

Rapport de projet long
Attaques sur un AR Drone 2.0 Parrot

Kevyn LEDIEU, Ferréol PENNEL, Alexis PERNOT

4 mars 2019

Table des matières

1	Introduction	2
2	Matériel et Méthode	3
	2.1 Matériel : AR DRONE 2.0	3
	2.2 Méthode	3
3	Hypothèse de travail	4
4	Présentation vulgarisée du travail	5
	4.1 Premiers pas avec le drone	5
	4.2 Prise de contrôle du drone	5
	4.3 Injection de commandes	5
	4.4 Virus sur le drone	5
	4.5 Conclusion	5
5	Présentation scientifique du travail	7
	5.1 Introduction	7
	5.2 Premier pas avec le drone	7
	5.3 Prise de contrôle du drone par désauthentification du client	8
	5.4 Injection de paquets	9
	5.5 Exploitation d'une connexion Telnet	9
6	Tutoriel	11
	6.1 Initialisation de l'application	11
	6.2 Menu principal	11
	6.3 Prise de contrôle du drone	12
	6.4 Injection de commandes	13
	6.5 Dépose de virus sur le drone	14
7	Sécurisation du drone	15
	7.1 Sécurisation via le Wifi	15
8	Conclusion	16

1 Introduction

De plus en plus présents autour de nous, les drones de loisirs représentent à la fois des opportunités technologiques et des risques de sécurité. Régulièrement, nous pouvons observer des exemples de drones ayant perturber le trafic aérien par leur présence aux abords d'un aéroport. Ainsi un premier risque de sécurité qu'ils représentent est leur intégration dans l'espace aérien, espace que ces nouveaux aéronefs partagent avec de nombreux autres de toutes les tailles. Aussi des nouvelles règles sont à l'étude afin de réglementer ces activités de loisirs. Toutefois, même une fois réglementée et contrôlée, l'activité des drones de loisir présente un second risque de sécurité lié non plus à la gestion du drone par l'opérateur mais au drone lui-même. En effet, dans la course à l'innovation dans ce domaine porteur qu'est le drone de loisir, les entreprises négligent potentiellement l'aspect sécurité hardware et logicielle de leurs drones. Aussi, ceux-ci peuvent présenter de nombreuses vulnérabilités permettant à un attaquant extérieur de potentiellement prendre le contrôle du drone. Dans ce contexte, nous avons décidé d'étudier un drone grand public proposé par un des leaders du marché, la société *Parrot*. Nous étudierons les différentes vulnérabilités potentiellement présentes sur ce drone et mettront en oeuvre un scénario d'attaque sous forme de tutoriel.

2 Matériel et Méthode

2.1 Matériel : AR Drone 2.0

Nous allons étudier un AR DRONE 2.0. C'est un hélicoptère quadrirotor pilotable via une liaison WiFi au travers d'une application disponible sous iOS, Android, Linux ou Windows. C'est un drone civil principalement destiné au divertissement. Il est équipé de :

- un *processeur ARM Cortex A8 32 bits cadencé à 1 GHz*
- *1 Go de RAM DDR2 cadencée à 200 MHz*
- un *système d'exploitation Linux 2.6.32*
- un *module WiFi b/g/n*
- un *accéléromètre 3 axes*
- un *gyroscope 3 axes*
- un *capteur de pression*
- un *magnétomètre 3 axes*
- des *capteurs de proximité à ultrasons*
- une *caméra vericale QVGA*
- un *port USB 2.0*

2.2 Méthode

3 Hypothèse de travail

Pour ce projet, nous supposons que le drone utilisé est un ARDrone 2.0 qui n'a pas subi de modifications logicielles et qui est donc dans un état identique à sa sortie d'usine. Il dispose ainsi uniquement des protections éventuelles prévues par le constructeur Parrot. Nous supposons dans le cadre de ce projet que nous sommes dans la position de l'attaquant et que l'ARDrone 2.0 est connecté et contrôlé par un client légitime.

4 Présentation vulgarisée du travail

4.1 Premiers pas avec le drone

Ce projet est centré sur la découverte de vulnérabilités sur l'ARDrone 2.0. Une première mise sous tension du drone nous a permis de découvrir que celui-ci propose un réseau Wifi ouvert, donc non protégé, permettant de se connecter à celui-ci et de le contrôler. Cette observation a grandement orienté notre travail. En effet, nous nous attendions à trouver un réseau Wifi sécurisé qu'il aurait été nécessaire de contourner ou de pénétrer afin d'avoir accès au drone. Cependant, le réseau ouvert nous permet en tant qu'attaquant de nous connecter directement au réseau Wifi créé par le drone. L'ARDrone 2.0 supporte la connexion de plusieurs clients simultanés à son réseau Wifi, toutefois seul le premier client à envoyer des paquets UDP de commande est maître du drone et a la possibilité de le contrôler. En supposant qu'un client légitime est connecté au drone, la question est : que peut faire l'attaquant ?

4.2 Prise de contrôle du drone

Une première idée est la prise de contrôle du drone par l'attaquant. Une fois connecté au réseau du drone, l'attaquant n'a qu'à déconnecter l'utilisateur légitime pour devenir le maître du drone. Ainsi en envoyant des messages au drone demandant la déconnexion du client légitime, l'attaquant est capable de reprendre le contrôle du drone une fois celui-ci déconnecté.

4.3 Injection de commandes

Dans ce cas, le client légitime reste maître du drone. Toutefois l'attaquant se fait passer pour le client légitime et envoie des messages au drone. Il peut ainsi lui envoyer des instructions que le client légitime n'a jamais envoyées. Par exemple, l'attaquant peut envoyer au drone l'instruction d'atterrir à la place du client légitime.

4.4 Virus sur le drone

Ce troisième point exploite une faille importante du drone. En effet, celui-ci offre à tout utilisateur connecté à son réseau Wifi la possibilité d'accéder directement au système d'exploitation du drone en ayant tous les droits sur celui-ci et sans authentification et protection. Ainsi, en tant qu'attaquant connecté au réseau Wifi du drone, nous utilisons cet accès au drone pour déposer sur celui-ci un script. Ce script est chargé de copier une image sur toute clé USB connectée au drone ceci afin de démontrer le potentiel de l'attaque. Il est en effet aisé de diffuser n'importe quel virus qui se diffuse par clé USB grâce au drone et ceci sans difficultés particulières.

4.5 Conclusion

Ces trois attaques différentes permettent de démontrer les vulnérabilités majeures que présente l'ARDrone 2.0. Une des failles principales de celui-ci est son réseau Wifi non protégé. La protection de celui-ci par du WPA2 permettrait de rendre ces trois différentes attaques beaucoup plus complexes car l'attaquant aurait dans un premier temps besoin de casser le réseau Wifi. De plus, le drone offre des accès non protégés et privilégiés qui

sont une faille majeure et permettent à un attaquant une prise de contrôle complète sur le drone.

5 Présentation scientifique du travail

5.1 Introduction

L'ARDrone 2.0 est un drone grand public Parrot dont nous allons présenter trois exploitations de failles de sécurité présentes au sein de celui-ci. Ces attaques seront présentées grâce à une application en Python appelée *Krok mou*. La première attaque sera la prise de contrôle du drone par désauthentification du client, la seconde sera l'injection de commandes sur le drone et la dernière sera l'exploitation d'une connexion Telnet sur le drone.

5.2 Premier pas avec le drone

Dans un premier temps, après avoir allumé le drone, nous avons étudié celui-ci. La première chose que nous notons est que le drone crée un point d'accès Wifi (Access Point) afin que le client puisse se connecter à celui-ci et le contrôler au travers d'une application dédiée sur des supports Android, iOS ou PC. Toutefois, ce Wifi est un réseau ouvert et non sécurisé. Ainsi, toute personne disposant d'un matériel doté d'une carte Wifi et à portée Wifi du drone peut se connecter à celui-ci sans authentification. Toutes les communications entre le drone et le client sont donc en clair et non sécurisées. Cette faille facilite grandement l'accès au drone à l'attaquant qui n'a ainsi pas besoin de faire face à un réseau Wifi sécurisé pour accéder au drone. Ayant découvert cet accès facilité au drone, nous nous connectons à celui-ci avec un Linux et lançons un scan avec *nmap* sur l'IP du drone

192.168.1.1

afin de connaître les ports ouverts sur le drone et découvrir des moyens d'accéder à celui-ci. Nous obtenons les résultats suivants :



FIGURE 1 – Résultat du scan *nmap* sur le drone

Nous observons un service **ftp** permettant de partager les vidéos filmées par le drone. Nous notons également un service **telnet** disponible sur le drone. Une rapide connexion à celui-ci, nous permet de voir que nous nous connectons sans identification au drone et, plus important, nous sommes **root** sur le drone! Nous avons donc déjà potentiellement un contrôle total du drone car nous avons un accès illimité au système d'exploitation du drone.

Dans le même temps, nous nous documentons sur l'ARDrone 2.0. Grâce au SDK disponible sur le site **Parrot**, nous sommes en mesure de comprendre comment forger des commandes pour les envoyer au drone ainsi que les règles de contrôle du drone. Ainsi, nous savons que plusieurs clients peuvent être connectés au drone en même temps mais que c'est le premier qui envoie des paquets de commande UDP au drone qui en devient le "maître" et peut le contrôler.

Après cette découverte du drone, nous établissons les trois scénarios d'attaques présentés en introduction que nous allons décrire par la suite.

5.3 Prise de contrôle du drone par désauthentification du client

La première attaque que nous allons présenter est une attaque permettant la prise de contrôle complète de l'ARDrone 2.0. Cette attaque se base sur la vulnérabilité principale du drone : il génère un point d'accès ouvert (sans mot de passe) et autorise 4 connections en simultané. Ainsi, il est possible pour l'attaquant de se connecter au drone dès qu'il est à porté du signal wifi. Il est alors possible ensuite de déconnecter les clients du wifi.

Détection des clients Une fois la connection faite, l'attaquant peut effectuer un rapide scan du réseau wifi avec l'outil **Nmap**, qui permet d'obtenir la liste des appareils connecter au réseau (adresses IP et MAC).



FIGURE 2 – Nmap du réseau wifi

Déconnection du wifi Une fois la liste établie, il est alors possible de désauthentifier les différents clients du drone. Mais avant cela, regardons de plus près cette attaque :

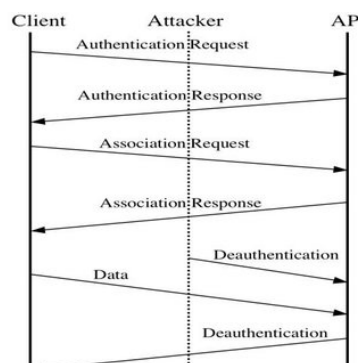


FIGURE 3 – Désauthentification d'un client wifi

Lors d'une connexion wifi de ce type, les messages liés à la désauthentification ne sont pas chiffrés, il est alors possible pour un attaquant de forger un paquet de désauthentification avec l'adresse de la victime et de l'envoyer au drone. Le drone recevant ce paquet considère donc que la connexion avec le client est donc close.



FIGURE 4 – Paquet de désauthentification

Pour cela, on utilise la suite d'outil bien connue sur Kali Linux, **Aircrack-ng** et plus particulièrement **Aireplay-ng** dans notre cas. **Aireplay-ng** va nous permettre d'envoyer ces paquets de désauthentification au drone. La commande est la suivante :

```
aireplay-ng -O 1 -e essid_drone -a @mac_drone -c @mac_client interface
```

Une fois les clients désauthentifier, nous nous reconnectons immédiatement au drone et sommes donc les premiers connectés au drone et les premiers à communiquer avec celui-ci donc "maître" du drone. Nous utilisons ensuite une application de contrôle via le navigateur web - disponible à l'adresse suivante : <https://github.com/functino/drone-browser> - afin de contrôler le drone avec le PC.

5.4 Injection de paquets

Cette seconde attaque a pour objectif d'injecter des commandes au drone sans en prendre le contrôle complètement.

5.5 Exploitation d'une connexion Telnet

La dernière attaque exploite une vulnérabilité du drone. Un service **Telnet** est ouvert et permet d'accéder à un shell **root** sur le drone.



FIGURE 5 – Accès **Telnet root** sur l'ARDrone 2.0

Ainsi une fois connecté au réseau du drone, n'importe qui peut utiliser cette connexion **Telnet** pour être administrateur sur le drone. Une fois le shell **root** obtenu, on se retrouve avec un accès au système d'exploitation du drone, qui est un **Linux**, et il est possible de faire ce que l'on veut. L'attaquant peut alors réaliser une large variété d'attaques directement sur le système d'exploitation. Il peut interagir avec les processus qui tournent sur celui-ci et notamment le processus qui pilote le drone **AJOUTER NOM PROCESSUS**.



FIGURE 6 – Processus s'exécutant sur l'ARDrone 2.0

Il est ainsi possible de modifier n'importe quel fichier du système d'exploitation et de réaliser par exemple un Déni de service sur le drone depuis "l'intérieur" de celui-ci. Etant **root** sur le drone sans nécessité d'escalade de privilèges, nous cherchons ce qui serait le plus intéressant de faire avec ce contrôle du drone. Nous décidons de démontrer la

possibilité d'implanter un virus sur le drone. Ainsi nous avons développé un script en bash qui sera envoyé sur le drone par l'application *Krokmou* accompagné d'un fichier au choix de l'attaquant. L'envoi se fait via la connexion **FTP** au drone. Une fois les deux fichiers sur le drone, l'application utilise la connexion **Telnet** afin d'exécuter le script. Celui-ci se copie alors au sein du dossier

`/bin`

du drone et s'ajoute à la liste des processus à lancer au démarrage du drone afin qu'il s'exécute en permanence sur le drone. Le script va alors régulièrement essayer de copier le fichier envoyé par l'attaquant avec le script sur une clé USB qui serait connectée au drone. L'utilisateur légitime peut utiliser une clé USB pour récupérer des vidéos filmées par le drone et enregistrées sur celle-ci. Par défaut et à des fins de démonstration, le script dépose sur les clés USBs connectées une image.



FIGURE 7 – Dépose du virus et du fichier par l'application

Cette attaque démontre que le drone peut facilement servir de vecteur d'attaque pour diffuser un virus par clé USB.

6 Tutoriel

Le tutoriel du projet se présente sous la forme d’une application Linux développée en Python permettant d’exploiter les trois types d’attaques présentées précédemment. Disponible à l’adresse suivante : <https://github.com/ferreolpennel/Krok mou>, cette application de démonstration est utilisable par tout utilisateur satisfaisant les pré-requis à son installation. L’application, appelée KROKMOU, est dédiée à l’ARDrone 2.0 et ne permet des attaques que contre ce type de drone et ce à des fins de démonstration uniquement. Elle permet ainsi de prendre le contrôle d’un drone à la place d’un utilisateur légitime déjà connecté au drone, d’envoyer des commandes pirates au drone sans déconnecter l’utilisateur légitime de celui-ci et de déposer un virus de démonstration sur le drone. Elle illustre ainsi les attaques présentées précédemment et met en relief les failles correspondantes sur ce type de drone.

6.1 Initialisation de l’application

L’application permet de sélectionner l’interface Wifi à utiliser pour se connecter au drone. Elle réalise ensuite un scan des réseaux Wifi alentours et affiche ensuite uniquement les réseaux Wifi de drone Parrot. Il suffit à l’attaquant de sélectionner le drone auquel il veut se connecter puis l’application configure l’interface Wifi pour se connecter au drone.

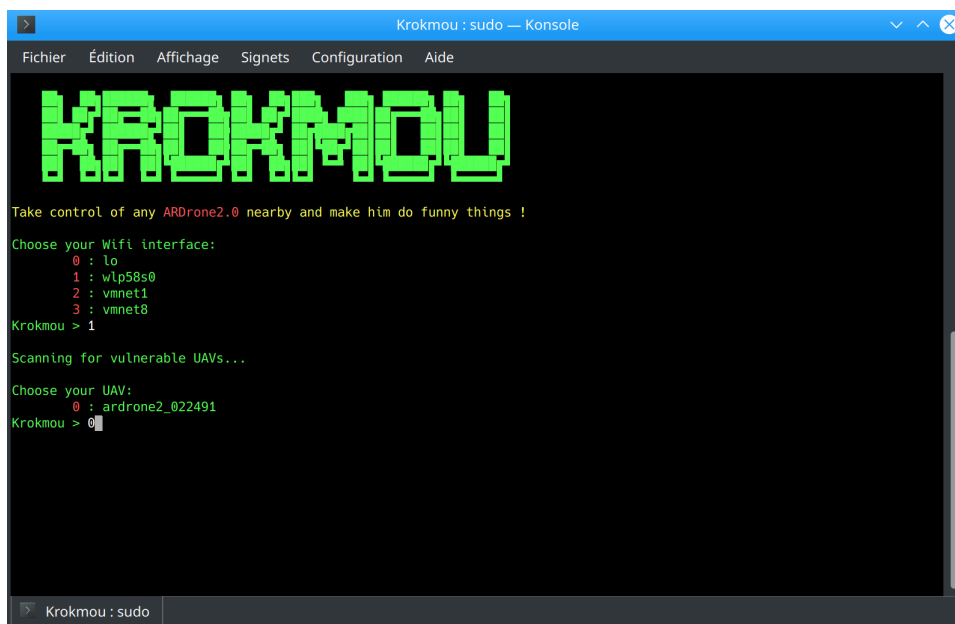


FIGURE 8 – Initialisation de l’application

6.2 Menu principal

Le menu principal de l’application permet de sélectionner une des trois attaques afin de la réaliser sur le drone auquel l’attaquant s’est connecté précédemment.



FIGURE 9 – Menu principal de l'application

6.3 Prise de contrôle du drone

Cette option du menu permet à l'attaquant de prendre le contrôle du drone à la place de l'utilisateur légitime grâce à l'attaque décrite précédemment dans ce rapport. Le contrôle du drone se réalise au travers du navigateur Web et d'un serveur **Node.js** issu d'un dépôt Github (<https://github.com/functino/drone-browser>).

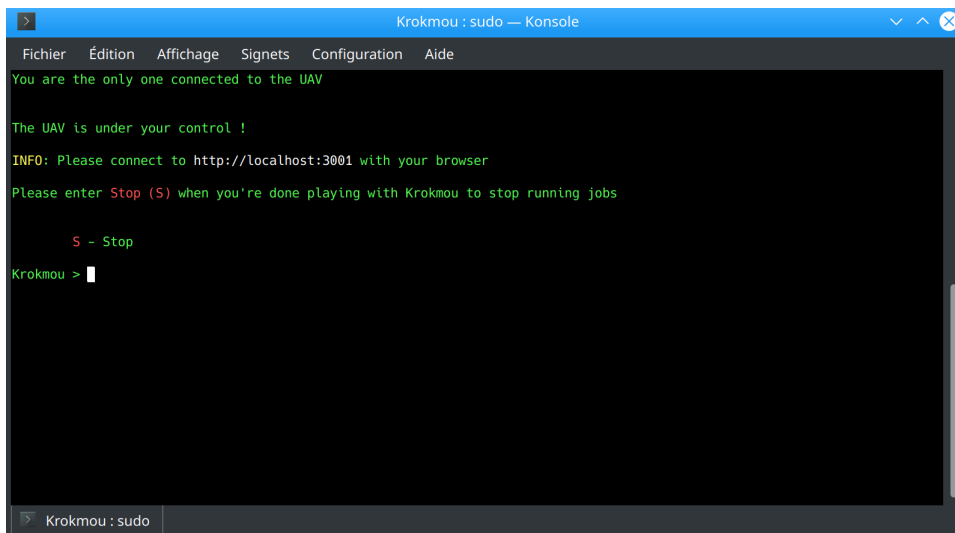


FIGURE 10 – Prise de contrôle du drone par l'application

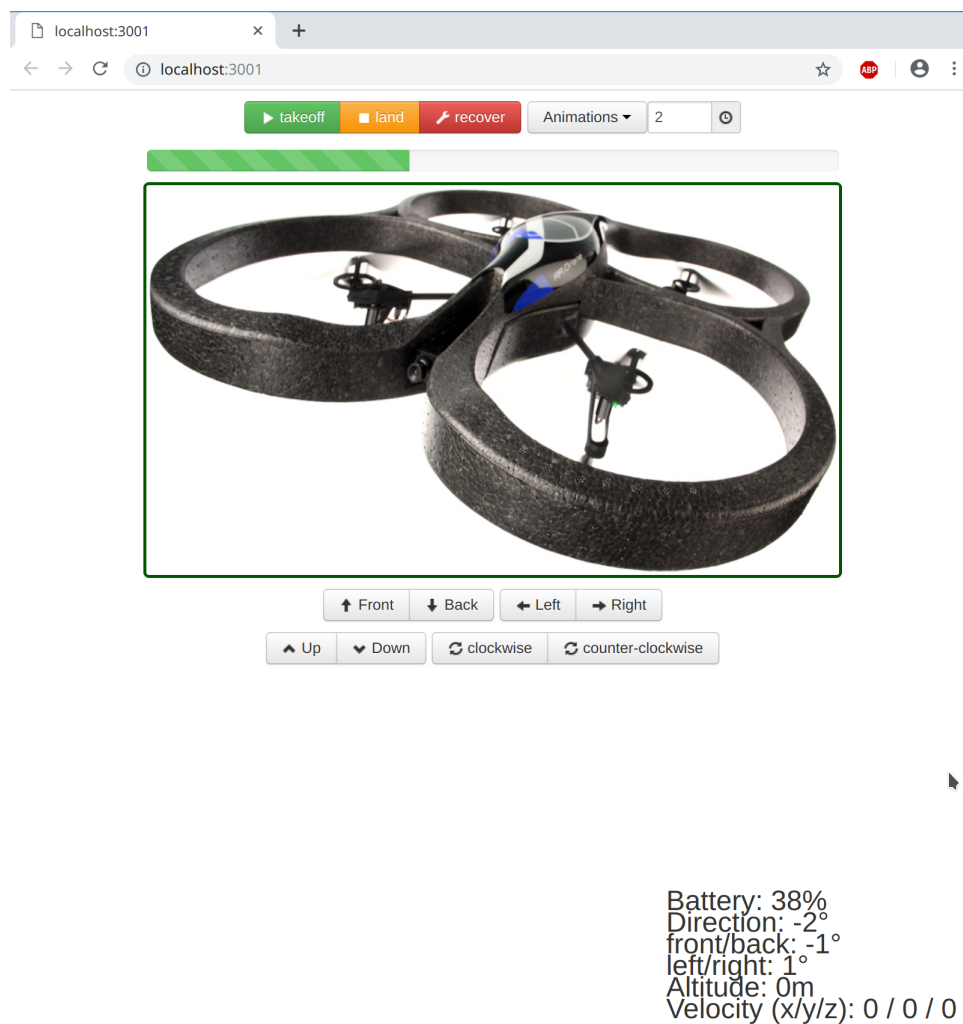


FIGURE 11 – Interface de contrôle web

6.4 Injection de commandes

Ce sous-menu permet à l'attaquant d'envoyer des instructions au drone sans déconnecter le client légitime de celui-ci à travers une injection de paquets.

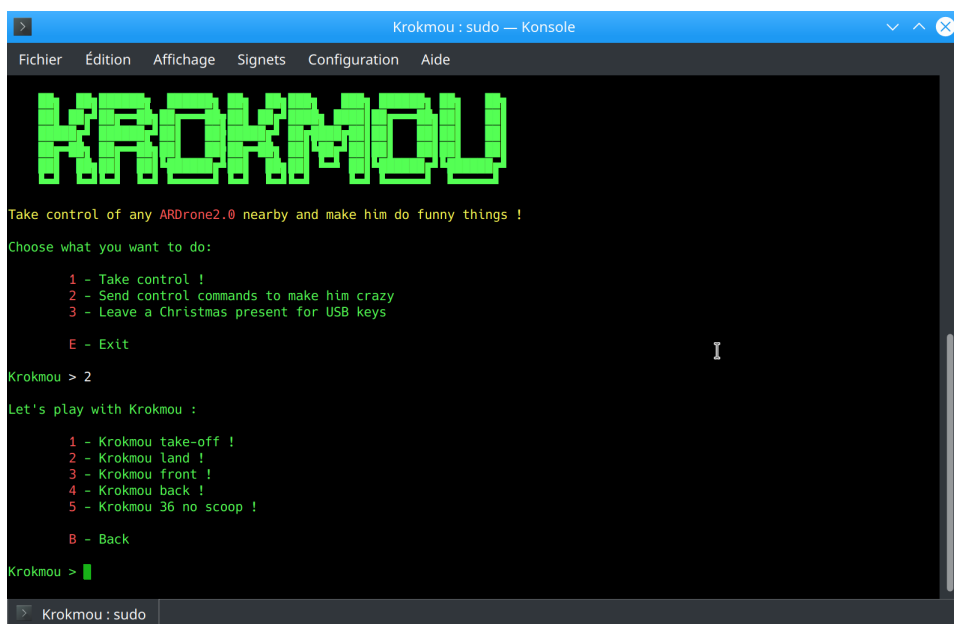


FIGURE 12 – Sous-menu d’injection de commandes

6.5 Dépense de virus sur le drone

Cette option permet d’exploiter une vulnérabilité laissant à l’attaquant un contrôle total du drone. Dans le cadre de la démonstration, l’application dépose un virus et un fichier sélectionné par l’utilisateur sur le drone. Ce fichier sera copié sur toute clé USB qui sera connectée au drone qui sera par conséquent considérée comme infectée. Par défaut, l’application dépose le virus et une image sur le drone. C’est cette image qui sera copiée sur toute clé USB connectée au drone toujours à des fins de démonstration. Cependant, l’attaquant peut indiquer le chemin d’un fichier de son choix au moment où l’application lui propose afin de remplacer cette image.

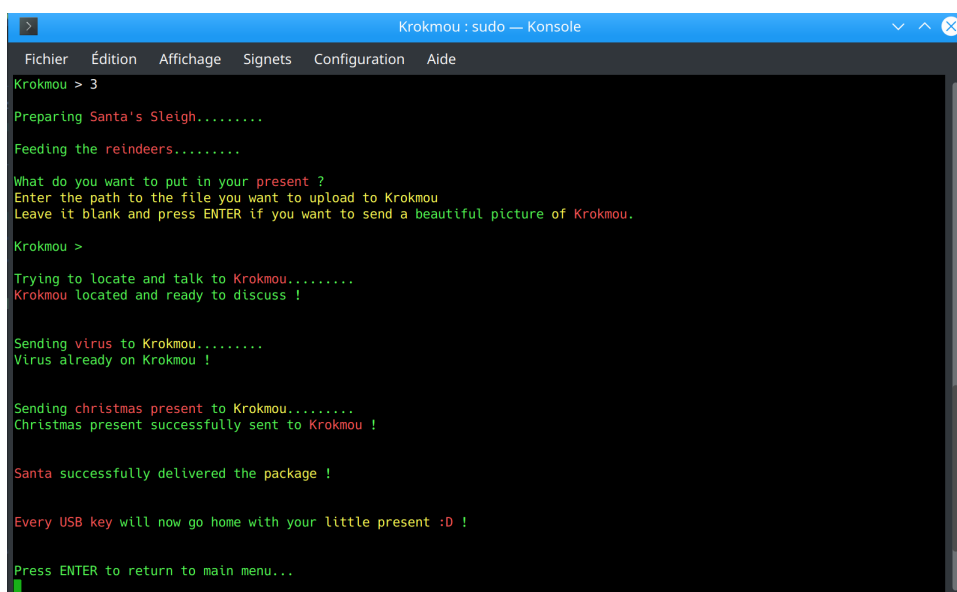


FIGURE 13 – Envoi du virus et du fichier sur le drone

7 Sécurisation du drone

Comme nous avons pu le voir, cet AR Drone 2.0 de Parrot rencontre de nombreux problèmes de sécurité et reste vulnérable à certaines attaques. L'une des vulnérabilités principales se trouve dans le point d'accès Wifi qui est un réseau ouvert donc accessible à toute personne se trouvant à portée du drone.

7.1 Sécurisation via le Wifi

Modification du point d'accès L'une des premières mesures pour ce drone serait donc une modification de ce point d'accès Wifi en y ajoutant un mot de passe afin de le rendre privée. Afin de minimiser les risques de compromission du réseau, l'utilisation de la norme WPA2 semble optimale. Après un rapide état de l'art sur internet, il semblerait que personne ne se soit réellement penché sur le problème mais un fichier bash présent sur le réseau, *nom du fichier*, laisse présager que cette modification est possible.

Utilisation du drone comme un client Une autre solution consisterait à utiliser le drone non comme un point d'accès mais comme un client du Wifi. Afin de pouvoir connecter le drone à un réseau en WPA2, il est nécessaire d'effectuer de la compilation croisée sur le module *wpa_supplicant*, qui gère les connections au wifi WPA2 sur les environnements Unix. En effet, le drone possède une architecture ARM et non x86. Heureusement, la communauté est riche de talent, et ce travail a déjà été fait dans ce dépôt Github : <https://github.com/daraosn/ardrone-wpa2>.

Cette manipulation se fait en plusieurs étapes :

- installation du module *wpa_supplicant* sur le drone.
- connecter le drone au point d'accès WPA2 du téléphone.
- faire en sorte que le drone est l'adresse 192.168.1.1. Changer l'adresse du point d'accès pour le permettre.
- contrôler le drone via le téléphone.

Avec ce procédé, on bénéficie alors d'une connexion sécurisée avec le drone que l'on pilote. Attention toutefois à bien choisir son mot de passe. En effet, si une personne arrive à se connecter au Wifi du téléphone, le drone redevient totalement vulnérable. La contrainte de cette technique est donc l'utilisation d'un point d'accès wifi annexe avec la bonne adresse ip pour le routeur. Dans un premier temps, nous l'avons essayé rapidement avec un iPhone comme point d'accès mais celui-ci n'offre pas un réseau interne du type *191.168.1.0/24* et il n'est pas possible de modifier cela dans les paramètres.

8 Conclusion