

CS0424

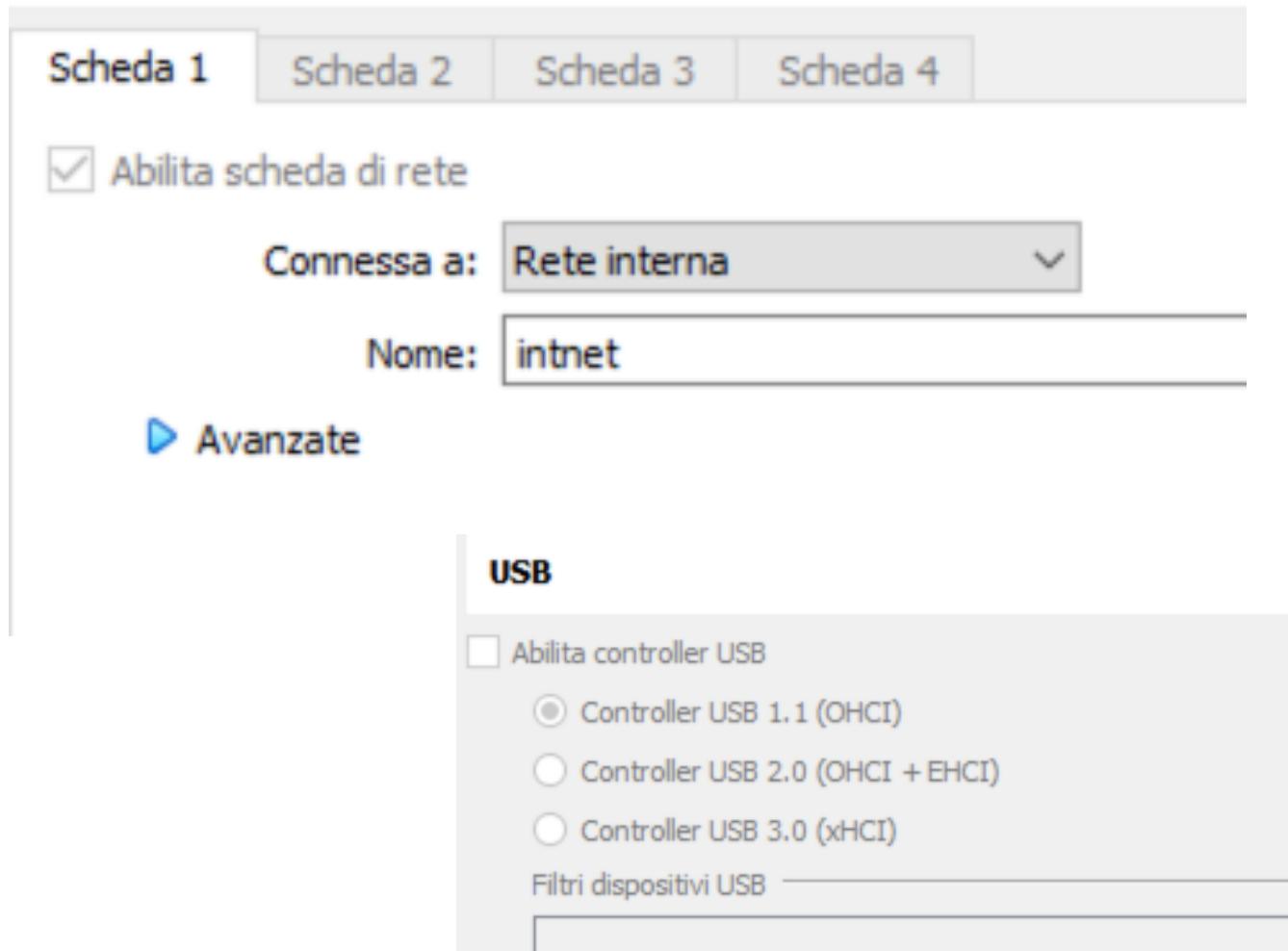
S10-L2

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' instantanea della macchina prima di eseguire il malware, per poterla ripristinare facilmente.



2. Azioni sul file system:

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

Process Monitor Filter

Display entries matching these conditions:

Process Name is AdwereCleaner.exe then Include

Reset Add Remove

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ... Process Name PID Operation Path Result Detail

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:17:...	AdwereCleaner....	2484	Process Start		SUCCESS	Parent PID: 1404, ...
16:17:...	AdwereCleaner....	2484	Thread Create		SUCCESS	Thread ID: 2428
16:17:...	AdwereCleaner....	2484	Load Image	C:\Users\user\Desktop\MALWARE\Ad... SUCCESS		Image Base: 0x400...
16:17:...	AdwereCleaner....	2484	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x773...
16:17:...	AdwereCleaner....	2484	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x775...
16:17:...	AdwereCleaner....	2484	ReadFile	C:	SUCCESS	Offset: 0, Length: 4...
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\Prefetch\ADWERECLEA... NAME NOT FOUND Desired Access: G...		
16:17:...	AdwereCleaner....	2484	RegOpenKey	HKLM\Software\Microsoft\Windows N... SUCCESS		Desired Access: Q...
16:17:...	AdwereCleaner....	2484	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window... NAME NOT FOUND Length: 1.024		
16:17:...	AdwereCleaner....	2484	RegOpenKey	HKLM\System\CurrentControlSet\Contr... REPARSE		Desired Access: R...
16:17:...	AdwereCleaner....	2484	RegOpenKey	HKLM\System\CurrentControlSet\Contr... SUCCESS		Desired Access: R...
16:17:...	AdwereCleaner....	2484	RegQueryValue	HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 1.024		
16:17:...	AdwereCleaner....	2484	RegCloseKey	HKLM\System\CurrentControlSet\Contr... SUCCESS		
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	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 30/0...
16:17:...	AdwereCleaner....	2484	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:17:...	AdwereCleaner....	2484	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
16:17:...	AdwereCleaner....	2484	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x749...
16:17:...	AdwereCleaner....	2484	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 30/0...
16:17:...	AdwereCleaner....	2484	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:17:...	AdwereCleaner....	2484	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
16:17:...	AdwereCleaner....	2484	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x748...
16:17:...	AdwereCleaner....	2484	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
16:17:...	AdwereCleaner....	2484	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...

Showing 7.701 of 93.867 events (8.%) Backed by virtual memory

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

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

PID is 2484 Include

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: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7ef...
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\vsaenh.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\assembly\NativeImages_v...	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\vasapi32.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\vasman.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\wnsi.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\vtutils.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\WSHCTPIP.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\dhcpsvc6.dll	SUCCESS	Image Base: 0x7ef...
16:17:...	6AdwCleaner.exe	2400	Load Image	C:\Windows\System32\dhcpsvc.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\vasadhlp.dll	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\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\verutil.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: 0x7ef...
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\virtmarta.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
<input checked="" type="checkbox"/>  PID	is	2484	Include
<input checked="" type="checkbox"/>  PID	is	2400	Include
<input checked="" type="checkbox"/>  Operation	is	CreateFile	Include
<input checked="" type="checkbox"/>  Operation	is	CloseFile	Include
<input checked="" type="checkbox"/>  Operation	is	WriteFile	Include
<input checked="" type="checkbox"/>  Operation	is	ReadFile	Include

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\nmm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	>CreateFile	C:\Windows\SysWOW64\nmm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	>CreateFile	C:\Windows\SysWOW64\nmm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	>CreateFile	C:\Windows\SysWOW64\nmm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	>CreateFile	C:\Windows\SysWOW64\nmm32.dll	SUCCESS	Desired Access: R...
16:17:...	AdwereCleaner....	2484	>CreateFile	C:\Windows\SysWOW64\vpccs.dll	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	>CreateFile	C:\Windows\SysWOW64\vpccs.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\NS...	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\Localization\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:\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\Microso...	NAME COLLISION	Desired Access: R...
16:17:...	AdwereCleaner....	2484	>CreateFile	C:\Users\user\AppData\Local\Microso...	SUCCESS	Desired Access: G...
16:17:...	AdwereCleaner....	2484	>CreateFile	C:\Users\user\Desktop\MALWARE\Vrt...	NAME NOT FOUND	Desired Access: R...
16:17:...	AdwereCleaner....	2484	>CreateFile	C:\Windows\SysWOW64\trans.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

The screenshot shows the Process Monitor interface with several filter rules applied at the top:

Operation	is	Process Create	Include
Operation	is	Process Start	Include
Operation	is	Process Exit	Include
Operation	is	Thread Create	Include
Operation	is	Thread Exit	Include
<input checked="" type="checkbox"/>		Operation is	Process Create Include
<input checked="" type="checkbox"/>		Operation is	Process Start Include
<input checked="" type="checkbox"/>		Operation is	Process Exit Include
<input type="checkbox"/>		Operation is	Thread Create Include
<input type="checkbox"/>		Operation is	Thread Exit Include

The main pane displays a table of events:

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:17:...	AdwCleaner....	2484	Process Start		SUCCESS	Parent PID: 1404, ...
16:17:...	AdwCleaner....	2484	Process Create	C:\Users\user\AppData\Local\6AdwCl...	SUCCESS	PID: 2400, Comma...
16:17:...	6AdwCleaner.exe	2400	Process Start		SUCCESS	Parent PID: 2484, ...
16:17:...	AdwCleaner....	2484	Process Exit		SUCCESS	Exit Status: 0, User...
16:18:...	6AdwCleaner.exe	2400	Process Exit		SUCCESS	Exit Status: 0, User...

The screenshot shows the Process Monitor interface with several filter rules applied at the top:

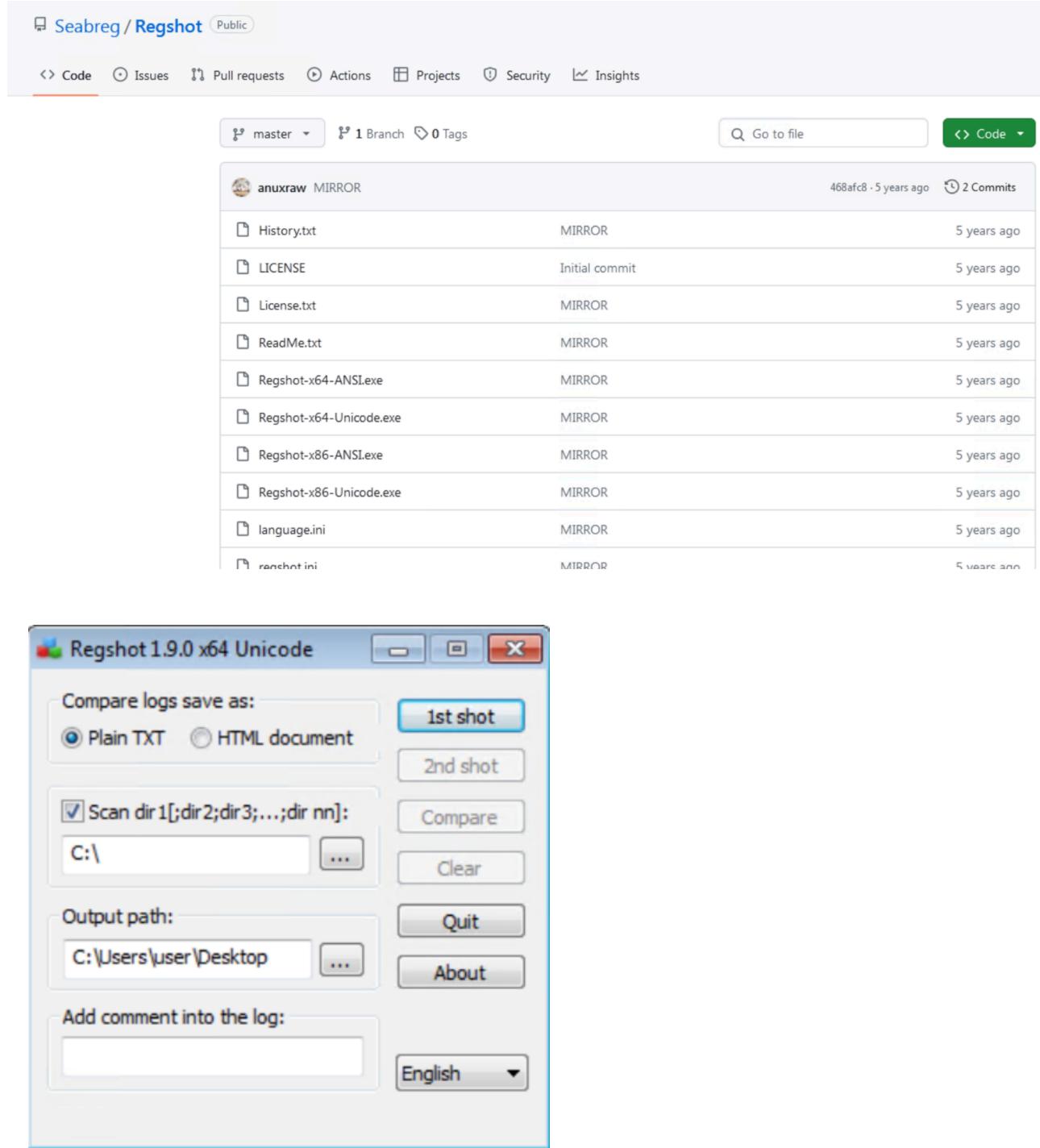
Operation	is	Process Create	Include
Operation	is	Process Start	Include
Operation	is	Process Exit	Include
Operation	is	Thread Create	Include
Operation	is	Thread Exit	Include
<input checked="" type="checkbox"/>		Operation is	Process Create Include
<input checked="" type="checkbox"/>		Operation is	Process Start Include
<input checked="" type="checkbox"/>		Operation is	Process Exit Include
<input type="checkbox"/>		Operation is	Thread Create Include
<input type="checkbox"/>		Operation is	Thread Exit Include

The main pane displays a table of events:

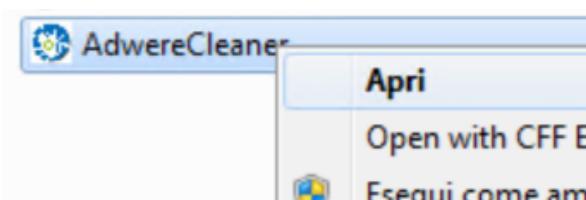
Time ...	Process Name	PID	Operation	Path	Result	Detail
16:17:...	AdwCleaner....	2484	Thread Create		SUCCESS	Thread ID: 2428
16:17:...	AdwCleaner....	2484	Thread Create		SUCCESS	Thread ID: 3024
16:17:...	AdwCleaner....	2484	Thread Create		SUCCESS	Thread ID: 2560
16:17:...	AdwCleaner....	2484	Thread Create		SUCCESS	Thread ID: 344
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 1236
16:17:...	AdwCleaner....	2484	Thread Exit		SUCCESS	Thread ID: 2560, ...
16:17:...	AdwCleaner....	2484	Thread Exit		SUCCESS	Thread ID: 2428, ...
16:17:...	AdwCleaner....	2484	Thread Exit		SUCCESS	Thread ID: 344, Us...
16:17:...	AdwCleaner....	2484	Thread Exit		SUCCESS	Thread ID: 3024, ...
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 1948
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2756
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2508
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2648
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2664
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2780
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2828
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2804
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2796
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 548
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 1284
16:17:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2964
16:18:...	6AdwCleaner.exe	2400	Thread Create		SUCCESS	Thread ID: 2868
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2756, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2868, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 1284, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2796, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2828, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2664, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2508, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 1948, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2964, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 548, Us...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2804, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2648, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 2780, ...
16:18:...	6AdwCleaner.exe	2400	Thread Exit		SUCCESS	Thread ID: 1236, ...

4. Modifiche del registro da parte del malware:

Per trovare le differenze nel registro da prima dell'esecuzione del malware a dopo ho utilizzato un 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.

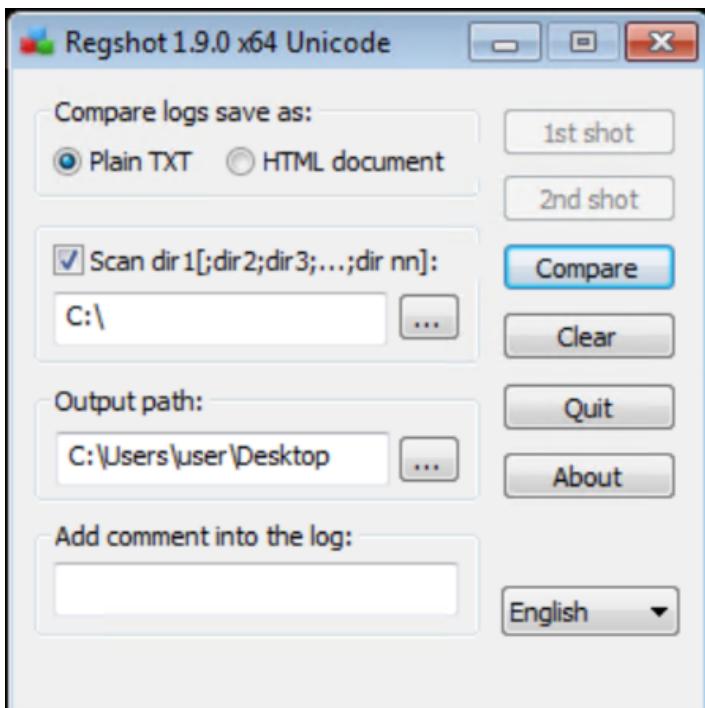
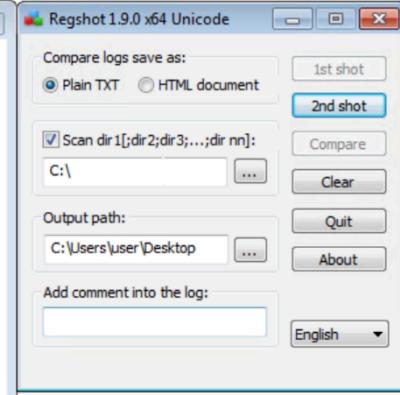




Welcome To AdwCleaner

If you have downloaded and ran this application, we assume you are looking for a solution for the ads and popups that litter your system. These popups are not generated by the websites you visit, but are generated by adware on your PC.

AdwCleaner will scan your system and alert you of any threats that are present, after a scan and removal of the malicious software the popups should be gone and your pc much faster and easier to use then it is now.



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

```

~res-x64 - Blocco note
File Modifica Formato Visualizza ?
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2024/7/30 22:15:22 , 2024/7/30 22:22:58
Computer: USER-PC , USER-PC
Username: user , user

-----
Keys added: 11
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASAPI32
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASMANCS
HKEY\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\Session1
HKEY\Software\Microsoft\Windows NT\CurrentVersion\Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\70d4
HKEY\Software\Microsoft\Windows NT\CurrentVersion\Accessibility
HKEY\Software\Microsoft\Windows NT\CurrentVersion\AccessibilityTemp
HKEY\Software\Microsoft\Windows NT\CurrentVersion\MS Switch
HKEY\Software\Microsoft\OSK
HKEY\Software\Microsoft\TPG
HKEY\Software\Microsoft\TPG\Recognizers
HKEY\Software\AdwCleaner

-----
Values added: 48
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableFileTracing: 0x00000000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableConsoleTracing: 0x00000000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASAPI32\FileTracingMask: 0xFFFF0000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASAPI32\ConsoleTracingMask: 0xFFFF0000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASAPI32\MaxFileSize: 0x00100000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASAPI32\Directory: "%windir%\tracing"
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASMANCS\EnableFileTracing: 0x00000000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASMANCS\EnableConsoleTracing: 0x00000000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASMANCS\FileTracingMask: 0xFFFF0000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASMANCS\ConsoleTracingMask: 0xFFFF0000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASMANCS\MaxFileSize: 0x00100000
HKEY\Software\Microsoft\Tracing\6AdwCleaner_RASMANCS\Directory: "%windir%\tracing"
HKEY\Software\Windows NT\CurrentVersion\Accessibility\Session1\Configuration: ""
HKEY\Software\Windows NT\CurrentVersion\Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\70d4
HKEY\Software\Windows NT\CurrentVersion\Explorer\Complg32\OpenSavePidlMRU\*: 5C C
HKEY\Software\Windows NT\CurrentVersion\Explorer\Complg32\OpenSavePidlMRU\hivu\1: 31 00 73 00 68 00 6
HKEY\Software\Windows NT\CurrentVersion\Explorer\RecentDocs\25: 31 00 73 00 68 00 6
HKEY\Software\Windows NT\CurrentVersion\Explorer\RecentDocs\hivu\1: 31 00 73 00 68 00 6
HKEY\Software\Windows NT\CurrentVersion\Explorer\UserAssist\{CEBF5CD-ACE2-4F4F-9178}
HKEY\Software\Windows NT\CurrentVersion\Explorer\UserAssist\{CEBF5CD-ACE2-4F4F-9178}
HKEY\Software\Windows NT\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-4F50-A9AE}
HKEY\Software\Windows NT\CurrentVersion\Run\AdwCleaner: "c:\Users\user\AppData\Loca
HKEY\Software\Windows NT\CurrentVersion\Accessibility\Configuration: ""
HKEY\Software\Windows NT\CurrentVersion\Accessibility\Temp\osk: 0x00000000
HKEY\Software\Windows NT\CurrentVersion\Accessibility\WindowLeft: 0x00000064
HKEY\Software\Windows NT\CurrentVersion\Accessibility\WindowTop: 0x00000064
HKEY\Software\Windows NT\CurrentVersion\Accessibility\WindowWidth: 0x0000033c
HKEY\Software\Windows NT\CurrentVersion\Accessibility\WindowHeight: 0x000000ec
HKEY\Software\Windows NT\CurrentVersion\Accessibility\ClickSound: 0x00000001

```

values modified: 16

Files added: 11

```
C:\ProgramData\Microsoft\Windows_Defender\Scans\History\Results\Resource\[d84c29d5-af83-493b-ba84-5599d00a9325]
C:\Users\All Users\Microsoft\Windows_Defender\Scans\History\Results\Resource\[d84c29d5-af83-493b-ba84-5599d00a9325]
C:\Users\user\AppData\Local\6adwcleaner.exe
C:\Users\user\AppData\LocalLow\Microsoft\Cryptnetur\cache\Content\b8cc409acdfb2a4f0e4c56f2875b1f06
C:\Users\user\AppData\LocalLow\Microsoft\Cryptnetur\cache\Content\b9081179068a74c79d1bc450c2894b1_A54f26a8a41de52c237d54d67f12793f
C:\Users\user\AppData\LocalLow\Microsoft\Cryptnetur\cache\Content\f4d9c88987aeBCF4e1a2daabc53628a_77d78d611e65a2a81ea974847cb0c84
C:\Users\user\AppData\LocalLow\Microsoft\Cryptnetur\cache\Metadata\b8cc409acdfb2a4f0e4c56f2875b1f06
C:\Users\user\AppData\LocalLow\Microsoft\Cryptnetur\cache\Metadata\b9081179068a74c79d1bc450c2894b1_A54f26a8a41de52c237d54d67f12793f
C:\Users\user\AppData\LocalLow\Microsoft\Cryptnetur\cache\Metadata\f4d9c88987aeBCF4e1a2daabc53628a_77d78d611e65a2a81ea974847cb0c84
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\1shot.hivu.lnk
C:\Users\user\Desktop\1shot.hivu
```

Files deleted: 2

C:\Windows\Temp\TMP0000021D5C45BCFD0489823
C:\Windows\Temp\TMP00000231F33E17DD94F6D2F

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\cryptnetui\Cache\Metadata\b77EC638DA74B  
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b  
C:\Users\user\NTUSER.DAT
```

Ha rilevato un totale di 101 modifiche di cui:

11 chiavi aggiunte

48 valori aggiuntivi

16 valori modificati

11 file aggiunt

2 file eliminati