Una extensión de navegador maliciosa con 350 variantes se hace pasar por un complemento de Google Translate como parte de una campaña de adware dirigida a los usuarios rusos de los navegadores web Google Chrome, Opera y Mozilla Firefox.

La compañía de seguridad móvil Zimperium, denominó a la familia de malware como ABCsoup, afirmando que *«las extensiones se instalan en la máquina de la víctima por medio de un ejecutable basado en Windows, sin pasar por la mayoría de las soluciones de seguridad de punto final, junto con los controles de seguridad que se encuentran en las tiendas de extensiones oficiales».*

Los complementos falsos del navegador vienen con la misma ID de extensión que la de Google Translate en un intento por engañar a los usuarios haciéndoles creer que han instalado una extensión legítima.

Las extensiones no están disponibles en las propias tiendas web oficiales del navegador. Se entregan a través de distintos ejecutables de Windows que instalan el complemento en el navegador web de la víctima.

En caso de que el usuario objetivo ya tenga instalada la extensión Google Translate, reemplaza la versión original con la variante maliciosa debido a sus números de versión más altos (30.2.5 frente a 2.0.10).

> *«Además, cuando se instala esta extensión, Chrome Web Store asume que es Google Translate y no la extensión maliciosa, ya que Web Store solo verifica las ID de extensión»,* dijo Nipun Gupta, investigador de Zimperium.

Todas las variantes observadas de la extensión están orientadas a servir ventanas emergentes, recolectar información personal para entregar anuncios específicos de objetivos,

búsquedas de huellas dactilares e inyectar JavaScript malicioso que puede actuar como spyware para capturar pulsaciones de teclas y monitorear la actividad del navegador web.

La función principal de ABCsoup implica verificar los servicios de redes sociales rusas como Odnoklassniki y VK entre los sitios web actuales abiertos en el navegador, y de ser así, recopilar los nombres y apellidos de los usuarios, las fechas de nacimiento y el sexo, y transmitir los datos a un servidor remoto.

El malware no solo usa esta información para publicar anuncios personalizados, la extensión también cuenta con capacidades para inyectar código JavaScript personalizado basado en sitios web abiertos. Esto incluye YouTube, Facebook, ASKfm, Mail.ru, Yandex, Rambler, Avito, Brainly´s Znanija, Kismia y rollApp, lo que sugiere un fuerte enfoque en Rusia.

Zimperium atribuyó la campaña a un *«grupo bien organizado»* de origen ruso y de Europa del Este, con las extensiones diseñadas para destacar a los usuarios rusos dada la amplia variedad de dominios locales presentados.

> *«Este malware está diseñado a propósito para apuntar a todo tipo de usuarios y cumple su propósito de recuperar información del usuario. Los scripts inyectados se pueden utilizar fácilmente para presentar un comportamiento más malicioso en la sesión del navegador, como el mapeo de pulsaciones de teclas y la filtración de datos»,* dijo Gupta.