Más de 1.31 millones de usuarios intentaron instalar extensiones de navegador web maliciosas o no deseadas al menos una vez, según los nuevos hallazgos de la compañía de seguridad cibernética Kaspersky.

> *«Desde enero de 2020 hasta junio de 2022, más de 4.3 millones de usuarios únicos fueron atacados por adware escondido en las extensiones del navegador, lo que representa aproximadamente el 70% de todos los usuarios afectados por complementos maliciosos y no deseados»,* dijo la compañía.

Hasta 1,311,557 usuarios entran en esta categoría en la primera mitad de 2022, según los datos de telemetría de Kaspersky. En comparación, el número de dichos usuarios alcanzó su punto máximo en 2020 con casi 3,660,236, seguido de 1,823,263 usuarios únicos en 2021.

La amenaza más frecuente es una familia de adware llamada WebSearch, que se hace pasar por visores de PDF y otras utilidades, y cuenta con capacidades para recopilar y analizar consultas de búsqueda y redirigir a los usuarios a enlaces de afiliados.

WebSearh también se destaca por modificar la página de inicio del navegador web, que contiene un motor de búsqueda y una serie de enlaces a fuentes de terceros como AliExpress que, al hacer clic en ellos, ayudan a los desarrolladores de extensiones a ganar dinero por medio de enlaces de afiliados.

> *«Además, la extensión modifica el motor de búsqueda predeterminado del navegador a search.myway[.]com, que puede capturar las consultas de los usuarios, recopilarlas y analizarlas. Dependiendo de lo que el usuario haya buscado, los sitios asociados más relevantes se promocionarán activamente en los resultados de búsqueda»,* dijo Kaspersky.

Un segundo conjunto de extensiones involucra una amenaza llamada AddScript, que oculta

su funcionalidad maliciosa bajo la apariencia de descargadores de videos. Aunque los complementos ofrecen las soluciones anunciadas, también están diseñados para comunicarse con un servidor remoto para recuperar y ejecutar un código JavaScript arbitrario.

Más de un millón de usuarios encontraron adware solo en el primer semestre de 2022, con WebSearch y AdScript dirigidos a 876,924 y 156,698 usuarios únicos.

También se encontraron instancias de malware para robar información como FB Stealer, cuyo objetivo es robar las credenciales de inicio de sesión de Facebook y las cookies de sesión de los usuarios que han iniciado sesión. FB Stealer ha sido responsable de 3077 intentos únicos de infección en el primer semestre de 2022.

El malware identifica principalmente a los usuarios que buscan software hackeado en los motores de búsqueda, con FB Stealer entregado a través de un troyano llamado NullMixer, que se propaga por medio de instaladores pirateados para software como SolarWinds Broadband Engineers Edition.

> *«FB Stealer es instalado por el malware y no por el usuario. Una vez agregado al navegador, imita la extensión de Chrome inofensiva y de aspecto estándar de Google Translate»,* dijeron los investigadores.

Estos ataques también tienen una motivación financiera. Los operadores del malware, después de tomar las cookies de autenticación, inician sesión en la cuenta de Facebook del objetivo y la secuestran cambiando la contraseña, bloqueando efectivamente a la víctima. Los atacantes pueden entonces abusar del acceso para pedir dinero a los amigos de la víctima.

Los hallazgos llegan poco más de un mes después de que Zimperium revelara una familia de malware llamada ABCsoup, que se hace pasar por una extensión de Google Translate como parte de una campaña de adware dirigida a los usuarios rusos de los navegadores Google

Chrome, Opera y Mozilla Firefox.

Para mantener el navegador web libre de infecciones, se recomienda que los usuarios utilicen fuentes confiables para descargar software, revisar los permisos de las extensiones y revisar y desinstalar periódicamente los complementos que *«ya no usa o que no reconoce».*