Investigadores de seguridad cibernética descubrieron un esquema malicioso sofisticado que se dirige principalmente a los usuarios chinos a través de aplicaciones de imitación en Android e iOS, que imitan los servicios legítimos de billetera digital para desviar fondos de criptomonedas.

> *«Estas aplicaciones maliciosas pudieron robar las frases seed secretas de las víctimas haciéndose pasar por Coinbase, imToken, MetaMask, Trust Wallet, Bitpie, TokenPocket o OneKey»,* dijo Lukas Stefanko, investigador sénior de malware de ESET.

Se dice que los servicios de billetera se distribuyeron por medio de una red de más de 40 sitios web de billetera falsificados que se promocionan con la ayuda de artículos engañosos publicados en sitios web chinos legítimos, así como mediante el reclutamiento de intermediarios a través de grupos de Telegram y Facebook, en un intento por engañar a los visitantes desprevenidos para que descarguen las aplicaciones maliciosas.

ESET, que ha estado rastreando la campaña desde mayo de 2021, la atribuyó al trabajo de un solo grupo criminal. Las aplicaciones de billetera de criptomonedas troyanizadas están diseñadas de tal forma que replican la misma funcionalidad de sus contrapartes originales, al tiempo que incorporan cambios de código malicioso que permiten el robo de activos criptográficos.

> *«Estas aplicaciones maliciosas también representan otra amenaza para las víctimas, ya que algunas de ellas envían frases semilla secretas de víctimas al servidor de los atacantes mediante una conexión HTTP no segura. Esto significa que los fondos de las víctimas podrían ser robados no solo por el operador de este esquema, sino también por un atacante diferente que escucha a escondidas en la misma red»,* dijo Stefanko.

ESET dijo que encontró docenas de grupos que promocionaban copias maliciosas de estas aplicaciones de billetera en la aplicación Telegram, que a su vez, se compartían en al menos 56 grupos de Facebook con la esperanza de conseguir nuevos socios de distribución para el esquema fraudulento.

> *«Según la información obtenida por estos grupos, a una persona que distribuye este malware se le ofrece una comisión del 50% sobre el contenido robado de la billetera»,* dijo ESET.

En un giro único, las aplicaciones, una vez instaladas, se configuran de forma diferente según el sistema operativo de los dispositivos móviles comprometidos. En Android, las aplicaciones están dirigidas a usuarios de criptomonedas que aún no tienen instalada ninguna de las aplicaciones de billetera objetivo, mientras que en iOS, las víctimas pueden tener ambas versiones instaladas.

Cabe mencionar que las aplicaciones de billetera falsa no están disponibles directamente en la tienda de aplicaciones de iOS. Más bien, solo se pueden descargar al visitar uno de los sitios web maliciosos que utilizan perfiles de configuración que permiten instalar aplicaciones que no están verificadas por Apple y de fuentes externas a la App Store.

La investigación también descubrió 13 aplicaciones maliciosas que se hicieron pasar por Jaxx Liberty Wallet en Google Play Store, todas las cuales se eliminaron del mercado de aplicaciones de Android en enero de 2022. Se instalaron de forma colectiva más de 1100 veces.

> *«Su objetivo era simplemente descifrar la frase inicial de recuperación del usuario y enviarla al servidor de los atacantes o a un grupo de chat secreto de Telegram»,*

> dijo Stefanko.

Con los atacantes detrás de la operación reclutando activamente socios a través de las redes sociales y aplicaciones de mensajería y ofreciéndoles un porcentaje de la moneda digital robada, ESET advierte que los ataques podrían extenderse a otras partes del mundo en el futuro.

> *«Además, parece que el código fuente de esta amenaza se filtró y se compartió en algunos sitios web chinos, lo que podría atraer a varios actores de amenazas y propagar esta amenaza aún más»*, agregó Stefanko.