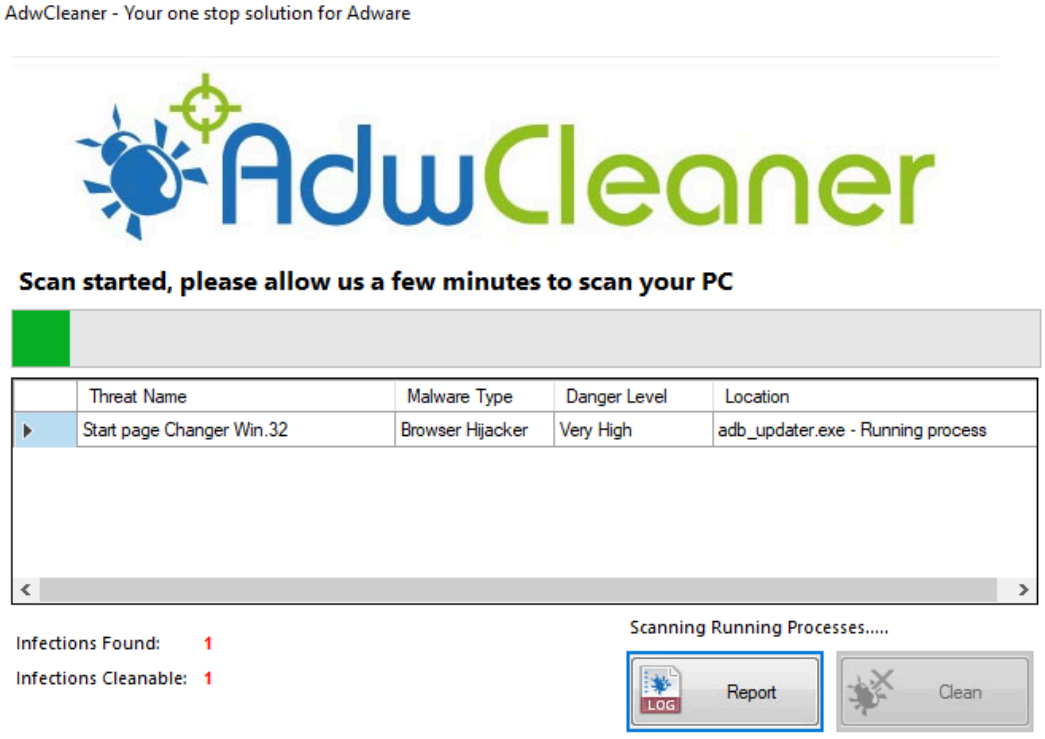
ANALISI DINAMICA DEL MALWARE “AdwereCleaner.exe”

1.Preparazione del laboratorio:

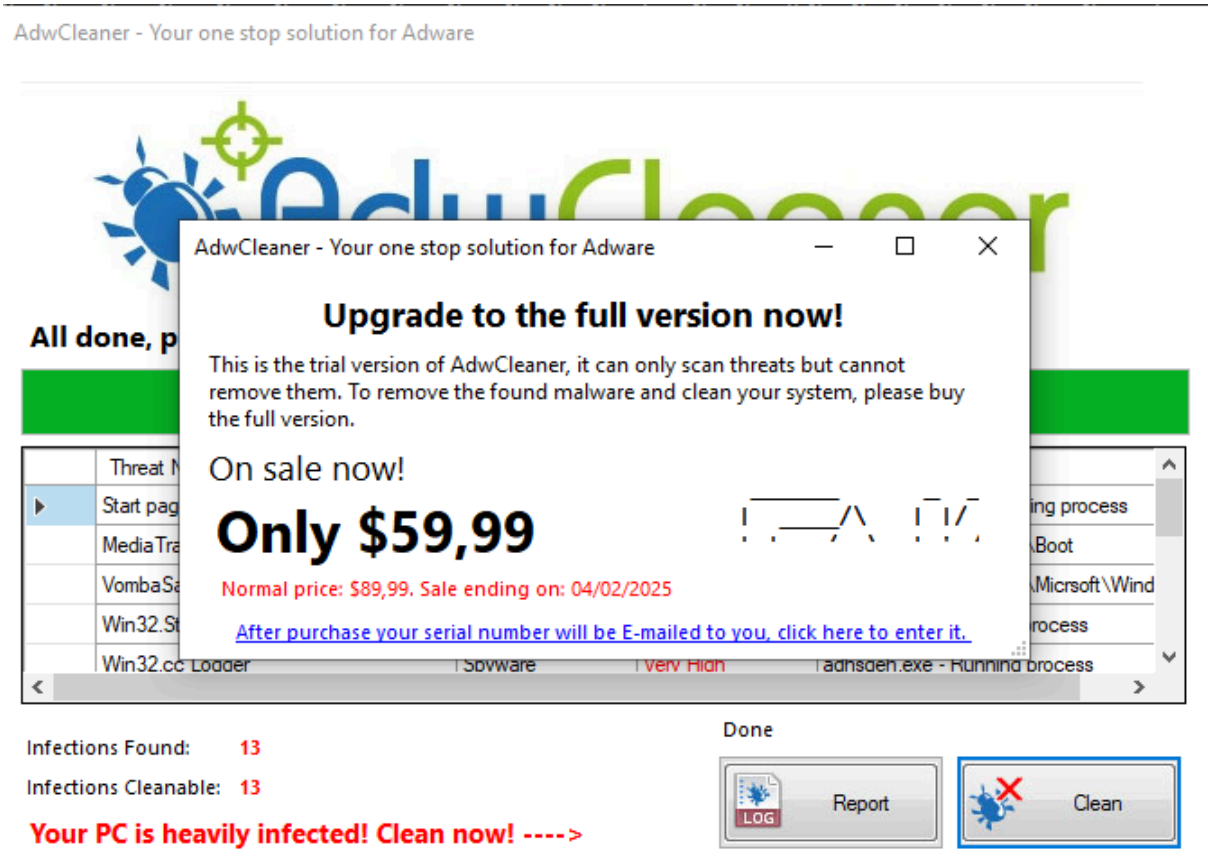
- Adopereremo la flareVM e vari tool, per l’analisi dinamica di questo malware.
    - REGSHOT: per creare un “immagine” dei registri prima e dopo l’esecuzione del malware, in modo da capire quali chiavi di registro vengono aggiunte, eliminate o modificate dal programma malevolo.
    - FAKENET: questo strumento ci consentirà di intercettare e reindirizzare tutto o parte del traffico di rete specifico simulando servizi di rete legittimi.
    - WIRESHARK: eseguiremo una scansione di rete con wireshark.
    - PROCMON: utilizzeremo procmon per tenere monitorati i processi che avvierà il malware.

2.Avvio e comportamento del malware:

- Il programma malevolo si presenta come un Adware Cleaner, inizia facendo una scansione, quasi sicuramente finta, mostrando varie minacce locali e il livello del pericolo di queste:



- Una volta finita la scansione il programma ci chiede come vogliamo continuare, se riportare ciò che è stato trovato o “pulire” il sistema operativo dalle minacce. Dopo aver cliccato su “clean” il programma ci avvisa che per continuare dobbiamo pagare la versione premium del tool:



3.Cosa ha fatto realmente il malware:

Dalle istantanee create con regshot e poi confrontate, abbiamo dedotto che:

AdwCleaner ha eliminato diverse chiavi di registro, tra cui:

- **HKU...\Internet Settings\5.0\Cache\Extensible Cache\MSHist012025011420250115**
- **HKU...\Internet Settings\5.0\Cache\Extensible Cache\MSHist012025011520250116**
- **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DhcpNameServer: "10.0.2.3"**

La cancellazione di chiavi di rete e cache del browser potrebbe essere un tentativo di nascondere attività dannose o impedire il ripristino delle configurazioni legittime del sistema.

AdwCleaner ha creato nuove chiavi di registro, tra cui:

- **HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32**
- **HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS**

- **HKU...\Software\AdwCleaner**

L'aggiunta di queste chiavi indica un tracciamento delle attività del sistema, potenzialmente per scopi malevoli. La presenza di chiavi sotto "Tracing" suggerisce un possibile monitoraggio delle operazioni eseguite dall'utente o dal sistema operativo.

AdwCleaner ha alterato diversi valori di registro critici:

- **HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings...\AdwCleaner.exe**
- **HKU...\Software\Microsoft\Windows\CurrentVersion\Run\AdwCleaner**

L'inserimento in **CurrentVersion\Run** implica che AdwCleaner si autoesegue all'avvio del sistema, comportamento tipico di software persistenti e potenzialmente dannosi. Questo potrebbe permettere al malware di rimanere attivo anche dopo riavvii o tentativi di rimozione manuale.

Il comportamento osservato indica un potenziale malware che potrebbe compromettere la sicurezza del sistema, eseguendo azioni senza il consenso dell'utente e garantendosi la persistenza nel sistema operativo.

Dai log di fakenet abbiamo evidenziato che:

Il malware fa richiesta a vari domini in cui poi vengono eseguite richieste GET o POST così abbiamo stilato alcune ipotesi di ciò che realmente fa il programma:

- Risoluzione e C2 (Command and Control):
    - Il dominio `www.vikingwebscanner.com` potrebbe essere utilizzato per la comunicazione con il server C2. Il malware potrebbe cercare di scaricare istruzioni o aggiornamenti da lì.
    - Le richieste HTTP GET potrebbero servire a recuperare payload aggiuntivi o ottenere configurazioni da un server remoto.
- Verifica della connettività o evasione delle sandbox:
    - Il malware potrebbe eseguire richieste a domini legittimi per verificare se ha accesso a Internet o se è in un ambiente di analisi (sandbox).
    - `ocsp.usertrust.com` è un dominio legittimo utilizzato per la verifica dei certificati digitali tramite il protocollo OCSP. Un malware potrebbe abusare di queste richieste per confondersi con il traffico legittimo.
- Esfiltrazione di dati:
    - Le richieste POST a `ocsp.usertrust.com` potrebbero essere un tentativo di esfiltrare dati mascherandoli come traffico legittimo.