

BUILD WEEK III

“Esercizio 1 – Malware Analysis”

Dopo aver scaricato il malware come richiesto siamo passati inizialmente all'analisi statica ed in seguito dinamica dello stesso.

ANALISI STATICA

In prima analisi abbiamo sfruttato VirusTotal per testare il malware, ottenendo così i seguenti dati:

51290129cccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc

56 / 71

Community Score -219

56/71 security vendors flagged this file as malicious

Reanalyze Similar More

51290129cccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc

FakeAdwCleaner.exe

Size 190.82 KB Last Analysis Date 1 month ago

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

persistence detect-debug-environment nsis

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 21+

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

Popular threat label trojan.porcupine/mint Threat categories trojan fakeav Family labels porcupine mint boy2napig

Security vendors' analysis

Vendor	Detection	Vendor	Detection
AhnLab-V3	Dropper/Win32.Dapato.R137988	Alibaba	Hoax:MSIL/Porcupine.e66e0e97
AliCloud	Trojan:MSIL/Hoax.Akgpp	Antiy-AVL	HackTool[Hoax]/MSIL.Agent
Arcabit	Trojan.Mint.Porcupine.ED5D10	Arctic Wolf	Unsafe

-estratto generale dell'analisi-

Basic properties

MD5 248aadd395ffa7ffb1670392a9398454

SHA-1 c53c140bbdeb556fca33bc7f9b2e44e9061ea3e5

SHA-256 51290129cccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc

Vhash 015056655d5c05709043z8003d7z47z62z3f03dz

Authentihash 8eb8f3a6371a77e2b5002de83a5955d4d5fb7f2cdb7d8642138bb20d243be578

Imphash e160ef8e55bb9d162da4e266afd9eef3

Rich PE header hash ecf81400e80e4d5ebc5ac2f7c2aacea3

SSDEEP 3072:15TDpNfVbxDSXJFFGhcBR1WLZ37p73G8Wn7GID0g+ELqdSxo5XtIzjnvxRJgghaR:157TcfFPB6B3GL7g+me5aZjn5Vil9T/

TLSH T17B1412524AF05AFFFB4384712AFDE1B9E7B7828C5274A9974B148E323B440D74F8611A

File type Win32 EXE

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

Varist packer NSIS

-proprietà di base-

Contacted IP addresses (77)

IP	Detections	Autonomous System	Country
104.247.81.133	0 / 95	206834	CA
104.247.81.53	0 / 95	206834	CA
104.71.214.69	0 / 95	16625	US
114.114.114.114	0 / 95	21859	CN
117.18.237.29	0 / 95	-	AU
131.107.255.255	0 / 95	3598	US
185.53.177.53	0 / 95	61969	DE
185.53.178.7	0 / 95	61969	DE
192.168.0.195	0 / 95	-	-
192.168.0.4	0 / 95	-	-

-indirizzi IP contattati-

Contacted Domains (40) ⓘ			
Domain	Detections	Created	Registrar
1.155.190.20.in-addr.arpa	0 / 95	-	-
106.89.54.20.in-addr.arpa	0 / 95	-	-
133.81.247.104.in-addr.arpa	0 / 95	-	-
202.216.231.44.in-addr.arpa	0 / 95	-	-
79.49.8.65.in-addr.arpa	0 / 95	-	-
80.69.35.23.in-addr.arpa	0 / 95	-	-
a233.dscd.akamai.net	0 / 95	1999-03-03	MarkMonitor Inc.
adobe.com	0 / 95	1986-11-17	NOM-IQ Ltd dba Com Laude
armmf.adobe.com	0 / 95	1986-11-17	NOM-IQ Ltd dba Com Laude
assets.msn.com	0 / 95	1994-11-10	MarkMonitor Inc.

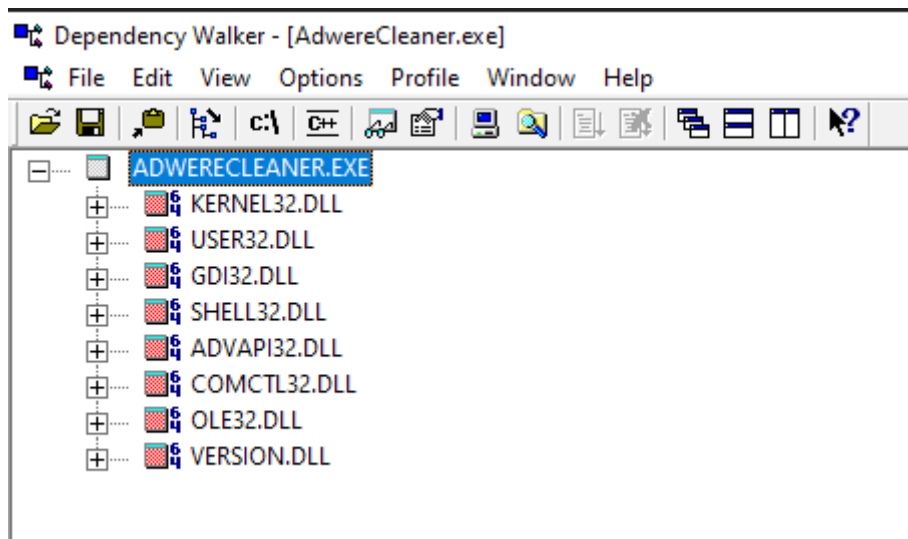
-domini contattati-

Dropped Files (13) ⓘ			
Scanned	Detections	File type	Name
2025-05-30	0 / 62	?	1F356F4D07FE8C483E769E4586569404
2025-05-30	0 / 62	?	B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F
2025-08-14	53 / 72	Win32 EXE	6AdwCleaner.exe
2025-03-10	44 / 68	Win32 EXE	6adwcleaner.exe
?	?	file	0bfa420acf2ad034dca670926bf30a1d5f05ffd6087fde2d8ae4eee5d29c74da
?	?	file	4F0033E811FE2497B38F0D45DF958829D01933EBE7D331079EEFC8E38FBEAA61
?	?	file	5d695998f311e05d7bfc4f76f948fb6c78572a2137e03f5cb6c41794c06afa0e
?	?	file	7a2e8ffe5697837feedebc5525e1ea3305589f2de399195dbd5860bf7b4760d8
?	?	file	819b63fa98c0f590ed6e6404270cbe5d262918e141fa3cfb2f81e09886c47f4d
?	?	file	91a623eacdf1e2a0c229d52c64c980833dc332053f7003c163e35f2cfa7d4ef3

-file droppati-

Names ⓘ
FakeAdwCleaner.exe
AdwereCleaner.exe
fakeadwcleaner.exe
Endermanch@FakeAdwCleaner.exe
7ac27f7b8c68f4c5d547891d991001661a1a6af1-d659d96d15c7a1206f44eb36ed72495563140859
bf832162-104c-4773-9c5e-9a9aaa876444.exe
858858dd-26e0-4876-bd5d-4ecb3d200fee.exe
91440ed8-e5ef-4a38-ada2-6666b60726a4.exe
AdwereCleaner (1).exe
AdwereCleaner.zOtfFhsJ.exe.part
Unconfirmed 567426.crdownload
AdwereCleaner (2).exe
ADWERECLEANER.EXE
481953.exe
AdwereCleaner(6).exe
AdwereCleaner(3).exe
AdwereCleaner(1).exe
Non confermato 637281.crdownload

-nomi alternativi del file-



-dll prese in esame-

In seguito all'analisi statica, siamo giunti già alla conclusione che 56 su 71 motori di sicurezza riconoscono il malware come altamente pericoloso, classificandolo come *Trojan* o *FakeAV* (Fake AntiVirus).

Nel dettaglio la natura del file è associata ad un eseguibile Windows 32bit legato alle possibili famiglie Porcupine, Mint.

Riusciamo inoltre ad intuire che il malware è progettato per ingannare l'utente simulando un software di pulizia o rimozione adware, che, dopo una scansione simulata troverà falsamente decine o centinaia di minacce critiche al fine di indurre il bersaglio ad eseguire azioni dannose o pagare per la rimozione di minacce inesistenti.

Siamo andati poi a visualizzare gli IoC (Indicator of Compromission), trovando i seguenti hash che sono essenziali per il rilevamento e la mitigazione:

- SHA-256 51290129cccca38c8c3b444d0fd8d0848c08fc2e5291fc0d219fd542530adc
- SHA-1 c53c140b0deb56fca33bc789b24e4e06c1ea3e5
- MD5 248aadd39f5fa7ffb1670392a8399454

Abbiamo inoltre delle informazioni di base aggiuntive:

- Nome File Rilevato *FakeAdwCleaner.exe*
- Dimensione *190.82 KB*
- Tipo di File *PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive*
- Compilatore/Packer *Il file è stato compilato utilizzando NSIS (Nullsoft Scriptable Install System), un programma di installazione legittimo spesso abusato dai malware per impacchettare script e payload dannosi.*

N.B. Non è da escludere una possibile installazione di adware o spyware.

ANALISI DINAMICA

Ai fini di un'analisi dinamica del malware, abbiamo inserito nella sandbox any.run il file malevolo per osservarne il comportamento:

The screenshot displays the ANY.RUN dynamic analysis sandbox interface. The main window shows a Windows desktop environment with a large red play button in the center, indicating that the analysis is in progress. The desktop includes icons for Recycle bin, VLC media player, and several documents. The taskbar at the bottom shows the Start button, a search bar, and several pinned applications. The bottom status bar indicates the current status as 'Guest' and 'Access Period: unlimited'.

On the right side, the 'Malicious activity' panel is visible, showing details for the process 'AdwareCleaner.exe'. It includes indicators for Get sample, IOC, MalConf, and Restart, along with buttons for Text report, Graph, ATTACK, Summary, and Export. Below this, a table lists processes with their PIDs, names, and various metrics.

The bottom panel shows the 'HTTP Requests' tab, which displays a list of network requests. The table includes columns for Time, Method, Status, Rep, PID, Process name, CN, URL, and Content. The requests are filtered by PID or name and can be sorted by PCAP.

Time	Method	Status	Rep	PID	Process name	CN	URL	Content
3019 ms	GET	200: OK	✓	1268	svchost.exe	✓	http://cf.limicrosoft.com/pkgs/cf/products/McRocSecAut2011_2011_03_22.crl	825 b + binary
3036 ms	GET	200: OK	✓	1268	svchost.exe	✓	http://www.microsoft.com/pkgs/cf/McSecSerCA2011_2011-10-18.crl	868 b + binary
3048 ms	GET	200: OK	✓	5944	MsIscCoreWorker.exe	✓	http://www.microsoft.com/pkgs/cf/McSecSerCA2011_2011-10-18.crl	868 b + binary
50181 ms	POST	500: Int Server E...	✓	-	-	✓	https://activation-v2.sls.microsoft.com/SLActivateProduct/SLActivateProduct.aspx?configtensi...	17 kb + text 512 b + xml
110.44 s	POST	500: Int Server E...	✓	-	-	✓	https://activation-v2.sls.microsoft.com/SLActivateProduct/SLActivateProduct.aspx?configtensi...	17 kb + text 512 b + xml

-schermata principale (http request)-

This screenshot is identical to the one above, showing the ANY.RUN dynamic analysis sandbox interface. The main window displays a Windows desktop with a large red play button. The right panel shows the 'Malicious activity' for 'AdwareCleaner.exe'. The bottom panel shows the 'Connections' tab, which displays a list of network connections. The table includes columns for Time, Method, Status, Rep, PID, Process name, CN, URL, and Content. The connections are filtered by PID or name and can be sorted by PCAP.

Time	Method	Status	Rep	PID	Process name	CN	URL	Content
3019 ms	GET	200: OK	✓	1268	svchost.exe	✓	http://cf.limicrosoft.com/pkgs/cf/products/McRocSecAut2011_2011_03_22.crl	825 b + binary
3036 ms	GET	200: OK	✓	1268	svchost.exe	✓	http://www.microsoft.com/pkgs/cf/McSecSerCA2011_2011-10-18.crl	868 b + binary
3048 ms	GET	200: OK	✓	5944	MsIscCoreWorker.exe	✓	http://www.microsoft.com/pkgs/cf/McSecSerCA2011_2011-10-18.crl	868 b + binary
50181 ms	POST	500: Int Server E...	✓	-	-	✓	https://activation-v2.sls.microsoft.com/SLActivateProduct/SLActivateProduct.aspx?configtensi...	17 kb + text 512 b + xml
110.44 s	POST	500: Int Server E...	✓	-	-	✓	https://activation-v2.sls.microsoft.com/SLActivateProduct/SLActivateProduct.aspx?configtensi...	17 kb + text 512 b + xml

-schermata principale (connections)-

CREAZIONI DI FILE E DROP DEL PAYLOAD:

Il file iniziale, *AdwareCleaner.exe* (eseguito da desktop) è un installer che rilascia e lancia un secondo eseguibile:

- Drop del Payload *C:\Users\admin\AppData\Local\6AdwCleaner.exe*
- Hash del Payload

MD5 *87E4959FEFEC297EBBF42DE7985088F6*

SHA256 *4F0033E811FE2497B38F0D45DF958829001933EBE7D331079EEFC8E38FBEEA61*

PROCESS TREE (catena di infezione)

Il grafico mostra poi il flusso dell'attacco:

- | | |
|---------------------------------|--|
| 1. Start | La vittima esegue il file iniziale <i>AdwareCleaner.exe</i> |
| 2. Drop/Esecuzione | <i>AdwareCleaner.exe</i> , rilascia ed esegue <i>6AdwCleaner.exe</i> |
| 3. Persistenza/Esec. Automatica | <i>6AdwCleaner.exe</i> è il responsabile della scrittura su registro per la persistenza e dell'esecuzione con l'opzione <i>-auto</i> |
| 4. Processi collaterali | Si notano inoltre attività relative a <i>slui.exe</i> (Windows Activation Client) e <i>svchost.exe</i> , che in questo particolare caso potrebbero essere tentativi di innalzamento dei privilegi o di interferenza dei processi |

ALTRE ATTIVITA' SOSPETTE

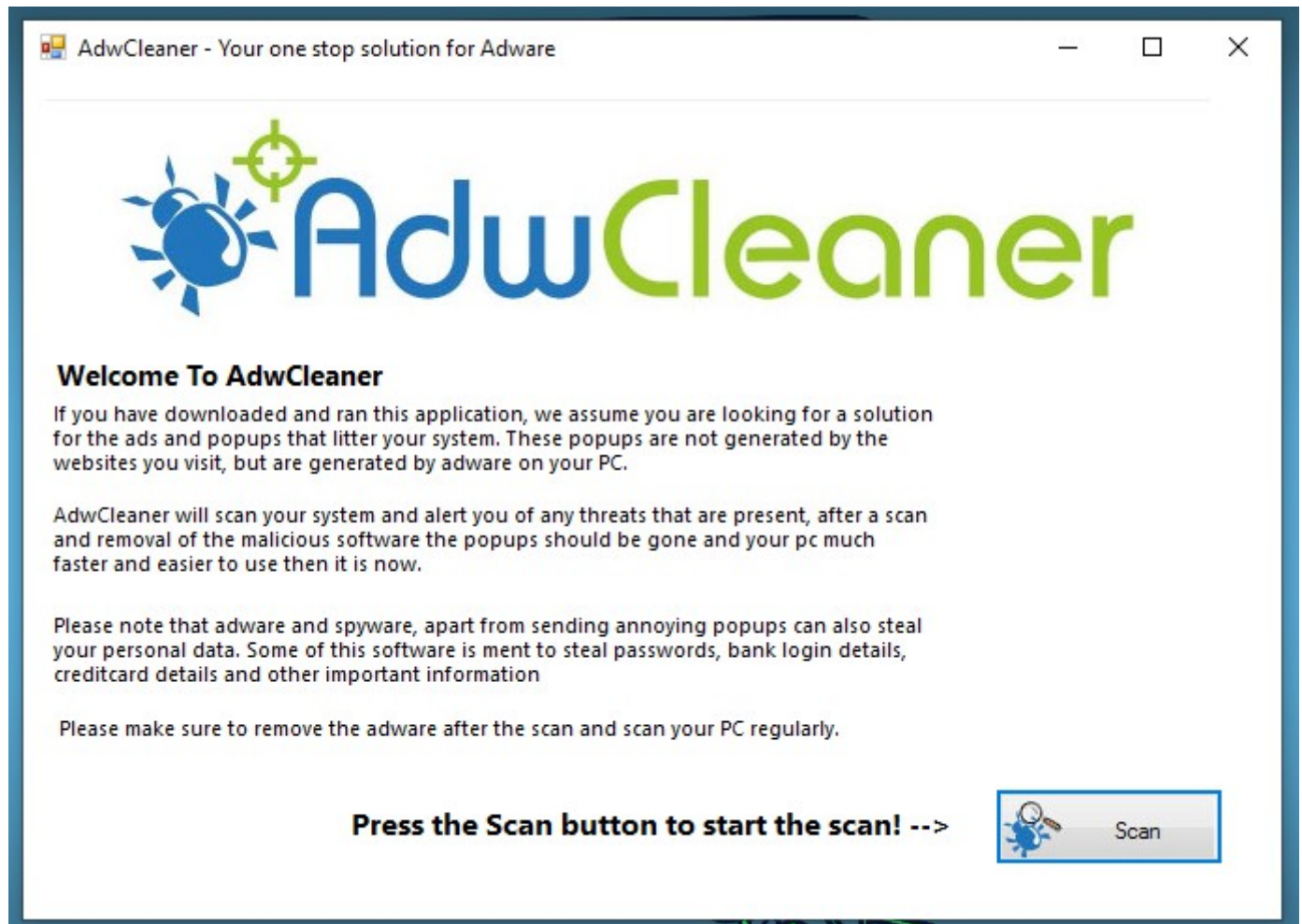
- Controllo delle lingue supportate
- Lettura del nome del PC
- Lettura del Machine GUID dal registro
- Controllo delle impostazioni del server proxy
- Lettura delle impostazioni di Internet Explorer

TENTATIVI DI OFFUSCAMENTO

6AdwCleaner.exe tenta di disabilitare i log di traccia (disable trace logs), nel tentativo di ostacolare l'analisi.⁷

AVVIO IN AMBIENTE PROTETTO ED ULTIME IMPRESSIONI

In ultima analisi, IN AMBIENTE PROTETTO, abbiamo avviato il file sospetto per analizzarne il comportamento:



-avvio del file-

Subito dopo l'avvio, il software richiederà, come previsto una scansione del pc.



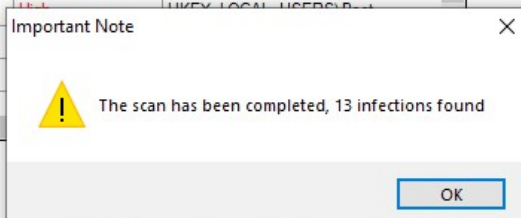
All done, please review results below

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		HKLM\LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{...}
VombaSavers	Advertising		
Win32.Stealer Trojan	Spyware		
Win32.cc Loader	Spyware		

Infections Found: 13

Infections Cleanable: 13

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



-fine della "scansione"-



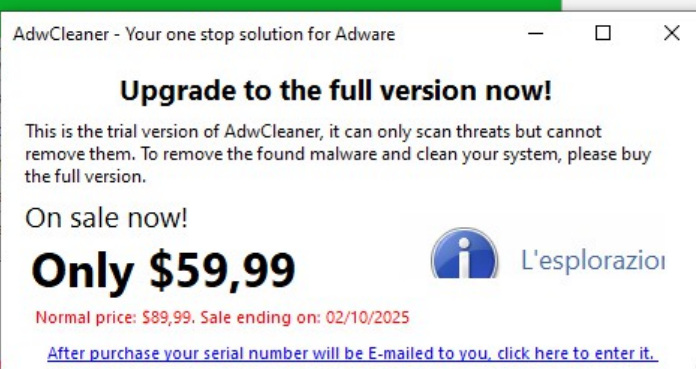
All done, please review results below

Threat Name	Malware Type
Start page Changer Win.32	Browser Hijacker
MediaTraffic Feed	Popup Advertising
VombaSavers	Advertising
Win32.Stealer Trojan	Spyware
Win32.cc Loader	Spyware

Infections Found: 13

Infections Cleanable: 13

Your PC is heavily infected! Clean now!



-richiesta in denaro per provvedere alla rimozione-

Non appena avrà terminato, lo stesso richiederà informazioni personali come e-mail, numero della carta di credito per provvedere alla pulizia.

RICORDIAMO CHE DALLE PRECEDENTI ANALISI, E' RISULTATO UN FAKEAV/TROJAN.

Nome	PID	Stato	Nome ute...	CPU	Memoria (...)	Virtualizzazion...
6AdwCleaner.exe	1452	In esecuzione	User	00	23.696 K	Non consentito

-avvio del software dannoso in background-

E possiamo notare come nel frattempo abbia avviato il processo prima descritto: 6AdwCleaner.exe.

CONCLUSIONI

Dopo l'analisi statica e dinamica, possiamo affermare che:

- Il file è un installer dannoso, che dropa un eseguibile secondario
- Il suo scopo primario, è stabilire la persistenza modificando la chiave Run del Registro
- Svolge chiaramente una ricognizione dell'ambiente prima di agire

Si raccomanda caldamente l'eliminazione sicura del file e l'impedimento della sua apertura all'interno delle piattaforme aziendali.