REPORT ANALISI MALWARE

File: AdwereCleaner.exe

HASH:

MD5: 248aadd395ffa7ffb1670392a9398454

SHA-1: C53C140B8DEB556FCA33BC7F9B2E44E9061EA3E5

Dimensione: 195400 bytes

ANALISI PRELIMINARE: Il file sembra essere un installer NSIS (Nullsoft Scriptable Install System), ma potrebbe essere un malware mascherato da software legittimo.

FUNZIONALITÀ IDENTIFICATE:

Il malware AdwereCleaner.exe mostra diverse capacità avanzate, utilizzando API specifiche per raggiungere vari obiettivi:

1. **Gestione File e Directory**: Utilizza funzioni come CreateFileA, DeleteFileA e CopyFileA per manipolare i file (cancellare, spostare, creare directory) e SHFileOperationA per operazioni di gestione file più complesse.
2. **Accesso e Modifica del Registro di Sistema**: Sfrutta funzioni come RegCreateKeyExA e RegSetValueExA per creare o modificare chiavi nel registro di sistema, e RegDeleteKeyA per rimuoverle, il che facilita sia la persistenza che l'occultamento delle tracce.
3. **Gestione del Contesto di Esecuzione**: Funzioni come LoadLibraryA e GetProcAddress permettono di caricare librerie dinamicamente, modulando il comportamento del malware in base all'ambiente.
4. **Privilegi Elevati e Accesso ai Processi**: Utilizza AdjustTokenPrivileges e OpenProcessToken per ottenere privilegi elevati e accedere a token di sicurezza, aumentando il controllo sul sistema.
5. **Interazione con l'Interfaccia Utente**: Funzioni come FindWindowExA e SendMessageA consentono di interagire con finestre aperte, suggerendo la capacità di monitorare o influenzare le interazioni utente.
6. **Persistenza e Installazione**: Riferimenti a messaggi di errore di integrità e funzioni come CreateProcessA indicano che il malware si presenta come un installer, permettendo di eseguire processi e mantenere la persistenza.

Parallelamente, l'analisi rivela:

- **Uso di Certificati Digitali**: Certificati di autorità note (come DigiCert e COMODO) potrebbero essere utilizzati per firmare digitalmente il codice, camuffando il malware come software legittimo.

- **Verifica di Certificati**: Include URL di revoca (CRL) e servizi OCSP per verificare i certificati, mostrando un tentativo di rafforzare l’apparenza di legittimità.
- **Possibili Identità False**: Sono presenti riferimenti a nomi di aziende e email che potrebbero rappresentare entità fasulle, come "WAT Software Rotterdam," per simulare autenticità.

Nel complesso, questo malware sfrutta metodi sofisticati per la persistenza, la mimetizzazione e l'accesso elevato, con l’obiettivo di aggirare i sistemi di sicurezza e mantenere il controllo sul sistema compromesso.

REPORT ANALISI MODIFICHE AL REGISTRO

Data: 28 Ottobre 2024 Computer: DESKTOP-V34O7KL Utente: flare Intervallo temporale: 13:54:12 - 14:01:28

SOMMARIO MODIFICHE:

- Chiavi aggiunte: 12
- Valori aggiunti: 30
- Valori modificati: 23
- Totale cambiamenti: 65

ANALISI PRINCIPALI MODIFICHE:

1. **Installazione Certificati:**

- Aggiunto certificato Sectigo (UTN Object) nel percorso: HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\E12DFB4B41D7D9C32B30514BAC1D81D8385E2D46

2. **Tracciamento e Logging:**

- Creati due set di chiavi per il tracciamento (RASAPI32 e RASMANCS):
    - HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
    - HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
- Disabilitati vari tipi di tracciamento (EnableFileTracing, EnableAutoFileTracing, EnableConsoleTracing)

3. **Modifiche alla Persistenza:**

- Aggiunta chiave di avvio automatico: HKU... \SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AdwCleaner Con valore: "C:\Users\flare\AppData\Local\6AdwCleaner.exe" -auto

4. **User Interface e Shell:**

- Numerose modifiche alle impostazioni della shell di Windows
- Modifiche alle posizioni delle finestre e impostazioni di visualizzazione
- Aggiornamenti a UserAssist per il tracciamento dell'utilizzo delle applicazioni

5. **Registrazione Programma:**

- Creata chiave: HKU...\SOFTWARE\AdwCleaner
- Aggiunto ID univoco per l'installazione