Primer Backdoor Que Afecta A Los Drones

La llegada de la **tecnología de los Drones** ha abierto un panorama en el uso y beneficio de algunas áreas. El uso de estos se ha diversificado, han sido usados para entregar Pizza, hasta el espionaje militar.

Recientemente, un investigador de seguridad informática ha encontrado un Backdoor en los **AR Drones Parrot**, fabricados por una empresa con sede en Francia, que podría **permitir a un hacker secuestrar remotamente el helicóptero radiocontrolado Quadcopter**.

El **Parrot AR Drone**, es un cuadricóptero que se puede controlar con el teléfono inteligente o tablet. Cuenta con dos cámaras incorporadas, es fácil de volar, y se puede controlar sin demasiado riesgo de que se estrelle contra los objetos.

Malware First Ever Que Afecta Drones

El investigador de seguridad, Rahul Sasi afirmó haber desarrollado el primer Malware para un Drone con **sistema ARM Linux**, apodado Maldrone [Malware para Drone].

El ***Maldrone*** se pueden utilizar para raptar Drones de forma remota, como se muestra en un vídeo de demostración publicado por el hacker.

> *«En este vídeo se muestra como se **infecta un Drone con Maldrone** y luego se espera una conexión tcp inversa desde el Drone. Una vez establecida la conexión, podemos interactuar con el software. Se puede observar como se activa el piloto*

> *automático, luego el backdoor elimina el piloto automático y toma el control. El Backdoor es persistente a través de reinicios «, explicó en un vídeo.*

Según el investigador, Maldrone puede interactuar con los controladores y sensores del dispositivo del Drone de forma silenciosa, y permite que el atacante pueda controlar de forma remota el dispositivo no tripulado.

Rahul dijo que el Maldrone también podría ser utilizado para atacar a otros fabricantes de Drones. Sin embargo, la puerta trasera podría ser explotado dentro de determinado rango inalámbrico.