

Orange
Cyberdefense

Drone2Pwn

SecSea2K24



Nicolas Bourras - 12/10/2024



A propos





- Auditeur sécurité junior @ Orange Cyberdefense
- LinkedIn : Nicolas Bourras
- Discord : discere (alias: vivescere)
- <https://nicolasb.fr>



Contexte

Un jour, en mission

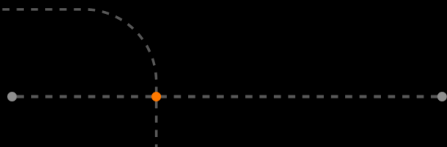
- En test interne, avec une prestation WiFi
- Sur le parking de l'entreprise
- Avec Wifite
- Un petit coup de Hashcat, et...

BROKEN RATIO				TOTAL TASKS
1 / 1 100% 	1 / 1	7 / 7	-	8 / 8

Contexte

Un jour, en mission

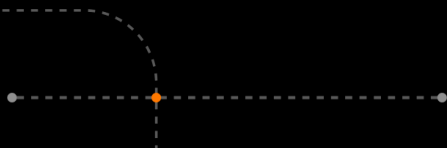
- Sauf que...



Contexte

Un jour, en mission

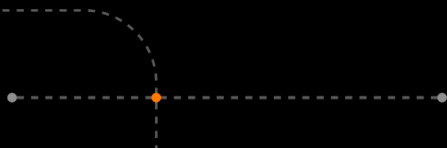
- Des solutions ?
 - Une grosse antenne ?
 - Rentrer dans le parking ?
 - Menace interne / phishing ?
- Et pourquoi pas ... un drone ?



Contexte

Un jour, en mission

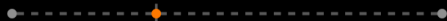
« Personne ne ferait ça »



Contexte

L'idée

- Venir poser un drone sur le toit du bâtiment
 - Potentiellement de nuit
 - Attaquer le WiFi
 - Et repartir :)
-
- A utiliser en Test Interne, en Red Team, et en Purple Team



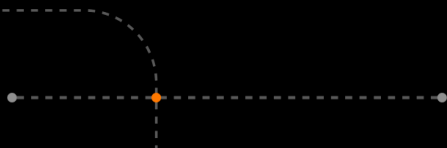
Sommaire

1. A propos
2. Contexte
3. Attaques WiFi
4. Problématiques
5. Historique
6. Prototype
7. Travail restant

Attaques WiFi

Clef PSK faible

- Deauthentication
- Capture de Handshake
- Et ... Hashcat :)



Attaques WiFi

Réseaux invités

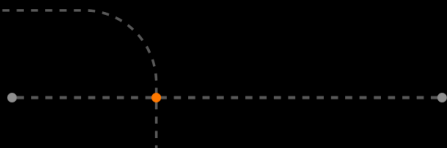
- Avec un portail captif
- Ou du filtrage MAC
- Et parfois avec un cloisonnement douteux



Attaques WiFi

Réseaux ouverts

- Absence d'authentification
- Réseaux IoT, industriels, ...



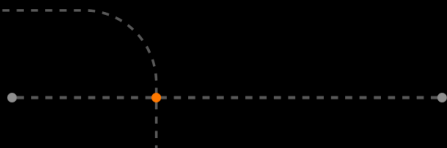
Sommaire

1. A propos
2. Contexte
3. Attaques WiFi
4. Problématiques
5. Historique
6. Prototype
7. Travail restant

Problématiques

Type de drone

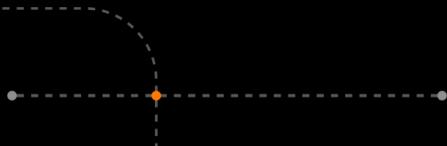
- Avion RC ?
- Hélicoptère RC ?
- Drone ?



Problématiques

Moyen de communication

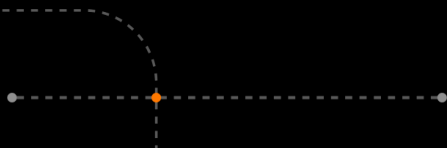
- Bluetooth ?
- WiFi ?
- LoRa ?
- 4G / 5G ?



Problématiques

Batterie et poids

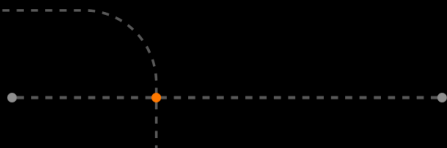
- Batterie de 30 minutes
- Possibilité de porter un poids de plus de 100 grames

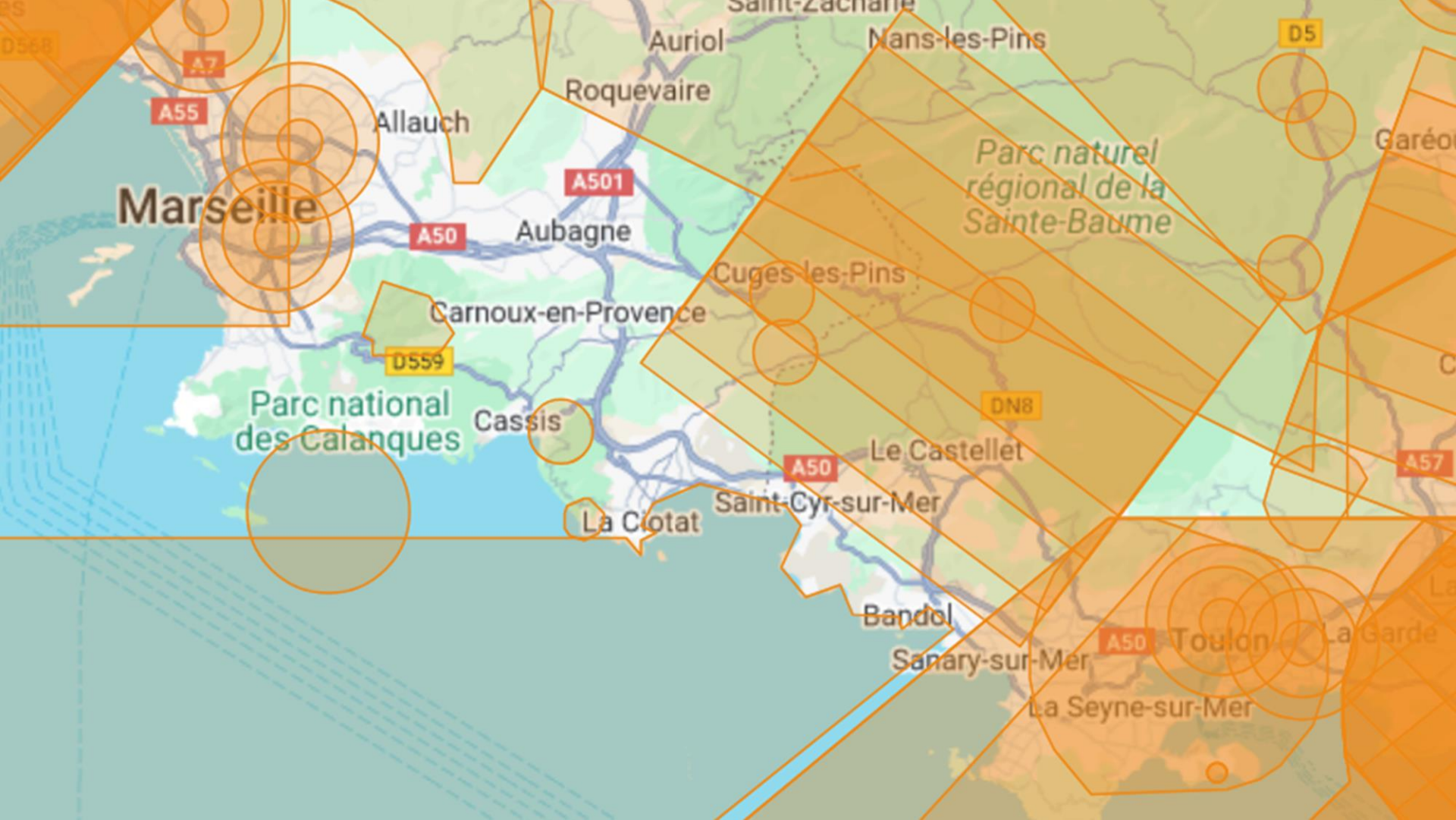


Problématiques

Législation : zones géo

- Zones restreintes
- Zones à altitude limitée
- Zones d'autorisation
- Zones de prudence accrue
- Zones de prudence





Marseille

Parc national
des Calanques

Parc naturel
régional de la
Sainte-Baume

Toulon



Agliana

Prato

SR302

Iolo

Calenzano

SS65

Quarrata

Campi
Bisenzio

Sesto
Fiorentino

SS65

Poggio
a Caiano

Fiesole

SS67

Florence

Pontass

Montelupo
Fiorentino

mpoli

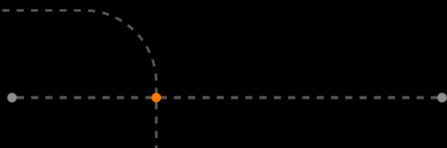
Rign
sull'

A1

Problématiques

Législation : catégories de drones

- **C0** : Moins de 250 grammes, sans caméra ou avec une caméra jouet.
- **C1** : Moins de 900 grammes, avec des dispositifs de protection des données.
- **C2** : Moins de 4 kilogrammes, avec des dispositifs de réduction de vitesse.
- **C3 et C4** : Moins de 25 kilogrammes, avec des règles spécifiques pour les drones sans modes de contrôle automatique.

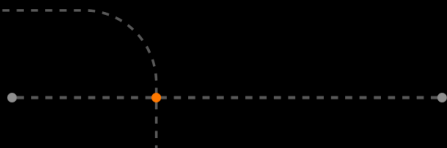


Problématiques

Législation : catégorie spécifique

Scénarios :

- **S1** : Vols à vue directe, à une distance maximale de 200 mètres du pilote.
- **S2** : Vols hors de la vue directe du pilote, jusqu'à une distance de 1 km.
- **S3** : Vols à proximité des personnes, à une distance de 100 mètres.
- **S4** : Vols hors de la vue directe dans des zones éloignées, sous conditions strictes.



Problématiques

Législation : réglementation

- Enregistrement du drone
 - Site Alphotango
 - Etiquette sur le drone (numéro enregistrement et exploitant UAS)
- Pour les professionnels
 - Certificat d'Aptitude Théorique de Télépilote (CATT)
 - Brevet théorique de pilote ULM
 - Assurances
 - Déclaration de son activité



Sommaire

1. A propos
2. Contexte
3. Attaques WiFi
4. Problématiques
5. Historique
6. Prototype
7. Travail restant

Historique

Octobre 2022

- U.S. Financial Services Company
- Deux drones :



DJI Phantom

WiFi Pineapple



15K \$



MATRICE 600

Raspberry Pi, batteries, GPD series mini laptop
4G modem, another Wifi-Device

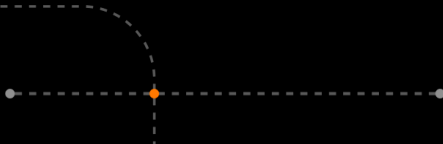
Sommaire

1. A propos
2. Contexte
3. Attaques WiFi
4. Problématiques
5. Historique
6. Prototype
7. Travail restant

Prototype

Choix du drone

- Drone facile à acheter
- Permettant de voler jusqu'à au moins quelques kms
- Permettant de porter une charge

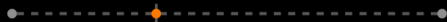


Prototype

DJI : Légalité

- DJI Fly Safe unlock

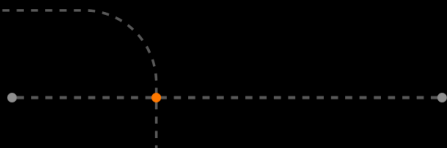
```
mount -o remount,rw /amt  
cd amt  
rm -r nfz  
exit
```



Prototype

DJI : Allumage à distance

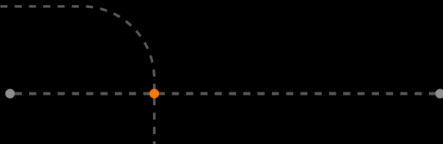
- Comment éteindre, puis redémarrer le drone ?
- Une solution « avancée » : souder des cables
- Mais sinon...



Prototype

DJI : Accrochage de charge utile

- Et si on regardait du côté des pêcheurs ?



Prototype

DJI : Accrochage de charge utile



€56.07

VAT included (where applicable), [plus shipping](#)

Drone Attachment Dropper/Delivery for DJI Phantom drones

TheStorkDesign

Add to cart

Item details

Highlights

 Made by **TheStorkDesign**

 Materials: plastic

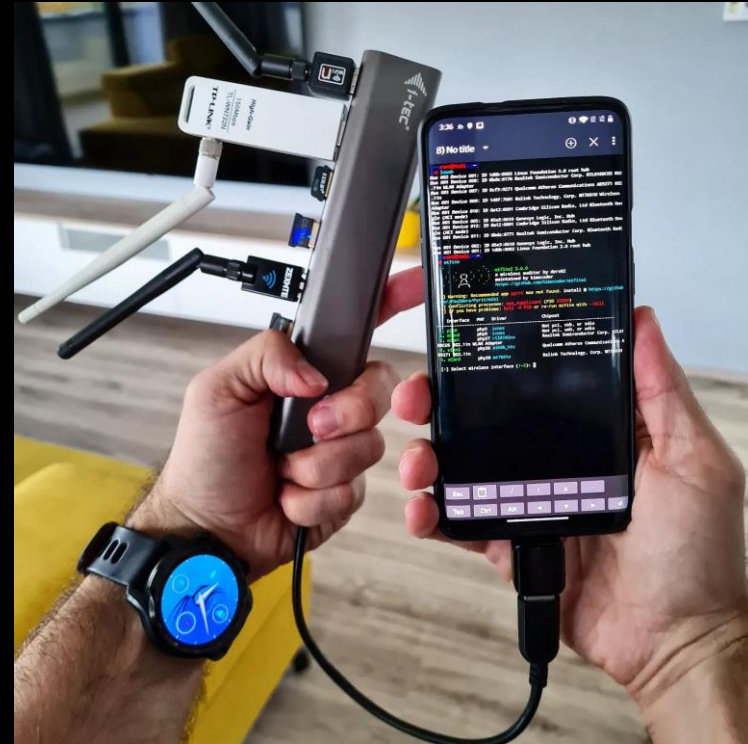
About this item

Here is our Stork Drone Drop Box it is an attachment for your DJI Phantom 4 Drones

Prototype

Charge utile

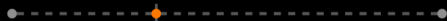
- Il nous faut :
 - Une antenne 4G
 - Une batterie
 - Une antenne WiFi
- Un téléphone ?



Prototype

Un téléphone ?

- Nécessite le monitor mode
- Utilisation d'une antenne WiFi externe ?
- Accès à distance ?
- Mais sinon...



Prototype

Un ananas ?

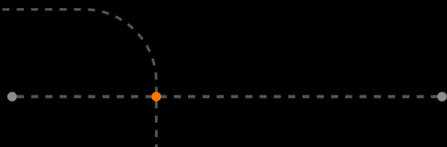


Sommaire

1. A propos
2. Contexte
3. Attaques WiFi
4. Problématiques
5. Historique
6. Prototype
7. Travail restant

Travail restant (Petite) liste

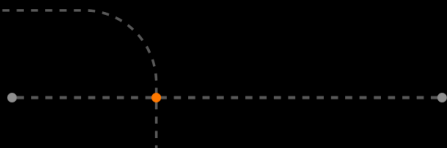
- Faire fonctionner le prototype !
- Ennuyer le nouveau juriste de l'équipe
- Partir en mission :)
- Améliorations :
 - Communication complète via 4G
 - Solution pour les clients en zone blanche
 - Cartographie 3D du signal WiFi



Travail restant

Recommendations

- Que recommander au client ?
- Radar ?
- Analyseur RF ?
- Brouilleur ?



Orange
Cyberdefense

Merci

[orangecyberdefense.com](https://orange.cyberdefense.com)

