

## Report Malware Analysis

Nella seguente immagine utilizziamo il tool VirusTotal per scansionare ed analizzare il file Adwere.exe, in cui possiamo notare come 55 Servizi di Antivirus su 71 rilevano il file come potenzialmente dannoso:

55  
/ 71

Community Score -219

55/71 security vendors flagged this file as malicious

Reanalyze Similar More

51290129ccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc

AdwereCleaner.exe

Size 190.82 KB

Last Analysis Date 6 days ago

EXE

peexe persistence checks-user-input runtime-modules overlay revoked-cert direct-cpu-clock-access signed nsis executes-dropped-file detect-debug-environment checks-network-adapters invalid-signature

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 21+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	248aadd395ffa7ffb1670392a9398454
SHA-1	c53c140bbdb556fca33bc7f9b2e44e9061ea3e5
SHA-256	51290129ccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc
Vhash	015056655d5c05709043z8003d7z47z62z3f03dz
Authentihash	8eb8f3a6371a77e2b5002de83a5955d4d5fb7f2cdb7d8642138bb20d243be578
Imphash	e160ef8e55bb9d162da4e266afd9eef3
Rich PE header hash	ecf81400e80e4d5ebc5ac2f7c2aace3
SSDEEP	3072:15TDpNFVbxD5XJFFGhcBR1WLZ37p73G8Wn7GIDOG+ELqdSxo5XtIzjnvxRJgghaR:157TcfFPB6B3GL7g+me5aZjn5VI9T/
TLSH	T17B1412524AF05AFFFB4384712AFDE1B9E7B7828C5274A9974B148E323B440D74F8611A
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
TrID	NSIS - Nullsoft Scriptable Install System (92.7%)   Win32 Executable MS Visual C++ (generic) (3.4%)   Win64 Executable (generic) (1.1%)   Win32 Dynamic Link Library (ge...
DetectItEasy	PE32   Installer: Nullsoft Scriptable Install System (3.0a2) [zlib,solid]   Compiler: Microsoft Visual C/C++ [12.20.9044] [C]   Linker: Microsoft Linker (6.0)   Tool: Visual St...
Magika	PEBIN
File size	190.82 KB (195400 bytes)
F-PROT packer	NSIS, appended

History

Creation Time	2013-12-25 05:01:41 UTC
Signature Date	2015-02-04 20:05:00 UTC
First Seen In The Wild	2022-04-24 06:21:31 UTC
First Submission	2015-02-11 15:48:03 UTC
Last Submission	2024-10-24 11:17:43 UTC
Last Analysis	2024-10-21 14:02:44 UTC

Names

AdwereCleaner.exe  
Endermanch@FakeAdwCleaner.exe  
FakeAdwCleaner.exe  
fakeadwcleaner.exe  
AdwCleaner.exe  
623786656.exe

Dopo aver scansionato ed analizzato il file malevolo Adwere.exe con VirusTotal, per l’analisi statica, utilizziamo il tool Sandbox Cuckoo, per l’analisi dinamica, in cui possiamo notare come il Malware, può effettuare:

- **Privilege Escalation**
- **Acquire Screenshot**
- **Modificare il registro di Sistema**
- **Manipolare file e Token di Sistema**

Summary

File AdwereCleaner.exe

Summary

Download

Resubmit sample

Size

190.8KB

Type

PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

MD5

248aadd395ffa7ffb1678392a9398454

SHA1

c53c140bbdeb556fca33bc7f9b2e44e9061ea3e5

SHA256

51290129cccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc

SHA512

Show SHA512

CRC32

12441207

ssdeep

None

Yara

escalate\_priv - Escalade privileges

screenshot - Take screenshot

win\_registry - Affect system registries

win\_token - Affect system token

win\_private\_profile - Affect private profile

win\_files\_operation - Affect private profile

Tramite YARA possiamo vedere nel dettaglio le azioni che esegue il Malware Adwere.exe all’interno del Sistema

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
FILE	Oct. 28, 2024, 10:32 a.m.	Oct. 28, 2024, 10:35 a.m.	177 seconds	internet	Show Analyzer Log Show Cuckoo Log

Signatures

Yara rules detected for file (6 events)

description	Escalade privileges	rule	escalate_priv
description	Take screenshot	rule	screenshot
description	Affect system registries	rule	win_registry
description	Affect system token	rule	win_token
description	Affect private profile	rule	win_private_profile
description	Affect private profile	rule	win_files_operation

Successivamente alla scansione ed analisi statica e dinamica, con i relativi tool illustrati in precedenza, utilizziamo il tool CFF Explorer per analizzare gli header e le importazioni delle librerie e sul funzionamento ed azioni che il Malware, esegue nel Sistema:

CFF Explorer VIII - [AdwareCleaner.exe]

File Settings ?

File: AdwareCleaner.exe

Dos Header

Nt Headers

File Header

Optional Header

Data Directories [x]

Section Headers [x]

Import Directory

Resource Directory

Address Converter

Dependency Walker

Hex Editor

Identifier

Import Adder

Quick Disassembler

Rebuilder

Resource Editor

UPX Utility

AdwareCleaner.exe

Property	Value
File Name	C:\Users\flare\Desktop\Malware\rogues\AdwareCleaner.exe
File Type	Portable Executable 32
File Info	Nullsoft PiMP Stub -> SFX
File Size	190.82 KB (195400 bytes)
PE Size	75.50 KB (77312 bytes)
Created	Wednesday 09 October 2024, 11.37.27
Modified	Wednesday 09 October 2024, 11.37.27
Accessed	Monday 28 October 2024, 10.05.08
MD5	248AADD395FFA7FFB1670392A9398454
SHA-1	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5

Property	Value
Empty	No additional info available

Andando nella scheda Import Directory di CFF Explorer, possiamo vedere i nomi delle librerie più conosciute come:

- **KERNEL32.dll**
- **USER32.dll**
- **GDI32.dll**

**Le quali hanno la funzione principale di gestire le funzioni di sistema e dell'interfaccia dell'utente**

Quindi possiamo vedere dalle seguenti immagini come il Malware, agisca principalmente e direttamente su:

- **KERNEL32.dll**
- **USER32.dll**

CFF Explorer VIII - [AdwareCleaner.exe]

File Settings ?

AdwareCleaner.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	61	000075C4	00000000	00000000	00007C12	00007060
USER32.dll	63	000076D8	00000000	00000000	00008022	00007174
GDI32.dll	8	000075A0	00000000	00000000	000080B4	0000703C
SHELL32.dll	6	000076BC	00000000	00000000	00008140	00007158
ADVAPI32.dll	9	00007564	00000000	00000000	000081E2	00007000
COMCTL32.dll	4	0000758C	00000000	00000000	0000822E	00007028
ole32.dll	4	000077E8	00000000	00000000	00008282	00007284
VERSION.dll	3	000077D8	00000000	00000000	000082CE	00007274

File: AdwareCleaner.exe

- Dos Header
- Nt Headers
  - File Header
  - Optional Header
    - Data Directories [x]
- Section Headers [x]
- Import Directory**
- Resource Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

## **Il Malware Adwere.exe agisce sulle voci descritte di seguito:**

### Azioni di Adwere.exe sui File System

- **MoveFileA**
- **CopyFileA**
- **CreateFileA**
- **RemoveDirectoryA**
- **SetFileAttributesA**
- **GetTempFileNameA**

### Azioni di Adwere.exe sui Processi ed i Threads

- **CreateThread**
- **CreateProcessA**
- **ExitProcess**
- **GetCurrentProcess**

### Azioni di Adwere.exe sull'Ambiente di Sistema

- **SetEnvironmentVariableA**
- **GetWindowsDirectoryA**
- **GetCurrentProcess**
- **GetTempPathA**

### Azioni di Adwere.exe sulle Librerie e sulla Memoria

- **LoadLibraryA**
- **FreeLibrary**

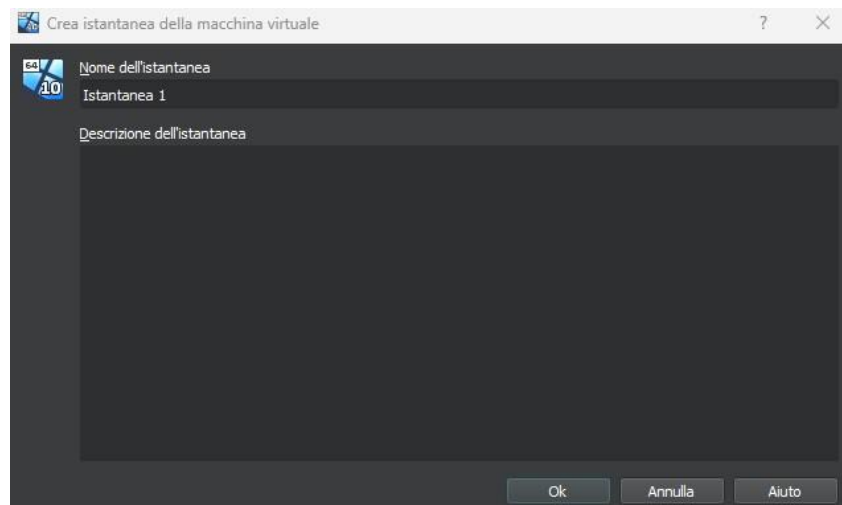


**AdwareCleaner.exe**

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00006E12	N/A	000066B0	000066B4	000066B8	000066BC	000066C0
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	61	000075C4	00000000	00000000	00007C12	00007060
USER32.dll	63	000076D8	00000000	00000000	00008022	00007174
GDI32.dll	8	000075A0	00000000	00000000	000080B4	0000703C
SHELL32.dll	6	000076BC	00000000	00000000	00008140	00007158
ADVAPI32.dll	9	00007564	00000000	00000000	000081E2	00007000
COMCTL32.dll	4	0000758C	00000000	00000000	0000822E	00007028
ole32.dll	4	000077E8	00000000	00000000	00008282	00007284
VERSION.dll	3	000077D8	00000000	00000000	000082CE	00007274

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00007A40	00007A40	01DF	GetTickCount
000079B0	000079B0	0169	GetFullPathNameA
000079C4	000079C4	026E	MoveFileA
000079D0	000079D0	030A	SetCurrentDirectoryA
000079E8	000079E8	015E	GetFileAttributesA
000079FE	000079FE	0171	GetLastError
00007A0E	00007A0E	004B	CreateDirectoryA
00007A22	00007A22	0319	SetFileAttributesA
0000798E	0000798E	02DB	SearchPathA
0000799C	0000799C	01B5	GetShortPathNameA
00007A50	00007A50	0163	GetFileSize
00007A5E	00007A5E	017D	GetModuleFileNameA
00007A74	00007A74	0142	GetCurrentProcess
00007A88	00007A88	0043	CopyFileA
00007A94	00007A94	00B9	ExitProcess
00007AA2	00007AA2	0313	SetEnvironmentVariableA
00007ABC	00007ABC	01F3	GetWindowsDirectoryA
00007AD4	00007AD4	01D5	GetTempPathA
00007A38	00007A38	0356	Sleep
00007960	00007960	0034	CloseHandle
00007B06	00007B06	0252	LoadLibraryA
00007B16	00007B16	03CC	lstrlenA
00007B22	00007B22	03C9	lstrcpyA
00007B2E	00007B2E	014D	GetDiskFreeSpaceA
00007B42	00007B42	020A	GlobalUnlock
00007B52	00007B52	0203	GlobalLock
00007B60	00007B60	006F	CreateThread
00007B70	00007B70	0066	CreateProcessA
00007B82	00007B82	02C4	RemoveDirectoryA
00007B96	00007B96	0053	CreateFileA
00007BA4	00007BA4	01D3	GetTempFileNameA

Nella seguente immagine abbiamo effettuato un'istantanea della macchina, così da poterla recuperare, dall'ultima operazione, in caso Adwere.exe la comprometta.



Nella seguente immagine, dopo aver avviato il Malware, con il tool Procmon (Process Monitor), possiamo vedere come con il passare del tempo Adwere, come agisce sul Sistema:

Time	Process Name	PID	Operation	Path	Result	Detail
10:51:...	svchost.exe	2980	TCP Send	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 295, start...
10:51:...	svchost.exe	2980	TCP Receive	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 550, seqn...
10:51:...	svchost.exe	2980	TCP Send	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 346, start...
10:51:...	svchost.exe	2980	TCP Receive	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 2904, seq...
10:51:...	svchost.exe	2980	TCP Send	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 1460, seq...
10:51:...	svchost.exe	2980	TCP Receive	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 1444, seq...
10:51:...	svchost.exe	2980	TCP Send	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 1460, seq...
10:51:...	svchost.exe	2980	TCP Receive	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 596, seqn...
10:51:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:64746 -> w...	SUCCESS	Length: 44, sequ...
10:51:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:64746 -> w...	SUCCESS	Length: 96, sequ...
10:51:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:62198 -> w...	SUCCESS	Length: 42, sequ...
10:51:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:62198 -> w...	SUCCESS	Length: 67, sequ...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 1250, seq...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 1250, seq...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 81, sequ...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 40, sequ...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 1250, seq...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 1250, seq...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 302, seqn...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 948, seqn...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 31, sequ...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 1250, seq...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 31, sequ...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 1246, seq...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 325, seqn...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 24, sequ...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 120, seqn...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 29, sequ...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 25, sequ...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 31, sequ...
10:51:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:55535 -> w...	SUCCESS	Length: 44, sequ...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 415, seqn...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 335, seqn...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 35, sequ...
10:51:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:55535 -> w...	SUCCESS	Length: 82, sequ...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 24, sequ...
10:52:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:62163 -> w...	SUCCESS	Length: 42, sequ...
10:52:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:62163 -> w...	SUCCESS	Length: 115, seqn...
10:53:...	svchost.exe	2980	TCP Receive	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 0, seqnum...
10:53:...	svchost.exe	2980	TCP Disconnect	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 0, seqnum...
10:53:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:59833 -> w...	SUCCESS	Length: 42, sequ...
10:53:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:59833 -> w...	SUCCESS	Length: 42, sequ...
10:53:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:64706 -> w...	SUCCESS	Length: 35, sequ...
10:53:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:64706 -> w...	SUCCESS	Length: 143, seqn...
10:53:...	6AdwCleaner.exe	4952	TCP Connect	DESKTOP-876K1T5.station:49722 -> 1...	SUCCESS	Length: 0, mss: 14...
10:53:...	6AdwCleaner.exe	4952	TCP Send	DESKTOP-876K1T5.station:49722 -> 1...	SUCCESS	Length: 142, start...
10:53:...	6AdwCleaner.exe	4952	TCP Receive	DESKTOP-876K1T5.station:49722 -> 1...	SUCCESS	Length: 1640, seq...
10:53:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:57935 -> w...	SUCCESS	Length: 36, sequ...
10:53:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:57935 -> w...	SUCCESS	Length: 118, seqn...
10:53:...	6AdwCleaner.exe	4952	TCP Connect	DESKTOP-876K1T5.station:49723 -> 1...	SUCCESS	Length: 0, mss: 14...
10:53:...	6AdwCleaner.exe	4952	TCP Send	DESKTOP-876K1T5.station:49723 -> 1...	SUCCESS	Length: 233, start...
10:53:...	6AdwCleaner.exe	4952	TCP Receive	DESKTOP-876K1T5.station:49723 -> 1...	SUCCESS	Length: 378, seqn...
10:53:...	6AdwCleaner.exe	4952	TCP Send	DESKTOP-876K1T5.station:49723 -> 1...	SUCCESS	Length: 276, start...
10:53:...	6AdwCleaner.exe	4952	TCP Receive	DESKTOP-876K1T5.station:49723 -> 1...	SUCCESS	Length: 378, sear...



Dopo aver seguito i passaggi descritti ed illustrati in precedenza con i tool di scansione ed analisi del Malware Adware, e aver eseguito il Malware, per osservare le azioni eseguite sul Sistema, utilizziamo la FakeNet, per illudere il Malware, di essere in grado di sfruttare un vero Internet, e possiamo osservare, come ci sia un incremento del traffico di rete:


[illegible]



Dopo aver avviato il file malevolo possiamo notare che dopo una scansione fittizia di AdwCleaner, file mascherato come legittimo, ci esce l'avviso che dice di aver trovato 13 file infetti, e se proviamo a pulire i file infetti, ci esce l'avviso di dover pagare per poter pulire, i file infetti, ma in realtà si tratta di un Virus, e possiamo dedurlo dalla frase:

**Your PC is heavily infected ! Clean now !**

AdwCleaner - Your one stop solution for Adware



**All done, please review results below**

Threat Name	Malware Type	Danger Level	Location
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
Win32.cc Loader	Sovware	Very High	adhsaeh.exe - Running process

Infections Found: 13  
Infections Cleanable: 13

**Your PC is heavily infected! Clean now! ---->**

Done

Report Clean

**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.

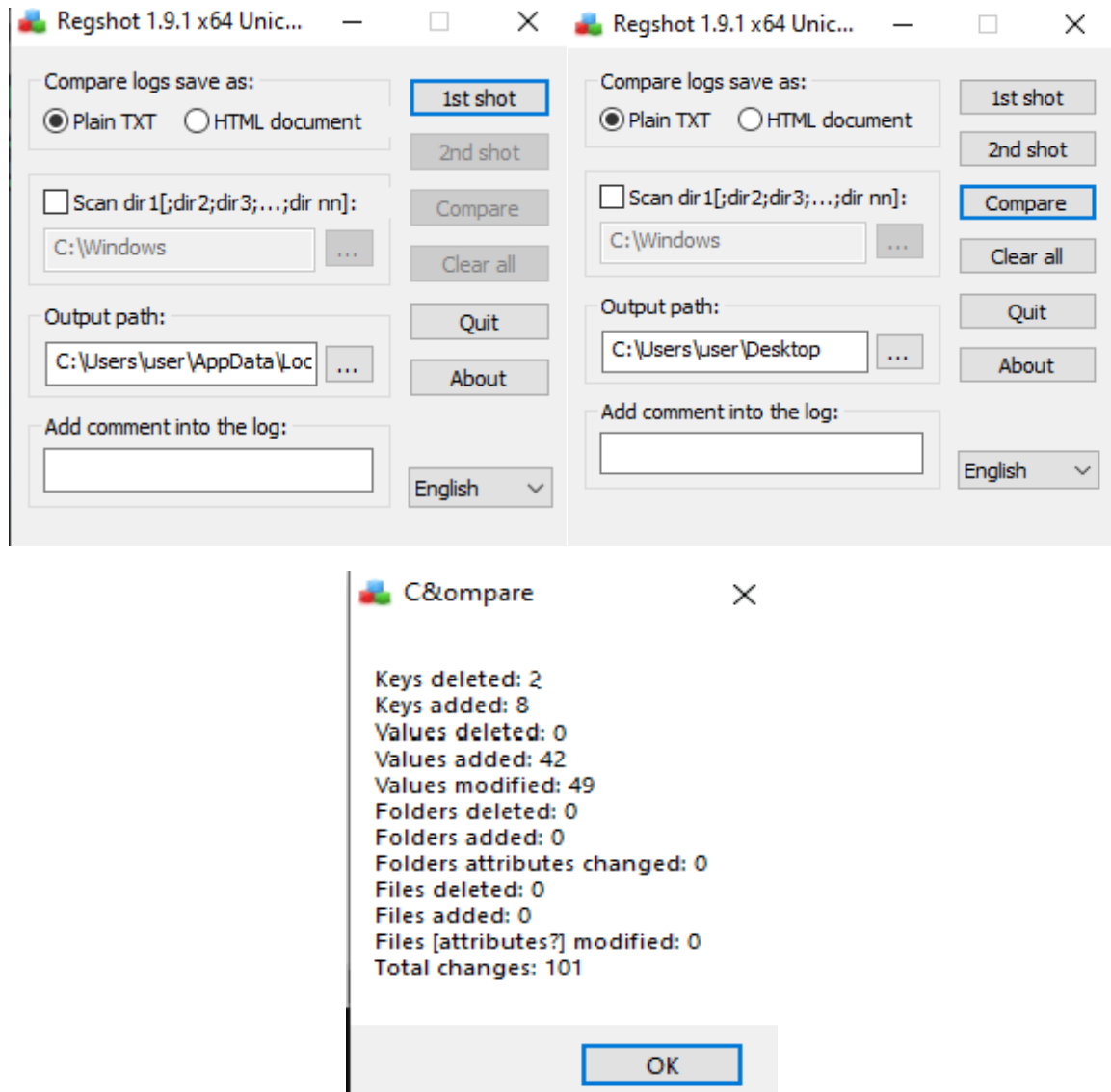
On sale now!

**Only \$59,99**

Normal price: \$89,99. Sale ending on: 29/10/2024

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

Alla fine dei vari procedimenti, scansioni ed analisi del Malware, con e senza l'utilizzo di FakeNet, utilizzo il tool Regshot, per eseguire un 1st shot prima dell'esecuzione, e successivamente faccio un 2nd shot, dopo aver eseguito il Malware, ed infine sempre con Regshot, faccio il Compare, per vedere le azioni eseguite da Adwere.exe:



Nella seguente ed ultima immagine, possiamo vedere dopo aver fatto il Compare, con Regshot, il report di FakeNet, sulle azioni eseguite dal Malware Adwere.exe, come illustrato di seguito

-----  
Keys deleted: 2  
-----

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\367a6d02-dd5a-46cb-b31c-c1208007f9a1  
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\367a6d02-dd5a-46cb-b31c-c1208007f9a1

-----  
Keys added: 8  
-----

HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner\_RASAPI32  
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner\_RASMANCS  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\324e26c-85c9-4e3d-80bb-aa03513a4a8e  
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\324e26c-85c9-4e3d-80bb-aa03513a4a8e  
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Google\Chrome\ThirdParty  
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000404A6  
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000001003E6  
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\AdwCleaner

## Mitigation

- Isolare il sistema
- Bloccare le connessioni a primo impatto sospette
- Avviare il Sistema in modalità provvisoria

## Remediation

- Rimuovere il Malware con il tool Antivirus
- Utilizzare strumenti specifici per la rimozione del Malware
- Ripristinare il Sistema dopo l'eliminazione
- Pulizia completa delle Chiavi di Registro
- Aggiornare il Sistema Operativo ed eventuali Software di Sistema