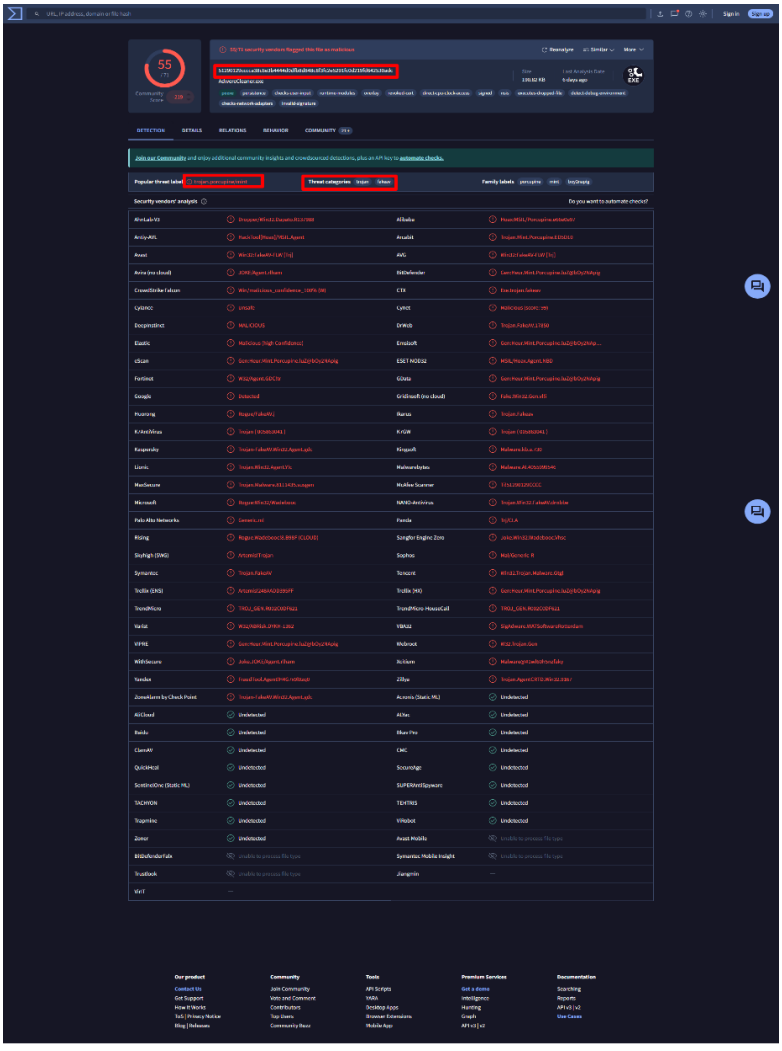
Esercizio 1 - Malware analysis *AdwareCleaner.exe* - Analisi Statica - VirusTotal

Abbiamo iniziato l'analisi caricando *AdwareCleaner.exe* su VirusTotal, una piattaforma che esegue scansioni statiche su file sospetti utilizzando più di 70 motori antivirus. I risultati di questa scansione sono stati significativi:

- **Punteggio di rilevamento**: 55 su 71 motori antivirus hanno identificato il file come maligno.
- **Community Score**: -219, un indicatore negativo che ha evidenziato un forte consenso della comunità riguardo alla natura dannosa del file.
- **Identificazione del tipo di malware**: *Trojan FakeAV*, un tipo di malware che simula un software antivirus per ingannare l'utente e mascherare le sue azioni dannose.

FakeAV (Fake Antivirus): Un Trojan che si finge un antivirus legittimo. Solitamente visualizza avvisi fasulli di minacce e tenta di indurre l'utente a installare software aggiuntivo o pagare per la rimozione di minacce inesistenti.

Questa analisi preliminare ha indicato che *AdwareCleaner.exe* potrebbe non solo mascherarsi come un software antivirus, ma anche compiere azioni dannose che abbiamo approfondito con un'analisi dinamica.



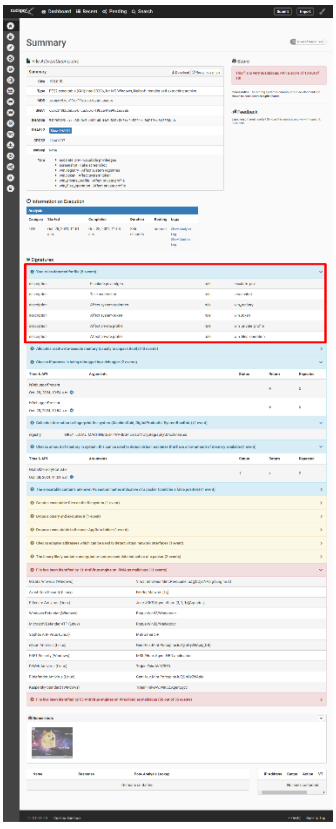
2. Analisi Dinamica: Cuckoo Sandbox

Per verificare il comportamento effettivo di *AdwareCleaner.exe*, abbiamo utilizzato Cuckoo Sandbox, un ambiente di analisi dinamica che simula l'esecuzione di file sospetti e ne traccia le azioni all'interno di un sistema protetto. I risultati principali sono stati:

- **Obiettivi del Malware**:
  - **Escalation dei Privilegi**: Il malware tenta di ottenere livelli di accesso più alti nel sistema per aumentare la sua capacità d'azione.
  - **Modifiche al Registro di Sistema**: Modifica, aggiunge o cancella voci di registro per garantire persistenza o danneggiare il sistema.
  - **Screenshot del Sistema**: Registra immagini dello schermo, suggerendo la raccolta di dati sensibili.
  - **Accesso a Token e Profili Privati**: Raccoglie dati dai profili utente e utilizza token di sistema per aumentare le autorizzazioni.
  - **Interventi su File di Windows**: Interagisce direttamente con file di sistema, un comportamento tipico per malware che tenta di rimanere nascosto.

Escalation dei Privilegi: Un attacco che mira ad ottenere accessi non autorizzati ai privilegi di amministratore, permettendo al malware di eseguire azioni che richiedono permessi elevati.

Questa analisi dinamica ha evidenziato come *AdwareCleaner.exe* sia progettato per eseguire operazioni invasive, tipiche di malware avanzati.



3. Analisi Approfondita Tramite FLARE VM

Abbiamo poi eseguito un'analisi più dettagliata su FLARE VM, un ambiente virtuale sicuro per l'analisi di malware, configurando la rete in modalità *Solo Host* per evitare connessioni esterne non controllate. Abbiamo utilizzato vari strumenti per osservare i cambiamenti del sistema e verificare ulteriori tentativi di collegamento a server esterni.

a) Fakenet: Monitoraggio delle Connessioni di Rete

Abbiamo avviato *Fakenet*, un tool per osservare e simulare connessioni di rete per malware. Questo ci ha permesso di monitorare eventuali tentativi di connessione esterna da parte di *AdwareCleaner.exe*. Nonostante non siano stati rilevati tentativi immediati di collegamento, l'uso di Fakenet è stato fondamentale per tenere sotto controllo le potenziali connessioni di rete del malware.

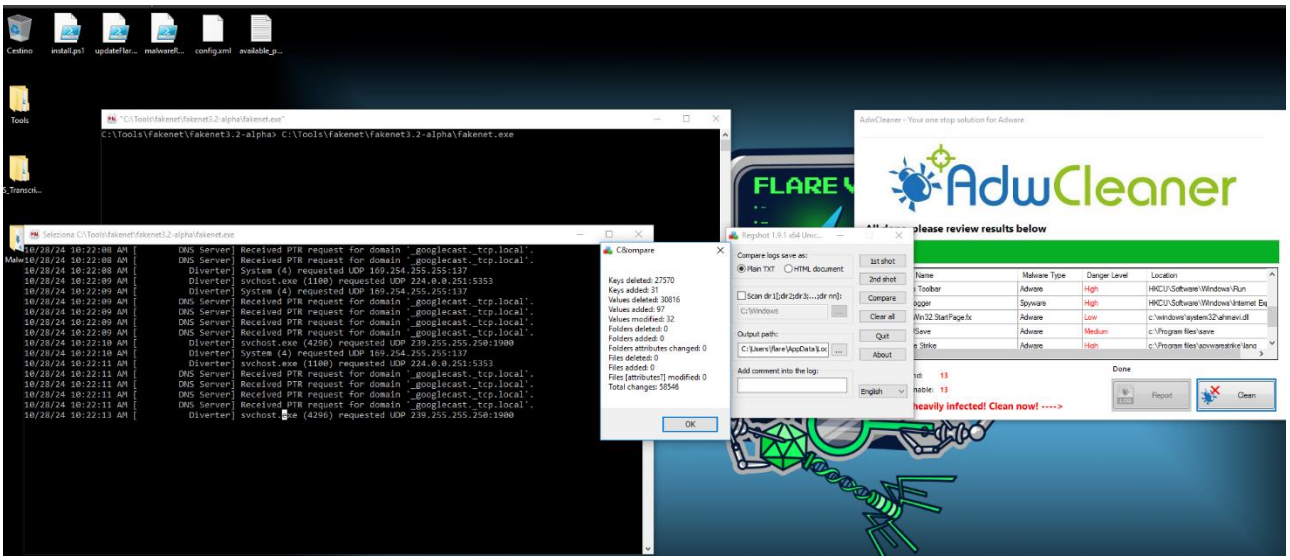
b) Regshot: Monitoraggio del Registro di Sistema

Abbiamo eseguito il software *Regshot* per catturare una "foto" dello stato del registro di sistema prima e dopo l'avvio di *AdwareCleaner.exe*. I risultati mostrano che il malware ha eseguito un numero elevato di modifiche:

- **Chiavi di Registro Cancellate**: 27,570
- **Chiavi di Registro Aggiunte**: 31
- **Valori di Registro Cancellati**: 30,816
- **Valori di Registro Aggiunti**: 97
- **Valori di Registro Modificati**: 32

Totale Modifiche al Registro: 58,546

Questa notevole quantità di modifiche dimostra l'aggressività di *AdwareCleaner.exe* e il suo intento di compromissione del sistema.



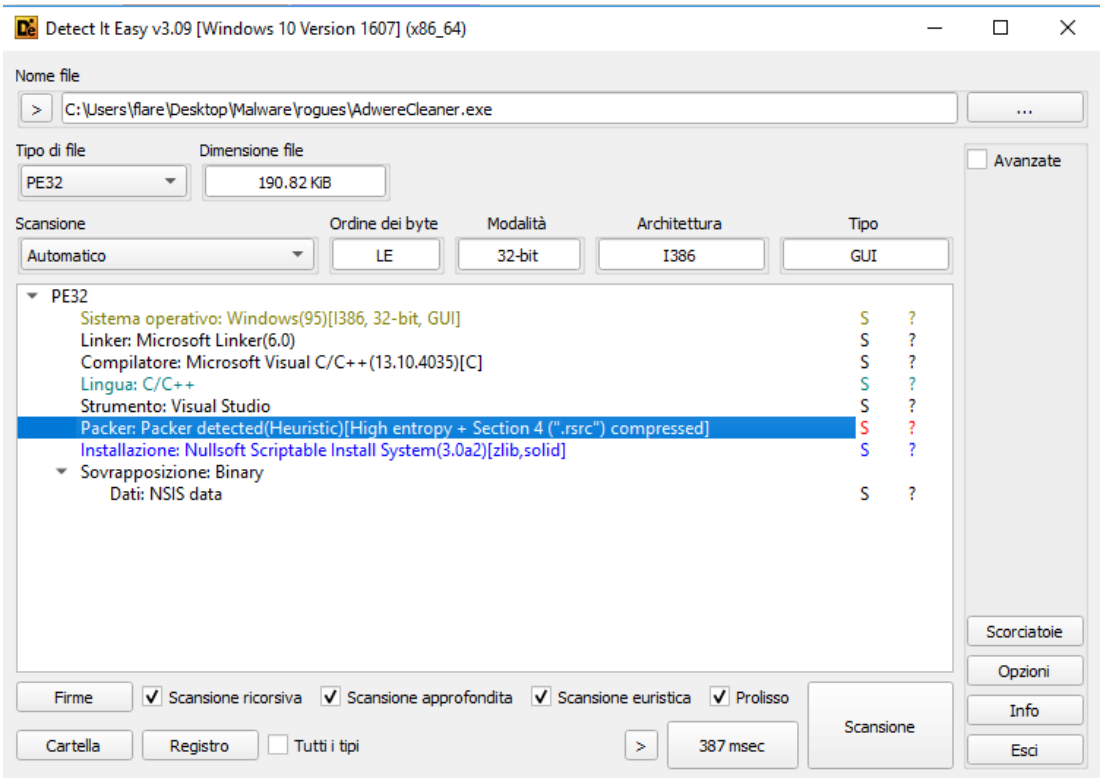
4. Analisi con Detect It Easy ed Euristiche di Rilevamento

Per ottenere ulteriori informazioni sulla struttura del file, abbiamo utilizzato *Detect It Easy* per un'analisi euristica, che ha rivelato informazioni sul codice del malware e sul linguaggio di programmazione utilizzato. Utilizzando funzioni avanzate, siamo riusciti a individuare componenti chiave del codice, tra cui:

- **Packer**: Un metodo utilizzato per mascherare il codice del malware, rendendolo più difficile da analizzare.
- **Anti-Debugging e Anti-Analisi**: Tecniche implementate per impedire che il malware venga facilmente esaminato o fermato.
- **Tecniche di Offuscamento e Cifratura**: Metodi avanzati per nascondere le istruzioni del codice e sfuggire ai controlli di sicurezza.

Packer: Un software o una tecnica che "impacchetta" un programma per nasconderne la struttura e rendere più difficile la sua analisi.

L'uso di queste tecniche evidenzia come il malware sia stato progettato non solo per compiere azioni dannose, ma anche per evitare il rilevamento da parte dei software di sicurezza tradizionali, mascherandosi da applicazione sicura.

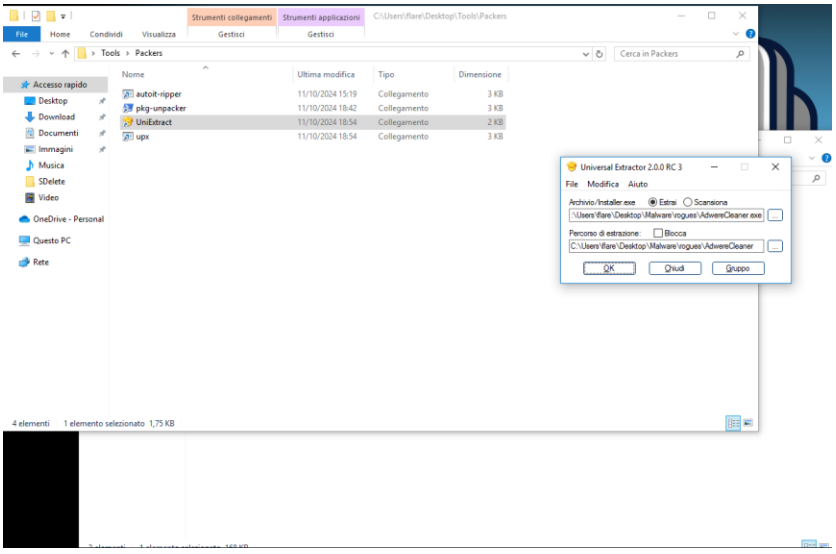


Proseguendo con l'analisi su FLARE VM, abbiamo utilizzato *Universal Extractor* (*UniExtract*) per esaminare ulteriormente il file sospetto *AdwareCleaner.exe*. Questo strumento ci ha permesso di estrarre i componenti interni dell'eseguibile, rivelando un secondo file denominato *6AdwCleaner.exe*.

Analisi del file estratto: *6AdwCleaner.exe*

1. **Scansione Statica**: Una volta estratto, abbiamo sottoposto *6AdwCleaner.exe* a una scansione statica per verificare se fosse anch'esso un elemento dannoso. Analogamente al file principale, il punteggio di rilevamento è stato elevato, confermando la natura sospetta di questo componente.
2. **Comportamento e Struttura**:
    - **Funzionalità di Anti-Analisi**: Abbiamo riscontrato la presenza di tecniche avanzate di anti-debugging e offuscamento simili a quelle del file principale, confermando che anche *6AdwCleaner.exe* è stato progettato per evitare l'individuazione e l'analisi.
    - **Packer**: L'analisi strutturale ha rivelato l'uso di un packer, una tecnica che maschera la struttura del file. Questo è stato utilizzato per complicare ulteriormente la decompilazione e nascondere le vere istruzioni del codice maligno.
3. **Potenziale di Escalation dei Privilegi e Persistenza**: Le analisi dinamiche sul file estratto hanno suggerito che *6AdwCleaner.exe* possiede anch'esso funzioni per modificare il sistema operativo, cercando di ottenere persistenza attraverso chiavi di registro e permessi elevati. Queste azioni indicano che l'exe estratto è probabilmente un elemento secondario del malware, progettato per attivarsi come backup o per aumentare la stabilità del malware nel sistema.

In sintesi, l'uso di *UniExtract* ha permesso di identificare *6AdwCleaner.exe* come parte integrante del malware, confermando una struttura multicomponente che agisce con tecniche di evasione e persistente compromissione del sistema. Questa scoperta evidenzia la complessità del malware *AdwareCleaner.exe*, il cui scopo è mantenere una presenza stabile e nascosta nel sistema infetto.



Abbiamo quindi fatto un'analisi veloce delle strutture principali del codice e delle sue caratteristiche salienti. Il codice è un complesso script di rilevamento euristico, creato per individuare e segnalare comportamenti anomali o sospetti in file binari, con particolare attenzione a file .NET e nativi.

Conclusioni

Il codice è progettato per eseguire un'analisi statica del file, sfruttando diverse tecniche di rilevamento euristico per identificare possibili tentativi di nascondere codice maligno. Queste tecniche comprendono:

- Rilevamento di punti d'ingresso modificati.
- Identificazione di funzioni di anti-debugging e anti-analisi.
- Verifica della presenza di tecniche di cifratura e di offuscamento avanzate.

Questa combinazione di controlli rende il codice efficace nell'individuare potenziali minacce. Tuttavia, gli stessi metodi potrebbero essere utilizzati per mascherare codice dannoso ed evitare il rilevamento da parte di software di sicurezza, rendendo cruciale una supervisione attenta del suo utilizzo.

Considerazioni Finali

L'analisi di *AdwareCleaner.exe* ha rivelato che si tratta di un malware avanzato che utilizza tecniche sofisticate per compromettere il sistema, nascondere il suo codice e sfuggire ai rilevamenti. Dalle varie analisi effettuate, possiamo concludere che *AdwareCleaner.exe* agisce come un Trojan FakeAV, caratterizzato da:

- Simulazione di funzionalità antivirus per ingannare l'utente.
- Tentativi di escalation dei privilegi per ottenere accesso a livelli di sistema elevati.
- Modifiche aggressive al registro di sistema e azioni su file di sistema critici.
- Tecniche di anti-analisi e offuscamento avanzato.

Questa combinazione di funzionalità rende il malware estremamente pericoloso. Pertanto, è cruciale adottare misure di sicurezza avanzate e continuare a monitorare strumenti come FLARE VM e VirusTotal per rilevare e comprendere le minacce emergenti.

Raccomandazioni: Si consiglia di evitare di eseguire file sospetti su sistemi di produzione e di utilizzare macchine virtuali o ambienti di testing per le analisi. I file rilevati come *FakeAV* dovrebbero essere eliminati immediatamente per evitare compromissioni del sistema.