La empresa Bluebox Security advirtió hoy y puso al descubierto una nueva vulnerabilidad para el sistema móvil Android, la cual permite que un hacker pueda convertir cualquier aplicación en un troyano malicioso.

El director de tecnología de la firma en seguridad móvil, Jeff Forristal, aseguro que lo anterior es totalmente desapercibido tanto por la tienda de aplicaciones, el teléfono, o el usuario final, y que las implicaciones que ello tiene son «enormes».

Agregó que dicha vulnerabilidad, por lo menos desde el lanzamiento de Android 1.6, podría afectar a cualquier teléfono Android lanzado en los últimos cuatro años, lo que equivale a casi 900 millones de dispositivos.

Asimismo, expuso que un hacker puede explotar la vulnerabilidad de cualquier cosa, desde el robo de datos, hasta la creación de una red de bots móviles.

Pero el riesgo para el individuo y la empresa es grande, pues una aplicación maliciosa puede acceder a los datos individuales o entrar al sistema de la compañía, riesgo que se agrava si se tienen en cuenta las aplicaciones desarrolladas por los fabricantes de dispositivos o de terceros que trabajan en cooperación con el fabricante del dispositivo y que se otorgan privilegios elevados especiales dentro de Android, puntualizó.

La debilidad permite que se pueda modificar el código del paquete APK sin romper la firma cifrada de la aplicación, lo que en apariencia parecería una aplicación legítima.

La aplicación entonces no sólo tiene la capacidad de leer los datos de aplicaciones arbitrarias en el dispositivo como correo electrónico, mensajes de texto y documentos, entre otros, recupera todas las cuentas y contraseñas almacenados.

También puede tomar básicamente en el funcionamiento normal del teléfono y controlar cualquier función del mismo, desde hacer llamadas telefónicas enviar mensajes SMS, encender la cámara y grabar las llamadas.

Por ello, Bluebox recomienda a los propietarios de dispositivos ser muy prudentes en la identificación del editor de la aplicación que desea descargar y actualizar constantemente los equipos móviles.

Fuente: eleconomista