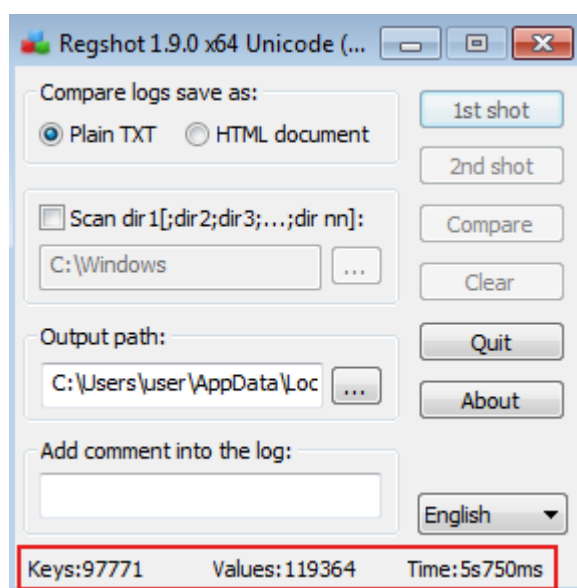
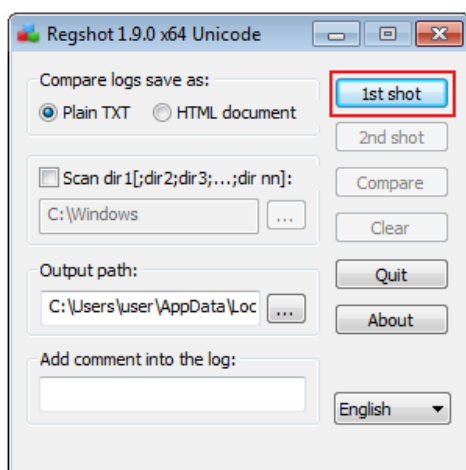


## CONSEGNA U3 S10 L2

- **Preparazione ambiente di analisi**

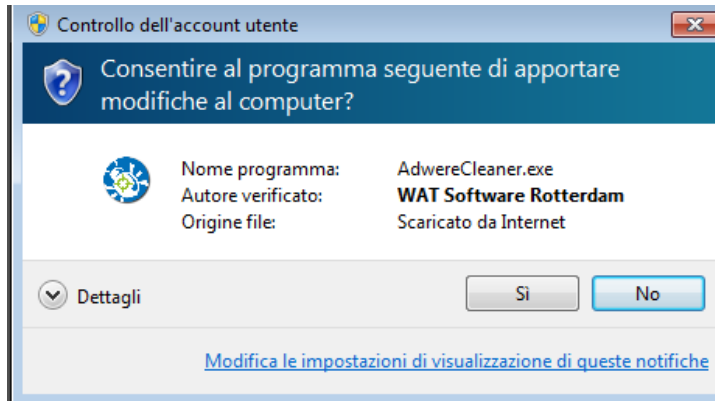
Inizio con l'avviare i programmi necessari per l'**analisi dinamica** del malware. Quindi avvio sia **Regshot** che **Process Monitor**. **Regshot** lo avvio per darmi una mano nell'analisi delle eventuali modifiche alle chiavi di registro di Windows. Mentre **Process Monitor** mi serve per analizzare le modifiche al **file system** e il comportamento dei **processi** in esecuzione.

Eseguo il **primo shot** del registro prima di avviare il malware.



- **Esecuzione del malware**

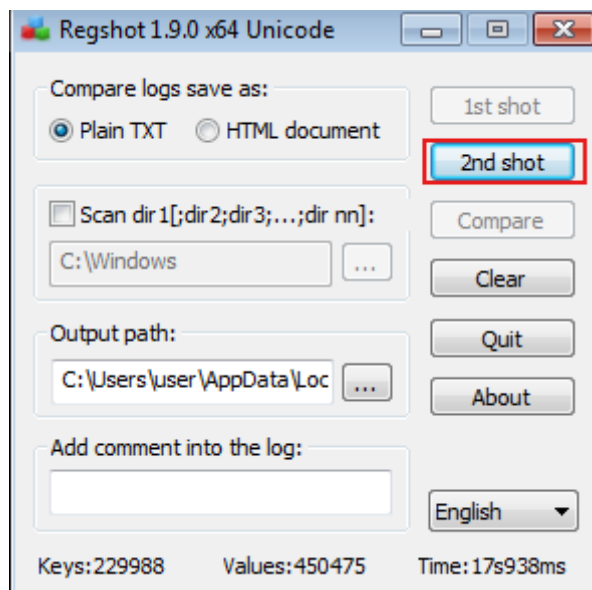
Avvio il malware sul sistema.



Dopo qualche secondo, appare la schermata di benvenuto.



Dopo aver atteso qualche minuto ho eseguito il **secondo shot** con **Regshot** per poi eseguire la comparazione delle differenze non il pulsante **Compare**.



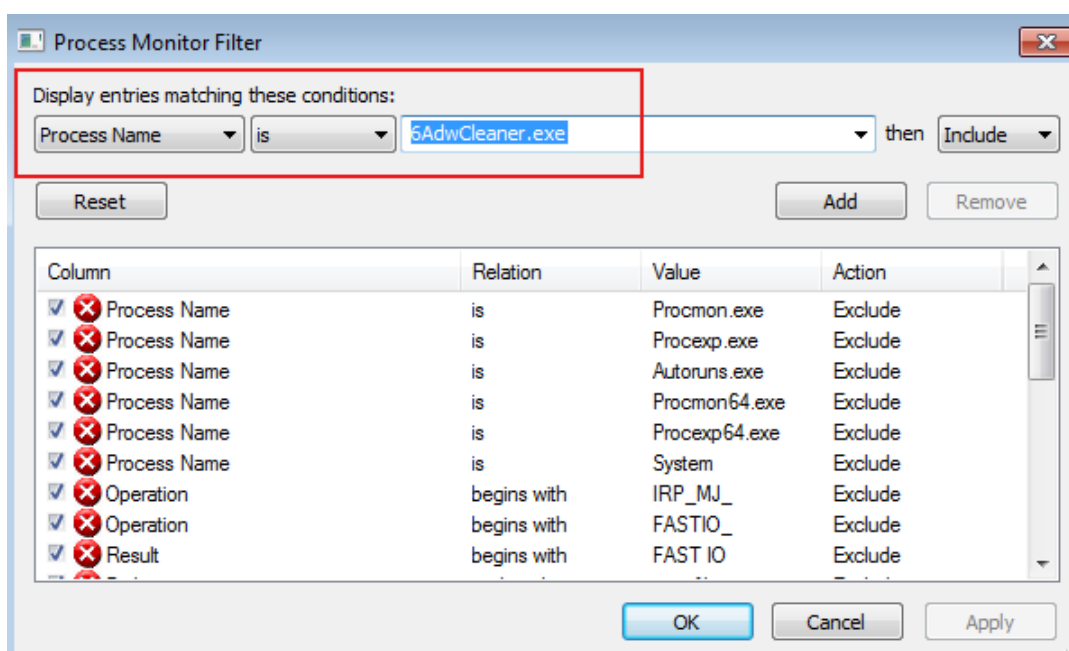
- **Analisi finale dei risultati**

Adesso è il momento di analizzare ciò che è accaduto alla macchina dopo l'esecuzione del malware e le modifiche che sono state effettuate nel sistema.

Inizio settando un filtro su **Process Monitor**, aprendo la voce **Filtri** e poi cercando nel menu a tendina la parola chiave corrispondente al nome del malware.

Risultano due denominazioni diverse: **AdwereCleaner.exe** e **6AdwCleaner.exe**.

Inizio cercando tramite filtri la voce **6AdwCleaner.exe**. Clicco sul pulsante **Add** e poi su **OK**.

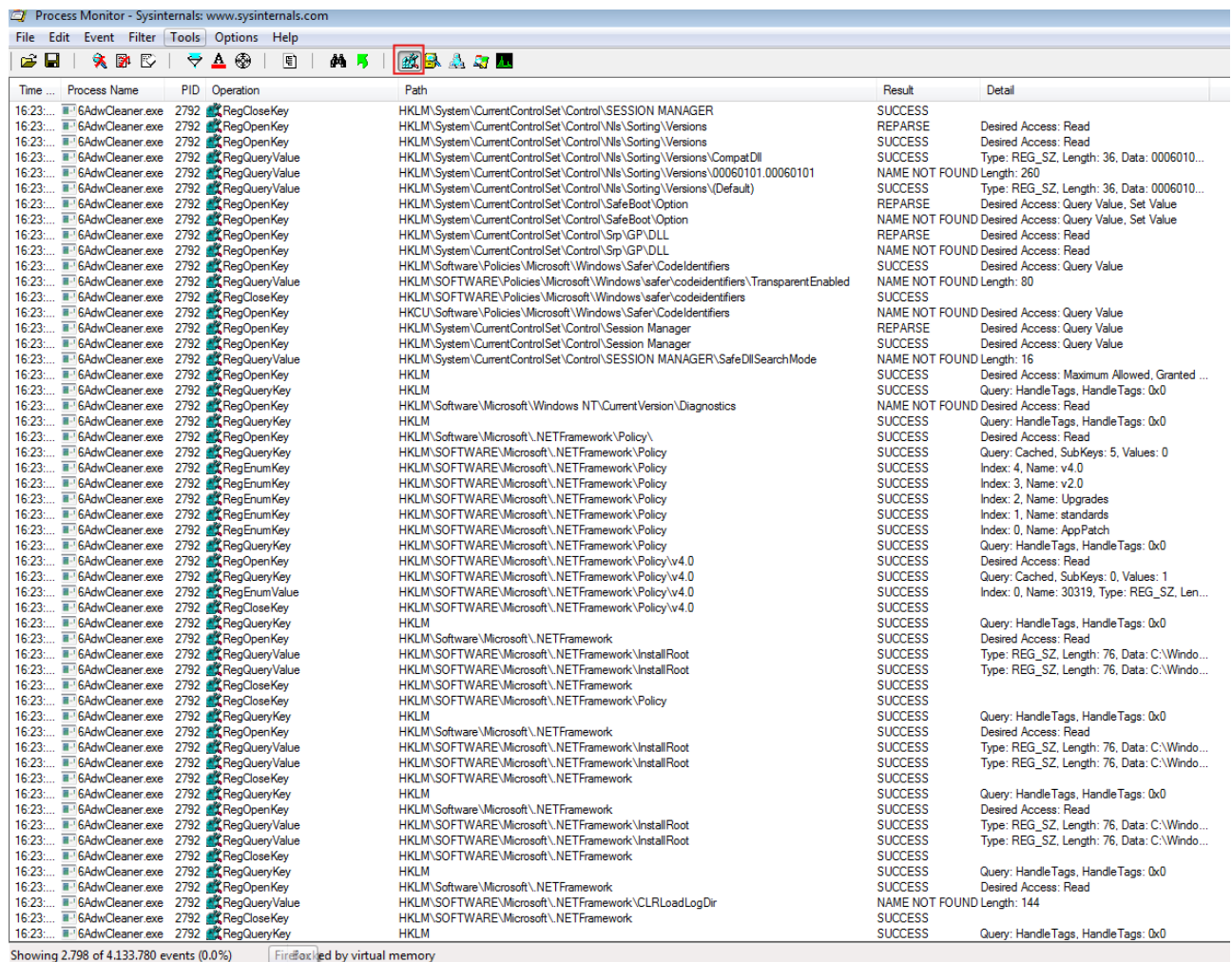


Ecco che compaiono tutte le voci che interessano l'attività malevola del programma. In questa schermata sono visibili gli accessi al **file system**. Si nota la manipolazione di alcune **dll**, ovvero le librerie dinamiche. Il programma effettua prima la creazione e poi varie modifiche seguendo diverse letture e scritture.

Time ...	Process Name	PID	Operation	Path	Result	Detail
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\Prefetch\6ADWCLEANER.EXE-A4D6D516.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: ...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Users\User\AppData\Local	SUCCESS	Desired Access: Execute/Traverse, Synchro...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\System32\mscorlib.dll	SUCCESS	Desired Access: Read Attributes, Disposition...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\System32\mscorlib.dll	SUCCESS	CreationTime: 21/11/2010 05:23:48, LastAc...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\System32\mscorlib.dll	SUCCESS	
16.23...	6AdwCleaner.exe	2792	CreateFileMapping	C:\Windows\System32\mscorlib.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PagePr...
16.23...	6AdwCleaner.exe	2792	CreateFileMapping	C:\Windows\System32\mscorlib.dll	SUCCESS	SyncType: SyncTypeOther
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\System32\mscorlib.dll	SUCCESS	
16.23...	6AdwCleaner.exe	2792	ReadFile	C:\Windows\System32\mscorlib.dll	SUCCESS	Offset: 414.720, Length: 16.384, I/O Flags: ...
16.23...	6AdwCleaner.exe	2792	ReadFile	C:\Windows\System32\mscorlib.dll	SUCCESS	Offset: 402.432, Length: 12.288, I/O Flags: ...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\System32\sechost.dll	SUCCESS	Desired Access: Read Attributes, Disposition...
16.23...	6AdwCleaner.exe	2792	QueryBasicInformationFile	C:\Windows\System32\sechost.dll	SUCCESS	CreationTime: 14/07/2009 01:20:52, LastAc...
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\System32\sechost.dll	SUCCESS	
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\System32\sechost.dll	SUCCESS	Desired Access: Read Data/List Directory, E...
16.23...	6AdwCleaner.exe	2792	CreateFileMapping	C:\Windows\System32\sechost.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PagePr...
16.23...	6AdwCleaner.exe	2792	CreateFileMapping	C:\Windows\System32\sechost.dll	SUCCESS	SyncType: SyncTypeOther
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\System32\sechost.dll	SUCCESS	
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\System32\mscorlib.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319	SUCCESS	Desired Access: Read Data/List Directory, S...
16.23...	6AdwCleaner.exe	2792	QueryDirectory	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	Filter: mscorlib.dll, 1: mscorlib.dll
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319	SUCCESS	
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319	SUCCESS	Desired Access: Read Data/List Directory, S...
16.23...	6AdwCleaner.exe	2792	QueryDirectory	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	Filter: mscorlib.dll, 1: mscorlib.dll
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319	SUCCESS	
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	Desired Access: Read Attributes, Disposition...
16.23...	6AdwCleaner.exe	2792	QueryBasicInformationFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	CreationTime: 18/03/2010 14:27:14, LastAc...
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	Desired Access: Read Data/List Directory, E...
16.23...	6AdwCleaner.exe	2792	CreateFileMapping	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PagePr...
16.23...	6AdwCleaner.exe	2792	CreateFileMapping	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	SyncType: SyncTypeOther
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	
16.23...	6AdwCleaner.exe	2792	ReadFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	Offset: 553.472, Length: 14.848, I/O Flags: ...
16.23...	6AdwCleaner.exe	2792	ReadFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	Offset: 541.184, Length: 12.288, I/O Flags: ...
16.23...	6AdwCleaner.exe	2792	ReadFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	Offset: 456.192, Length: 16.384, I/O Flags: ...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\System32\mscorlib.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\Microsoft.NET\Framework64	SUCCESS	Desired Access: Read Data/List Directory, S...
16.23...	6AdwCleaner.exe	2792	QueryDirectory	C:\Windows\Microsoft.NET\Framework64	SUCCESS	Filter: ", 1: "
16.23...	6AdwCleaner.exe	2792	QueryDirectory	C:\Windows\Microsoft.NET\Framework64	SUCCESS	0: ..., 1: 1040, 2: sbscmp10.dll, 3: sbscmp20...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll	NAME NOT FOUND	Desired Access: Read Attributes, Read Cont...
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.dll	SUCCESS	Desired Access: Read Attributes, Read Cont...
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.dll	SUCCESS	
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll	SUCCESS	Desired Access: Read Attributes, Read Cont...
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll	SUCCESS	
16.23...	6AdwCleaner.exe	2792	QueryDirectory	C:\Windows\Microsoft.NET\Framework64	NO MORE FILES	
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\Microsoft.NET\Framework64	SUCCESS	
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: Read Attributes, Disposition...
16.23...	6AdwCleaner.exe	2792	QueryBasicInformationFile	C:\Windows\System32\imm32.dll	SUCCESS	CreationTime: 14/07/2009 01:38:08, LastAc...
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS	
16.23...	6AdwCleaner.exe	2792	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: Read Data/List Directory, S...
16.23...	6AdwCleaner.exe	2792	CreateFileMapping	C:\Windows\System32\imm32.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PagePr...
16.23...	6AdwCleaner.exe	2792	QueryStandardInformationFile	C:\Windows\System32\imm32.dll	SUCCESS	AllocationSize: 167.936, EndOfFile: 167.424...
16.23...	6AdwCleaner.exe	2792	CreateFileMapping	C:\Windows\System32\imm32.dll	SUCCESS	SyncType: SyncTypeOther
16.23...	6AdwCleaner.exe	2792	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS	

Showing 2,840 of 4,133,780 events (0.0%)      Backed by virtual memory

In quest'altro screenshot della schermata dedicata alle modifiche di registro si nota l'accesso che effettua il programma a varie chiavi. Ne esegue la lettura tramite l'operazione definita **RegOpenKey**, ma in alcuni casi tramite l'esecuzione di altri comandi (**RegQueryValue**, **RegSetInfoKey**) va a compiere altre operazioni come probabilmente anche la modifica di valori al loro interno.



Time ...	Process Name	PID	Operation	Path	Result	Detail
16:23...	6AdwCleaner.exe	2792	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	SUCCESS	
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	REPARSE	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\CompatDll	SUCCESS	Type: REG_SZ, Length: 36, Data: 0006010...
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\00060101.00060101	NAME NOT FOUND	Length: 260
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\Default	SUCCESS	Type: REG_SZ, Length: 36, Data: 0006010...
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Query Value, Set Value
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	REPARSE	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled	NAME NOT FOUND	Length: 80
16:23...	6AdwCleaner.exe	2792	RegCloseKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Query Value
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\SafeDllSearchMode	NAME NOT FOUND	Length: 16
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM	SUCCESS	Desired Access: Maximum Allowed, Granted ...
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\Software\Microsoft\NETFramework\Policy\	SUCCESS	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM\Software\Microsoft\NETFramework\Policy\	SUCCESS	Query: Cached, SubKeys: 5, Values: 0
16:23...	6AdwCleaner.exe	2792	RegEnumKey	HKLM\Software\Microsoft\NETFramework\Policy\	SUCCESS	Index: 4, Name: v4.0
16:23...	6AdwCleaner.exe	2792	RegEnumKey	HKLM\Software\Microsoft\NETFramework\Policy\	SUCCESS	Index: 3, Name: v2.0
16:23...	6AdwCleaner.exe	2792	RegEnumKey	HKLM\Software\Microsoft\NETFramework\Policy\	SUCCESS	Index: 2, Name: Upgrades
16:23...	6AdwCleaner.exe	2792	RegEnumKey	HKLM\Software\Microsoft\NETFramework\Policy\	SUCCESS	Index: 1, Name: standards
16:23...	6AdwCleaner.exe	2792	RegEnumKey	HKLM\Software\Microsoft\NETFramework\Policy\	SUCCESS	Index: 0, Name: AppPatch
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM\Software\Microsoft\NETFramework\Policy\	SUCCESS	Query: HandleTags, HandleTags: 0x0
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\Software\Microsoft\NETFramework\Policy\v4.0	SUCCESS	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM\Software\Microsoft\NETFramework\Policy\v4.0	SUCCESS	Query: Cached, SubKeys: 0, Values: 1
16:23...	6AdwCleaner.exe	2792	RegEnumValue	HKLM\Software\Microsoft\NETFramework\Policy\v4.0	SUCCESS	Index: 0, Name: 30319, Type: REG_SZ, Len...
16:23...	6AdwCleaner.exe	2792	RegCloseKey	HKLM\Software\Microsoft\NETFramework\Policy\v4.0	SUCCESS	
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\Software\Microsoft\NETFramework\	SUCCESS	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\Software\Microsoft\NETFramework\InstallRoot	SUCCESS	Type: REG_SZ, Length: 76, Data: C:\Windo...
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\Software\Microsoft\NETFramework\InstallRoot	SUCCESS	Type: REG_SZ, Length: 76, Data: C:\Windo...
16:23...	6AdwCleaner.exe	2792	RegCloseKey	HKLM\Software\Microsoft\NETFramework\	SUCCESS	
16:23...	6AdwCleaner.exe	2792	RegCloseKey	HKLM\Software\Microsoft\NETFramework\Policy	SUCCESS	
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\Software\Microsoft\NETFramework\	SUCCESS	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\Software\Microsoft\NETFramework\InstallRoot	SUCCESS	Type: REG_SZ, Length: 76, Data: C:\Windo...
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\Software\Microsoft\NETFramework\InstallRoot	SUCCESS	Type: REG_SZ, Length: 76, Data: C:\Windo...
16:23...	6AdwCleaner.exe	2792	RegCloseKey	HKLM\Software\Microsoft\NETFramework\	SUCCESS	
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
16:23...	6AdwCleaner.exe	2792	RegOpenKey	HKLM\Software\Microsoft\NETFramework\	SUCCESS	Desired Access: Read
16:23...	6AdwCleaner.exe	2792	RegQueryValue	HKLM\Software\Microsoft\NETFramework\CLRLoadLogDir	NAME NOT FOUND	Length: 144
16:23...	6AdwCleaner.exe	2792	RegCloseKey	HKLM\Software\Microsoft\NETFramework\	SUCCESS	
16:23...	6AdwCleaner.exe	2792	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0

Showing 2,798 of 4,133,780 events (0.0%) | Filtered by virtual memory



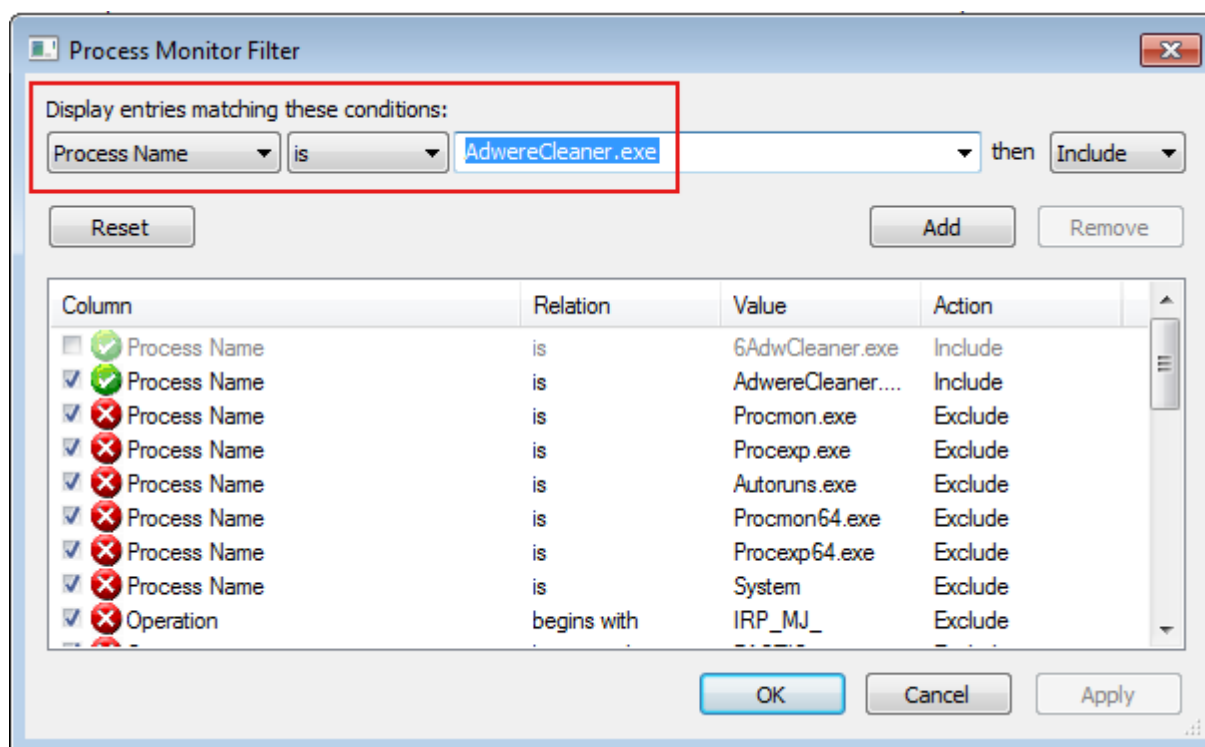
La seguente schermata del programma **Process Monitor** ci mostra invece i processi eseguiti sul sistema. Si può notare l'attimo in cui è stato eseguito il programma, dove appunto è presente la creazione del processo, e anche la creazione di vari **threads**. Viene eseguito anche il caricamento di varie **dll**, probabilmente utili al corretto funzionamento del programma.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
16:23:...	6AdwCleaner.exe	2792	Process Start		SUCCESS	Parent PID: 2104, Command line: "C:\Users\...\
16:23:...	6AdwCleaner.exe	2792	Thread Create		SUCCESS	Thread ID: 2608
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Users\user\AppData\Local\6AdwCleaner.exe	SUCCESS	Image Base: 0xa60000, Image Size: 0x2e000
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77340000, Image Size: 0x19f...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\mscoree.dll	SUCCESS	Image Base: 0x7ef3b0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77220000, Image Size: 0x11f...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ef320000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ef380000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\msvrt.dll	SUCCESS	Image Base: 0x7ef340000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ef360000, Image Size: 0x1...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\vpport4.dll	SUCCESS	Image Base: 0x7ef3c0000, Image Size: 0x1...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	Image Base: 0x7ef21d0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\shlwapi.dll	SUCCESS	Image Base: 0x7ef3a0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ef3d0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x77120000, Image Size: 0xfa0...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\lpk.dll	SUCCESS	Image Base: 0x7ef390000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\usp10.dll	SUCCESS	Image Base: 0x7ef3c0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\imm32.dll	SUCCESS	Image Base: 0x7ef330000, Image Size: 0x2...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\msctf.dll	SUCCESS	Image Base: 0x7ef320000, Image Size: 0x1...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll	SUCCESS	Image Base: 0x7ef380000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\msvcr100_clr0400.dll	SUCCESS	Image Base: 0x7ef3780000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Thread Create		SUCCESS	Thread ID: 2432
16:23:...	6AdwCleaner.exe	2792	Thread Create		SUCCESS	Thread ID: 2476
16:23:...	6AdwCleaner.exe	2792	Thread Create		SUCCESS	Thread ID: 2480
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib.bc19222db4406c472d9aa1f8b...	SUCCESS	Image Base: 0x7ef0500000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\ole32.dll	SUCCESS	Image Base: 0x7ef3a0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\cryptbase.dll	SUCCESS	Image Base: 0x7ef3d160000, Image Size: 0xf...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\uxtheme.dll	SUCCESS	Image Base: 0x7ef3930000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	SUCCESS	Image Base: 0x7ef3c30000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clijit.dll	SUCCESS	Image Base: 0x7ef3030000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\oleaut32.dll	SUCCESS	Image Base: 0x7ef39a0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_64\System\0f8f78b729ce16dd078f5d5f734...	SUCCESS	Image Base: 0x7ef3e850000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\1266d26c7b7843d308...	SUCCESS	Image Base: 0x7ef3e620000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\0acb5c0e7dc2...	SUCCESS	Image Base: 0x7ef3e5d0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\7a93c267da35a9f16b6fa5...	SUCCESS	Image Base: 0x7ef3e4d10000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\cryptsp.dll	SUCCESS	Image Base: 0x7ef3cab0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\rsaenh.dll	SUCCESS	Image Base: 0x7ef3c7b0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\11581b5eba4b3f...	SUCCESS	Image Base: 0x7ef3ead0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\5d9f385419332f14eaf9375...	SUCCESS	Image Base: 0x7ef3ead420000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\rasapi32.dll	SUCCESS	Image Base: 0x7ef35950000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\rasman.dll	SUCCESS	Image Base: 0x7ef38330000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\ws2_32.dll	SUCCESS	Image Base: 0x7ef380000, Image Size: 0x4...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\rsi.dll	SUCCESS	Image Base: 0x7ef3ec90000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\rtutils.dll	SUCCESS	Image Base: 0x7ef3acc0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\mswsock.dll	SUCCESS	Image Base: 0x7ef3ca50000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\WSH_TCPIP.DLL	SUCCESS	Image Base: 0x7ef3c3c0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\wsip6.dll	SUCCESS	Image Base: 0x7ef3ca40000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Thread Create		SUCCESS	Thread ID: 1396
16:23:...	6AdwCleaner.exe	2792	Thread Create		SUCCESS	Thread ID: 3512
16:23:...	6AdwCleaner.exe	2792	Thread Create		SUCCESS	Thread ID: 2644
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\winhttp.dll	SUCCESS	Image Base: 0x7ef3a220000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\webio.dll	SUCCESS	Image Base: 0x7ef3a60000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\sspicli.dll	SUCCESS	Image Base: 0x7ef3d0d0000, Image Size: 0x...
16:23:...	6AdwCleaner.exe	2792	Load Image	C:\Windows\System32\credssp.dll	SUCCESS	Image Base: 0x7ef3c700000, Image Size: 0x...

Showing 87 of 4,133,780 events (0.0%)

Backed by virtual memory

Eseguendo successivamente, la ricerca tramite filtro del nome processo **AdwereCleaner.exe**, si ottengono le stesse schermate.




























Si vede sempre il tentativo del programma di leggere e possibilmente modificare le chiavi di registro.

Process Monitor - Sysinternals www.sysinternals.com

File Edit View Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Desired Access: Query Value, Enumerate Su...
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Disa...	NAME NOT FOUND	Length: 1,024
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Read
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Read
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWDIllegalDLLSearch	NAME NOT FOUND	Length: 1,024
16:23...	AdwCleaner	2104	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	SUCCESS	
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT FOUND	Desired Access: Query Value
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution ...	REPARSE	Desired Access: Query Value, Enumerate Su...
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Desired Access: Query Value, Enumerate Su...
16:23...	AdwCleaner	2104	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	KeySetInformationClass: KeySetHandleTags...
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Disa...	NAME NOT FOUND	Length: 1,024
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Read
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Read
16:23...	AdwCleaner	2104	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	SUCCESS	KeySetInformationClass: KeySetHandleTags...
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWDIllegalDLLSearch	NAME NOT FOUND	Length: 1,024
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	SUCCESS	
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Query Value, Set Value
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	REPARSE	Desired Access: Read
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access: Read
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\Codelidentifiers	REPARSE	Desired Access: Query Value
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\Codelidentifiers	SUCCESS	Desired Access: Query Value
16:23...	AdwCleaner	2104	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\Codelidentifiers	SUCCESS	KeySetInformationClass: KeySetHandleTags...
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\Codelidentifiers\TransparentEnabled	NAME NOT FOUND	Length: 80
16:23...	AdwCleaner	2104	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\Codelidentifiers	SUCCESS	
16:23...	AdwCleaner	2104	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\Codelidentifiers	NAME NOT FOUND	Desired Access: Query Value
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\AssemblySto...	NAME NOT FOUND	Desired Access: Enumerate Sub Keys
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	REPARSE	Desired Access: Read
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	Desired Access: Read
16:23...	AdwCleaner	2104	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	KeySetInformationClass: KeySetHandleTags...
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\CompDll	NAME NOT FOUND	Type: REG_SZ, Length: 36, Data: 0006010...
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\00060101.00060101	NAME NOT FOUND	Length: 260
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\Default	SUCCESS	Type: REG_SZ, Length: 36, Data: 0006010...
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
16:23...	AdwCleaner	2104	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	SUCCESS	KeySetInformationClass: KeySetHandleTags...
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\SafeDllSearchMode	NAME NOT FOUND	Length: 16
16:23...	AdwCleaner	2104	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed, Granted ...
16:23...	AdwCleaner	2104	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
16:23...	AdwCleaner	2104	RegQueryKey	HKLM	SUCCESS	Query: Name
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: Read
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	REPARSE	Desired Access: Read
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: Read
16:23...	AdwCleaner	2104	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	KeySetInformationClass: KeySetHandleTags...
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles	NAME NOT FOUND	Length: 20
16:23...	AdwCleaner	2104	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS	Desired Access: Read
16:23...	AdwCleaner	2104	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32\A...	NAME NOT FOUND	Length: 172
16:23...	AdwCleaner	2104	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS	
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\IME Compatibility	NAME NOT FOUND	Desired Access: Read
16:23...	AdwCleaner	2104	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
16:23...	AdwCleaner	2104	RegQueryKey	HKLM	SUCCESS	Query: Name
16:23...	AdwCleaner	2104	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	Desired Access: Read
16:23...	AdwCleaner	2104	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	KeySetInformationClass: KeySetHandleTags...

Showing 6,436 of 4,133,780 events (0.1%)

Backed by virtual memory.

## Le varie attività di lettura e scrittura sul file system della macchina.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
16:23...	AdwCleaner...	2104	ReadFile	C:	SUCCESS	Offset: 0, Length: 4 096, I/O Flags: Non-cac...
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\Prefetch\ADWERCLEANER.EXE-7432BA41.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: ...
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows	SUCCESS	Desired Access: Execute/Traverse, Synchro...
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Attributes, Disposition...
16:23...	AdwCleaner...	2104	QueryBasicInformationFile	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 30/07/2024 11:51:59, LastAc...
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Data/List Directory, E...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	Sync Type: SyncTypeCreateSection, PagePr...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\System32\wow64.dll	SUCCESS	Sync Type: SyncTypeOther
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: Read Attributes, Disposition...
16:23...	AdwCleaner...	2104	QueryBasicInformationFile	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 30/07/2024 11:51:59, LastAc...
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: Read Data/List Directory, E...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	Sync Type: SyncTypeCreateSection, PagePr...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\System32\wow64win.dll	SUCCESS	Sync Type: SyncTypeOther
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: Read Attributes, Disposition...
16:23...	AdwCleaner...	2104	QueryBasicInformationFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 30/07/2024 11:51:59, LastAc...
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: Read Data/List Directory, E...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	Sync Type: SyncTypeCreateSection, PagePr...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\System32\wow64cpu.dll	SUCCESS	Sync Type: SyncTypeOther
16:23...	C:\Users\user\Downloads\AdwCleaner.exe			C:\Windows\System32\wow64cpu.dll	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition...
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows	SUCCESS	Desired Access: Read Attributes, Synchroniz...
16:23...	AdwCleaner...	2104	QueryNameInformationFile	C:\Windows	SUCCESS	Name: \Windows
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Users\user\Downloads	SUCCESS	Desired Access: Execute/Traverse, Synchro...
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: Read Attributes, Disposition...
16:23...	AdwCleaner...	2104	QueryBasicInformationFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	CreationTime: 14/07/2009 01:11:59, LastAc...
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: Read Data/List Directory, E...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\SysWOW64\sechost.dll	FILE LOCKED WI...	Sync Type: SyncTypeCreateSection, PagePr...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Sync Type: SyncTypeOther
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Users\user\Downloads\AdwCleaner.exe.Local	NAME NOT FOUND	Desired Access: Read Attributes, Disposition...
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Desired Access: Read Attributes, Disposition...
16:23...	AdwCleaner...	2104	QueryBasicInformationFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	CreationTime: 21/11/2010 05:24:13, LastAc...
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Desired Access: Execute/Traverse, Synchro...
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Desired Access: Read Attributes, Disposition...
16:23...	AdwCleaner...	2104	QueryBasicInformationFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	CreationTime: 21/11/2010 05:24:09, LastAc...
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	
16:23...	AdwCleaner...	2104	CreateFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Desired Access: Read Data/List Directory, E...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	FILE LOCKED WI...	Sync Type: SyncTypeCreateSection, PagePr...
16:23...	AdwCleaner...	2104	QueryStandardInformationFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	AllocationSize: 532 480, EndOfFile: 530 432...
16:23...	AdwCleaner...	2104	ReadFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Offset: 0, Length: 4 096, I/O Flags: Non-cac...
16:23...	AdwCleaner...	2104	ReadFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Offset: 514 048, Length: 16 384, I/O Flags: ...
16:23...	AdwCleaner...	2104	CreateFileMapping	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Sync Type: SyncTypeOther
16:23...	AdwCleaner...	2104	ReadFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Offset: 140 288, Length: 32 768, I/O Flags: ...
16:23...	AdwCleaner...	2104	CloseFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	
16:23...	AdwCleaner...	2104	ReadFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Offset: 487 936, Length: 16 384, I/O Flags: ...
16:23...	AdwCleaner...	2104	ReadFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	Offset: 447 488, Length: 29 184, I/O Flags: ...
16:23...	AdwCleaner...	2104	ReadFile	C:\Windows\winxs\x86_microsoft.windows.common-controls_6595b64144cdf1df_5.82.7601.1...	SUCCESS	

Showing 964 of 4.133.780 events (0.0%)

Backed by virtual memory

Qui poi si nota di nuovo l'avvio del processo padre e la creazione di vari **threads**, nonché l'accesso a varie **dll** di sistema.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
16:23...	AdwareCleaner...	2104	Process Start		SUCCESS	Parent PID: 2008, Command line: "C:\Users\...
16:23...	AdwareCleaner...	2104	Thread Create		SUCCESS	Thread ID: 2376
16:23...	AdwareCleaner...	2104	Load Image	C:\Users\user\Downloads\AdwareCleaner.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x43000
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77340000, Image Size: 0x19f...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77500000, Image Size: 0x18...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x74fc0000, Image Size: 0x3f000
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x74f60000, Image Size: 0x5c0...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x74f50000, Image Size: 0x8000
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77220000, Image Size: 0x1f...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76ba0000, Image Size: 0x1f...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77220000, Image Size: 0x1f...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x77120000, Image Size: 0xfa0...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76ba0000, Image Size: 0x11...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x76d60000, Image Size: 0x47...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x76740000, Image Size: 0x10...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x76530000, Image Size: 0x90...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x76f20000, Image Size: 0xa000
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x76f20000, Image Size: 0x9d...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x76cb0000, Image Size: 0xac...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x76540000, Image Size: 0xa1...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x76350000, Image Size: 0x19...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\vpct4.dll	SUCCESS	Image Base: 0x761a0000, Image Size: 0xf00...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Image Base: 0x76050000, Image Size: 0x60...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Image Base: 0x76040000, Image Size: 0xc000
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x753f0000, Image Size: 0xc4a...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x76eb0000, Image Size: 0x57...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.1...	SUCCESS	Image Base: 0x73430000, Image Size: 0x84...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x76a70000, Image Size: 0x15...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\version.dll	SUCCESS	Image Base: 0x74400000, Image Size: 0x9000
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x76140000, Image Size: 0x60...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Image Base: 0x76ad0000, Image Size: 0xccc...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Image Base: 0x74ca0000, Image Size: 0x80...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\ehfolder.dll	SUCCESS	Image Base: 0x74ca20000, Image Size: 0x5000
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17...	SUCCESS	Image Base: 0x76440000, Image Size: 0x19...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x76db0000, Image Size: 0x8f0...
16:23...	AdwareCleaner...	2104	Thread Create		SUCCESS	Thread ID: 3188
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\clbcatq.dll	SUCCESS	Image Base: 0x752c0000, Image Size: 0x83...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\setupapi.dll	SUCCESS	Image Base: 0x76320000, Image Size: 0x19...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\cfgmgr32.dll	SUCCESS	Image Base: 0x76f80000, Image Size: 0x270...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\devobj.dll	SUCCESS	Image Base: 0x76e40000, Image Size: 0x12...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\propkeys.dll	SUCCESS	Image Base: 0x73d30000, Image Size: 0xf50...
16:23...	AdwareCleaner...	2104	Thread Create		SUCCESS	Thread ID: 1492
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS	Image Base: 0x74c70000, Image Size: 0x21...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\Wdap32.dll	SUCCESS	Image Base: 0x76290000, Image Size: 0x45...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\prcfapi.dll	SUCCESS	Image Base: 0x74c50000, Image Size: 0xb000
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\IconCodecService.dll	SUCCESS	Image Base: 0x73ed0000, Image Size: 0x6000
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\WindowsCodecs.dll	SUCCESS	Image Base: 0x73330000, Image Size: 0xfb0...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x73ee0000, Image Size: 0x4c...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\shdocvw.dll	SUCCESS	Image Base: 0x73ea0000, Image Size: 0x2e...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\shdocvw.dll	SUCCESS	Image Base: 0x73ce0000, Image Size: 0x2e...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\shdocvw.dll	SUCCESS	Image Base: 0x73ce0000, Image Size: 0x2e...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\shdocvw.dll	SUCCESS	Image Base: 0x73ce0000, Image Size: 0x2e...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x24b0000, Image Size: 0xc4a...
16:23...	AdwareCleaner...	2104	Load Image	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Image Base: 0x750b0000, Image Size: 0x13...

Showing 66 of 4.133.780 events (0.0%)

Backed by virtual memory

[illegible]

