Se ha detectado que una extensión de Google Chrome con la insignia “Featured” y más de seis millones de usuarios recopilaba de forma silenciosa cada mensaje que los usuarios ingresaban en chatbots impulsados por inteligencia artificial (IA), como OpenAI ChatGPT, Anthropic Claude, Microsoft Copilot, DeepSeek, Google Gemini, xAI Grok, Meta AI y Perplexity.

La extensión implicada es Urban VPN Proxy, que cuenta con una calificación de 4.7 en la Chrome Web Store. Se promociona como el “mejor acceso VPN gratuito y seguro a cualquier sitio web, con capacidad para desbloquear contenido”. Su desarrollador es Urban Cyber Security Inc., una empresa con sede en Delaware. En la tienda de complementos de Microsoft Edge, la extensión acumula 1.3 millones de instalaciones.

A pesar de afirmar que permite a los usuarios *“proteger su identidad en línea, mantenerse seguros y ocultar su IP”*, la extensión fue actualizada el 9 de julio de 2025 con el lanzamiento de la versión 5.5.0, la cual incorporó por defecto la recolección de datos de IA mediante configuraciones integradas directamente en el código.

En concreto, este mecanismo funciona a través de un ejecutor JavaScript personalizado que se activa de manera individual para cada uno de los chatbots de IA (por ejemplo, chatgpt.js, claude.js y gemini.js), interceptando y recopilando las conversaciones cada vez que un usuario con la extensión instalada accede a cualquiera de las plataformas objetivo.

Una vez inyectado el script, este reemplaza las API del navegador utilizadas para gestionar solicitudes de red —fetch() y XMLHttpRequest()— con el fin de garantizar que cada petición pase primero por el código de la extensión. De esta forma, se capturan los datos de las conversaciones, incluidos los mensajes de los usuarios y las respuestas de los chatbots, y posteriormente se envían a dos servidores remotos (“analytics.urban-vpn[.]com” y “stats.urban-vpn[.]com”).

La lista exacta de información recopilada por la extensión incluye:

- Mensajes introducidos por el usuario

- Respuestas generadas por el chatbot
- Identificadores de conversación y marcas de tiempo
- Metadatos de sesión
- Plataforma de IA y modelo utilizado

"Las extensiones de Chrome y Edge se actualizan automáticamente de forma predeterminada", señaló Idan Dardikman, de Koi Security, en un informe publicado hoy. *"Los usuarios que instalaron Urban VPN por su función declarada —ofrecer una VPN— se encontraron un día con nuevo código que recopilaba silenciosamente sus conversaciones con IA"*.

Cabe destacar que la política de privacidad actualizada de Urban VPN, vigente desde el 25 de junio de 2025, indica que estos datos se recogen para mejorar la navegación segura y con fines de análisis de marketing. También señala que cualquier uso secundario de los mensajes de IA recopilados se realizará sobre datos desidentificados y anonimizados:

Como parte de los Datos de Navegación, recopilaremos los mensajes y resultados solicitados [sic] por el Usuario Final o generados por el proveedor de IA, según corresponda. Es decir, solo nos interesa el mensaje de IA y los resultados de su interacción con el chatbot.

Debido a la naturaleza de los datos contenidos en los mensajes de IA, es posible que se procese información personal sensible. Sin embargo, el objetivo de este tratamiento no es recopilar datos personales o identificables. No podemos garantizar completamente la eliminación de toda información sensible o personal, pero implementamos medidas para filtrar o eliminar identificadores y desidentificar y agregar los datos recopilados.

Entre los terceros con los que comparte los "Datos de Navegación Web" se encuentra una empresa afiliada de inteligencia publicitaria y monitoreo de marcas llamada BIScience. Según el fabricante del software VPN, esta compañía utiliza los datos en bruto (sin anonimizar) para generar análisis que se *"usan comercialmente y se comparten con socios comerciales"*.

Es relevante señalar que BIScience, que además es propietaria de Urban Cyber Security Inc.,

fue señalada por un investigador anónimo a principios de enero por recopilar el historial de navegación de los usuarios, también conocido como datos de clickstream, bajo declaraciones engañosas en su política de privacidad.

Presuntamente, la empresa ofrece un kit de desarrollo de software (SDK) a desarrolladores externos de extensiones asociadas, permitiéndoles recolectar datos de clickstream que luego se transmiten a dominios como sclpfybn[.]com y otros puntos finales bajo su control.

"BIScience y sus socios aprovechan vacíos en las políticas de la Chrome Web Store, principalmente las excepciones incluidas en la política de Uso Limitado, que corresponden a los 'casos de uso aprobados'", explicó el investigador, agregando que *"desarrollan funciones visibles para el usuario que supuestamente requieren acceso al historial de navegación, con el fin de acogerse a la excepción de 'necesario para proporcionar o mejorar su único propósito'"*.

En la página de la extensión, Urban VPN también destaca una función de *"protección de IA"*, la cual afirma analizar los mensajes en busca de datos personales, revisar las respuestas de los chatbots para detectar enlaces sospechosos o inseguros y mostrar advertencias antes de que los usuarios envíen sus mensajes o hagan clic en ellos.

Aunque esta supervisión se presenta como una medida para evitar que los usuarios compartan accidentalmente información personal, los desarrolladores no aclaran que la recopilación de datos ocurre incluso si esta función está desactivada.

"La función de protección muestra advertencias ocasionales sobre compartir datos sensibles con empresas de IA", afirmó Dardikman. *"La función de recopilación envía exactamente esa información sensible —y todo lo demás— a los servidores de Urban VPN, donde se vende a anunciantes. La extensión te advierte sobre compartir tu correo electrónico con ChatGPT mientras, al mismo tiempo, envía toda tu conversación a un intermediario de datos"*.

Koi Security indicó que detectó la misma funcionalidad de recolección de datos de IA en otras tres extensiones diferentes del mismo editor, tanto en Chrome como en Microsoft Edge, elevando la base total de instalaciones a más de ocho millones:

- 1ClickVPN Proxy
- Urban Browser Guard
- Urban Ad Blocker

Todas estas extensiones, salvo Urban Ad Blocker para Edge, cuentan con la insignia "Featured", lo que da a los usuarios la impresión de que cumplen con las *"mejores prácticas y un alto estándar de experiencia de usuario y diseño"* de la plataforma.

"Estas insignias transmiten a los usuarios que las extensiones han sido revisadas y cumplen

con los estándares de calidad de la plataforma”, señaló Dardikman. *“Para muchos usuarios, la etiqueta Featured es decisiva entre instalar una extensión o ignorarla: es una aprobación implícita por parte de Google y Microsoft”*.

Los hallazgos vuelven a demostrar cómo la confianza asociada a los mercados de extensiones puede ser explotada para recopilar datos sensibles a gran escala, especialmente en un momento en el que los usuarios comparten información profundamente personal, buscan consejos y expresan emociones a través de chatbots de IA.