La billetera criptográfica multicadena descentralizada, BitKeep, confirmó el miércoles un ataque cibernético que permitió a los hackers distribuir versiones fraudulentas de su aplicación de Android con el objetivo de robar las criptomonedas de los usuarios.

> *«Con un código implantado maliciosamente, el APK alterado condujo a la filtración de las claves privadas del usuario y permitió al hacker mover los fondos»,* dijo Kevin Como, CEO de BitKeep.

Según la empresa de seguridad de cadenas de bloques PeckShield y el explorador de cadenas de bloques múltiples OKLink, hasta ahora se ha robado activos por un valor estimado de 9.9 millones de dólares.

> *«Los fondos robados están en BNB Chain, Ethereum, TRON y Polygon. Se usaron más de 200 direcciones en las otras tres cadenas en el atraco, y al final todos los fondos se transfirieron a 2 direcciones principales»,* dijo BitKeep en una serie de tuits.

Se cree que el incidente tuvo lugar el 26 de diciembre de 2022, cuando el atacante explotó y secuestró la versión 7.2.9 del archivo del paquete de aplicaciones de Android (.APK) alojado en su sitio web para distribuir la variante troyana.

El robo digital no afecta a las aplicaciones de BitKeep descargadas a través de Google Play, Apple App Store o Google Chrome Web Store.

Se han identificado hasta cinco versiones falsificadas distintas de la aplicación de Android con los siguientes nombres de paquetes, lo que sugiere que las aplicaciones se distribuyeron potencialmente a través de sitios web de phishing. El nombre legítimo del paquete es «com.bitkeep.wallet«.

- com.bitkeep.app
- com.bitkeep.w4
- com.bitkeep.w5
- com.bitkeep.wallet5
- io.bitkeep.wallet

La compañía con sede en Singapur, fundada en 2018, dijo que rastreó la dirección de la billetera usada para realizar el robo y que algunos de los activos digitales desviados se congelaron.

Se recomienda a los usuarios que hayan descargado el archivo APK para la versión 7.2.9 que instalen la última versión (7.3.0) lanzada el jueves y transfieran los fondos a una dirección de billetera recién generada.

Esta no es la primera vez que BitKeep sufre un ataque cibernético. El 18 de octubre de 2022, reveló otro incidente de seguridad dirigido a su servicio BitKeep Swap que ocasionó pérdidas de alrededor de un millón de dólares.