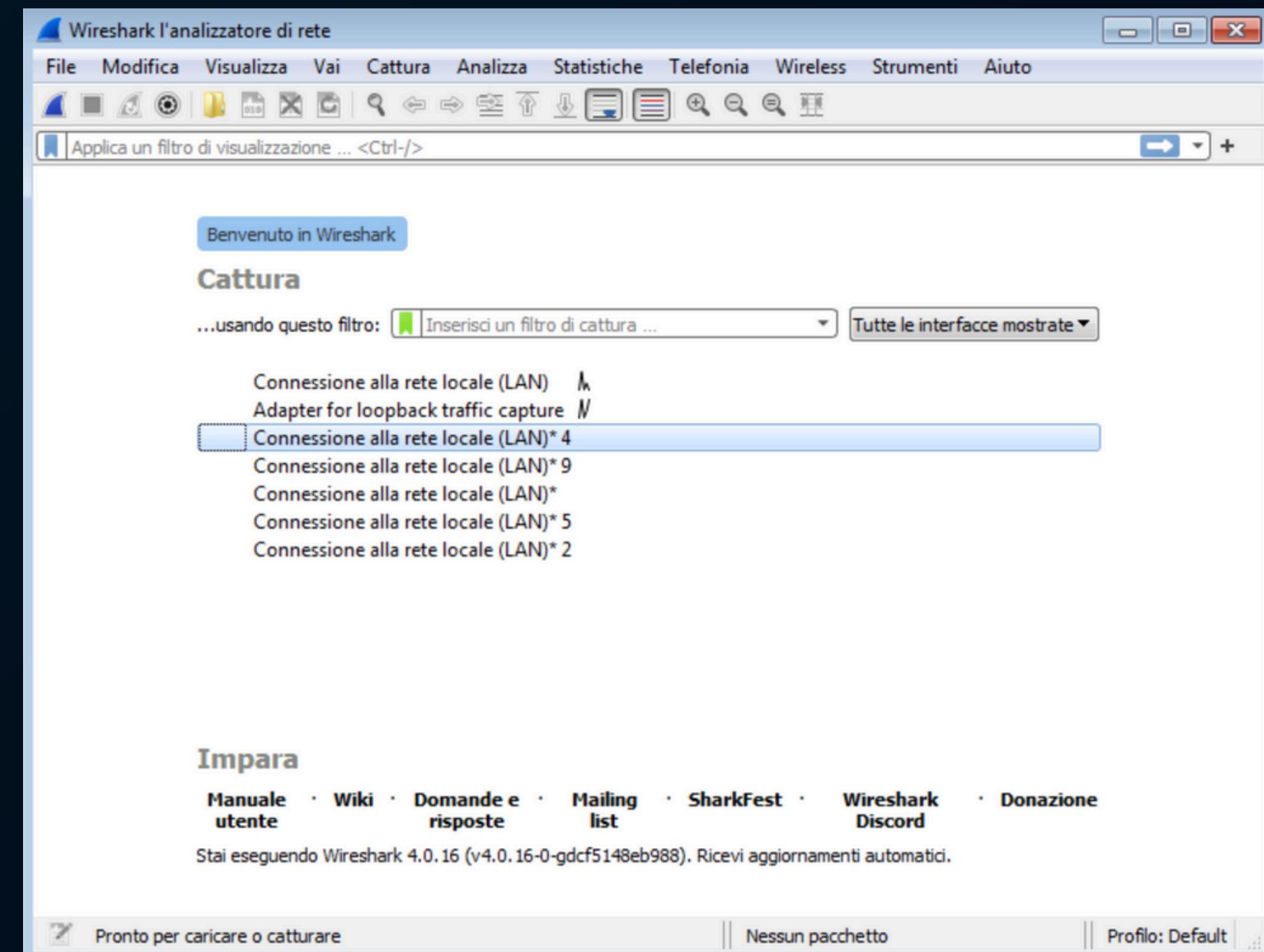


REPORT

S10-L2

Prima di tutto avvio tutti i programmi necessari per l'analisi dinamica del malware
1-Wireshark



2-Apro Process Monitor, lo metto in pausa e faccio un clear, più avanti metterò dei filtri per filtrare solo quello che mi interessa

The image displays two side-by-side windows of the Process Monitor application. Both windows have a title bar 'Process Monitor - Sysinternals: www.sysinternals.com' and a standard Windows-style menu bar.

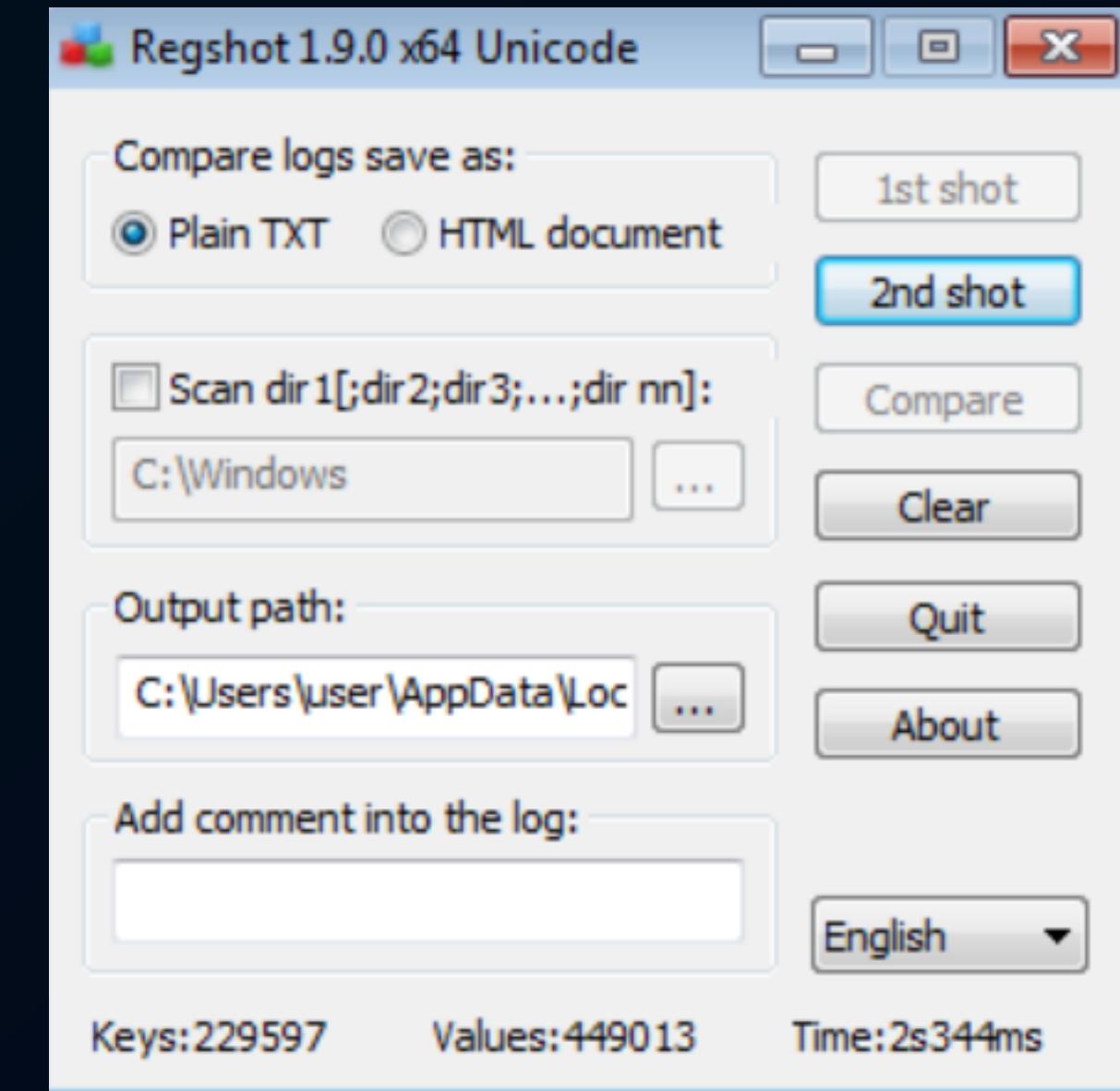
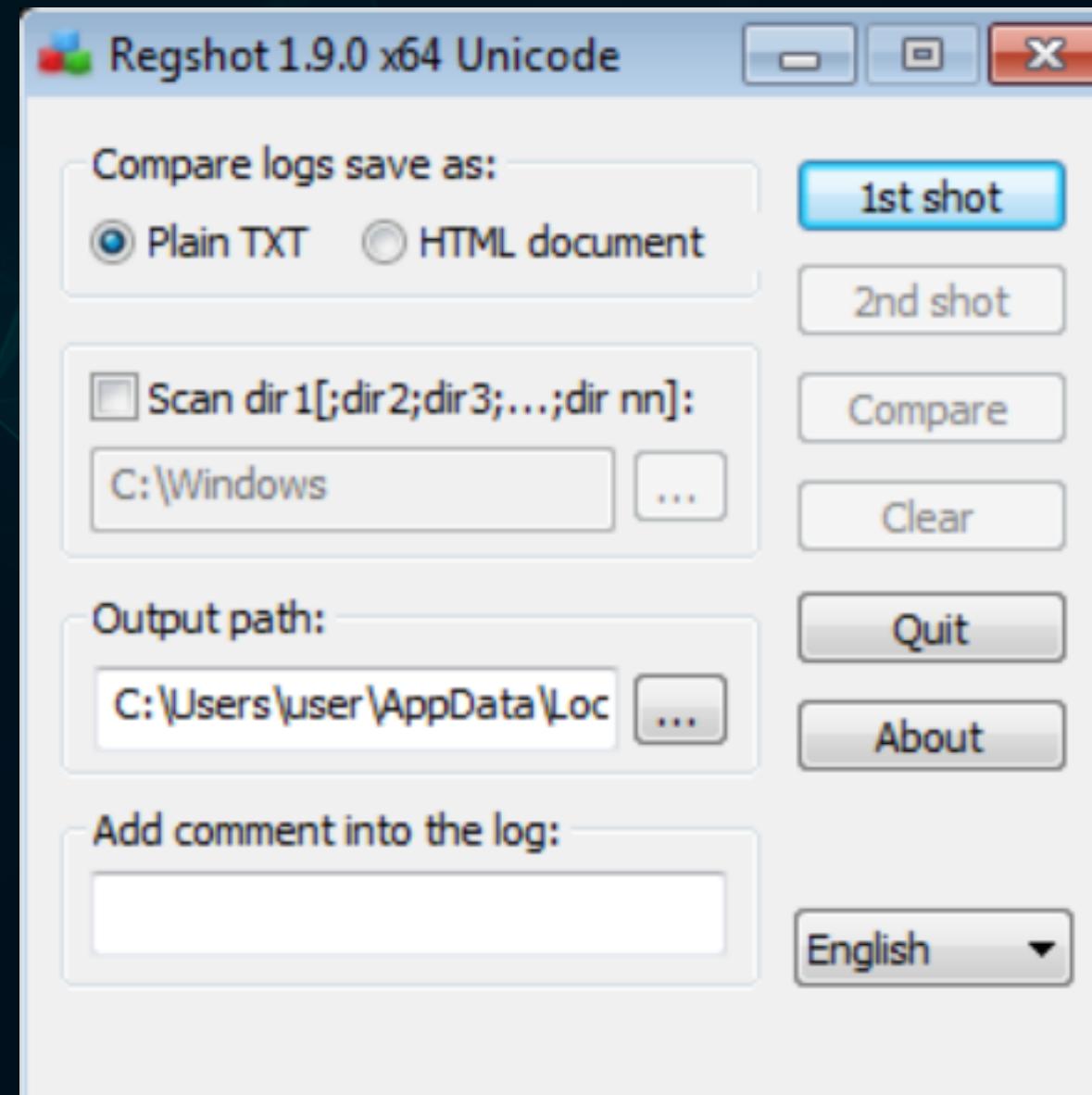
Left Window (Captured Events):

- Header:** Time ..., Process Name, PID, Operation, Path, Result, Detail
- Events:** A list of 34 events from 15:28:... to 15:28:...
 - SearchIndexer.exe (PID 1996) performing multiple File Control operations (FSCTL_Q...) on paths like 'C:\Windows\system32\kernel32.dll'. All results are SUCCESS.
 - Isass.exe (PID 472) performing multiple Registry operations (RegOpenKey, RegQueryValue, RegCloseKey) on paths like 'HKLM\SAM\SAM\DOMAINS\Account\...'. Desired Access is R... (Read). Type is REG_BINARY.
 - VBoxTray.exe (PID 1860) performing Thread Create operations. One entry shows Thread ID: 1824.
 - VBoxService.exe (PID 628) performing Registry operations on paths like 'HKLM\System\CurrentControlSet\...'. Operations include RegQueryKey, RegOpenKey, RegQueryValue, and RegCloseKey. Desired Access is R... (Read).
- Status Bar:** Showing 34 of 60.992 events (0.0%) and Backed by virtual memory.

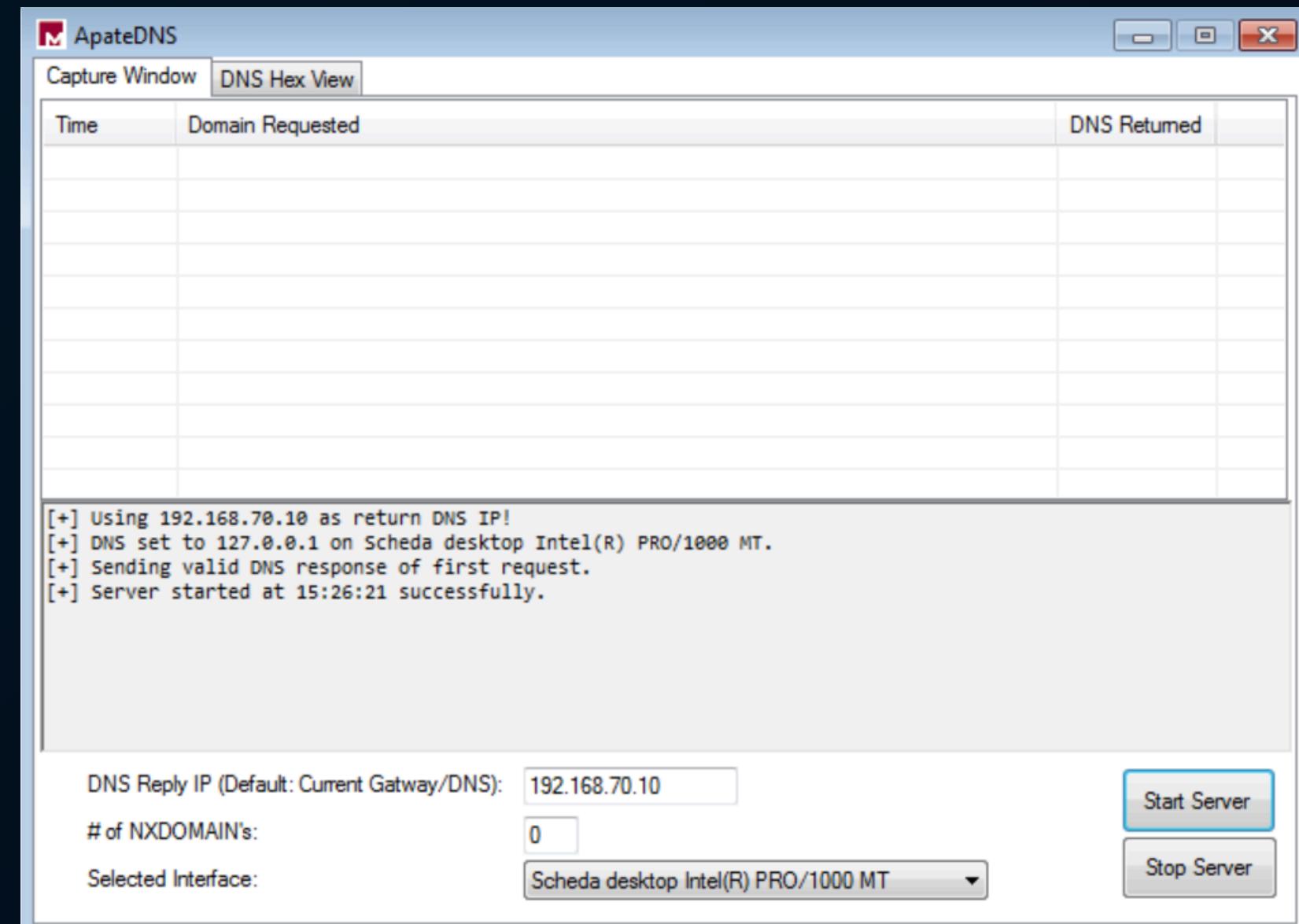
Right Window (Cleared Log):

- Header:** Time ..., Process Name, PID, Operation, Path, Result, Detail
- Events:** A single event from VBoxService.exe (PID 628) at 15:28:... showing a RegOpenKey operation on 'HKLM\SYSTEM\CurrentControlSet\...'. Desired Access is R... (Read). The result is REPARSE.
- Status Bar:** No events (capture disabled) and Backed by virtual memory.

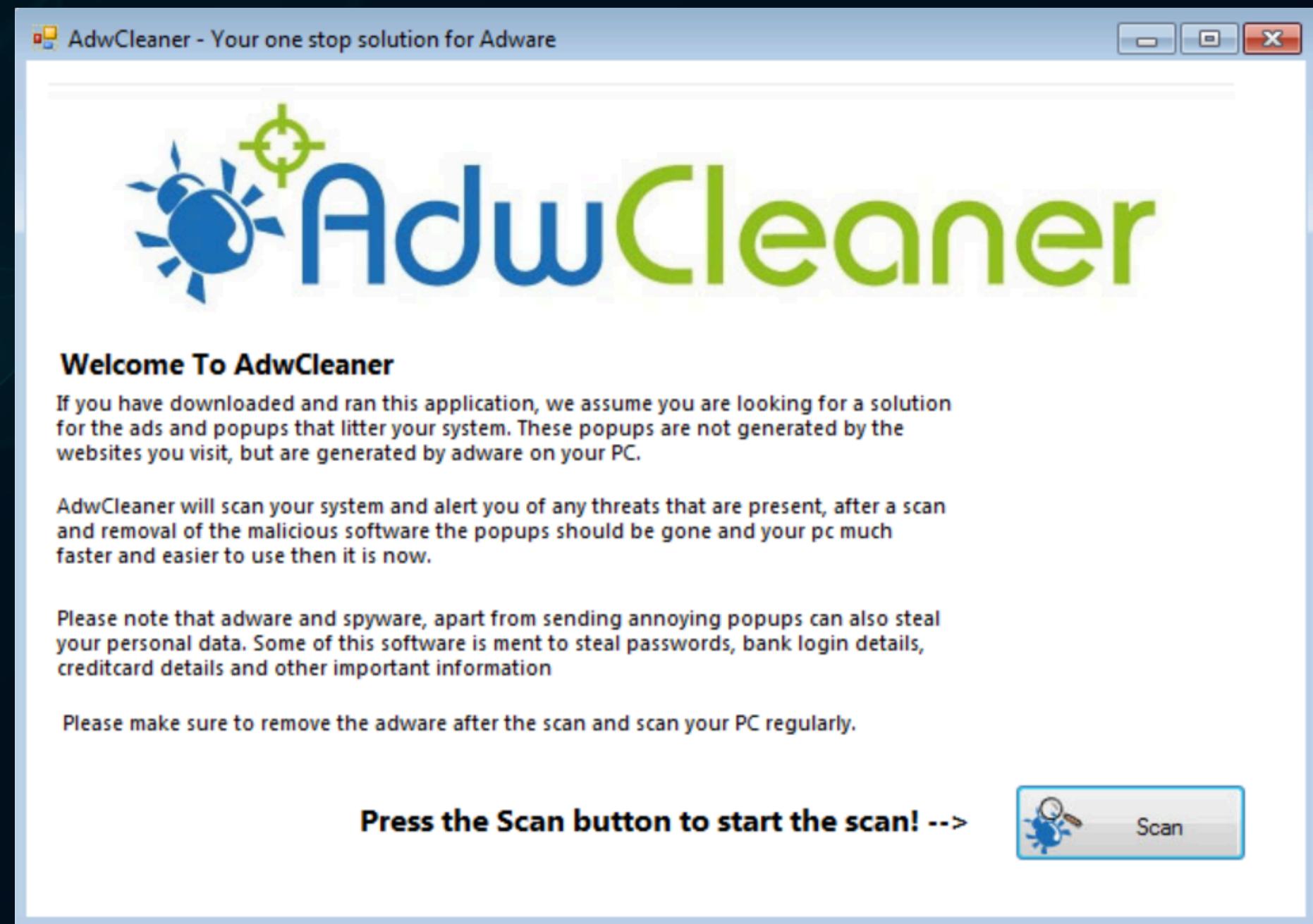
3-Apro Regshot e faccio una prima scansione delle chiavi e dei loro valori

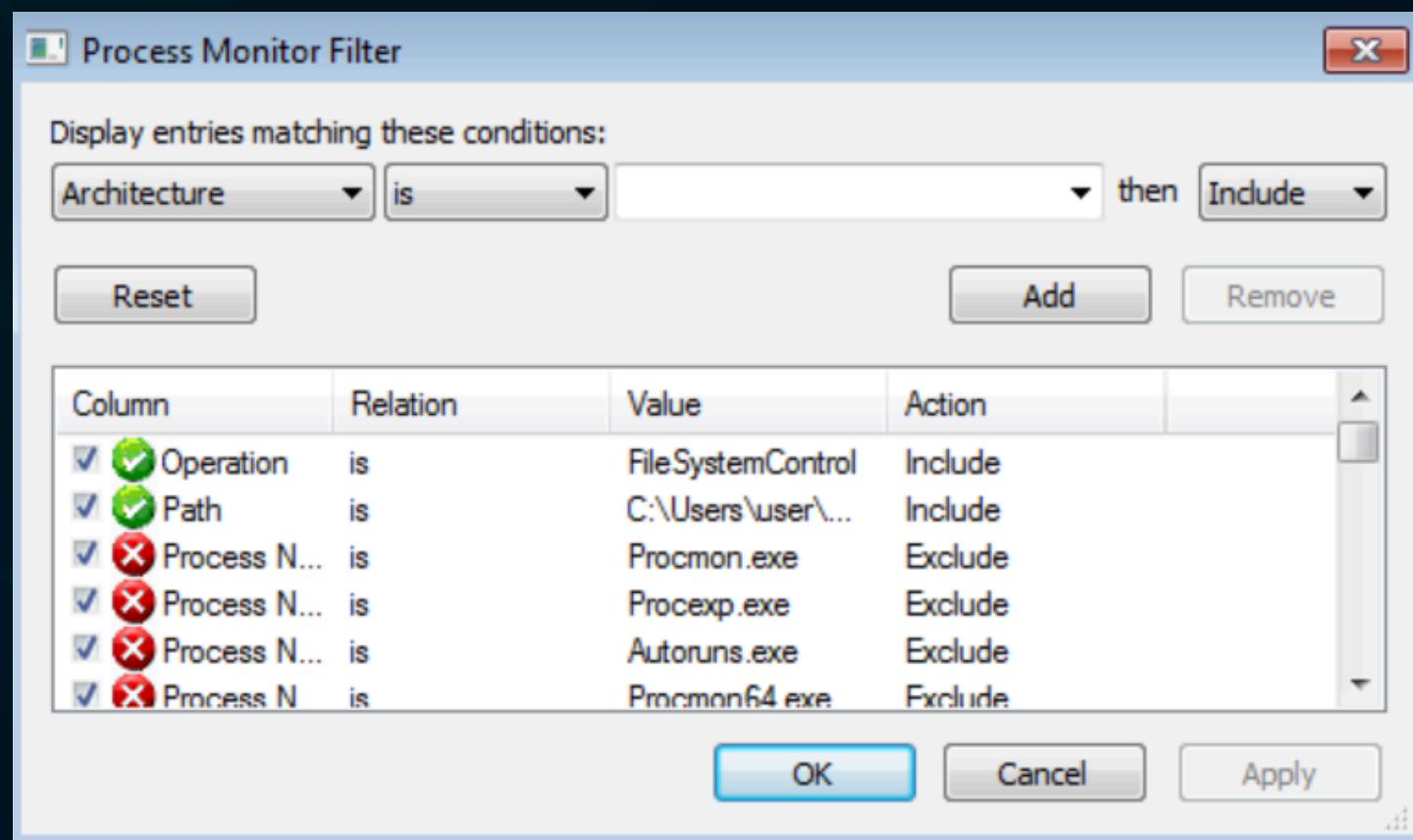


4-Apro ApateDNS ed avvio un server inserendo come DNS il mio IP



5- Avvio il malware che si presenta come un programma legittimo per rimuovere gli Adw





Aggiungo due filtri per filtrare i cambiamenti che mi ha generato il malware, quindi inserisco il path del malware e come tipo di operazione FileSystem

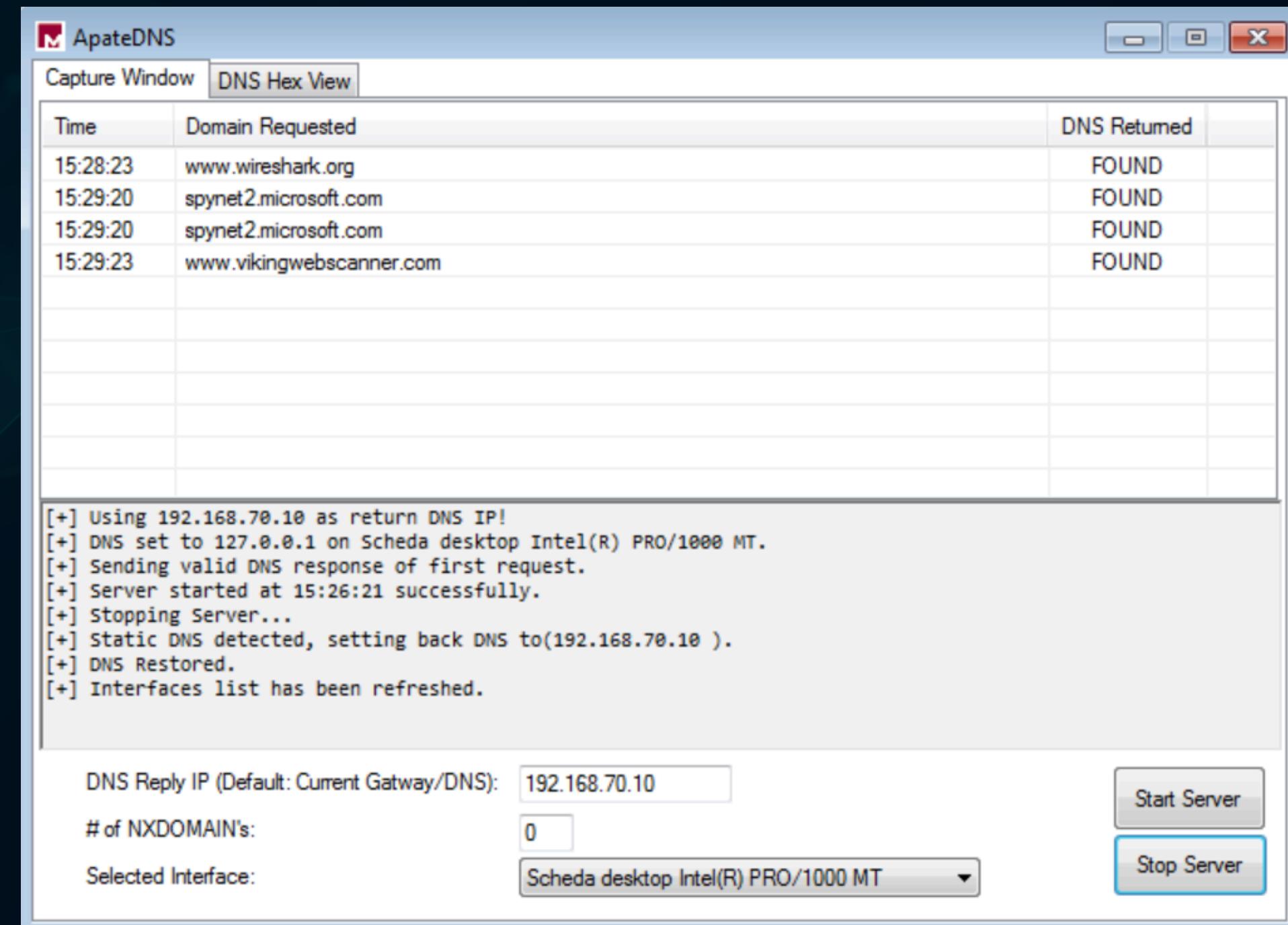
The screenshot shows the main Process Monitor window titled 'Process Monitor - Sysinternals: www.sysinternals.com'. The window displays a list of events in a table with columns: Time, Process Name, PID, Operation, Path, Result, and Detail. The events listed are:

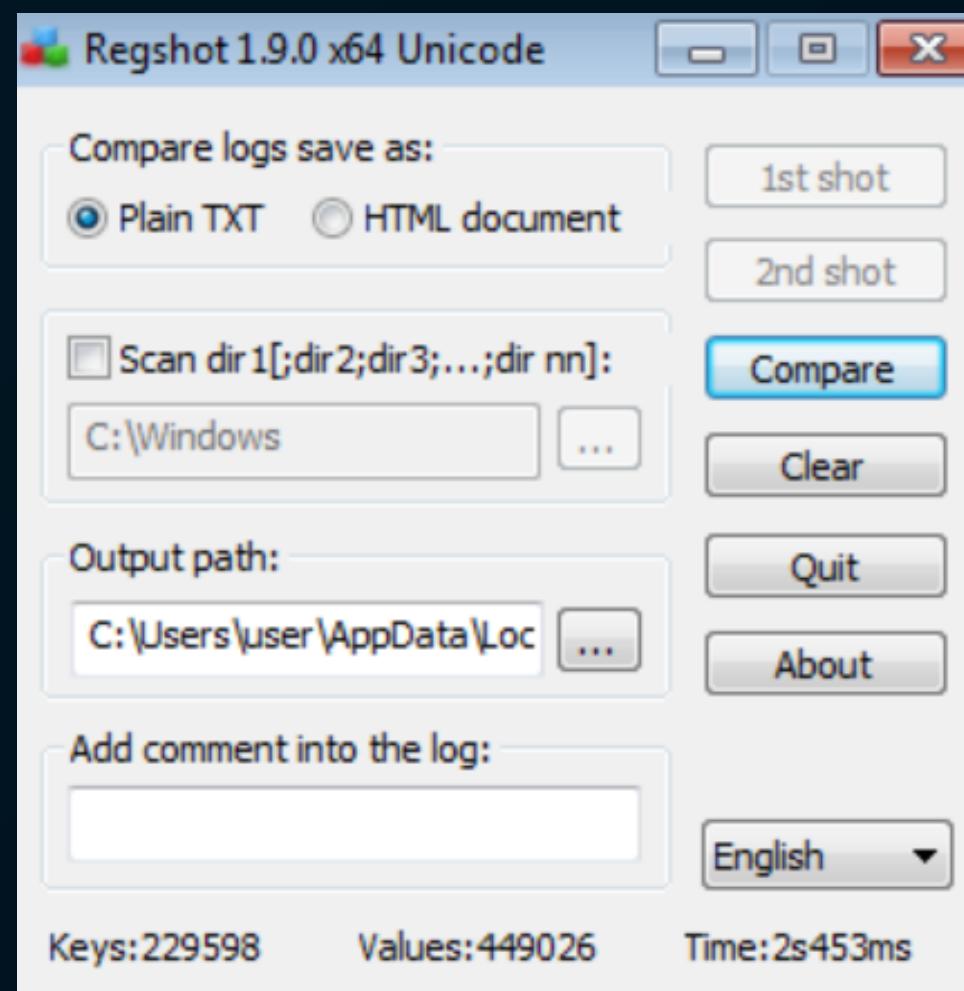
Time	Process Name	PID	Operation	Path	Result	Detail
15:29:...	Explorer.EXE	596	FileSystemControl	C:\Users\user\Downloads\AdwereClea...	SUCCESS	Control: FSCTL_R...
15:29:...	Explorer.EXE	596	FileSystemControl	C:\Users\user\Downloads\AdwereClea...	SUCCESS	Control: FSCTL_R...
15:29:...	Explorer.EXE	596	FileSystemControl	C:\Users\user\Downloads\AdwereClea...	SUCCESS	Control: FSCTL_R...
15:29:...	svchost.exe	2540	FileSystemControl	C:\Users\user\Downloads\AdwereClea...	SUCCESS	Control: FSCTL_R...
15:29:...	svchost.exe	2540	FileSystemControl	C:\Users\user\Downloads\AdwereClea...	OPLOCK NOT GR...	Control: FSCTL_R...
15:29:...	svchost.exe	2540	FileSystemControl	C:\Users\user\Downloads\AdwereClea...	SUCCESS	Control: FSCTL_R...
15:29:...	svchost.exe	2540	FileSystemControl	C:\Users\user\Downloads\AdwereClea...	SUCCESS	Control: FSCTL_R...

At the bottom of the window, it says 'Showing 7 of 583.803 events (0.0%)' and 'Backed by virtual memory'.

Noto che il malware mi ha cambiato diverse chiavi di registro

Inoltre noto che ha fatto provato a connettersi a domini particolari come vikingwebscanner.com





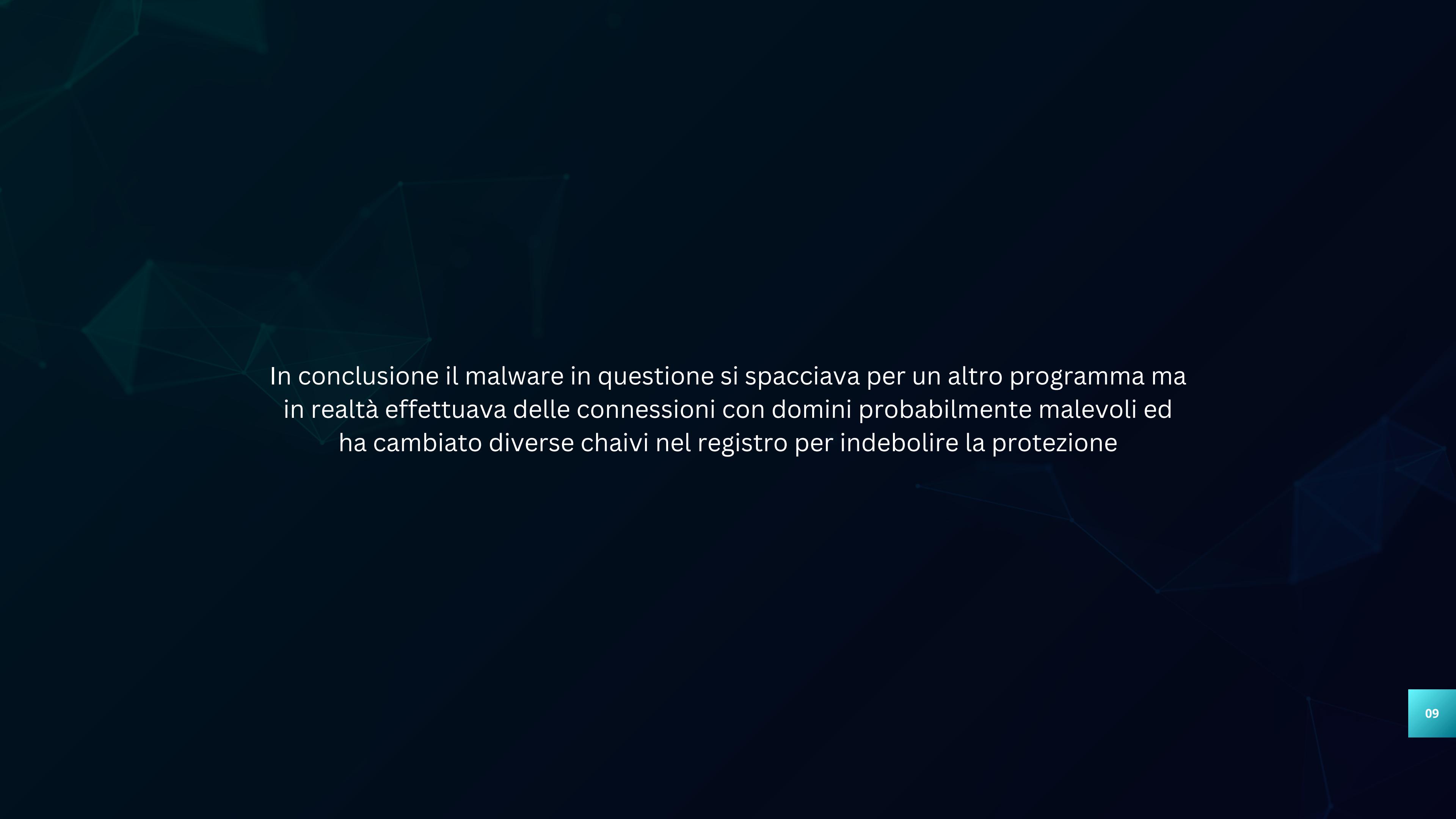
Faccio la seconda scansione con Regshot e la comparazione con la prima scansione, noto che è stata aggiunta una chiave, 13 valori aggiunti e 17 modificati

```
~res-x64 - Blocco note
File Modifica Formato Visualizza ?
Regshot 1.9.0 x64 unicode
Comments:
Datetime: 2024/7/30 13:27:43 , 2024/7/30 13:30:37
Computer: USER-PC , USER-PC
Username: user , user

-----
Keys added: 1
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AdwCleaner

-----
values added: 13
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Run\AdwC1
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\MuiCache\4\7F06864B
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AdwCleaner\id: "0"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\classes\Local Settings\MuiCache\4\7F06864B@%system
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\classes\Local Settings\MuiCache\4\7F06864B@C:\wind
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\classes\Local Settings\MuiCache\4\7F06864B@C:\wind
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\classes\Local Settings\MuiCache\4\7F06864B@C:\wind
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\classes\Local Settings\MuiCache\4\7F06864B@C:\win

-----
values modified: 17
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\4EB6D578499B1CCF5F581EAD56BE3D9B674
00 30 82 04 D3 30 82 03 BB A0 03 02 01 02 02 10 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A 30
0B 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 0
C 92 67 18 E5 F4 06 04 EF 90 B9 E4 00 E4 DD 3A B5 19 FF 02 BA F4 3C EE E0 8B EB 37 8B EC F4 D7 AC F2
BD 77 F6 A5 79 22 38 EC C4 A7 A0 78 12 AD 62 0E 45 70 64 C5 E7 97 66 2D 98 09 7E 5F AF D6 CC 28 65
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\4EB6D578499B1CCF5F581EAD56BE3D9B674
38 7D EE 94 C9 04 00 00 01 00 00 10 00 00 00 CB 17 E4 31 67 3E E2 09 FE 45 57 93 F3 0A FA 1C
30 09 06 03 55 04 06 13 02 55 53 31 17 30 15 06 03 55 04 0A 13 0E 56 65 72 69 53 69 67 6E 2C 20 49 6
1 C2 33 49 D8 43 63 6A 52 4B D2 8F E8 70 51 4D D1 89 69 7B C7 70 F6 B3 DC 12 74 DB 78 5D 4B 56 D3 96
43 39 FA 02 AF 33 31 33 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 03 82 01 01 00 93 24 4A 30 5F
```



In conclusione il malware in questione si spacciava per un altro programma ma in realtà effettuava delle connessioni con domini probabilmente malevoli ed ha cambiato diverse chiavi nel registro per indebolire la protezione