



MALWARE ANALYSIS



VIRUSTOTAL SCANNING



Utilizziamo il tool VirusTotal per effettuare una prima analisi, sul file
AdwereCleaner.exe

55/71 security vendors flagged this file as malicious

Adwere.exe è potenzialmente dannoso

The screenshot shows the VirusTotal analysis interface for the file `AdwereCleaner.exe`. The main summary card indicates a **Community Score** of **55 / 71**, with a note that **55/71 security vendors flagged this file as malicious**. The file size is **190.82 KB** and it was last analyzed **6 days ago**. The file type is identified as **EXE**. The analysis details tab is selected, showing the following properties:

Basic properties	Value
MDS	248aadd395faffb1670392a9398454
SHA-1	c53c140bbde6536ca3b7f962e4e9061ea3e5
SHA-256	51290129ccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc
Vhash	015056655dsd505709043x8003d7z47z62z3f3dz
Authentihash	8eb0f3a6371a77e2b5002de83a5955d4df5fb7f2cd7d8642138bb20d243be578
ImpHash	e160ef0e55b99162da4e266af99e5
Rich PE header hash	ecf81400e804d5e5c5ac27f2aace3
SSDeep	3072:15TDpNIVbxoSXJFGHcBRIWLZ3Tp73G8Wn7GIDog+ElqdSxo5xtIZ nvxRJggHaR:1577cfPB6B3GL7g+me5aZjnSVI9T/
TLSH	T17B1412524AF05AFFFB4384712AFDE1189f7B7828C5274A9974B148E323B440074F8611A
File type	Win32 EXE [executable] [windows] [win32] [pe] [peee]
Magic	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
TrID	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Scriptable Install System (92.7%) Win32 Executable MS Visual C++ (generic) (3.4%) Win64 Executable (generic) (1.1%) Win32 Dynamic Link Library (ge...
DetectEasy	PES2 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Magika	PEBIN
File size	190.82 KB (195400 bytes)
F-PROT packer	NSIS, appended

Below the properties, the history section shows the following timeline:

Event	Date
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

The names section lists several aliases for the file:

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



SANDBOX CUCKOO



cuckoo Dashboard Recent Pending Search

Insights

Cuckoo Installation

Version	2.0.7
You are up to date.	

Usage statistics

reported	5335460
completed	4
total	5376172
running	3

Cuckoo

SUBMIT A FILE FOR ANALYSIS

Drag your file into the left field or click the icon to select a file.

Yara rules detected for file (6 events)
Allocates read-write-execute memory (usually to unpack itself) (43 events)
Checks if process is being debugged by a debugger (2 events)
Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)
Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event)
Creates executable files on the filesystem (1 event)
Drops a binary and executes it (1 event)
Drops an executable to the user AppData folder (1 event)
Checks adapter addresses which can be used to detect virtual network interfaces (1 event)
The binary likely contains encrypted or compressed data indicative of a packer (2 events)
File has been identified by 11 AntiVirus engine on IRMA as malicious (11 events)
File has been identified by 55 AntiVirus engines on VirusTotal as malicious (50 out of 55 events)

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	

Escalade_priv: Tentativi di ottenere privilegi elevati.

Screenshot: Il malware tenta di acquisire screenshot del sistema.

Win_registry: Modifica delle chiavi di registro di sistema.

Win_token: Manipolazione dei token di sistema.

Win_private_profile: Accesso o modifica ai profili privati.

Win_files_operation: Operazioni sui file privati dell'utente.

Avviamo CFF Explorer, per un ulteriore analisi del Malware.

Andando su Section Header, troviamo le varie Sezioni dell'eseguibile

The screenshot shows the CFF Explorer VIII interface. The title bar reads "CFF Explorer VIII - [AdwereCleaner.exe]". The menu bar includes "File", "Settings", and "?". Below the menu is a toolbar with icons for File, Open, Save, and Exit. On the left, a tree view shows the file structure: "File: AdwereCleaner.exe" is selected, followed by "Dos Header", "Nt Headers" (expanded to show "File Header", "Optional Header", and "Data Directories [x]"), "Section Headers [x]", "Import Directory", "Resource Directory", and several utility icons: "Address Converter", "Dependency Walker", "Hex Editor", "Identifier", "Import Adder", "Quick Disassembler", "Rebuilder", "Resource Editor", and "UPX Utility". The main right pane displays the properties of "AdwereCleaner.exe" in a table format:

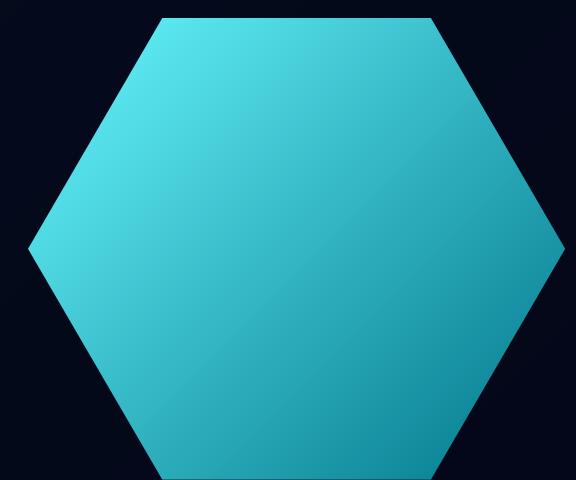
Property	Value
File Name	C:\Users\flare\Desktop\Malware\rogues\AdwereCleaner.exe
File Type	Portable Executable 32
File Info	Nullsoft PiMP Stub -> SFX
File Size	190.82 KB (195400 bytes)
PE Size	75.50 KB (77312 bytes)
Created	Wednesday 09 October 2024, 11.37.27
Modified	Wednesday 09 October 2024, 11.37.27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

Below this table is another table with one row:

Property	Value
Empty	No additional info available

AdwereCleaner.exe							
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...
000001E8	000001F0	000001F4	000001F8	000001FC	00000200	00000204	00000208
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word
.text	00005DE2	00001000	00005E00	00000400	00000000	00000000	0000
.rdata	000012DA	00007000	00001400	00006200	00000000	00000000	0000
.data	00025498	00009000	00000400	00007600	00000000	00000000	0000
.ndata	00008000	0002F000	00000000	00000000	00000000	00000000	0000
.rsrc	0000B268	00037000	0000B400	00007A00	00000000	00000000	0000

.rdata: Contiene dati di sola lettura come puntatori e stringhe costanti



Analizzando la
Sezione di “.rdata”
troviamo una
richiesta di far
partire con un
Quick Launch,
Internet Explorer



Nella voce "Import Directory" invece,
vediamo le liste DLL

CFF Explorer VIII - [AdwereCleaner.exe]

File Settings ?

AdwereCleaner.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

Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility

AdwereCleaner.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

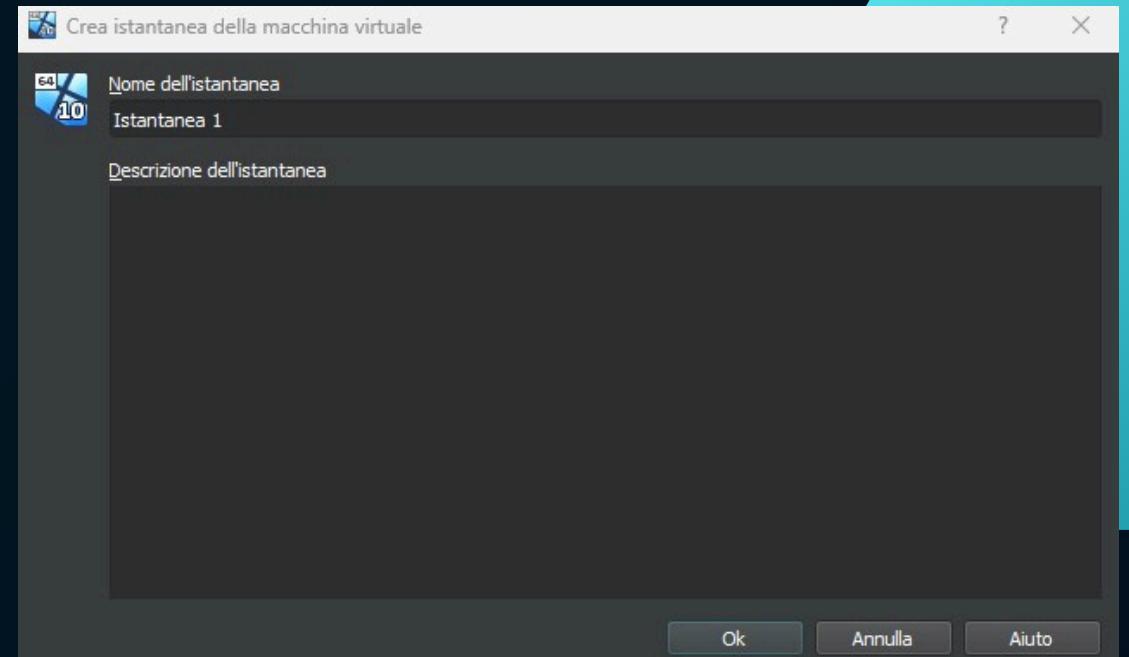
La presenza di funzioni come:
 LoadLibraryA
 CreateThread
 CreateProcessA
 RemoveDirectoryA
 GetTempFileNameA

Suggerisce che questo software:
 Carica altre librerie dinamicamente
 Crea nuovi processi e thread
 Manipola file e directory temporanee
 Rimuove directory

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	IstrlenA
00007B22	00007B22	03C9	IstrcpynA
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



Prima di avviare il malware, abbiamo creato un istantanea della macchina virtuale, per lavorare in sicurezza e non compromettere la macchina



Con Procmon, abbiamo notato che una volta avviato il malware, inizia a inviare richieste TCP

10:53:...	6AdwCleaner.exe	4952	TCP Connect	DESKTOP-876K1T5.station:49722 -> 1... SUCCESS
10:53:...	6AdwCleaner.exe	4952	TCP Send	DESKTOP-876K1T5.station:49722 -> 1... SUCCESS
10:53:...	6AdwCleaner.exe	4952	TCP Receive	DESKTOP-876K1T5.station:49722 -> 1... SUCCESS
10:53:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:57935 -> w... SUCCESS
10:53:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:57935 -> w... SUCCESS
10:53:...	6AdwCleaner.exe	4952	TCP Connect	DESKTOP-876K1T5.station:49723 -> 1... SUCCESS
10:53:...	6AdwCleaner.exe	4952	TCP Send	DESKTOP-876K1T5.station:49723 -> 1... SUCCESS
10:53:...	6AdwCleaner.exe	4952	TCP Receive	DESKTOP-876K1T5.station:49723 -> 1... SUCCESS
10:53:...	6AdwCleaner.exe	4952	TCP Send	DESKTOP-876K1T5.station:49723 -> 1... SUCCESS
10:53:...	6AdwCleaner.exe	4952	TCP Receive	DESKTOP-876K1T5.station:49723 -> 1... SUCCESS

Showing 128 of 573.007 events (0.0%)

Backed by virtual memory

Time ...	Process Name	PID	Operation	Path	Result	Detail
10:51:...	svchost.exe	2980	TCP Send	DESKTOP-876K1T5.station:49720 -> 1...	SUCCESS	Length: 295, starti...
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 Receive	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 Receive	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, seqnu...
10:51:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:64746 -> w...	SUCCESS	Length: 96, seqnu...
10:51:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:62198 -> w...	SUCCESS	Length: 42, seqnu...
10:51:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:62198 -> w...	SUCCESS	Length: 67, seqnu...
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, seqnu...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 40, seqnu...
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, seqnu...
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, seqnu...
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, seq...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 24, seqnu...
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, seqnu...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 25, seqnu...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 31, seqnu...
10:51:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:55535 -> w...	SUCCESS	Length: 44, seqnu...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:55535 -> w...	SUCCESS	Length: 415, seqn...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:55535 -> w...	SUCCESS	Length: 335, seqn...
10:51:...	chrome.exe	3404	UDP Send	DESKTOP-876K1T5.station:55535 -> w...	SUCCESS	Length: 35, seqnu...
10:51:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:55535 -> w...	SUCCESS	Length: 82, seqnu...
10:51:...	chrome.exe	3404	UDP Receive	DESKTOP-876K1T5.station:52187 -> mi...	SUCCESS	Length: 24, seqnu...
10:52:...	svchost.exe	984	UDP Send	DESKTOP-876K1T5.station:62163 -> w...	SUCCESS	Length: 42, seqnu...
10:52:...	svchost.exe	984	UDP Receive	DESKTOP-876K1T5.station:62163 -> w...	SUCCESS	Length: 115, seqn...

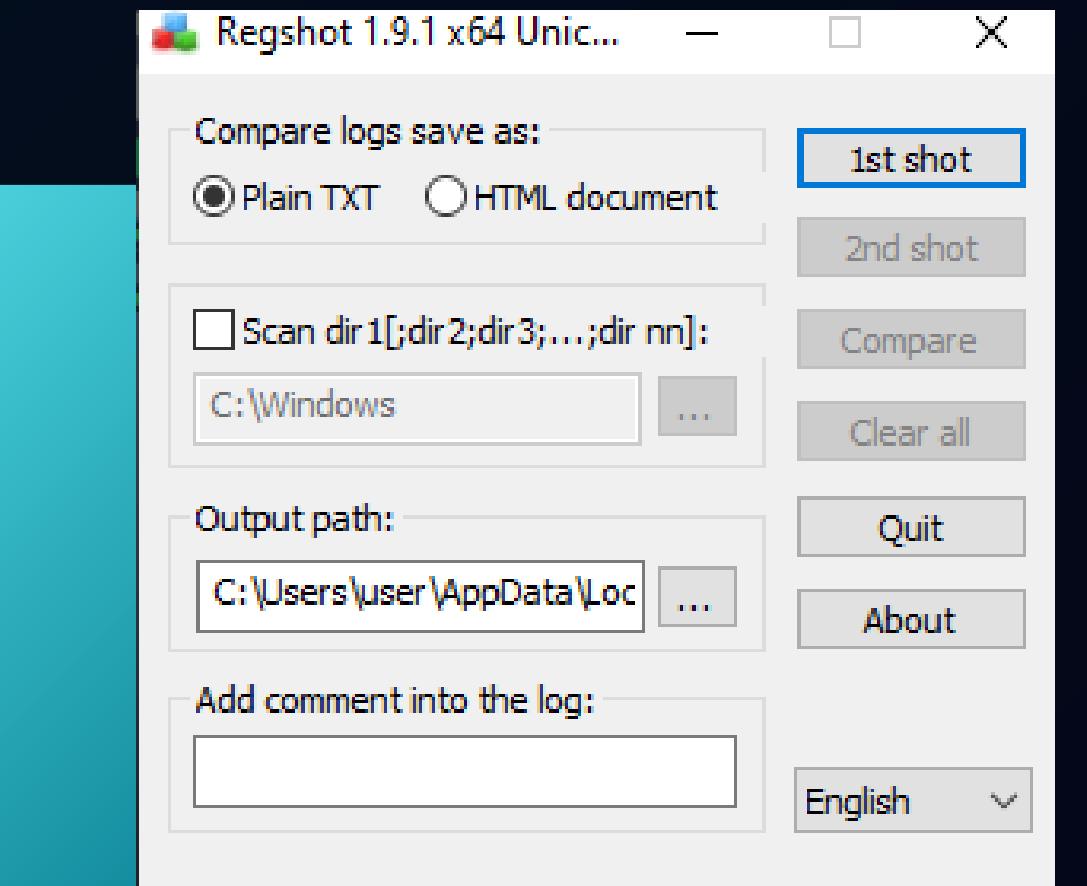


Avviamo Fakenet: uno strumento utile per analizzare malware in ambienti controllati, simulando un ambiente di rete.

The screenshot shows the Fakenet 3.2-alpha application window. At the top, it displays the path "C:\Tools\fakenet\fakenet3.2-alpha\fakenet.exe". Below this is the Fakenet logo and the text "Version 3.2". A copyright notice follows: "Developed by FLARE Team Copyright (C) 2016-2024 Mandiant, Inc. All rights reserved." The main area of the window is a terminal-like log output window. The log shows network traffic captured by Fakenet, including logs from "FakeNet", "Divterer", "svchost.exe", and "HTTPListener80". The log entries are timestamped and show various network requests and responses, such as DNS queries and HTTP POST requests to Microsoft's DeviceMetadataService.

```
0/28/24 10:39:35 AM [FakeNet] Loaded configuration file: C:\Tools\fakenet\fakenet3.2-alpha\configs\default.ini
0/28/24 10:39:36 AM [Divterer] Capturing traffic to packets_20241028_103936.pcap
0/28/24 10:39:36 AM [FTP] concurrency model: multi-thread
0/28/24 10:39:36 AM [FTP] masquerade (NAT) address: None
0/28/24 10:39:36 AM [FTP] passive ports: 60000->60010
0/28/24 10:39:36 AM [Divterer] Set DNS server 192.168.50.168 on the adapter: Ethernet
0/28/24 10:39:36 AM [Divterer] OpenService failed for DnsCache
0/28/24 10:39:36 AM [Divterer] Failed to call CloseServiceHandle
0/28/24 10:39:36 AM [Divterer] svchost.exe (1228) requested UDP 224.0.0.251:5353
0/28/24 10:39:36 AM [Divterer] svchost.exe (1000) requested UDP 192.168.50.1:67
0/28/24 10:39:36 AM [Divterer] svchost.exe (1988) requested UDP 239.255.255.250:1900
0/28/24 10:39:36 AM [Divterer] msedge.exe (4220) requested UDP 224.0.0.251:5353
0/28/24 10:39:36 AM [DNS Server] Received ANY request for domain 'DESKTOP-KH6PO3M.local'.
0/28/24 10:39:36 AM [Divterer] svchost.exe (1228) requested UDP 224.0.0.252:5355
0/28/24 10:39:36 AM [DNS Server] Received ANY request for domain 'DESKTOP-KH6PO3M.local'.
0/28/24 10:39:36 AM [DNS Server] Received ANY request for domain 'DESKTOP-KH6PO3M.local'.
0/28/24 10:39:36 AM [DNS Server] Received ANY request for domain 'DESKTOP-KH6PO3M.local'.
0/28/24 10:39:36 AM [Divterer] svchost.exe (1988) requested UDP 239.255.255.250:1900
0/28/24 10:39:40 AM [Divterer] svchost.exe (1228) requested UDP 192.168.50.168:53
0/28/24 10:39:42 AM [DNS Server] Received A request for domain 'go.microsoft.com'.
0/28/24 10:39:42 AM [Divterer] svchost.exe (988) requested TCP 192.0.2.123:80
0/28/24 10:39:42 AM [HTTPListener80] POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1
0/28/24 10:39:42 AM [HTTPListener80] Connection: Keep-Alive
0/28/24 10:39:42 AM [HTTPListener80] Content-Type: text/xml; charset="UTF-16LE"
0/28/24 10:39:42 AM [HTTPListener80] User-Agent: MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT
0/28/24 10:39:42 AM [HTTPListener80] SOAPAction: "http://schemas.microsoft.com/windowsmetadata/services/2007/09/18/dms/DeviceMetadataService/GetDeviceMetadata"
0/28/24 10:39:42 AM [HTTPListener80] Content-Length: 1424
0/28/24 10:39:42 AM [HTTPListener80] Host: go.microsoft.com
0/28/24 10:39:42 AM [HTTPListener80]
0/28/24 10:39:42 AM [HTTPListener80] b' \xff\xfe<\x00?\x00\x00m\x001\x00 \x00v\x00e\x00r\x00s\x00i\x00o\x00n\x00=\x00"\x001\x00.\x000\x00"\x00 \x00e\x00n\x00c\x00o\x00o\x00\x00\x00<\x00c\x00a\x00.\x00f\x00a\x00n\x00a\x00v\x00a\x001\x00a\x00n\x00a\x00 \x00x\x00m\x001\x001\x00a\x00n\x00s\x00i\x00a\x00.\x00a\x00s\x00i\x00a\x00=\x00"\x00a\x00h\x00a\x00t\x00a\x00n\x00a\x00.\x00a\x00/\x00a\x00/\x00a\x00s\x00c\x00a\x00h\x00a\x00e\x00o\x00'
```

Avviamo anche Regshot, così da poter verificare i relativi danni causati da un Malware, avviato dopo aver cliccato "1st shot"





Avviando il Malware scaricato, notiamo che dopo la scansione, ci chiede di pagare il programma, per eliminare i file

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 Looor	Software	Very High	adhsoc.exe - Running process

Infections Found: 13
Infections Cleanable: 13
Your PC is heavily infected! Clean now! ---->

Done

Report Clean

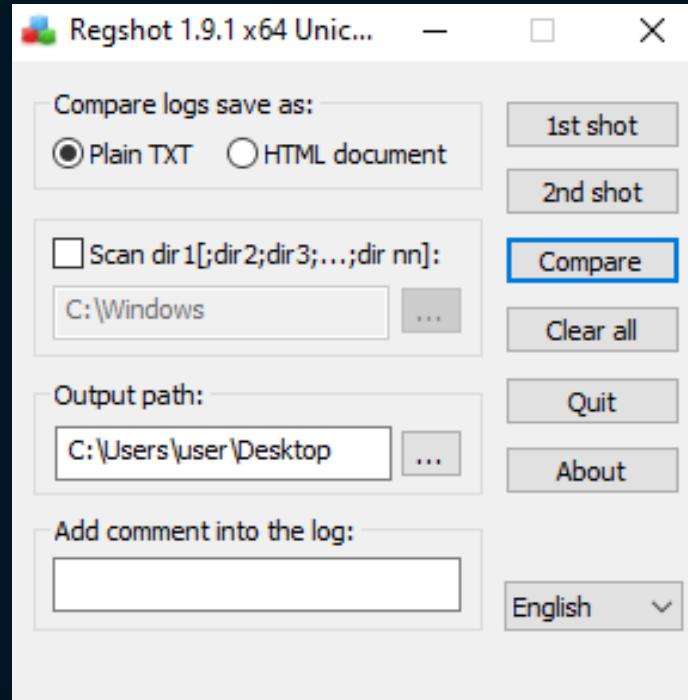
Important Note
The scan has been completed, 13 infections found
OK

Dopo aver avviato il Malware possiamo notare su Fakenet un incremento del traffico di rete, dopo che il malware ha finito la sua "Scansione".

```
10/28/24 10:53:39 AM [ HTTPListener80] Host: ocsp.usertrust.com
10/28/24 10:53:39 AM [ HTTPListener80]
10/28/24 10:53:39 AM [ HTTPListener80]
10/28/24 10:53:39 AM [ HTTPListener80] b' 0Q000M0K0I0\t\x06\x05+\x0e\x03\x02\x1a\x05\x00\x04\x14|\xb1fT\x9c\xab\xdbD
\xeeb&\x16\xad\xf4e{\xf7z\xd5\x94\x04\x14\xad\xbd\x98z4\xb4&\xf7\xfa\xc4&T\xef\x03\xbd\xe0$\xcbT\x1a\x02\x10B\x1a\xf2\x9
4\t\x84\x19\x1fR'
10/28/24 10:53:39 AM [ HTTPListener80] b' K\xc6$&\xa7K'
10/28/24 10:53:39 AM [ HTTPListener80] Storing HTTP POST headers and data to http_20241028_105339.txt.
10/28/24 10:53:39 AM [ Divter] svchost.exe (1228) requested UDP 192.168.50.168:53
10/28/24 10:53:39 AM [ DNS Server] Received A request for domain 'crl.usertrust.com'.
10/28/24 10:53:39 AM [ Divter] 6AdwCleaner.exe (5844) requested TCP 192.0.2.123:80
10/28/24 10:53:39 AM [ HTTPListener80] GET /AddTrustExternalCARoot.crl HTTP/1.1
10/28/24 10:53:39 AM [ HTTPListener80] Connection: Keep-Alive
10/28/24 10:53:39 AM [ HTTPListener80] Accept: /*
10/28/24 10:53:39 AM [ HTTPListener80] User-Agent: Microsoft-CryptoAPI/10.0
10/28/24 10:53:39 AM [ HTTPListener80] Host: crl.usertrust.com
10/28/24 10:53:39 AM [ HTTPListener80]
10/28/24 10:53:45 AM [ Divter] msedge.exe (4692) requested UDP 192.168.50.168:53
10/28/24 10:53:45 AM [ DNS Server] Received A request for domain 'edge.microsoft.com'.
10/28/24 10:53:45 AM [ DNS Server] Received HTTPS request for domain 'edge.microsoft.com'.
10/28/24 10:53:45 AM [ Divter] msedge.exe (4692) requested TCP 192.0.2.123:443
10/28/24 10:53:57 AM [ Divter] svchost.exe (1228) requested UDP 192.168.50.168:53
10/28/24 10:53:57 AM [ DNS Server] Received A request for domain 'tlu.d1.delivery.mp.microsoft.com'.
10/28/24 10:53:57 AM [ Divter] ICMP type 8 code 0 192.168.50.168->192.0.2.123
10/28/24 10:53:57 AM [ Divter] Modifying ICMP packet (type 8, code 0):
10/28/24 10:53:57 AM [ Divter] from: 192.168.50.168->192.0.2.123
10/28/24 10:53:57 AM [ Divter] to: 192.168.50.168->192.168.50.168
10/28/24 10:53:57 AM [ Divter] ICMP type 0 code 0 192.168.50.168->192.168.50.168
```



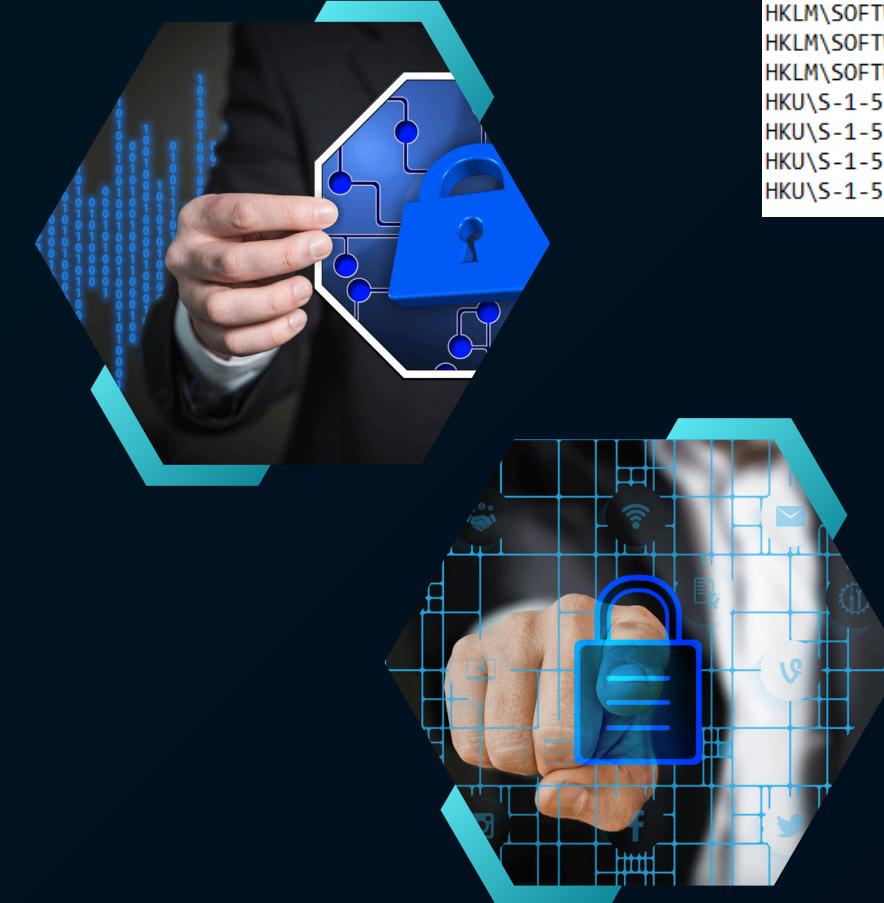
HKEY_LOCAL_MACHINE
contiene le informazioni
relative alla configurazione
del Computer



Una volta che il Malware ha terminato
la sua esecuzione, clicchiamo su
"Compare", per ricevere il report finale



Inoltre notiamo nel report che
ci sono vari tentativi di
connessione e accesso alle
risorse di sistema e alle chiavi
di registro, e anche prove di
accesso ai Server ed i Domini



```
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_RASMNCs
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\W32:00000000001003E6
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\AdwCleaner
```

Possiamo anche vedere il report sotto forma di testo, per poterlo analizzare meglio.
Notiamo che sono state rimosse delle policy dal nostro PC

Cercando con chat Gpt, ci dice che:

HKLM\SOFTWARE\Microsoft\Tracing...: indica che ci sono vari tentativi di connessione da parte
del Malware che tenta di cambiare le configurazioni di Sistema e/o Servizi di Rete



HTTP LISTENER

```
</pre></b>
```

FakeNet-NG is a next generation dynamic network analysis tool for malware analysts and penetration testers. It is open source and designed for the latest versions of Windows.

The tool allows you to intercept and redirect all or specific network traffic while simulating legitimate network services. Using FakeNet-NG, malware analysts can quickly identify malware's functionality and capture network signatures. Penetration testers and bug hunters will find FakeNet-NG's configurable interception engine and modular framework highly useful when testing application's specific functionality and prototyping PoCs.

FakeNet-NG is based on the excellent Fakenet tool developed by Andrew Honig and Michael Sikorski.

Contact

For bugs, crashes, or other comments please contact **The FLARE Team** by email **FakeNet@mandiant.com**.

</body>

</html>

```
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Classes\Local Settings\MuiCache\86\FE2848FA\%systemroot%\system32\FirewallControlPanel.dll
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\86\FE2848FA\%SystemRoot%\System32\ngcsvc.dll,-100: "Microsoft Passport"
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\86\FE2848FA\%SystemRoot%\System32\NgCtnrSvc.dll,-1: "Contenitore Microsoft Passport"
```



THANK YOU