

Un experto en seguridad hackea el coche de un amigo

✖ Ken Munro, un experto de seguridad de la empresa PenTestParners, ha conseguido hackear un Mitsubishi Outlander híbrido de última generación a través de WiFi, accediendo así a las funciones remotas del coche como apagar la alarma.

Ken Munro, uno de los especialistas de la empresa de seguridad informática **PenTestPartners** (“Penetration testing and security services”), estaba esperando dentro de su coche a que salieran los niños del colegio. Durante la espera se puso a jugar con su teléfono móvil como haría cualquier padre de hoy en día. Mientras buscaba un punto WiFi al que conectarse, se percató de un nombre de red curioso. Al parecer el coche de algún otro padre estaba equipado con red WiFi, como hacen algunos modelos nuevos.

En este caso la red pertenecía al coche de un padre amigo suyo. Se acercó a hablar con él y éste le enseñó el flagrante SUV que se acababa de comprar, un **Mitsubishi Outlander** enchufable. Ken le preguntó por la WiFi y el padre le explicó que servía para que desde una aplicación móvil pudiera controlar diversas funciones del coche como las luces, las puertas e incluso... la alarma! A Ken se le iluminaron los ojos, tenía que probar eso.

Comprar para probar

Ken sospechó de la seguridad del sistema y decidió que sería bueno realizar un test. Y para ello se dirigió a un concesionario y compró el mismo coche que su amigo. Sin duda la prueba le salió cara pero después de 4 días en la empresa consiguieron hackear completamente el sistema de control del

coche, accediendo a las funciones proporcionadas por el fabricante, entre las que como ya hemos comentado está desactivar la alarma.

El fallo de seguridad reside en el hecho de que los comandos son enviados directamente al coche sin pasar por un servidor de Internet, lo que nos ahorra consumo de datos a cambio eso sí de rebajar enormemente la seguridad.

Después de un informe y una demo a la empresa, Mitsubishi aconsejó a todos los propietarios del coche desactivar este servicio hasta que encuentren una solución.

Riesgo global

Más allá de lo gracioso de la noticia, la realidad es que el incremento en la conectividad de muchos elementos que utilizamos a diario está empezando a poner en riesgo nuestra seguridad.

Muchos expertos están avisando ya que la transición a la

“Internet de las cosas” (**IoT** en sus siglas en inglés) o lo que es lo mismo, una infraestructura de Internet donde no sólo estemos conectados nosotros sino multitud de dispositivos inteligentes, puede traernos problemas si no se lleva a cabo correctamente. Para ello reclaman por ejemplo que las comunicaciones sean siempre encriptadas, hecho que parece ser no se está cumpliendo siempre.

Quién sabe si de aquí unos años estaremos anunciado esta misma noticia con la nevera de alguien.

fuentes: pcactual.

