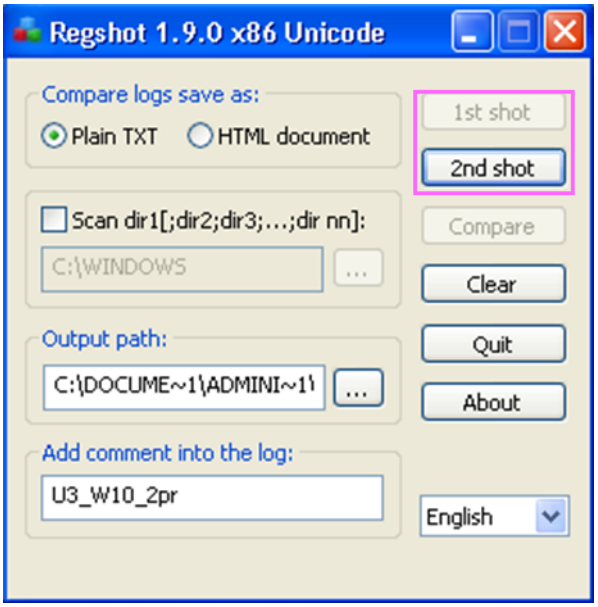
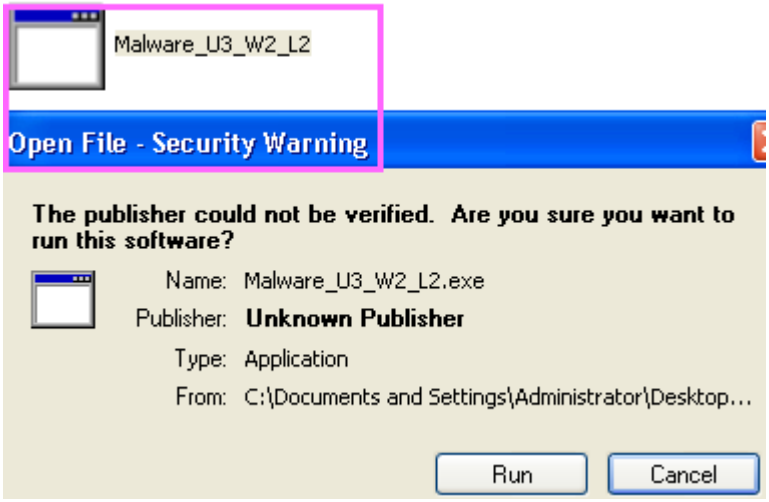
Report UNIT 3 WEEK 10.2

ANALISI DINAMICA

Avvio **Process Monitor** e con **RegShot** salvo la prima istantanea.



Faccio partire il malware.



Faccio un secondo shot e comparo i risultati.

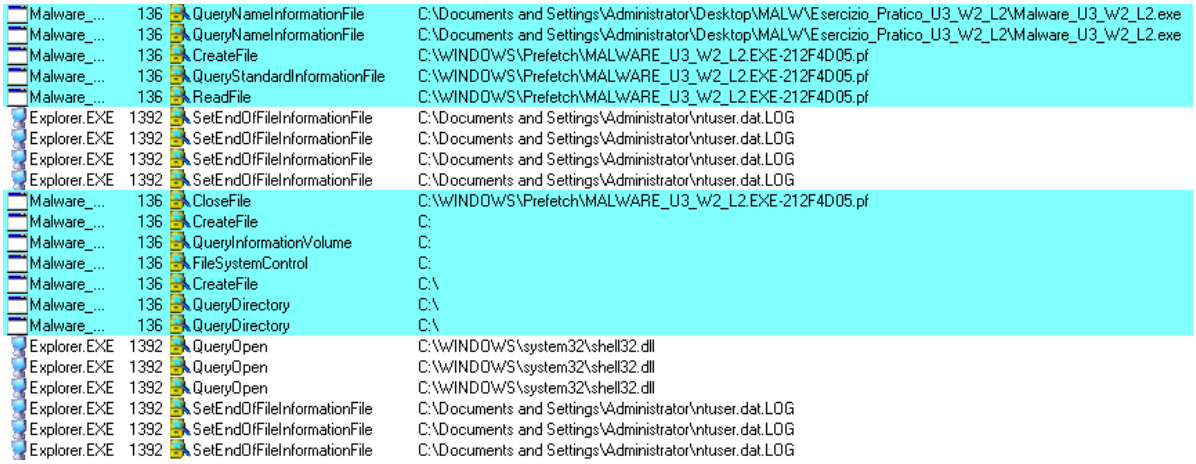
Sono state aggiunte 10 keys, 30 values e modificate 25 values per un totale di 65 modifiche al registro.

```
Regshot 1.9.0 x86 Unicode
Comments: U3_W10_2dopo
Datetime: 2023/7/4 12:21:59   ,   2023/7/4 12:27:12
Computer: WINXPS3 , WINXPS3
Username: Administrator , Administrator

----------------------------------
Keys added: 10
----------------------------------

----------------------------------
Values added: 30
----------------------------------

----------------------------------
Values modified: 25
----------------------------------

----------------------------------
Total changes: 65
----------------------------------
```

Su Process Monitor filtro per il file system.

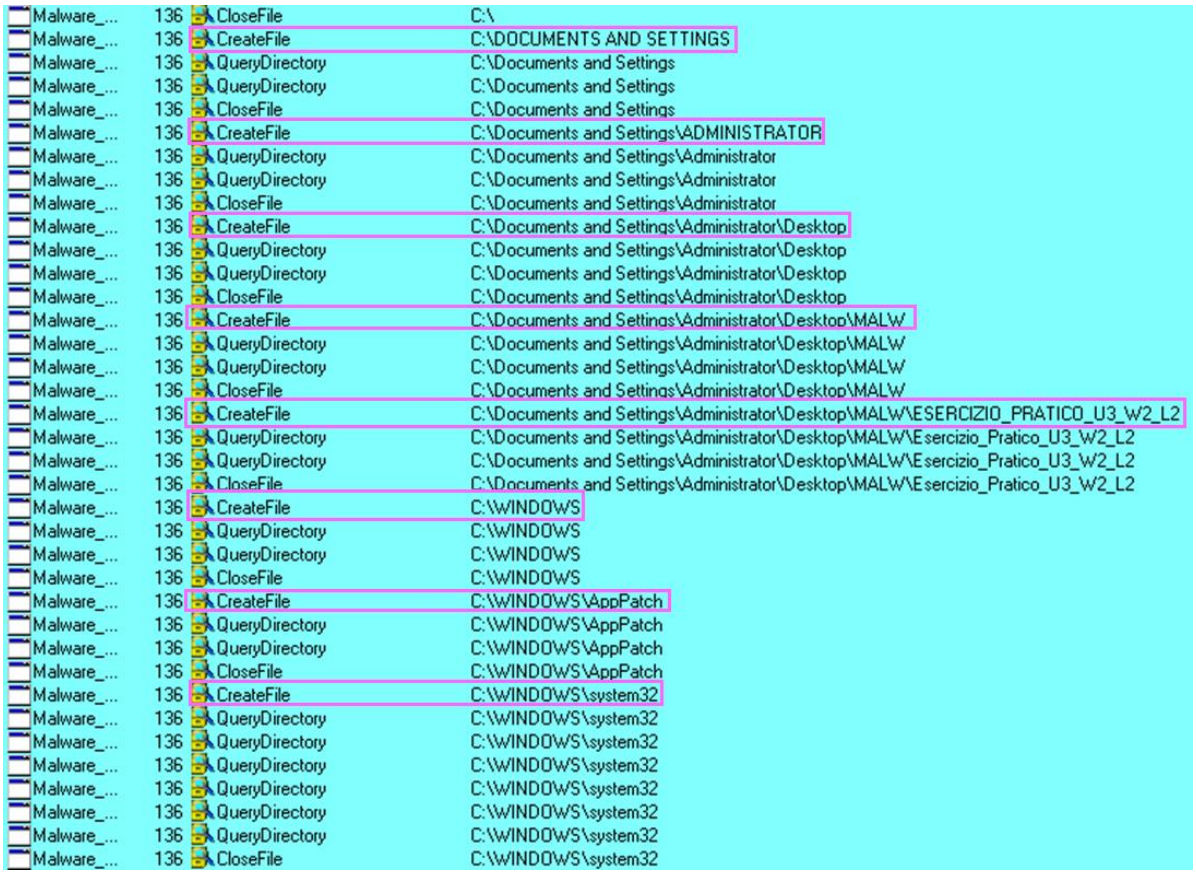
Aprendo il programma per la prima volta vengono creati file di **prefetching** nella cartella Prefetch per ottimizzare le prestazioni durante l'avvio. Successivamente viene ridimensionato il file ntuser.dat.LOG da parte di explorer.exe probabilmente per aggiungere nuove voci di registro o gestire le dimensioni del file stesso.

In seguito, viene chiuso il file di prefetching perché le risorse necessarie sono state caricate nella memoria. Viene creato un file in C, viene fatta una chiamata per ottenere informazioni sull'unità (QueryInformationVolume), viene fatta una chiamata per eseguire un'operazione legata al FileSystem(FileSystemControl). Ne consegue la creazione di un file nella directory C e vengono eseguite due query per ottenere informazioni sui file e le cartelle presenti all'interno di essa (QueryDirectory). QueryOpen verifica la possibilità di aprire la libreria shell32.dll.



Malware_...	136	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_...	136	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_...	136	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-212F4D05.pf
Malware_...	136	QueryStandardInformationFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-212F4D05.pf
Malware_...	136	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-212F4D05.pf
Explorer.EXE	1392	SetEndOfFileInformationFile	C:\Documents and Settings\Administrator\ntuser.dat.LOG
Explorer.EXE	1392	SetEndOfFileInformationFile	C:\Documents and Settings\Administrator\ntuser.dat.LOG
Explorer.EXE	1392	SetEndOfFileInformationFile	C:\Documents and Settings\Administrator\ntuser.dat.LOG
Explorer.EXE	1392	SetEndOfFileInformationFile	C:\Documents and Settings\Administrator\ntuser.dat.LOG
Malware_...	136	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-212F4D05.pf
Malware_...	136	CreateFile	C:
Malware_...	136	QueryInformationVolume	C:
Malware_...	136	FileSystemControl	C:
Malware_...	136	CreateFile	C:\
Malware_...	136	QueryDirectory	C:\
Malware_...	136	QueryDirectory	C:\
Explorer.EXE	1392	QueryOpen	C:\WINDOWS\system32\shell32.dll
Explorer.EXE	1392	QueryOpen	C:\WINDOWS\system32\shell32.dll
Explorer.EXE	1392	QueryOpen	C:\WINDOWS\system32\shell32.dll
Explorer.EXE	1392	SetEndOfFileInformationFile	C:\Documents and Settings\Administrator\ntuser.dat.LOG
Explorer.EXE	1392	SetEndOfFileInformationFile	C:\Documents and Settings\Administrator\ntuser.dat.LOG
Explorer.EXE	1392	SetEndOfFileInformationFile	C:\Documents and Settings\Administrator\ntuser.dat.LOG

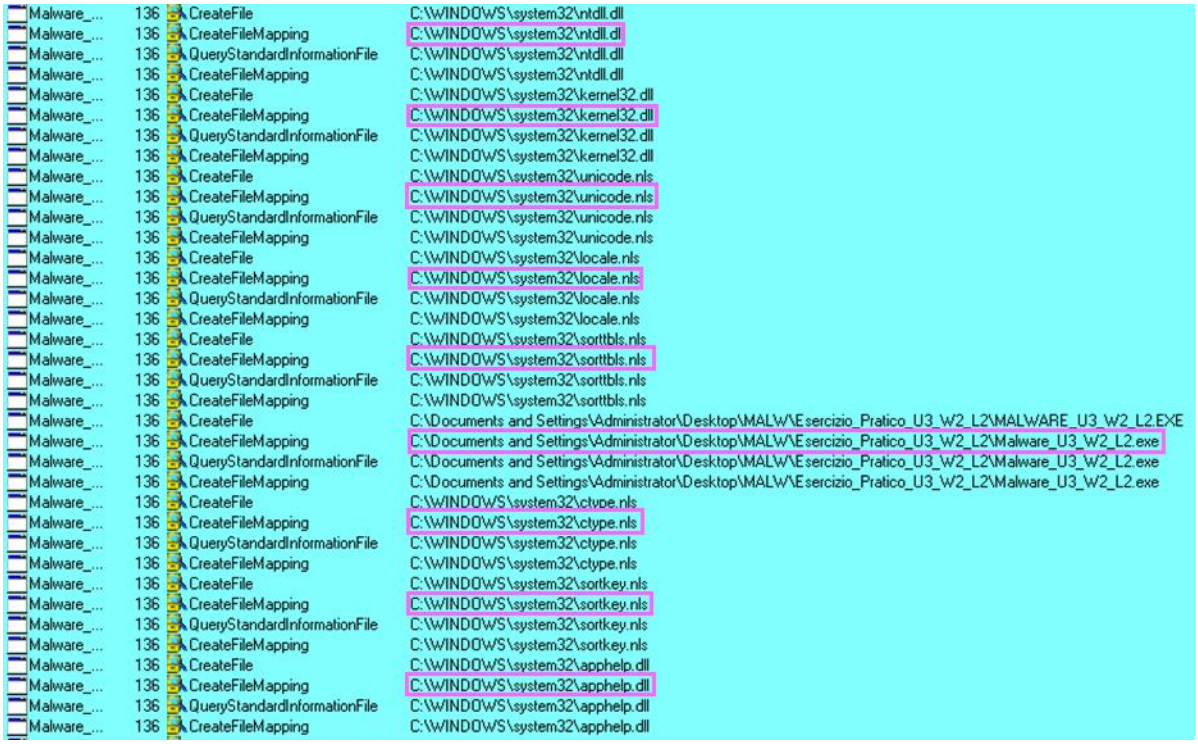
Successivamente vediamo lo stesso comportamento ripetersi per la creazione di più file, facendo query per ricavarne le informazioni all'interno e aprendo e chiudendo i correspettivi.



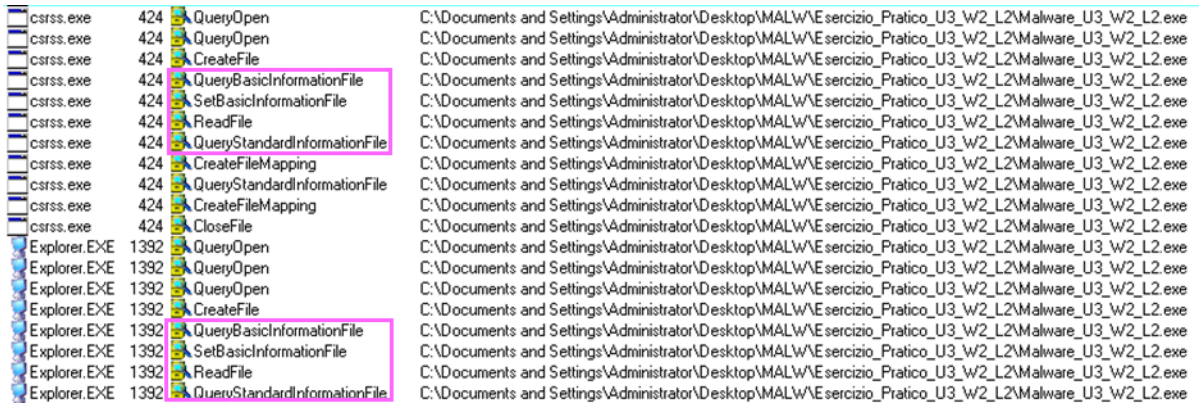
Malware_...	136	CloseFile	C:\
Malware_...	136	CreateFile	C:\DOCUMENTS AND SETTINGS
Malware_...	136	QueryDirectory	C:\Documents and Settings
Malware_...	136	QueryDirectory	C:\Documents and Settings
Malware_...	136	CloseFile	C:\Documents and Settings
Malware_...	136	CreateFile	C:\Documents and Settings\ADMINISTRATOR
Malware_...	136	QueryDirectory	C:\Documents and Settings\Administrator
Malware_...	136	QueryDirectory	C:\Documents and Settings\Administrator
Malware_...	136	CloseFile	C:\Documents and Settings\Administrator
Malware_...	136	CreateFile	C:\Documents and Settings\Administrator\Desktop
Malware_...	136	QueryDirectory	C:\Documents and Settings\Administrator\Desktop
Malware_...	136	QueryDirectory	C:\Documents and Settings\Administrator\Desktop
Malware_...	136	CloseFile	C:\Documents and Settings\Administrator\Desktop
Malware_...	136	CreateFile	C:\Documents and Settings\Administrator\Desktop\MALW
Malware_...	136	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\MALW
Malware_...	136	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\MALW
Malware_...	136	CloseFile	C:\Documents and Settings\Administrator\Desktop\MALW
Malware_...	136	CreateFile	C:\Documents and Settings\Administrator\Desktop\MALW\ESERCIZIO_PRATICO_U3_W2_L2
Malware_...	136	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L2
Malware_...	136	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L2
Malware_...	136	CloseFile	C:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L2
Malware_...	136	CreateFile	C:\WINDOWS
Malware_...	136	QueryDirectory	C:\WINDOWS
Malware_...	136	QueryDirectory	C:\WINDOWS
Malware_...	136	CloseFile	C:\WINDOWS
Malware_...	136	CreateFile	C:\WINDOWS\AppPatch
Malware_...	136	QueryDirectory	C:\WINDOWS\AppPatch
Malware_...	136	QueryDirectory	C:\WINDOWS\AppPatch
Malware_...	136	CloseFile	C:\WINDOWS\AppPatch
Malware_...	136	CreateFile	C:\WINDOWS\system32
Malware_...	136	QueryDirectory	C:\WINDOWS\system32
Malware_...	136	QueryDirectory	C:\WINDOWS\system32
Malware_...	136	QueryDirectory	C:\WINDOWS\system32
Malware_...	136	QueryDirectory	C:\WINDOWS\system32
Malware_...	136	QueryDirectory	C:\WINDOWS\system32
Malware_...	136	QueryDirectory	C:\WINDOWS\system32
Malware_...	136	CloseFile	C:\WINDOWS\system32

Viene creata una mappatura di file in memoria condivisa tra processi (CreateFileMapping) per accedere ai dati del file come se fossero presenti nella memoria del processo.

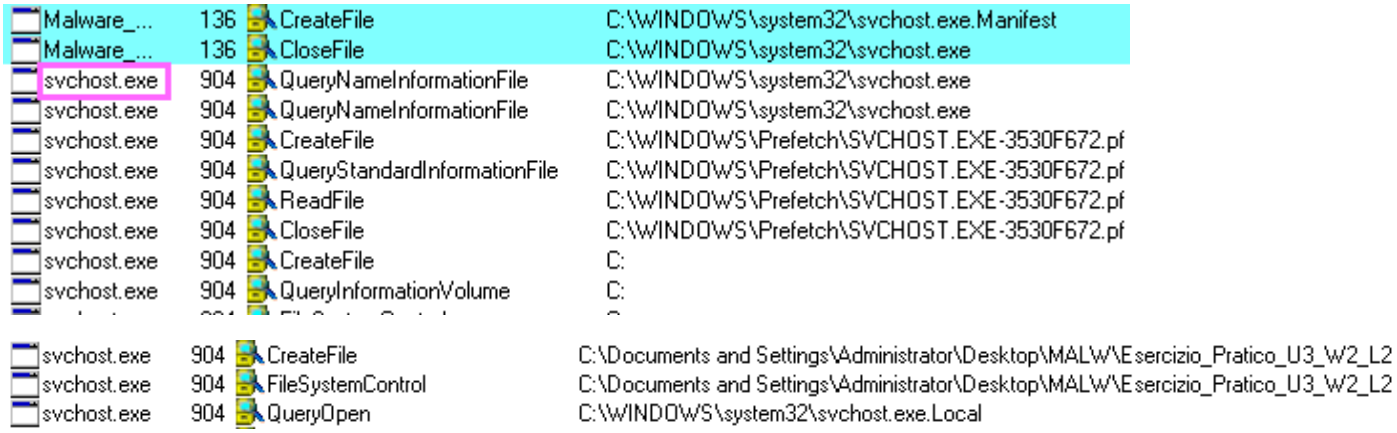
In generale, durante il primo avvio di un'applicazione, è comune che vengano effettuati vari processi di caricamento di librerie, accesso a file di dati e risorse, inizializzazione di vari componenti e preparazione dell'ambiente di esecuzione per l'applicazione stessa.



Sia csrss.exe che Explorer.EXE fanno delle query per ottenere informazioni sul file prima di aprirlo.



Questo comportamento si ripete non solo per il processo del Malware ma anche per svchost.exe, ricavando informazioni su files e directories.



Impostando il filtro per processi e threads vediamo come il comportamento visto precedentemente si rifletta anche a livello di threads e processi.

Una volta avviato il processo ed il thread del malware, vengono importate le librerie necessarie e viene fatto partire il processo svchost per ospitare i servizi necessari al funzionamento.

Lo stesso pattern si ripete per svchost.

Explorer.EXE	1392	Thread Create	
Explorer.EXE	1392	Process Create	C:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_...	136	Process Start	
Malware_...	136	Thread Create	
Malware_...	136	Load Image	C:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_...	136	Load Image	C:\WINDOWS\system32\ntdll.dll
Malware_...	136	Load Image	C:\WINDOWS\system32\kernel32.dll
Malware_...	136	Load Image	C:\WINDOWS\system32\apphelp.dll
Malware_...	136	Load Image	C:\WINDOWS\system32\version.dll
Malware_...	136	Load Image	C:\WINDOWS\system32\advapi32.dll
Malware_...	136	Load Image	C:\WINDOWS\system32\rpcrt4.dll
Malware_...	136	Load Image	C:\WINDOWS\system32\secur32.dll
Malware_...	136	Process Create	C:\WINDOWS\system32\svchost.exe
svchost.exe	904	Process Start	
svchost.exe	904	Thread Create	
svchost.exe	904	Load Image	C:\WINDOWS\system32\ntdll.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\kernel32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\user32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\gdi32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\shimeng.dll
svchost.exe	904	Load Image	C:\WINDOWS\AppPatch\AcGenral.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\advapi32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\rpcrt4.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\secur32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\winmm.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\ole32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\msvcrt.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\oleaut32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\msacm32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\version.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\shell32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\shlwapi.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\userenv.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\uxtheme.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\imm32.dll
svchost.exe	904	Load Image	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\comctl32.dll
svchost.exe	904	Load Image	C:\WINDOWS\system32\MSCTF.dll
Malware_...	136	Thread Exit	
Malware_...	136	Process Exit	
lsass.exe	516	Thread Exit	