

# Analisi Statica AdwareCleaner.exe

## Introduzione

Questa relazione descrive i risultati di un'analisi statica eseguita su un file binario identificato come potenzialmente dannoso. L'analisi è stata effettuata utilizzando diversi strumenti forensi, quali Pestudio, Detect It Easy (DIE), CFF Explorer, Binwalk, File, Unzip/Gunzip, Strings e VirusTotal. L'obiettivo principale è stato quello di determinare caratteristiche anomale, potenziali vettori di attacco e indicazioni di comportamenti sospetti. Nel corso della relazione, i risultati saranno illustrati passo per passo, corredati da esempi visuali tratti dagli strumenti utilizzati.

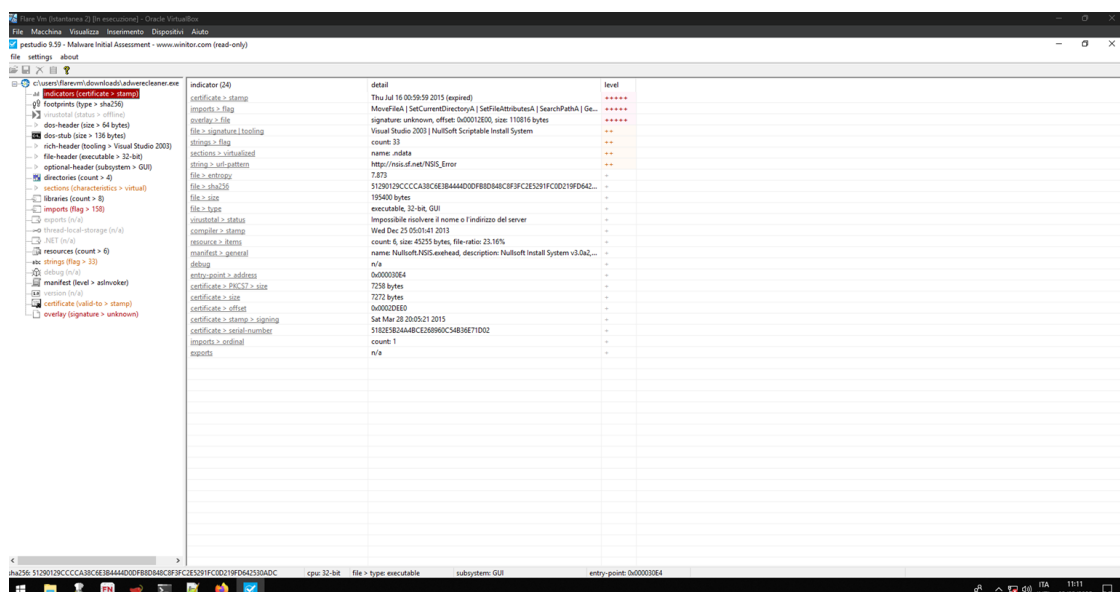
## Analisi dettagliata

### Pestudio

L'analisi condotta con Pestudio ha evidenziato diversi indicatori di anomalie nel file analizzato. Il certificato digitale associato risulta scaduto, con una firma sconosciuta o assente. Questo può indicare che il file è stato modificato o che non è stato firmato da una fonte affidabile. Inoltre, l'overlay rilevato (signature > unknown) suggerisce la possibile aggiunta di dati non standard al file.

Un aspetto particolarmente interessante è l'entry-point del file, che si trova a 0x000030E4. Questo valore appare anomalo e potrebbe indicare manipolazioni o compressioni del codice. Pestudio ha anche segnalato l'assenza di informazioni di debug, elemento che conferma che il file è stato compilato senza dettagli tecnici per ostacolare ulteriori analisi. L'hash SHA256 del file è stato analizzato tramite VirusTotal, ottenendo risultati che confermano la natura malevola del file.

Inoltre, è stato osservato l'uso di API sospette, tra cui ADVAPI32.dll e SHELL32.dll. Queste librerie sono comunemente sfruttate dai malware per attività come la modifica del registro di sistema e l'interazione con il file system. La sezione risorse del file contiene un'icona utilizzata probabilmente per imitare software legittimi. Tuttavia, è stata identificata una risorsa con elevata entropia, denominata instance1 e delle dimensioni di 43.826 byte, che potrebbe contenere dati compressi o cifrati.



| name       | instance (6) | signature  | location        | size (45255 bytes) | file-ratio (23.16%) | footprint (sha256)                  | entropy | language   | first-bytes-hex                           | first-bytes-text           |
|------------|--------------|------------|-----------------|--------------------|---------------------|-------------------------------------|---------|------------|---|----------------------------|
| icon       | 1            | icon       | rscc-0x00007890 | 43826              | 22.43 %             | 9390720DFA8CB2E3CF46E0FAE4236A3E... | 7.979   | English-US | 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 4...  | ..PNG.....IHDR.....        |
| manifest   | 1            | manifest   | rscc-0x00012960 | 773                | 0.40 %              | C8E88CC8B88E0FC62E36462A5D3F466...  | 5.270   | English-US | 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E... | <?xml version="1.0" enc... |
| icon-group | 103          | icon-group | rscc-0x00012940 | 20                 | 0.01 %              | C1EE3C4E96687338193C7C787A4E4C8...  | 1.517   | English-US | 00 00 01 00 01 00 00 00 00 00 01 00 25... | .....Z.....                |
| dialog     | 105          | dialog     | rscc-0x000138C0 | 296                | 0.13 %              | FECD8955807E1C708F81A7980461...     | 2.662   | English-US | 01 00 FF FF 00 00 00 00 00 00 00 48...    | .....H.....                |
| dialog     | 111          | dialog     | rscc-0x000127C0 | 284                | 0.15 %              | 6987C734E1491E830248D052C2897396... | 2.881   | English-US | 01 00 FF FF 00 00 00 00 00 00 00 48...    | .....H.....                |
| dialog     |              |            | rscc-0x000128E0 | 96                 | 0.05 %              | 85075C8556952FA6651C2468C8A0D588... | 2.488   | English-US | 01 00 FF FF 00 00 00 00 00 00 00 C8...    | .....@.....                |

Il primo screenshot mostra gli indicatori principali identificati con Pestudio, tra cui l'entry-point anomalo e l'assenza di debug.

Il secondo screenshot evidenzia la sezione risorse, con l'icona e la risorsa a elevata entropia.

### Detect It Easy (DIE)

Il file è stato analizzato utilizzando Detect It Easy, che ha confermato che si tratta di un eseguibile PE32 per sistemi Windows a 32 bit. L'analisi ha evidenziato la presenza di HeurPacker, indicando che il file è stato compresso, e una sezione . rsrc con un livello di entropia particolarmente alto, segno che potrebbe contenere dati cifrati o compressi.

| Nome file                                   | Dimensione file | Scansione  | Ordine dei byte | Modalità | Architettura | Tipo |
|---|-----------------|------------|-----------------|----------|--------------|------|
| C:\Users\flavem\Downloads\AdwareCleaner.exe | 190.82 KiB      | Automatica | LE              | 32-bit   | IA32         | GUI  |

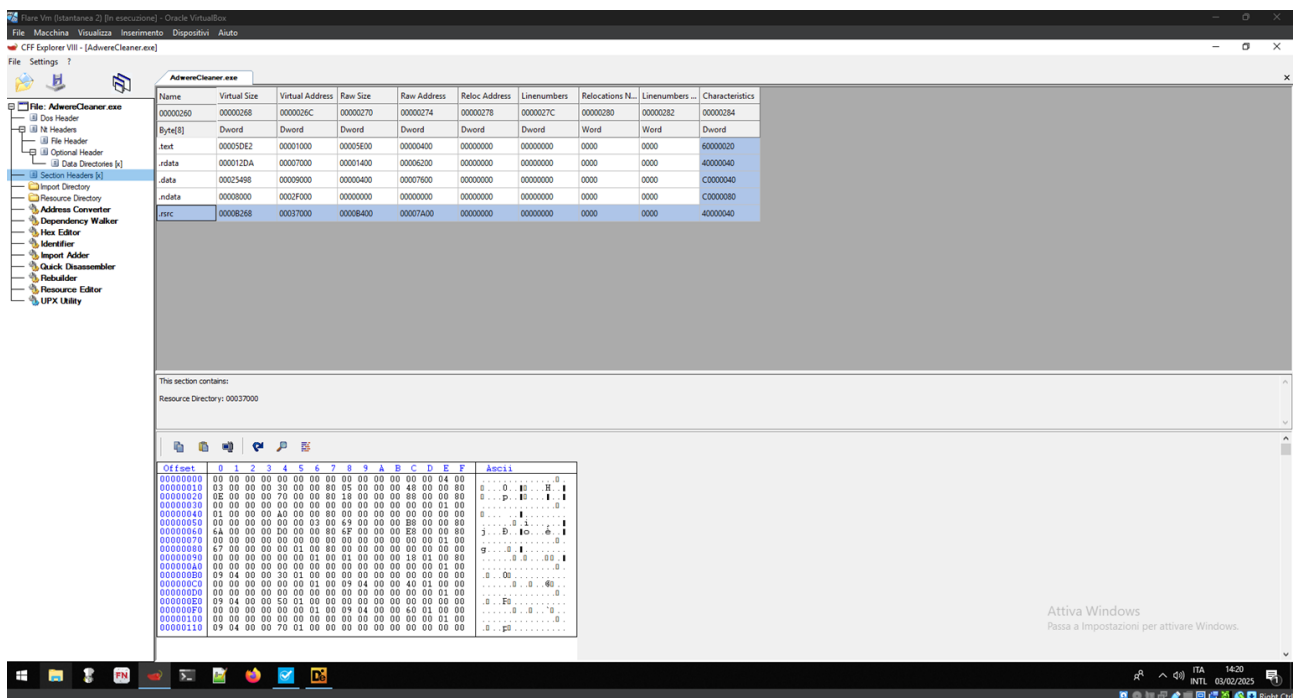
| PE32  | System | Language | Compiler                                | Installation                                       | Signature                                   | Archive                    | Data      |
|---|--------|----------|---|--|---|----------------------------|-----------|
| Windows 95/98/NT/2000/XP/2003/2008/2009/2012/2016/2019/2022 | C      | C        | Microsoft Visual C/C++ (13.10.4035) [C] | Nullsoft Scriptable Install System (3.0.2) [solid] | Binary/Offset=0x0012400;Dimension=0x001c640 | Raw Deflate stream (0x20h) | NSIS data |

Questo screenshot mostra le informazioni estratte tramite DIE, con l'indicazione della compressione e l'alta entropia della sezione `.rsrc`.

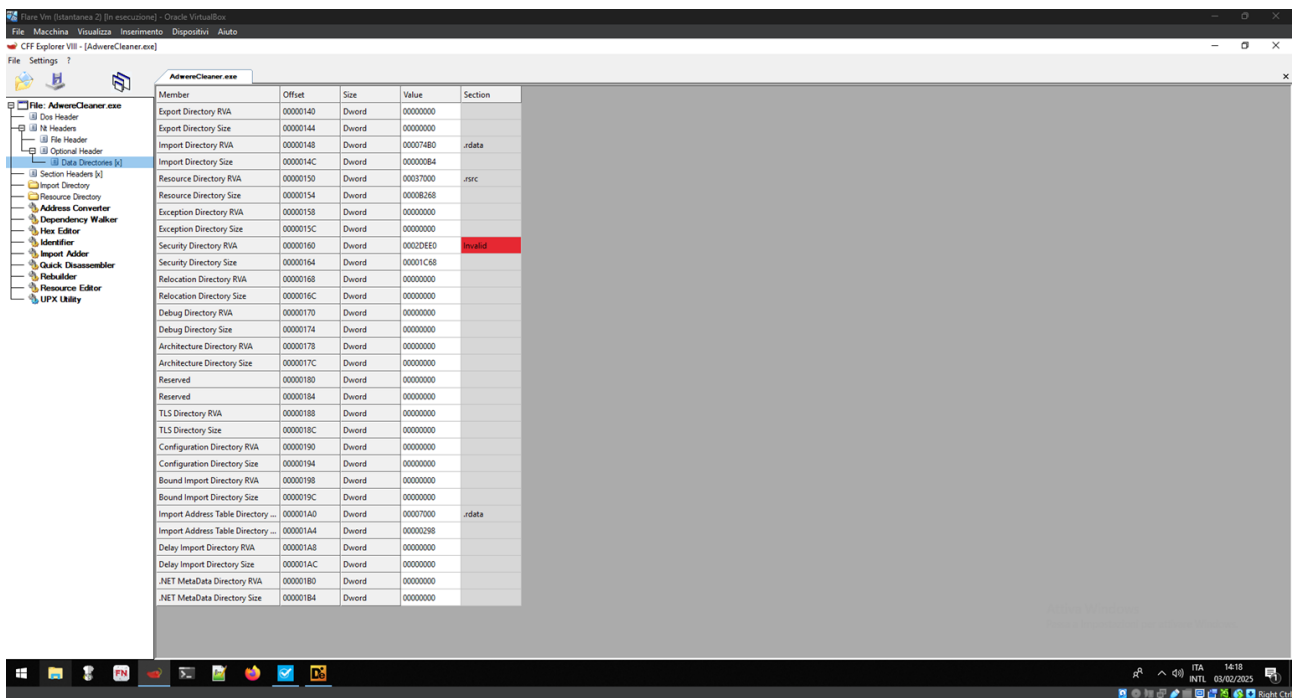
## CFF Explorer

L'analisi con CFF Explorer ha rivelato ulteriori dettagli interessanti. La directory `Security` del file presenta un RVA invalido, il che suggerisce una probabile manipolazione della firma digitale. Inoltre, la sezione `.rsrc`, già segnalata da DIE, conferma un'elevata entropia, potenzialmente indicativa di dati compressi o nascosti.

Un altro elemento critico emerso riguarda la Import Directory, che include riferimenti a librerie come `ADVAPI32.dll` e `SHELL32.dll`. Queste librerie sono spesso utilizzate dai malware per garantire persistenza o alterare il registro di sistema.



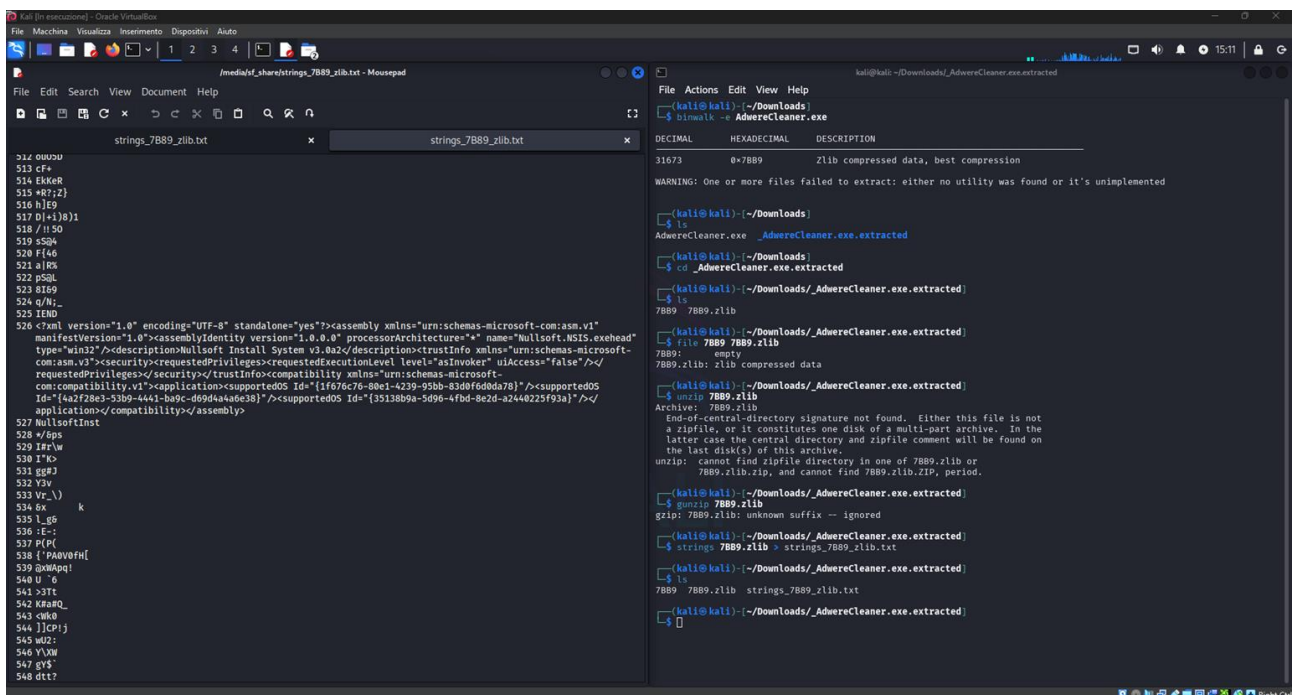
L'immagine mostra i dettagli delle sezioni, con particolare attenzione alla `.rsrc` e al suo livello di entropia.



Questo screenshot evidenzia l'RVA invalido della directory Security, che supporta l'ipotesi di manipolazione.

## Binwalk

L'utilizzo di Binwalk ("binwalk -e") ha generato una directory per i file estratti, ma non è stato possibile identificare componenti significativi. Questo potrebbe essere dovuto alla presenza di compressioni o cifrature non standard.



Lo screenshot illustra l'output di Binwalk durante il tentativo di estrazione dei file.

## Strings

Con il comando `strings`, è stato possibile estrarre stringhe leggibili dal file. Tra queste, sono stati individuati riferimenti a XML, descrizioni di sistema e alcune stringhe potenzialmente offuscate. Nonostante l'offuscamento, alcune di queste stringhe potrebbero rappresentare URL o comandi utilizzati dal malware.

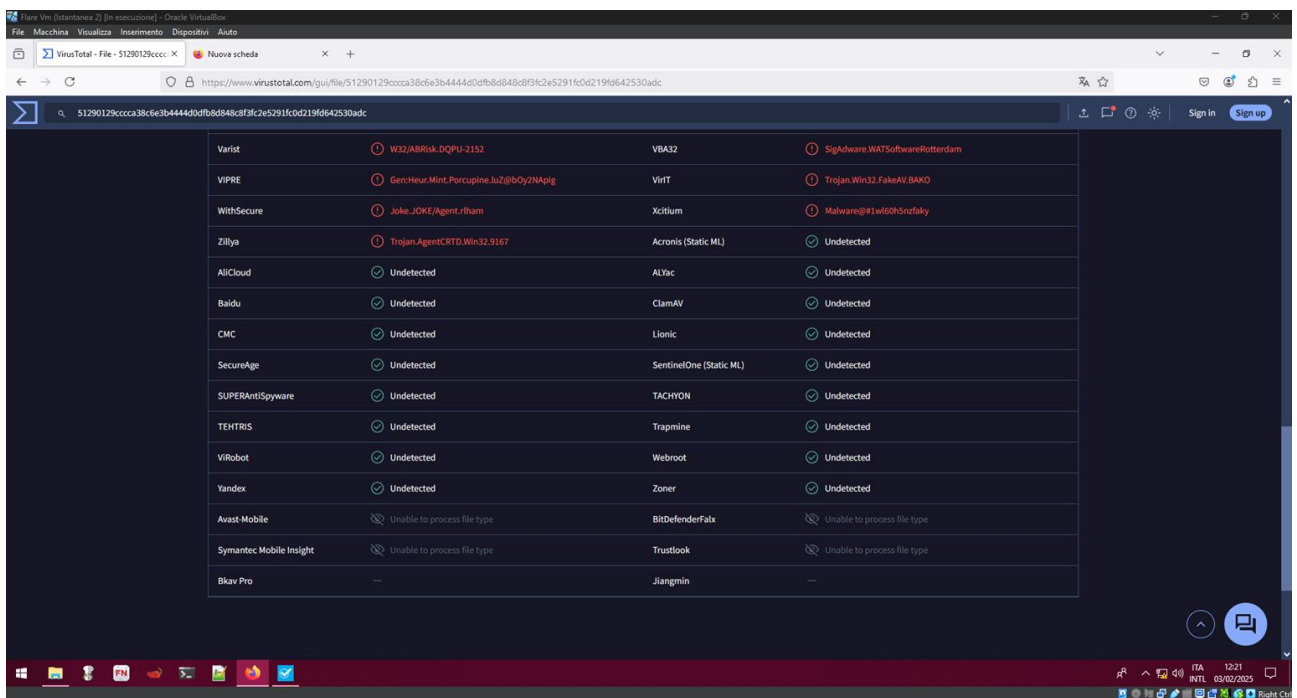
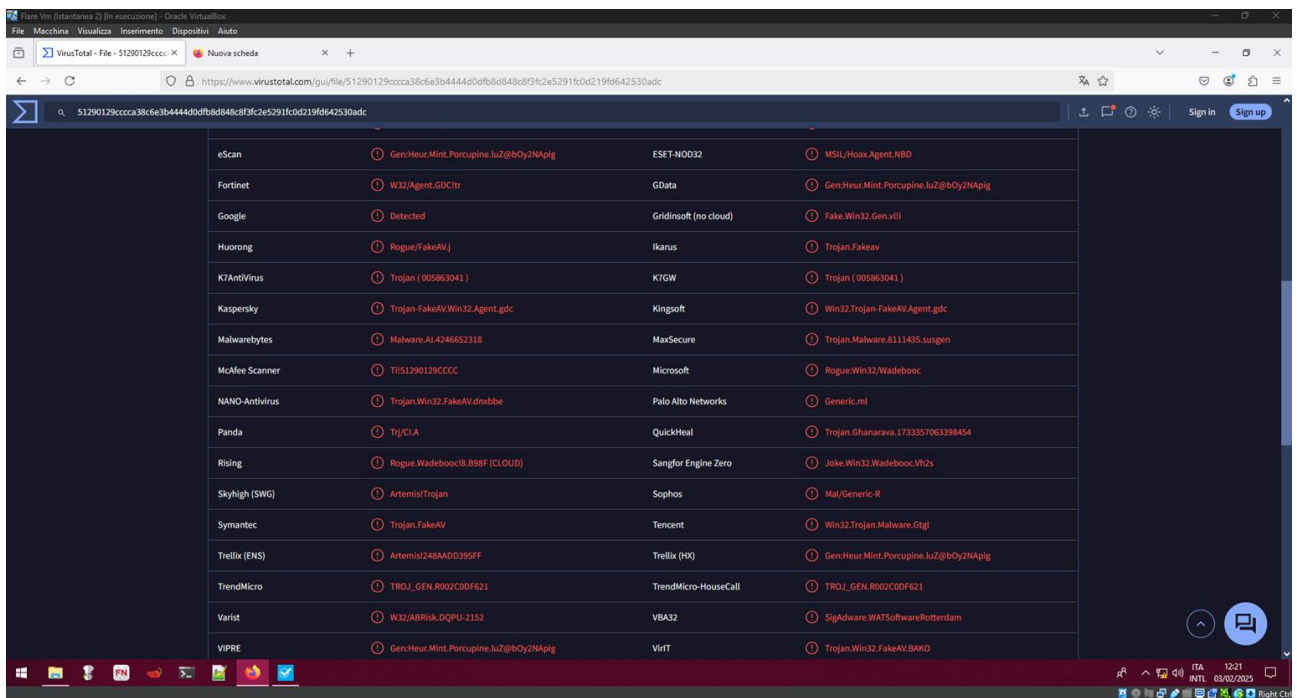
## VirusTotal

Infine, il file è stato caricato su VirusTotal, dove 53 motori antivirus su 70 lo hanno classificato come malevolo. L'analisi ha identificato il file come un Dropper o un Trojan, con riferimenti a categorie come FakeAV e Porcupine. Gli indicatori di comportamento, come "execute-dropped-file" e "invalid-signature", confermano la natura sospetta del file.

The screenshot displays the VirusTotal analysis interface for a file identified as `AdwareCleaner.exe`. The file's SHA-256 hash is `51290129cccca38c6e3b4444d0fb8d848c8f3c2e5291fc0d219f6642530adc`. The analysis shows that 53 out of 70 security vendors flagged the file as malicious, with a community score of -219. The file is classified as a `Dropper` and `Trojan`, with threat categories including `trojan` and `fakeav`. The file size is 190.82 KB, and the last analysis was performed 6 days ago. The analysis also identifies several behaviors, including `execute-dropped-file` and `invalid-signature`.

**Security vendors' analysis**

| Vendor             | Detection                           | Category    | Family                                  |
|--------------------|-------------------------------------|-------------|---|
| AhnLab-V3          | ⓘ Dropper/Win32.Dapato.R137988      | Alibaba     | ⓘ Hoax:MSIL/Porcupine.e66e0e97          |
| Antiy-AVL          | ⓘ HackTool[Hoax]/MSIL_Agent         | Arcabit     | ⓘ Trojan.Mint.Porcupine.ED5010          |
| Avast              | ⓘ Win32-FakeAV-FLW [Trj]            | AVG         | ⓘ Win32.FakeAV-FLW [Trj]                |
| Avira (no cloud)   | ⓘ JOKE/Agent.rham                   | BitDefender | ⓘ Gen:Heur.Mint.Porcupine.luZ@bOy2NApig |
| CrowdStrike Falcon | ⓘ Win/malicious_confidence_100% (W) | CTX         | ⓘ Exe.trojan.fakeav                     |
| Cylance            | ⓘ Unsafe                            | Cynet       | ⓘ Malicious (score: 99)                 |
| DeepInstinct       | ⓘ MALICIOUS                         | DrWeb       | ⓘ Trojan.FakeAV.17850                   |



Le immagini evidenziano i risultati dell'analisi su VirusTotal, con il tasso di rilevamento e i dettagli comportamentali.

## **Conclusioni**

L'analisi statica del file ha evidenziato numerosi indicatori di comportamenti malevoli. I dettagli tecnici confermano che il file presenta caratteristiche tipiche di un dropper o trojan, con potenziale capacità di persistenza, modifica del registro e distribuzione di payload nascosti.

## **Analisi Dinamica**





All done, please review results below

| Threat Name               | Malware Type | Danger Level | Location                          |
|---------------------------|--------------|--------------|-----------------------------------|
| Savings Toolbar           | Adware       | High         | HKCU\Software\Windows\Run         |
| Login Logger              | Spyware      | High         | HKCU\Software\Windows\Internet Ex |
| Trojan.Win32.StartPage.fx | Adware       | Low          | c:\windows\system32\ahmavi.dll    |
| WhenUSave                 | Adware       |              |                                   |
| Sovware Strike            | Adware       |              |                                   |

Infections Found: 13

Infections Cleanable: 13

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

AdwCleaner - Your one stop solution for Adware

### 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 upgrade to the full version.

On sale now!

**Only \$59,99**

Normal price: \$89,99. Sale ending on: 04/02/2025

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



L'esplo

### Introduzione al Malware:

Il file analizzato, **AdwareCleaner.exe**, si presenta come un software legittimo per la pulizia del sistema, ma una volta eseguito attiva una serie di comportamenti sospetti e dannosi. Il malware



compromette la sicurezza del sistema generando processi per scaricare ulteriori file, manipolare il registro di sistema e alterare configurazioni critiche.

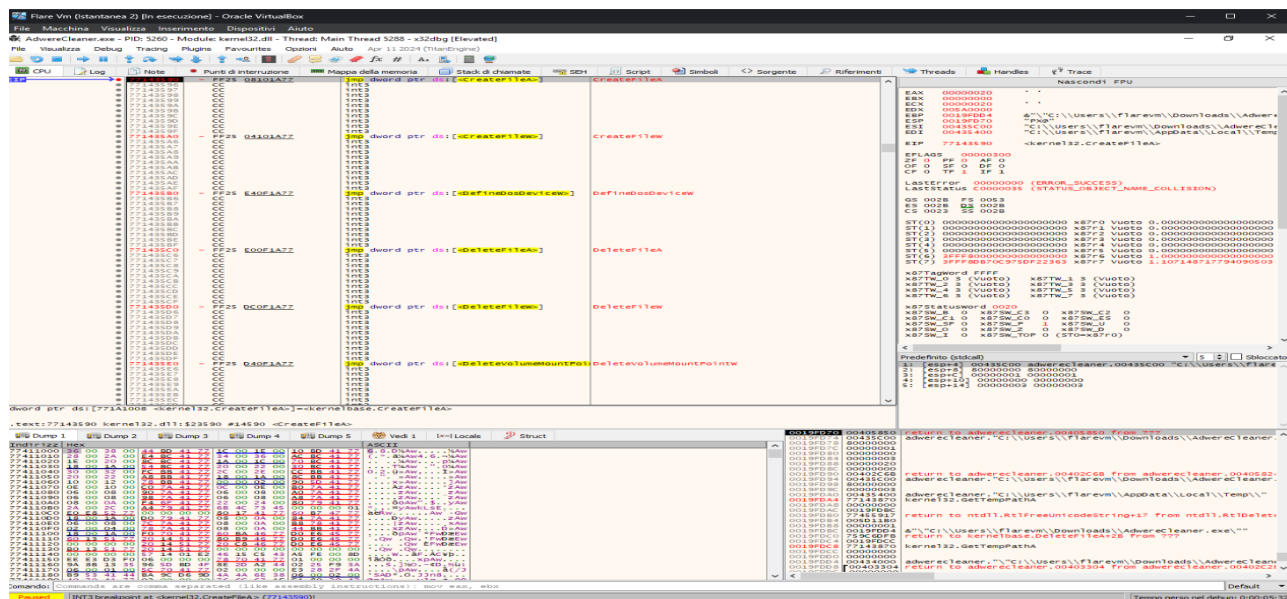
L'esecuzione del malware ha rivelato le seguenti attività:

### Modifiche al Registro di Sistema:

Il malware accede e modifica chiavi strategiche per ottenere persistenza:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet

| Process Monitor - Sysinternals: www.sysinternals.com |               |      |              |  |   |
|--|---------------|------|--------------|--|---|
| File Edit Event Filter Tools Options Help            |               |      |              |  |   |
| Process Monitor - Sysinternals: www.sysinternals.com |               |      |              |  |   |
| Time   | Process Name  | PID  | Operation    | Path   | Result / Detail   |
| 11:48...   | AdwareCleaner | 4788 | RegCreateKey | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SyncRootManager                | SUCCESS<br>Desired Access: Notify, Disposition: REG_OPENED_EXISTING_KEY                   |
| 11:48...   | AdwareCleaner | 4788 | RegCreateKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap               | SUCCESS<br>Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY               |
| 11:48...   | AdwareCleaner | 4788 | RegSetValue  | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass   | SUCCESS<br>Type: REG_DWORD, Length: 4, Data: 1  |
| 11:48...   | AdwareCleaner | 4788 | RegSetValue  | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName  | SUCCESS<br>Type: REG_DWORD, Length: 4, Data: 1  |
| 11:48...   | AdwareCleaner | 4788 | RegSetValue  | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet | SUCCESS<br>Type: REG_DWORD, Length: 4, Data: 1  |
| 11:48...   | AdwareCleaner | 4788 | RegSetValue  | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect    | SUCCESS<br>Type: REG_DWORD, Length: 4, Data: 0  |
| 11:48...   | AdwareCleaner | 4788 | RegSetValue  | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass   | SUCCESS<br>Type: REG_DWORD, Length: 4, Data: 1  |
| 11:48...   | AdwareCleaner | 4788 | RegSetValue  | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName  | SUCCESS<br>Type: REG_DWORD, Length: 4, Data: 1  |
| 11:48...   | AdwareCleaner | 4788 | RegSetValue  | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet | SUCCESS<br>Type: REG_DWORD, Length: 4, Data: 1  |
| 11:48...   | AdwareCleaner | 4788 | RegSetValue  | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect    | SUCCESS<br>Type: REG_DWORD, Length: 4, Data: 0  |
| 11:48...   | AdwareCleaner | 4788 | RegSetValue  | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475  | SUCCESS<br>Type: REG_BINARY, Length: 392, Data: 76 02 00 00 00 00 00 00 04 00 01 02 05 00 |



### Attività di Creazione e Gestione Processi:

L'analisi con x32dbg mostra l'uso di funzioni API critiche:

- CreateProcessA e CreateProcessAsUserA per la creazione di processi sospetti.
- CreateFileW e DeleteFileA per la manipolazione di file.

Flare Vm (Istantanea 2) [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Adwercleaner.exe - PID: 5260 - Module: kernel32.dll - Thread: Main Thread 5268 - x32dbg [Elevated]

File Visualizza Debug Tracing Plugins Favourites Opzioni Auto Apr 11 2024 (TitanEngine)

CPU Log Note Punti di interruzione Mappa della memoria Stack di chiamate SEH Script Simboli Sorgente Riferimenti Threads Handles Trace

77143590 CC FF25 08101A77 jmp dword ptr ds:[<CreateFileA>] CreateFileA

77143591 CC

77143592 CC

77143593 CC

77143594 CC

77143595 CC

77143596 CC

77143597 CC

77143598 CC

77143599 CC

771435A0 CC

771435A1 CC

771435A2 CC

771435A3 CC

771435A4 CC

771435A5 CC

771435A6 CC

771435A7 CC

771435A8 CC

771435A9 CC

771435AA CC

771435AB CC

771435AC CC

771435AD CC

771435AE CC

771435AF CC

771435B0 CC FF25 E40F1A77 jmp dword ptr ds:[<DefineDosDevice>] DefineDosDevice

771435B1 CC

771435B2 CC

771435B3 CC

771435B4 CC

771435B5 CC

771435B6 CC

771435B7 CC

771435B8 CC

771435B9 CC

771435BA CC

771435BB CC

771435BC CC

771435BD CC

771435BE CC

771435BF CC

771435C0 CC FF25 E00F1A77 jmp dword ptr ds:[<DeleteFileA>] DeleteFileA

771435C1 CC

771435C2 CC

771435C3 CC

771435C4 CC

771435C5 CC

771435C6 CC

771435C7 CC

771435C8 CC

771435C9 CC

771435CA CC

771435CB CC

771435CC CC

771435CD CC

771435CE CC

771435CF CC

771435D0 CC FF25 D00F1A77 jmp dword ptr ds:[<DeleteFileA>] DeleteFileA

771435D1 CC

771435D2 CC

771435D3 CC

771435D4 CC

771435D5 CC

771435D6 CC

771435D7 CC

771435D8 CC

771435D9 CC

771435DA CC

771435DB CC

771435DC CC

771435DD CC

771435DE CC

771435DF CC

771435E0 CC FF25 D40F1A77 jmp dword ptr ds:[<DeleteVolumeMountPoint>] DeleteVolumeMountPoint

771435E1 CC

771435E2 CC

771435E3 CC

771435E4 CC

771435E5 CC

771435E6 CC

771435E7 CC

771435E8 CC

771435E9 CC

771435EA CC

771435EB CC

771435EC CC

771435ED CC

dword ptr ds:[77141008 <kernel32.CreateFileA>] = <kernel32.CreateFileA>

.text:77143590 kernel32.dll:123590 #14590 <CreateFileA>

0019FD70 00405850 return to adwercleaner.00405850 from ???

0019FD74 00435C00 adwercleaner."C:\Users\flarevm\Downloads\Adwercleaner.exe"

0019FD78 80000000

0019FD7C 00000001

0019FD80 00000000

0019FD84 00000003

0019FD88 00000020

0019FD8C 00000000

0019FD90 00402C68 return to adwercleaner.00402C68 from adwercleaner.0040582c

0019FD94 00435C00 adwercleaner."C:\Users\flarevm\Downloads\Adwercleaner.exe"

0019FD98 80000000

0019FD9C 00000003

0019FDA0 00435400 adwercleaner."C:\Users\flarevm\AppData\Local\Temp\kernel32.GetTempPathA"

0019FDA4 77143870

0019FDA8 00000000

0019FDAC 0019FDBC return to ntddl.RtlFreeUnicodeString+17 from ntddl.RtlDeleteUnicodeString+17

0019FDB0 77455917

0019FDB4 005D1180

0019FDB8 00000001

0019FDBC 0019FDD4

0019FDC0 753C0F8

0019FDC4 0019FDDC

0019FDC8 77143870

0019FDCC 00000000

0019FDD0 00000000

0019FDD4 00435400

0019FDD8 00403304 return to adwercleaner.00403304 from adwercleaner.00402C21

0019FDE0 00000000

Commands are comma separated (like assembly instructions): mov eax, ebx

Paused [INT3 breakpoint at <kernel32.CreateFileA> (77143590)]

Tempo perso nel debug: 0:00:05:32

## Persistenza e Auto-Avvio:

Il malware garantisce la persistenza configurando chiavi di avvio automatico nel registro (HKEY/Run).



## Comunicazioni di Rete:

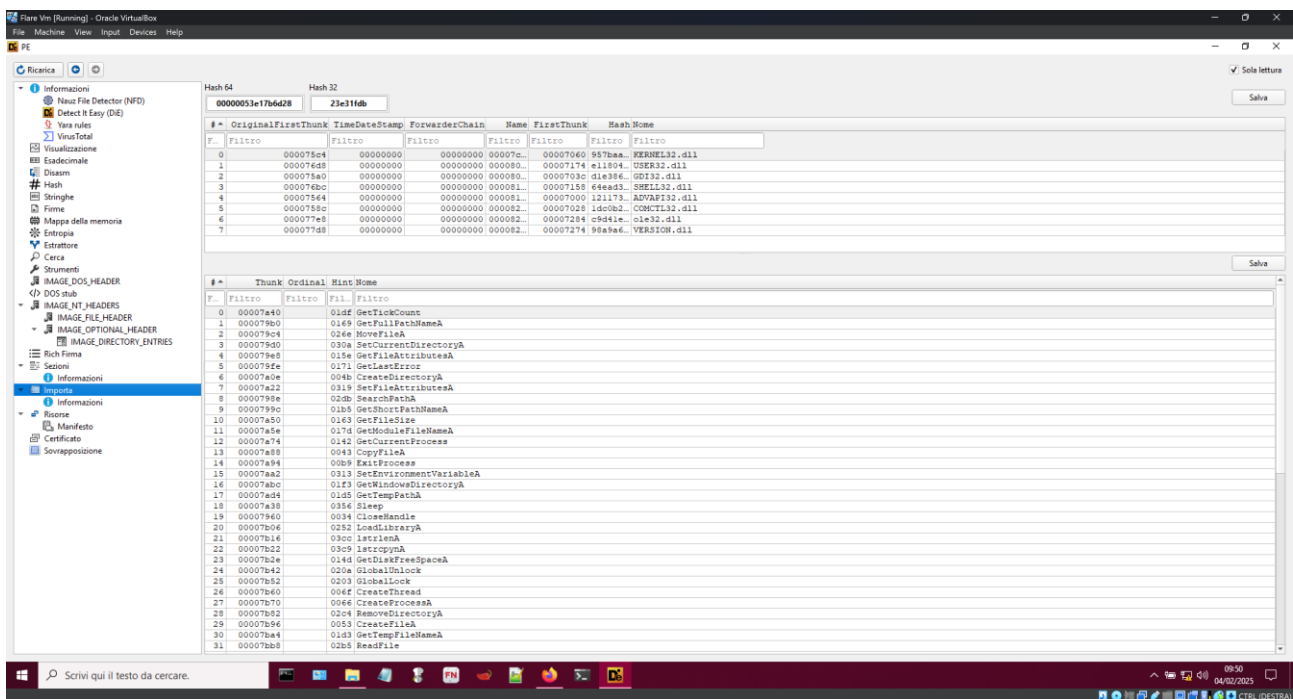
Il traffico monitorato con Wireshark ha evidenziato connessioni verso IP sospetti e richieste TCP non autorizzate.

|          |           |                          |                        |
|----------|-----------|--------------------------|------------------------|
|          |           |                          | 2.16.164.82            |
|          |           |                          | 2.16.164.81            |
|          |           |                          | 2.16.164.24            |
|          |           |                          | 2.16.164.89            |
| BEFORE   | Responded | google.com               | 142.250.185.78         |
| BEFORE   | Responded | www.microsoft.com        | 95.101.149.131         |
| 9256 ms  | Requested | www.vikingwebscanner.com | IP Addresses not found |
|          |           |                          | 2.21.65.157            |
| 11275 ms | Responded | www.bing.com             | 2.21.65.132            |
|          |           |                          | 2.21.65.154            |
|          |           |                          | 2.21.65.153            |
| 14395 ms | Responded | go.microsoft.com         | 184.28.89.167          |

## Analisi delle Librerie e API Importate:

Il malware sfrutta diverse API critiche per eseguire operazioni malevole:

- MoveFileA, DeleteFileA, CreateProcessA (gestione file e processi).
- SetCurrentDirectoryA, ShellExecuteA (modifica ambienti di lavoro).
- GlobalAlloc, GlobalFree, ReadFile, WriteFile (gestione memoria e file).



## Conclusioni:

Il malware AdwareCleaner.exe sfrutta tecniche classiche per ottenere persistenza, eludere i meccanismi di sicurezza e stabilire una connessione remota per il controllo del sistema. Le modifiche alle chiavi di registro e le API invocate indicano comportamenti tipici di un dropper o backdoor.

## Suggerimenti per la Difesa:

- Monitorare regolarmente le chiavi di registro critiche.
- Analizzare il traffico di rete in uscita per individuare connessioni sospette.

- Utilizzare strumenti di sandboxing per testare software sospetti prima della distribuzione.

## **Raccomandazioni Finali:**

### **Isolamento e Contenimento:**

- Isolare immediatamente il sistema infetto per limitare la diffusione del malware su eventuali reti aziendali.
- Disattivare temporaneamente le connessioni di rete per prevenire ulteriori comunicazioni con server C2 (Command and Control).

### **Analisi Approfondita del Sistema:**

- Effettuare una scansione completa del sistema con software anti-malware aggiornati.
- Verificare la presenza di processi sospetti in esecuzione, file anomali e configurazioni del registro di sistema alterate.

### **Ripristino delle Configurazioni Compromesse:**

- Ripristinare le impostazioni di sicurezza del sistema e rimuovere le chiavi di registro modificate dal malware.
- Controllare le configurazioni di rete, inclusi proxy e DNS, per individuare modifiche non autorizzate.

### **Prevenzione e Sicurezza Proattiva:**

- Implementare soluzioni EDR (Endpoint Detection and Response) per il monitoraggio continuo delle attività sospette.
- Abilitare il logging avanzato e la registrazione degli eventi per facilitare l'individuazione di comportamenti anomali in futuro.

### **Formazione e Consapevolezza:**



- Condurre sessioni di formazione per il personale, focalizzate sul riconoscimento di tentativi di phishing e pratiche di sicurezza informatica.
- Promuovere una cultura della sicurezza informatica per ridurre il rischio umano, spesso il punto più vulnerabile.


### **Piano di Risposta agli Incidenti:**

- Aggiornare o implementare un piano di risposta agli incidenti per gestire efficacemente futuri attacchi.
- Effettuare simulazioni periodiche per testare la reattività del team IT e del personale coinvolto nella gestione delle emergenze.

## General Info

☒ Add for printing 

File name: AdwereCleaner.exe  
Full analysis: <https://app.any.run/tasks/702e863d-30e8-4d62-9d31-fef7980335d1>  
Verdict: **No threats detected**  
Analysis date: February 04, 2025 at 12:46:27  
OS: Windows 10 Professional (build: 19045, 64 bit)  
Indicators:    
MIME: application/vnd.microsoft.portable-executable  
File info: PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive, 5 sections  
MD5: 248AADD395FFA7FFB1670392A9398454  
SHA1: C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5  
SHA256: 51290129CCCCA38C6E3B4444D0DFB8D848C8F3FC2E5291FC0D219FD642530ADC  
SSDEEP: 3072:15TDpNFVbxDSXJFFGhcBR1WLZ37p73G8Wn7GID0g+ELqdSxo5XtIzJnvxRJgghaR:157TcfFPB6B3GL7g+me5aZjn5VII9T/

 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

## Behavior activities

☒ Add for printing 

### MALICIOUS


No malicious indicators.

### SUSPICIOUS

Reads security settings of Internet Explorer  
• AdwereCleaner.exe (PID: 6336)  
Executable content was dropped or overwritten  
• AdwereCleaner.exe (PID: 6336)

### INFO

Checks supported languages  
• AdwereCleaner.exe (PID: 6336)  
Process checks computer location settings  
• AdwereCleaner.exe (PID: 6336)  
Reads the computer name  
• AdwereCleaner.exe (PID: 6336)

 Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the [full report](#) 

## Malware configuration

☒ Add for printing 

No Malware configuration.

Static information

☒ Add for printing

TRiD

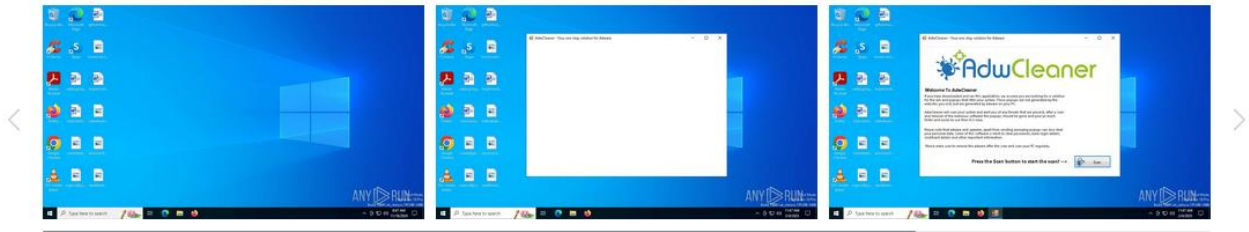
|      |  |  |
|------|--|--|
| .exe |  | NSIS - Nullsoft Scriptable Install System (91.9) |
| .exe |  | Win32 Executable MS Visual C++ (generic) (3.3)   |
| .exe |  | Win64 Executable (generic) (3)                   |
| .dll |  | Win32 Dynamic Link Library (generic) (0.7)       |
| .exe |  | Win32 Executable (generic) (0.4)                 |

EXIF

|                           |   |
|---------------------------|---|
| EXE                       |   |
| Subsystem:                | Windows GUI   |
| SubsystemVersion:         | 4   |
| ImageVersion:             | 6   |
| OSVersion:                | 4   |
| EntryPoint:               | 0x30e4  |
| UninitializedDataSize:    | 1024  |
| InitializedDataSize:      | 162816  |
| CodeSize:                 | 24064   |
| LinkerVersion:            | 6   |
| PEType:                   | PE32  |
| ImageFileCharacteristics: | No relocs, Executable, No line numbers, No symbols, 3 2-bit |
| TimeStamp:                | 2013:12:25 05:01:41+00:00                                   |
| MachineType:              | Intel 386 or later, and compatibles                         |

Video and screenshots

☒ Add for printing



All screenshots are available in the [full report](#)

Processes

☒ Add for printing

|                 |                     |                     |                      |
|-----------------|---------------------|---------------------|----------------------|
| Total processes | Monitored processes | Malicious processes | Suspicious processes |
| 125             | 2                   | 0                   | 0                    |

|          |           |   |                          |
|----------|-----------|---|--------------------------|
|          |           |   | 2.16.164.82              |
|          |           |   | 2.16.164.81              |
|          |           |   | 2.16.164.24              |
|          |           |   | 2.16.164.89              |
| BEFORE   | Responded | ✓ | google.com               |
| BEFORE   | Responded | ✓ | www.microsoft.com        |
| 9256 ms  | Requested | 🔥 | www.vikingwebscanner.com |
|          |           |   | IP Addresses not found   |
|          |           |   | 2.21.65.157              |
| 11275 ms | Responded | ✓ | www.bing.com             |
|          |           |   | 2.21.65.132              |
|          |           |   | 2.21.65.154              |
|          |           |   | 2.21.65.153              |
| 14395 ms | Responded | ✓ | go.microsoft.com         |
|          |           |   | 184.28.89.167            |

