Investigadores en ciberseguridad han alertado sobre varias extensiones populares de Google Chrome que transmiten información a través de HTTP sin cifrado y contienen secretos codificados directamente en su código, lo que representa serios riesgos para la privacidad y seguridad de los usuarios.

> *«Varias extensiones ampliamente utilizadas [...] transmiten sin querer datos sensibles usando HTTP sin cifrar. Al hacerlo, revelan dominios de navegación, identificadores de máquina, detalles del sistema operativo, métricas de uso e incluso información relacionada con la desinstalación, todo en texto plano»*, indicó Yuanjing Guo, investigador de seguridad del equipo Security Technology and Response de Symantec.

El hecho de que el tráfico de red no esté cifrado implica que estas extensiones son vulnerables a ataques de tipo *«adversario en el medio»* (AitM). Esto significa que actores maliciosos conectados a la misma red, como en un Wi-Fi público, pueden interceptar e incluso modificar los datos transmitidos, lo cual podría derivar en consecuencias mucho más graves.

Las extensiones señaladas incluyen:

- SEMRush Rank (ID: `idbhoeaiokcojcgappfigpifhpkjgmab`) y PI Rank (ID: `ccgdboldgdlngcgfdolahmiilojmfndl`), que acceden al sitio «rank.trellian[.]com» mediante HTTP simple.
- Browsec VPN (ID: `omghfjlpggmjjaagoclmmobgdodcjboh`), que al ser desinstalada realiza una petición HTTP a «browsec-uninstall.s3-website.eu-central-1.amazonaws[.]com».
- MSN New Tab (ID: `lklfbkdigihjaaeamncibechhgalldgl`) y MSN Homepage, Bing Search & News (ID: `midiombanaceofjhodpdibeppmnamfcj`), que envían identificadores únicos de máquina y otros datos a «g.ceipmsn[.]com» a través de HTTP.
- DualSafe Password Manager & Digital Vault (ID:

`lgbjhdkjmpgjgcbcdlhkokkckpjmedgc`), que genera peticiones HTTP hacia «stats.itopupdate[.]com», incluyendo información sobre la versión de la extensión, el idioma del navegador y el tipo de uso.

> *«Aunque no parece que se filtren credenciales o contraseñas, el hecho de que un administrador de contraseñas use solicitudes sin cifrar para telemetría reduce la confianza en su seguridad general»,* subrayó Guo.

Symantec también descubrió extensiones que tienen claves API, secretos y tokens incrustados directamente en el código JavaScript, los cuales podrían ser aprovechados por atacantes para realizar acciones maliciosas:

- Online Security & Privacy (ID: `gomekmidlodglbbmalcneegieacbdmki`), AVG Online Security (ID: `nbmoafcmbajniiapeidgficgifbfmjfo`), Speed Dial [FVD] (ID: `llaficoajjainaijghjlofdfmbjpebpa`) y SellerSprite – Amazon Research Tool (ID: `lnbmbgocenenhhhdojdielgnmeflbnfb`), que contienen una clave secreta de Google Analytics 4 (GA4) que podría usarse para manipular métricas.
- Equatio – Math Made Digital (ID: `hjngolefdpdnooamgdldlkjgmdcmcjnc`), con una clave API de Microsoft Azure incrustada, que podría ser utilizada para generar costos indebidos al desarrollador o agotar sus límites de uso.
- Awesome Screen Recorder & Screenshot (ID: `nlipoenfbbikpbjkfpfillcgkoblgpmj`) y Scrolling Screenshot Tool & Screen Capture (ID: `mfpiaehgjbbfednooihadalhehabhcjo`), que exponen claves de acceso a AWS utilizadas para cargar capturas a un bucket de S3 del desarrollador.
- Microsoft Editor – Spelling & Grammar Checker (ID: `gpaiobkfhnonedkhhfjpmhdalgeoebfa`), que revela una clave de telemetría llamada «StatsApiKey» para registrar datos de usuario.
- Antidote Connector (ID: `lmbopdiikkamfphhgcckcjhojnokgfeo`), que incluye una librería de terceros llamada InboxSDK con credenciales codificadas como claves API.
- Watch2Gether (ID: `cimpffimgeipdhnhjohpbehjkcdpjolg`), que expone una clave API del buscador de GIFs Tenor.

- Trust Wallet (ID: `egjidjbpglichdcondbcbdnbeeppgdph`), que deja visible una clave API asociada a Ramp Network, una plataforma Web3 que permite la compra/venta de criptomonedas desde la app.
- TravelArrow – Your Virtual Travel Agent (ID: `coplmfnphahpcknbchcehdikbdieognn`), que revela una clave de geolocalización al consultar el servicio «ip-api[.]com».

Los atacantes que obtengan estas claves pueden utilizarlas para incrementar costos de servicios API, distribuir contenido ilegal, enviar datos de telemetría falsificados o simular transacciones de criptomonedas, con el riesgo adicional de que el desarrollador pueda ser suspendido de la plataforma.

Preocupa especialmente que Antidote Connector sea solo una de más de 90 extensiones que usan InboxSDK, lo que sugiere que muchas otras podrían tener las mismas vulnerabilidades, aunque Symantec no reveló sus nombres.

> *«Desde secretos de GA4 hasta claves de Azure y credenciales de AWS, cada uno de estos fragmentos de código demuestra cómo unas pocas líneas pueden comprometer servicios enteros. La solución: nunca guardar credenciales sensibles en el cliente*«, comentó Guo.

Los desarrolladores deberían utilizar HTTPS para el envío y recepción de datos, almacenar claves de manera segura en un servidor backend con servicios de gestión de credenciales y rotar estas claves periódicamente para reducir riesgos.

Estos hallazgos demuestran que incluso extensiones populares con cientos de miles de instalaciones pueden estar mal configuradas o contener errores graves de seguridad, como el uso de credenciales codificadas directamente, poniendo en peligro la información del usuario.

> *«Los usuarios de estas extensiones deberían considerar eliminarlas hasta que los desarrolladores solucionen el uso inseguro de [HTTP]. El riesgo no es hipotético; el tráfico sin cifrar es fácil de capturar, y los datos pueden utilizarse para crear perfiles, realizar ataques de phishing o lanzar otros ataques dirigidos»,* advirtió la empresa.
>
> *«La lección general es que una base de usuarios grande o una marca reconocida no garantiza buenas prácticas de seguridad. Las extensiones deben evaluarse según los protocolos que emplean y los datos que transmiten, para asegurar que la información del usuario esté verdaderamente protegida».*