Rapporto di Analisi di Adware

Oggetto Analizzato: File Eseguibile Sospetto (Classificato come Adware/Spyware)

1. Sommario

Il file analizzato rivela un **adware** abbastanza primitivo. Non si limita a mostrare pubblicità, ma è anche progettato per raccogliere informazioni sensibili. Si proclama un come cleaner di adware, ma la sua funzione è tutt'altro che amichevole.

Il codice è stato sviluppato per garantire la **persistenza** nel sistema compromesso, utilizzando metodi multipli. Questo rende la disinstallazione particolarmente complessa per un utente medio, spesso richiedendo strumenti di sicurezza specifici.

Oltre alla persistenza, il programma esegue **azioni di manipolazione dell'interfaccia utente**, come la lettura delle impostazioni del browser e l'iniezione di annunci indesiderati. Queste manipolazioni degradano l'esperienza utente ed espongono a ulteriori rischi di sicurezza.

Per verificare ciò è stata fatta un'analisi statica con CFF Explorer.

Funzionalità Principale	**Moduli Importati Coinvolti**
Persistenza & Installazione	KERNEL32.dll, ADVAPI32.dll
Intrusività UI	USER32.dll
Evasione & Offuscamento	KERNEL32.dll
Payload Rilevato (IoC)	C:\Users\User\AppData\Local\ δAdwCleaner.exe

2. Analisi Statica

Il modo più efficace per identificare il set di strumenti di un malware è esaminare la sua tabella di importazione (Import Table).

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	61	000075C4	00000000	00000000	00007C12	00007060
USER32.dll	63	000076D8	00000000	00000000	00008022	00007174
GDI32.dll	8	000075A0	00000000	00000000	000080B4	0000703C
SHELL32.dll	6	000076BC	00000000	00000000	00008140	00007158
ADVAPI32.dll	9	00007564	00000000	00000000	000081E2	00007000
COMCTL32.dll	4	0000758C	00000000	00000000	0000822E	00007028
ole32.dll	4	000077E8	00000000	00000000	00008282	00007284
VERSION.dll	3	000077D8	00000000	00000000	000082CE	00007274

A. ADVAPI32.dll (Persistenza e Registro)

Questo modulo è l'indicatore primario della persistenza tramite Registro di Sistema.

- **RegSetValueExA / RegCreateKeyExA:** Conferma la capacità di scrivere e creare valori nel Registro.
- **RegDeleteKeyA / RegDeleteValueA:** Indica la capacità di ripulire le tracce o di rimuovere configurazioni precedenti/concorrenti.
- **Implicazione:** Il malware, con un'azione subdola e persistente, non si limita alla semplice installazione sul sistema operativo. La sua natura gli consente di gestire attivamente la propria presenza nel Registro di sistema, eludendo le tradizionali chiavi di auto-avvio come le voci "Run". Questo comportamento indica una strategia avanzata per garantirsi la persistenza e sfuggire ai controlli di sicurezza più comuni, potrebbe rendere la sua individuazione e rimozione più complesse.

B. USER32.dll (Interazione Utente e Spionaggio)

L'uso estensivo di questo modulo (63 importazioni) dimostra che il file è una GUI (Graphical User Interface) invasiva e ostile.

- **CreateWindowExA / ShowWindow / SetForegroundWindow:** Queste funzioni sono utilizzate per creare finestre e **forzarle in primo piano**, ed è possibile che causi pop-up aggressivi e indesiderati che interferiscono con l'uso normale del computer.
- **FindWindowExA:** Utilizzata per la **ricognizione** e per individuare processi specifici (come i browser) in cui potrebbe iniettare annunci o modificare il comportamento.

C. KERNEL32.dll (I/O, Evasione e Controllo di Basso Livello)

Questo modulo rivela il ciclo di vita e le tecniche di offuscamento del malware.

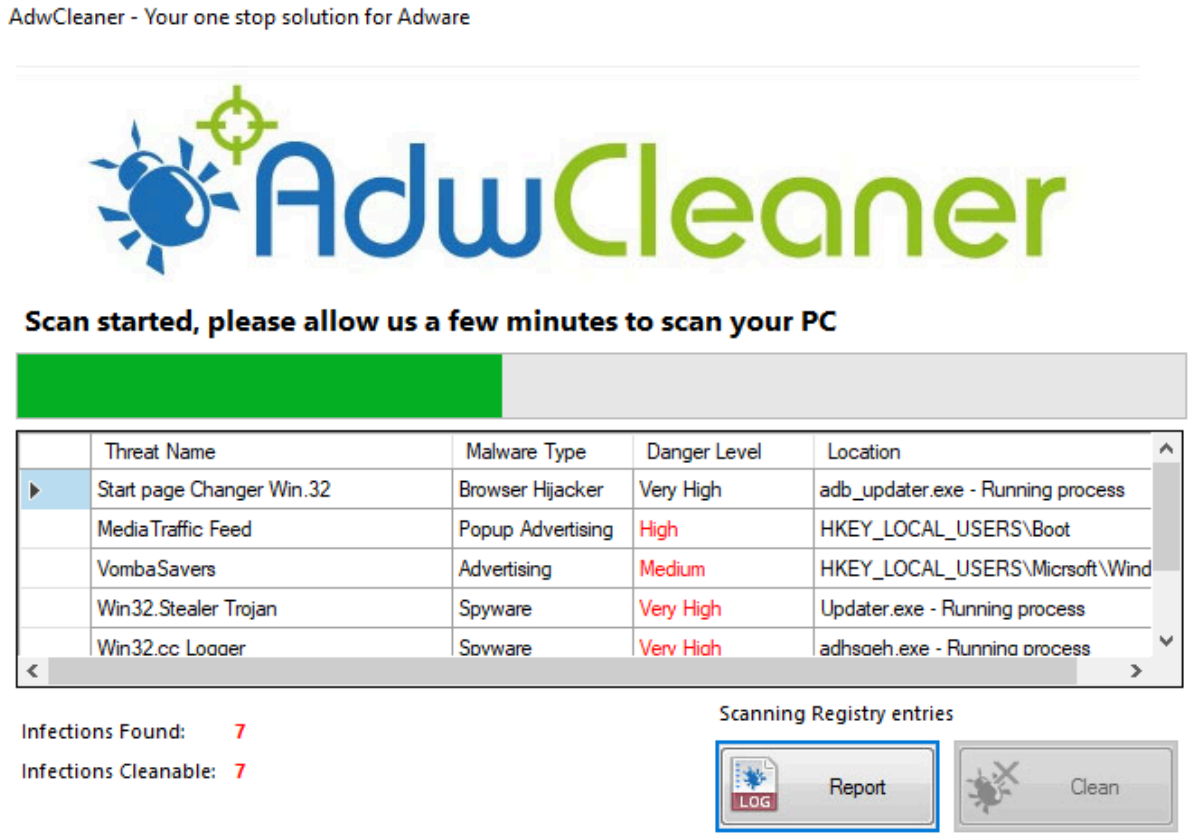
- **Persistenza/Installazione:**
  - **GetModuleFileNameA / GetTempFileNameA / CopyFileA / WriteFile:** Confermano il ciclo di vita dell'installazione: localizzare sé stesso, trovare una destinazione nella directory utente.
- **Evasione e Offuscamento (Caricamento Dinamico):**
  - **LoadLibraryA / GetProcAddress:** L'uso di queste API è la tecnica primaria di offuscamento. Le API più dannose (come quelle di rete o di iniezione) non appaiono in chiaro nella tabella e vengono risolte solo a runtime, eludendo la scansione statica.
  - **Sleep:** Utilizzato per introdurre ritardi che contrastano l'analisi in ambienti virtuali automatici (sandboxing).
- **Controllo Processi:**
  - **CreateThread / CreateProcessA:** Necessario per lanciare il payload come processo figlio, o per eseguire task in background (ad esempio, le richieste di rete per gli annunci).

3. Analisi Dinamica (ProcMon)

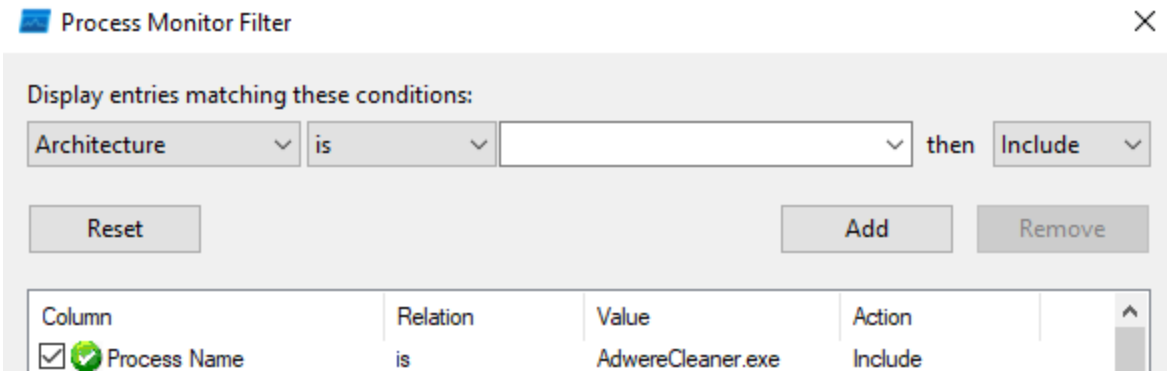
Per eseguire l'analisi dinamica del malware, è stato usato Process Monitor. Prima di eseguire il malware, si deve fare molta attenzione per far sì che la nostra macchina virtuale **NON sia connessa in internet**, deve essere quindi isolata. Una volta scollegati da internet possiamo quindi partire con l'analisi e avviare malware e process monitor in contemporanea.

Prima di lanciare il malware dobbiamo attivare la sezione di cattura processi di Process Monitor.

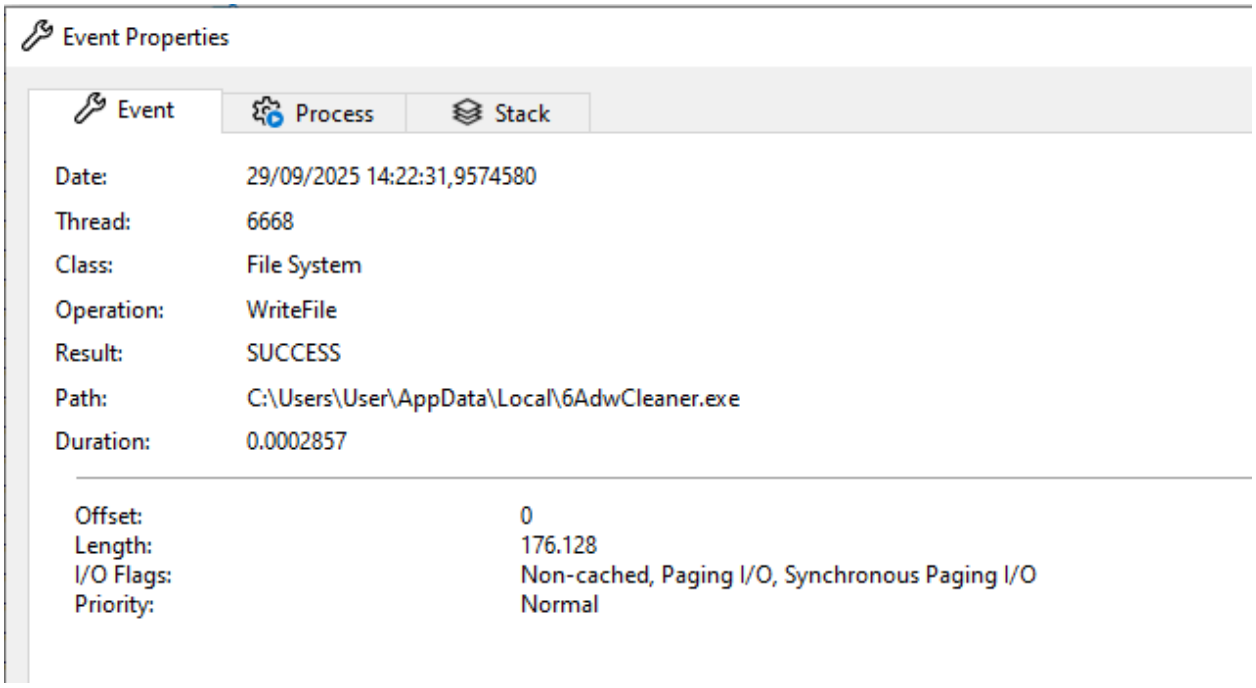
Una volta avviato l'eseguibile si avvierà l'applicazione che all'apparenza sia un cleaner di popup e pubblicità che tormentano il nostro pc. Una volta cliccato sul pulsante scan, verrà avviata una scansione fasulla che ci notificherà la presenza di più malware.



Una volta eseguito il malware passiamo a Process Monitor, dove attiviamo un filtro che ci mostrerà solamente i processi relativi all'applicazione.

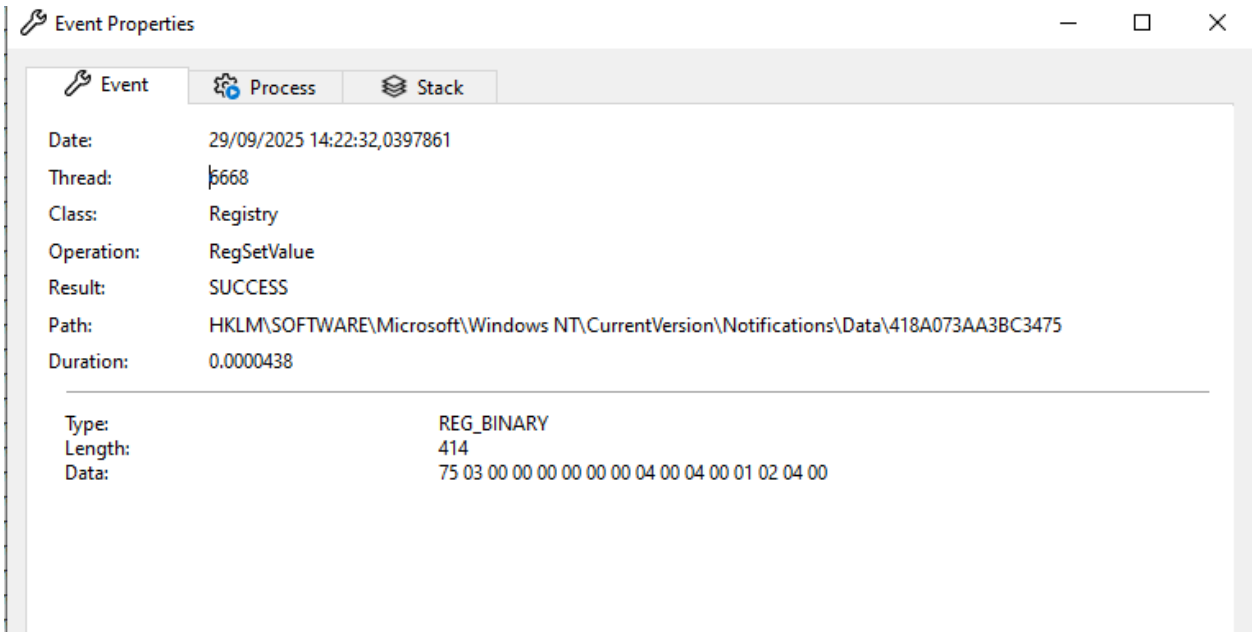


In seguito ci spostiamo negli eventi e facendo una ricerca mirata troviamo un processo interessante.



Qui notiamo un'operazione WriteFile avvenuta con successo. E' anche segnato il path in cui viene copiata la copia del malware. Viene scelta la cartella AppData\Local perché non ha permessi elevati per la scrittura e viene spesso ignorata dagli utenti. Questa è la prima tecnica di persistenza che usa il malware.

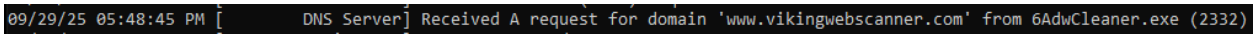
Cercando tra i processi in esecuzione troviamo una seconda tecnica di persistenza. Questa in particolare utilizza una chiave di registro, grazie al modulo **RegSetValue**.



L'adware quindi sta sfruttando il sottosistema di **Notifiche di Windows**. Questo è un metodo avanzato per la persistenza perché:

- **È più discreto:** Molti analisti cercano solo le classiche chiavi Run.
- **È efficace:** Windows carica i dati da questa chiave per gestire e visualizzare le notifiche utente. L'adware potrebbe iniettarsi nel processo di gestione delle notifiche o forzare l'esecuzione del suo payload quando un'azione di notifica viene attivata.

Successivamente mi sono avvalso dello strumento **fakenet** per creare una simulazione di rete e intercettare l'URL a cui l'adware cerca di connettersi. Mentre eseguiamo il malware, notiamo una richiesta DNS ad un sito:



Da qui partono delle richieste GET verso link esterni, non possiamo sapere a cosa si riferiscono ma molto probabilmente i nomi suggeriscono che siano pop-up per richieste di pagamento:

- /scripts/paymore.php
- /scripts/paydefault.php?id=0

Molto probabilmente l'obiettivo del sito è quello di scaricare il payload finale con la vera e propria iniezione di annunci oppure portare l'utente ad effettuare pagamenti illegittimi, visto che il sito www.vikingwebscanner.com non è più in funzione, queste sono solo ipotesi.

4. Conclusione

Il file analizzato è un **Adware**, progettato per stabilire una persistenza profonda nel sistema e compiere azioni invasive di tracciamento e visualizzazione di annunci, celando le sue operazioni attraverso tecniche di offuscamento.La sua interfaccia ingannevole, che si presenta come un "adware cleaner", sfrutta la paura dell'utente e la preoccupazione per la sicurezza del proprio sistema. Notificando la presenza di molteplici minacce inesistenti, induce l'utente a compiere azioni non specificate che, in realtà, servono solo a rafforzare la presenza e le funzionalità dannose dell'adware, potenzialmente portando a pagamenti illegittimi o all'installazione di ulteriori payload.