Rapporto Dettagliato di Analisi Malware per AdwCleaner.exe

1. Informazioni Generali del File

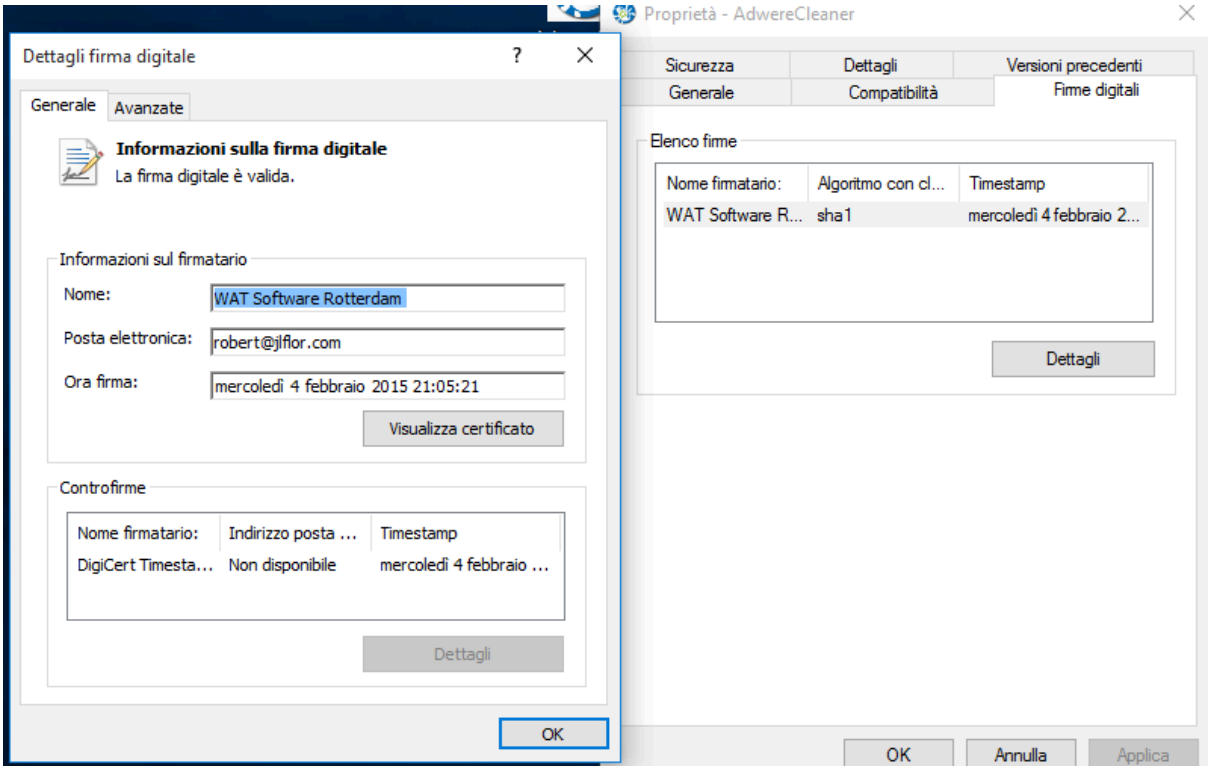
- Nome del file: AdwCleaner.exe
- Verdetto: Attività Malevola
- Data di analisi: 17 Dicembre 2024
- Sistema Operativo Analizzato: Windows 10 Professional (Build 19045, 64-bit)
- Indicatori Hash:
    - MD5: 74B6CB94FA7823F226CFE862D0D8F65
    - SHA1: 8210DFDE1A045EA09A7683CC04081BD316205470
    - SHA256: 6515BDA500BF9E89FBCA8D507FE098C11EB298CDC544405A5B1B1E4FBB12D2

2. Comportamento del File

2.1 Attività Malevole

Queste azioni confermano l'intento dannoso del file:

- Esecuzione con un certificato non affidabile
    - Il file si avvia senza un certificato digitale valido, il che lo rende sospetto e non verificabile.



    - Implicazione: Questo comportamento indica che l'eseguibile potrebbe bypassare controlli di sicurezza o provenire da fonti malevole.
- Modifica delle impostazioni di avvio automatico (autorun) nel registro
    - Il malware inserisce o modifica voci nel registro di sistema per garantirsi persistenza, avviandosi ogni volta che il sistema viene riavviato.
    - Chiave di registro coinvolta: Autorun
    - Implicazione: Persistenza sul sistema e possibile esecuzione non rilevata di payload aggiuntivi.

2.2 Attività Sospette

Queste azioni non sono immediatamente malevole ma suscitano preoccupazione:

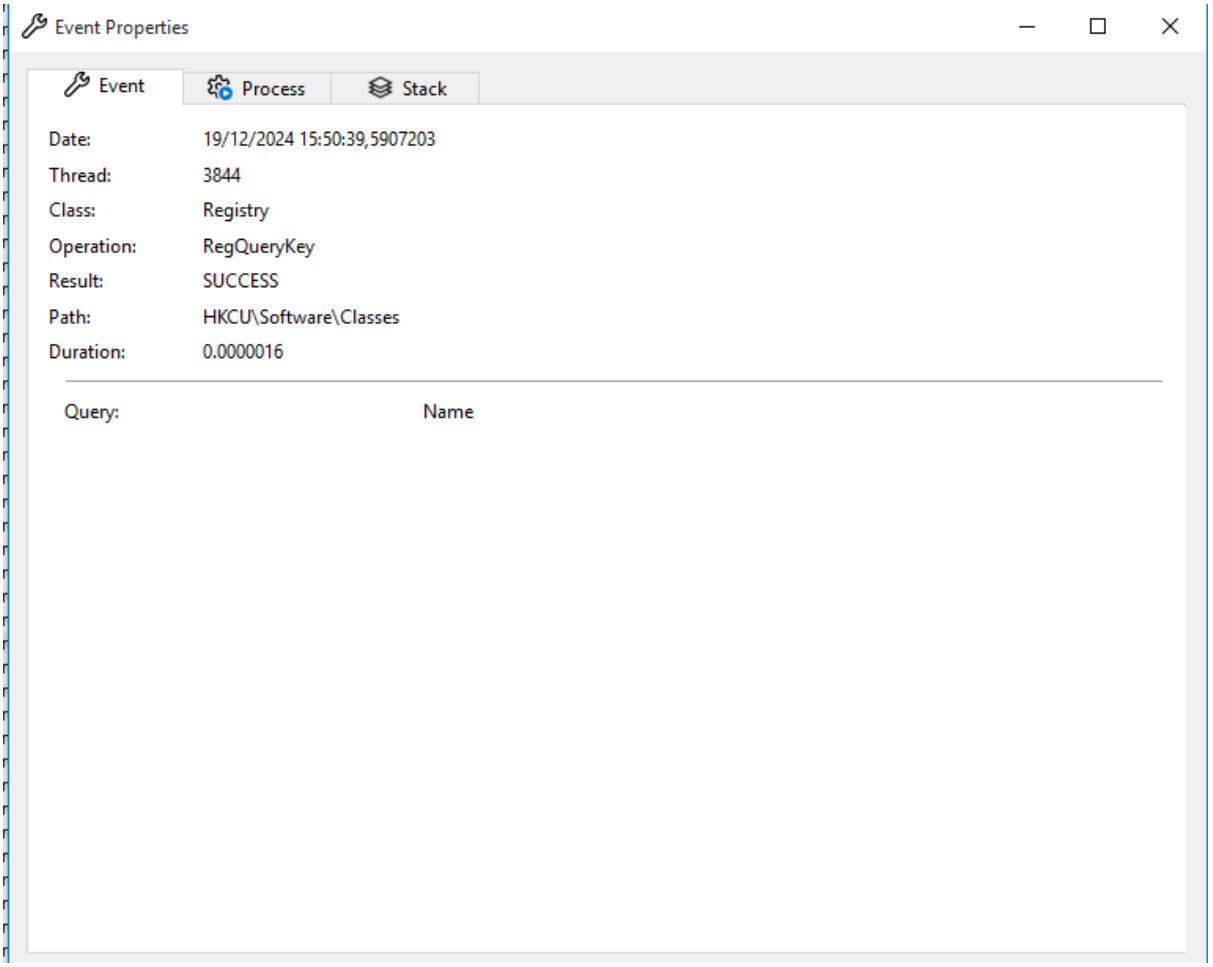
1. Sovrascrittura o rilascio di file eseguibili
    - Il file crea nuovi eseguibili o sovrascrive quelli esistenti.
    - Implicazione: Potrebbe installare altri malware o alterare file critici per compromettere il sistema.
2. Lettura delle impostazioni di sicurezza di Internet Explorer
    - Il malware raccoglie dettagli sulle configurazioni di sicurezza del browser.
    - Implicazione: Può modificare o indebolire i parametri di protezione per facilitare attacchi basati sul browser, come download dannosi o script malevoli.
3. Verifica delle impostazioni di fiducia di Windows
    - Controllo delle politiche di sicurezza e certificati di fiducia del sistema.
    - Implicazione: Il malware potrebbe prepararsi per escalation dei privilegi o bypass delle difese di Windows.

2.3 Attività Informative

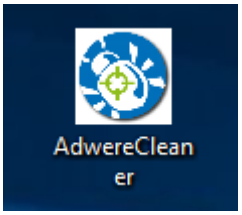
Queste azioni suggeriscono la raccolta di informazioni utili da parte del malware:

- Utilizzo del file scaricato
    - Processi come msedge.exe richiamano il file eseguibile scaricato.
    - Processi coinvolti:
        - msedge.exe (PID: 3812)
        - AdwereCleaner.exe (PID: 488)
    - Implicazione: Possibile interazione con browser o esecuzione di comandi aggiuntivi.
- Lettura delle variabili di ambiente
    - Il file raccoglie variabili di sistema, come PATH, OS, utente corrente, ecc.
    - Processi coinvolti:
        - identity_helper.exe
        - 6AdwCleaner.exe
    - Implicazione: Fingerprinting del sistema per adattare il comportamento del malware.

- Lettura del nome del computer e GUID dal registro
    - Recupera il nome del sistema e il GUID univoco (identificatore).



    - Processi coinvolti:
        - 6AdwCleaner.exe (PID: 3888)
        - AdwereCleaner.exe (PID: 488)
    - Implicazione: Rilevamento e tracciamento della macchina per campagne mirate.
- Esecuzione manuale da parte dell'utente
    - Il file richiede interazione per essere avviato.
    - Implicazione: Potrebbe mascherarsi come un programma utile o legittimo per ingannare l'utente.



3. Implicazioni per il Sistema

1. Persistenza:
    - Tramite modifiche alle chiavi autorun, il malware si garantisce l'avvio automatico ad ogni riavvio del sistema.
2. Compromissione della Sicurezza:
    - Modifica o verifica delle impostazioni di sicurezza di Windows e browser per indebolire le difese del sistema.
3. Esecuzione di Payload Aggiuntivi:
    - Rilascia o sovrascrive file eseguibili, aprendo la strada ad altri malware o esecuzioni dannose.
4. Raccolta di Informazioni:
    - Raccolta di variabili di ambiente, nome del computer e GUID per fini di fingerprinting o tracciamento.
5. Interazione con l'Utente:
    - Il malware può richiedere esecuzione manuale, suggerendo un attacco ingegneristico-sociale (inganno dell'utente).

4. Raccomandazioni per la Mitigazione

1. Eliminazione Immediata:
    - Rimuovere il file AdwCleaner.exe dal sistema e isolarlo per ulteriori analisi.
2. Scansione Antivirus e Anti-malware:
    - Eseguire una scansione completa con strumenti affidabili come Windows Defender, Malwarebytes o ESET.
3. Verifica del Registro:
    - Controllare le chiavi di registro autorun e rimuovere eventuali voci sospette:
        - Percorso: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
4. Monitoraggio del Traffico di Rete:
    - Analizzare le connessioni di rete per rilevare attività sospette di comunicazione con server esterni.
5. Ripristino delle Impostazioni di Sicurezza del Browser:
    - Ripristinare le configurazioni di Internet Explorer o altri browser utilizzati.
6. Isolamento della Macchina:
    - Disconnettere la macchina dalla rete per evitare ulteriori compromissioni o movimenti laterali.
7. Utilizzo di Soluzioni EDR:
    - Implementare soluzioni di Endpoint Detection and Response (EDR) per rilevare comportamenti anomali e dannosi.

Conclusione

Il file AdwCleaner.exe dimostra chiari comportamenti malevoli, come la modifica del registro per ottenere persistenza, il rilascio di eseguibili sospetti e la raccolta di dati di sistema. Tali attività sono indicatrici di un malware progettato per compromettere la sicurezza del sistema, indebolire le protezioni e prepararsi ad attacchi futuri.