Publicado en Ciudad de México el 25/05/2018

# [Avast: Distribuyen miles de dispositivos Android con Malware preinstalado](http://www.notasdeprensa.es)

## El Laboratorio de Amenazas de Avast analiza el adware para dispositivos móviles que ha encontrado preinstalado en miles de teléfonos Android en todo el mundo

 El Laboratorio de Amenazas de Avast ha encontrado un adware preinstalado en cientos de diferentes modelos y versiones de dispositivos Android de fabricantes como ZTE, Archos y myPhone. La mayoría de estos dispositivos no están certificados por Google. El adware se llama `Cosiloon´ y crea una capa superficial para mostrar publicidad sobre las páginas web en el navegador. Miles de usuarios se han visto afectados y sólo el mes pasado el Laboratorio de Amenazas de Avast ha detectado la última versión de este adware en cerca de 18.000 dispositivos que pertenecían a clientes de Avast ubicados en más de 100 países, incluidos Rusia, Italia, Alemania, Reino Unido, así como algunos usuarios en España, Argentina, México, Brasil y Estados Unidos. Una antigua versión del adware fue analizada en su día por Dr.Web y ha estado activo durante al menos tres años: su erradicación es compleja, dado que se encuentra instalado en el nivel del soporte lógico inalterable (firmware) y está eficazmente oculto. El Laboratorio de Amenazas de Avast está en contacto con Google, que está al tanto del problema y ha tomado medidas para mitigar el potencial malicioso de las múltiples versiones de esta aplicación en varios modelos de dispositivos, empleando técnicas desarrolladas internamente. Google Play Protect ha sido actualizado para garantizar que exista una cobertura para estas aplicaciones maliciosas en el futuro. Sin embargo, como las aplicaciones vienen preinstaladas en firmware, el problema es difícil de solucionar. Por ello, Google ha contactado a desarrolladores de firmware para transmitirles esta preocupación y alentarlos a tomar medidas para afrontar el problema. Identificando a CosiloonLos últimos años, el Laboratorio de Amenazas de Avast ha observado como aparecían en su base de datos, cada cierto tiempo, extrañas muestras adware en dispositivos Android. Las muestras aparentan ser similares a la de cualquier otro adware, con la excepción de que este adware pareciera no tener un punto de infección, como si no existiera un vector de entrada. Utilizan muchos nombres de paquete diferentes, estos son algunos de los más comunes: com.google.eMediaService, com.google.eMusic1Service, com.google.ePlay3Service y com.google.eVideo2Service. Los dispositivos vienen con una aplicación maliciosa preinstalada, un downloader. Este downloader se conecta a un servidor controlado por los atacantes para recibir instrucciones e instalar el payload, el adware que mostrará publicidad a los usuarios de dispositivos afectados. Algunas aplicaciones antivirus son capaces de detectar el adware, pero el downloader los vuelve a instalar de inmediato, y este downloader no puede ser neutralizado por los antivirus. Avast ha intentado deshabilitar el servidor de comando y control (C and C server) de Cosiloon enviando peticiones a las entidades de registro de dominios y a los proveedores del servidor. El primer proveedor, Zenlayer, respondió rápidamente y desconectó el servidor, pero fue reactivado tiempo después usando un proveedor diferente. Las entidades registradoras de dominio no han respondido aún a la solicitud de Avast, por lo cual el servidor C and C todavía está en funcionamiento. "Las apps maliciosas pueden, desafortunadamente, ser instaladas en el nivel del firmware antes de que los dispositivos sean distribuidos a los usuarios y probablemente sin el conocimiento del fabricante", señala Nikolaos Chrysaidos, líder de Inteligencia y Seguridad ante Amenazas Móviles de Avast. "Si una aplicación es instalada en el nivel del firmware es muy difícil de remover, por lo cual una colaboración entre los diferentes actores de la industria, vendedores de programas de seguridad, Google y fabricantes de equipos originales (OEMs) es imperativa. Juntos, podemos asegurar un ecosistema de dispositivos móviles más seguro para los usuarios de Android". Avast Mobile Security puede detectar y desinstalar los payloads, pero no cuenta con los permisos requeridos para deshabilitar el downloader, por lo cual a Google Play Protect le toca el trabajo más pesado. Si un dispositivo está infectado debe automáticamente desactivarse el downloader y el payload. Avast sabe que este procedimiento es efectivo porque el Laboratorio de Amenazas de Avast ha observado una caída en la cantidad de dispositivos infectados por nuevas versiones de payload después de que Play Protect empezó a detectar Cosiloon. ¿Cómo desactivar Cosiloon?Los usuarios pueden encontrar el downloader en las preferencias (bajo el nombre (`CrashService´, `ImeMess´ o `Terminal´, con el icono genérico de Android), y puede hacer clic en el botón `desactivar´ de la página de la aplicación, si está disponible (según la versión Android). Esto desactivará el downloader y una vez que Avast elimine el payload, este no volverá a aparecer. Avast Mobile Security puede ser descargado gratuitamente de la tienda Google Play. Avast también está trabajando con proveedores de soporte de todo el mundo, incluidos los cuatro mayores de Estados Unidos, para proteger a los usuarios de las amenazas móviles. Acerca de AvastAvast (www.avast.com) es el líder global en productos de seguridad digital para consumidores y empresas, protege a más de 400 millones de personas en línea. Avast ofrece productos con las marcas Avast y AVG que protegen a los usuarios de amenazas en internet y el escenario de amenazas de Internet de las Cosas que está en constante evolución. La red de detección de amenazas de la empresa está entre las más avanzadas del mundo, y utiliza tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital Avast para dispositivos móviles, PC o Mac están clasificados como los mejores y certificados por VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros. Avast cuenta con el respaldo de CVC Capital Partners y Summit Partners, que son sociedades de inversión de capital privado líderes en el mundo.

**Datos de contacto:**

Flor Carreno

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-distribuyen-miles-de-dispositivos](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad Dispositivos móviles Ciudad de México



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)