

Analisi Dinamica Basica

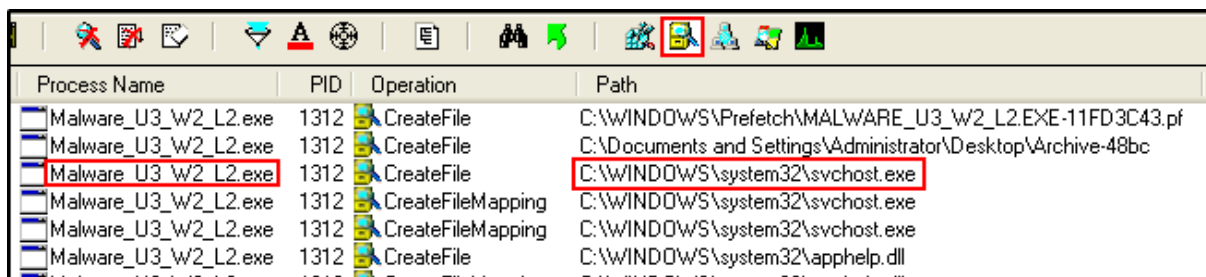
Traccia

Prendendo come riferimento l'esecuibile Malware_U3_W2_L2.exe rispondiamo 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
- Modifiche del registro dopo il malware
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Azioni malware su file system

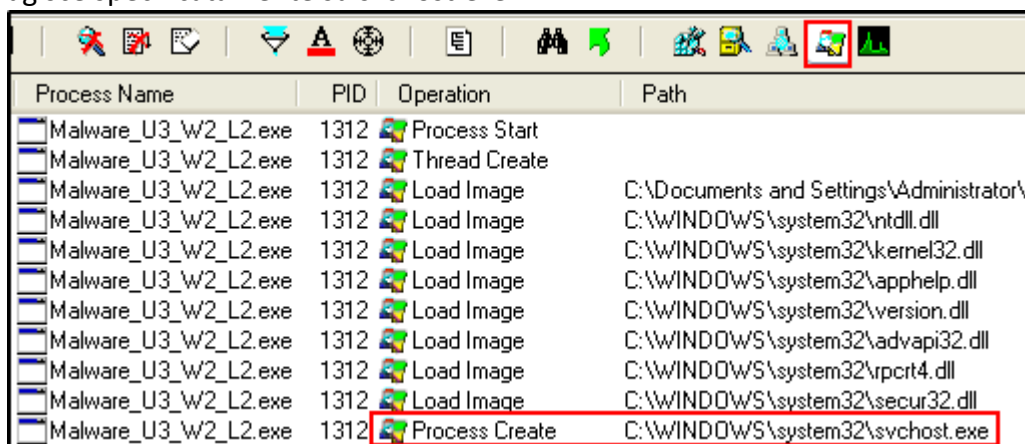
Filtrando per nome del file e tipo di file system andiamo a scoprire che il Malware in question va ad accedere e modificare processi di sistema come svchost.exe



Process Name	PID	Operation	Path
Malware_U3_W2_L2.exe	1312	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-11FD3C43.pf
Malware_U3_W2_L2.exe	1312	CreateFile	C:\Documents and Settings\Administrator\Desktop\Archive-48bc
Malware_U3_W2_L2.exe	1312	CreateFile	C:\WINDOWS\system32\svchost.exe
Malware_U3_W2_L2.exe	1312	CreateFileMapping	C:\WINDOWS\system32\svchost.exe
Malware_U3_W2_L2.exe	1312	CreateFileMapping	C:\WINDOWS\system32\svchost.exe
Malware_U3_W2_L2.exe	1312	CreateFile	C:\WINDOWS\system32\apphelp.dll

Azioni malware su Processi e Thread

Filtrando per nome del file e tipo di processi e thread andiamo a confermare che il Malware agisce specificatamente su svchost.exe



Process Name	PID	Operation	Path
Malware_U3_W2_L2.exe	1312	Process Start	
Malware_U3_W2_L2.exe	1312	Thread Create	
Malware_U3_W2_L2.exe	1312	Load Image	C:\Documents and Settings\Administrator\...
Malware_U3_W2_L2.exe	1312	Load Image	C:\WINDOWS\system32\ntdll.dll
Malware_U3_W2_L2.exe	1312	Load Image	C:\WINDOWS\system32\kernel32.dll
Malware_U3_W2_L2.exe	1312	Load Image	C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe	1312	Load Image	C:\WINDOWS\system32\version.dll
Malware_U3_W2_L2.exe	1312	Load Image	C:\WINDOWS\system32\advapi32.dll
Malware_U3_W2_L2.exe	1312	Load Image	C:\WINDOWS\system32\rpcrt4.dll
Malware_U3_W2_L2.exe	1312	Load Image	C:\WINDOWS\system32\secur32.dll
Malware_U3_W2_L2.exe	1312	Process Create	C:\WINDOWS\system32\svchost.exe

Modifiche di registro dopo il Malware

Con Regshot notiamo che il malware va a modificare il registro di sistema inserendo nuove voci

```
Regshot 1.9.0 x86 unicode
Comments:
Datetime: 2024/2/13 18:41:26 , 2024/2/13 18:41:35
Computer: WINDOWSXP , WINDOWSXP
Username: Administrator , Administrator
-----
Values added: 4
HKLM\SYSTEM\ControlSet001\Services\Kmixer\Enum\0: "sw\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9b365890-165f-11d0-a195-0020afd156e4}"
HKLM\SYSTEM\CurrentControlSet\Services\Kmixer\Enum\0: "sw\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9b365890-165f-11d0-a195-0020afd156e4}"
HKU\S-1-5-21-1645522239-813497703-854245398-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-ef1f-11d0-9888-006097deacf9}\Count\HR
ZR_EHACNGU:P:\qophzragf nag Fraggvatf\Nqzvavfgengbe\Qrfxgbc\Nepuvlr-48op\Znyjner_H3_J2_Y2.rkr: 08 00 00 00 06 00 00 00 c0 51 3e 41 ac 5e da 01
HKU\S-1-5-21-1645522239-813497703-854245398-500\Software\Microsoft\Windows\Shell\NoBgam\UICache\C:\Documents and
Settings\Administrator\Desktop\Archive-48bc\Malware_U3_W2_L2.exe: "Malware_U3_W2_L2"
```

Profilazione con correlazione operation e path

Esplorando ulteriormente la correlazione fra operation e path notiamo che il servizio svchost.exe precedentemente infettato dal malware va a scrivere un file nella cartella dove abbiamo eseguito il malware

Process Name	PID	Operation	Path
svchost.exe	1588	CreateFile	C:\Documents and Settings\Administrator\Desktop\Archive-48bc\practicalmalwareanalysis.log
svchost.exe	1588	QueryStandardInfor...	C:\Documents and Settings\Administrator\Desktop\Archive-48bc\practicalmalwareanalysis.log
svchost.exe	1588	WriteFile	C:\Documents and Settings\Administrator\Desktop\Archive-48bc\practicalmalwareanalysis.log
svchost.exe	1588	WriteFile	C:\Documents and Settings\Administrator\Desktop\Archive-48bc\practicalmalwareanalysis.log
svchost.exe	1588	WriteFile	C:\Documents and Settings\Administrator\Desktop\Archive-48bc\practicalmalwareanalysis.log
svchost.exe	1588	CloseFile	C:\Documents and Settings\Administrator\Desktop\Archive-48bc\practicalmalwareanalysis.log
Explorer.EXE	1132	NotifyChangeDirectory	C:\Documents and Settings\Administrator\Desktop\Archive-48bc

Cosa che andiamo a confermare scoprendo che si tratta di un Keylogger

