Se descubrió que los certificados de plataforma utilizados por los proveedores de teléfonos inteligentes Android como Samsung, LG y MediaTek, se abusan para firmar aplicaciones maliciosas.

Los hallazgos fueron descubiertos e informados por primera vez por el ingeniero inverso de Google, Lukasz Siewierki el jueves pasado.

> *«Un certificado de plataforma es el certificado de firma de la aplicación que se utiliza para firmar la aplicación 'android' en la imagen del sistema»*, dice el informe presentado a través de la Iniciativa de Vulnerabilidad de Socios de Android (AVPI).

> *«La aplicación 'android' se ejecuta con una identificación de usuario altamente privilegiada, android.uid.system, y tiene permisos del sistema, incluidos los permisos para acceder a los datos del usuario».*

Esto significa que una aplicación no autorizada firmada con el mismo certificado puede obtener el nive más alto de privilegios que el sistema operativo Android, lo que le permite recopilar todo tipo de información confidencial de un dispositivo comprometido.

La lista de paquetes de aplicaciones de Android maliciosos que han abusado de los certificados se encuentra a continuación:

- com.ruso.signato.renewis
- com.sledsdffsjkh.Search
- com.android.poder
- com.management.propaganda
- com.sec.android.musicplayer
- com.houla.quicken
- com.attd.da

- com.arlo.fappx
- com.metasploit.stage
- com.vantage.ectronic.cornmuni

No está claro aún cómo y dónde se encontraron los artefactos, y si se usaron como parte de alguna campaña activa de malware.

Una búsqueda en VirusTotal informa que las muestras identificadas han sido marcadas por soluciones antivirus como adware HiddenAds, Metasploit, ladrones de información, descargadores y otro malware ofuscado.

Cuando se contactó para hacer comentarios, Google dijo que informó a todos los proveedores afectados que rotaran los certificados y que no hay evidencia de que estas aplicaciones se hayan entregado a través de Play Store.

> *«Los socios OEM implementaron rápidamente medidas de mitigación tan pronto como informamos el compromiso clave. Los usuarios finales estarán protegidos por las mitigaciones de usuarios implementadas por los socios OEM»,* dijo la compañía.

> *«Google ha implementado detecciones amplias para el malware en Build Test Suite, que escanea imágenes del sistema. Google Play Protect también detecta el malware. No hay indicios de que este malware esté o haya estado en Google Play Store. Como siempre, recomendamos a los usuarios que se aseguren de que estén ejecutando la última versión de Android».*