Una campaña de software espía para Android en rápida evolución, conocida como ClayRat, ha estado atacando a usuarios en Rusia mediante una combinación de canales de Telegram y sitios web falsos que imitan aplicaciones populares como WhatsApp, Google Fotos, TikTok y YouTube, utilizándolas como señuelo para inducir a las víctimas a instalarlas.

"Una vez activo, el spyware puede robar mensajes SMS, registros de llamadas, notificaciones e información del dispositivo; tomar fotos con la cámara frontal; e incluso enviar mensajes de texto o realizar llamadas directamente desde el dispositivo comprometido", señaló el investigador de Zimperium, Vishnu Pratapagiri, en un informe.

Este malware también ha sido diseñado para replicarse a sí mismo, enviando enlaces maliciosos a todos los contactos almacenados en el dispositivo de la víctima, lo que revela una estrategia agresiva por parte de los atacantes para utilizar los teléfonos infectados como medio de propagación.

La empresa de seguridad móvil reportó haber detectado al menos 600 variantes y 50 aplicaciones portadoras (droppers) en los últimos 90 días, cada una con técnicas de ofuscación más complejas que buscan eludir los sistemas de detección y mantenerse un paso adelante de las defensas de seguridad. El nombre ClayRat proviene del panel de comando y control (C2) utilizado para manejar remotamente los dispositivos comprometidos.

La cadena de ataque implica redirigir a los usuarios desprevenidos desde estos sitios fraudulentos hacia canales de Telegram controlados por los atacantes, donde son convencidos de descargar archivos APK, utilizando cifras de descargas infladas artificialmente y testimonios falsos como evidencia de popularidad.

En otros casos, sitios fraudulentos que ofrecen una supuesta versión «YouTube Plus» con funciones premium han sido utilizados para alojar archivos APK capaces de eludir las protecciones de seguridad impuestas por Google, diseñadas para impedir la instalación de aplicaciones por fuera de la Play Store en dispositivos con Android 13 o versiones posteriores.

"Para esquivar las restricciones de la plataforma y las nuevas barreras introducidas en

versiones más recientes de Android, algunas variantes de ClayRat actúan como droppers: la aplicación visible es simplemente un instalador ligero que muestra una falsa pantalla de actualización de la Play Store, mientras que el verdadero contenido cifrado está oculto en los recursos de la app", explicó la empresa. *"Este método de instalación por sesión reduce la percepción de riesgo y aumenta la probabilidad de que una simple visita a una página web termine con el spyware instalado"*.

Una vez dentro del sistema, ClayRat se comunica con su infraestructura C2 usando HTTP estándar y solicita convertirse en la aplicación de SMS predeterminada para poder acceder a mensajes, notificaciones y registros de llamadas. Esto le permite capturar de forma encubierta datos sensibles y continuar diseminando el malware a los contactos del usuario infectado.

Entre otras funciones adicionales, el spyware puede realizar llamadas telefónicas, recopilar datos del dispositivo, capturar imágenes con la cámara y enviar al servidor C2 una lista completa de las aplicaciones instaladas.

ClayRat representa una amenaza seria no solo por sus capacidades de espionaje, sino también por su potencial para transformar un dispositivo comprometido en un nodo de distribución automatizado, lo que permite a los atacantes ampliar su alcance de forma rápida y sin intervención manual.

Este desarrollo se da en paralelo a una investigación realizada por académicos de la Universidad de Luxemburgo y la Université Cheikh Anta Diop, quienes descubrieron que aplicaciones preinstaladas en teléfonos Android de bajo costo vendidos en África operan con privilegios elevados. Uno de estos paquetes, proporcionado por el fabricante, incluso transmite identificadores del dispositivo y datos de localización a un tercero externo.

El estudio analizó 1,544 archivos APK recopilados de siete modelos de smartphones distribuidos en África y halló que *"145 aplicaciones (9%) revelan datos sensibles, 249 (16%) exponen componentes críticos sin protecciones adecuadas, y muchas presentan riesgos adicionales: 226 ejecutan comandos privilegiados o peligrosos, 79 interactúan con mensajes*

SMS (leer, enviar o eliminar), y 33 realizan instalaciones silenciosas”.