Publicado en Redwood City, California, a de 23 de 2019. el 24/04/2019

# [Avast encuentra adware en apps de estilo de vida en Google Play Store](http://www.notasdeprensa.es)

## Con más de 30 millones de instalaciones, se trata de un Adware invasivo en apps de música, fitness y edición de fotos que muestra anuncios a pantalla completa descubiertos por apklab.io de Avast

 2019 Avast (LSE: AVST), el líder mundial en productos de seguridad digital, anunció que decubrió 50 apps de adware en Google Play Store utilizando la plataforma móvil de inteligencia de amenazas de Avast, apklab.io. Las descargas de las apps, a las que Avast se refiere como TsSdk, van desde instalaciones de 5K a 5M. El adware se muestra de forma persistente en los anuncios a pantalla completa y, en algunos casos, intenta convencer al usuario de que instale más aplicaciones. Las aplicaciones con adware están vinculadas entre sí mediante el uso de bibliotecas de terceros de Android que evitan las restricciones de servicio en segundo plano presentes en las versiones más recientes de Android. Aunque la omisión en sí no está explícitamente prohibida en Play Store, Avast lo detecta con Android:Agent-SEB [PUP], porque las aplicaciones que usan estas bibliotecas gastan la batería del usuario y hacen que el dispositivo sea más lento. Las aplicaciones utilizan las bibliotecas para mostrar cada vez más y más anuncios al usuario, yendo en contra de las reglas de Play Store. Avast se ha contactado con Google para que elimine estas aplicaciones. Avast llamó al adware TsSdk, porque el término se encontró en la primera versión del adware. El originalUsando apklab.io, Avast encontró dos versiones de TsSdk en Play Store, unidas por el mismo código. La más antigua de las dos versiones ha sido instalada 3.6 millones de veces y estaba contenida en apps simples de juegos, fitness y edición de fotos; En su mayoría se ha instalado en India, Indonesia, Filipinas, Pakistán, Bangladesh y Nepal. Una vez instaladas, la mayoría de las aplicaciones que contienen la versión anterior parecen funcionar como se anuncia en sus páginas de Google Play, sin embargo, los accesos directos se colocan en la pantalla de inicio y los anuncios de pantalla completa se muestran al usuario al encender pantalla, y en algunos casos, los anuncios se muestran periódicamente cuando el usuario utiliza el dispositivo. Además, algunas aplicaciones contienen un código capaz de descargar aplicaciones adicionales, lo que solicita a los usuarios que las instalen. La mayoría de las muestras anteriores también agregaron un acceso directo a un and #39;Game Center and #39; en la pantalla de inicio del dispositivo infectado, que abre una página que anuncia diferentes juegos. http://h5games.top/. El nombre and #39;H5GameCenter and #39; también formó parte del malware preinstalado por Cosiloon que Avast informó el año pasado. Los investigadores de Avast no están seguros de si los dos están relacionados entre sí. Actualizando el código de adwareLa versión más reciente se ha instalado aproximadamente 28 millones de veces, desde el catálogo de aplicaciones de música y fitness. Las descargas se concentran en Filipinas, India, Indonesia, Malasia, Brasil y el Reino Unido. El código de la nueva versión está mejor protegido; ya que se cifra mediante el empaquetador Tencent, que es bastante difícil de desempaquetar por los analistas, pero se captura fácilmente durante el análisis dinámico en apklab.io Esta versión lleva a cabo varias comprobaciones antes de implementar anuncios a pantalla completa. En primer lugar, el adware solo se activa si el usuario instala la aplicación haciendo clic en un anuncio de Facebook. La aplicación puede detectar esto usando una función de SDK de Facebook llamado and #39;deferred deep linking and #39;. El adware solo muestra anuncios dentro de las primeras cuatro horas de instalación de la aplicación y luego con mucha menos frecuencia. A partir del código, se sabe que dentro de las primeras cuatro horas, los anuncios a pantalla completa se muestran al azar cuando se desbloquea el teléfono o cada 15 minutos y cada 30 minutos después de una hora. La nueva versión del adware no parece funcionar en la versión de Android 8.0 y superior debido a los cambios en la administración del servicio en segundo plano en estas nuevas versiones de Android. Debido a la cantidad de muestras, Avast solo seleccionó la última APK de cada aplicación y las puso en este documento. Capturas de pantalla de Google Play Store y las páginas de Facebook están disponibles aquí. Muchas de las versiones anteriores del adware ya existían en Play Store, con Google eliminando las aplicaciones, incluida una llamada Pro Piczoo, que se instaló más de un millón de veces. Consejos para evitar el AdwareTener cuidado al descargar aplicaciones. Lea las revisiones de las aplicaciones antes de instalar una nueva, leyendo atentamente las críticas tanto positivas como negativas. Observar si los revisores comentan si la aplicación hace o no lo que dice que hará. Si la revisión de una aplicación incluye comentarios como and #39;esta aplicación no hace lo que promete and #39; o and #39;esta aplicación está llena de adware and #39;, uno debería reconsiderar la descarga de la aplicación. Revisiones como esta son una señal de que algo no está bien. Siempre revisar cuidadosamente los permisos de las aplicaciones, mirando de cerca para ver si tienen sentido. La concesión de permisos incorrectos puede enviar datos confidenciales a los hackers, incluida información como los contactos almacenados en el dispositivo, los archivos multimedia y las perspectivas de los chats personales. Si algo parece fuera de lo común o más allá de lo que parece apropiado, la aplicación no debe descargarse. Instalar una aplicación antivirus confiable. Antivirus actúa como una red de seguridad y puede identificar aplicaciones que están infectadas con programas publicitarios, protegiendo a los usuarios de estas aplicaciones no deseadas. Sobre AvastAvast (LSE: AVST) es el líder mundial en productos de seguridad digital. Con más de 400 millones de usuarios en línea, Avast ofrece productos bajo las marcas Avast y AVG que protegen a las personas de las amenazas en Internet y la evolución del panorama de amenazas de IoT. La red de detección de amenazas de la compañía se encuentra entre las más avanzadas del mundo, y utiliza el aprendizaje automático y las tecnologías de inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital de Avast para dispositivos móviles, PC o Mac son los mejores clasificados y certificados por VB100, AV-Comparatives, AV-Test, OPSWAT, West CoastLabs y otros. Visita: www.avast.com

**Datos de contacto:**

Marketing Q S

Agencia de Relaciones Públicas

+ 52 55 5615

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-encuentra-adware-en-apps-de-estilo-de\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Nacional Hardware E-Commerce Software Dispositivos móviles Fitness



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