Alerta

Técnica

Campaña de Adware/Trojan WebCompanion

COLCERT AL – 20260321 - 098

TIC

TLP:CLEAR

Resumen Ejecutivo

Se ha identificado actividad relacionada con el **instalador de Web Companion (desarrollado por Lavasoft/Adaware)**. Aunque se promociona como una herramienta de seguridad, este software exhibe comportamientos intrusivos de tipo troyano, incluyendo persistencia mediante llaves de registro, modificación de configuraciones del navegador y telemetría no autorizada.

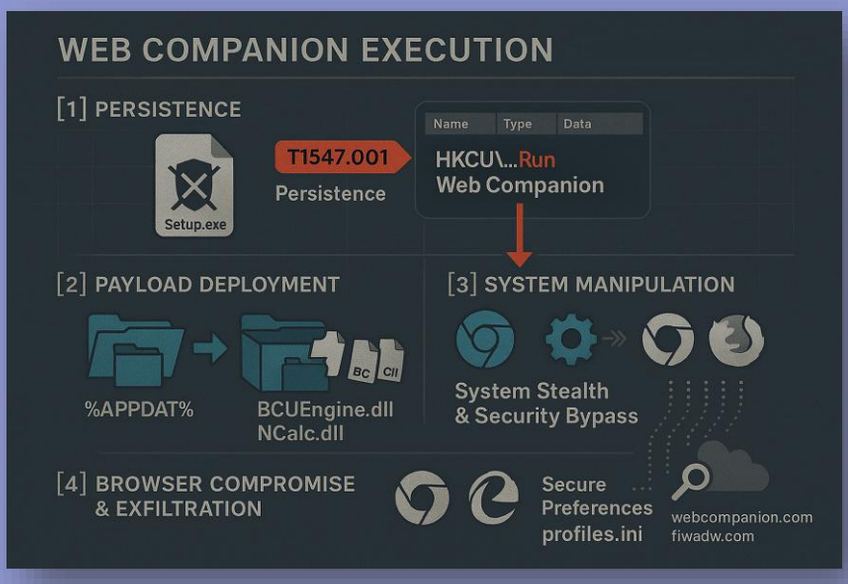
NIVEL DE RIESGO

MEDIO

Análisis de Comportamiento (TTPs)

El malware utiliza la técnica de MITRE ATT&CK **T1547.001 (Registry Run Keys / Startup Folder)** para garantizar su persistencia en el sistema tras el reinicio. Una vez instalado, el software conecta con servidores externos para descargar componentes adicionales en formato ZIP y DLL, modificando las zonas de seguridad del navegador para facilitar su actividad publicitaria y de recolección de datos.

Persistencia y modificación del sistema

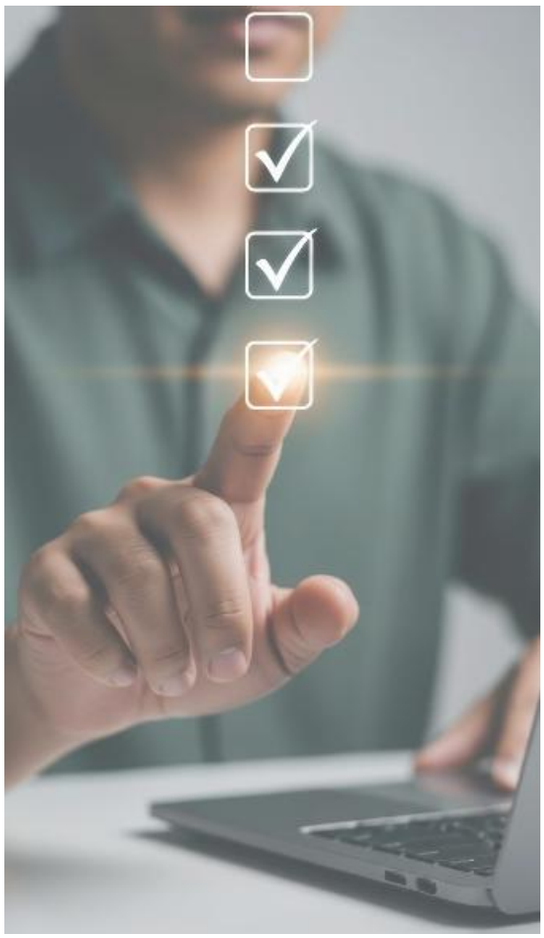


- **Modificación del registro:** El instalador modifica la Runclave de Windows para garantizar WebCompanion.exe que se inicie automáticamente durante el inicio de sesión del usuario:HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Web Companion.
- **Secuestro de navegador:** El análisis de Sigma confirma que el malware intenta cambiar la configuración de zona de Internet Explorer y ocultar las extensiones de archivo para disimular su presencia. También ataca a Google Chrome y Mozilla Firefox accediendo a los archivos de preferencias y, potencialmente, modificándolos.
- **Infraestructura:** El ejecutable coloca numerosos componentes en **%APPDATA%\Roaming\Lavasoft\Web Companion\Application**, incluyendo binarios adicionales como7za.exe y DLL especializadas para el manejo de archivos zip y la administración de bases de datos.

Medidas de mitigación

Identificación y eliminación

- **Escaneo y cuarentena**: Utilice una solución de detección y respuesta (EDR) o antimalware de buena reputación para realizar un escaneo completo del sistema. Este archivo es detectado por 34 motores como **trojan.webcompanion/msilo PUP.Optional.WebCompanion**.
- **Desinstalar la aplicación**: Intente desinstalar "Web Companion" a través del Panel de control de Windows. Sin embargo, se recomienda la limpieza manual de los archivos **%APPDATA%\Roaming\Lavasoft\residuales %LOCALAPPDATA%\Lavasoft\.**
- **Limpieza del registro**: Elimine la entrada de persistencia ubicada en **HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Web Companion.**



Recomendaciones

- **Bloqueo de dominio**: Bloquee la comunicación a los dominios de comando y control (C2) y de seguimiento identificados, específicamente webcompanion.com, lavasoft.com, y flwadw.com, a nivel de firewall o DNS.
- **Monitorización de Registro**: Configurar alertas para la creación o modificación de valores en las llaves de registro de inicio (Run/RunOnce). Se recomienda el uso de Sysmon (Event ID 13) para este fin.
- Políticas de restricción de software: Implemente AppLocker o políticas de restricción de software similares para evitar la ejecución de instaladores no firmados o no autorizados en directorios temporales (%TEMP%).
- **Seguridad del navegador**: Restablezca la configuración del navegador a los valores predeterminados para Google Chrome y Mozilla Firefox para eliminar las extensiones no deseadas o la configuración de búsqueda secuestrada instalada por este paquete.

Indicadores de Compromiso (IoCs)

Tipo	Indicador	Descripción
Archivo (Hash)	70a10e559c27092a2f22db963989eb8f6c28b846b67b417b4d97a13d462dc56e	Instalador principal (Installer.exe / Setup.exe)
Dominio (C2/Stats)	webcompanion.com	Dominio principal de descarga e instalación
Dominio (C2/Stats)	flwadw.com	Telemetría y estadísticas de eventos
Dominio (C2/Stats)	geo.lavasoft.com	Geolocalización de la víctima

Fuentes

CVE Program. (2025, octubre 8). CVE-2025-45095: Unquoted search path or element in Lavasoft Web Companion versions 8.9.0.1091 through 12.1.3.1037.
https://www.cve.org/CVERecord?id=CVE-2025-45095
Cybersecurity and Infrastructure Security Agency (CISA). (2019, noviembre 7). CVE-2019-25287: WCAssistantService unquoted service path vulnerability in Adaware Web Companion.
https://nvd.nist.gov/vuln/detail/CVE-2019-25287
Google Threat Intelligence. (2026, marzo 21). Análisis estático y dinámico del archivo ejecutable (Hash: 70a10e559c27092a2f22db963989eb8f6c28b846b67b417b4d97a13d462dc56e).
Huntress Labs. (s.f.). Potentially unwanted program (PUP) analysis: Web Companion and its distribution tactics. https://www.huntress.com/blog/
Lavasoft / Adaware. (2026, marzo 21). Web Companion installation and telemetry services.
https://webcompanion.com/
Microsoft Security Response Center. (2024). Evaluation of potentially unwanted applications (PUA) and browser modification behaviors.
https://www.microsoft.com/en-us/security/
MITRE Corporation. (2024). Technique T1547.001: Boot or logon autostart execution: Registry run keys / startup folder. MITRE ATT&CK.
https://attack.mitre.org/techniques/T1547/001/
OnTrust / OneTrust. (2024). Geolocation and compliance telemetry data for bundled applications.
https://www.onetrust.com/
PCrisk Security. (2025). Adware Web Companion (Lavasoft) removal guide and behavior report.
https://www.pcrisk.com/removal-guides/