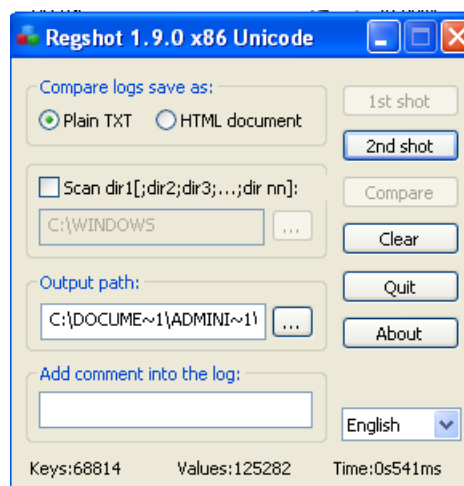


Analisi dinamica basica

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



Faccio partire il malware.



Faccio un secondo shot con Regshot e comparo i risultati. RegShot è un tool che permette di paragonare due istanze delle chiavi di registro salvate in due momenti diversi, prima e dopo l'esecuzione del malware.

La comparazione ci riporta l'aggiunta di 60 chiavi, 8 valori cancellati e 184 valori aggiunti.


```
-----
keys added: 60  values deleted: 8  values added: 184
-----
```

Mi sposto su process Monitor e filtro per il file system.

Aprendo il programma per la prima volta vengono creati file di prefetching nella cartella di Prefetch per ottimizzare le prestazioni durante l'avvio. Vedo che mi crea anche un file nel patch dove si trova il malware.

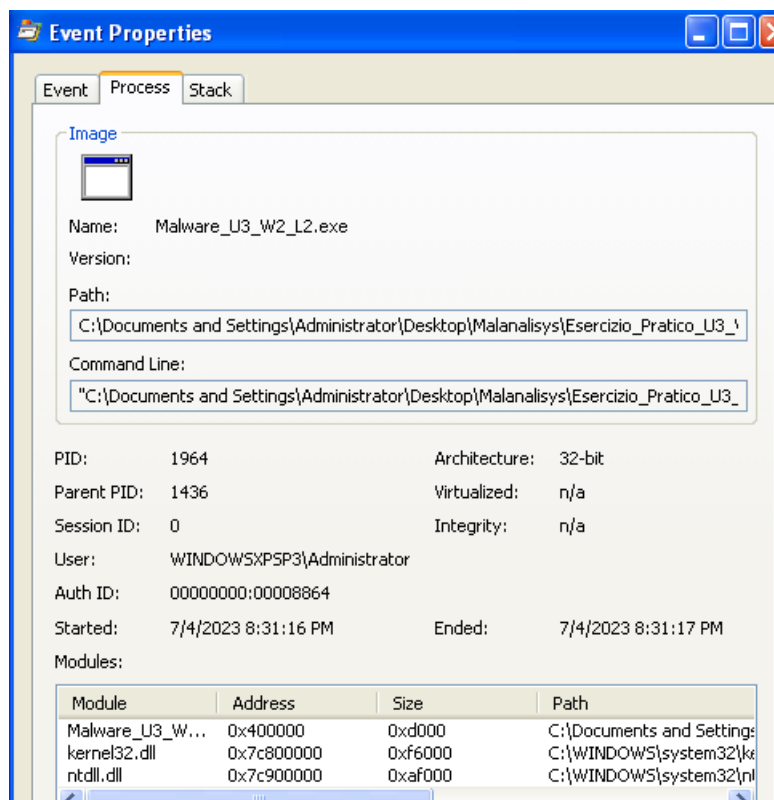
8:31:1...	Malware_U3_...	1964	QueryNameInfo...	C:\Documents and Settings\Administrat...	SUCCESS	Name: \Document...
8:31:1...	Malware_U3_...	1964	QueryNameInfo...	C:\Documents and Settings\Administrat...	SUCCESS	Name: \Document...
8:31:1...	Malware_U3_...	1964	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U...	NAME NOT FOUND	Desired Access: G...
8:31:1...	Explorer.EXE	1436	SetEndOfFileInf...	C:\Documents and Settings\Administrat...	SUCCESS	EndOfFile: 32,768
8:31:1...	Malware_U3_...	1964	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: E...
8:31:1...	Malware_U3_...	1964	FileSystemControl	C:\Documents and Settings\Administrat...	SUCCESS	Control: FSCTL_IS...
8:31:1...	Malware_U3_...	1964	QueryOpen	C:\Documents and Settings\Administrat...	NAME NOT FOUND	

Scorrendo in basso vedo che il malware esegue la lettura di diverse librerie e successivamente crea un file chiamato svchost.exe, stesso nome di un processo reale, caratteristica che si ritrova molto spesso nei malware, copiare nomi di processi reali.



8:31:1...	Malware_U3_...	1964	ReadFile	C:\Documents and Settings\Administrat...	SUCCESS	Offset: 4,096, Leng.
8:31:1...	Malware_U3_...	1964	ReadFile	C:\Documents and Settings\Administrat...	SUCCESS	Offset: 20,480, Len.
8:31:1...	Explorer.EXE	1436	QueryBasicInfor...	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 4/8/...
8:31:1...	Malware_U3_...	1964	ReadFile	C:\Documents and Settings\Administrat...	SUCCESS	Offset: 40,960, Len.
8:31:1...	Explorer.EXE	1436	SetBasicInfor...	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 1/1/...
8:31:1...	Explorer.EXE	1436	ReadFile	C:\Documents and Settings\Administrat...	SUCCESS	Offset: 0, Length: 12
8:31:1...	Malware_U3_...	1964	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: R...
8:31:1...	Malware_U3_...	1964	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
8:31:1...	Malware_U3_...	1964	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
8:31:1...	Malware_U3_...	1964	QueryOpen	C:\WINDOWS\system32\apphelp.dll	SUCCESS	CreationTime: 4/14...
8:31:1...	Malware_U3_...	1964	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: E...
8:31:1...	Malware_U3_...	1964	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
8:31:1...	Malware_U3_...	1964	QueryStandardl...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	AllocationSize: 126...
8:31:1...	Malware_U3_...	1964	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
8:31:1...	Malware_U3_...	1964	CloseFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	
8:31:1...	Malware_U3_...	1964	QueryOpen	C:\WINDOWS\system32\apphelp.dll	SUCCESS	CreationTime: 4/14...
8:31:1...	Malware_U3_...	1964	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: E...
8:31:1...	Malware_U3_...	1964	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
8:31:1...	Malware_U3_...	1964	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
8:31:1...	Malware_U3_...	1964	CloseFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	
8:31:1...	Malware_U3_...	1964	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: G...
8:31:1...	Malware_U3_...	1964	QueryStandardl...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 1,2...
8:31:1...	Malware_U3_...	1964	CreateFileMapp...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTy...

Infatti aprendo il processo il path risulta essere proprio quello del malware.



Event Properties

Event | **Process** | Stack

Image

Name: Malware_U3_W2_L2.exe

Version:

Path: C:\Documents and Settings\Administrator\Desktop\Malanalysis\Esercizio_Pratico_U3_...

Command Line: "C:\Documents and Settings\Administrator\Desktop\Malanalysis\Esercizio_Pratico_U3_...

PID: 1964 Architecture: 32-bit

Parent PID: 1436 Virtualized: n/a

Session ID: 0 Integrity: n/a

User: WINDOWSXPSP3\Administrator

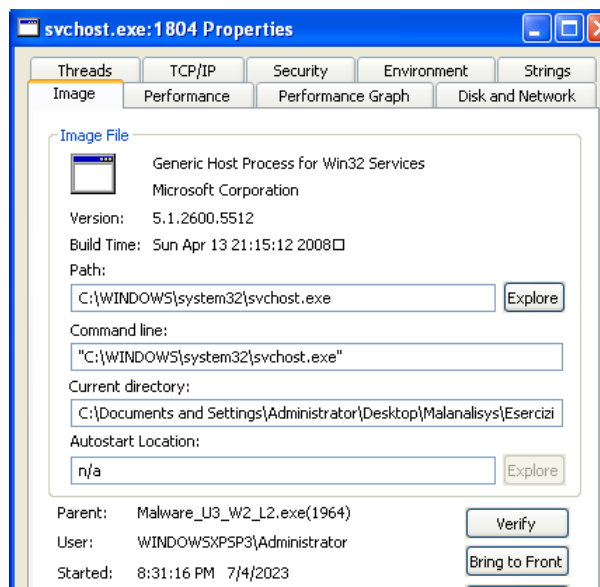
Auth ID: 00000000:00008864

Started: 7/4/2023 8:31:16 PM Ended: 7/4/2023 8:31:17 PM

Modules:

Module	Address	Size	Path
Malware_U3_W...	0x400000	0xd000	C:\Documents and Settings...
kernel32.dll	0x7c800000	0xf6000	C:\WINDOWS\system32\ke...
ntdll.dll	0x7c900000	0xaf000	C:\WINDOWS\system32\ntl...

Effettuo un ulteriore controllo con Process Explorer e vedo che c'è un eseguibile svchost.exe, nei processi attivi, non nei servizi eseguibili ma tra le applicazioni in esecuzione. Ci clicco e noto che anche qui la directory corrente è quella del malware.



Impostando ora il filtro per processi e threads vediamo come vengono caricate le librerie e viene creato il processo del svchost.exe, processo relativo al file creato precedentemente in file system.

8:31:1...	Explorer.EXE	1436	Process Create	C:\Documents and Settings\Administrat...	SUCCESS	PID: 1964, Comma...
8:31:1...	Malware_U3_...	1964	Process Start		SUCCESS	Parent PID: 1436, ...
8:31:1...	Malware_U3_...	1964	Thread Create		SUCCESS	Thread ID: 1960
8:31:1...	Malware_U3_...	1964	Load Image	C:\Documents and Settings\Administrat...	SUCCESS	Image Base: 0x400...
8:31:1...	Malware_U3_...	1964	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
8:31:1...	Malware_U3_...	1964	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
8:31:1...	csrss.exe	440	Thread Create		SUCCESS	Thread ID: 1968
8:31:1...	Malware_U3_...	1964	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b...
8:31:1...	Malware_U3_...	1964	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c...
8:31:1...	Malware_U3_...	1964	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
8:31:1...	Malware_U3_...	1964	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e...
8:31:1...	Malware_U3_...	1964	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
8:31:1...	Malware_U3_...	1964	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1804, Comma...
8:31:1...	svchost.exe	1804	Process Start		SUCCESS	Parent PID: 1964, ...
8:31:1...	svchost.exe	1804	Thread Create		SUCCESS	Thread ID: 1796
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e4...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0x77f...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\shimeng.dll	SUCCESS	Image Base: 0x5cb...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\AppPatch\AcGeneral.dll	SUCCESS	Image Base: 0x6f8...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\winmm.dll	SUCCESS	Image Base: 0x76b...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x774...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Image Base: 0x77c...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	Image Base: 0x771...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\msacm32.dll	SUCCESS	Image Base: 0x77b...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\shell32.dll	SUCCESS	Image Base: 0x7c9...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Image Base: 0x77f...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\userenv.dll	SUCCESS	Image Base: 0x769...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\uxtheme.dll	SUCCESS	Image Base: 0x5ad...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\imm32.dll	SUCCESS	Image Base: 0x763...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\WinSxS\x86_Microsoft...	SUCCESS	Image Base: 0x773...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\comctl32.dll	SUCCESS	Image Base: 0x5d0...
8:31:1...	svchost.exe	1804	Load Image	C:\WINDOWS\system32\MSCTF.dll	SUCCESS	Image Base: 0x747...
8:31:1...	Malware_U3_...	1964	Thread Exit		SUCCESS	Thread ID: 1960, ...
8:31:1...	Malware_U3_...	1964	Process Exit		SUCCESS	Exit Status: 0, User...
8:31:1...	svchost.exe	916	Thread Create		SUCCESS	Thread ID: 1988