

# 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:

The screenshot shows the Virustotal analysis interface for the file 51290129ccccca38c6e3b444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc. The main summary indicates 53/70 security vendors flagged the file as malicious. Below this, detailed information includes the file name (AdwereCleaner.exe), size (190.82 KB), last analysis date (1 month ago), and a file icon. A list of detected threat categories follows: peste, invalid-signature, runtime-modules, direct-cpu-clock-access, detect-debug-environment, executes-dropped-file, revoked-cert, checks-network-adapters, checks-user-input, persistence, signed, nsis, and overlay. The interface also features tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 21+ entries). A prominent green bar encourages users to join the community. Below the main summary, there's a table titled "Security vendors' analysis" listing various vendor names and their corresponding detection results. The table includes columns for vendor name, threat type, and detection status. Some entries include additional context like file hashes or specific detection details.

Security vendor	Threat type	Detection status
AhnLab-V3	Dropper/Win32.Dapato.R137988	Alibaba (Hoax/MSIL/Porcupine.e66e0e97)
AliCloud	Trojan:MSIL/Hoax.Akgpp	AntiAVL (HackTool[Hoax].MSIL.Agent)
Arcabit	Trojan.Mint.Porcupine.ED5D10	Arctic Wolf (Unsafe)
Avast	Win32:FakeAV-FLW [Trj]	AVG (Win32-FakeAV-FLW [Trj])
Avira (no cloud)	JOKE/Agent.rlham	BitDefender (Gen:Heur.Mint.Porcupine.luZ@bOy2NApig)
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX (Exe.trojan.fakeav)
Cynet	Malicious (score: 99)	Deepinstinct (MALICIOUS)
DrWeb	Trojan.FakeAV.17850	Elastic (Malicious (high Confidence))
Emsisoft	Gen:Heur.Mint.Porcupine.luZ@bOy2NApig...	eScan (Gen:Heur.Mint.Porcupine.luZ@bOy2NApig)
ESET-NOD32	MSIL/Hoax.Agent.NBD	Fortinet (W32/Agent.GDCItr)
GData	Gen:Heur.Mint.Porcupine.luZ@bOy2NApig	Google (Detected)
Gridinsoft (no cloud)	Fake.Win32.Gen.vlli	Huorong (Rogue/FakeAV.j)
Ikarus	Trojan.Fakeav	K7AntiVirus (Trojan (005863041))
K7GW	Trojan (005863041)	Kaspersky (Trojan-FakeAV.Win32.Agent.gdc)
Kingssoft	Win32.Trojan-FakeAV.Agent.scd	Lionic (Trojan.Win32.Agent.ylc)

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 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**.

**ANYRUN**  
INTERACTIVE MALWARE ANALYSIS

General Behavior MalConf Static information Video Screenshots System events Network  

**General Info** 

File name: adwcleaner.exe  
Full analysis: <https://app.any.run/tasks/eb21dc4b-6c0a-47b3-836a-127d9a302bae>  
Verdict: **Malicious activity**  
Threats: **Stealer**

Stealers are a group of malicious software that are intended for gaining unauthorized access to users' information and transferring it to the attacker. The stealer malware category includes various types of programs that focus on their particular kind of data, including files, passwords, and cryptocurrency. Stealers are capable of spying on their targets by recording their keystrokes and taking screenshots. This type of malware is primarily distributed as part of phishing campaigns.

Analysis date: May 31, 2025 at 17:17:25  
OS: Windows 10 Professional (build: 19044, 64 bit)  
Tags:    
Indicators:   
MIME: application/vnd.microsoft.portable-executable  
File info: PE32 executable (console) Intel 80386, for MS Windows, UPX compressed, 3 sections  
MD5: 177F7C43CD99F26FE1EC73C9CBA98408  
SHA1: 8A2148DB3C4599B9B8E67E6834FA2C0CF78FC0DD  
SHA256: 4D428B3F1846A253FB18EF489EEFFE43DB25DA249A3424066B74D808F2587C81  
SSDEEP: 98304:zQRbhMmvWvODLPgnMPWwq61NjKEM0xfDzKJ6+ZF7D5AKxbImRZufZxZ+h3hVVWQ:lkdcjeVQ/iXiBQKXm5owAA

 ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

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

attivano:

## Behavior activities

Add for printing ▾

MALICIOUS	SUSPICIOUS	INFO
<p>Steals credentials from Web Browsers</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>	<p>The process verifies whether the antivirus software is installed</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>	<p>The sample compiled with english language support</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li><li>MBsetup-adwc.adwc100.exe (PID: 1680)</li><li>MBAMInstallerService.exe (PID: 3420)</li></ul>
<p>Changes the autorun value in the registry</p> <ul style="list-style-type: none"><li>netsh.exe (PID: 5956)</li></ul>	<p>Reads the BIOS version</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>	<p>Checks supported languages</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li><li>OfficeClickToRun.exe (PID: 1328)</li><li>SearchApp.exe (PID: 1600)</li><li>StartMenuExperienceHost.exe (PID: 5260)</li></ul>
	<p>Uses NETSH.EXE to change the status of the firewall</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>	<p>Reads the computer name</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li><li>OfficeClickToRun.exe (PID: 1328)</li><li>StartMenuExperienceHost.exe (PID: 5260)</li><li>SearchApp.exe (PID: 1600)</li></ul>
	<p>Modifies hosts file to alter network resolution</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>	<p>Reads the software policy settings</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>
	<p>Searches for installed software</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>	<p>UPX packer has been detected</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>
	<p>Suspicious use of NETSH.EXE</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>	<p>Checks proxy server information</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li><li>OfficeClickToRun.exe (PID: 1328)</li></ul>
	<p>Process uses IPCONFIG to clear DNS cache</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>	<p>Create files in a temporary directory</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>
	<p>Reads security settings of Internet Explorer</p> <ul style="list-style-type: none"><li>StartMenuExperienceHost.exe (PID: 5260)</li></ul>	<p>Executes as Windows Service</p> <ul style="list-style-type: none"><li>OfficeClickToRun.exe (PID: 1328)</li></ul>
	<p>Reads the date of Windows installation</p> <ul style="list-style-type: none"><li>StartMenuExperienceHost.exe (PID: 5260)</li></ul>	<p>Uses BITSADMIN.EXE</p> <ul style="list-style-type: none"><li>adwcleaner.exe (PID: 5968)</li></ul>
	<p>Executable content was dropped or overwritten</p> <ul style="list-style-type: none"><li>MBsetup-adwc.adwc100.exe (PID: 1680)</li><li>adwcleaner.exe (PID: 5968)</li></ul>	<p>Reads the machine GUID from the registry</p> <ul style="list-style-type: none"><li>OfficeClickToRun.exe (PID: 1328)</li><li>adwcleaner.exe (PID: 5968)</li></ul>
	<p>Executes as Windows Service</p> <ul style="list-style-type: none"><li>MBAMInstallerService.exe (PID: 3420)</li></ul>	<p>Reads Microsoft Office registry keys</p> <ul style="list-style-type: none"><li>OfficeClickToRun.exe (PID: 1328)</li></ul>
		<p>Launch of the file from Registry key</p> <ul style="list-style-type: none"><li>netsh.exe (PID: 5956)</li></ul>
		<p>Disables trace logs</p> <ul style="list-style-type: none"><li>netsh.exe (PID: 8140)</li></ul>
		<p>Process checks computer location settings</p> <ul style="list-style-type: none"><li>StartMenuExperienceHost.exe (PID: 5260)</li></ul>

 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.

## MITRE ATT&CK Matrix

Tactics 6 | Techniques 16 | Events 209

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery
	System Services (1/3)	BITS Jobs 1	Boot or Logon Autostart Execution (1/14)	BITS Jobs 1	Unsecured Credentials (1/8)	Query Registry 54 21
	Service Execution 1 1	Boot or Logon Autostart Execution (1/14)	Registry Run Keys / Startup Folder 50	File and Directory Permissions Modification (1/2)	Credentials In Files 2	System Network Configuration Discovery (1/2)
		Registry Run Keys / Startup Folder 50		Windows File and Directory Permissions Modification 1	Credentials from Password Stores (1/6)	Internet Connection Discovery 1
				Virtualization/Sandbox Evasion (2/3)	Credentials from Web Browsers 2	System Information Discovery 2 10
				System Checks 1		Virtualization/Sandbox Evasion (2/3)
				Time Based Checks 1		System Checks 1
				Impair Defenses (2/12)		Time Based Checks 1
				Disable Windows Event Logging 1		Software Discovery (1/2)
				Disable or Modify System Firewall 1		Security Software Discovery 4
						Backup Software Discovery
						System Location Discovery (0/1) 1

### 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 presenta come una soluzione per le pubblicità e i popup che si generano per la presenza di adware.

A screenshot of the AdwCleaner application window showing the results of a scan. The title bar reads "AdwCleaner - Your one stop solution for Adware". The main area features the AdwCleaner logo and the text "All done, please review results below". Below this is a table listing the detected threats. The table has columns for Threat Name, Malware Type, Danger Level, and Location. The threats listed are: Start page Changer Win.32 (Browser Hijacker, Very High, adb\_updater.exe - Running process), MediaTraffic Feed (Popup Advertising, High, HKEY\_LOCAL\_USERS\Boot), VombaSavers (Advertising, Medium, HKEY\_LOCAL\_USERS\Microsoft\Wind), Win32.Stealer.Trojan (Spyware, Very High, Updater.exe - Running process), and Win32.cc.Lodder (Spyware, Very High, adhsoeh.exe - Running process). At the bottom left, it says "Infections Found: 13" and "Infections Cleanable: 13". A red warning message "Your PC is heavily infected! Clean now! ----&gt;" is displayed. A modal dialog box titled "Important Note" shows a yellow exclamation mark icon and the text "The scan has been completed, 13 infections found". An "OK" button is at the bottom right of the dialog.

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.

## Upgrade to the full version now!

This is the trial version of AdwCleaner, it can only scan threats but cannot remove them. To remove the found malware and clean your system, please buy the full version.

On sale now!

**Only \$59,99**



L'esplorazio

Normal price: \$89,99. Sale ending on: 10/12/2025

[After purchase your serial number will be E-mailed to you, click here to enter it.](#)

Analizzando il “process tree” è possibile vedere che tra tutti i processi attivi sulla macchina, l’Adwreecleaner (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... Applicazione sottosistema spooler		Microsoft Corporation	NT AUTHORITY\SYSTEM
spoolsv.exe (1604)		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...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (1296)	Processo host per servizi di Win...	C:\Windows\System32\svchost...		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...
mgsvc.exe (2236)	Message Queuing Service	C:\Windows\system32\mgsvc.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...		Microsoft Corporation	NT AUTHORITY\SYSTEM
* svchost.exe (2648)	Processo host per servizi di Win...	C:\Windows\System32\svchost...		Microsoft Corporation	NT AUTHORITY\SYSTEM
* w3wp.exe (2564)	IIS Worker Process	c:\windows\system32\inetsrv\w3...		Microsoft Corporation	IIS APPPOOL\DefaultAppPool
* SearchIndexer.exe (4048)	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...		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\DWIM-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 Corporation	DESKTOP-9K1O4BT\user
* Procmon64.exe (5076)	Process Monitor	C:\Users\user\Desktop\Program...		Sysinternals - www.sysinternals.com	DESKTOP-9K1O4BT\user
* AdwreCleaner (2).exe (4964)	Process Monitor	C:\Users\user\AppData\Local\Te...		Sysinternals - www.sysinternals.com	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 AdwreCleaner 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).

User	Process Name	File Operation	Path	Result	Detail
04:15:05:8243752	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows	SUCCESS	Desired Access: Read Attributes, Synchronize, Di...
04:15:05:8251830	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Users\user\Desktop	SUCCESS	Desired Access: Execute/Traverse, Synchronize, ...
04:15:05:8261850	Explorer.EXE	3904 ↗CreateFile	C:\Users\user\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Read A...
04:15:05:8262404	Explorer.EXE	3904 ↗CreateFile	C:\Users\user\Desktop\%1	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Di...
04:15:05:8263609	Explorer.EXE	3904 ↗CreateFile	C:\Users\Public\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Read A...
04:15:05:8264682	Explorer.EXE	3904 ↗CreateFile	C:\Users\Public\Desktop\%1	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Di...
04:15:05:8275119	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Op...
04:15:05:8278333	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Data/List Directory, Execut...
04:15:05:8286370	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Users\user\Desktop\AdwreCleaner (2).exe	SUCCESS	Desired Access: Read Control, Disposition: Open...
04:15:05:8286861	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\ndl.dll	SUCCESS	Desired Access: Read Control, Disposition: Open...
04:15:05:8287357	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Desired Access: Read Control, Disposition: Open...
04:15:05:8287824	C:\Users\user\Desktop\AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\kernelbase.dll	SUCCESS	Desired Access: Read Control, Disposition: Open...
04:15:05:8288236	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
04:15:05:8291360	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Users\user\Desktop\AdwreCleaner (2).exe	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
04:15:05:8292021	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
04:15:05:8292438	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\AppPatch\appatch64\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
04:15:05:8293006	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Users\user\Desktop\AdwreCleaner (2).exe	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
04:15:05:8297321	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
04:15:05:8307865	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8308600	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Users\user\Desktop\AdwreCleaner (2).exe	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8309187	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
04:15:05:8309572	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\AppPatch\appatch64\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
04:15:05:8321734	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8322482	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8323207	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8359339	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Users\user\Desktop\AdwreCleaner (2).exe	Local NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Ope...
04:15:05:8361100	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6...	SUCCESS	Desired Access: Execute/Traverse, Synchronize, ...
04:15:05:8374396	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6...	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8374850	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6...	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8381475	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Users\user\Desktop\VERSION.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Ope...
04:15:05:8385253	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\version.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8385841	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\version.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8388814	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8389338	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\user32.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8392036	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\msvcr.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8401324	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8402924	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8406536	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8416040	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\spicid.dll	SUCCESS	Desired Access: Read Attributes, Disposition: O...
04:15:05:8417245	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Desired Access: Read Control, Disposition: Open...
04:15:05:8417761	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\combase.dll	SUCCESS	Desired Access: Read Control, Disposition: Open...
04:15:05:8420703	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\adapi32.dll	SUCCESS	Desired Access: Read Control, Disposition: Open...
04:15:05:8422927	AdwreCleaner (2).exe	4964 ↗CreateFile	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Desired Access: Read Control, Disposition: Open...

## 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'indirizzoIpv4 48.209.108.37 mentre il secondo tramite la porta 80 all'indirizzoIpv4 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	192.168.50.11	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.