BW3- Esercizio 1

Malware Analysis - Analisi Statica e Dinamica: AdwereCleaner.exe

Autore: Cybereagles

Classificazione: Adware / PUA (Potentially Unwanted Application) - Dropper

---

Sintesi

Il presente report documenta l'attività di **Malware Analysis** (Statica e Dinamica) condotta sul campione sospetto denominato **AdwereCleaner.exe**. L'analisi ha confermato che il file, presentatosi superficialmente come una utility di pulizia per il sistema, è in realtà un'applicazione potenzialmente indesiderata (PUA) operante come **dropper**. Il test ha dimostrato la capacità del malware di ingannare l'utente con finti prompt di attivazione, eludere i controlli dell'UAC (**User Account Control**) installando copie di sé stesso in directory non privilegiate (**AppData**), alterare pesantemente le policy di sicurezza di Windows (modifica della **ZoneMap**) e stabilire comunicazioni non autorizzate con un'infrastruttura di **Comando e Controllo (C2)** remota a scopo di tracking.

Scopo del test e analisi dello scenario

Scenario e Obiettivi

L'attività di reverse engineering e analisi comportamentale si è svolta all'interno di un ambiente di laboratorio rigorosamente isolato (**Sandbox**) per prevenire la compromissione dell'host fisico e la propagazione sulla rete locale.

- **Ambiente di Analisi:** FlareVM (Windows OS), configurato con Network Adapter in modalità Non connesso e funzionalità di Snapshot per il ripristino istantaneo.
- **Target:** Eseguibile binario **AdwereCleaner.exe** (SHA-256: 51290129CCCCA38C6E3B4444D0DFB8D848C8F3FC2E5291FC0D219FD642530ADC).
- **Obiettivo Principale:** Identificare i vettori di infezione, estrarre gli **Indicatori di Compromissione** (IoC) a livello host e network, documentare le alterazioni al sistema operativo e definire una procedura sicura di eradicazione e mitigazione.

Strumenti Utilizzati

- **PowerShell (Get-FileHash):** Per il calcolo dell'impronta crittografica e la verifica dell'integrità del campione.
- **Detect It Easy (DIE):** Strumento essenziale di reverse engineering utilizzato per l'analisi dell'entropia, l'identificazione del compilatore nativo, dell'architettura e per rilevare firme di eventuali packer o installer (es. identificazione di NSIS).

- **CFF Explorer:** Suite per l'analisi profonda dell'intestazione PE (Portable Executable), utilizzato per esaminare le sezioni del dropper iniziale.
- **dnSpy:** De-compilatore e debugger per ambienti .NET. Strumento fondamentale utilizzato per disassemblare il payload secondario (**AdwareBooC**), permettendo l'analisi in chiaro del codice sorgente, l'individuazione delle API critiche e l'estrazione degli URL di Comando e Controllo (C2).
- **Process Monitor (Procmon) / Sysinternals:** Per il tracciamento dinamico e granulare delle chiamate di sistema (API Hooking), con particolare focus sulle modifiche al File System e al Registro di configurazione.
- **Wireshark:** Analizzatore di protocolli di rete utilizzato per l'intercettazione dei pacchetti (PCAP) durante la detonazione, al fine di validare dinamicamente le comunicazioni HTTP in uscita verso l'infrastruttura C2.

Svolgimento

Fase 1: Analisi Statica (Assessment Preliminare)

L'analisi statica ha permesso di dissezionare la struttura del campione e di mapparne le funzionalità primarie senza procedere alla detonazione.

1.1 Struttura del File e Vettori di Infezione

L'indagine iniziale condotta tramite **Detect It Easy (DIE)** ha rivelato l'assenza di packer complessi, identificando immediatamente l'eseguibile AdwereCleaner.exe come un **installer NSIS SFX** (Nullsoft Scriptable Install System - Self-Extracting). La sua funzione primaria è quella di fungere da "dropper": una volta avviato, estrae silenziosamente ed esegue il vero payload malevolo, che DIE ha identificato essere stato compilato in **.NET** (internamente noto come AdwareBooC).

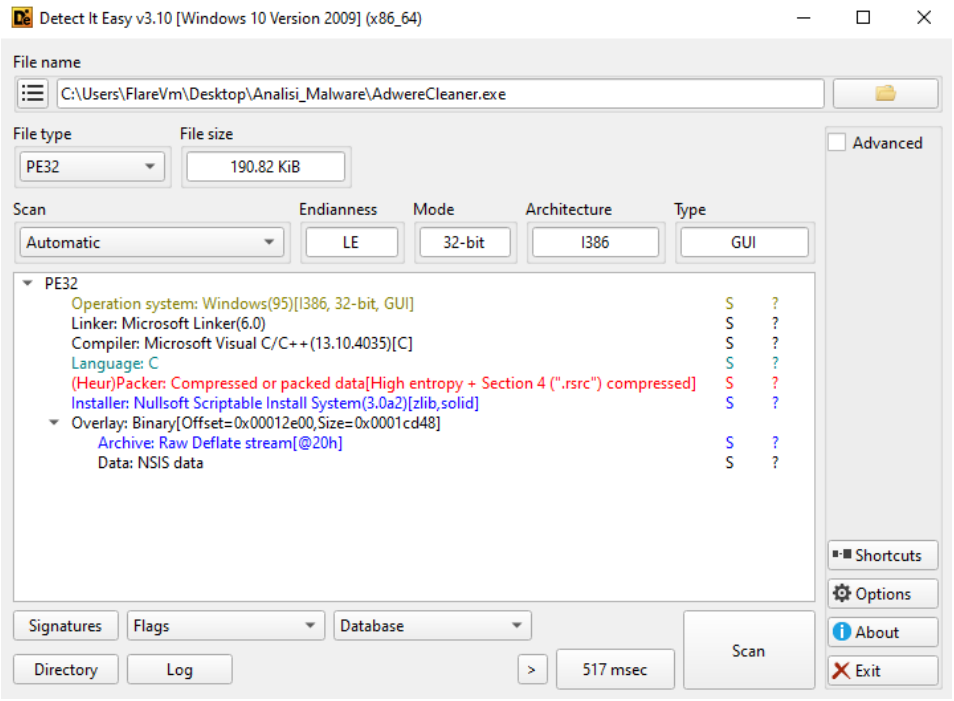

Figura 1 Identificazione dell'architettura e del compilatore tramite Detect It Easy.

1.2 Flusso di Esecuzione e Finta Attivazione (Trial Version)

Approfondendo l'analisi del binario, il payload .NET estratto dall'installer NSIS è stato de-compilato **tramite dnSpy**. Questo ha permesso di ispezionare direttamente il codice sorgente in C#, analizzando le stringhe in chiaro e le chiamate API effettuate dal malware. Da questo esame è emerso un comportamento tipico dei ***Rogue Antivirus / Fleeceware***:

- Il malware presenta all'utente un finto avviso di "**Trial Version**".
- Include un form di attivazione (serial). Se l'utente interagisce simulando un'attivazione, il software utilizza l'API `File.WriteAllText` per creare un file indicatore (marker) denominato licensed all'interno della directory `%APPDATA%`.
- Successivamente, istanzia un processo (`Process.Start`) per aprire il browser predefinito reindirizzando la vittima verso l'URL: http://www.vikingwebscanner.com/succes/index.php.
- Subito dopo questa finta attivazione, il malware tenta di ripulire le proprie tracce iniziali eliminando la chiave Run dal registro.

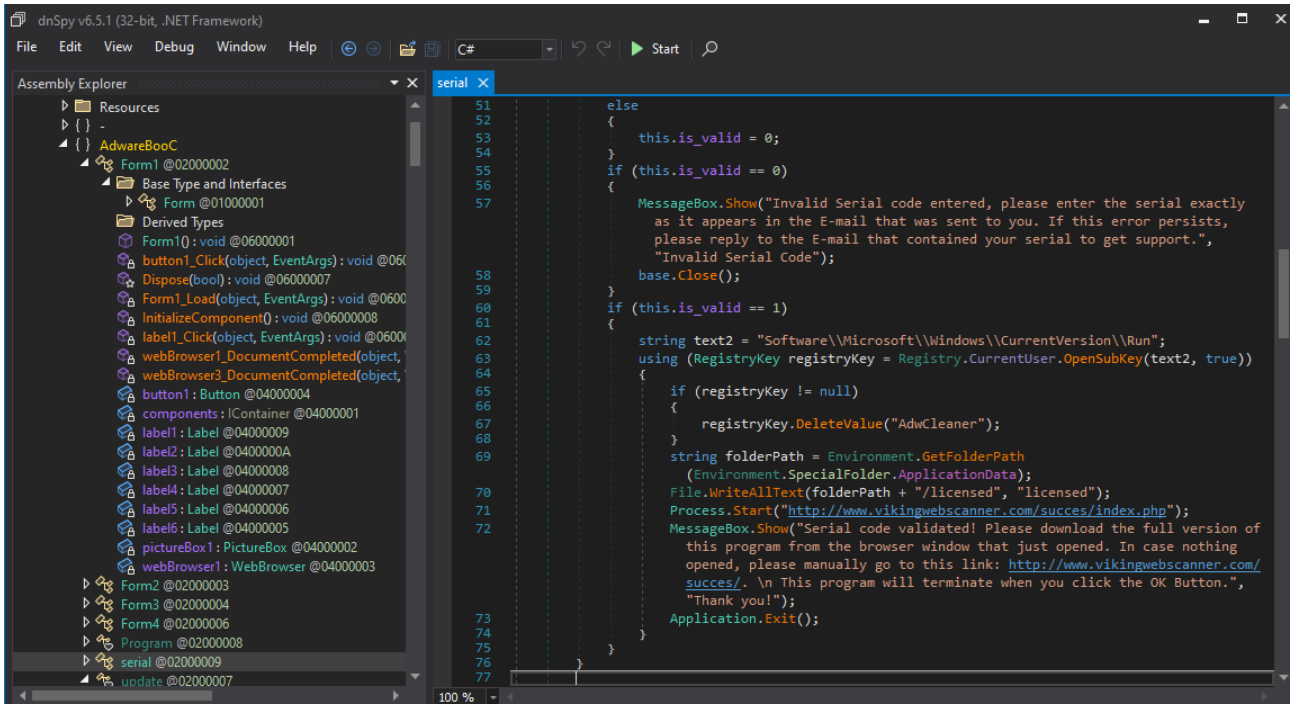

Figura 2 Dettaglio della funzione di convalida del seriale. Il codice conferma la creazione del file marker "licensed" in %APPDATA% e l'uso di Process.Start per forzare l'apertura del browser verso l'URL di redirect dopo la finta attivazione.

1.3 Telemetria, Tracking e Persistenza

Il codice del payload mostra routine di tracking avanzate e tentativi di garantirsi la persistenza nel sistema:

- **Persistenza:** Sono presenti istruzioni per l'inserimento del valore `AdwCleaner = "<path> -auto"` all'interno della chiave di registro `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`. Questo garantisce che il malware si riavvii automaticamente, in background, a ogni login dell'utente.
- **Tracking e C2:** Il payload interroga un'infrastruttura di Comando e Controllo (C2) registrando le nuove infezioni e lo stato della macchina tramite richieste HTTP GET (`/scripts/new_install.php?owner=<owner>`), salvando un ID univoco della vittima nel registro (`HKCU\Software\AdwCleaner -> value: id`).

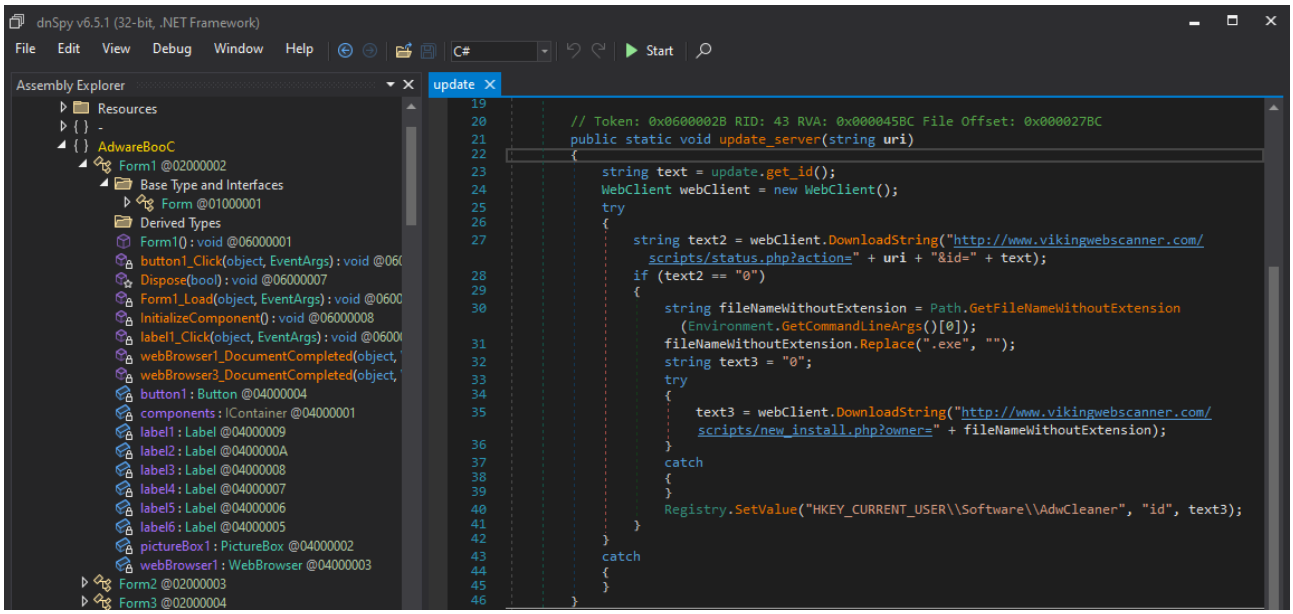

Figura 3 Dettaglio della routine di telemetria. Il malware contatta l'infrastruttura C2 per registrare la nuova infezione e memorizza un identificativo univoco (ID) nel registro di sistema per scopi di tracking.

Fase 2: Analisi Dinamica (Detonazione e Monitoraggio)

Per validare le ipotesi formulate in fase statica, il malware è stato **detonato** all'interno della **FlareVM**. Il tracciamento tramite **Process Monitor** ha generato un log di oltre 11.600 eventi. L'applicazione di filtri mirati (esclusione del rumore di fondo, inclusione esclusiva del processo AdwereCleaner.exe e delle operazioni con esito **SUCCESS**) ha permesso di isolare le seguenti azioni critiche e confermare gli IoC definitivi:

2.1 Attività sul File System (Dropping ed Evasione UAC)

L'analisi degli eventi `WriteFile` e `CreateFile` ha rivelato che il malware agisce interamente nello spazio utente (User-Space), bypassando la necessità di privilegi di Amministratore. Questo garantisce un'infezione silenziosa senza innescare i prompt del Controllo Account Utente (UAC). Sono stati scritti i seguenti artefatti su disco:

- `C:\Users\FlareVm\AppData\Local\6AdwCleaner.exe` (Copia del payload malevolo per garantire la persistenza).
- `C:\Users\FlareVm\AppData\Local\Temp\nst2287.tmp` (File temporaneo legato all'estrazione NSIS).

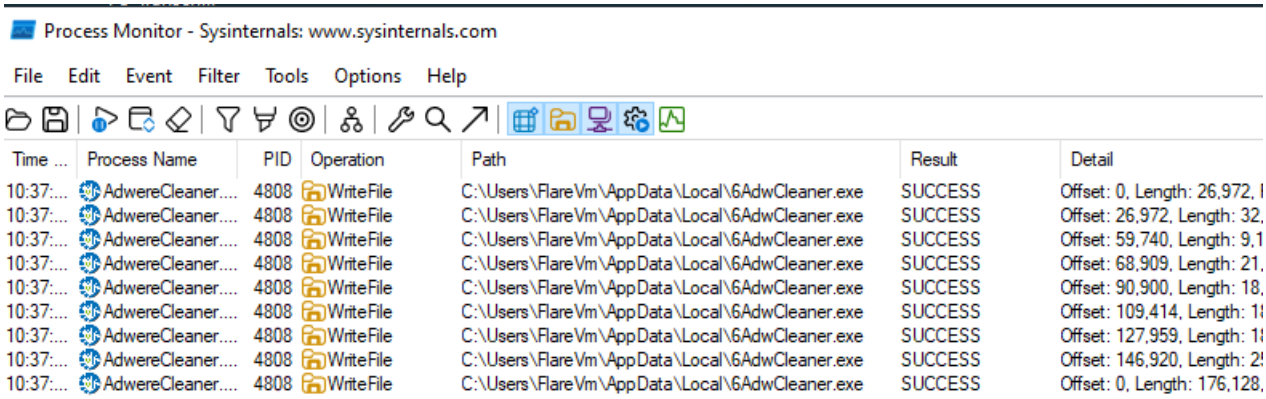

Figura 4 Output di Procmon che documenta l'azione di dropping del payload secondario all'interno della directory nascosta AppData.

2.2 Alterazione Furtiva del Registro di Sistema (Abbassamento delle Difese)

L'analisi degli eventi `RegSetValue` ha portato alla luce il comportamento più critico del malware: l'alterazione mirata delle chiavi di registro preposte alla gestione della sicurezza di rete in ambiente Windows. Il malware ha iniettato parametri all'interno delle Internet `Settings\ZoneMap`:

- `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass`
- `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName`
- `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet`
- `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect`

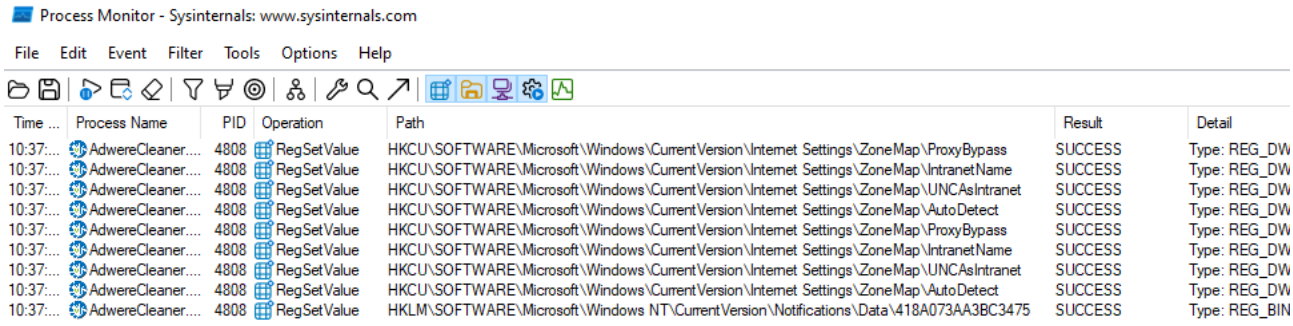

Figura 5 Tracciamento delle modifiche al registro finalizzate all'indebolimento delle policy di sicurezza di rete (ZoneMap).

2.3 Analisi del Traffico di Rete (Efficacia del contenimento)

Il monitoraggio di rete tramite **Wireshark** ha rilevato continui messaggi di ***ICMP Destination Unreachable*** provenienti e diretti all'host locale. Questo conferma i tentativi del malware di contattare l'infrastruttura C2 individuata nell'analisi statica. Tuttavia, grazie alla rigorosa configurazione isolata della **Sandbox** (assenza di risoluzione DNS e di routing verso l'esterno), le richieste di tracking HTTP non sono mai state generate, impedendo con successo l'esfiltrazione dei dati

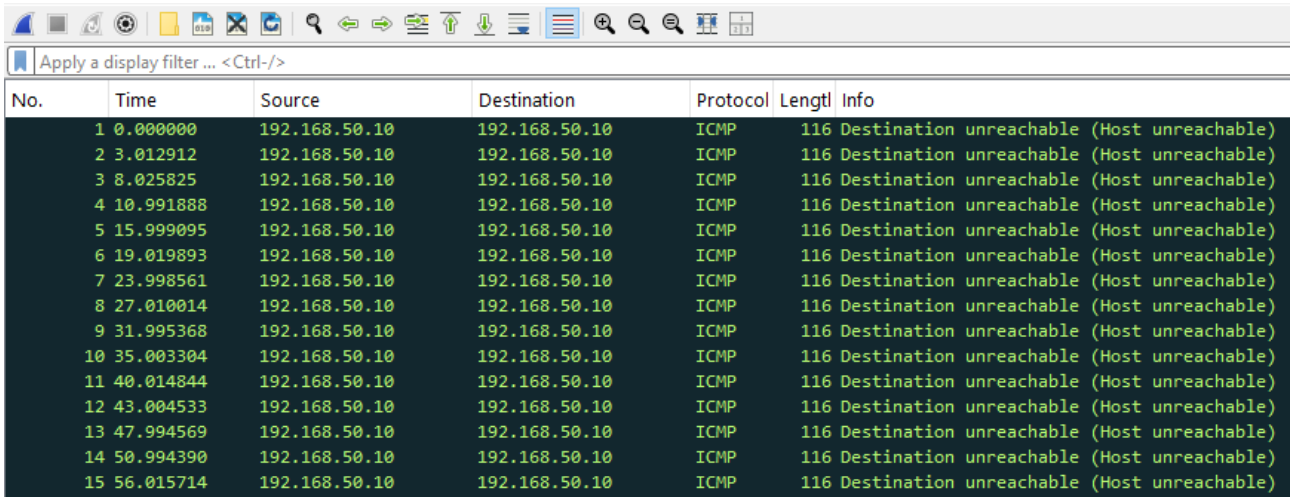

Figura 6 Dimostrazione dell'isolamento corretto

Analisi del Rischio

La manipolazione della `ZoneMap` è una tecnica elusiva ben nota. Modificando questi valori, il malware istruisce il sistema operativo a bypassare eventuali **proxy** di sicurezza aziendali e a mappare specifiche risorse esterne (o **percorsi UNC**) come se facessero parte della **Intranet Locale** (che gode di policy di sicurezza molto più permissive rispetto alla zona "Internet"). Questo facilita il download di payload aggiuntivi senza far scattare gli avvisi di sicurezza nativi di Windows.

Fase 3: Pulizia delle Tracce (Remediation)

La rimozione di un malware che ha dimostrato la capacità di alterare configurazioni di sistema profonde (come la ZoneMap) tramite la semplice cancellazione manuale dei file droppati in `%AppData%` e delle chiavi di registro visibili **non è una pratica sicura né ammissibile** in ambito di **Incident Response**. Questo approccio non garantisce la rimozione di eventuali hook in memoria o componenti offuscati.

Procedura di Eradicazione Applicata:

1. Isolamento totale della FlareVM dalla rete virtuale (scollegamento interfaccia).
2. Spegnimento forzato del sistema operativo ospite.
3. Esecuzione del comando di **Restore Snapshot** (ripristino allo stato pre-detonazione) tramite il pannello di controllo dell'Hypervisor. Questo metodo assicura la distruzione crittografica di ogni modifica apportata dal malware al disco virtuale e alla RAM, garantendo il ritorno a uno stato crittograficamente "Clean" e verificato.

Conclusioni e Mitigazione

L'attività di testing ha confermato in modo inequivocabile che AdwereCleaner.exe non è un software legittimo. Si tratta di un Adware nocivo che impiega tecniche di dropper, sfrutta l'ingegneria sociale (finto

avviso di trial) e manipola furtivamente le policy di sicurezza di sistema (ZoneMap) per stabilire persistenza, eludere i proxy ed esfiltrare dati telemetrici verso server di terze parti.

Al fine di mettere in sicurezza gli endpoint aziendali da minacce basate sulle medesime Tattiche, Tecniche e Procedure (TTPs), si raccomanda l'implementazione immediata delle seguenti azioni correttive:

1. **Protezione Perimetrale (Network/EDR):** Inserire l'Hash SHA-256 (51290129CCCCA38C6E3B4444D0DFB8D848C8F3FC2E5291FC0D219FD642530ADC) e i domini associati all'infrastruttura C2 (*vikingwebscanner.com*) nelle **blocklist** dei **Firewall** aziendali e delle piattaforme EDR (**Endpoint Detection and Response**).
2. **Hardening delle Directory Utente:** Implementare **Software Restriction Policies (SRP)** tramite Active Directory o AppLocker per negare l'esecuzione di file .exe e script non firmati digitalmente qualora vengano lanciati direttamente dai percorsi `%AppData%`, `%LocalAppData%` e `%Temp%` (vettori di infezione standard per i dropper).
3. **Monitoraggio e Blocco del Registro:** Configurare l'**EDR** per generare alert ad alta priorità e bloccare automaticamente qualsiasi processo non autorizzato (es. processi non appartenenti a System o TrustedInstaller) che tenti di alterare le chiavi di registro sotto l'hive Internet `Settings\ZoneMap` e `CurrentVersion\Run`.