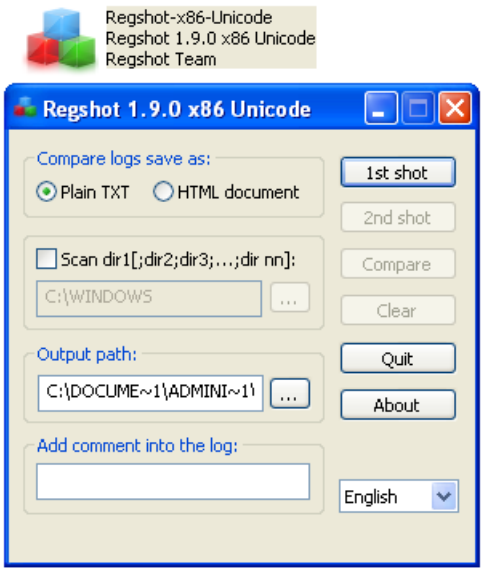
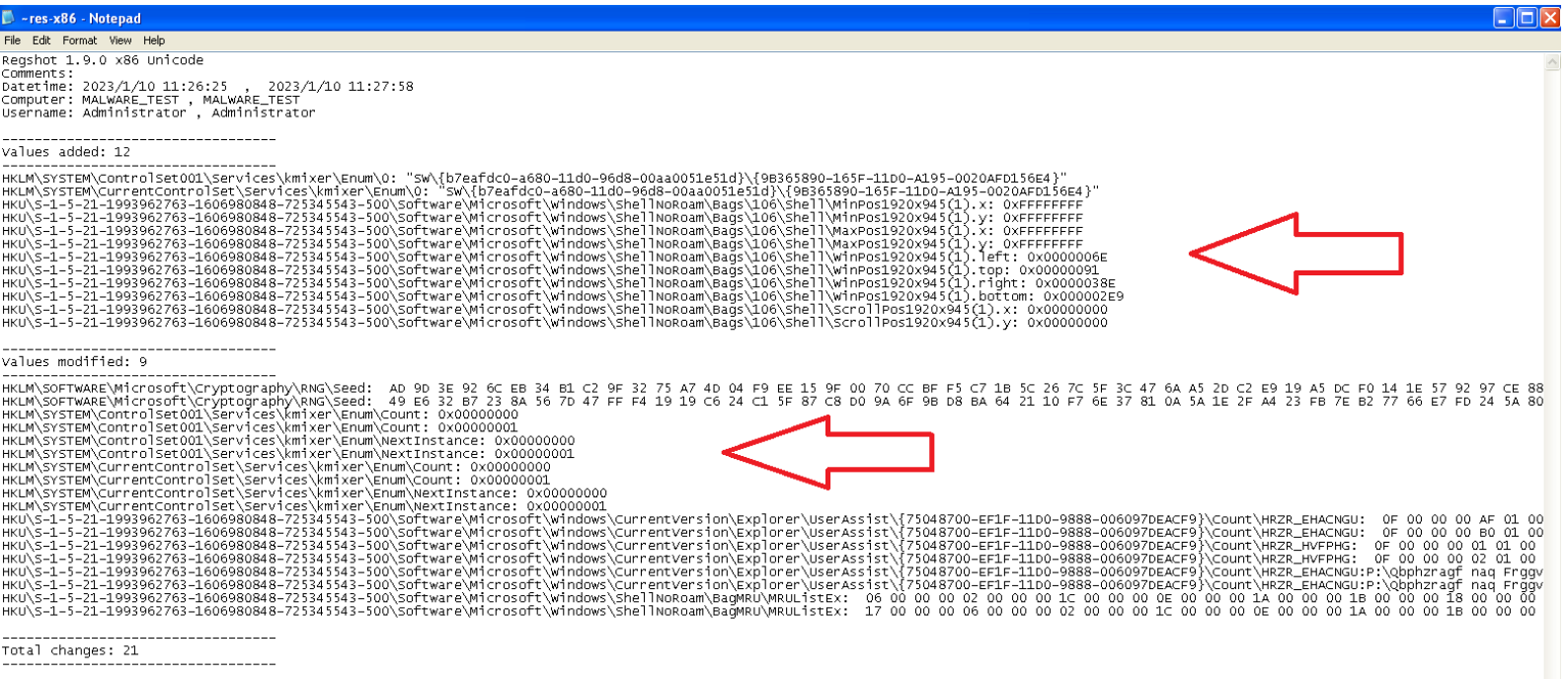
Analisi Dinamica Basica

Esercizio_Pratico_U3_W2_L2

Come richiesto nella traccia effettueremo:

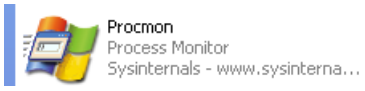


RegShot ci permette di salvare delle istantanee delle chiavi di registro in due momenti a nostra scelta e poi compararli. Ci basterà cliccare su **1StShot -> Shot** per salvare il primo screen, poi quando vorremmo effettuare il secondo, ci basterà cliccare **2nd Shot -> Shot** , una volta eseguita questa operazione cliccheremo su **Compare** e automaticamente il programma ci creerà il nostro TXT.

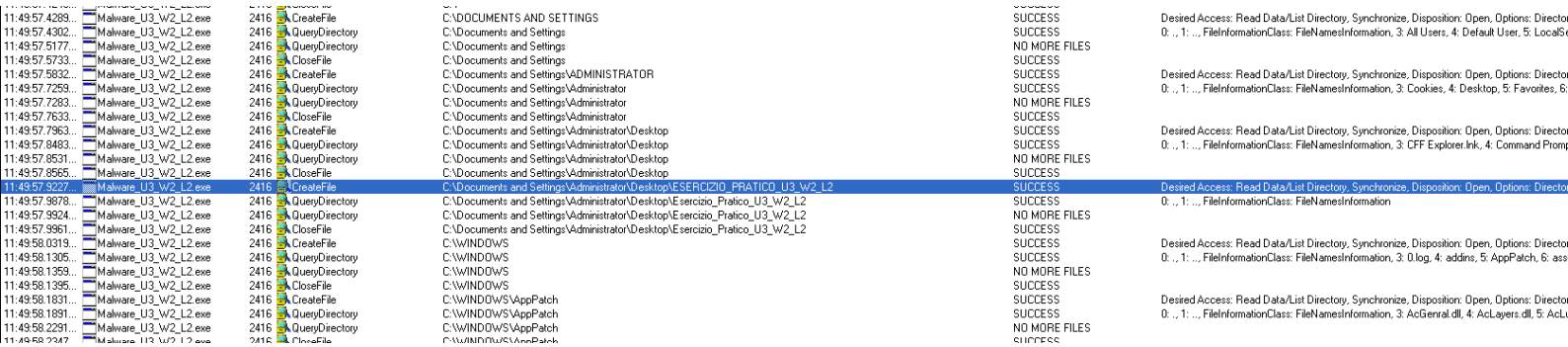


Come vedremmo dal nostro screen, nella parte superiore troveremo il **1StShot** con le chiavi di registro iniziale, nella parte inferiore il **2StShot**, scattato dopo aver avviato il Malware. Come si può notare sono state modificate delle chiavi di registro.

Siamo passati poi all'utilizzo di Procmon (Process Monitor) che ci permette di monitorare i processi ed i thread attivi, l'attività di rete, l'accesso ai file e le chiamate di sistema effettuate sul sistema operativo



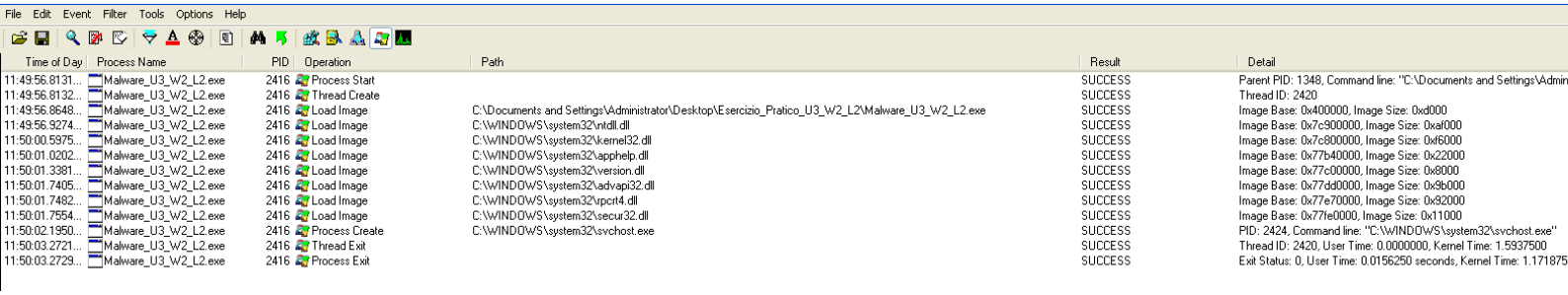
Passiamo poi ad identificare le azioni del Malware sul file System, utilizzando appunto Procmon.



11:49:57.4289...	Malware_U3_W2_L2.exe	2416	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
11:49:57.4302...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalSe
11:49:57.5177...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
11:49:57.5733...	Malware_U3_W2_L2.exe	2416	CloseFile	C:\Documents and Settings	SUCCESS	
11:49:57.5832...	Malware_U3_W2_L2.exe	2416	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
11:49:57.7259...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: Cookies, 4: Desktop, 5: Favorites, 6:
11:49:57.7283...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
11:49:57.7633...	Malware_U3_W2_L2.exe	2416	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
11:49:57.7963...	Malware_U3_W2_L2.exe	2416	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
11:49:57.8483...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: CFF Explorer.lnk, 4: Command Promp
11:49:57.8531...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
11:49:57.8565...	Malware_U3_W2_L2.exe	2416	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
11:49:57.9227...	Malware_U3_W2_L2.exe	2416	CreateFile	C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directo
11:49:57.9878...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation
11:49:57.9924...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
11:49:57.9961...	Malware_U3_W2_L2.exe	2416	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
11:49:58.0319...	Malware_U3_W2_L2.exe	2416	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
11:49:58.1305...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: ass
11:49:58.1359...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\WINDOWS	NO MORE FILES	
11:49:58.1395...	Malware_U3_W2_L2.exe	2416	CloseFile	C:\WINDOWS	SUCCESS	
11:49:58.1831...	Malware_U3_W2_L2.exe	2416	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
11:49:58.1891...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\WINDOWS\AppPatch	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: AcGenral.dll, 4: AcLayers.dll, 5: AcL
11:49:58.2291...	Malware_U3_W2_L2.exe	2416	QueryDirectory	C:\WINDOWS\AppPatch	NO MORE FILES	

Come possiamo vedere il Malware è attivo sul nostro sistema operativo, notando come abbia infettato e modificato molti dei parametri.

Queste sono le modifiche che sono state apportate sui processi e Thread



File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:49:56.8131...	Malware_U3_W2_L2.exe	2416	Process Start		SUCCESS	Parent PID: 1348, Command line: "C:\Documents and Settings\Admin
11:49:56.8132...	Malware_U3_W2_L2.exe	2416	Thread Create		SUCCESS	Thread ID: 2420
11:49:56.8648...	Malware_U3_W2_L2.exe	2416	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
11:49:56.9274...	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
11:50:00.5975...	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
11:50:01.0202...	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
11:50:01.3381...	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
11:50:01.7405...	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
11:50:01.7482...	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
11:50:01.7554...	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fe0000, Image Size: 0x11000
11:50:02.1950...	Malware_U3_W2_L2.exe	2416	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2424, Command line: "C:\WINDOWS\system32\svchost.exe"
11:50:03.2721...	Malware_U3_W2_L2.exe	2416	Thread Exit		SUCCESS	Thread ID: 2420, User Time: 0.0000000, Kernel Time: 1.5937500
11:50:03.2729...	Malware_U3_W2_L2.exe	2416	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 1.171875

Da questo screen possiamo notare come è stato creato un nuovo processo (Process Create) **svchost.exe,** è un processo di sistema che può ospitare uno o più servizi del sistema operativo Windows e dove possono essere inseriti dei file dannosi.

Quello che possiamo ipotizzare è che questo Malware sia un Trojan,