Desde febrero de 2024, se ha vinculado a un actor de amenazas desconocido con la creación de múltiples extensiones maliciosas para el navegador Chrome. Estas extensiones aparentan ser herramientas útiles e inofensivas, pero en realidad contienen funciones ocultas diseñadas para robar información, recibir órdenes remotas y ejecutar código arbitrario.

> *«El actor crea sitios web que simulan ser servicios legítimos, herramientas de productividad, asistentes de creación o análisis de anuncios y medios, servicios de VPN, criptomonedas, banca y más, con el fin de dirigir a los usuarios a instalar extensiones maliciosas correspondientes en la Chrome Web Store (CWS) de Google»*, indicó el equipo de inteligencia de DomainTools (DTI) en un informe.

Aunque estas extensiones aparentan funcionar como se anuncia, también permiten el robo de credenciales y cookies, el secuestro de sesiones, la inyección de anuncios, redireccionamientos no autorizados, manipulación del tráfico y ataques de phishing mediante alteraciones del DOM.

Un aspecto técnico preocupante es que estas extensiones solicitan permisos excesivos a través del archivo `manifest.json`, lo que les otorga capacidad para interactuar con todos los sitios web visitados, ejecutar código desde dominios bajo control del atacante, redirigir al usuario de forma maliciosa e incluso insertar publicidad no deseada.

Además, se ha observado que algunas extensiones utilizan el evento `onreset` en un elemento DOM temporal para ejecutar código, posiblemente como técnica para evadir políticas de seguridad de contenido (CSP).

Algunos de los sitios utilizados como señuelos imitan plataformas legítimas como DeepSeek, Manus, DeBank, FortiVPN y Site Stats, con el objetivo de convencer a los usuarios de instalar las extensiones. Una vez instaladas, estas recolectan cookies del navegador, descargan scripts desde servidores remotos y establecen conexiones WebSocket que funcionan como proxies para redirigir el tráfico.

Actualmente no se tiene certeza sobre los métodos usados para atraer a las víctimas a estos sitios falsos, aunque DomainTools señaló que es probable que se empleen estrategias comunes como campañas de phishing o promoción en redes sociales.

> *«Como aparecen tanto en la Chrome Web Store como en sitios web asociados, pueden mostrarse como resultados en búsquedas comunes o dentro de la tienda de Chrome. Muchos de los sitios señuelo usan identificadores de seguimiento de Facebook, lo que sugiere fuertemente que están aprovechando plataformas de Meta, como Facebook, para atraer visitantes. Posiblemente a través de páginas, grupos o anuncios»*, explicó la empresa.

Hasta el momento, no se ha identificado al grupo responsable de esta campaña, aunque se han detectado más de 100 sitios falsos y extensiones maliciosas asociadas. Google ya ha eliminado algunas de estas extensiones de su tienda.

Para reducir los riesgos, se recomienda a los usuarios instalar extensiones solo de desarrolladores verificados, revisar cuidadosamente los permisos solicitados, analizar las reseñas y evitar extensiones que imiten servicios conocidos.

Sin embargo, también es importante considerar que las calificaciones pueden estar manipuladas. DomainTools descubrió que ciertas extensiones que suplantaban a DeepSeek redirigían a los usuarios que daban puntuaciones bajas (entre 1 y 3 estrellas) a un formulario privado en el dominio `ai-chat-bot[.]pro`, mientras que los que otorgaban puntuaciones altas (4 o 5 estrellas) eran enviados a la página oficial de reseñas en la Chrome Web Store.