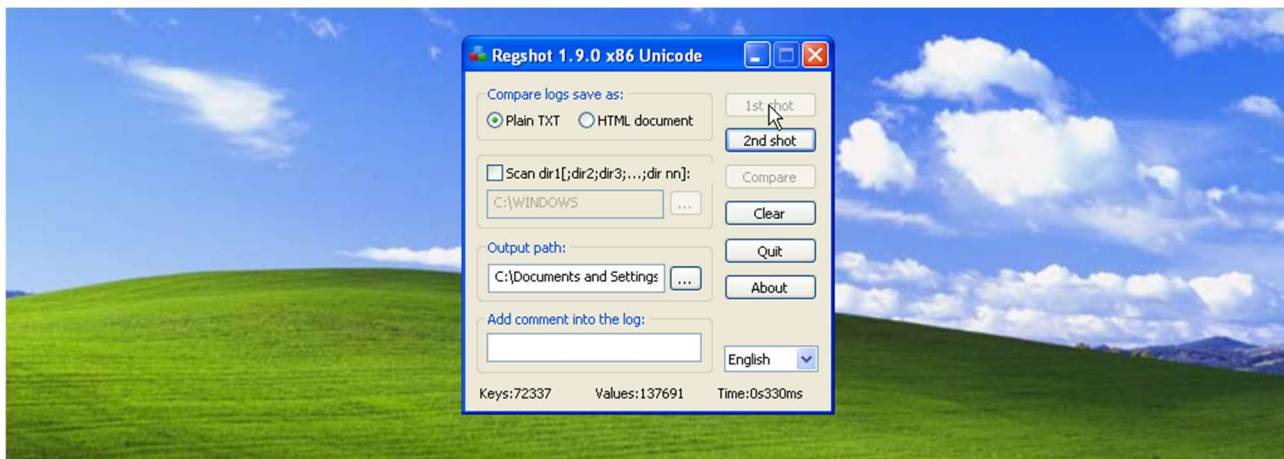


Esercizio 1 + 2

La prima azione da compiere è creare una istantanea del registro di sistema tramite RegShot prima dell'analisi del malware. Questo ci permetterà di identificare eventuali modifiche che si potrebbero andare a creare dopo l'esecuzione del malware.



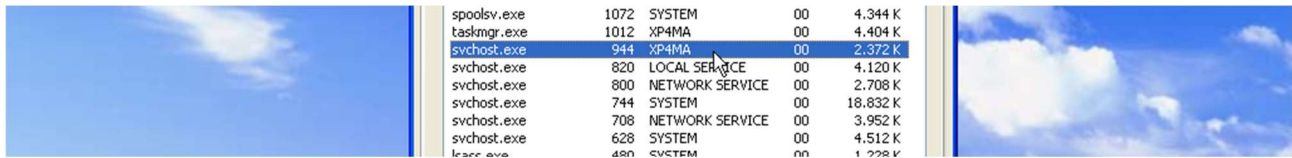
Lanciamo poi ProcMon utilizzando come filtro il nome del file infetto compreso di estensione, lanciamo il malware, lasciamo che l'output si popoli e creiamo poi una seconda istantanea tramite RegShot da utilizzare come confronto a fine processo.

16.31....	Malware_U3_W2_L2.exe	916	CloseFile	C:\WINDOWS	SUCCESS	
16.31....	Malware_U3_W2_L2.exe	916	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Dire...
16.31....	Malware_U3_W2_L2.exe	916	QueryDirectory	C:\WINDOWS\system32\svchost.exe	SUCCESS	Filter: svchost.exe, 1: svchost.exe
16.31....	Malware_U3_W2_L2.exe	916	CloseFile	C:\WINDOWS\system32	SUCCESS	
16.31....	Malware_U3_W2_L2.exe	916	CloseFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	
16.31....	Malware_U3_W2_L2.exe	916	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set V...
16.31....	Malware_U3_W2_L2.exe	916	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
16.31....	Malware_U3_W2_L2.exe	916	RegQueryValue	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\...	SUCCESS	Type: REG_DWORD, Length: 4, Da...
16.31....	Malware_U3_W2_L2.exe	916	RegQueryValue	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\...	SUCCESS	Type: REG_DWORD, Length: 4, Da...
16.31....	Malware_U3_W2_L2.exe	916	RegCloseKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
16.31....	Malware_U3_W2_L2.exe	916	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Siz...
16.31....	Malware_U3_W2_L2.exe	916	Load Image	C:\WINDOWS\system32\upcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Siz...
16.31....	Malware_U3_W2_L2.exe	916	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77e00000, Image Siz...
16.31....	Malware_U3_W2_L2.exe	916	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exe...	NAME NOT FOUND	Desired Access: Read
16.31....	Malware_U3_W2_L2.exe	916	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exe...	NAME NOT FOUND	Desired Access: Read
16.31....	Malware_U3_W2_L2.exe	916	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exe...	NAME NOT FOUND	Desired Access: Read
16.31....	Malware_U3_W2_L2.exe	916	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server\TCAP\Control	SUCCESS	Desired Access: Read
16.31....	Malware_U3_W2_L2.exe	916	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server\TCAP\Control	SUCCESS	Type: REG_DWORD, Length: 4, Da...

Analizzando la cattura di ProcMon notiamo che il malware ha richiamato diverse librerie di sistema per poi andare a creare un processo svchost.exe all'interno della directory di sistema (system32).

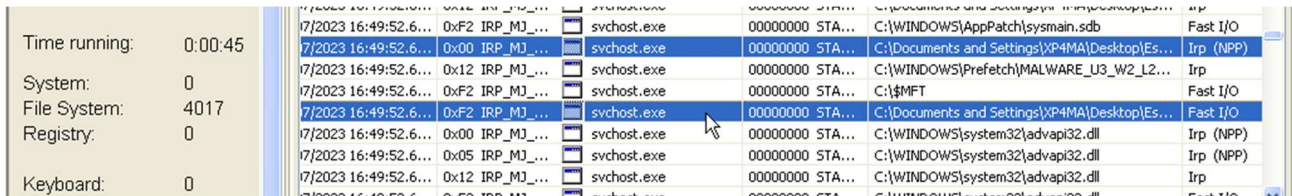
16.31....	Malware_U3_W2_L2.exe	916	RegCloseKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
16.31....	Malware_U3_W2_L2.exe	916	QueryNameInfo	C:\WINDOWS\system32\svchost.exe	SUCCESS	Name: \WINDOWS\system32\svch...
16.31....	Malware_U3_W2_L2.exe	916	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime: 14/04/2008 14.00.00...
16.31....	Malware_U3_W2_L2.exe	916	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Dire...
16.31....	Malware_U3_W2_L2.exe	916	QueryDirectory	C:\WINDOWS	SUCCESS	Filter: WINDOWS, 1: WINDOWS
16.31....	Malware_U3_W2_L2.exe	916	CloseFile	C:\	SUCCESS	
16.31....	Malware_U3_W2_L2.exe	916	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Dire...
16.31....	Malware_U3_W2_L2.exe	916	QueryDirectory	C:\WINDOWS\system32	SUCCESS	Filter: system32, 1: system32
16.31....	Malware_U3_W2_L2.exe	916	CloseFile	C:\WINDOWS	SUCCESS	
16.31....	Malware_U3_W2_L2.exe	916	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Dire...
16.31....	Malware_U3_W2_L2.exe	916	QueryDirectory	C:\WINDOWS\system32\svchost.exe	SUCCESS	Filter: svchost.exe, 1: svchost.exe
16.31....	Malware_U3_W2_L2.exe	916	CloseFile	C:\WINDOWS\system32	SUCCESS	
16.31....	Malware_U3_W2_L2.exe	916	QueryStandard...	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize: 16,384, EndOfFile: 14...
16.31....	Malware_U3_W2_L2.exe	916	CreateFileMap...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTypeCreateSection, ...
16.31....	Malware_U3_W2_L2.exe	916	QueryStandard...	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize: 16,384, EndOfFile: 14...
16.31....	Malware_U3_W2_L2.exe	916	CreateFileMap...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
16.31....	Malware_U3_W2_L2.exe	916	RegOpenKey	HKCU	SUCCESS	Desired Access: Read
16.31....	Malware_U3_W2_L2.exe	916	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS	Desired Access: Read

A questo punto del monitoraggio l'esecuibile appena creato viene lanciato e possiamo trovarlo facilmente anche nel Task Manager di Windows, prova che il malware è in esecuzione.



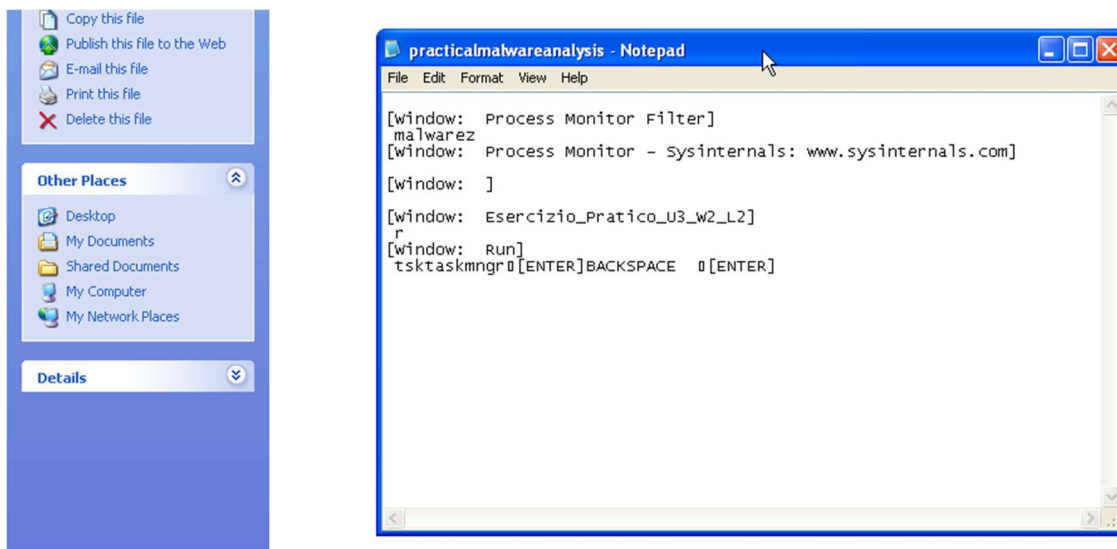
spoolsv.exe	1072	SYSTEM	00	4.344 K
taskmgr.exe	1012	XP4MA	00	4.404 K
svchost.exe	944	XP4MA	00	2.372 K
svchost.exe	820	LOCAL SERVICE	00	4.120 K
svchost.exe	800	NETWORK SERVICE	00	2.708 K
svchost.exe	744	SYSTEM	00	18.832 K
svchost.exe	708	NETWORK SERVICE	00	3.952 K
svchost.exe	628	SYSTEM	00	4.512 K
lsass.exe	480	SYSTEM	00	1.228 K

Lanciamo a questo punto MultiMon per monitorare più nel dettaglio le modifiche sul file system ed eventuali altre azioni.



Time running:	0:00:45	Time	Process	Operation	Path	Operation
System:	0	7/2023 16:49:52.6...	svchost.exe	00000000	C:\WINDOWS\AppPatch\sysmain.sdb	Fast I/O
File System:	4017	7/2023 16:49:52.6...	svchost.exe	00000000	C:\Documents and Settings\XP4MA\Desktop\Es...	Irp (NPP)
Registry:	0	7/2023 16:49:52.6...	svchost.exe	00000000	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2...	Irp
Keyboard:	0	7/2023 16:49:52.6...	svchost.exe	00000000	C:\\$MFT	Fast I/O
		7/2023 16:49:52.6...	svchost.exe	00000000	C:\Documents and Settings\XP4MA\Desktop\Es...	Fast I/O
		7/2023 16:49:52.6...	svchost.exe	00000000	C:\WINDOWS\system32\advapi32.dll	Irp (NPP)
		7/2023 16:49:52.6...	svchost.exe	00000000	C:\WINDOWS\system32\advapi32.dll	Irp (NPP)
		7/2023 16:49:52.6...	svchost.exe	00000000	C:\WINDOWS\system32\advapi32.dll	Irp
		7/2023 16:49:52.6...	svchost.exe	00000000	C:\WINDOWS\system32\advapi32.dll	Fast I/O

Notiamo subito che il processo svchost.exe visto in precedenza va a creare un file di testo nella cartella di origine del malware.



Raggiungendo il percorso indicatoci da MultiMon troviamo il file citato in precedenza; analizzandone il contenuto si può facilmente capire che il malware in questione è un logger. Per concludere andiamo ad analizzare il file di log di RegShot creato in precedenza per vedere quali e quante modifiche sono state apportate al registro durante la nostra analisi.

```
-----
Values added: 159
-----
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}\Class: "PROCMON23"
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}\NoDisplayClass: "1"
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}\NoUseClass: "1"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\NextInstance: 0x00000001
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Service: "PROCMON23"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Legacy: 0x00000001
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\ConfigFlags: 0x00000000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Class: "LegacyDriver"
```

Ovviamente non tutte le aggiunte sono da imputarsi al malware, in quanto il registro di sistema di Windows viene modificato continuamente durante l'esecuzione del sistema operativo. Un confronto tra l'output di ProcMon e il log di RegShot ci darà la conferma del numero reale delle modifiche a cui prestare attenzione.