

Publicidad invasiva: Qué es y cómo evitarla

Posiblemente muchas veces al navegar por Internet aparecen ventanas emergentes con mensajes como: “ganaste un nuevo celular gratis haz clic AQUÍ”, “eres nuestro usuario 500.000 y has ganado un premio haz clic AQUÍ”, u otro tipo de mensajes similares que hacen referencia a cosas demasiado buenas para ser verdad. A través de este tipo de anuncios es cómo más comúnmente se presenta el adware a los usuarios, ya sea a través de la computadora o el smartphone. [ESET](#), compañía líder en detección proactiva de amenazas, advierte que si el usuario hace clic donde no debe y se infecta, probablemente comiencen a aparecer nuevas ventanas emergentes desplegando más publicidad invasiva y no deseada.

Adware es la combinación de las palabras “advertising” (publicidad) y “software” (programa) y se refiere a cualquier software, sea malicioso o no, que muestre anuncios en una app o sobre el navegador web para generar ganancias a partir de clics e impresiones en los anuncios. Se identifica un adware instalado en un dispositivo cuando se empiezan a observar ventanas emergentes con anuncios falsos sin ningún motivo aparente, o cuando aparecen varios anuncios de forma consecutiva causando una molestia a la hora de navegar, o siendo redirigidos a sitios no deseados que pueden llevar a la descarga de malware. Toda su actividad maliciosa es invasiva y notoria mientras el usuario navega por Internet.

“Si bien se suele hacer referencia al adware como un tipo de malware, la realidad es que el adware es considerado una aplicación potencialmente no deseada (PUA, por sus siglas en inglés). Esto quiere decir que, si bien puede conducir a sitios maliciosos, el riesgo de que realice otra acción maliciosa es menor, aunque puede ocurrir”, comenta **Camilo Gutiérrez Amaya**, Jefe del Laboratorio de Investigación de ESET Latinoamérica. Puede tener entre sus objetivos el recolectar datos, como fue el caso del [adware Wajam](#), que es capaz de recopilar y filtrar información del usuario víctima, como software instalado, el modelo del equipo, entre otros datos.

En cuanto a la instalación de estos, existen diversas maneras de ingresar este tipo de software no deseado en los dispositivos. Por ejemplo, puede colarse en la computadora al instalar un software gratuito (Freewares o Sharewares) y realizar modificaciones sobre el navegador. Muchas veces es el propio usuario el que acepta la instalación del adware por no prestar atención durante el proceso de instalación. Esto significa que el adware accede al sistema de manera “legal” porque el usuario aceptó la instalación. Lo que recomienda ESET es eliminar el archivo que es detectado por la solución de seguridad como adware, ya que existen posibilidades de que contenga código malicioso.

El adware puede propagarse e infectar un dispositivo de varias maneras, por ejemplo, instalando en el navegador extensiones no confiables o desconocidas, instalando software gratuito (Freewares o Sharewares) de sitios con una reputación dudosa, navegando en sitios “no confiables” o que estén infectados con adware, algunos de estos pueden mostrar contenido multimedia como películas online gratis, partidos de fútbol online gratis, contenido para adultos, minijuegos online, etc. También, puede ser a través de archivos ejecutables que se hacen pasar por un software en particular pero que terminan instalando otros, o haciendo clic en anuncios sospechosos.

A continuación, ESET comparte una serie de posibles comportamientos que pueden dar indicios de

una posible infección de adware:

- El navegador empieza a funcionar más lento que de costumbre o puede cerrarse de forma inesperada.
- Aparecen anuncios en páginas web donde antes no aparecían.
- Se modificó la página de inicio o la página de búsqueda sin la autorización del usuario.
- Cada vez que se visita una página web, el navegador es redirigido a una página diferente.
- Aparecen nuevas barras de herramientas (toolbars), plugins o extensiones en el navegador que antes no estaban.
- Al hacer clic en cualquier parte de una página web se abren una o más ventanas emergentes con anuncios no deseados.
- Se instalan aplicaciones no deseadas en la computadora sin permiso.

Los Adwares no solo afectan a las computadoras, también pueden propagarse en dispositivos móviles infectándolos por medio del navegador web, o a través de aplicaciones alojadas en tiendas tanto oficiales como tiendas no oficiales de terceros.

Para poder protegerse de este tipo de amenazas desde ESET recomiendan tener en cuenta los siguientes puntos:

- Mantener actualizado el navegador de web.
- Evitar abrir anuncios con falsas advertencias o aquellos que contengan mensajes muy buenos para ser verdad.
- Utilizar una [extensión confiable que bloquee anuncios](#) mientras se navega por Internet.
- Evitar navegar por sitios web no confiables, en especial aquellos que el navegador los marque como no seguros.
- Evitar descargar programas de fuentes no confiables
- Durante la instalación de un programa, leer con detenimiento los términos y condiciones de uso antes de aceptarlos.
- Contar con una [solución de seguridad](#) para bloquear este tipo de contenidos cuando se navega por Internet.