

Rapporto di Analisi di Adware

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



Per analizzare il file è stata utilizzata la FlareVM, una distribuzione basata su Windows che automatizza l'installazione e la configurazione di un ambiente di analisi di malware su una macchina virtuale.

Per verificare il comportamento del malware si procede con un'analisi statica eseguita con CFFExplorer.

1. 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.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
000081A2	000081A2	01CB	RegCloseKey
000081D2	000081D2	01EC	RegOpenKeyExA
000081C2	000081C2	01D4	RegDeleteKeyA
000081B0	000081B0	01D8	RegDeleteValueA
0000814C	0000814C	01E1	RegEnumValueA
00008190	00008190	01D1	RegCreateKeyExA
0000817E	0000817E	0204	RegSetValueExA
0000816A	0000816A	01F7	RegQueryValueExA
0000815C	0000815C	01DD	RegEnumKeyA

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.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00007DDE	00007DDE	0060	CreateWindowExA

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.

00007A5E	00007A5E	017D	GetModuleFileNameA
00007BA4	00007BA4	01D3	GetTempFileNameA
00007A88	00007A88	0043	CopyFileA
00007854	00007854	03A4	WriteFile

- **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.

00007B06	00007B06	0252	LoadLibraryA
00007C00	00007C00	01A0	GetProcAddress

- **Sleep:** Utilizzato per introdurre ritardi che contrastano l'analisi in ambienti virtuali automatici (sandboxing).

00007A38	00007A38	0356	Sleep
----------	----------	------	-------

- **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).

00007B60	00007B60	006F	CreateThread
00007B70	00007B70	0066	CreateProcessA

2. 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.



Scan started, please allow us a few minutes to scan your PC

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	High	HKEY_LOCAL_USERS\Boot
VombaSavers	Advertising	Medium	HKEY_LOCAL_USERS\Microsoft\Wind
Win32.Stealer Trojan	Spyware	Very High	Updater.exe - Running process
Win32.cc Loader	Sovware	Very High	adhsaeh.exe - Running process

Infections Found: **7**

Infections Cleanable: **7**

Scanning Registry entries



Possiamo vedere come l'applicazione mostri dei finti pericoli presenti nel nostro computer, mettendo timore all'utente su una possibile compromissione. Terminata la scansione vengono notificate 13 "infezioni al computer" e premendo su **clean** viene richiesto un pagamento per passare alla versione completa.

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!

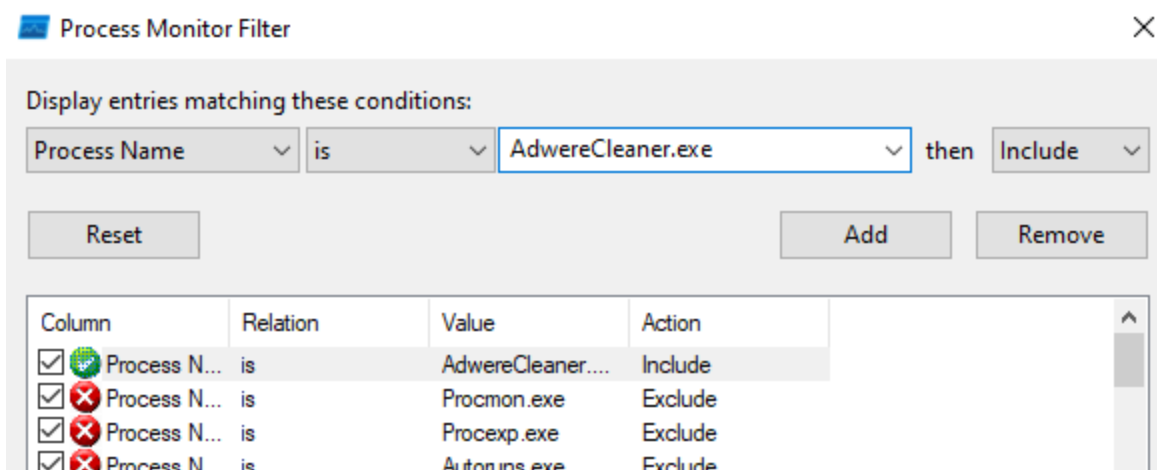
Only \$59,99

Normal price: \$89,99. Sale ending on: 01/10/2025

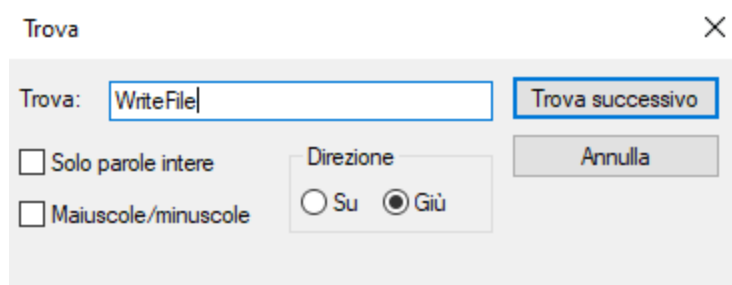
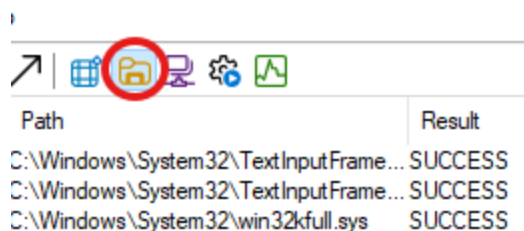
[After purchase your serial number will be E-mailed to you, click here to enter it.](#)

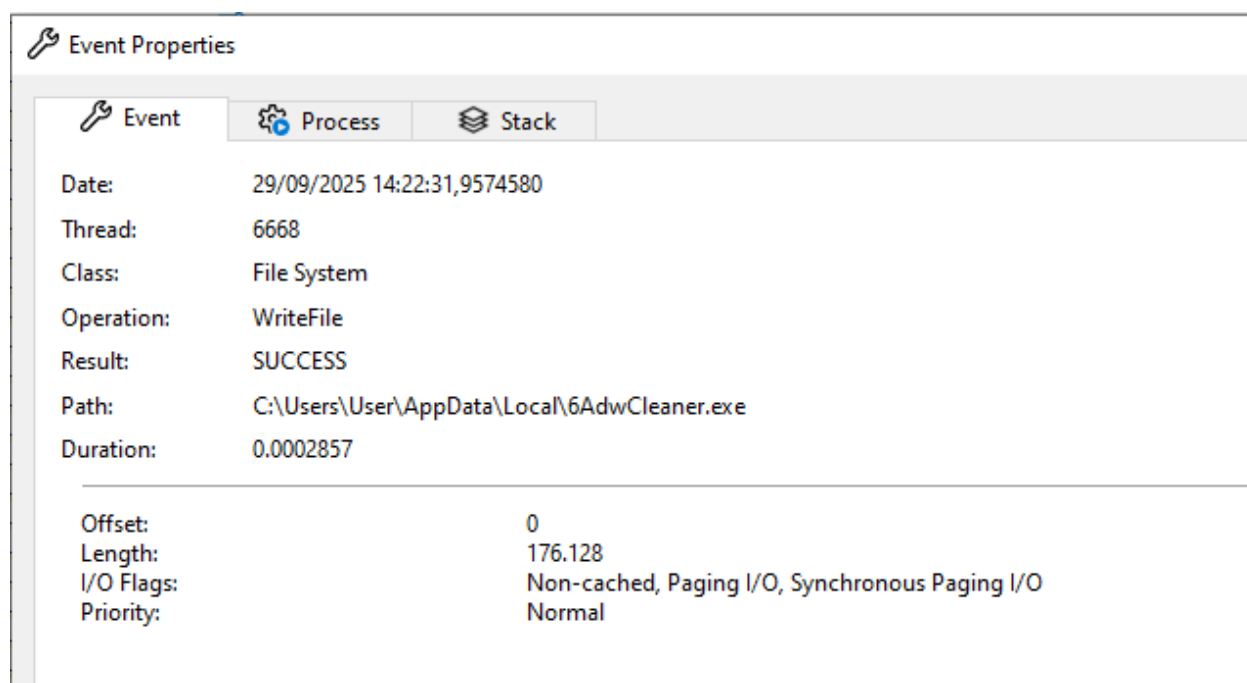
 L'esplorazione

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





In seguito ci spostiamo negli eventi e facendo una ricerca mirata alle attività dei file di sistema e ricercando la parola chiave **WriteFile**, troviamo un processo interessante.



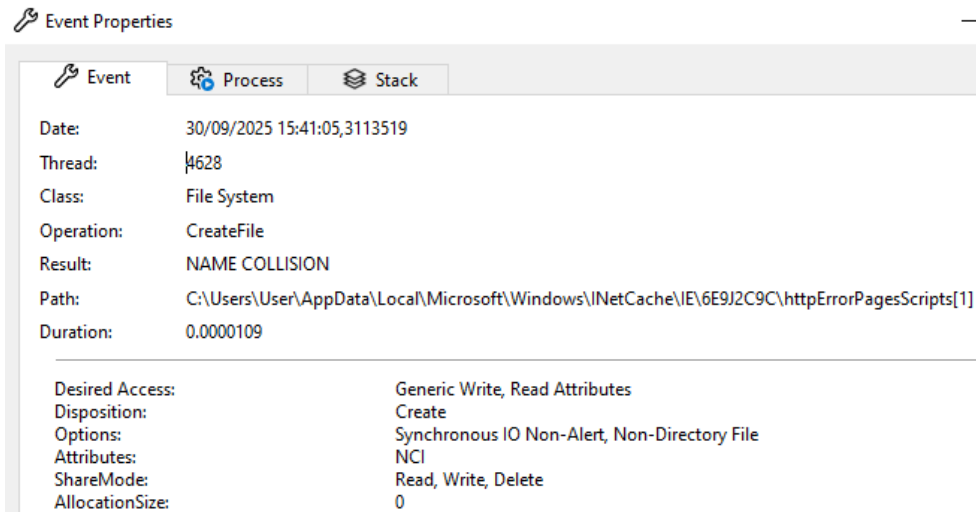


Qui notiamo che l'operazione WriteFile è avvenuta con successo. E' anche segnato il path in cui viene copiata la copia del malware. Viene scelta la cartella AppData\Local perché non ha permessi elevati per la scrittura e viene spesso ignorata dagli utenti.

Visto che viene aggiunto questo file figlio, analizzo anche quest'ultimo su ProcessMonitor, aggiungendolo al filtro.

Column	Relation	Value	Action
<input checked="" type="checkbox"/>  Process Name	is	AdwereCleaner....	Include
<input checked="" type="checkbox"/>  Process Name	is	6AdwCleaner.exe	Include

Vediamo che questo eseguibile scrive nella cache **InetCache\IE** dei file come **ErrorPageTemplate** e **httpErrorPagesScripts**, comportamento tipico quando un'app tenta di connettersi a una pagina o risorsa, c'è quindi un tentativo di contattare risorse web.



Venuto a conoscenza della richiesta di connessione, 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:

```
09/29/25 05:48:45 PM [ DNS Server] Received A request for domain 'www.vikingwebscanner.com' from 6AdwCleaner.exe (2332)
```

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.

3. Conclusione

Il file analizzato è un **rogue security software**, 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, potenzialmente portando a pagamenti illegittimi o all'installazione di ulteriori payload.