Se ha observado que más de 200 aplicaciones de Android que se hacen pasar por aplicaciones de acondicionamiento físico, edición de fotos y rompecabezas, están distribuyendo el software espía llamado Facestealer, para desviar las credenciales de los usuarios y otra información valiosa.

> *«Al igual que Joker, otra pieza de malware móvil, Facestealer cambia su código con frecuencia, lo que genera muchas variantes. Desde su descubrimiento, el spyware ha asediado continuamente a Google Play»,* dijeron los analistas de Trend Micro, Cifer Fang, Ford Quin y Zhengyu Dong.

Facestealer, documentado por primera vez por Doctor Web en julio de 2021, se refiere a un grupo de aplicaciones fraudulentas que invaden el mercado oficial de aplicaciones para Android, con el objetivo de saquear datos confidenciales como las credenciales de inicio de sesión de Facebook.

De las 200 aplicaciones, 42 son servicios VPN, seguidas de cámara (20) y aplicaciones de edición de fotos (13). Además de recopilar credenciales, las aplicaciones también están diseñadas para recopilar cookies de Facebook e información de identificación personal asociada con la cuenta de la víctima.

Además, Trend Micro reveló que descubrió más de 40 aplicaciones de minería de criptomonedas deshonestas que se dirigen a usuarios interesados en criptomonedas. Estas aplicaciones contienen malware diseñado para engañar a los usuarios para que vean anuncios y paguen por servicios de suscripción.

Algunas de las aplicaciones criptográficas falsas, como Cryptomining Farm Your own Coin, van un paso más allá al intentar robar claves privadas y frases mnemotécnicas que se utilizan para recuperar el acceso a una billetera de criptomonedas.

Nuevo estudio analiza las aplicaciones maliciosas de Android instaladas en la naturaleza

Los hallazgos se producen cuando los investigadores de NortonLifeLock y la Universidad de Boston publicaron el *«estudio en dispositivo más grande»* de aplicaciones potencialmente dañinas (PHA) en Android, basado en 8.8 millones de PHA instalados en más de 11.7 millones de dispositivos entre 2019 y 2020.

«Los PHA persisten en Google Play durante 77 días en promedio y 34 días en mercados de terceros», dice el estudio, que también señala la demora entre el momento en que se identifican los PHA y el momento en que se eliminan, agregando 3553 aplicaciones que exhibieron migración entre mercados después de ser derribados.

Además, la investigación también muestra que los PHA permanecen por un período mucho más largo en promedio cuando los usuarios cambian de dispositivo e instalan automáticamente las aplicaciones al restaurar desde una copia de seguridad.

Se dice que se transfirieron hasta 14,000 PHA a 35,500 nuevos dispositivos Samsung mediante el uso de la aplicación móvil Samsung Smart Switch, y las aplicaciones duraron en los teléfonos por un período de aproximadamente 93 días.

> *«El modelo de seguridad de Android limita severamente lo que pueden hacer los productos de seguridad móvil al detectar una aplicación maliciosa, lo que permite que los PHA persistan durante muchos días en los dispositivos de las víctimas. El sistema de advertencia actual empleado por los programas de seguridad móvil no es eficaz para convencer a los usuarios de que desinstalen rápidamente las PHA»,* dijeron los académicos.