Report Esercizio 1: Malware analysis

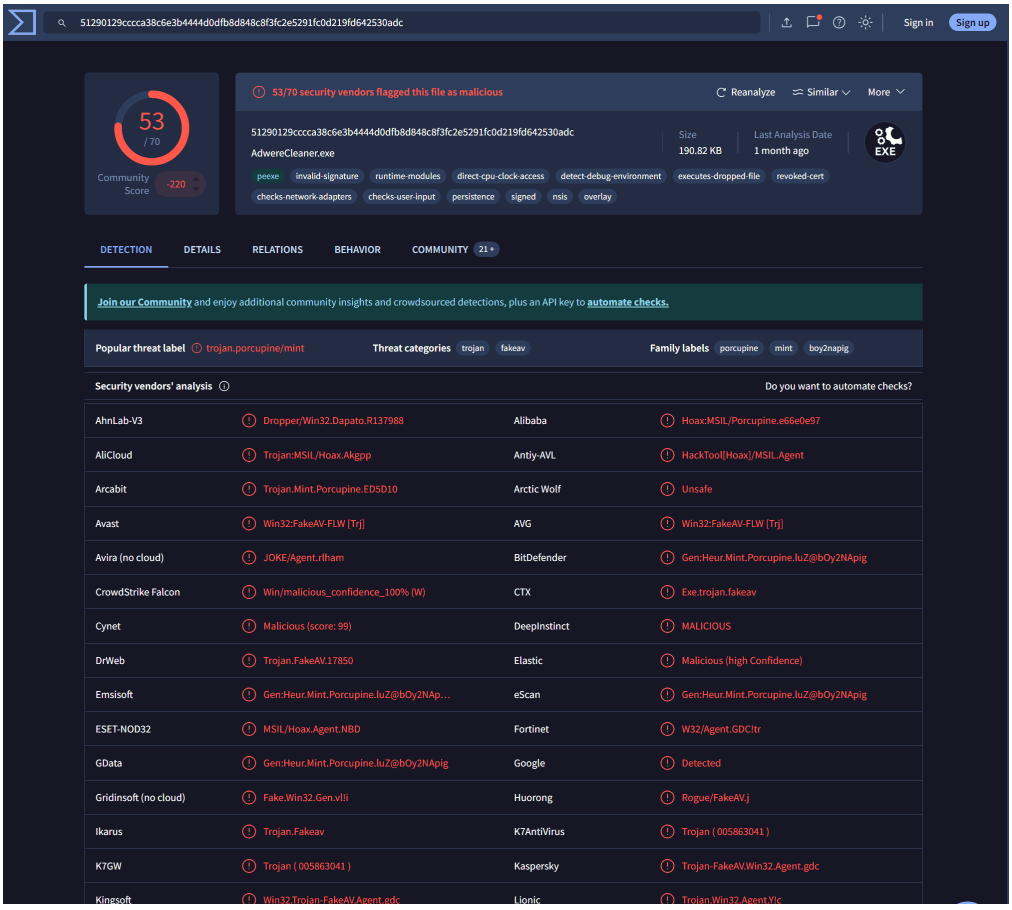
> A cura di Iris Canole, Federico Giannini, Daniele Castello, Luca Pani, Rosario Papa, Yari Olmi, Alessandro Salerno

Introduzione

Scaricare il MALWARE presente in questo link, effettuare un'analisi completa, pulire le tracce e creare un report
scaricando il malware dal seguente link: `The-MALWARE-Repo/rogues/AdwereCleaner.exe at master · Da2dalus/The-MALWARE-Repo](https://github.com/Da2dalus/The-MALWARE-Repo/blob/master/rogues/AdwereCleaner.exe)`

Parte 1: Analisi statica

Per eseguire l'analisi statica abbiamo in primis scaricato il file sulla Kali e fatto analizzare il malware a Virustotal che ha restituito come output il seguente:



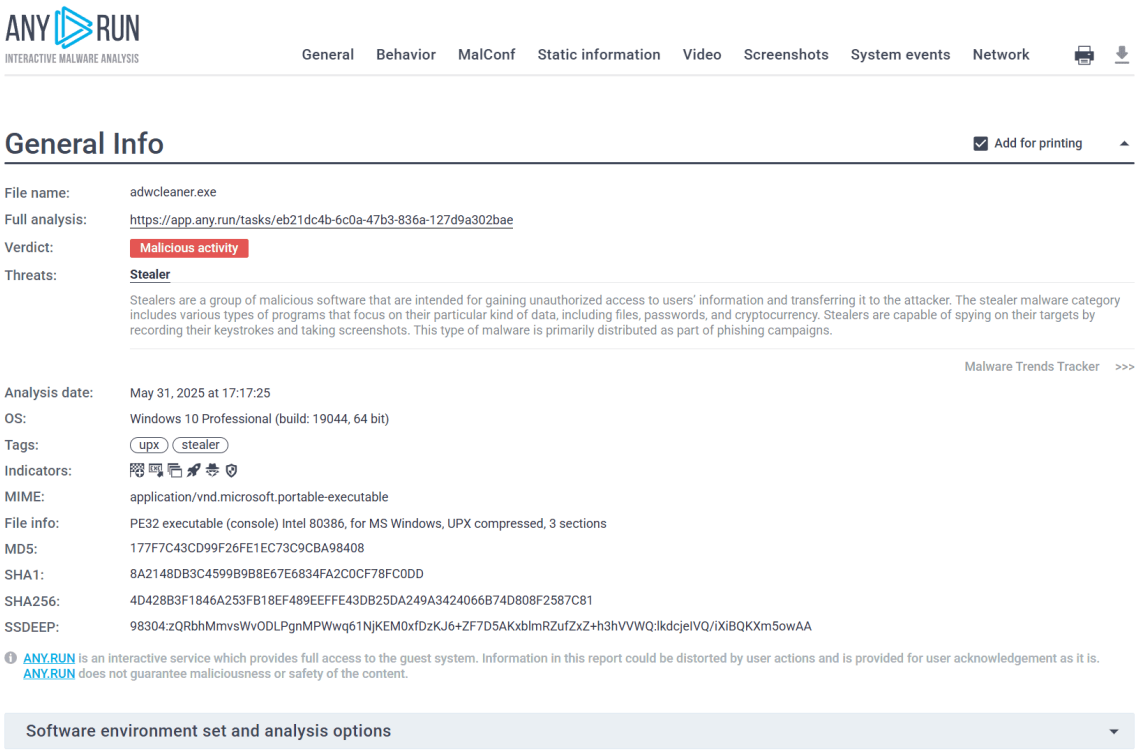
Il **malware** viene definito come `Trojan-FakeAV`. Questi programmi cercano di **simulare** l'attività di

un software **antivirus** o dei moduli di sicurezza del sistema operativo.
Le minacce informatiche che i `Trojan-FakeAV` notificano, in realtà, **non** esistono affatto ma sono solo un escamotage per avere accesso ai dati di un Host con intenti malevoli. In genere, questi software maligni fanno apparire dei pop-up sullo schermo del computer, nel tentativo di generare una forte **preoccupazione** riguardo allo stato di sicurezza del sistema sul quale l'utente opera, inducendo quest'ultimo a pagare una determinata cifra per poter usufruire di un "programma antivirus" (ovviamente fasullo).

Cercando il **malware** anche su **Anyrun** per avere una panoramica più dettagliata vediamo che il malware viene definito come **stealer**.

> **Stealer**
> Gli "stealers" sono sono un gruppo di software dannosi progettati per ottenere l'accesso non autorizzato alle informazioni degli utenti e trasferirle all'autore dell'attacco.

La categoria dei malware stealer comprende vari tipi di programmi che si concentrano su particolari tipi di dati, tra cui file, password e criptovalute." Inoltre nel report sono già descritti i vari hash `MD5`, `SHA1`, `SHA256` e `SSDEEP`.



Questi sono tutta la lista dei comportamenti malevoli messi in atto con i relativi processi che si

attivano:

Behavior activities

Add for printing

MALICIOUS

Steals credentials from Web Browsers
- adwcleaner.exe (PID: 5968)

Changes the autorun value in the registry
- netsh.exe (PID: 5956)

SUSPICIOUS

The process verifies whether the antivirus software is installed
- adwcleaner.exe (PID: 5968)

Reads the BIOS version
- adwcleaner.exe (PID: 5968)

Uses NETSH.EXE to change the status of the firewall
- adwcleaner.exe (PID: 5968)

Modifies hosts file to alter network resolution
- adwcleaner.exe (PID: 5968)

Searches for installed software
- adwcleaner.exe (PID: 5968)

Suspicious use of NETSH.EXE
- adwcleaner.exe (PID: 5968)

Process uses IPCONFIG to clear DNS cache
- adwcleaner.exe (PID: 5968)

Reads security settings of Internet Explorer
- StartMenuExperienceHost.exe (PID: 5260)

Reads the date of Windows installation
- StartMenuExperienceHost.exe (PID: 5260)

Executable content was dropped or overwritten
- MBsetup-adwc.adwc100.exe (PID: 1680)
- adwcleaner.exe (PID: 5968)

Executes as Windows Service
- MBAMInstallerService.exe (PID: 3420)

INFO

The sample compiled with english language support
- adwcleaner.exe (PID: 5968)
- MBsetup-adwc.adwc100.exe (PID: 1680)
- MBAMInstallerService.exe (PID: 3420)

Checks supported languages
- adwcleaner.exe (PID: 5968)
- OfficeClickToRun.exe (PID: 1328)
- SearchApp.exe (PID: 1600)
- StartMenuExperienceHost.exe (PID: 5260)

Reads the computer name
- adwcleaner.exe (PID: 5968)
- OfficeClickToRun.exe (PID: 1328)
- StartMenuExperienceHost.exe (PID: 5260)
- SearchApp.exe (PID: 1600)

Reads the software policy settings
- adwcleaner.exe (PID: 5968)

UPX packer has been detected
- adwcleaner.exe (PID: 5968)

Checks proxy server information
- adwcleaner.exe (PID: 5968)
- OfficeClickToRun.exe (PID: 1328)

Create files in a temporary directory
- adwcleaner.exe (PID: 5968)

Executes as Windows Service
- OfficeClickToRun.exe (PID: 1328)

Uses BITSADMIN.EXE
- adwcleaner.exe (PID: 5968)

Reads the machine GUID from the registry
- OfficeClickToRun.exe (PID: 1328)
- adwcleaner.exe (PID: 5968)

Reads Microsoft Office registry keys
- OfficeClickToRun.exe (PID: 1328)

Launch of the file from Registry key
- netsh.exe (PID: 5956)

Disables trace logs
- netsh.exe (PID: 8140)

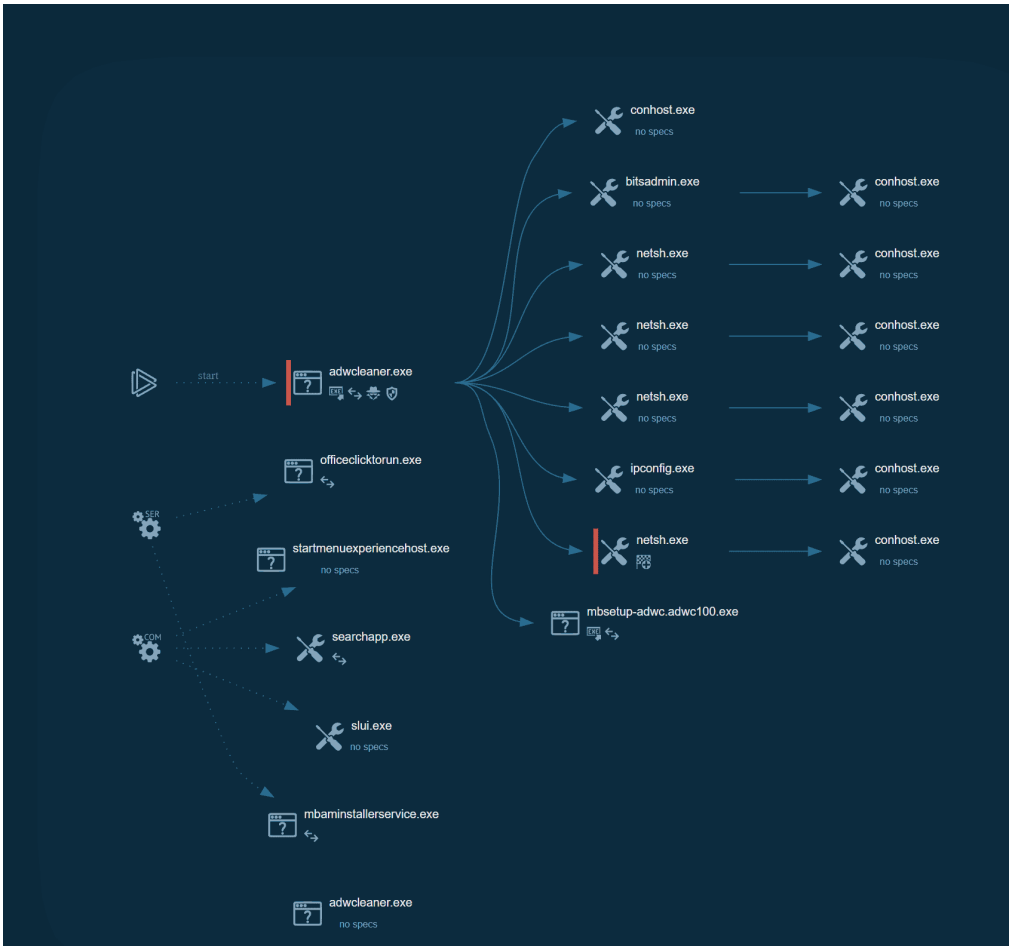
Process checks computer location settings
- StartMenuExperienceHost.exe (PID: 5260)

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report

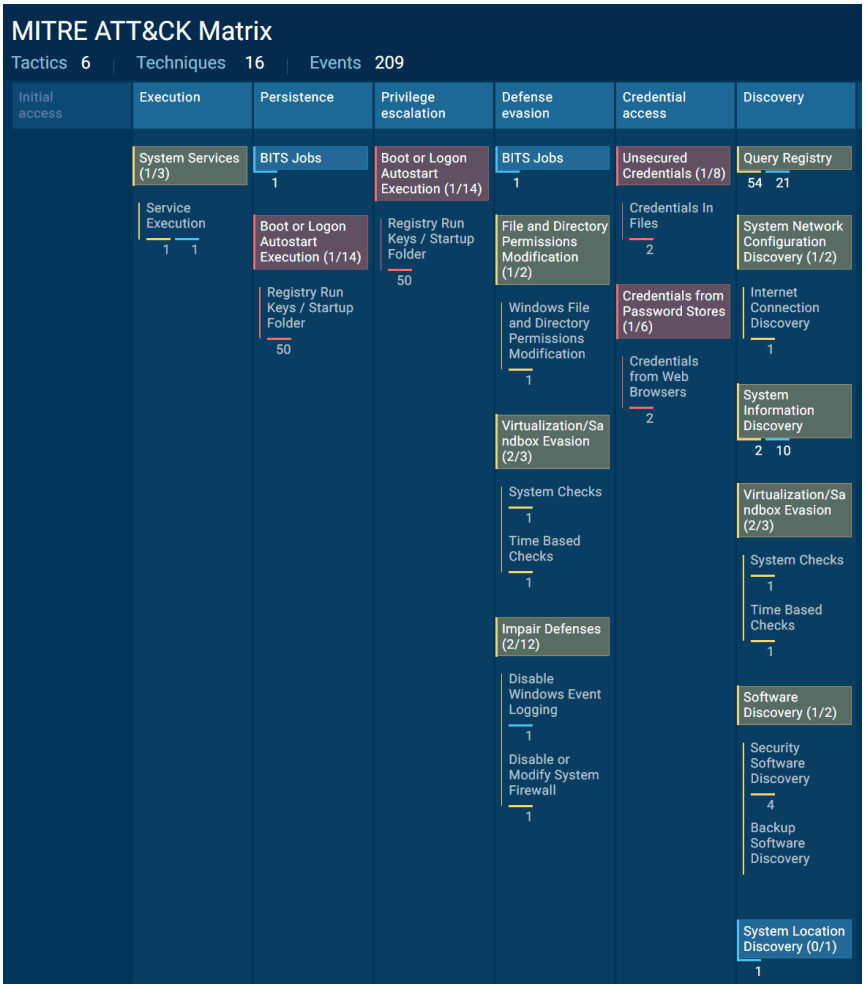
Malware configuration

Add for printing

L’albero con tutta la “genitorialità dei processi”



e infine la matrice del **MITRE** in cui vengono descritte nel dettaglio le tecniche e le tattiche messe in atto dal malware per aggirare i sistemi di sicurezza, mantenere la presenza all'interno della macchina e esfiltrare dati.

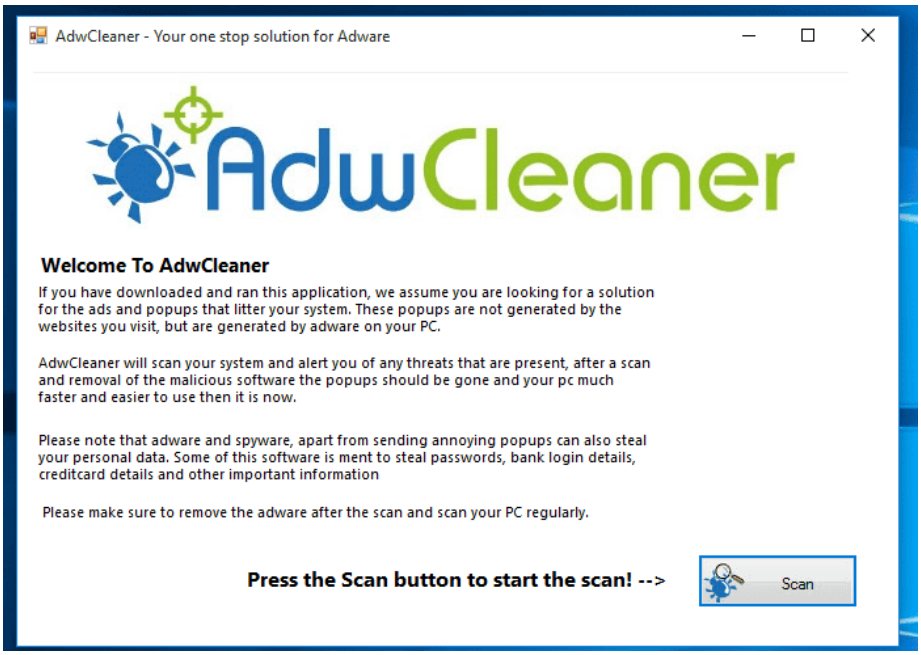


> **ANY.RUN**
>
> **ANY.RUN** è un popolare **servizio di analisi malware basato su cloud** che fornisce una **sandbox** interattiva.
>
> È una piattaforma online che consente ai professionisti della cybersecurity (analisti, ricercatori) di caricare e lanciare in sicurezza file sospetti (come eseguibili, documenti o URL) all'interno di un **ambiente virtuale isolato** (la sandbox).
>
> La sua caratteristica distintiva è l'**interattività in tempo reale**: l'utente può interagire con la macchina virtuale e con il malware in esecuzione come se fosse sul proprio computer, osservando il suo comportamento passo dopo passo.

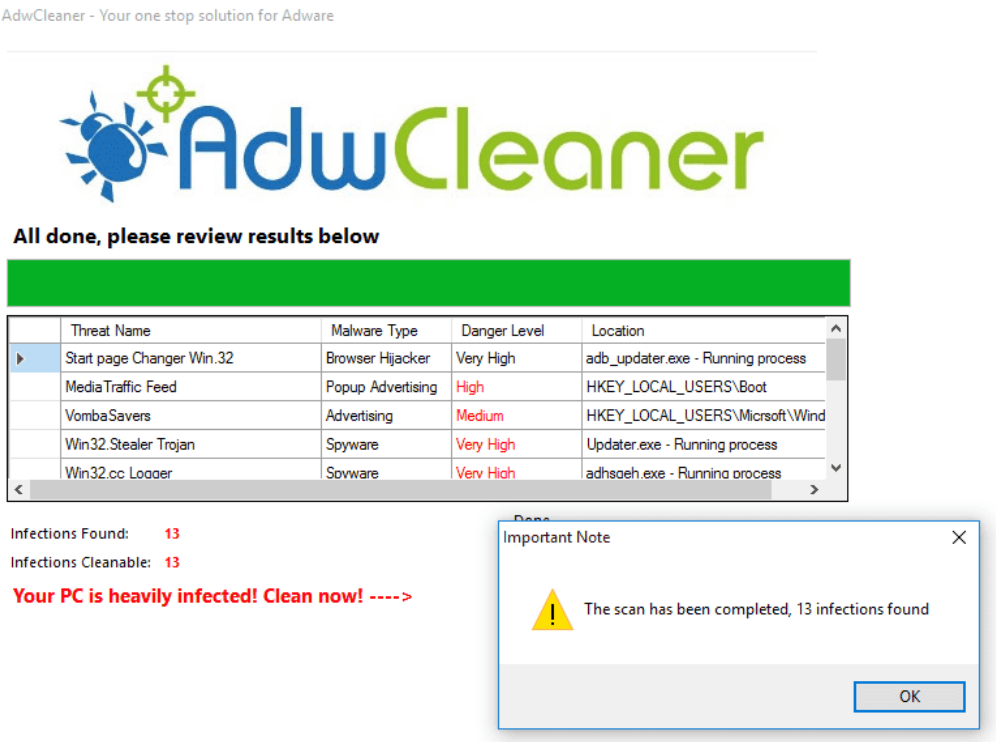
Parte 2: Analisi dinamica su Windows

A questo punto scarichiamo il file anche su una macchina Windows, utilizzando una VM che in un primo momento sarà anche disconnessa totalmente dalla rete, per evitare quanto più possibile rischi di compromissione del sistema principale.

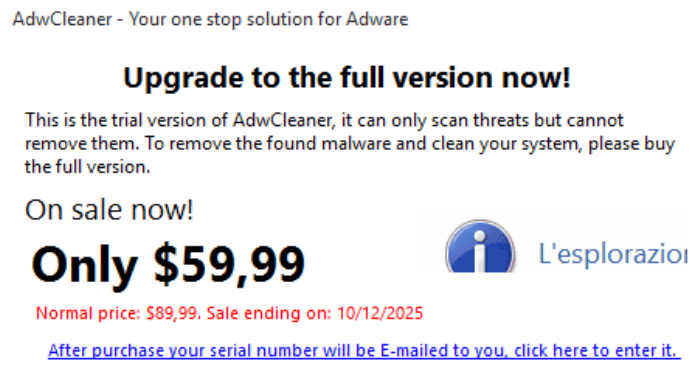
Una volta scaricato “l’antivirus” lo avviamo, lasciando in background `Procmon` per indagare tutte le modifiche che cercherà di mettere in atto sul nostro Pc.



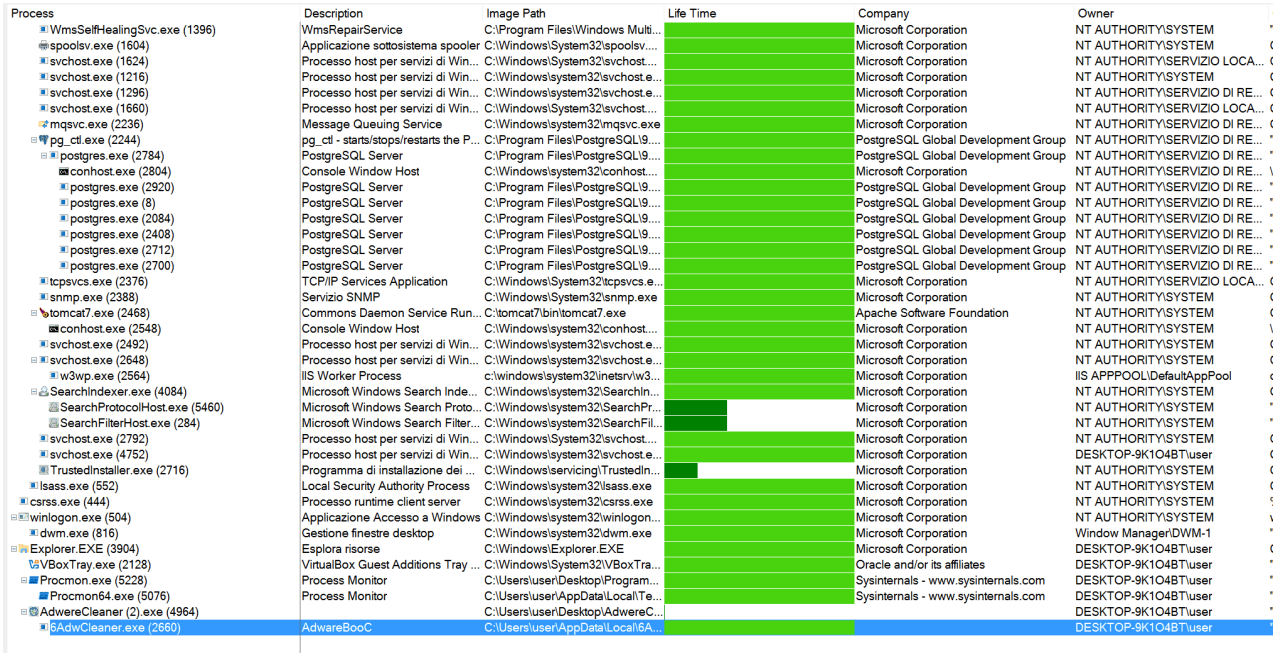
Il programma si presente come una soluzione per le pubblicità e i popup che si generano per la presenza di adware.



Secondo lo scan sono presenti **13 infezioni** che però sono ripulibili da quest’ultimo alla modifica cifra di 59,99$ ma solo entro le prossime 24 ore.

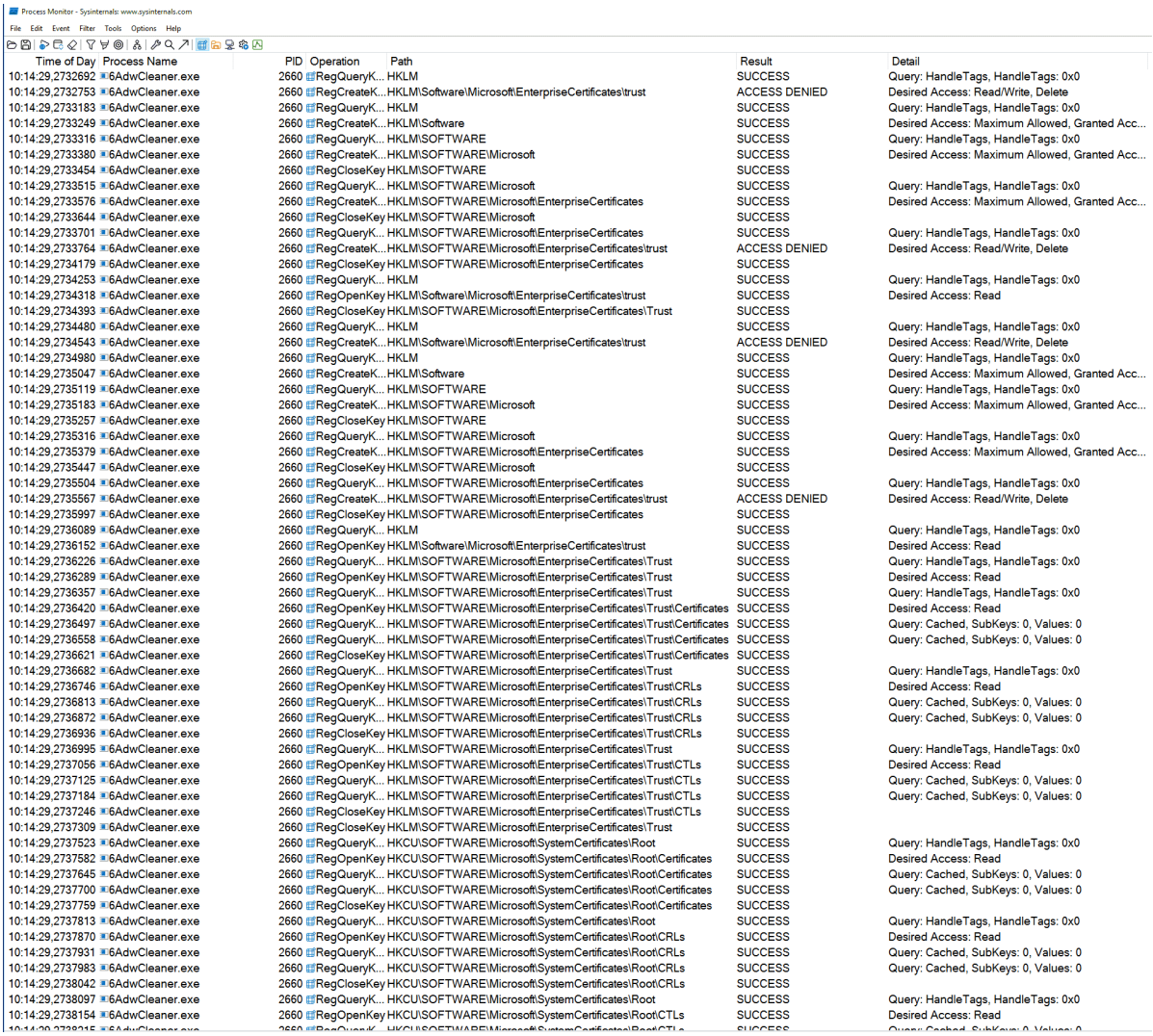


Analizzando il “process tree” è possibile vedere che tra tutti i processi attivi sulla macchina, l’Adwerecleaner (chiamato `6AdwCleaner`) tra i processi è l’unico che non ha un nome specificato nella colonna della “Company”.



Process	Description	Image Path	Life Time	Company	Owner
WmsSelfHealingSvc.exe (1396)	WmsRepairService	C:\Program Files\Windows Multi...		Microsoft Corporation	NT AUTHORITY\SYSTEM
spoolsv.exe (1604)	Applicazione sottosistema spooler	C:\Windows\System32\spoolsv....		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (1624)	Processo host per servizi di Win...	C:\Windows\System32\svchost....		Microsoft Corporation	NT AUTHORITY\SERVIZIO LOCA...
svchost.exe (1216)	Processo host per servizi di Win...	C:\Windows\system32\svchost.e...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (1296)	Processo host per servizi di Win...	C:\Windows\system32\svchost.e...		Microsoft Corporation	NT AUTHORITY\SERVIZIO DI RE...
svchost.exe (1660)	Processo host per servizi di Win...	C:\Windows\System32\svchost....		Microsoft Corporation	NT AUTHORITY\SERVIZIO LOCA...
mqsvc.exe (2236)	Message Queuing Service	C:\Windows\system32\mqsvc.exe		Microsoft Corporation	NT AUTHORITY\SERVIZIO DI RE...
pg_ctl.exe (2244)	pg_ctl - starts/stops/restarts the P...	C:\Program Files\PostgreSQL\9....		PostgreSQL Global Development Group	NT AUTHORITY\SERVIZIO DI RE...
postgres.exe (2784)	PostgreSQL Server	C:\Program Files\PostgreSQL\9....		PostgreSQL Global Development Group	NT AUTHORITY\SERVIZIO DI RE...
conhost.exe (2804)	Console Window Host	C:\Windows\system32\conhost....		Microsoft Corporation	NT AUTHORITY\SERVIZIO DI RE...
postgres.exe (2920)	PostgreSQL Server	C:\Program Files\PostgreSQL\9....		PostgreSQL Global Development Group	NT AUTHORITY\SERVIZIO DI RE...
postgres.exe (8)	PostgreSQL Server	C:\Program Files\PostgreSQL\9....		PostgreSQL Global Development Group	NT AUTHORITY\SERVIZIO DI RE...
postgres.exe (2084)	PostgreSQL Server	C:\Program Files\PostgreSQL\9....		PostgreSQL Global Development Group	NT AUTHORITY\SERVIZIO DI RE...
postgres.exe (2408)	PostgreSQL Server	C:\Program Files\PostgreSQL\9....		PostgreSQL Global Development Group	NT AUTHORITY\SERVIZIO DI RE...
postgres.exe (2712)	PostgreSQL Server	C:\Program Files\PostgreSQL\9....		PostgreSQL Global Development Group	NT AUTHORITY\SERVIZIO DI RE...
postgres.exe (2700)	PostgreSQL Server	C:\Program Files\PostgreSQL\9....		PostgreSQL Global Development Group	NT AUTHORITY\SERVIZIO DI RE...
tcpsvcs.exe (2376)	TCP/IP Services Application	C:\Windows\System32\tcpsvcs.e...		Microsoft Corporation	NT AUTHORITY\SERVIZIO LOCA...
snmp.exe (2388)	Servizio SNMP	C:\Windows\System32\snmp.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM
tomcat7.exe (2468)	Commons Daemon Service Run...	C:\tomcat7\bin\tomcat7.exe		Apache Software Foundation	NT AUTHORITY\SYSTEM
conhost.exe (2548)	Console Window Host	C:\Windows\system32\conhost....		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (2492)	Processo host per servizi di Win...	C:\Windows\system32\svchost.e...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (2648)	Processo host per servizi di Win...	C:\Windows\system32\svchost.e...		Microsoft Corporation	NT AUTHORITY\SYSTEM
w3wp.exe (2564)	IIS Worker Process	c:\windows\system32\inetsrv\w3...		Microsoft Corporation	IIS APPPOOL\DefaultAppPool
SearchIndexer.exe (4084)	Microsoft Windows Search Inde...	C:\Windows\system32\SearchIn...		Microsoft Corporation	NT AUTHORITY\SYSTEM
SearchProtocolHost.exe (5460)	Microsoft Windows Search Proto...	C:\Windows\system32\SearchPr...		Microsoft Corporation	NT AUTHORITY\SYSTEM
SearchFilterHost.exe (284)	Microsoft Windows Search Filter...	C:\Windows\system32\SearchFil...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (2792)	Processo host per servizi di Win...	C:\Windows\System32\svchost....		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (4752)	Processo host per servizi di Win...	C:\Windows\system32\svchost.e...		Microsoft Corporation	DESKTOP-9K1O4BT\user
TrustedInstaller.exe (2716)	Programma di installazione dei ...	C:\Windows\servicing\TrustedIn...		Microsoft Corporation	NT AUTHORITY\SYSTEM
lsass.exe (552)	Local Security Authority Process	C:\Windows\system32\lsass.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM
csrss.exe (444)	Processo runtime client server	C:\Windows\system32\csrss.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM
winlogon.exe (504)	Applicazione Accesso a Windows	C:\Windows\system32\winlogon...		Microsoft Corporation	NT AUTHORITY\SYSTEM
dwm.exe (816)	Gestione finestre desktop	C:\Windows\system32\dwm.exe		Microsoft Corporation	Window Manager\DWM-1
Explorer.EXE (3904)	Esplora risorse	C:\Windows\Explorer.EXE		Microsoft Corporation	DESKTOP-9K1O4BT\user
VBoxTray.exe (2128)	VirtualBox Guest Additions Tray ...	C:\Windows\System32\VBoxTra...		Oracle and/or its affiliates	DESKTOP-9K1O4BT\user
Procmon.exe (5228)	Process Monitor	C:\Users\user\Desktop\Program...		Sysinternals - www.sysinternals.com	DESKTOP-9K1O4BT\user
Procmon64.exe (5076)	Process Monitor	C:\Users\user\AppData\Local\Te...		Sysinternals - www.sysinternals.com	DESKTOP-9K1O4BT\user
AdwereCleaner (2).exe (4964)		C:\Users\user\Desktop\AdwereC...			DESKTOP-9K1O4BT\user
6AdwCleaner.exe (2660)	AdwareBooC	C:\Users\user\AppData\Local\6A...			DESKTOP-9K1O4BT\user

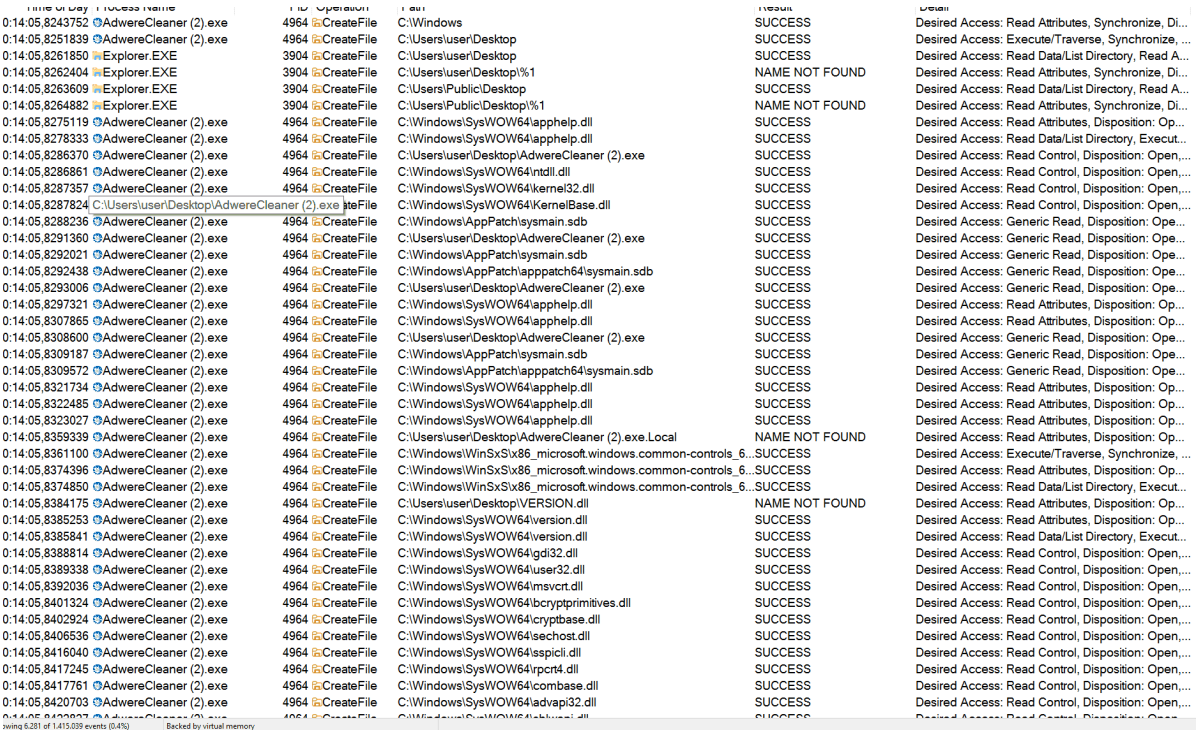
Facendo l’analisi più approfondita sulle operazioni messe in atto da AdwereCleaner è possibile notare una sfilza enorme di apertura chiusura e modifica alle chiavi di registro oltre che, filtrando solo l’operazione di “creazione di cartella”, innumerevoli cartelle create per poter scaricare librerie di collegamento dinamico (ossia i file con estensione `.dll`).



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:14:29,2732692	6AdwCleaner.exe	2660	RegQueryK...	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2732753	6AdwCleaner.exe	2660	RegCreateK...	HKLM\Software\Microsoft\EnterpriseCertificates\trust	ACCESS DENIED	Desired Access: Read/Write, Delete
10:14:29,2733183	6AdwCleaner.exe	2660	RegQueryK...	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2733249	6AdwCleaner.exe	2660	RegCreateK...	HKLM\Software	SUCCESS	Desired Access: Maximum Allowed, Granted Acc...
10:14:29,2733316	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2733380	6AdwCleaner.exe	2660	RegCreateK...	HKLM\SOFTWARE\Microsoft	SUCCESS	Desired Access: Maximum Allowed, Granted Acc...
10:14:29,2733454	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE	SUCCESS	
10:14:29,2733515	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2733576	6AdwCleaner.exe	2660	RegCreateK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates	SUCCESS	Desired Access: Maximum Allowed, Granted Acc...
10:14:29,2733644	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE\Microsoft	SUCCESS	
10:14:29,2733701	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2733764	6AdwCleaner.exe	2660	RegCreateK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\trust	ACCESS DENIED	Desired Access: Read/Write, Delete
10:14:29,2734179	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates	SUCCESS	
10:14:29,2734253	6AdwCleaner.exe	2660	RegQueryK...	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2734318	6AdwCleaner.exe	2660	RegOpenKey	HKLM\Software\Microsoft\EnterpriseCertificates\trust	SUCCESS	Desired Access: Read
10:14:29,2734393	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust	SUCCESS	
10:14:29,2734480	6AdwCleaner.exe	2660	RegQueryK...	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2734543	6AdwCleaner.exe	2660	RegCreateK...	HKLM\Software\Microsoft\EnterpriseCertificates\trust	ACCESS DENIED	Desired Access: Read/Write, Delete
10:14:29,2734980	6AdwCleaner.exe	2660	RegQueryK...	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2735047	6AdwCleaner.exe	2660	RegCreateK...	HKLM\Software	SUCCESS	Desired Access: Maximum Allowed, Granted Acc...
10:14:29,2735119	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2735183	6AdwCleaner.exe	2660	RegCreateK...	HKLM\SOFTWARE\Microsoft	SUCCESS	Desired Access: Maximum Allowed, Granted Acc...
10:14:29,2735257	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE	SUCCESS	
10:14:29,2735316	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2735379	6AdwCleaner.exe	2660	RegCreateK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates	SUCCESS	Desired Access: Maximum Allowed, Granted Acc...
10:14:29,2735447	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE\Microsoft	SUCCESS	
10:14:29,2735504	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2735567	6AdwCleaner.exe	2660	RegCreateK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\trust	ACCESS DENIED	Desired Access: Read/Write, Delete
10:14:29,2735997	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates	SUCCESS	
10:14:29,2736089	6AdwCleaner.exe	2660	RegQueryK...	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2736152	6AdwCleaner.exe	2660	RegOpenKey	HKLM\Software\Microsoft\EnterpriseCertificates\trust	SUCCESS	Desired Access: Read
10:14:29,2736226	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2736289	6AdwCleaner.exe	2660	RegOpenKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust	SUCCESS	Desired Access: Read
10:14:29,2736357	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2736420	6AdwCleaner.exe	2660	RegOpenKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\Certificates	SUCCESS	Desired Access: Read
10:14:29,2736497	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\Certificates	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2736558	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\Certificates	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2736621	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\Certificates	SUCCESS	
10:14:29,2736682	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2736746	6AdwCleaner.exe	2660	RegOpenKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\CRLs	SUCCESS	Desired Access: Read
10:14:29,2736813	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\CRLs	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2736872	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\CRLs	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2736936	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\CRLs	SUCCESS	
10:14:29,2736995	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2737056	6AdwCleaner.exe	2660	RegOpenKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\CTLs	SUCCESS	Desired Access: Read
10:14:29,2737125	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\CTLs	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2737184	6AdwCleaner.exe	2660	RegQueryK...	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\CTLs	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2737246	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust\CTLs	SUCCESS	
10:14:29,2737309	6AdwCleaner.exe	2660	RegCloseKey	HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust	SUCCESS	
10:14:29,2737523	6AdwCleaner.exe	2660	RegQueryK...	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2737582	6AdwCleaner.exe	2660	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root\Certificates	SUCCESS	Desired Access: Read
10:14:29,2737645	6AdwCleaner.exe	2660	RegQueryK...	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root\Certificates	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2737700	6AdwCleaner.exe	2660	RegQueryK...	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root\Certificates	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2737759	6AdwCleaner.exe	2660	RegCloseKey	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root\Certificates	SUCCESS	
10:14:29,2737813	6AdwCleaner.exe	2660	RegQueryK...	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2737870	6AdwCleaner.exe	2660	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root\CRLs	SUCCESS	Desired Access: Read
10:14:29,2737931	6AdwCleaner.exe	2660	RegQueryK...	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root\CRLs	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2737983	6AdwCleaner.exe	2660	RegQueryK...	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root\CRLs	SUCCESS	Query: Cached, SubKeys: 0, Values: 0
10:14:29,2738042	6AdwCleaner.exe	2660	RegCloseKey	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root\CRLs	SUCCESS	
10:14:29,2738097	6AdwCleaner.exe	2660	RegQueryK...	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root	SUCCESS	Query: HandleTags, HandleTags: 0x0
10:14:29,2738154	6AdwCleaner.exe	2660	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemCertificates\Root\CTLs	SUCCESS	Desired Access: Read



Time of Day	Process Name	PID	Operation	Path	Result	Detail
0:14:05,8243752	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows	SUCCESS	Desired Access: Read Attributes, Synchronize, Di...
0:14:05,8251839	AdwereCleaner (2).exe	4964	CreateFile	C:\Users\user\Desktop	SUCCESS	Desired Access: Execute/Traverse, Synchronize, ...
0:14:05,8261850	Explorer.EXE	3904	CreateFile	C:\Users\user\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Read A...
0:14:05,8262404	Explorer.EXE	3904	CreateFile	C:\Users\user\Desktop\%1	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Di...
0:14:05,8263609	Explorer.EXE	3904	CreateFile	C:\Users\Public\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Read A...
0:14:05,8264882	Explorer.EXE	3904	CreateFile	C:\Users\Public\Desktop\%1	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Di...
0:14:05,8275119	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8278333	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Data/List Directory, Execut...
0:14:05,8286370	AdwereCleaner (2).exe	4964	CreateFile	C:\Users\user\Desktop\AdwereCleaner (2).exe	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8286861	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8287357	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8287824	C:\Users\user\Desktop\AdwereCleaner (2).exe	teFile		C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8288236	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
0:14:05,8291360	AdwereCleaner (2).exe	4964	CreateFile	C:\Users\user\Desktop\AdwereCleaner (2).exe	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
0:14:05,8292021	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
0:14:05,8292438	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\AppPatch\apppatch64\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
0:14:05,8293006	AdwereCleaner (2).exe	4964	CreateFile	C:\Users\user\Desktop\AdwereCleaner (2).exe	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
0:14:05,8297321	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8307865	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8308600	AdwereCleaner (2).exe	4964	CreateFile	C:\Users\user\Desktop\AdwereCleaner (2).exe	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
0:14:05,8309187	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
0:14:05,8309572	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\AppPatch\apppatch64\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
0:14:05,8321734	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8322485	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8323027	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8359339	AdwereCleaner (2).exe	4964	CreateFile	C:\Users\user\Desktop\AdwereCleaner (2).exe.Local	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8361100	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6...	SUCCESS	Desired Access: Execute/Traverse, Synchronize, ...
0:14:05,8374396	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6...	SUCCESS	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8374850	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6...	SUCCESS	Desired Access: Read Data/List Directory, Execut...
0:14:05,8384175	AdwereCleaner (2).exe	4964	CreateFile	C:\Users\user\Desktop\VERSION.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8385253	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\version.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Op...
0:14:05,8385841	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\version.dll	SUCCESS	Desired Access: Read Data/List Directory, Execut...
0:14:05,8388814	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8389338	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\user32.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8392036	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8401324	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8402924	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8406536	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8416040	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8417245	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8417761	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\combase.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...
0:14:05,8420703	AdwereCleaner (2).exe	4964	CreateFile	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Desired Access: Read Control, Disposition: Open,...

xwing 6,281 of 1,415,039 events (0.4%) Backed by virtual memory

Parte 3: analisi del traffico con Wireshark

A questo punto poi abbiamo anche provato ad riattivare la rete per fare l'analisi del traffico tramite Wireshark durante uno `scan` e si possono vedere due tentativi di collegamento, uno tramite la porta `443` all'indirizzo Ipv4 `48.209.108.37` mentre il secondo tramite la porta `80` all'indirizzo Ipv4 `184.26.9.132`.

23 31.547080	48.209.108.37	192.168.50.11	TCP	60 443 → 49825 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
24 31.547222	192.168.50.11	48.209.108.37	TCP	54 49825 → 443 [ACK] Seq=1 Ack=2 Win=63998 Len=0
25 31.548442	192.168.50.11	48.209.108.37	TLSv1.2	85 Encrypted Alert
26 31.548489	192.168.50.11	48.209.108.37	TCP	54 49825 → 443 [FIN, ACK] Seq=32 Ack=2 Win=63998 Len=0
27 31.548547	48.209.108.37	192.168.50.11	TCP	60 443 → 49825 [ACK] Seq=2 Ack=32 Win=65535 Len=0
28 31.548680	48.209.108.37	192.168.50.11	TCP	60 443 → 49825 [ACK] Seq=2 Ack=33 Win=65535 Len=0
29 42.005533	192.168.50.11	184.26.9.132	TCP	54 49834 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63844 Len=0
30 42.005752	184.26.9.132	192.168.50.11	TCP	60 80 → 49834 [ACK] Seq=1 Ack=2 Win=65535 Len=0
31 42.022297	184.26.9.132	192.168.50.11	TCP	60 80 → 49834 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
32 42.022347	192.168.50.11	184.26.9.132	TCP	54 49834 → 80 [ACK] Seq=2 Ack=2 Win=63844 Len=0
33 102.297736	20.191.45.158	192.168.50.11	TLSv1.2	131 Application Data, Encrypted Alert
34 102.297736	20.191.45.158	192.168.50.11	TCP	60 443 → 49826 [FIN, ACK] Seq=78 Ack=1 Win=65535 Len=0
35 102.297888	192.168.50.11	20.191.45.158	TCP	54 49826 → 443 [ACK] Seq=1 Ack=79 Win=65535 Len=0
36 102.298137	192.168.50.11	20.191.45.158	TCP	54 49826 → 443 [FIN, ACK] Seq=1 Ack=79 Win=65535 Len=0
37 102.298371	20.191.45.158	192.168.50.11	TCP	60 443 → 49826 [ACK] Seq=79 Ack=2 Win=65535 Len=0
38 103.053126	52.113.196.254	192.168.50.11	TCP	60 443 → 49871 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
39 103.806193	79.140.81.153	192.168.50.11	TLSv1.2	85 Encrypted Alert
40 103.806193	79.140.81.153	192.168.50.11	TCP	60 443 → 49829 [FIN, ACK] Seq=32 Ack=1 Win=65535 Len=0
41 103.806278	192.168.50.11	79.140.81.153	TCP	54 49829 → 443 [ACK] Seq=1 Ack=33 Win=65535 Len=0
42 105.406844	204.79.197.222	192.168.50.11	TCP	60 443 → 49830 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
43 106.549205	13.107.3.254	192.168.50.11	TCP	60 443 → 49872 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
44 106.976549	PCSSystemtec_96:c2:…	52:55:c0:a8:32:01	ARP	42 Who has 192.168.50.1? Tell 192.168.50.11
45 106.976695	52:55:c0:a8:32:01	PCSSystemtec_96:c2:…	ARP	64 192.168.50.1 is at 52:55:c0:a8:32:01
46 107.033761	70.153.80.24	192.168.50.11	TCP	60 443 → 49876 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
47 108.263638	150.171.28.254	192.168.50.11	TCP	60 443 → 49874 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
48 109.852826	150.171.73.254	192.168.50.11	TCP	60 443 → 49875 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
49 124.311597	192.168.50.11	4.207.247.137	TLSv1.2	153 Application Data
50 124.311854	4.207.247.137	192.168.50.11	TCP	60 443 → 49797 [ACK] Seq=1 Ack=100 Win=65535 Len=0
51 124.358880	4.207.247.137	192.168.50.11	TLSv1.2	223 Application Data
52 124.407998	192.168.50.11	4.207.247.137	TCP	54 49797 → 443 [ACK] Seq=100 Ack=170 Win=63792 Len=0

> **Wireshark**
>
> **Wireshark** è il più popolare e diffuso **analizzatore di protocollo di rete** (chiamato anche *sniffer*).
>
> Wireshark intercetta il **traffico dati** che passa attraverso un'interfaccia di rete (come una scheda Wi-Fi o Ethernet) e lo acquisisce. Permette di "aprire" e decodificare ogni singolo **pacchetto di dati** in un formato leggibile e analizzabile dall'utente, esponendo i dettagli di protocolli come TCP, IP, HTTP, ecc.

Conclusioni

Il file eseguibile, seppur apparentemente **legittimo** dal suo **aspetto**, si è rivelato infine essere estremamente **malevolo** nelle intenzioni, con lo scopo di rubare dati e potenzialmente chiedere un riscatto alla vittima.

L’analisi statica e soprattutto quella dinamica hanno messo in mostra l’enorme attività che si celava dietro questo finto `adware scan,` con tutte le modifiche messe in atto nel sistema per non essere scoperto, oltre che nel tentativo di comunicare con una macchina esterna i dati esfiltrati.

Gli innumerevoli IoC presenti nel report suggeriscono che, in caso di compromissione di un sistema, con questo malware sarebbe meglio **isolare il computer dalla rete** oltre che disinstallare il file in maniera tempestiva.