Los modelos económicos de dispositivos Android, que son versiones falsificadas asociadas con marcas populares de smartphones, albergan múltiples troyanos diseñados para apuntar a las aplicaciones de mensajería instantánea de WhatsApp y WhatsApp Business.

Los troyanos, que Doctor Web detectó por primera vez en julio de 2022, se descubrieron en la partición del sistema de al menos cuatro teléfonos inteligentes: P48pro, radmi note 8, Note30u y Mate40

> *«Estos incidentes están unidos por el hecho de que los dispositivos atacados eran imitaciones de modelos de marcas famosas»,* dijo la compañía de seguridad.

> *«Además, en lugar de tener una de las últimas versiones del sistema operativo con la información correspondiente que se muestra en los detalles del dispositivo (por ejmplo, Android 10), tenían la versión 4.4.2 obsoleta».*

Específicamente, la manipulación se refiere a dos archivos «/system/lib/libcutils.so» y «/system/lib/libmtd.so» que se modifican de tal forma que cuando cualquier aplicación usa la biblioteca del sistema libcutils.so, desencadena la ejecución de un troyano incorporado en libmtd.so.

Si las aplicaciones que usan las bibliotecas son WhatsApp y WhatsApp Business, libmtd.so procede a lanzar una tercera puerta trasera cuya principal responsabilidad es descargar e instalar complementos adicionales desde un servidor remoto en los dispositivos comprometidos.

> *«El peligro de las puertas traseras descubiertas y los módulos que descargan es que funcionan de tal forma que en realidad se convierten en parte de las aplicaciones objetivo»,* dijeron los investigadores.

> *«Como resultado, obtienen acceso a los archivos de las aplicaciones atacadas y pueden leer chats, enviar spam, interceptar y escuchar llamadas telefónicas y ejecutar otras acciones maliciosas, según la funcionalidad de los módulos descargados».*

Por otro lado, si la aplicación que utiliza las bibliotecas resulta ser wpa_supplicant, un daemon del sistema que se usa para administrar las conexiones de red, libmtd.so está configurado para iniciar un servidor local que permite conexiones desde un cliente remoto o local por medio de «mysh».

Doctor Web cree que los implantes de partición del sistema podrían ser parte de la familia de malware FakeUpdates (también conocido como SocGholish) basado en el descubrimiento de otro troyano incrustado en la aplicación del sistema responsable de las actualizaciones de firmware por aire (OTA).

La aplicación no autorizada, por su parte, está diseñada para filtrar metadatos detallados sobre el dispositivo infectado, así como para descargar e instalar otro software sin el conocimiento de los usuarios por medio de secuencias de comandos Lua.

Para evitar el riesgo de ser víctima de dichos ataques de malware, se recomienda que los usuarios compren dispositivos móviles solo en tiendas oficiales y distribuidores legítimos.