

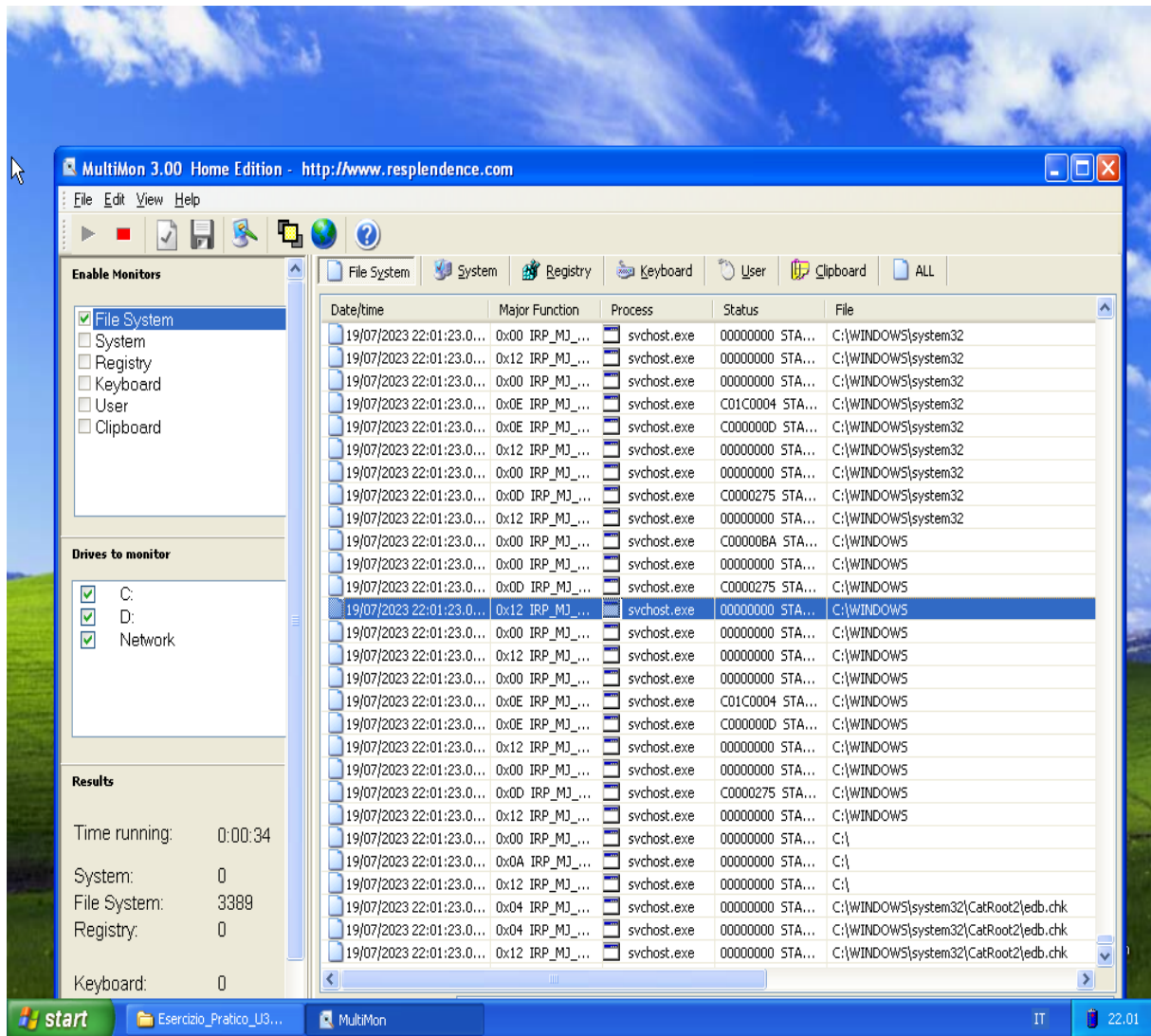
M6 D1

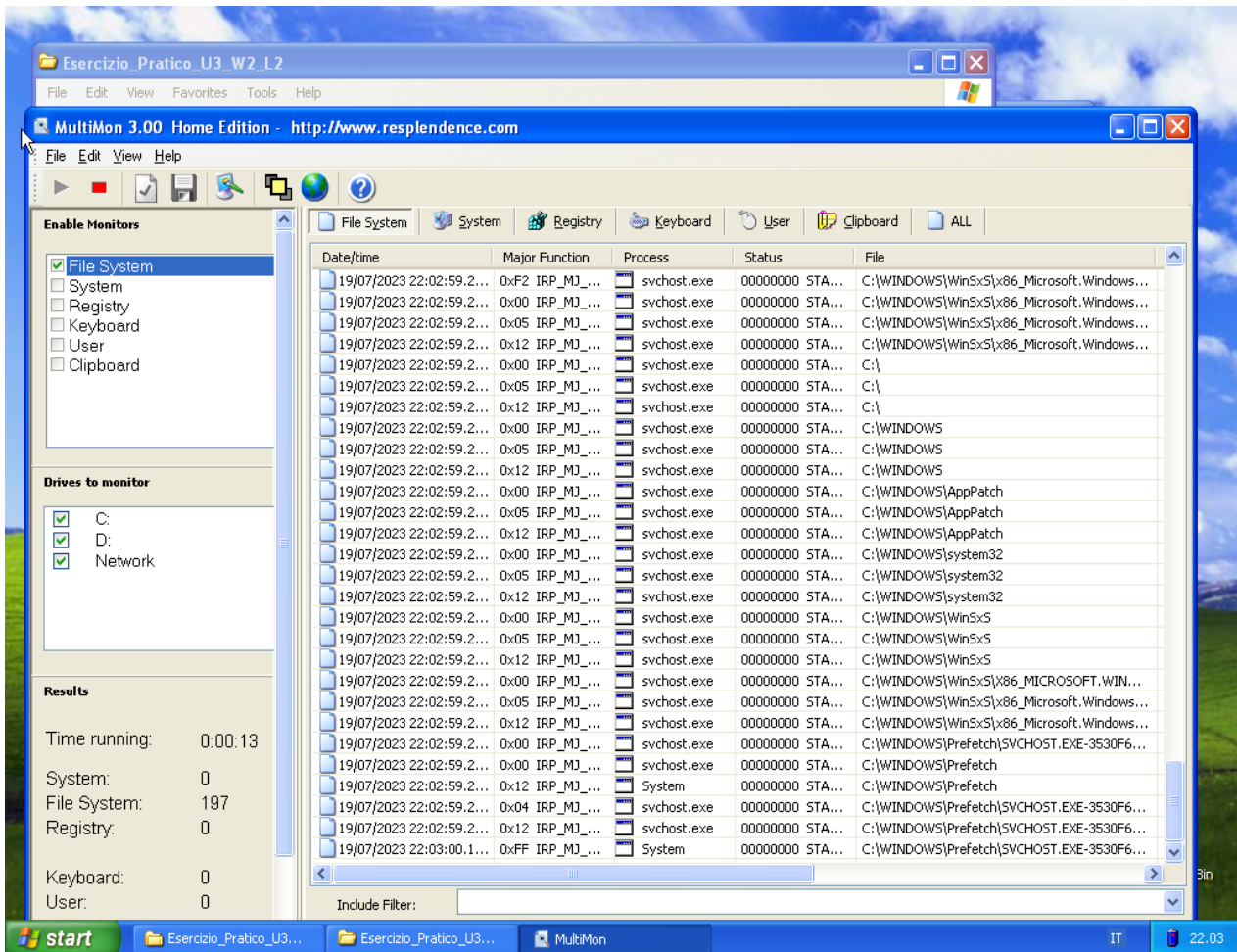
ESERCIZIO 2

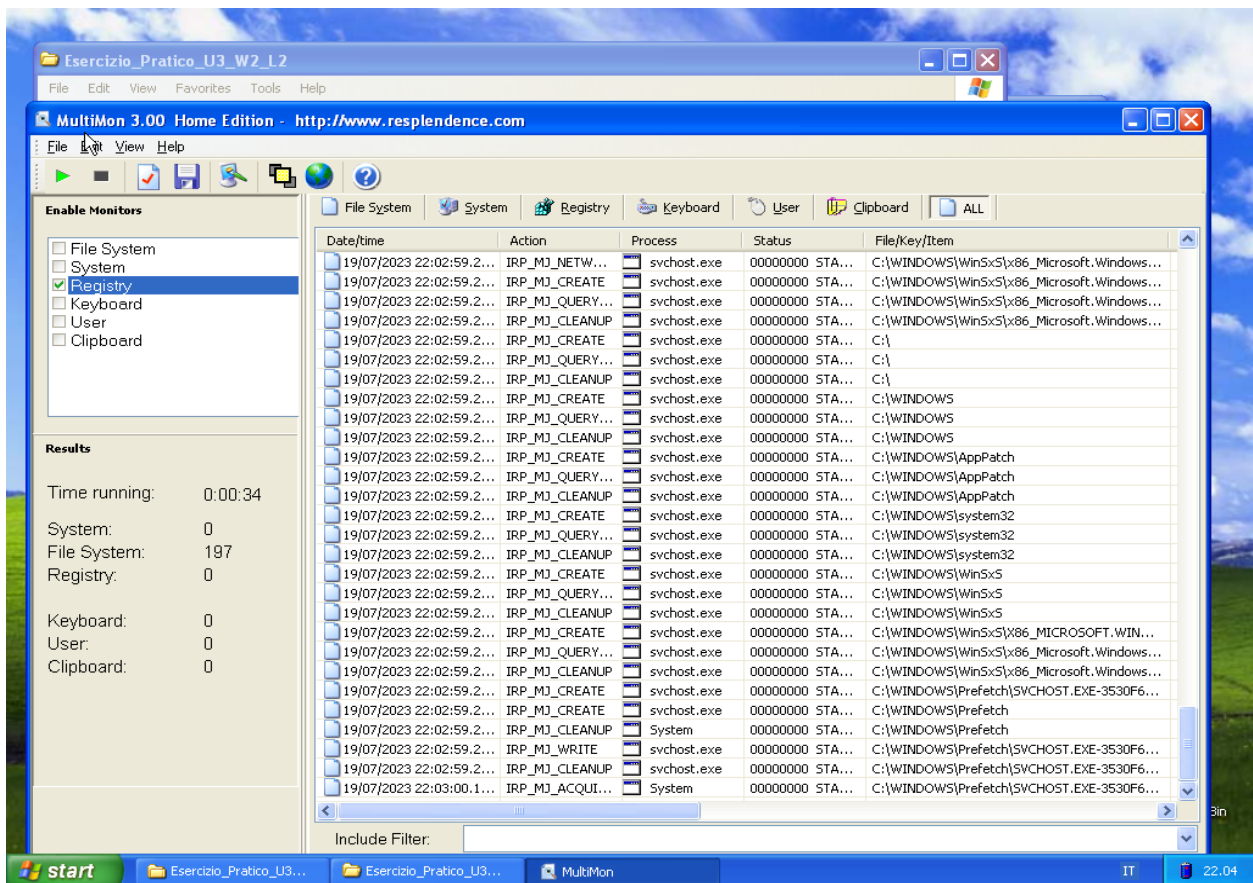
ANALISI DINAMICA BASICA

ESECUZIONE DEL MALWARE


UTILIZZO E RISPOSTA DEL TOOL MULTIMON







A questo punto del monitoraggio l'eseguibile 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	SP4MA	00	4,404 K
svchost.exe	944	SP4MA	00	2,372 K
svchost.exe	620	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	688	SYSTEM	00	1,756 K

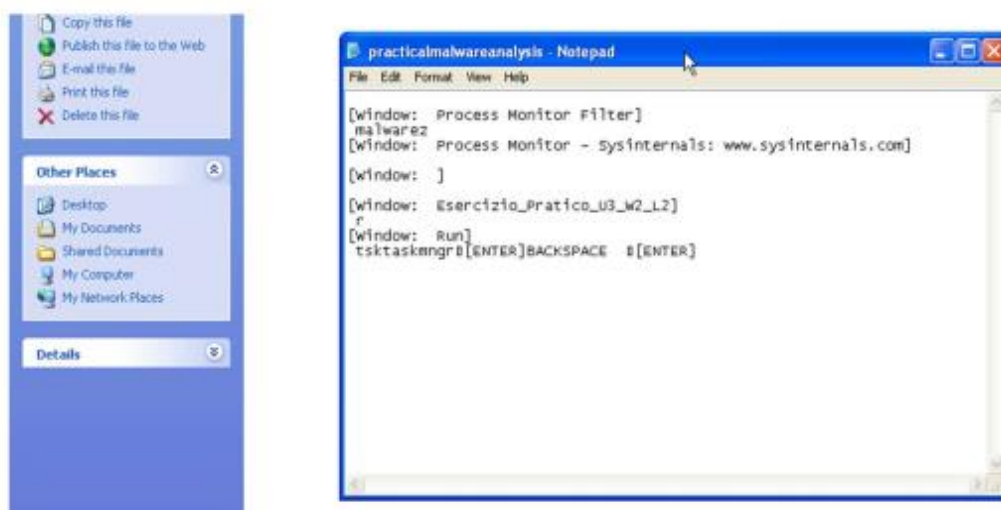
Lanciamo a questo punto MultiMon per monitorare più nel dettaglio le modifiche sul file system ed eventuali altre azioni.



Time running:	0:00:45
System:	0
File System:	4017
Registry:	0
Keyboard:	0

Time	Process	Operation	Path	Result
7/2023 16:49:52.6...	svchost.exe	0x02 IRP_MJ_...	C:\WINDOWS\system32\advapi32.dll	Fast I/O
7/2023 16:49:52.6...	svchost.exe	0x00 IRP_MJ_...	C:\WINDOWS\system32\advapi32.dll	Fast I/O
7/2023 16:49:52.6...	svchost.exe	0x02 IRP_MJ_...	C:\WINDOWS\system32\advapi32.dll	Fast I/O
7/2023 16:49:52.6...	svchost.exe	0x00 IRP_MJ_...	C:\WINDOWS\system32\advapi32.dll	Fast I/O
7/2023 16:49:52.6...	svchost.exe	0x02 IRP_MJ_...	C:\WINDOWS\system32\advapi32.dll	Fast I/O
7/2023 16:49:52.6...	svchost.exe	0x00 IRP_MJ_...	C:\WINDOWS\system32\advapi32.dll	Fast I/O
7/2023 16:49:52.6...	svchost.exe	0x02 IRP_MJ_...	C:\WINDOWS\system32\advapi32.dll	Fast I/O
7/2023 16:49:52.6...	svchost.exe	0x00 IRP_MJ_...	C:\WINDOWS\system32\advapi32.dll	Fast I/O
7/2023 16:49:52.6...	svchost.exe	0x02 IRP_MJ_...	C:\WINDOWS\system32\advapi32.dll	Fast I/O
7/2023 16:49:52.6...	svchost.exe	0x00 IRP_MJ_...	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-04D25EB00905}\Class: "PROCMON23"
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB00905}\ModifiableClass: "1"
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB00905}\ModifiableClass: "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\ConfFlags: 0x00000000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\ConfFlags: 0x00000000

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.