MOTOR

Así podrían los hackers hacerse con el control de infraestructuras clave

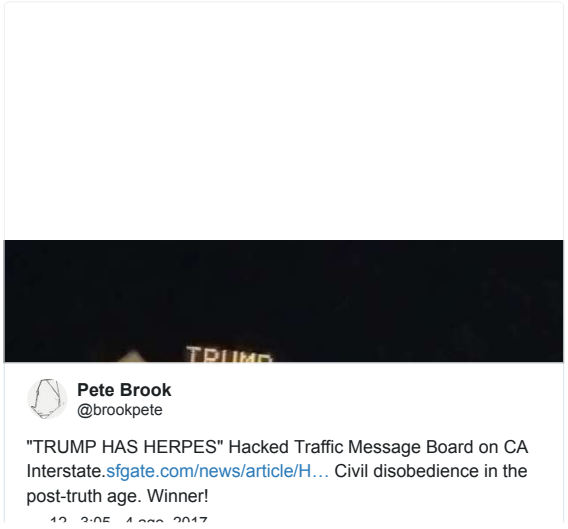
Vicente Cano 23 Feb 2018 11:51h. - Actualizado: 9 Ago 2018

El punto neurálgico de las ciudades son sus redes de transporte, cada vez más automatizadas e interconectadas. Pixabay.

- **Las redes de transporte inteligente sufren el riesgo de ser secuestradas por piratas informáticos.**
- **Cuando aparezcan los coches autónomos, las consecuencias de algo así serán potencialmente catastróficas para una ciudad.**
- **"Que un modelo de coche sea totalmente nuevo no es bueno", afirma un experto en seguridad informática.**

Si se teclea en un buscador "***hackeo* de transportes", aparecen docenas de gamberradas. Aunque todavía no se ha llegado catástrofes** como el secuestro de ciudades, los expertos en ciberseguridad alertan que podrá pasar en el futuro. Tales advertencias no parecen descabelladas si se atiende al nivel de alguno de estos ataques.

Desde un cartel de tráfico con la frase "Trump tiene herpes" o "Hoy no se trabaja. Vuelvan a casa" a emitir vídeos pornográficos en los paneles de la red de metro de Moscú empieza a haber un trecho. Seguro que eso mismo es lo que pensará ahora quien hizo lo propio en una pantalla pública de Yakarta, y a quien le pueden llegar a caer hasta 12 años de prisión tras ser identificado y arrestado por ello en 2016.



En Indonesia, las leyes tienen menos sentido del humor todavía con la exposición de contenido para adultos que con el ***hackeo* de las redes de transporte**. Sin embargo, en Europa, los **ciberataques a infraestructuras inteligentes** tienen una impunidad mucho mayor. Hablamos de los casos más preocupantes con David Sancho, analista senior de Trend Micro, una empresa especializada en el análisis de riesgos cibernéticos.

Sancho relata para *Business Insider* algunos casos y, sobre todo, analiza el trabajo de sus compañeros Numaan Huq, Rainer Vosseler y Morton Swimmer, que acaban de publicar un trabajo en el que caracterizan hasta el 53,8% de las ***ciberamenazas* al transporte inteligente** como de muy graves. "Se han dado ya multitud de casos del tipo de cambiar el mensaje en los paneles informativos de una estación con contenidos que pueden parecer hasta graciosos. Sin embargo, una vez que un *hacker* está dentro de una red de transporte, también puede cambiar las agujas de los trenes, los semáforos de un cruce o **impedir el cobro en una autopista**", afirma.

"Pero lo peor está por llegar, porque **cuando haya coches 100% automatizados, los piratas informáticos podrán hacerse con su control** y, entonces, tendrán el potencial de poder bloquear una carretera por completo", prosigue Sancho. Por suerte, según este analista de riesgos informáticos, los conductores no tienen tantos motivos para estar preocupados por su seguridad como los gestores de las infraestructuras inteligentes.

"Ya se puede operar un coche pirateado a distancia y, por ejemplo, accionar su sistema de frenos pero, ¿con qué objetivo? Algo así no tiene sentido de cara a un móvil económico", puntualiza. Sin embargo, prosigue: "El potencial de riesgo es brutal porque se puede llegar a ***hackear* por completo toda una red de transporte**, que hoy esté muy automatizada y, con ella, llegar a bloquear una ciudad entera. Wannacry ya proyectó imágenes pidiendo un rescate en algunos paneles, pero esto fue solo un pequeño ejemplo de lo que puede llegar a pasar".

Salih SARIKAYA
@SalihSarikaya

Someone hacked San Francisco's transport systems digitalreview.co/someone-hacked… @DigitalReview_ aracılığıyla

5 17:00 - 28 nov. 2016

Ver los otros Tweets de Salih SARIKAYA

Entre los **ataques a infraestructuras de transporte** más destacables de los últimos años, los más habituales son los que se perpetran contra el servicio de pago o expedición de billetes. Estos van desde la creación de tarjetas falsas para redes de metro como la Oyster Card de Londres —los *hackers* llegaron a publicar en internet un pdf con las instrucciones detalladas para que cualquiera pudiera hacerlo— a mafias organizadas que venden a terceros esta clase de *salvoconductos viarios*.

El "Trump es tonto" **que pudo leerse en otros carteles de autopistas de EE.UU.** es casi anecdótico si se compara con el daño que algo como lo anterior puede ocasionar a una conurbación como Londres y su área circundante. En Dinamarca, por ejemplo, **toda la red de transporte público ha permanecido pirateada por una mafia durante mucho tiempo.**

Y allí no solo se han dejado los códigos de pirateo disponibles online, también hay **tutoriales en youtube sobre cómo *crackear* la OV-Chipkaart danesa**. Así, no es de extrañar que, en más de una ocasión, se haya encontrado a chicos de relativamente corta edad utilizando tarjetas de transporte pirateadas.

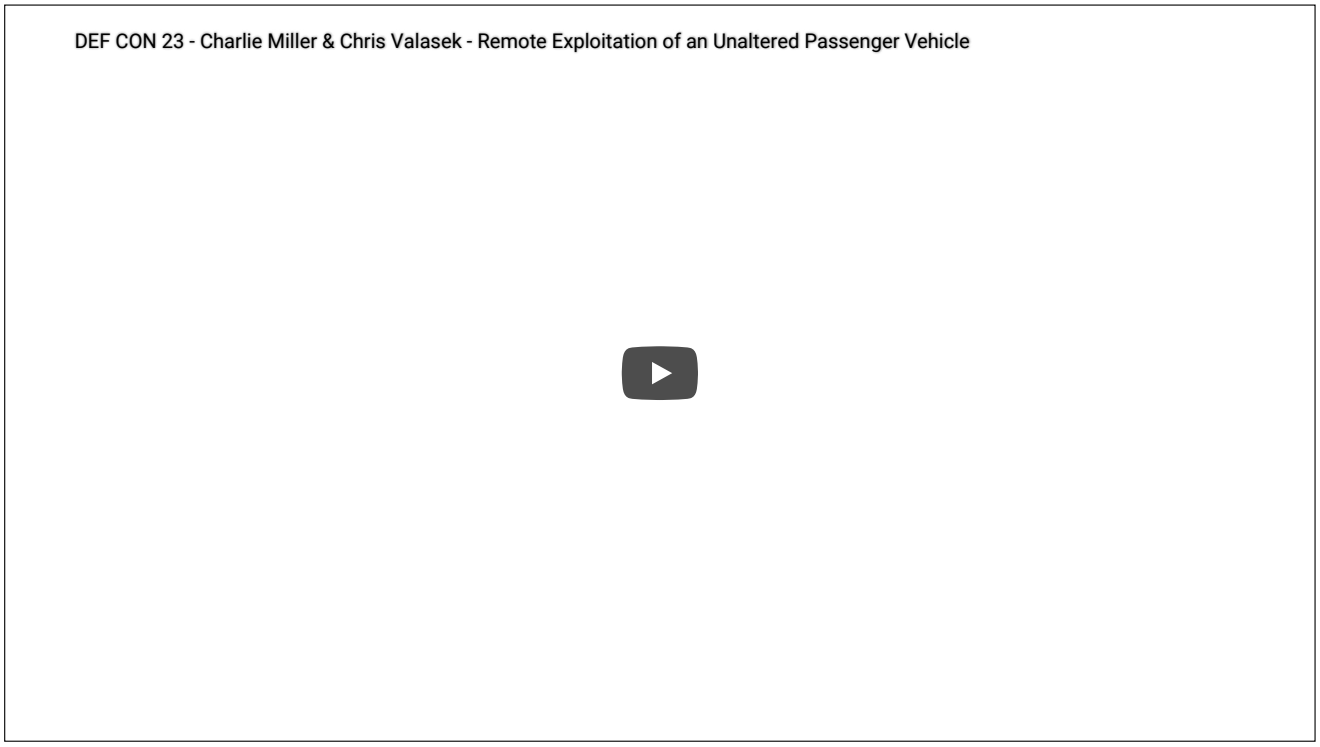
El *hackeo* de coches, cosas de niños

"Ya se han dado numerosos casos de coches que los investigadores han conseguido **detener por completo desde un ordenador**. Pero estos fallos de seguridad, una vez se detectan, se reportan y son *parcheados* rápidamente por los fabricantes", afirma Sancho.

"En sí mismos, los **coches cada vez más automatizados siempre van a entrañar más posibilidades de *hackeo***. De hecho, para nosotros, que cualquier equipo lleve un nuevo sistema operativo siempre es peor en términos de riesgo de seguridad. Pero además siguen apareciendo vulnerabilidades en vehículos y sistemas más antiguos y probados, como sucedió hace poco con Windows", prosigue.

"En términos de riesgo, lo más preocupantes para nosotros, además del coche autónomo, es la tendencia de la industria a que los **automóviles estén entre sí conectados por wifi**. Esto es bastante sencillo de piratear: con un equipo no profesional ya se puede conseguir desconectar todo el

Lo último que se ha dado a conocer respecto a las **redes de transporte inteligente es lo sencillo que puede ser piratear** los postes de recarga de coches eléctricos. Con solo un ordenador portátil, un lector de tarjetas y un señuelo similar al que usan los clonadores de tarjetas de crédito se puede hacer una copia del *chip* de carga y enchufar cualquier coche eléctrico a un poste público y cargarlo a costa de otro usuario. Esto también es posible incluso sin un ordenador, con un simple smartphone Android.



En 2016, Charlie Miller y Chris Valasek lograron hacerse detener por completo un coche desde un ordenador portátil. En 2015, los ***hackers*** **se cebaron con la red de servicios de conectividad** OnStar en EE.UU., que en Europa usan los coches de Opel/Vauxhall, y lograron interceptar la comunicación con los vehículos y robarles datos. A veces, el ciberataque se hace para practicar un robo industrial, como le pasó a Renault en 2017, que tuvo que parar la actividad en tres de sus plantas.

El mundo necesita los ITS –***Intelligent Transportation Systems***— para dar cabida a una población creciente y cada vez más urbana y móvil, pero estos entrañarán mayores riesgos. Por ahora, los peores casos son los descritos arriba, cuando el sistema de transporte de San Francisco fue afectado por un *ransomware*, sirenas de emergencia activadas *en masa o* hasta lavaderos de coches automáticos conectados secuestrados para atacar a los vehículos y sus ocupantes. Sin embargo, el ciberterrorismo de las redes de transporte puede ser el siguiente paso.