Google ha informado sobre una actualización de su Play Protect que incluye un escaneo en tiempo real a nivel de código para abordar aplicaciones maliciosas novedosas antes de su descarga e instalación en dispositivos Android.

> El gigante tecnológico mencionó: *«Google Play Protect ahora sugerirá un análisis en tiempo real de la aplicación al instalar aplicaciones que nunca antes hayan sido sometidas a escaneo, con el propósito de detectar posibles amenazas emergentes».*

Google Play Protect es un servicio gratuito integrado de detección de amenazas que examina dispositivos Android en busca de aplicaciones potencialmente dañinas descargadas desde la tienda Play Store y otras fuentes externas. En situaciones extremas, es posible que una aplicación sea bloqueada antes de su instalación.

Esta nueva medida de seguridad se suma a las protecciones existentes, que alertaban a los usuarios cuando se identificaba una aplicación como maliciosa gracias a la información de escaneo existente o cuando se detectaban indicios de sospecha mediante heurísticas recopiladas mediante el aprendizaje automático en el dispositivo.

Con las últimas salvaguardias, se extraen datos importantes de la aplicación y se envían a la infraestructura de Play Protect para una evaluación en tiempo real a nivel de código, con el fin de determinar si es seguro instalarla o si posee características maliciosas.

Google indicó: *«Esta mejora ayudará a proteger de manera más efectiva a los usuarios contra aplicaciones polimórficas maliciosas que emplean diversas técnicas, como la inteligencia artificial, para modificar su apariencia y evitar su detección».* Agregó que esta función se está implementando inicialmente en determinados países, comenzando por India.

Esta mejora en la seguridad se presenta en un momento en que los actores de amenazas continúan encontrando distintos métodos para propagar malware en Android, a menudo a través de enlaces a aplicaciones engañosas o archivos APK enviados mediante aplicaciones de mensajería.

Asimismo, se suma a una revisión del Android Security Paper, que «*brinda una descripción completa de las medidas de seguridad proactivas integradas en la plataforma, abarcando aspectos como el hardware, la protección contra explotaciones, los servicios de seguridad de Google y la variedad de API de gestión disponibles tanto para empresas como para gobiernos*».