Investigadores aseguran que la aplicación para Android de drones DJI roba información personal

Autor: I. Stepanenko

Fecha: Monday 3rd of August 2020 06:09:36 PM

Investigadores de seguridad cibernética revelaron este jueves problemas de seguridad en la aplicación de Android desarrollada por el fabricante chino de drones, Da Jiang Innovations (DJI), que cuenta con un mecanismo de actualización automática que evita Google Play Store y podría usarse para instalar apps maliciosas y transmitir información personal confidencial a los servidores de DJI.

Los informes de Synacktiv y GRIMM, especifican que la aplicación Go 4 de DJI para Android, no solo solicita permisos extensos y recopila datos personales (IMSI, IMEI, número de serie de SIM), sino que además, utiliza técnicas de anti depuración y de encriptación para frustrar el análisis de seguridad.

> «Este mecanismo es muy similar a los servidores de comando y control encontrados con malware. Dados los amplios permisos requeridos por DJI Go 4 (contactos, micrófono, cámara, ubicación, almacenamiento, cambio de conectividad de red), los servidores chinos DJI o Weibo tienen un control casi total sobre el teléfono del

> usuario», dijo Synacktiv.

La aplicación de Android tiene más de un millón de instalaciones a través de Google Play Store. Pero las vulnerabilidades de seguridad identificadas en la aplicación no se aplican a su versión de iOS, que no está ofuscada, ni tiene la función de actualización oculta.

GRIMM asegura que su investigación se realizó como respuesta a una auditoría de seguridad solicitada por un proveedor de tecnología de defensa y seguridad pública no identificado, que buscaba *«investigar las implicaciones de privacidad de los drones DJI dentro de la aplicación Android DJI Go 4».*

A su vez, Synacktiv dijo que descubrió la existencia de una URL («hxxps: //service-adhoc.dji.com/app/upgrade/public/check»), que utiliza para descargar una actualización de la aplicación y solicitar al usuario que conceda permiso para *«instalar aplicaciones desconocidas».*

> «Modificamos esta solicitud para activar una actualización forzada de una aplicación arbitraria, lo que llevó al usuario primero a permitir la instalación de aplicaciones que no son de confianza, y luego le impidió usar la aplicación hasta que se instaló la actualización», dijeron los investigadores.

No solo es una violación directa de las pautas de Google Play Store, sino que las implicaciones de esta función son enormes. Un atacante podría comprometer el servidor de actualización para apuntar a los usuarios con actualizaciones de aplicaciones maliciosas.

Además, la aplicación sigue ejecutándose en segundo plano, aún después de cerrarla, y aprovecha un SDK de Weibo («com.sina.weibo.sdk») para instalar una aplicación descargada arbitrariamente, activando la función para los usuarios que optaron por la transmisión en vivo de video de drones a través de Weibo. GRIMM dijo que no encontró evidencia de que fuera explotado para apuntar a personas con instalaciones de aplicaciones maliciosas.

Los investigadores también descubrieron que la aplicación aprovecha MobTech SDK para pasar metadatos sobre el teléfono, incluido el tamaño de la pantalla, el brillo, la dirección WLAN, la dirección MAC, los BSSID, las direcciones Bluetooth, los números IMEI e IMSI, el nombre del operador, el número de serie de la SIM, la información de la tarjeta SD, el idioma del sistema operativo, la versión del kernel y la información de ubicación.

Postura de DJI

DJI cuestionó la investigación y llamó a los hallazgos como *«preocupaciones típicas de software»,* afirmando que contradice los *«informes del Departamento de Seguridad Nacional de Estados Unidos, Booz Allen Hamilton y otros que no han encontrado evidencia de conexiones inesperadas de transmisión de datos de las aplicaciones de DJI diseñadas para clientes gubernamentales y profesionales».*

> «No hay evidencia de que alguna vez fueron explotados, y no se usaron en los sistemas de control de vuelo de DJI para clientes gubernamentales y profesionales. En futuras versiones, los usuarios también podrán descargar la versión oficial de Google Play si está disponible en su país. Si los usuarios no dan su consentimiento para hacerlo, su versión no autorizada de la aplicación se desactivará por razones de seguridad», dijo la compañía.

DJI es el mayor fabricante a nivel mundial de drones comerciales, y se ha enfrentado a un mayor escrutinio junto con otras compañías chinas debido a preocupaciones de seguridad nacional, lo que lleva al Departamento del Interior de Estados Unidos a aterrizar su flota de drones DJI a inicios de enero.

En mayo, advirtió a las empresas que sus datos pueden estar en riesgo si utilizan drones comerciales fabricados en China y que *«contienen componentes que pueden comprometer sus datos y compartir su información en un servidor al que se accede más allá de la propia empresa».*

«Esta decisión deja en claro que las preocupaciones del gobierno de Estados Unidos sobre los drones DJI, que constituyen una pequeña parte de la flota de DOI, tienen poco que ver con la seguridad y, en cambio, son parte de una agenda políticamente motivada para reducir la competencia en el mercado y apoyar el dron producido en el país, independientemente de sus méritos», dijo la compañía en un comunicado en enero.