

Analisi Statica

Definizione

Tecnica di analisi che consiste nell'analisi del malware senza eseguirlo. Si avvale dell'uso di software di analisi del codice e/o componenti dei file per analizzare:

- Struttura dei file
- Stringhe
- Chiamate di sistema
- Metadati

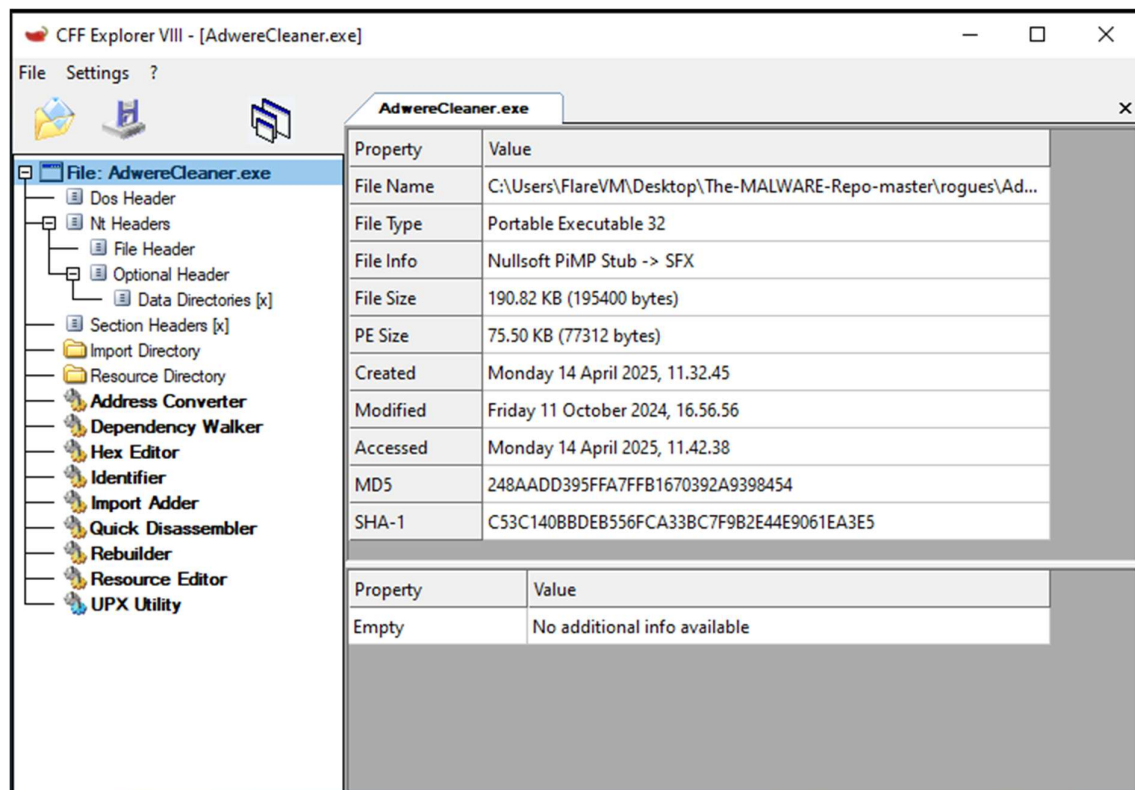
Al fine di ottenere informazioni preliminari sul comportamento potenziale del malware.

Tools Utilizzati

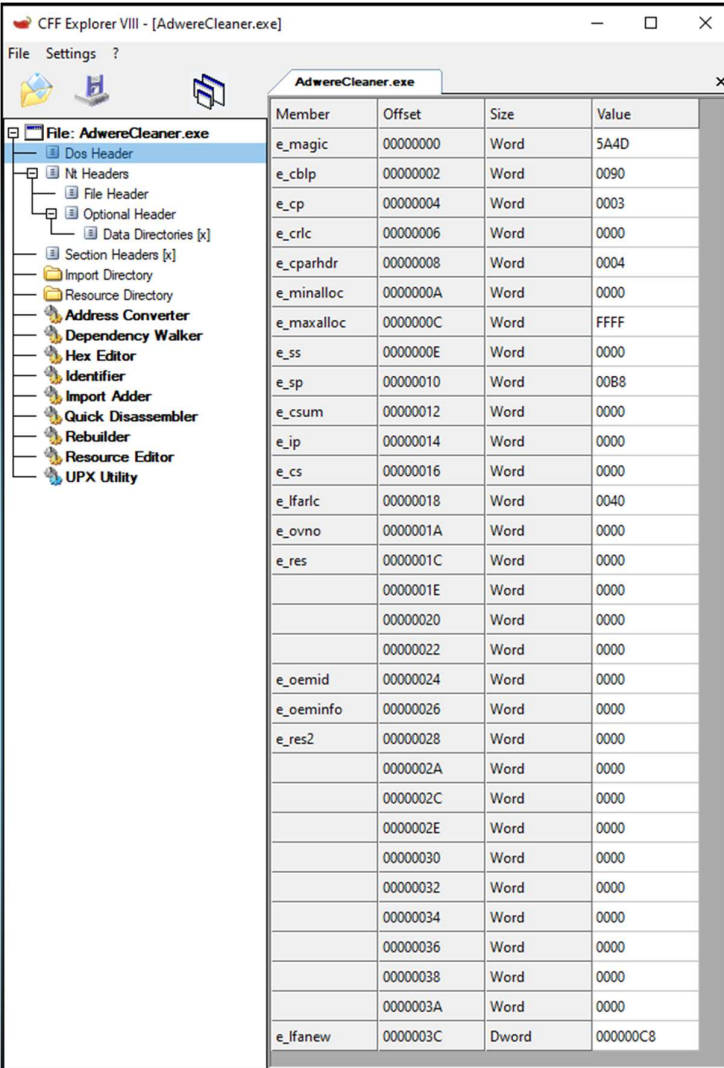
- CFF Explore VIII

CFF Explore VIII

CFF Explorer è un potente e versatile strumento gratuito per l'analisi e la modifica di file eseguibili Portable Executable (PE), formato standard per gli eseguibili in ambiente Windows. Permette di esaminare in dettaglio la struttura interna dei suddetti file.



Analisi Dos Header:



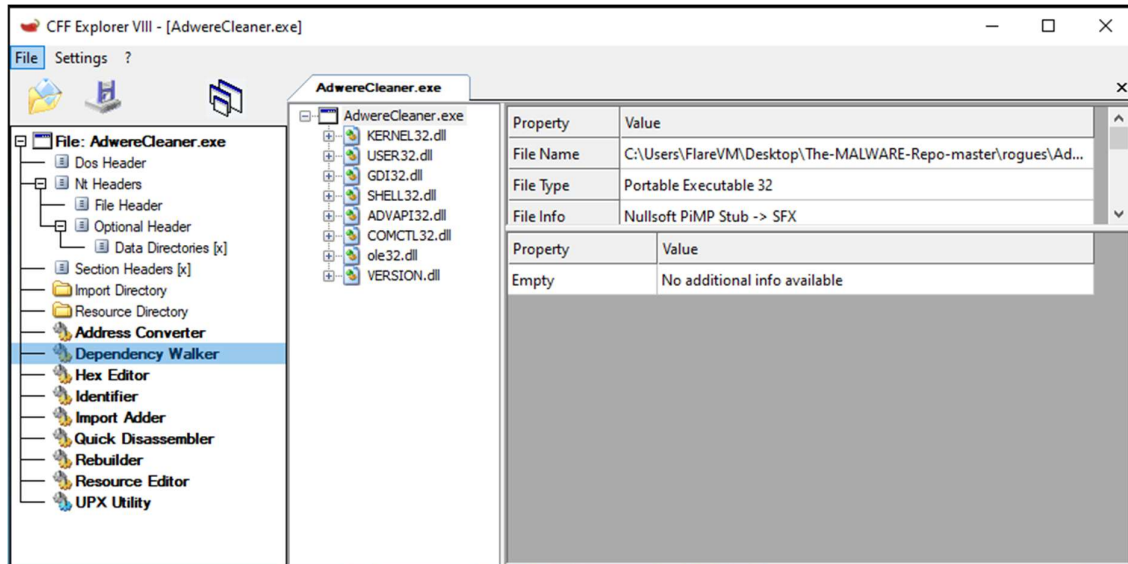
Member	Offset	Size	Value
e_magic	00000000	Word	5A4D
e_cblp	00000002	Word	0090
e_cp	00000004	Word	0003
e_crlc	00000006	Word	0000
e_cparhdr	00000008	Word	0004
e_minalloc	0000000A	Word	0000
e_maxalloc	0000000C	Word	FFFF
e_ss	0000000E	Word	0000
e_sp	00000010	Word	00B8
e_csum	00000012	Word	0000
e_ip	00000014	Word	0000
e_cs	00000016	Word	0000
e_lfarlc	00000018	Word	0040
e_ovno	0000001A	Word	0000
e_res	0000001C	Word	0000
	0000001E	Word	0000
	00000020	Word	0000
	00000022	Word	0000
e_oemid	00000024	Word	0000
e_oeminfo	00000026	Word	0000
e_res2	00000028	Word	0000
	0000002A	Word	0000
	0000002C	Word	0000
	0000002E	Word	0000
	00000030	Word	0000
	00000032	Word	0000
	00000034	Word	0000
	00000036	Word	0000
	00000038	Word	0000
	0000003A	Word	0000
e_lfanew	0000003C	Dword	000000C8

- e_magic: 5A4D -> Questo è il campo di firma del DOS Header. Il valore 5A4D corrisponde alle lettere "MZ" in ASCII, che è la firma standard per un file eseguibile DOS e indica che il file è un eseguibile valido
- e_cblp: 0090 -> Byte rimanenti nella pagina del file. Indica il numero di byte utilizzati nella pagina finale del file.
- e_cp: 0003 -> Numero di pagine nel file. Il file è suddiviso in pagine da 512 byte ciascuna.
- e_crlc: 0000 -> Numero di voci nel file di rilocalizzazione. Indica che non ci sono voci di rilocalizzazione.
- e_cparhdr: 0004 -> Dimensione dell'header in paragrafi. Indica la dimensione dell'header del DOS in paragrafi (1 paragrafo = 16 byte).
- e_minalloc: 0000 -> Minimo di paragrafi aggiuntivi necessari. Indica la quantità minima di memoria aggiuntiva richiesta dal programma.
- e_maxalloc: FFFF -> Massimo di paragrafi aggiuntivi necessari. Indica la quantità massima di memoria aggiuntiva richiesta dal programma.
- e_ss: 0000 -> Registro stack segment. Indica il segmento del registro stack.
- e_sp: 00B8 -> Registro stack pointer. Indica il puntatore dello stack iniziale.
- e_csum: 0000 -> Checksum del file. Non utilizzato spesso.
- e_ip: 0000 -> Registro instruction pointer. Indica l'offset iniziale dell'istruzione di esecuzione.
- e_cs: 0000 -> Registro code segment. Indica il segmento iniziale del codice.
- e_lfarlc: 0040 -> Offset dell'array delle voci di rilocalizzazione. Indica l'offset nel file dove

iniziano le voci di rilocazione.

- e_ovno: 0000 -> Numero dell'overlay.
- e_res: 0000 -> Riservato. Questi campi sono riservati e non utilizzati.
- e_oemid: 0000 -> Identificatore OEM (original equipment manufacturer). Non utilizzato spesso.
- e_oeminfo: 0000 -> Informazioni OEM. Non utilizzato spesso.
- e_res2: 0000 -> Riservato. Questi campi sono riservati e non utilizzati.
- e_lfanew: 000000C8 -> Offset al nuovo header. Indica l'offset nel file dove inizia il NT Header, che è la parte successiva dell'header PE.

Analisi Dependency Walker



DLL utilizzate:

- KERNEL32.dll => fornisce funzioni per la gestione della memoria e le operazioni di input/output
- USER32.dll => fornisce funzioni per creare e gestire le interfacce utente e gestire gli input forniti dall'utente
- GDI32.dll => fornisce funzioni per la creazione di oggetti bidimensionali
- SHELL32.dll => fornisce funzioni per la gestione della GUI, funzioni per avviare applicazioni
- ADVAPI32.dll => funzioni avanzate di basso livello per la gestione del sistema come interagire con i registri di sistema, funzioni per la gestione della sicurezza e il controllo di account utente
- COMCTL32.dll => fornisce controlli comuni della GUI
- ole32.dll => responsabile dell'implementazione e della gestione della tecnologia OLE (Object Linking and Embedding) e di COM (Component Object Model)
- VERSION.dll => funzioni per gestire e recuperare informazioni sulla versione dei file

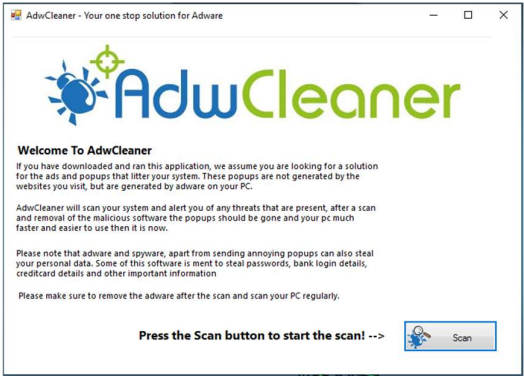
Analisi Dinamica

Definizione

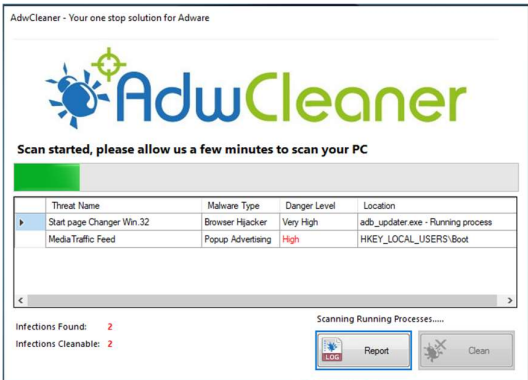
Tecnica di analisi di malware che mira nel comprendere il comportamento effettivo del programma. A differenza dell'analisi statica, l'analisi dinamica si effettua eseguendo il programma in un ambiente controllato, isolato e sicuro.

Esecuzione

L'esecuzione del file AdwareCleaner.exe crea una GUI che informa dello scopo del tool e presenta il Button per avviare la scansione



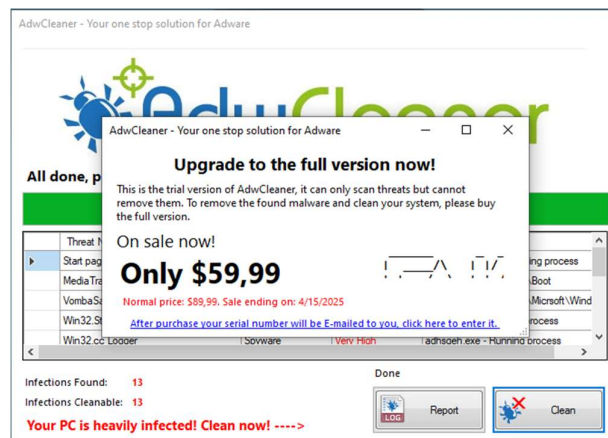
La pressione del Button cambia la GUI visualizzando una barra di progressione ad evidenziare l'avanzamento della scansione dell'intero sistema



Al completamento della scansione viene data la possibilità di “Pulire” il sistema



La pressione del pulsante “Clean” rimanda alla richiesta di effettuare l’upgrade, mezzo pagamento di \$59.99, per completare la rimozione dei file dannosi trovati.



Tools Utilizzati

- FlareVM
- Regshot 1.9.1
- FakeNet-NG 3.3
- Procmon

Regshot 1.9.1

Tool che permette di creare delle istantanee al registro di sistema di windows e generare un report in cui evidenzia le modifiche tra esse.

Viene utilizzato, catturando le istantanee prima e dopo l’esecuzione di un programma, per comprendere le modifiche che questo apporta sul registro di windows.

Modifiche apportate:

- Chiavi rimosse: 5

```
-----
Keys deleted: 5
-----
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\8a415067-ae91-486e-964b-258fdebe2c
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\8a415067-ae91-486e-964b-258fdebe2c
HKU\S-1-5-21-2617614941-1830582806-2752615194-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012025032420250415
```

Rimuove le chiavi contenenti le GPO e la cache del browser

- Chiavi aggiunte: 7
 - Ricrea la chiave della cache in un nuovo percorso
 - Crea le chiavi per il file tracing nel debug
- Valori aggiunti: 34

```
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableAutoFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\ConsoleTracingMask: 0xFFFF0000
```

- I valori nelle chiavi per il tracciamento dei file sono settati a 0 disabilitando il file tracing ai fini di debug sull’eseguibile

```
HKU\S-1-5-21-2617614941-1830582806-2752615194-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012025041420250415
```


- Ripopola la cache del browser con valori diversi da quelli rimossi
- Aggiunge l'avvio dell'eseguibile "6AdwCleaner.exe" all'avvio del sistema
- Popola chiavi con valori che ha ricevuto in risposta dal tool Fakenet

- Valori modificati: 24

FakeNet-NG è un tool di analisi della rete per analisi di malware e penetration testers. È un tool open-source ed è progettato per le ultime versioni di Windows.

Traffico di rete intercettato

1. Il processo con PID 4656 - 6AdwCleaner.exe – invia richiesta GET all’indirizzo www.vikingwebscanner.com/scripts/new_install.php?owner=6AdwCleaner
2. Il processo con PID 4656 - 6AdwCleaner.exe – invia richiesta GET all’indirizzo www.vikingwebscanner.com/scripts/status.php?action=scan&id=

www.vikingwebscanner.com/scripts/status.php?action=scan&id=

```
<html><head><title>FakeNet-NG</title></head><body><pre>HTTP LISTENER</pre></body></html>
```

- ocsp.usertrust.com
- ocsp.comodoca.com

```

D:\Server>
6AdwCleaner.exe (4656) requested UDP 192.168.56.102:53
DNS Server> Received A request for domain "ocsp.usertrust.com" from 6AdwCleaner.exe (4656)
6AdwCleaner.exe (4656) requested TCP 192.0.2.123:80
HTTPListener00 GET /MFwEwT2BMEswSJa2BgUrDgMCGuUAB8T161MY2X2B1PobAtwryIFz2BFgUduvWUQK8Ngq7OoYUqrTc5R8R14uHw4FLgCBBuWuX2F1VAjXJMGAB20RdbS3D HTTP/1.1
HTTPListener00 Connection: Keep-Alive
HTTPListener00 Accept: */*
HTTPListener00 User-Agent: Microsoft-CryptoAPI/10.0
HTTPListener00 Host: ocsp.usertrust.com
HTTPListener00
HTTPListener00
Diverter> 6AdwCleaner.exe (4656) requested UDP 192.168.56.102:53
DNS Server> Received A request for domain "ocsp.usertrust.com" from 6AdwCleaner.exe (4656)
Diverter> 6AdwCleaner.exe (4656) requested TCP 192.0.2.123:80
HTTPListener00 POST / HTTP/1.1
HTTPListener00 Cache-Control: no-cache
HTTPListener00 Connection: Keep-Alive
HTTPListener00 Pragma: no-cache
HTTPListener00 Content-Type: application/ocsp-request
HTTPListener00 Accept: */*
HTTPListener00 User-Agent: Microsoft-CryptoAPI/10.0
HTTPListener00 Content-Length: 83
HTTPListener00 Host: ocsp.usertrust.com
HTTPListener00
HTTPListener00
HTTPListener00 b' 0Q00M0K0I0(\t\x06\x05\x0e\x03\x02\x1a\x05\x00\x04\x14\x0e\x07\x0a\x0c\x02\x0e\x08\x07'
HTTPListener00 b' \xf2 \x85\x05\x1d\x0f\x04\x14\x03\x0b\x0e\x09\x0f\x0d\x0c\x0b\x02\x10\x10p\x0d\x0f\x08\x08\x0e\x0a\x09\x0b'
HTTPListener00 Storing HTTP POST headers and data to http_20250414_151206.txt.
Diverter> 6AdwCleaner.exe (4656) requested UDP 192.168.56.102:53
DNS Server> Received A request for domain "crl.usertrust.com" from 6AdwCleaner.exe (4656)
Diverter> 6AdwCleaner.exe (4656) requested TCP 192.0.2.123:80
HTTPListener00 GET /UTH-USERFirst-Object.crl HTTP/1.1
HTTPListener00 Connection: Keep-Alive
HTTPListener00 Accept: */*
HTTPListener00 User-Agent: Microsoft-CryptoAPI/10.0
HTTPListener00 Host: crl.usertrust.com
HTTPListener00
HTTPListener00
HTTPListener00
Diverter> 6AdwCleaner.exe (4656) requested UDP 192.168.56.102:53
DNS Server> Received A request for domain "ocsp.comodoca.com" from 6AdwCleaner.exe (4656)
Diverter> 6AdwCleaner.exe (4656) requested TCP 192.0.2.123:80
HTTPListener00 GET /MFwEwT2BMEswSJa2BgUrDgMCGuUAB8S0JaE2H4HHYQ:P74hlUo41NG32BEAQUHsWkLH2H3gofCw8DA0EPP73pCEFG6C5JCS84m1WDF5zbhNqI3D HTTP/1.1
HTTPListener00 Connection: Keep-Alive
HTTPListener00 Accept: */*
HTTPListener00 User-Agent: Microsoft-CryptoAPI/10.0
HTTPListener00 Host: ocsp.comodoca.com
HTTPListener00
HTTPListener00
HTTPListener00
Diverter> 6AdwCleaner.exe (4656) requested UDP 192.168.56.102:53
DNS Server> Received A request for domain "ocsp.comodoca.com" from 6AdwCleaner.exe (4656)
Diverter> 6AdwCleaner.exe (4656) requested TCP 192.0.2.123:80
HTTPListener00 POST / HTTP/1.1
HTTPListener00 Cache-Control: no-cache
HTTPListener00 Connection: Keep-Alive
HTTPListener00 Pragma: no-cache
HTTPListener00 Content-Type: application/ocsp-request
HTTPListener00 Accept: */*
HTTPListener00 User-Agent: Microsoft-CryptoAPI/10.0
HTTPListener00 Content-Length: 83
HTTPListener00 Host: ocsp.comodoca.com
HTTPListener00
HTTPListener00
HTTPListener00
HTTPListener00 b' 0Q00M0K0I0(\t\x06\x05\x0e\x03\x02\x1a\x05\x00\x04\x14\x0e\x07\x0a\x0c\x02\x0e\x08\x07'
HTTPListener00 b' \xf2 \x85\x05\x1d\x0f\x04\x14\x03\x0b\x0e\x09\x0f\x0d\x0c\x0b\x02\x10\x10p\x0d\x0f\x08\x08\x0e\x0a\x09\x0b'
HTTPListener00 Storing HTTP POST headers and data to http_20250414_151206.txt.
Diverter> 6AdwCleaner.exe (4656) requested UDP 192.168.56.102:53
DNS Server> Received A request for domain "crl.comodoca.com" from 6AdwCleaner.exe (4656)
Diverter> 6AdwCleaner.exe (4656) requested TCP 192.0.2.123:80
HTTPListener00 GET /COMODOCodeSigningC2.crl HTTP/1.1
HTTPListener00 Connection: Keep-Alive
HTTPListener00 Accept: */*
HTTPListener00 User-Agent: Microsoft-CryptoAPI/10.0
HTTPListener00 Host: crl.comodoca.com
HTTPListener00

```

4. La pressione del pulsante “Clean” avvia le richieste GET visualizzate nell’immagine sottostante

[illegible]

Come si può notare dallo screenshot successivo, la parte a destra della finestra è stata popolata da informazioni ricevute tramite una GET

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 buy the full version.

On sale now!

Only \$59,99

Normal price: \$89,99. Sale ending on: 4/15/2025

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

Procmon

Per analizzare nello specifico il malware abbiamo usufruito di Procmon, un tool che registra tutte le azioni che avvengono nel pc.

Analizzando il malware con esso è stato possibile vedere le modifiche avvenute nel "windows registry" da parte di "AdwereCleaner" e il secondo software installato inconsapevolmente "6AdwCleaner".

Alcune operazioni compiute all'avvio di AdwereCleaner

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
18:29:...	AdwereCleaner...	5652	Process Start		SUCCESS	Parent PID: 4784, ...
18:29:...	AdwereCleaner...	5652	Thread Create		SUCCESS	Thread ID: 6788
18:29:...	AdwereCleaner...	5652	Load Image	C:\Users\FlareVM\Desktop\Malware\ro...	SUCCESS	Image Base: 0x400...
18:29:...	AdwereCleaner...	5652	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffe...
18:29:...	AdwereCleaner...	5652	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x775...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
18:29:...	AdwereCleaner...	5652	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
18:29:...	AdwereCleaner...	5652	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
18:29:...	AdwereCleaner...	5652	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
18:29:...	AdwereCleaner...	5652	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ffe...
18:29:...	AdwereCleaner...	5652	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ffe...
18:29:...	AdwereCleaner...	5652	QueryOpen	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	
18:29:...	AdwereCleaner...	5652	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
18:29:...	AdwereCleaner...	5652	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
18:29:...	AdwereCleaner...	5652	CloseFile	C:\Windows	SUCCESS	
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\Software\Microsoft\Wow64\86	SUCCESS	Desired Access: R...
18:29:...	AdwereCleaner...	5652	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	NAME NOT FOUND	Length: 520
18:29:...	AdwereCleaner...	5652	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	Type: REG_SZ, Le...
18:29:...	AdwereCleaner...	5652	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	
18:29:...	AdwereCleaner...	5652	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x775...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
18:29:...	AdwereCleaner...	5652	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
18:29:...	AdwereCleaner...	5652	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
18:29:...	AdwereCleaner...	5652	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
18:29:...	AdwereCleaner...	5652	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
18:29:...	AdwereCleaner...	5652	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
18:29:...	AdwereCleaner...	5652	CreateFile	C:\Users\FlareVM\Desktop\Malware\ro...	SUCCESS	Desired Access: E...
18:29:...	AdwereCleaner...	5652	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75f...
18:29:...	AdwereCleaner...	5652	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x75f...

Showing 23,631 of 546,199 events (4.%)

Backed by virtual memory

Creazione e modifica di file

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
18:29:...	AdwreCleaner...	5652	Process Start		SUCCESS	Parent PID: 4784, ...
18:29:...	AdwreCleaner...	5652	Thread Create		SUCCESS	Thread ID: 6788
18:29:...	AdwreCleaner...	5652	Load Image	C:\Users\FlareVM\Desktop\Malware\ro...	SUCCESS	Image Base: 0x400...
18:29:...	AdwreCleaner...	5652	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffe...
18:29:...	AdwreCleaner...	5652	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x775...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
18:29:...	AdwreCleaner...	5652	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
18:29:...	AdwreCleaner...	5652	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
18:29:...	AdwreCleaner...	5652	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
18:29:...	AdwreCleaner...	5652	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ffe...
18:29:...	AdwreCleaner...	5652	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ffe...
18:29:...	AdwreCleaner...	5652	QueryOpen	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	
18:29:...	AdwreCleaner...	5652	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
18:29:...	AdwreCleaner...	5652	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
18:29:...	AdwreCleaner...	5652	CloseFile	C:\Windows	SUCCESS	
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\Software\Microsoft\Wow64\86	SUCCESS	Desired Access: R...
18:29:...	AdwreCleaner...	5652	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	NAME NOT FOUND	Length: 520
18:29:...	AdwreCleaner...	5652	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	Type: REG_SZ, Le...
18:29:...	AdwreCleaner...	5652	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	
18:29:...	AdwreCleaner...	5652	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x775...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
18:29:...	AdwreCleaner...	5652	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
18:29:...	AdwreCleaner...	5652	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
18:29:...	AdwreCleaner...	5652	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
18:29:...	AdwreCleaner...	5652	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
18:29:...	AdwreCleaner...	5652	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
18:29:...	AdwreCleaner...	5652	CreateFile	C:\Users\FlareVM\Desktop\Malware\ro...	SUCCESS	Desired Access: E...
18:29:...	AdwreCleaner...	5652	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75f...
18:29:...	AdwreCleaner...	5652	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x75f...

Showing 23,631 of 546,199 events (4.%)

Backed by virtual memory

Salvataggio dell'eseguibile "6AdwCleaner.exe"

10:38:...	AdwreCleaner...	7452	QuerySecurityFile	C:\Windows\SysWOW64\OneCoreUAPCommonProxyStub.dll	BUFFER OVERFL...	Information: Owner
10:38:...	AdwreCleaner...	7452	QuerySecurityFile	C:\Windows\SysWOW64\OneCoreUAPCommonProxyStub.dll	SUCCESS	Information: Owner
10:38:...	AdwreCleaner...	7452	CloseFile	C:\Windows\SysWOW64\OneCoreUAPCommonProxyStub.dll	SUCCESS	
10:38:...	C:\Users\FlareVM\Desktop\AdwreCleaner.exe			C:\Users\FlareVM\AppData\Local	SUCCESS	CreationTime: 3/24/2025 8:0...
10:38:...	6AdwCleaner.exe	7452	CreateFile	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	Desired Access: Read Data/...
10:38:...	AdwreCleaner...	7452	CreateFileMapping	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	FILE LOCKED WI...	SyncType: SyncTypeCreateS...
10:38:...	AdwreCleaner...	7452	CreateFileMapping	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	SyncType: SyncTypeOther
10:38:...	AdwreCleaner...	7452	QuerySecurityFile	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	Information: Label
10:38:...	AdwreCleaner...	7452	QueryNameInformationFile	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	Name: \Users\FlareVM\AppData...
10:38:...	AdwreCleaner...	7452	Process Create	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	PID: 7552, Command line: "C:...
10:38:...	6AdwCleaner.exe	7552	Process Start		SUCCESS	Parent PID: 7452, Command l...
10:38:...	6AdwCleaner.exe	7552	Thread Create		SUCCESS	Thread ID: 2856

Esecuzione "6AdwCleaner.exe"

10:38:...	AdwreCleaner...	7452	CreateFile	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	Desired Access: Read Data/...
10:38:...	AdwreCleaner...	7452	CreateFileMapping	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	FILE LOCKED WI...	SyncType: SyncTypeCreateS...
10:38:...	AdwreCleaner...	7452	CreateFileMapping	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	SyncType: SyncTypeOther
10:38:...	AdwreCleaner...	7452	QuerySecurityFile	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	Information: Label
10:38:...	AdwreCleaner...	7452	QueryNameInformationFile	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	Name: \Users\FlareVM\AppData...
10:38:...	6AdwCleaner.exe	7452	Process Create	C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe	SUCCESS	PID: 7552, Command line: "C:...
10:38:...	6AdwCleaner.exe	7552	Process Start		SUCCESS	Parent PID: 7452, Command l...
10:38:...	6AdwCleaner.exe	7552	Thread Create		SUCCESS	Thread ID: 2856

Connessioni UDP e TCP inviate da 6AdwCleaner

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help



Time ...	Process Name	PID	Operation	Path	Result	Detail
18:29:...	6AdwCleaner.exe	4848	UDP Send	DESKTOP-4G3BOGK:64266 -> DESK...	SUCCESS	Length: 42, sequ...
18:29:...	6AdwCleaner.exe	4848	UDP Receive	DESKTOP-4G3BOGK:64266 -> DESK...	SUCCESS	Length: 58, sequ...
18:29:...	6AdwCleaner.exe	4848	TCP Connect	DESKTOP-4G3BOGK:50024 -> 192.0.2...	SUCCESS	Length: 0, mss: 14...
18:29:...	6AdwCleaner.exe	4848	TCP Send	DESKTOP-4G3BOGK:50024 -> 192.0.2...	SUCCESS	Length: 115, starti...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50024 -> 192.0.2...	SUCCESS	Length: 124, seqn...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50024 -> 192.0.2...	SUCCESS	Length: 1447, seq...
18:29:...	6AdwCleaner.exe	4848	TCP Disconnect	DESKTOP-4G3BOGK:50024 -> 192.0.2...	SUCCESS	Length: 0, sequum:...
18:29:...	6AdwCleaner.exe	4848	TCP Connect	DESKTOP-4G3BOGK:50026 -> 192.0.2...	SUCCESS	Length: 0, mss: 14...
18:29:...	6AdwCleaner.exe	4848	TCP Send	DESKTOP-4G3BOGK:50026 -> 192.0.2...	SUCCESS	Length: 2583, starti...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50026 -> 192.0.2...	SUCCESS	Length: 124, seqn...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50026 -> 192.0.2...	SUCCESS	Length: 1447, seq...
18:29:...	6AdwCleaner.exe	4848	TCP Disconnect	DESKTOP-4G3BOGK:50026 -> 192.0.2...	SUCCESS	Length: 0, sequum:...
18:29:...	6AdwCleaner.exe	4848	UDP Send	DESKTOP-4G3BOGK:58318 -> DESK...	SUCCESS	Length: 36, sequ...
18:29:...	6AdwCleaner.exe	4848	UDP Receive	DESKTOP-4G3BOGK:58318 -> DESK...	SUCCESS	Length: 52, sequ...
18:29:...	6AdwCleaner.exe	4848	TCP Connect	DESKTOP-4G3BOGK:50028 -> 192.0.2...	SUCCESS	Length: 0, mss: 14...
18:29:...	6AdwCleaner.exe	4848	TCP Send	DESKTOP-4G3BOGK:50028 -> 192.0.2...	SUCCESS	Length: 241, starti...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50028 -> 192.0.2...	SUCCESS	Length: 124, seqn...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50028 -> 192.0.2...	SUCCESS	Length: 1447, seq...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50028 -> 192.0.2...	SUCCESS	Length: 0, sequum:...
18:29:...	6AdwCleaner.exe	4848	TCP Disconnect	DESKTOP-4G3BOGK:50028 -> 192.0.2...	SUCCESS	Length: 0, sequum:...
18:29:...	6AdwCleaner.exe	4848	UDP Send	DESKTOP-4G3BOGK:51940 -> DESK...	SUCCESS	Length: 36, sequ...
18:29:...	6AdwCleaner.exe	4848	UDP Receive	DESKTOP-4G3BOGK:51940 -> DESK...	SUCCESS	Length: 52, sequ...
18:29:...	6AdwCleaner.exe	4848	TCP Connect	DESKTOP-4G3BOGK:50029 -> 192.0.2...	SUCCESS	Length: 0, mss: 14...
18:29:...	6AdwCleaner.exe	4848	TCP Send	DESKTOP-4G3BOGK:50029 -> 192.0.2...	SUCCESS	Length: 223, starti...
18:29:...	6AdwCleaner.exe	4848	TCP Send	DESKTOP-4G3BOGK:50029 -> 192.0.2...	SUCCESS	Length: 83, startim...
18:29:...	6AdwCleaner.exe	4848	TCP Send	DESKTOP-4G3BOGK:50029 -> 192.0.2...	SUCCESS	Length: 124, seqn...
18:29:...	6AdwCleaner.exe	4848	TCP Disconnect	DESKTOP-4G3BOGK:50029 -> 192.0.2...	SUCCESS	Length: 1447, seq...
18:29:...	6AdwCleaner.exe	4848	UDP Send	DESKTOP-4G3BOGK:52318 -> DESK...	SUCCESS	Length: 35, sequ...
18:29:...	6AdwCleaner.exe	4848	UDP Receive	DESKTOP-4G3BOGK:52318 -> DESK...	SUCCESS	Length: 51, sequ...
18:29:...	6AdwCleaner.exe	4848	TCP Connect	DESKTOP-4G3BOGK:50030 -> 192.0.2...	SUCCESS	Length: 0, mss: 14...
18:29:...	6AdwCleaner.exe	4848	TCP Send	DESKTOP-4G3BOGK:50030 -> 192.0.2...	SUCCESS	Length: 142, starti...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50030 -> 192.0.2...	SUCCESS	Length: 135, seqn...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50030 -> 192.0.2...	SUCCESS	Length: 1447, seq...
18:29:...	6AdwCleaner.exe	4848	TCP Disconnect	DESKTOP-4G3BOGK:50030 -> 192.0.2...	SUCCESS	Length: 0, sequum:...
18:29:...	6AdwCleaner.exe	4848	UDP Send	DESKTOP-4G3BOGK:62812 -> DESK...	SUCCESS	Length: 35, sequ...
18:29:...	6AdwCleaner.exe	4848	UDP Receive	DESKTOP-4G3BOGK:62812 -> DESK...	SUCCESS	Length: 51, sequ...
18:29:...	6AdwCleaner.exe	4848	TCP Connect	DESKTOP-4G3BOGK:50031 -> 192.0.2...	SUCCESS	Length: 0, mss: 14...
18:29:...	6AdwCleaner.exe	4848	TCP Send	DESKTOP-4G3BOGK:50031 -> 192.0.2...	SUCCESS	Length: 234, starti...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50031 -> 192.0.2...	SUCCESS	Length: 124, seqn...
18:29:...	6AdwCleaner.exe	4848	TCP Receive	DESKTOP-4G3BOGK:50031 -> 192.0.2...	SUCCESS	Length: 1447, seq...
18:29:...	6AdwCleaner.exe	4848	TCP Disconnect	DESKTOP-4G3BOGK:50031 -> 192.0.2...	SUCCESS	Length: 0, sequum:...

Showing 57 of 3.030.290 events (0.0%) Backed by virtual memory

Conclusioni

Il malware è pensato per fingersi il tool legittimo AdwCleaner sviluppato da Malwarebytes, finge di essere un pulitore di adware mentre compie altre azioni sospette.

Sono stati notati principalmente questi comportamenti:

- Modifica alle chiavi di registro disabilitando il logging dei file di AdwCleaner.
- Creazione di un'eseguibile, a insaputa dell'utente, e aggiunta di quest'ultimo alle applicazioni che si avviano allo startup del sistema
- Ripetuti tentativi di contattare un dominio non affidabile.
- Offre un servizio fasullo che richiede un pagamento per finire le "operazioni di pulizia".
- Scansiona molteplici chiavi di registro per acquisire informazioni personali.
- Non esegue nessuna reale scansione alla ricerca di Adware.