Los sitios web imitadores de aplicaciones de mensajería instantánea como Telegram y WhatsApp se están usando para distribuir versiones troyanizadas e infectar a los usuarios de sistemas operativos Android y Windows con el malware de minería de criptomonedas, Clipper.

> *«Todos ellos buscan los fondos de criptomonedas de las víctimas, y varios apuntan a las billeteras de criptomonedas»,* dijeron los investigadores de ESET, Lukas Stefanko y Peter Strycek.

Aunque la primera instancia de malware clipper en Google Play Store se remonta a 2019, el desarrollo marca la primera vez que el malware clipper basado en Android se integra en aplicaciones de mensajería instantánea.

> *«Además, algunas de estas aplicaciones usan el reconocimiento óptico de caracteres (OCR) para reconocer el texto de las capturas de pantalla almacenadas en los dispositivos comprometidos, que es otra novedad para el malware de Android»*, agregó la compañía de seguridad cibernética.

La cadena de ataque comienza con usuarios desprevenidos que hacen clic en anuncios fraudulentos en los resultados de búsqueda de Google que conducen a cientos de canales de YouTube incompletos, que después los dirigen a sitios web similares a Telegram y WhatsApp.

Lo novedoso del último lote de malware clipper es que es capaz de interceptar los chats de una víctima y reemplazar cualquier dirección de billetera de criptomonedas enviada y recibida con direcciones controladas por los hackers.

Otro grupo de malware clipper utiliza OCR para encontrar y robar frases iniciales aprovechando un complemento de aprendizaje automático legítimo llamado ML Kit en Android, lo que hace posible vaciar las billeteras.

Un tercer grupo está diseñado para controlar las conversaciones de Telegram para ciertas palabras clave chinas relacionadas con las criptomonedas, tanto codificadas como recibidas de un servidor, y si es así, filtrar el mensaje complejo, junto con el nombre de usuario, grupo o nombre del canal, a un servidor remoto.

Finalmente, un cuarto conjunto de cortadores de Android cuenta con capacidades para cambiar la dirección de la billetera, así como para recopilar información del dispositivo y datos de Telegram, como mensajes y contactos.

Los nombres de los paquetes APK de Android falsos se enumeran a continuación:

- org.telegram.messenger
- org.telegram.messenger.web2
- org.tgplus.messenger
- io.busniess.va.whatsapp
- com.whatsapp

ESET dijo que también encontró dos clústeres basados en Windows, uno que está diseñado para intercambiar direcciones de billetera y un segundo grupo que distribuye troyanos de acceso remoto (RAT) en lugar de clippers para obtener el control de los hosts infectados y realizar el robo de criptomonedas.

Todas las muestras de RAT analizadas se basan en Gh0st RAT disponible públicamente, excepto una, que emplea más controles de tiempo de ejecución antianálisis durante su ejecución y utiliza la biblioteca de socket HP para comunicarse con su servidor.

También cabe mencionar que estos grupos, a pesar de seguir un modus operandi idéntico, representan conjuntos dispares de actividad probablemente desarrollados por distintos atacantes.

La campaña, como una operación cibernética maliciosa similar que salió a la luz el año pasado, está dirigida a los usuarios de habla china, motivada principalmente por el hecho de

que tanto Telegram como WhatsApp están bloqueados en el país.

> *«Las personas que deseen utilizar estos servicios tienen que recurrir a medios indirectos para obtenerlos. Como era de esperar, esto constituye una gran oportunidad para que los hackers abusen de la situación»,* dijeron los investigadores.