No dejes que Evan se acerque a tu coche

Evan es la persona capaz de abrir cualquier coche y encender su motor sin necesidad de una llave

EvanConnect es el alias de un hacker que ha fabricado un inhibidor capaz de engañar a cualquier coche: **¿cómo lo hace?**

Reconoce la frecuencia a la que funcionan los coches de alta gama, para lograr abrirlos y acceder a ellos sin necesidad de una llave o un mando a distancia. A continuación, podemos ver en vídeo cómo actúa EvanConnect:

Como se aprecia en el vídeo, se acercan a un Jeep de color blanco y uno de los hombres intenta abrir la puerta del vehículo. Acto seguido, acciona el inhibidor e instantáneamente el automóvil se abrió. El individuo se monta en el vehículo y es capaz de encenderlo y acceder a diferentes ajustes y configuraciones.

Para demostrar la potencia y el alcance del dispositivo, el hombre apagó el mismo y trató de encender el vehículo: «Llavero no detectado».

A continuación, EvanConnect encendió de nuevo el dispositivo y volvió a intentarlo y, sorprendentemente, el vehículo encendió.

Puente entre el cibercrimen y el físico

EvanConnect representa esa unión entre ciberdelincuente y delincuente tradicional. Vende estos dispositivos por miles de dólares y afirma haber tenido clientes en Estados Unidos, Reino Unido, Australia y diversos países sudamericanos y europeos.

El vídeo no representa un robo real. Evan hizo el vídeo utilizando el Jeep de un amigo para demostrar el potencial de los dispositivos.

Es muy fácil de hacer, pero tal como lo veo: ¿por qué me ensuciaría las manos si puedo ganar dinero simplemente vendiendo las herramientas a otras personas» (EvanConnect para Motherboard)

La amenaza del robo digital de un coche es real

Ya en **2017**, el servicio de policía de **West Midlands** en Reino Unido mostró a dos hombres acercarse a un Mercedes estacionado en la casa del propietario.

Uno de ellos se situó al lado del vehículo con un dispositivo similar al de Evan, mientras que utilizó otro dispositivo más grande cerca de la casa, con la esperanza de captar la señal emitida por las llaves del coche almacenadas en el interior.

La policía de **Tampa** (Florida) afirmó el pasado año 2019 que estaban investigando un robo de un automóvil en el que el propietario lo bloqueó y pudo haber sido debido a un robo similar a este, a través de una interferencia electrónica.

Según Evan, los vehículos que funcionen con frecuencias entre los **22.000** y los **40.000 hertzios** son susceptibles de ser hackeados por esta clase de dispositivos.

Esta es una de las tendencias que, desde Dolbuck Ciberseguridad, hemos identificado para este 2020.