S10-L2

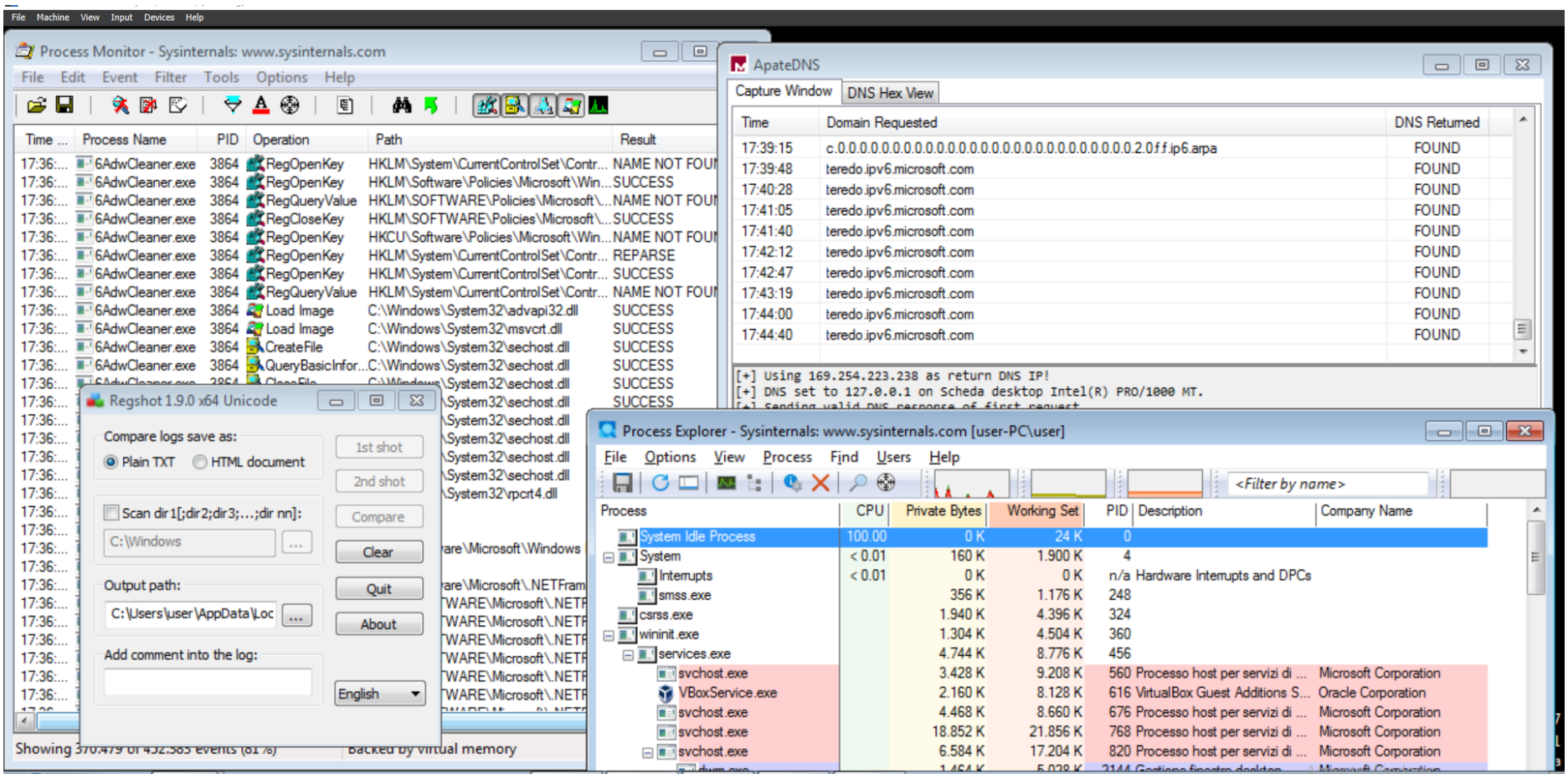
Introduzione

Prima di iniziare a lavorare facciamo uno snapshot per poter, a fine analisi, tornare a questo punto (pre-apertura del malware).

Spostiamoci in rete interna per evitare propagazioni (non sappiamo ancora cosa faccia questo malware).

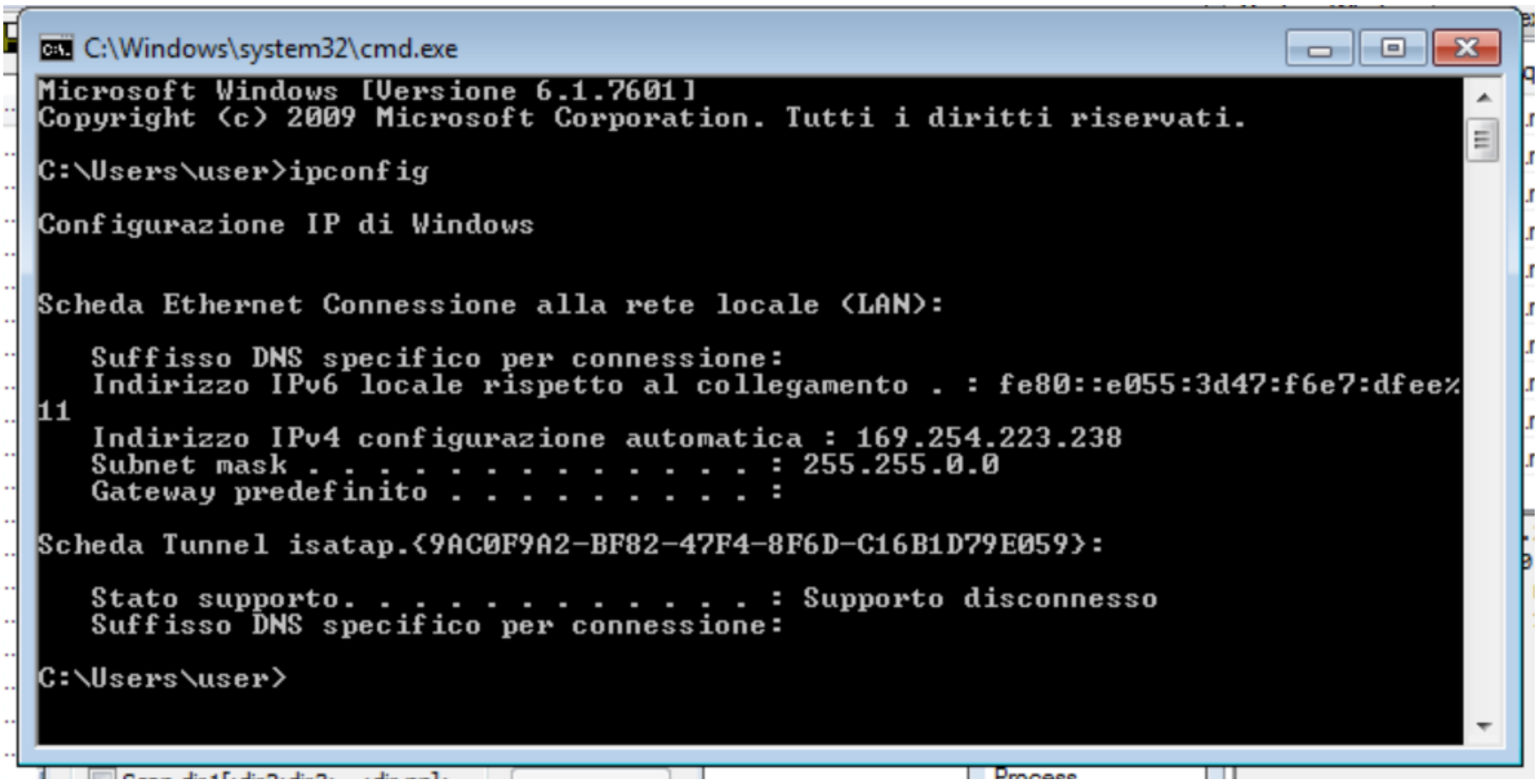
Strumenti

Ecco, in un unico screen, gli strumenti che utilizzeremo.
Il focus è su ProcMon e RegShot

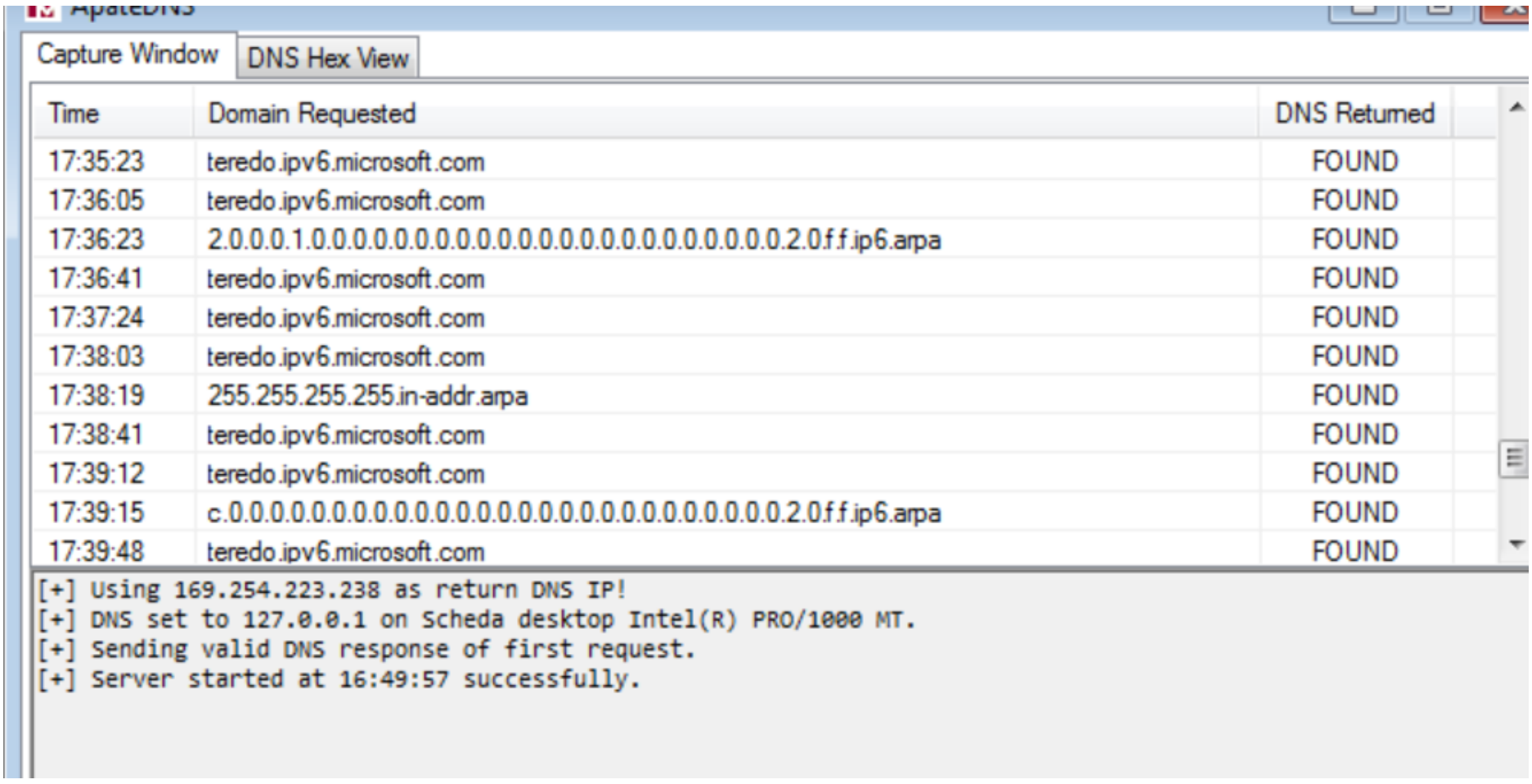


Avviamoli con ordine.

Prima di tutto dobbiamo vedere il nostro ip (Servirà in ApaceDNS)



Inseriamolo in ApaceDNS e lanciamo il tutto. Questo monitorerà la rete.



Avviamo regShot e facciamo il primo snap.

Avviamo il malware, facciamo la scansione e, finita, lasciamo il secondo snap (prima di questo abbiamo anche lanciato Procmon, ovvero process monitor).

Fatto questo compariamo i risultati.

~res-x64 - Blocco note

File Modifica Formato Visualizza ?

```
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2024/7/30 14:44:44   ,   2024/7/30 15:39:39
Computer: USER-PC , USER-PC
Username: user , user

----------------------------------
Keys added: 54
----------------------------------
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control
HKLM\SYSTEM\ControlSet001\services\PROCMON23
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Instances
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Instances\Process Monitor 23 Instance
HKLM\SYSTEM\ControlSet001\services\PROCMON24
HKLM\SYSTEM\ControlSet001\services\PROCMON24\Instances
HKLM\SYSTEM\ControlSet001\services\PROCMON24\Instances\Process Monitor 24 Instance
HKLM\SYSTEM\CurrentControlSet\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Instances
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Instances\Process Monitor 23 Instance
HKLM\SYSTEM\CurrentControlSet\services\PROCMON24
HKLM\SYSTEM\CurrentControlSet\services\PROCMON24\Instances
HKLM\SYSTEM\CurrentControlSet\services\PROCMON24\Instances\Process Monitor 24 Instance
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\f1eb6db9_0\{21
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\2206a68f_0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\2206a68f_0\{21

----------------------------------
Values deleted: 1
----------------------------------
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\C:\Users\user\AppData\Roaming\Mic

----------------------------------
Values added: 171
----------------------------------
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5\Blob:  5C 00 00 00 01 00 00 00 04 00 00 00 00 08 0(
 7F 00 00 00 01 00 00 00 2A 00 00 00 30 28 06 08 2B 06 01 05 05 07 03 02 06 08 2B 06 01 05 05 07 03 03 06 08 2B 06 01 05 05 07 03 04 06 08 2B 06 01 05 05 07
13 16 56 65 72 69 53 69 67 6E 20 54 72 75 73 74 20 4E 65 74 77 6F 72 6B 31 3A 30 38 06 03 55 04 0B 13 31 28 63 29 20 32 30 30 36 20 56 65 72 69 53 69 67 6E 2
5 72 69 53 69 67 6E 20 43 6C 61 73 73 20 33 20 50 75 62 6C 69 63 20 50 72 69 6D 61 72 79 20 43 65 72 74 69 66 69 63 61 74 69 6F 6E 20 41 75 74 68 6F 72 69 74
 33 0A CF 5D 3F 34 87 96 8A EE 53 E8 25 15 02 03 01 00 01 A3 81 B2 30 81 AF 30 0F 06 03 55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30 0E 06 03 55 1D 0F 01 01 FF
19 44 D2 41 7A 05 69 4A 58 4F 60 CA 7E 82 6A 0B 02 AA 25 17 39 B5 DB 7F E7 84 65 2A 95 8A BD 86 DE 5E 81 16 83 2D 10 CC DE FD A8 82 2A 6D 28 1F 0D 0B C4 E5 (
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\MaxFileSize: 0x00100000

HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\ProcMon.Logfile.1\:  "ProcMon Log File"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\ProcMon.Logfile.1\DefaultIcon\: ""C:\Users\user\Desktop\Software Malware analysis\SysinternalsSuite\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\ProcMon.Logfile.1\shell\open\command\: ""C:\Users\user\Desktop\Software Malware analysis\Sysinternal

----------------------------------
Values modified: 51
----------------------------------
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\WmiLastTime:  FF 26 54 94 8C E2 DA 01
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\WmiLastTime:  24 EC D5 1C 93 E2 DA 01
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\TransientValue:  3B 20 04 79 77 5B 1D 40
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\TransientValue:  06 A8 B5 DF A8 6C 1D 40
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\E12DFB4B41D7D9C32B30514BAC1D81D8385E2D46\Blob:  68 00 00 00 01 00 00 00 08 00 00 00 00 40 91
 2B 06 01 04 01 82 37 0A 03 04 06 08 2B 06 01 05 05 07 03 08 7E 00 00 00 01 00 00 00 08 00 00 00 00 00 63 F5 89 26 D7 01 20 00 00 00 01 00 00 00 6A 04 00 00
69 74 79 31 1E 30 1C 06 03 55 04 0A 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4E 65 74 77 6F 72 6B 31 21 30 1F 06 03 55 04 0B 13 18 68 74 74 70 3A 2F 2
9 28 FF BA 2E 11 C2 E5 E8 5B 92 48 FB 47 0B C2 6C DA AD 32 83 41 F3 A5 E5 41 70 FD 65 90 6D FA FA 51 C4 F9 BD 96 2B 19 04 2C D3 6D A7 DC F0 7F 6F 83 65 E2 6A
 48 F9 6B 25 25 2D 51 B6 2C 6D 45 C1 98 C8 8A 56 5D 3E EE 43 4E 3E 6B 27 8E D0 3A 4B 85 0B 5F D3 ED 6A A7 75 CB D1 5A 87 2F 39 75 13 5A 72 B0 02 81 9F BE F0
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\E12DFB4B41D7D9C32B30514BAC1D81D8385E2D46\Blob:  5C 00 00 00 01 00 00 00 04 00 00 00 00 08 00
 00 00 30 20 06 08 2B 06 01 05 05 07 03 03 06 0A 2B 06 01 04 01 82 37 0A 03 04 06 08 2B 06 01 05 05 07 03 08 7E 00 00 00 01 00 00 00 08 00 00 00 00 00 63 F5
06 03 55 04 06 13 02 55 53 31 0B 30 09 06 03 55 04 08 13 02 55 54 31 17 30 15 06 03 55 04 07 13 0E 53 61 6C 74 20 4C 61 6B 65 20 43 69 74 79 31 1E 30 1C 06 0
4 17 B7 FC 85 BE A4 AB C4 1C 31 DD D7 B6 D1 E4 F0 EF DF 16 8F B2 52 93 D7 A1 D4 89 A1 07 2E BF E1 01 12 42 1E 1A E1 D8 95 34 DB 64 79 28 FF BA 2E 11 C2 E5 E8
 4C C8 47 5A 69 EA E8 F0 35 35 F4 D0 25 F3 C8 A6 A4 87 4A BD 1B B1 73 08 BD D4 C3 CA B6 35 BB 59 86 77 31 CD A7 80 14 AE 13 EF FC B1 48 F9 6B 25 25 2D 51 B6
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000003
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000005
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\S-1-5-21-3771313050-58705377-3452663501-1001\Extension-List\{00000000-0000-0000-0000-000000

HKU\S-1-5-21-3771313050-58705377-34526

----------------------------------
Total changes: 277
----------------------------------
```

Tornando su Procmon possiamo notare cosa questo abbia provato a fare

Time ...	Process Name	PID	Operation	Path	Result	Detail
17:36:...	6AdwCleaner.exe	3864	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
17:36:...	6AdwCleaner.exe	3864	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 16
17:36:...	6AdwCleaner.exe	3864	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7fef...
17:36:...	6AdwCleaner.exe	3864	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7fef...
17:36:...	6AdwCleaner.exe	3864	CreateFile	C:\Windows\System32\sechost.dll	SUCCESS	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	QueryBasicInfor...	C:\Windows\System32\sechost.dll	SUCCESS	CreationTime: 14/0...
17:36:...	6AdwCleaner.exe	3864	CloseFile	C:\Windows\System32\sechost.dll	SUCCESS	
17:36:...	6AdwCleaner.exe	3864	CreateFile	C:\Windows\System32\sechost.dll	SUCCESS	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	CreateFileMapp...	C:\Windows\System32\sechost.dll	FILE LOCKED WI...	SyncType: SyncTy...
17:36:...	6AdwCleaner.exe	3864	CreateFileMapp...	C:\Windows\System32\sechost.dll	SUCCESS	SyncType: SyncTy...
17:36:...	6AdwCleaner.exe	3864	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7fef...
17:36:...	6AdwCleaner.exe	3864	CloseFile	C:\Windows\System32\sechost.dll	SUCCESS	
17:36:...	6AdwCleaner.exe	3864	Load Image	C:\Windows\System32\vpcrt4.dll	SUCCESS	Image Base: 0x7fef...
17:36:...	6AdwCleaner.exe	3864	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
17:36:...	6AdwCleaner.exe	3864	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
17:36:...	6AdwCleaner.exe	3864	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
17:36:...	6AdwCleaner.exe	3864	RegOpenKey	HKLM\Software\Microsoft\.NETFrame...	SUCCESS	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	RegQueryKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Query: Cached, Su...
17:36:...	6AdwCleaner.exe	3864	RegEnumKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Index: 4, Name: v4.0
17:36:...	6AdwCleaner.exe	3864	RegEnumKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Index: 3, Name: v2.0
17:36:...	6AdwCleaner.exe	3864	RegEnumKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Index: 2, Name: U...
17:36:...	6AdwCleaner.exe	3864	RegEnumKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Index: 1, Name: st...
17:36:...	6AdwCleaner.exe	3864	RegEnumKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Index: 0, Name: Ap...
17:36:...	6AdwCleaner.exe	3864	RegQueryKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Query: HandleTag...
17:36:...	6AdwCleaner.exe	3864	RegOpenKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	RegQueryKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Query: Cached, Su...
17:36:...	6AdwCleaner.exe	3864	RegEnumValue	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Index: 0, Name: 30...
17:36:...	6AdwCleaner.exe	3864	RegCloseKey	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	
17:36:...	6AdwCleaner.exe	3864	CreateFile	C:\Windows\System32\MSCOREE.DLL...	NAME NOT FOUND	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
17:36:...	6AdwCleaner.exe	3864	RegOpenKey	HKLM\Software\Microsoft\.NETFrame...	SUCCESS	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFR...	SUCCESS	Type: REG_SZ, Le...
17:36:...	AdwereCleaner....	3648	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
17:36:...	AdwereCleaner....	3648	CloseFile	C:\Windows\winsxs\x86_microsoft.wind...	SUCCESS	
17:36:...	AdwereCleaner....	3648	RegCloseKey	HKCU\Software\Classes	SUCCESS	
17:36:...	AdwereCleaner....	3648	CloseFile	C:\Users\user\AppData\Local	SUCCESS	
17:36:...	6AdwCleaner.exe	3864	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	QueryBasicInfor...	C:\Windows\System32\imm32.dll	SUCCESS	CreationTime: 14/0...
17:36:...	6AdwCleaner.exe	3864	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS	
17:36:...	6AdwCleaner.exe	3864	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	CreateFileMapp...	C:\Windows\System32\imm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
17:36:...	6AdwCleaner.exe	3864	QueryStandardI...	C:\Windows\System32\imm32.dll	SUCCESS	AllocationSize: 167...
17:36:...	6AdwCleaner.exe	3864	CreateFileMapp...	C:\Windows\System32\imm32.dll	SUCCESS	SyncType: SyncTy...
17:36:...	6AdwCleaner.exe	3864	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS	
17:36:...	6AdwCleaner.exe	3864	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	QueryBasicInfor...	C:\Windows\System32\imm32.dll	SUCCESS	CreationTime: 14/0...
17:36:...	6AdwCleaner.exe	3864	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS	
17:36:...	6AdwCleaner.exe	3864	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	CreateFileMapp...	C:\Windows\System32\imm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
17:36:...	6AdwCleaner.exe	3864	CreateFileMapp...	C:\Windows\System32\imm32.dll	SUCCESS	SyncType: SyncTy...
17:36:...	6AdwCleaner.exe	3864	Load Image	C:\Windows\System32\imm32.dll	SUCCESS	Image Base: 0x7fef...
17:36:...	6AdwCleaner.exe	3864	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS	
17:36:...	6AdwCleaner.exe	3864	Load Image	C:\Windows\System32\msctf.dll	SUCCESS	Image Base: 0x7fef...
17:36:...	6AdwCleaner.exe	3864	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
17:36:...	6AdwCleaner.exe	3864	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...