AirHub

Data security in drone operations

DRONE MISSIONS

AirHub

Drone security issues in the news

DJI insisted drone-tracking AeroScope signals were encrypted — now it admits they aren't

The packets are in the air for anyone to grab

By Sean Hollister | @StarFire2258 | Apr 28, 2022, 3:34pm EDT

SHARE

Onderzoek Chinese drones halen data binnen

Made for China

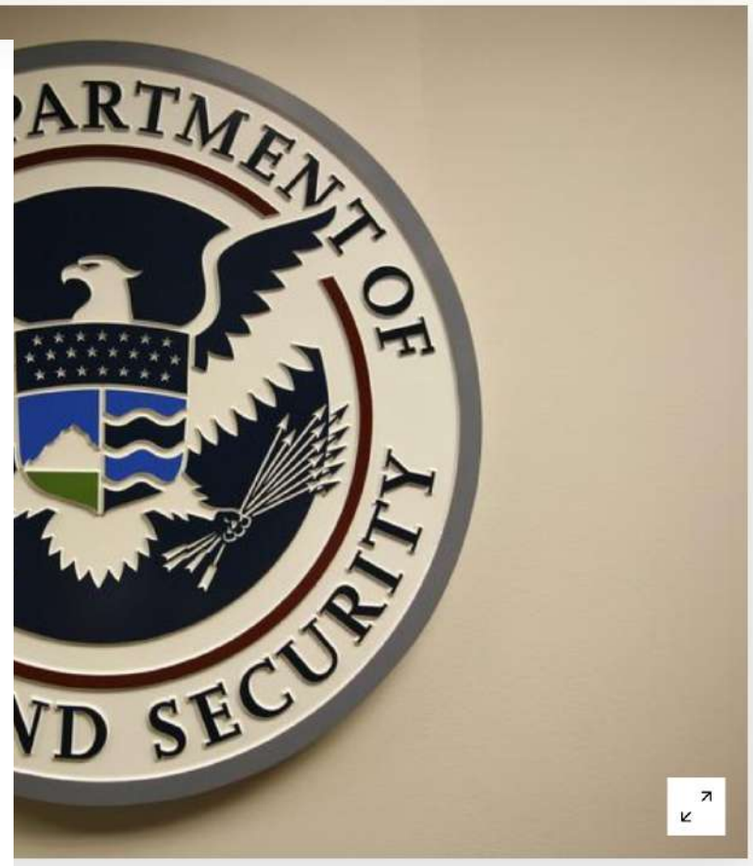
De mini-helikopters van DJI, gebruikt door onder meer de N
dataslurpers. Zonder toestemming van de gebruiker wordt s
toega

DHS warns of data threat from Chinese-made drones

By David Shepardson

2 MIN READ

FCC commissioner calls for tighter restrictions on DJI drones



Drone security issues

Summary of press research results

- Research shows that DJI drones collects more data than is needed for a flight, such as:
  -SIM card serial number
  -Information about devices in the same WiFi network
  -Phone screen brightness

- The US Federal Communications Commission claims that DJI collects sensitive data and therefore poses a "national security risk".

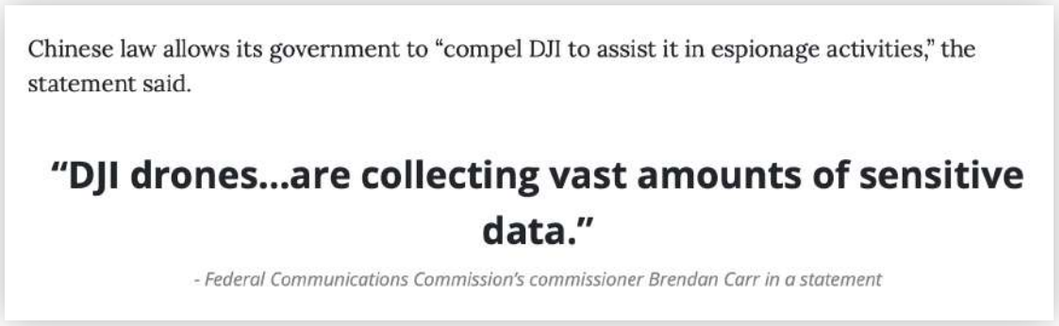
- Government organizations must take drastic precautions. Such as own operating software and own servers for data storage.

NEWS

Chinese Drone Maker DJI Faces More U.S. Restrictions

FCC commissioner wants to blacklist the best-selling drone builder in the U
poses a national security risk.

By Thom Patterson | October 21, 2021



Chinese law allows its government to “compel DJI to assist it in espionage activities,” the statement said.

“DJI drones…are collecting vast amounts of sensitive data.”

- Federal Communications Commission’s commissioner Brendan Carr in a statement

AirHub

DJI Security Audit by AirHub

DJI Cloud

DJI Apps

DJI Mobile SDK

DJI Smart Controller

AirHub

DJI Security Audit by AirHub

DJI Cloud

- The DJI cloud is a highly vulnerable product, where flight data and media are stored on Chinese servers. This service turned out to be relatively easy to access for malicious parties when in 2018 the IT security company Check Point was able to watch live flights as a result of a data breach.

- The DJI cloud leak is currently still unresolved, according to the multitude of platforms that offer DJI Import functions. Storing DJI credentials for this by third parties can lead to further security risks.

AirHub

DJI Security Audit by AirHub

DJI Apps

- AirHub has analyzed the requests sent from the following DJI apps: DJI GO4, DJI Fly, DJI Pilot.

- This showed that these apps send a multitude of requests to all kinds of different servers and websites. It is striking that this traffic differs per app in both amount and destination.

- Without logging in, functions are limited or an app can even become completely unusable. By logging in, DJI can link all kinds of data to its users.

AirHub

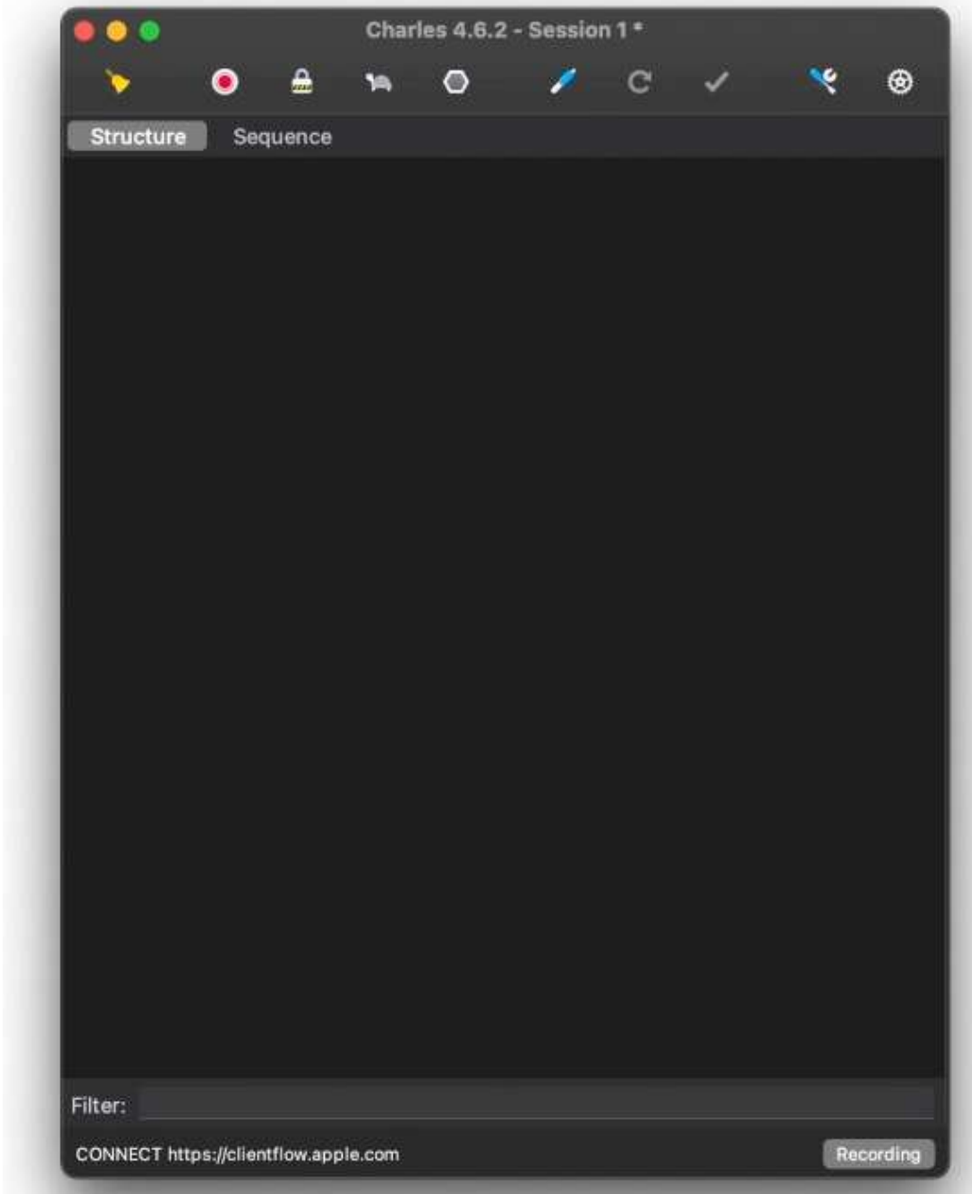
DJI Security Audit by AirHub

Data traffic – DJI GO4

AirHub

DJI Security Audit by AirHub

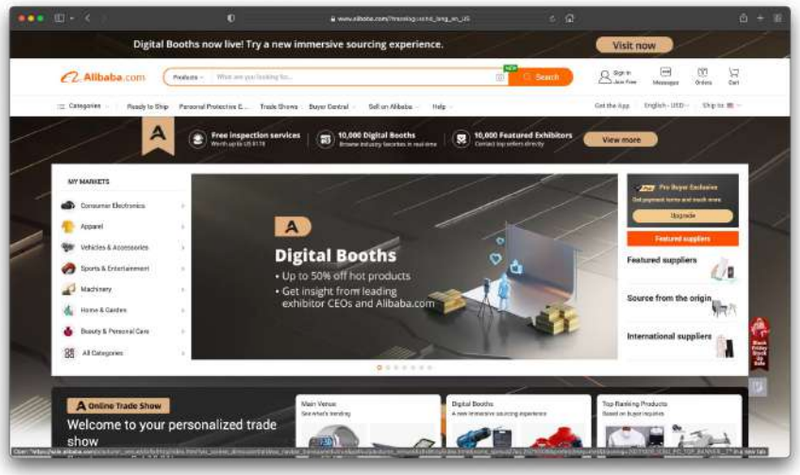
Data traffic - DJI GO4

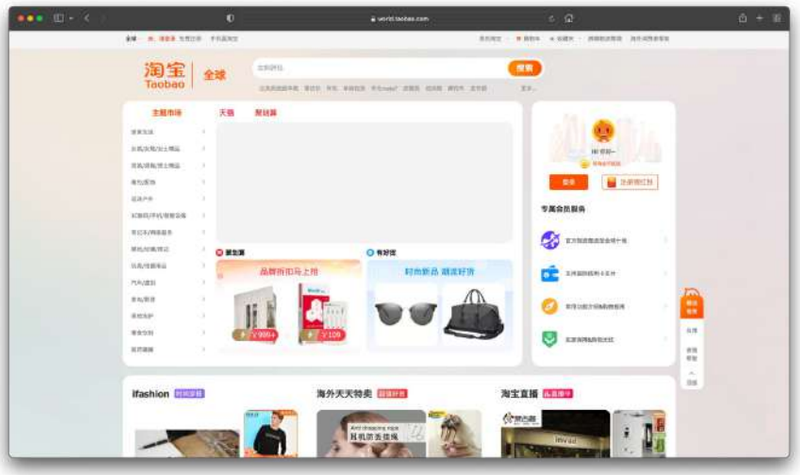


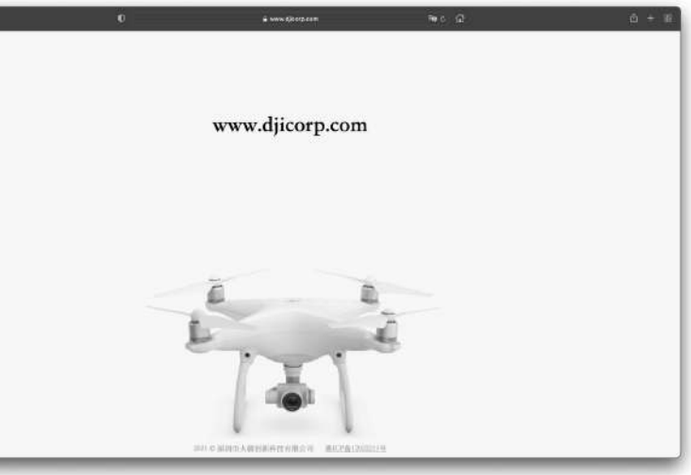
AirHub

DJI Security Audit by AirHub

DJI Apps – Requests







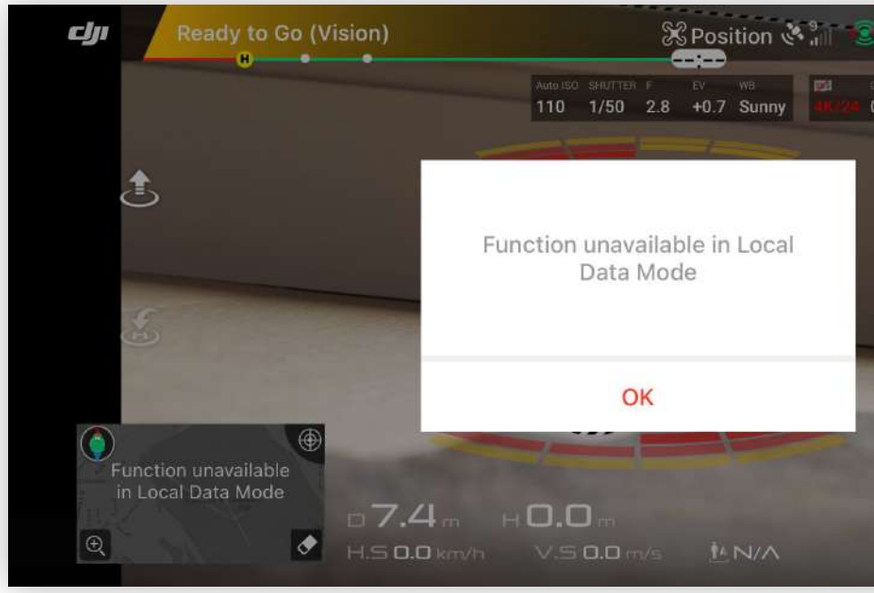
DJI Security Audit by AirHub

DJI Apps - LDM

- The Local Data Mode can be enabled from within the DJI Apps under the heading Privacy. LDM eliminates requests deemed unnecessary by DJI.

- When using LDM, DJI also determines when and especially what data is sent and where to. However, the number of requests from the apps is a lot lower. This does differ per app, which means that LDM is not a uniform product.

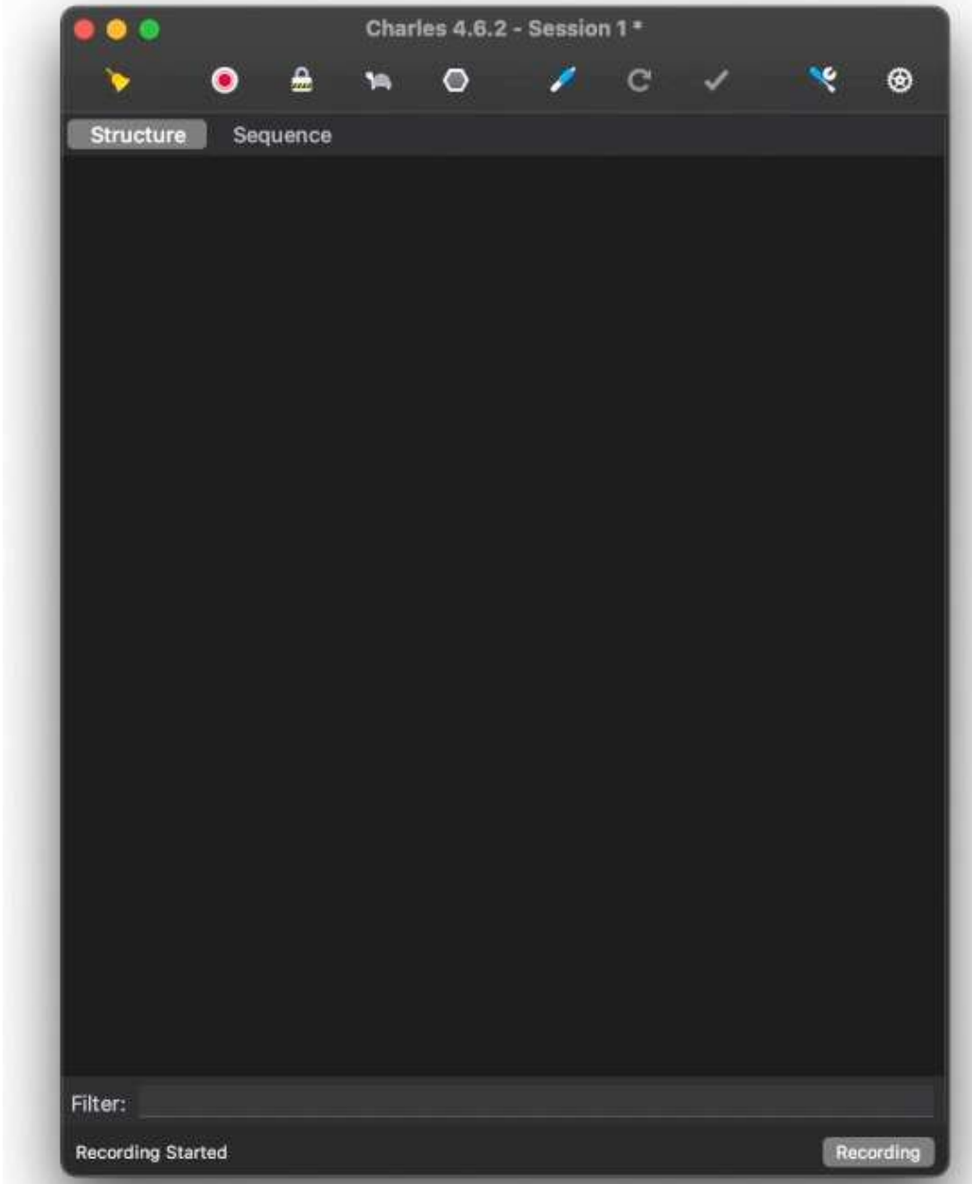
- The following functionalities are disabled when turning on LDM: Video streaming (YouTube, Facebook & RTMP) Unlock geofences (DJI verified)



AirHub

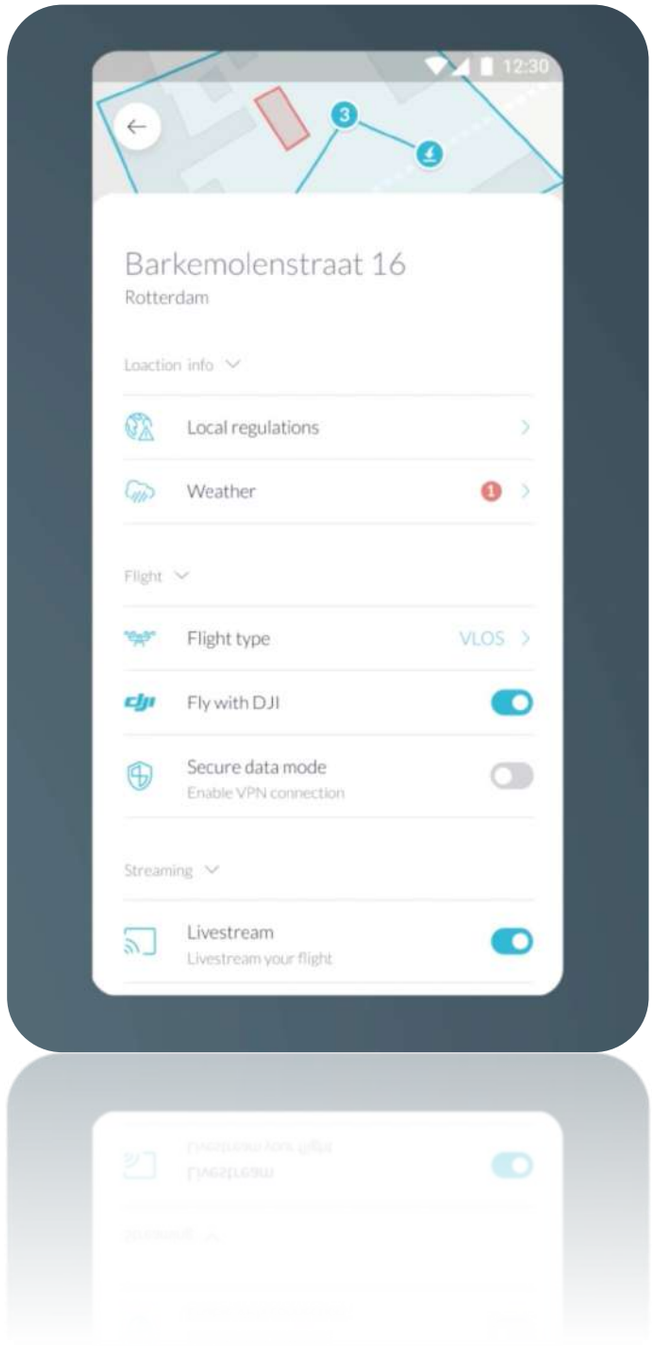
DJI Security Audit by AirHub

Data traffic - DJI Fly with LDM



AirHub

AirHub solution



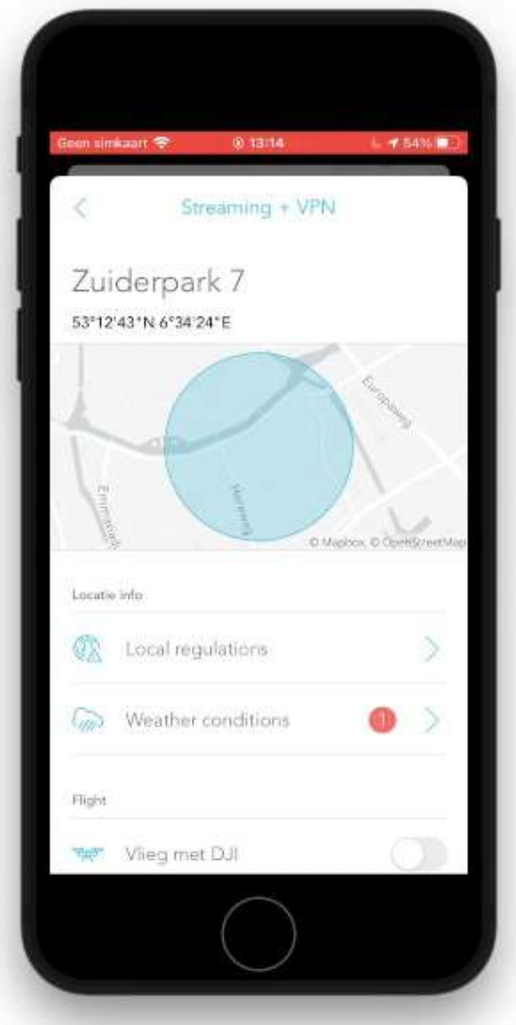
DJI Smart Controller

iOS & Android

AirHub

DJI Security Audit by AirHub

Streaming - DJI SDK with AirHub Secure Data Mode



AirHub

Thank you for your attention

AirHub