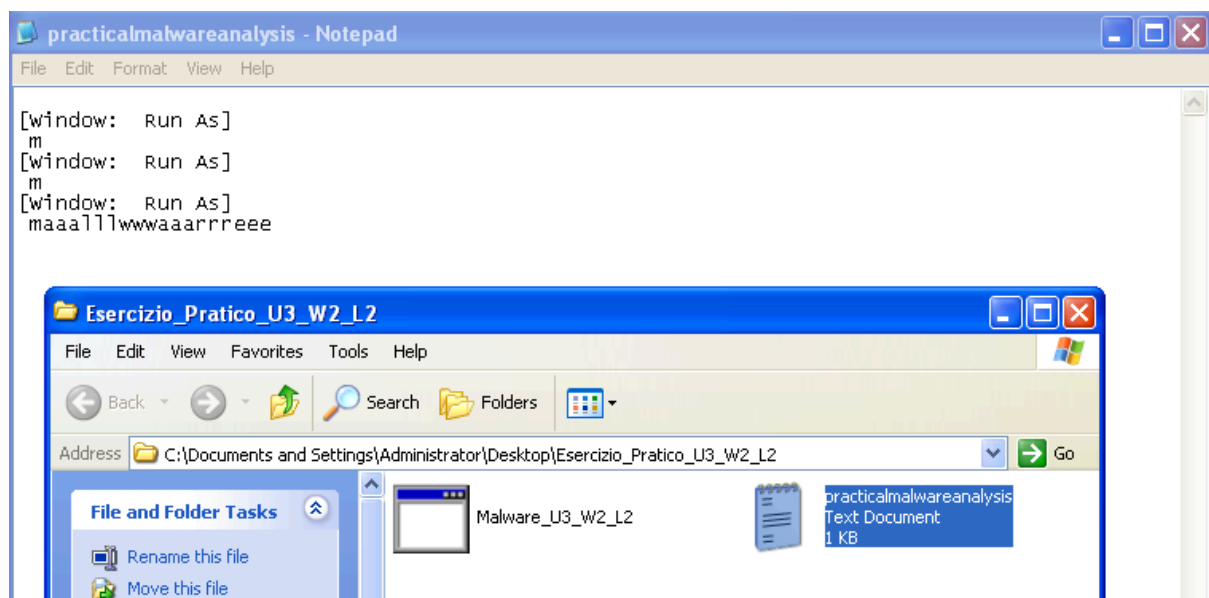
Nella seguente immagine vediamo come abbia creato un file .txt nella cartella dove risiede l’eseguibile.

Process Monitor - Sysinternals: www.sysinternals.com					
Time of Day	Process Name	PID	Operation	Path	Result
13.42.37.6125...	Malware_U3_W2_L2.exe	984	QueryNameInforma...	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwar...	SUCCESS
13.42.37.6130...	Malware_U3_W2_L2.exe	984	QueryNameInforma...	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwar...	SUCCESS
13.42.37.6131...	Malware_U3_W2_L2.exe	984	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
13.42.37.6132...	Malware_U3_W2_L2.exe	984	QueryStandardInfo...	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
13.42.37.6133...	Malware_U3_W2_L2.exe	984	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
13.42.37.6135...	Malware_U3_W2_L2.exe	984	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
13.42.37.6138...	Malware_U3_W2_L2.exe	984	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
13.42.37.6139...	Malware_U3_W2_L2.exe	984	FileSystemControl	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
13.42.37.6145...	Malware_U3_W2_L2.exe	984	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwar...	NAME NOT FOUND
13.42.37.6187...	Malware_U3_W2_L2.exe	984	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6189...	Malware_U3_W2_L2.exe	984	CreateFileMapping	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6189...	Malware_U3_W2_L2.exe	984	FASTIO_ACQUIR...	C:\WINDOWS\system32\svchost.exe	SUCCESS
13.42.37.6189...	Malware_U3_W2_L2.exe	984	FASTIO_RELEASE...	C:\WINDOWS\system32\svchost.exe	SUCCESS

Apriamo la cartella sul desktop per vedere se effettivamente questo file di testo è stato creato.

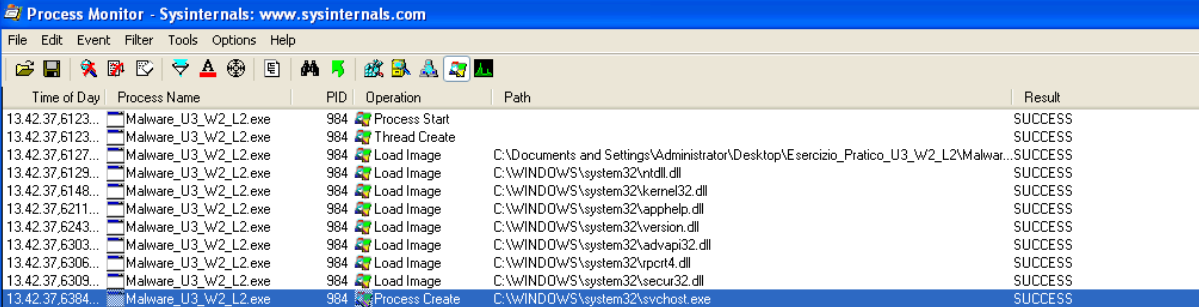


Il file c'è.
Andiamo ad aprirlo.



Notiamo che il file ha acquisito alcuni dei caratteri da tastiera utilizzati durante l'esercitazione, questo comportamento è spesso associabile ai keylogger.

Notiamo poi, filtrando per “processi e thread”, che il malware crea un processo chiamato “svchost.exe” che è generalmente un processo valido di window, questo sta ad indicare che sta provando a camuffarsi.



Time of Day	Process Name	PID	Operation	Path	Result
13.42.37.6123...	Malware_U3_W2_L2.exe	984	Process Start		SUCCESS
13.42.37.6123...	Malware_U3_W2_L2.exe	984	Thread Create		SUCCESS
13.42.37.6127...	Malware_U3_W2_L2.exe	984	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwar...	SUCCESS
13.42.37.6129...	Malware_U3_W2_L2.exe	984	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS
13.42.37.6148...	Malware_U3_W2_L2.exe	984	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS
13.42.37.6211...	Malware_U3_W2_L2.exe	984	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS
13.42.37.6243...	Malware_U3_W2_L2.exe	984	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS
13.42.37.6303...	Malware_U3_W2_L2.exe	984	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS
13.42.37.6306...	Malware_U3_W2_L2.exe	984	Load Image	C:\WINDOWS\system32\vpport4.dll	SUCCESS
13.42.37.6309...	Malware_U3_W2_L2.exe	984	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS
13.42.37.6384...	Malware_U3_W2_L2.exe	984	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS