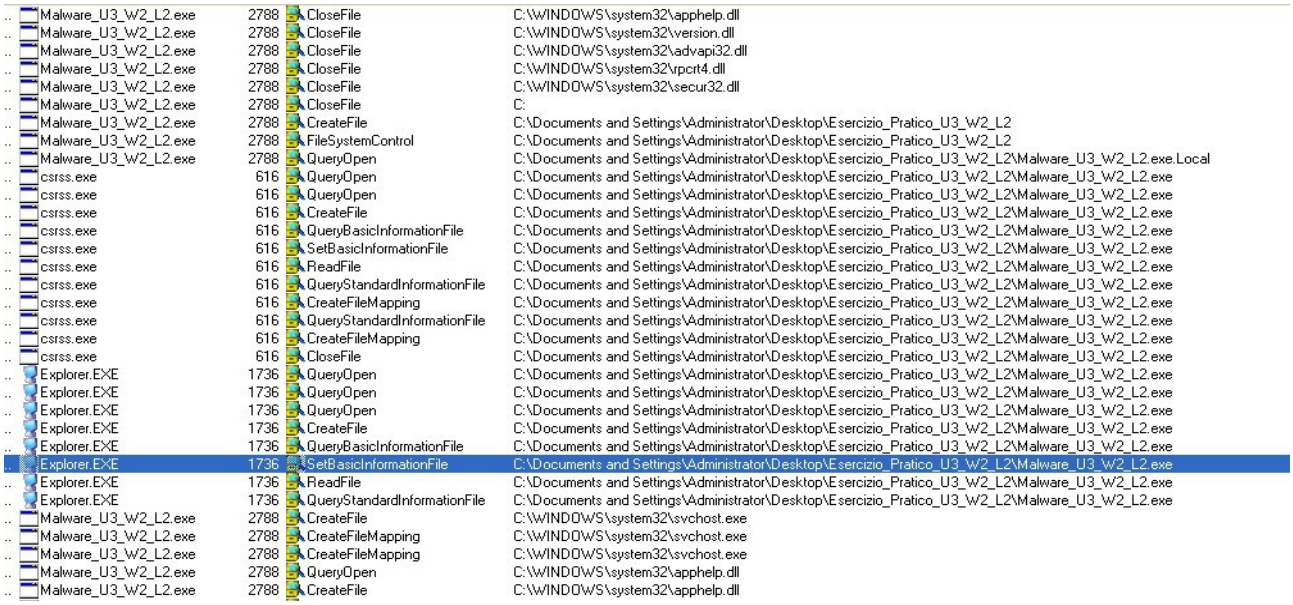
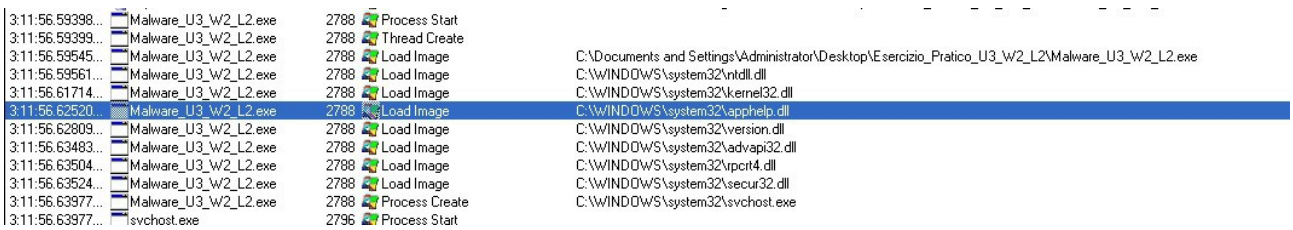
Analisi statica basica

Dopo aver avviato procmon e resettato i filtri presenti windows xp esegue i vari processi di sistema come da programmazione.

Appena viene lanciato il malware comincia a creare processi dati dal programma lanciato crea processi che vengono eseguiti come file system.



Malware_U3_W2_L2.exe	2788	CloseFile	C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe	2788	CloseFile	C:\WINDOWS\system32\version.dll
Malware_U3_W2_L2.exe	2788	CloseFile	C:\WINDOWS\system32\advapi32.dll
Malware_U3_W2_L2.exe	2788	CloseFile	C:\WINDOWS\system32\rpcrt4.dll
Malware_U3_W2_L2.exe	2788	CloseFile	C:\WINDOWS\system32\secur32.dll
Malware_U3_W2_L2.exe	2788	CloseFile	C:
Malware_U3_W2_L2.exe	2788	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2
Malware_U3_W2_L2.exe	2788	FileSystemControl	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2
Malware_U3_W2_L2.exe	2788	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe.Local
csrss.exe	616	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	QueryBasicInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	SetBasicInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	CreateFileMapping	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	CreateFileMapping	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
csrss.exe	616	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Explorer.EXE	1736	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Explorer.EXE	1736	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Explorer.EXE	1736	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Explorer.EXE	1736	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Explorer.EXE	1736	QueryBasicInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Explorer.EXE	1736	SetBasicInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Explorer.EXE	1736	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Explorer.EXE	1736	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_U3_W2_L2.exe	2788	CreateFile	C:\WINDOWS\system32\svchost.exe
Malware_U3_W2_L2.exe	2788	CreateFileMapping	C:\WINDOWS\system32\svchost.exe
Malware_U3_W2_L2.exe	2788	CreateFileMapping	C:\WINDOWS\system32\svchost.exe
Malware_U3_W2_L2.exe	2788	QueryOpen	C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe	2788	CreateFile	C:\WINDOWS\system32\apphelp.dll



3:11:56.59398...	Malware_U3_W2_L2.exe	2788	Process Start
3:11:56.59399...	Malware_U3_W2_L2.exe	2788	Thread Create
3:11:56.59545...	Malware_U3_W2_L2.exe	2788	Load Image C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
3:11:56.59561...	Malware_U3_W2_L2.exe	2788	Load Image C:\WINDOWS\system32\ntdll.dll
3:11:56.61714...	Malware_U3_W2_L2.exe	2788	Load Image C:\WINDOWS\system32\kernel32.dll
3:11:56.62520...	Malware_U3_W2_L2.exe	2788	Load Image C:\WINDOWS\system32\apphelp.dll
3:11:56.62809...	Malware_U3_W2_L2.exe	2788	Load Image C:\WINDOWS\system32\version.dll
3:11:56.63483...	Malware_U3_W2_L2.exe	2788	Load Image C:\WINDOWS\system32\advapi32.dll
3:11:56.63504...	Malware_U3_W2_L2.exe	2788	Load Image C:\WINDOWS\system32\rpcrt4.dll
3:11:56.63524...	Malware_U3_W2_L2.exe	2788	Load Image C:\WINDOWS\system32\secur32.dll
3:11:56.63977...	Malware_U3_W2_L2.exe	2788	Process Create C:\WINDOWS\system32\svchost.exe
3:11:56.63977...	svchost.exe	2796	Process Start