Espionaje masivo de usuarios del navegador Chrome de Google destapa nueva vulnerabilidad

Por: Reuters
18/06/2020

Un campaña de software espía descubierta recientemente atacó a los usuarios de Chrome a través de 32 millones de descargas de extensiones del navegador de Google, líder del mercado, según dijeron a Reuters investigadores de Awake Security.

Lo ocurrido pone de relieve el fracaso de la industria tecnológica en proteger la seguridad de unos navegadores que cada vez se utilizan más para consultar el correo electrónico, nóminas de trabajo y otra información de carácter sensible.

Google, que pertenece al grupo Alphabet Inc , dijo que eliminó más de 70 de los complementos maliciosos de su tienda web oficial de Chrome después de ser alertado por los investigadores el mes pasado.

“Cuando se nos alerta de extensiones en la tienda web que violan nuestras políticas, tomamos medidas y utilizamos esos incidentes como material de formación para mejorar nuestros análisis automatizados y nuestros manuales”, dijo a Reuters el portavoz de Google, Scott Westover.

La mayoría de las extensiones gratuitas pretendían advertir a los usuarios sobre sitios web cuestionables o convertir archivos de un formato a otro. Pero en su lugar, desviaban el historial de navegación y los datos que proporcionaban credenciales para el acceso a herramientas empresariales de uso interno.

Si se tiene en cuenta el número de descargas, fue la campaña maliciosa de mayor alcance que haya tenido la tienda de Chrome hasta la fecha, según el cofundador y jefe investigador de Awake, Gary Golomb.

Google se negó a discutir las comparaciones de este último “spyware” con campañas anteriores, la amplitud del daño o por qué no detectó y eliminó las extensiones maliciosas por su cuenta a pesar de las promesas pasadas de supervisar los complementos más de cerca.

No está claro quién está detrás de la campaña de distribución de este software malicioso. Awake dijo que los desarrolladores proporcionaron información de contacto falsa cuando enviaron las extensiones a Google.

“Cualquier cosa que te lleve al navegador o al correo electrónico de alguien o a otras áreas sensibles sería un objetivo para el espionaje nacional así como para el crimen organizado”, dijo el exingeniero de la Agencia de Seguridad Nacional de Estados Unidos, Ben Johnson, que fundó las empresas de seguridad Carbon Black y Obsidian Security.

Las extensiones fueron diseñadas para evitar la detección por parte de las compañías de antivirus o software de seguridad que evalúa la reputación de los dominios web, dijo Golomb.