Report di Analisi Malware: AdwCleaner.exe

Data dell'Analisi: 2025-04-14

1. Introduzione

Questo report documenta l'analisi statica e dinamica del file AdwCleaner.exe. L'analisi dinamica è stata condotta principalmente in un ambiente controllato Flare VM senza connessione internet, con monitoraggio tramite Procmon e Regshot. Per integrare l'analisi del traffico di rete, sono stati consultati i risultati di un'analisi automatizzata fornita da ANY.RUN. L'analisi dinamica ha rivelato attività sospette e potenzialmente malevole. Il file esegue un secondo eseguibile (6AdwCleaner.exe), legge le impostazioni di sicurezza di Internet Explorer e stabilisce la persistenza all'avvio del sistema modificando il valore autorun nel registro di Windows. L'analisi del traffico di rete, condotta tramite ANY.RUN, ha rivelato la comunicazione con un dominio che presenta indicazioni di essere associato a contenuti malevoli.

2. Dettagli del File:

Nome del File: AdwCleaner.exe

Tipo di File: Portable Executable 32 bit

Dimensioni: 190.82 KB (195,408 bytes)

Hash:

MD5: 248aadd395ffa7ffb1670392a9398454

SHA-1: c53c140bbdeb556fca33bc7f9b2e44e9061ea3e5

SHA-256: 51290129cccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc

Data di Creazione (Creation Time): 2013-12-25 05:01:41 UTC

3. Analisi Statica:

Strumenti Utilizzati: CFF Explorer, PEStudio

Formato del File: L'analisi statica ha confermato che AdwCleaner.exe è un eseguibile Portable Executable (PE) a 32 bit. L'esame delle sezioni PE e delle importazioni DLL tramite CFF Explorer e PEStudio [aggiungere qui dettagli specifici se hai identificato importazioni sospette o sezioni inusuali]. L'analisi delle firme del file suggerisce che potrebbe trattarsi un eseguibile compilato con Visual C++.

4. Analisi Dinamica:

Ambiente di Esecuzione: Flare VM

Strumenti di Monitoraggio: Procmon (Process Monitor), Regshot.

Analisi del Traffico di Rete: A causa della mancanza di connessione internet nella Flare VM durante l'analisi dinamica, l'analisi del traffico di rete è stata integrata consultando i risultati di un'analisi condotta da ANY.RUN.

Osservazioni Comportamentali (Analisi Manuale):

File Dropped: Durante l'esecuzione, AdwCleaner.exe ha creato un nuovo file eseguibile denominato 6AdwCleaner.exe nel percorso C:\Users\AppData\Local\. L'hash SHA256 di questo file è 4F0033E811FE2497B38F0D45DF958829D01933EBE7D331079EEFC8E38FBEAA61. Questo comportamento di "dropping" è comune per alcuni tipi di malware che utilizzano un "loader" per eseguire il payload principale.

Lettura Impostazioni di Sicurezza di Internet Explorer: È stata osservata attività di lettura di chiavi di registro e/o file di configurazione relativi alle impostazioni di sicurezza di Internet Explorer sia da AdwereCleaner.exe che da 6AdwCleaner.exe. Questo potrebbe suggerire un tentativo di verificare o manipolare queste impostazioni.

Creazione Servizio Autorun: L'analisi manuale con Procmon ha rilevato che 6AdwCleaner.exe crea un servizio autorun per la persistenza. [Aggiungere qui dettagli specifici se hai il nome del servizio e le chiavi di registro coinvolte dalla tua analisi manuale.]

Modifica del Valore Autorun nel Registro: È stata rilevata una modifica al registro di sistema che stabilisce la persistenza del file 6AdwCleaner.exe all'avvio del sistema. In particolare, è stata scritta una voce nella chiave HKCU\Software\Microsoft\Windows\CurrentVersion\Run con il nome AdwCleaner e il valore "C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe".

Osservazioni sul Traffico di Rete (da ANY.RUN): L'analisi del traffico di rete condotta da ANY.RUN ha rivelato che il processo ha stabilito connessioni, inclusa la comunicazione con il dominio www.vikingwebscanner.com. Questo dominio presenta indicazioni di essere associato a contenuti malevoli, suggerendo una potenziale interazione con un server di comando e controllo o la distribuzione di ulteriore malware.

5. Indicatori di Compromissione (IOCs):

AdwereCleaner.exe

6AdwCleaner.exe

Percorso del File Dropped: C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe

Chiave di Registro per la Persistenza:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AdwCleaner con valore "C:\Users\FlareVM\AppData\Local\6AdwCleaner.exe" -auto

Dominio Sospetto: www.vikingwebscanner.com

Comportamento Osservato: Dropping di un eseguibile, lettura delle impostazioni di sicurezza di IE (Internet Explorer), creazione di un servizio autorun, modifica del valore autorun nel registro, comunicazione di rete con un dominio sospetto.

6. Conclusioni:

L'analisi dinamica di AdwCleaner.exe, integrata con l'analisi del traffico di rete condotta esternamente, indica chiaramente la presenza di attività malevole. Il rilascio di un secondo eseguibile, la sua persistenza stabilita tramite la modifica del registro di sistema e la comunicazione con un dominio sospetto suggeriscono che questo file non è uno strumento legittimo di pulizia adware, ma piuttosto un malware progettato per persistere sul sistema ed eseguire azioni potenzialmente dannose, inclusa la comunicazione con infrastrutture esterne.

Raccomandazioni:

Il file AdwCleaner.exe e il file "dropped" 6AdwCleaner.exe devono essere considerati malware e rimossi immediatamente dal sistema.

Si raccomanda una scansione completa del sistema con un software antivirus aggiornato per rilevare ed eliminare eventuali componenti aggiuntivi o modifiche apportate da questo malware.

Se possibile effettuare un backup alla versione precedente all'installazione dei file malevoli.