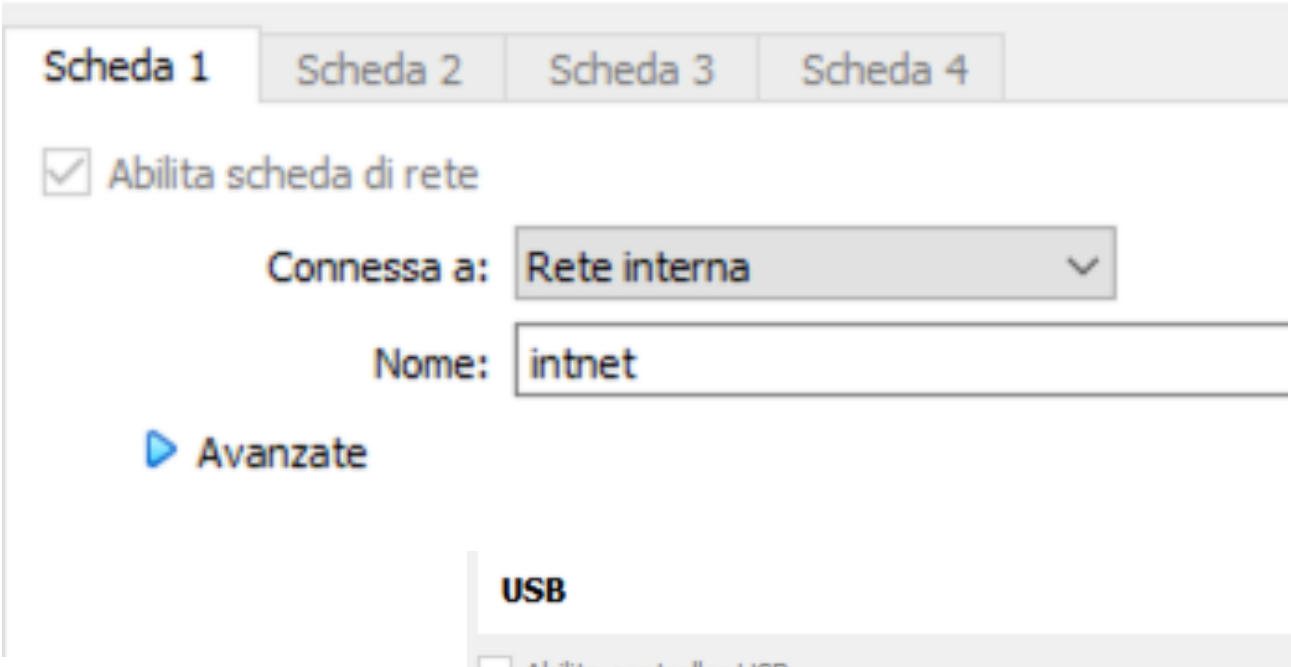
CS0424
S10-L2

Traccia:

1. Configurare la macchina virtuale per l'analisi dinamica.
2. Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon).
3. Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor.
4. Modifiche del registro dopo il malware (le differenze).
5. Provare a profilare il malware in base alla correlazione tra «operation» e Path.

1. Configurazione macchina:

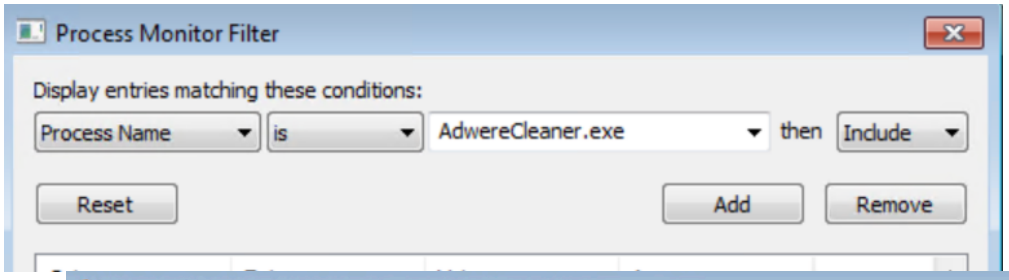
E' importante lavorare su una macchina virtuale che non abbia modo di comunicare con altre macchine o reti. Su virtualbox si può mettere in "rete interna" la macchina su cui verrà avviato il malware e disattivare le porte USB

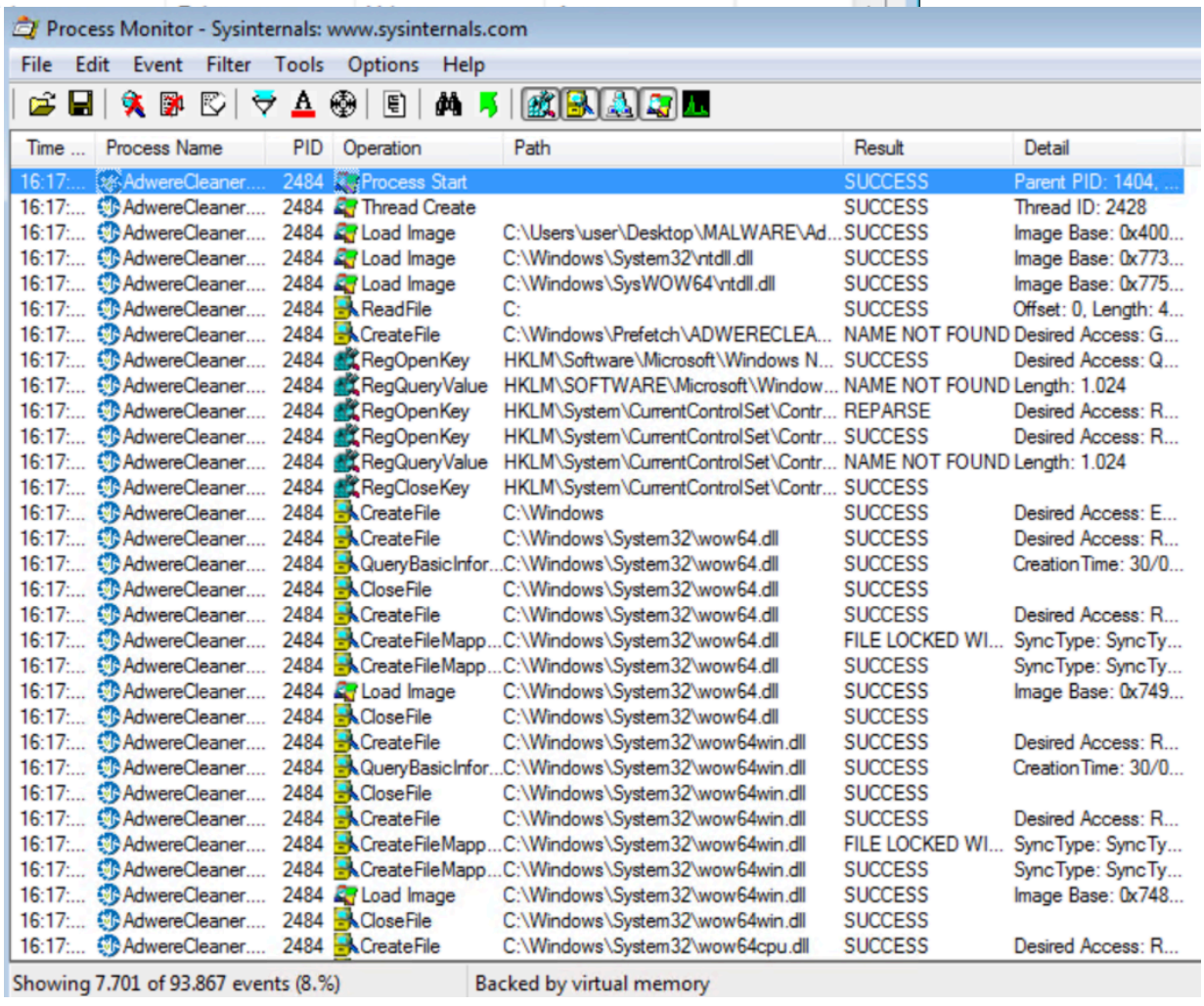


Ho anche effettuato un' istantanea della macchina prima di eseguire il malware, per poterla ripristinare facilmente.

2. Azioni sul file system:

Ho eseguito il malaware con procmon aperto, poi ho messo in pausa l'acquisizione e ho aggiunto un filtro per per visualizzare solo i processi di Adwerecleaner.exe





Con il filtro seguente ho cercato eventuali processi figli, trovandone uno chiamato 6AdwereCleaner.exe

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\oleaut32.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7e...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7e...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7e...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7e...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\cryptsp.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\rsaenh.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7e...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7e...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\rasapi32.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\rasman.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\ws2_32.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\nsi.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\rtutils.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\mswsock.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\WSHTCPIP.DLL	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\wship6.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\winhttp.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\webio.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\sspicli.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\credssp.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\winnsi.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\dhcpcsvc6.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\dhcpcsvc.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\cfgmgr32.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\RpcRtRemote.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\dnsapi.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\rasadhlp.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\winsxs\amd64_microsoft.w...	SUCCESS	Image Base: 0x7e...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\winsxs\amd64_microsoft.w...	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\winsxs\amd64_microsoft.w...	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\WindowsCodec...	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\clbcatq.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\ieframe.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\psapi.dll	SUCCESS	Image Base: 0x775...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\oleacc.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\shell32.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\iertutil.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\sxs.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\dwmapi.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\shfolder.dll	SUCCESS	Image Base: 0x7e...
16:18:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\wininet.dll	SUCCESS	Image Base: 0x7ef...
16:18:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\urlmon.dll	SUCCESS	Image Base: 0x7ef...
16:18:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\crypt32.dll	SUCCESS	Image Base: 0x7ef...
16:18:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\msasn1.dll	SUCCESS	Image Base: 0x7ef...
16:18:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\profapi.dll	SUCCESS	Image Base: 0x7ef...
16:18:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\ntmarta.dll	SUCCESS	Image Base: 0x7ef...
16:18:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\Wldap32.dll	SUCCESS	Image Base: 0x7ef...

Showing 74 of 93.867 events (0.0%) Backed by virtual memory

Column	Relation	Value	Action
PID	is	2484	Include
PID	is	2400	Include
Operation	is	CreateFile	Include
Operation	is	CloseFile	Include
Operation	is	WriteFile	Include
Operation	is	ReadFile	Include
[illegible]	[illegible]	[illegible]	[illegible]

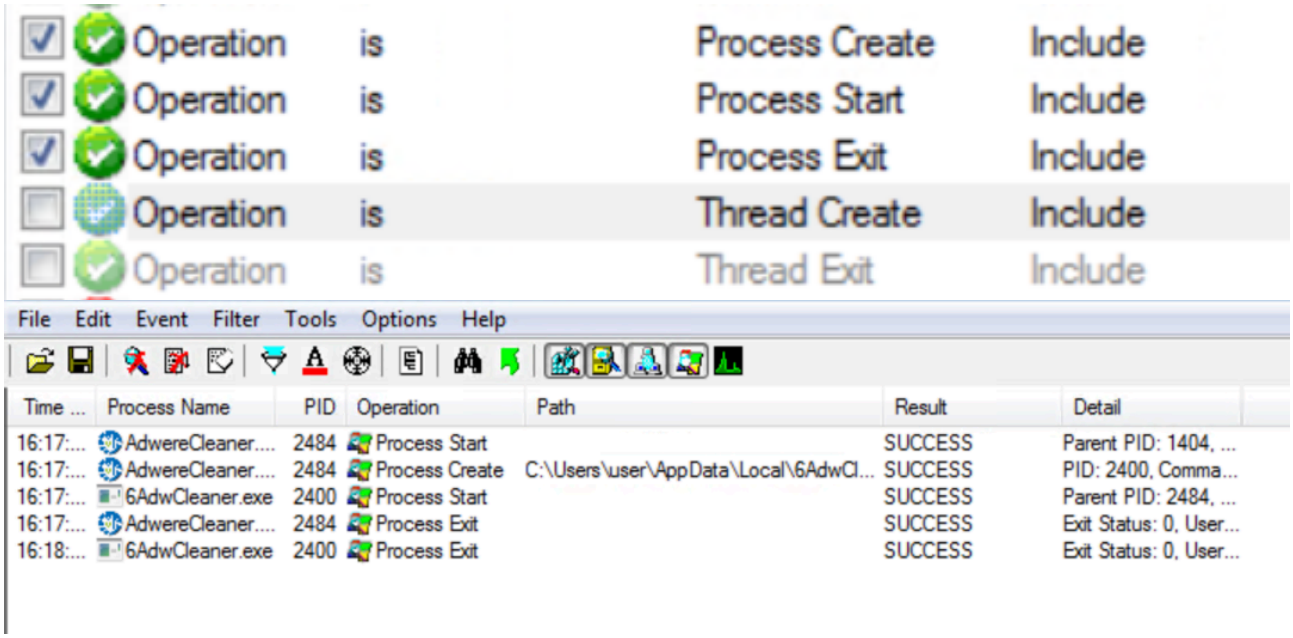
Con questi filtri è possibile visualizzare solo i processi precedentemente individuati e le operazioni che questi hanno eseguito sui file di sistema.

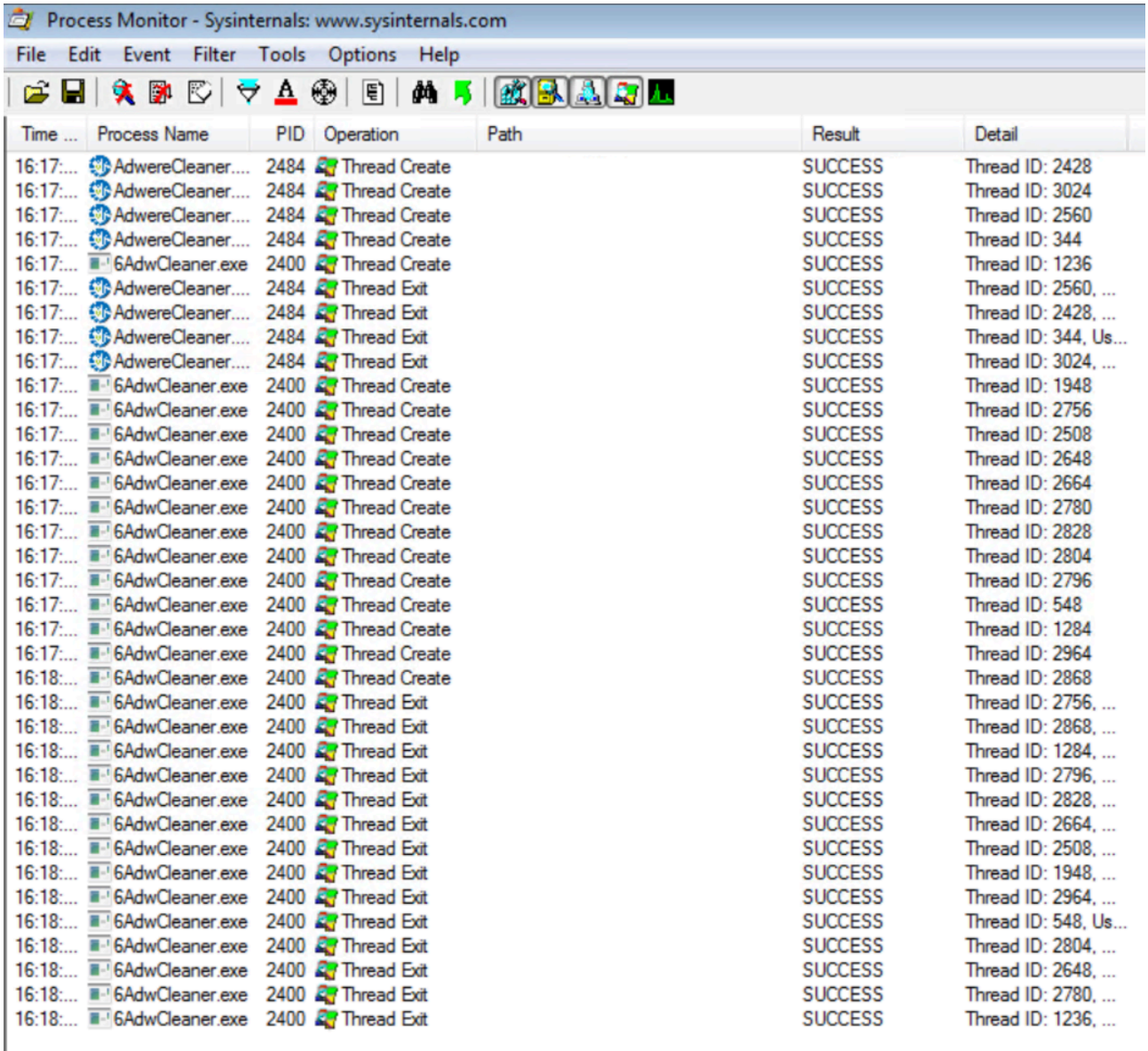
Time ...	Process Name	PID	Operation	Path	Result	Detail
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\Prefetch\ADWERECLEA...	NAME NOT FOUND	Desired Access: G...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Users\user\Desktop\MALWARE	SUCCESS	Desired Access: E...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Users\user\Desktop\MALWARE\Ad...	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\winsxs\x86_microsoft.wind...	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\winsxs\x86_microsoft.wind...	SUCCESS	Desired Access: E...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\winsxs\x86_microsoft.wind...	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\winsxs\x86_microsoft.wind...	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Users\user\Desktop\MALWARE\VE...	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\version.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\version.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\rpcss.dll	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\rpcss.dll	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Users\user\Desktop\MALWARE\S...	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\shfolder.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\shfolder.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\Globalization\Sorting\Sort...	SUCCESS	Desired Access: G...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Desired Access: G...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Users\user\Desktop\MALWARE\Ad...	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\winsxs\x86_microsoft.wind...	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\winsxs\x86_microsoft.wind...	SUCCESS	Desired Access: E...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\winsxs\x86_microsoft.wind...	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\winsxs\x86_microsoft.wind...	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\WindowsShell.Manifest	SUCCESS	Desired Access: G...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\propsys.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\propsys.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Users\user\AppData\Local\Microsof...	NAME COLLISION	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Users\user\AppData\Local\Microsof...	SUCCESS	Desired Access: G...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Users\user\Desktop\MALWARE\nt...	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS	Desired Access: R...

Showing 614 of 93.867 events (0.6%) Backed by virtual memory

3. Azioni del malware sui processi e thread:

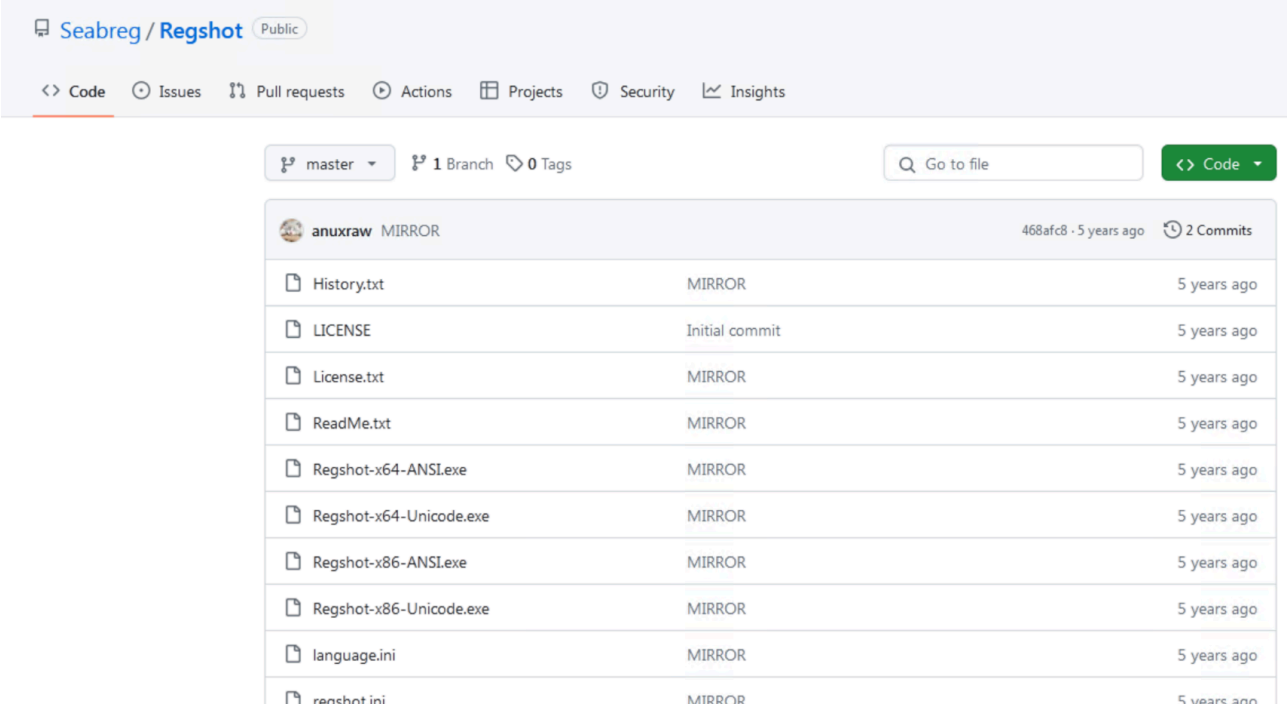
Ho aggiunto i seguenti filtri per vedere i processi e i thread creati/iniziati/chiusi

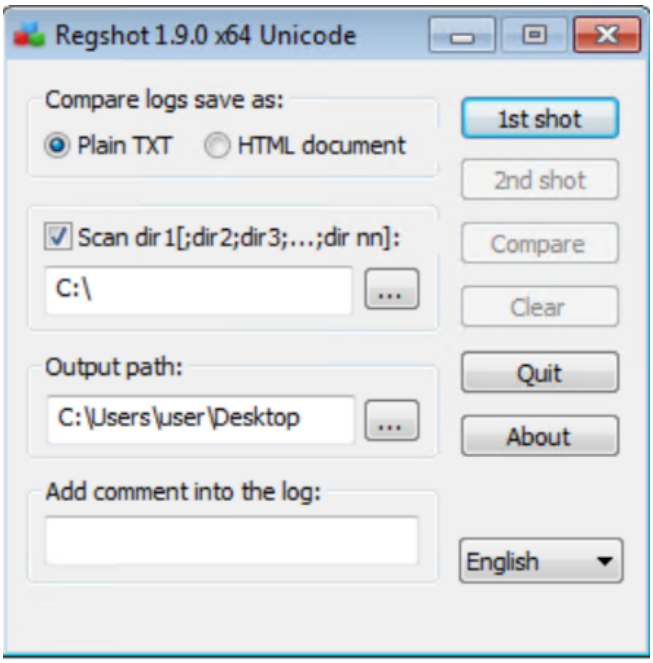




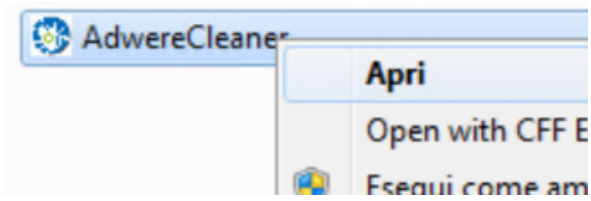
4. Modifiche del registro da parte del malware:

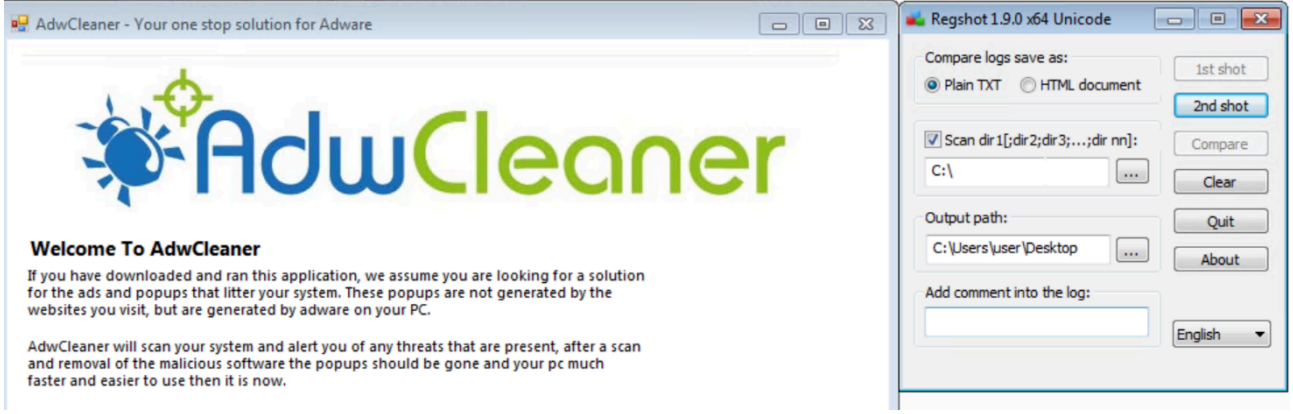
Per trovare le differenze nel registro da prima dell'esecuzione del malware a dopo ho utilizzato um tool opensource chiamato Regshot, ovviamente ho prima ripristinato lo stato della macchina grazie all'istantanea salvata prima

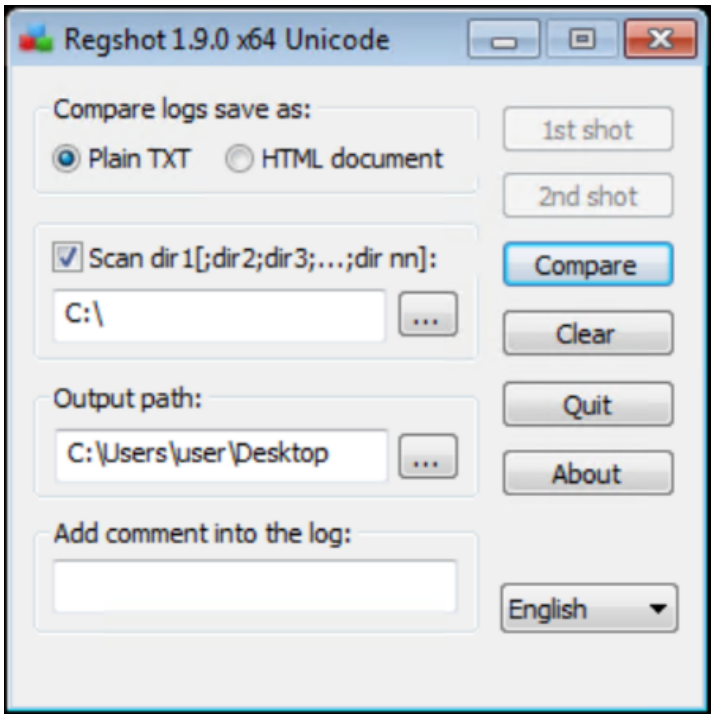




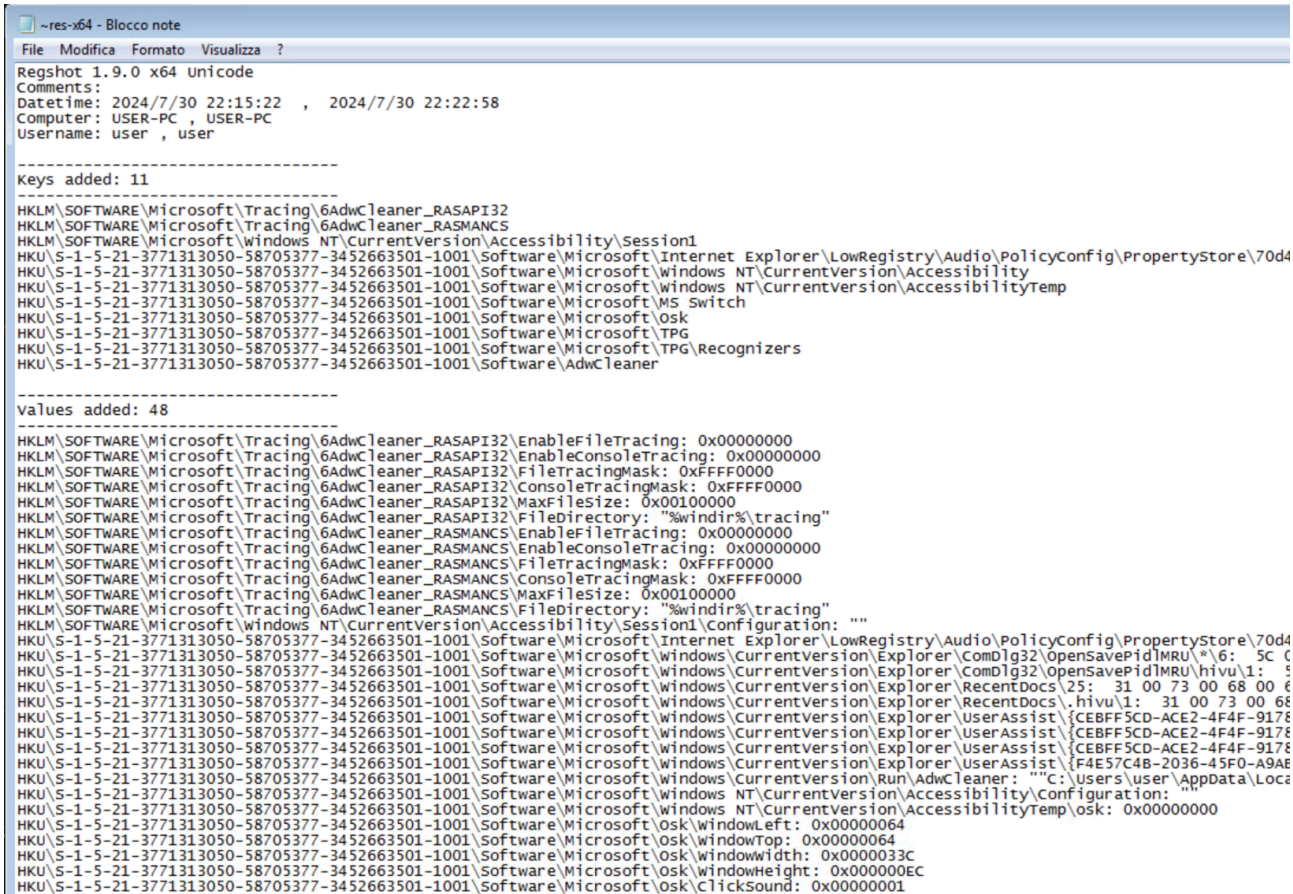
Questo tool permette di scansionare tutte le directory del sistema due volte e compararle, dando in output tutte le variazioni che ci sono state dalla prima alla seconda scansione.







E’ possibile vedere le variazioni rilevate dal tool nel file di testi che va a salvare.



```
Values modified: 16
----------------------------------
HKLM\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffffffff
HKLM\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffffffff
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{58e4c544-b521-11ee-8e5c-806e6f6e
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{58e4c544-b521-11ee-8e5c-806e6f6e
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{58e4c544-b521-11ee-8e5c-806e6f6e
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{58e4c544-b521-11ee-8e5c-806e6f6e
HKLM\SYSTEM\CurrentControlSet\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffff
HKLM\SYSTEM\CurrentControlSet\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffff
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{58e4c544-b521-11ee-8e5c-806e
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{58e4c544-b521-11ee-8e5c-806e
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{58e4c544-b521-11ee-8e5c-806e
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{58e4c544-b521-11ee-8e5c-806e
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
0 00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 0E 76 9E 77 00 00 00 00 00 00
 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 32 00 33 00 7D 00 5C 00 65
3D 00 00 00 00 00 78 7F CC C9 F0 1C F9 41 A1 1A 99 4B A5 A9 A5 4D 0D 00 00 00 01 00 00 00 1
0 00 00 00 00 10 E1 00 03 00 00 00 00 90 76 C6 08 00 00 00 00 92 15 38 FD FE 07 00 00 80 29
 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
0 00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 0E 76 9E 77 00 00 00 00 00 00
 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 32 00 33 00 7D 00 5C 00 65
00 03 00 00 00 00 00 00 00 00 00 00 00 00 8B 18 39 FD FE 07 00 00 F0 6C 83 02 00 00 00 00 0
0 00 00 00 00 01 00 00 00 00 00 00 00 00 3D 00 00 00 00 00 0B BD 14 77 00 00 00 00 00 00
 FF FF FF
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
7 00 00 00 00 D0 D7 95 02 00 00 00 00 01 00 00 00 00 00 00 00 F8 44 F4 FE FE 07 00 00 F0 BF
 00 34 00 38 00 42 00 32 00 34 00 42 00 36 00 43 00 37 00 31 00 37 00 34 00 7D 00 5C 00 54
00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 46 00 69 00 80 8A 50 04 00 00 00 00 1
0 00 00 00 00 30 CB 26 07 00 00 00 00 00 00 00 00 00 00 00 00 00 E5 66 CC FE FE 07 00 00 00
 31 AD 77
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\
7 00 00 00 00 D0 D7 95 02 00 00 00 00 01 00 00 00 00 00 00 00 F8 44 F4 FE FE 07 00 00 F0 BF
 00 34 00 38 00 42 00 32 00 34 00 42 00 36 00 43 00 37 00 31 00 37 00 34 00 7D 00 5C 00 54
00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 46 00 69 00 80 8A 50 04 00 00 00 00 1
0 00 00 00 00 30 CB 26 07 00 00 00 00 00 00 00 00 00 00 00 00 00 E5 66 CC FE FE 07 00 00 00
 31 AD 77
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\M
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\M
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\
```

```
----------------------------------
Files added: 11
----------------------------------
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Results\Resource\{D84C29D5-AF83-493B-BAB4-5599D00A9325}
C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Results\Resource\{D84C29D5-AF83-493B-BAB4-5599D00A9325}
C:\Users\user\AppData\Local\6AdwCleaner.exe
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B8CC409ACDBF2A2FE04C56F2875B1FD6
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F4D9C889B7AEBCF4E1A2DAABC5C3628A_77D782D611E65A2A81EA974847CB0C84
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B8CC409ACDBF2A2FE04C56F2875B1FD6
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F4D9C889B7AEBCF4E1A2DAABC5C3628A_77D782D611E65A2A81EA974847CB0C84
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\1shot.hivu.lnk
C:\Users\user\Desktop\1shot.hivu

----------------------------------
Files deleted: 2
----------------------------------
C:\Windows\Temp\TMP00000021D5C45BCFD0489823
C:\Windows\Temp\TMP000000231F33E17DD94F6D2F

----------------------------------
Files [attributes?] modified: 13
----------------------------------
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Service\Unknown.Log
C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Service\Unknown.Log
C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
C:\Users\user\NTUSER.DAT
```

Ha rilevato un totale di 101 modifiche di cui:

11 chiavi aggiunte

48 valori aggiunti

16 valori modificati

11 file aggiunti

2 file eliminati

13 file modificati