Fraudes de criptomonedas en Android

ESET presenta su informe acerca de estafas con criptomonedas en Android y sus técnicas y trucos. La compañía explica por qué el intercambio de criptomonedas representa un blanco atractivo para las estafas.

Quito, Ecuador - La creciente popularidad y aumento de valor de las criptomonedas, no solo atrae cantidades masivas de potenciales usuarios, sino que también inspira a los estafadores a buscar nuevas maneras obtener algún redito de estas monedas virtuales a costa de usuarios que buscan atacar. ESET, compañía líder en detección proactiva de amenazas, advierte que las estafas con criptomonedas no son exclusivas de las PC´s y surgieron en la plataforma Android, utilizando aplicaciones falsas relacionadas a las criptomonedas.

El intercambio de criptomonedas utilizando dispositivos móviles representa un blanco atractivo para las estafas, no solo por la popularidad de las criptomonedas, sino también porque son muy pocos los que ofrecen una aplicación para dispositivos móviles. Generalmente, el propósito de esta clase de aplicaciones falsas es robar las credenciales de acceso haciéndose pasar por una aplicación que sirva para hacer transacciones. En este sentido, los atacantes utilizan estas credenciales robadas para apoderarse de las cuentas reales. Para tentar a los usuarios y que se animen a compartir sus contraseñas, los estafadores simulan ser el servicio legítimo, imitando el nombre del desarrollador, icono de la aplicación y la interfaz de usuario, además la aplicación suele presentar buenas referencias debido a opiniones falsas.

Un ejemplo reciente de esta clase de estafas se descubrió en el 2017 sobre una falsa aplicación para el intercambio de criptomonedas de Poloniex en Google Play, la cual cada tanto vuelve a aparecer.

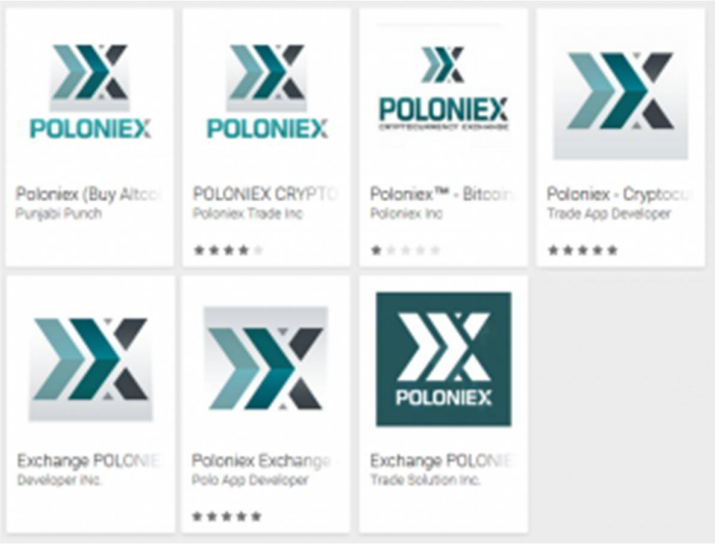

Imagen 1 _ La falsa aplicación Poloniex en Google Play

Otras estrategias de *phishing* afectan también a los usuarios de monederos de criptomonedas, donde los atacantes, en lugar de las contraseñas, buscan obtener las claves y frases privadas de acceso a los monederos. Esto representa un gran riesgo para el usuario ya que el robo de la contraseña de una aplicación para el intercambio de criptomonedas puede ser reseteada con la clave privada del usuario y la ayuda del proveedor del servicio, pero en el caso de un monedero, si la clave privada del usuario es lo que se ve comprometida y nadie puede brindar ayuda en este punto.

Este último caso se observó en aplicaciones que intentan suplantar la identidad de la aplicación MyEtherWallet, un popular monedero de criptomonedas de código abierto para Etherum. Las aplicaciones, subidas a Google Play en varias ocasiones en los últimos meses, amenazan con robar las claves privadas de los usuarios y/o las frases mnemotécnicas utilizando varios formularios de login falsos. **Tanto Poloniex como MyEtherWallet no cuentan con una aplicación oficial**, lo que los hace atractivos para los estafadores.

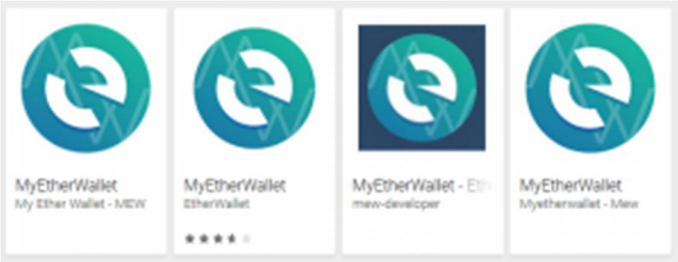

Imagen 2 _ Las aplicaciones falsas de MyEtherWallet en Google Play

Además de casos de phishing en aplicaciones, ESET también analizó casos de monederos de criptomonedas que intentan engañar a la víctima para que transfiera sus monedas a la cartera del atacante. Esta clase de estafas pretenden generar una clave pública para un nuevo monedero e instruir a los usuarios para que envíen sus monedas digitales a la dirección generada. Si los usuarios siguen las instrucciones, pronto caerán en la cuenta de que las monedas enviadas ya no están más.

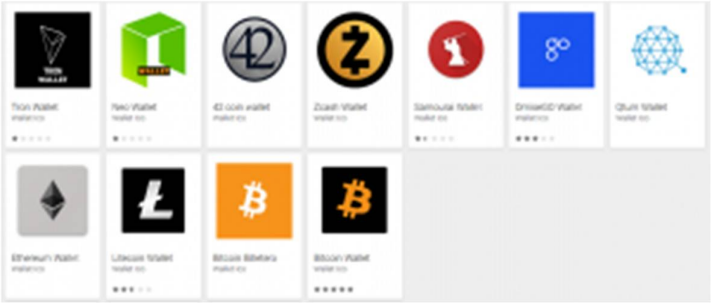

Imagen 3 _ Fraudes de aplicaciones de monederos que apuntan a usuarios de varias criptomonedas

Con el reciente auge en la minería de criptomonedas, el número de dispositivos Android utilizados para minar también creció. Para que una aplicación de minería de criptomonedas sea considerada maliciosa dependerá de si el usuario le dio o no su consentimiento. El malware de criptominería provoca que el dispositivo este siendo usado

por alguien más para su propio beneficio. Recientemente, se descubrió que la versión del juego Bug Smasher, instalado desde Google Play entre 1 y 5 millones de veces, estuvo minando de manera secreta en los usuarios la criptomoneda Monero.

Una categoría aparte dentro de las estafas de criptomonedas pertenece a la de aplicaciones que pretenden minar criptomonedas para el usuario, pero que en realidad no hacen más que mostrar anuncios. Algunos de los falsos mineros analizados por ESET incluso intentaban engañar a los usuarios para que los evalúen con cinco estrellas.

Todas las aplicaciones mencionadas anteriormente fueron detectadas y bloqueadas por los sistemas de ESET y fueron suspendidas de la tienda de Google Play. Los usuarios que tengan habilitado Google Play Protect estarán protegidos de este tipo de amenazas.

A continuación, el Laboratorio de Investigación de ESET Latinoamérica detalla algunos puntos a tener en cuenta para evitar ser víctima de estafas con criptomonedas en Android:

- Tratar el intercambio de criptomonedas y monederos con el mismo grado de precaución que se utiliza una aplicación bancaria.
- Cuando se descargue una aplicación para el intercambio o almacenamiento de criptomonedas, asegurarse de que el servicio realmente ofrezca una aplicación. La app oficial debería aparecer enlazada en la página oficial de quien ofrece el servicio.
- Si la opción está disponible, utilizar autenticación de dos factores (A2F) para proteger la cuenta de intercambio o monedero con una capa adicional de seguridad.
- Al descargar aplicaciones de Google Play, prestar atención al número de descargas, así como también a las calificaciones y los comentarios.
- Mantener los dispositivos Android actualizados y utilizar una solución de seguridad de confianza para protegerse de las últimas amenazas.

Para conocer más acerca de estafas con criptomonedas en Android y sus técnicas y trucos, lee el whitepaper elaborado por ESET, "Cryptocurrency scams on Android" (en inglés).

También se invita a discutir estos y otros temas con los expertos de ESET durante el Mobile World Congress 2018 en Barcelona, en el puesto 41 de la sala 7.

Para más información puede ingresas al portal de noticias de ESET llamado We Live Security en: https://www.welivesecurity.com/la-es/2018/02/28/estafas-criptomonedas-android/