Se detectó una aplicación de software espía de Android que se hace pasar por un servicio de *«Administrador de procesos»* para desviar de forma sigilosa la información confidencial almacenada en los dispositivos infectados.

La aplicación, con el nombre de paquete «com.remote.app«, establece contacto con un servidor de comando y control remoto, 82.146.35[.]240, que se identificó previamente como una infraestructura perteneciente a un grupo de piratería de Rusia conocido como Turla.

> *«Cuando se ejecuta la aplicación, aparece una advertencia sobre los permisos otorgados a la aplicación. Estos incluyen intentos de desbloqueo de pantalla, bloqueo de pantalla, configuración del proxy global del dispositivo, configuración de vencimiento de contraseña de bloqueo de pantalla, configuración de cifrado de almacenamiento y desactivación de cámaras»,* dijeron los investigadores de Lab52.

Una vez que la aplicación está *«activada»,* el malware elimina su icono con forma de engranaje de la pantalla de inicio y se ejecuta en segundo plano, abusando de sus amplios permisos para acceder a los contactos y registros de llamadas del dispositivo, rastrear su ubicación, enviar y leer mensajes, acceder a almacenamiento, tomar fotografías y grabar audio.

La información recopilada es capturada en formato JSON y posteriormente transmitida al servidor remoto antes mencionado. A pesar de la superposición en el servidor C2 utilizado, Lab52 dijo que no tiene suficiente evidencia para atribuir definitivamente el malware al grupo Turla.

También se desconoce en esta etapa el vector de acceso inicial exacto empleado para distribuir el software espía y los objetivos previstos de la campaña.

La aplicación maliciosa de Android también intenta descargar una aplicación legítima llamada Roz Dhan (que significa «riqueza diaria», traducido del hindi), que tiene más de 10 millones de instalaciones y permite a los usuarios obtener recompensas en efectivo por completar

encuestas y cuestionarios.

> *«La aplicación, que está en Google Play y se utiliza para ganar dinero, tiene un sistema de referencia que es abusado por el malware. El atacante lo instala en el dispositivo y obtiene una ganancia»,* dijeron los investigadores.