Más de 50 aplicaciones de Android en Google Play Store, de las cuales la mayoría fueron diseñadas para niños y han acumulado alrededor de 1 millón de descargas, fueron descubiertas utilizando un nuevo truco para hacer clic de forma secreta en anuncios sin el conocimiento de los usuarios de teléfonos inteligentes.

Apodado como «Tekya», el malware en las aplicaciones imitaba las acciones de los usuarios para hacer clic en anuncios de redes publicitarias como AdMob de Google, AppLovin, Facebook y Unity, según informó la compañía de seguridad cibernética Check Point Research en un informe.

> *«Veinticuatro de las aplicaciones infectadas estaban dirigidas a niños, y el resto son aplicaciones de utilidad (como aplicaciones de cocina, calculadoras, descargadores, traductores, etc.)»*, dijeron los investigadores.

Aunque las aplicaciones ya se eliminaron de Google Play, el hallazgo de Check Point Research es el último de una avalancha de esquemas de fraude publicitario que ha plagado la tienda de aplicaciones en los últimos años, con malware que se hace pasar por aplicaciones optimizadoras y de utilidad para realizar clics falsos en anuncios.

Según el informe, la campaña clonó aplicaciones populares legítimas para ganar audiencia, las 56 aplicaciones recientemente descubiertas se encontraron eludiendo las protecciones de Google Play Store al ofuscar su código nativo y confiando en la API MotionEvent de Android para simular los clics de los usuarios.

Una vez que un usuario involuntario instala una de las aplicaciones maliciosas, el malware Tekya registra un receptor, un componente de Android que se invoca cuando ocurre un determinado evento del sistema o aplicación, como un reinicio del dispositivo o cuando el usuario está utilizando el teléfono activamente.

El receptor, cuando detecta tales eventos, procede a cargar una biblioteca nativa llamada *«libtekya.so»* que incluye una subfunción llamada *«sub_AB2C»*, que crea y distribuye eventos táctiles, imitando así un clic por medio de la API MotionEvent.

El fraude publicitario móvil se manifiesta de distintas formas, incluidos los actores de amenazas que colocan anuncios con malware en teléfonos de usuarios o incrustan malware en aplicaciones y servicios en línea para generar clics fraudulentos y recibir pagos de redes publicitarias.

El análisis del proveedor de seguridad móvil Upstream con datos de 2019, reveló que las aplicaciones favoritas para ocultar el malware de fraude publicitario son aquellas que pretenden mejorar la productividad o mejorar la funcionalidad del dispositivo.

Casi el 23 por ciento de los anuncios maliciosos de Android que Upstream encontró el año pasado cayeron en esta categoría. Otras aplicaciones que los atacantes usaban con frecuencia para ocultar malware incluían aplicaciones de juegos, entretenimiento y aplicaciones de compras.

Por su parte, Google ha tratado de evitar que las aplicaciones de Android no autorizadas se infiltraran en Google Play Store. Google Play Protect aprovechó para detectar aplicaciones potencialmente dañinas y también forjó una «App Defense Alliance» en asociación con las empresas de seguridad cibernética ESET, Lookout y Zimperium para reducir el riesgo de malware basado en aplicaciones.