
RISCO
AUTO
CHECK
CAR
HACKING
Julio 2016

CONTENIDO

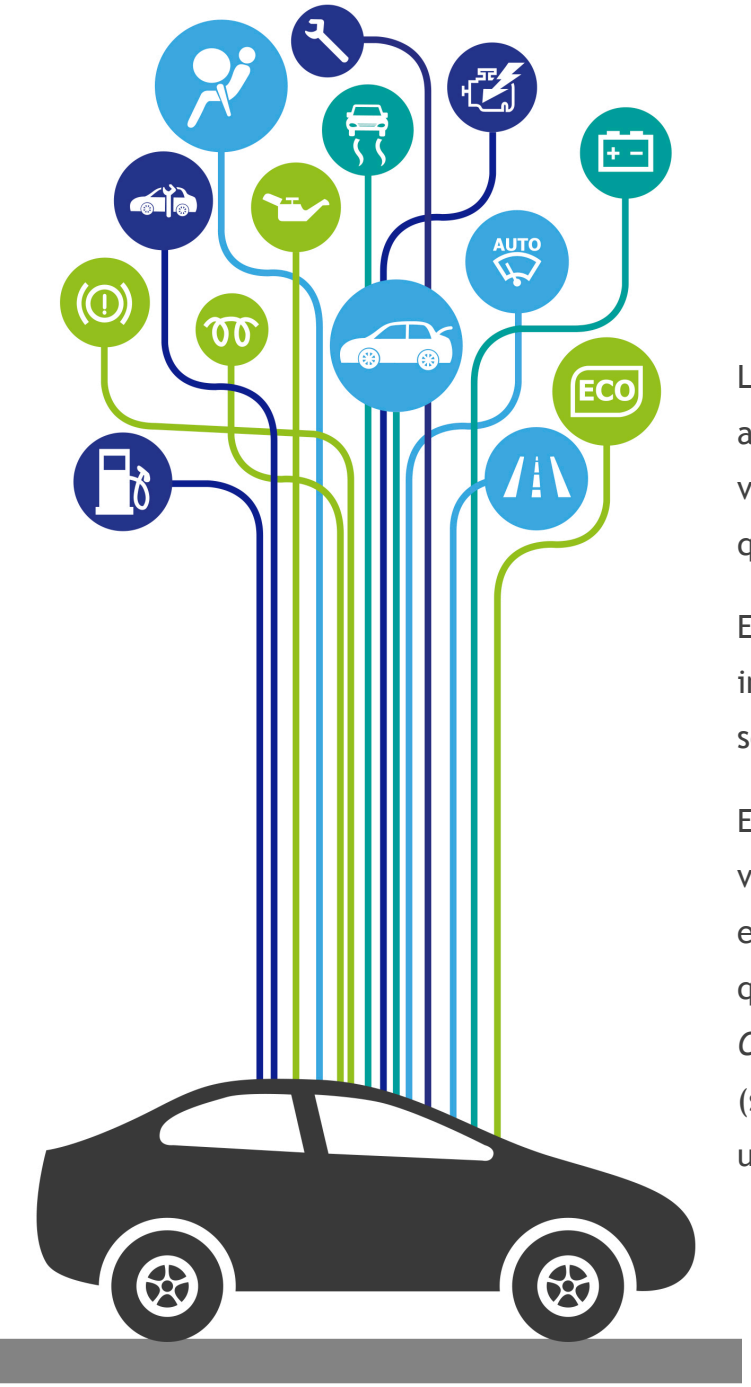
RESUMEN EJECUTIVO

Hoy día los autos son computadores sobre ruedas y están más computarizados que nunca antes. Sistemas de entretenimiento y navegación, Wi-Fi, actualizaciones automáticas de software, *Bluetooth*, compartir aplicaciones con teléfonos inteligentes, son algunas de las convenientes funciones que hacen más agradable la experiencia de conducir.

Toda esta funcionalidad ha permitido a *Hackers*, de manera inalámbrica, tomar control de las funciones del vehículo, desde el sistema de entretenimiento hasta inhibir los frenos y poder apagar el auto en marcha.

Los autos modernos tienen en promedio setenta (70) pequeños computadores para comunicarse y compartir información sobre la operación del auto entre sí, por medio su red interna (CAN – Bus *Controller Area Network System*). En caso de que no esté al tanto, un vehículo puede contener 100 millones de líneas de código de programación, en comparación con un Boeing 787 Dreamliner que tiene solo unos 6.5 millones.

Los riesgos de utilizar un auto moderno van desde que remotamente *Hackers* tomen control del mismo, inhiban los frenos, obtengan información personal almacenada en el auto, accedan a desplazamientos realizados por el auto, lo localicen o lo roben.



RESUMEN EJECUTIVO

La industria automotriz desde el año 2014 ha empezado a tomar muy seriamente la amenaza del *Car Hacking*. Aunado a lo anterior, los dueños de los autos, para no ser una víctima, deben adoptar prácticas de seguridad de información no muy diferentes a las que utilizan con su computador o teléfono inteligente.

En un Sondeo realizado en Panamá por RISCCO sobre *Car Hacking*, los participantes indicaron que es muy probable (29%) y probable (44%) que autos del año 2012 o después, sean vulnerables a *Hackers*.

El ciberataque a vehículos no es ciencia ficción. No pasará mucho tiempo para que las víctimas de un *Car Hacking,* narren su historia en los medios de comunicación. Tampoco es descabellado pensar que las primas de seguro de autos aumenten. De la misma forma que el "Hackeo" a las bases de datos de las organizaciones es parte del diario vivir, el *Car Hacking* aumentará. De los 64,737 autos nuevos vendidos en Panamá en el año 2015 (según la Contraloría General) son verdaderas computadoras sobre ruedas que, quizás usted este manejando sin saberlo.

INTRODUCCIÓN

El 24 de julio de 2015 el fabricante de autos Chrysler, tuvo que solicitar a los dueños de 1.4 millones de autos tipo Jeep, que bajaran de su página web una actualización del software de la computadora del tablero de instrumentos del auto, y que la instalaran es sus vehículos por medio del puerto USB que tiene el auto. Esto ocurrió semanas después que los investigadores Charlie Miller y Chris Valasek demostraron que de manera inalámbrica pudieron tomar control de las funciones del vehículo, desde el sistema de entretenimiento, hasta inhibir los frenos y poder apagar el auto en marcha. Ver https://www.youtube.com/watch?v=MK0SrxBC1xs

Hoy día los autos están más computarizados que nunca. Sistemas de entretenimiento y navegación, Wi-Fi, actualizaciones automáticas de software, *Bluetooth*, compartir aplicaciones con teléfonos inteligentes, son algunas de las convenientes funciones que hacen más agradable la experiencia de conducir.

Probablemente no lo sepa, pero un auto moderno puede tener en promedio setenta (70) pequeños computadores para comunicarse, compartir información entre sí y tomar decisiones, como por ejemplo, informar al tablero de control que las llantas están bajas. Esto ocurre gracias a millones de líneas de código de programación (LCP). Para que usted tenga una idea, según el DOT (Department of Transportation, USA) un auto de lujo puede contener 100 millones de LCP, en comparación con un Boeing 787 Dreamliner que tiene unos 6.5 millones de LCP o un avión F-22 que tiene cerca de 1.7 millones de LCP.

Es precisamente tantas líneas de programación dispersas en pequeños computadores, de diferentes proveedores, ensamblados en un auto, lo que los ha hecho vulnerables a los *Hackers*. Lo anterior reviste tal seriedad que, en USA, Senadores han propuesto leyes para que los fabricantes mejoren la ciberseguridad de los autos y también, que aquellos que hagan *Hacking* a un auto, sean condenados a cadena perpetua. Es importante comprender los riesgos a los que estamos expuestos.

COMPUTADORES SOBRE RUEDAS Y SUS RIESGOS

¿Cómo un *Hacker* puede controlar un auto?

Pueden existir fallas de seguridad entre los millones de líneas de códigos de programación, así como en las funciones de comunicación inalámbrica del auto con dispositivos como teléfonos inteligentes o *Tablets*, conectados al auto vía el puerto USB, *Bluetooth* o Wi-Fi. También es posible a través de dispositivos que se conectan al puerto de diagnóstico del auto (OBD-II *port*). A través de tales puntos de "acceso", un *Hacker* podría aprovecharse de vulnerabilidades y acceder a través de la red interna (CAN Bus) a las pequeñas computadoras (ECU - engine control units) que tiene los autos, principalmente a partir del año 2012.

RIESGOS

Con base en el artículo *"Connected cars: the open road for hackers"* de la Consultora FireEye de 2016, los riesgos pueden ser:

1. Obtener accedo físico no autorizado al vehículo, debido a que muchos autos han optado por reemplazar los sistemas de encendido físico (llave), con sistemas "sin llave" que utilizan "apps" desde un teléfono inteligente o llaves inalámbricas.

2. Robo de información del vehículo y personal del dueño, almacenada en el auto, tal como: Lista de contactos, cuando el vehículo se enciende y apaga, trayectorias y localización del auto; número de cédula, correo del propietario, celular, dirección, etc.

3. Manipular deliberadamente la operación de un vehículo de forma no autorizada, es decir, un *Hacker* podría remotamente y sin autorización, inhabilitar los frenos, apagar el auto, encender los limpia parabrisas, etc.

4. Utilizar las ECU's para soportar maliciosas actividades cibernéticas. En sentido práctico, los autos modernos son redes de computadoras conectadas a la Internet, desde la cual, se pueden lanzar ataques cibernéticos a organizaciones públicas o privadas.

5. Ser extorsionado por la implantación de un Ransomware en el auto. De la misma forma que hoy día los *Hackers* solicitan dinero para que usuarios infectados puedan recuperar el acceso a sus documentos de su computador (Ransomware), no sería descabellado pensar que le secuestren o bloqueen el encendido de su auto y tenga que pagar un rescate para que lo pueda utilizar.

¿Qué piensa el panameño sobre *Car Hacking*?

Entre el 19 y 24 de julio de 2016, RISCCO realizó en Panamá un Sondeo para obtener la opinión sobre qué piensan los panameños de ***Car Hacking***. Las respuestas de los **212 participantes** reflejan que sí se percibe que un auto es vulnerable a un ciberataque. A continuación los resultados.

	Muy Probable	Algo Probable	Poco Probable	Improbable
1. ¿Qué tan probable considera usted que un auto comprado en el año 2012 o después, sea remotamente vulnerable a un ciberataque e impida a su dueño encenderlo, utilizar la radio o que los frenos le funcionen?	29%	44%	24%	3%
2. ¿Qué pensaría si durante la compra de su nuevo auto, el vendedor le diga que también incluye programas de anti virus y software para impedir que usted sea víctima de un "*Car Hacking*"?	26%	36%	32%	7%

	1	2 - 10	11 - 20	21 - 30	Más de 30
3. Para autos comprados en el año 2012 o después existen pequeñas computadoras que gobiernan gran parte de su funcionamiento. ¿cuántas pequeñas computadoras internas considera que un auto en promedio tiene?	29%	48%	14%	3%	6%

Es claro que los participantes comprenden que los autos modernos son vulnerables a ciberataques. Considerando que el 77% de los participantes piensa que los autos modernos tienen diez o menos ECU´s, lo cierto es que en promedio tienen 70 ECU´s. Además, existen protocolos de comunicación como V2V (vehicle-to-vehicle communications) y V2I (vehicle-to-infrastructure) que facilitan la conducción al intercambiar información con otros autos, señales de tráfico y semáforos, entre otros.

Por lo anterior, es recomendable, que los usuarios de autos modernos, adopten ciertos consejos y buenas prácticas de seguridad de información con su vehículo.

Consejos para reducir un ciberataque en autos

1. Modifique cualquiera contraseña que el vehículo traiga de fábrica. Estas pueden ser del *Bluetooth*, Wi-Fi y la de la configuración de la funcionalidad del auto, entre otras. Cada cierto tiempo es sano modificar las contraseñas y ser cuidadoso al compartirlas.
2. Mantenga el software de su auto actualizado. Si el fabricante anuncia una actualización, tómese el tiempo para verificar su autenticidad y obténgala de un sitio certificado. Al instalarlo en su auto utilice USB u otros medios de almacenamiento de su confianza.
3. Sea cauteloso en la instalación de aplicaciones de software en su auto y/o aquellas que desde su teléfono inteligente o *Tablet* pueden comunicarse de forma inalámbrica con su auto.
4. Sea más receloso sobre quién tiene acceso físico a su auto. Por medio del puerto USB o el puerto de diagnóstico del auto (OBD-II *port*), se podría instalar un código malicioso que posteriormente permitiría a un atacante, remotamente tomar control del auto o simplemente robarlo.

Los fabricantes y proveedores de partes electrónicas de autos, están tomando en serio la ciberseguridad. Recientemente la compañía HARMAN, una de las más grandes en proveer sistemas de entretenimiento y funcionalidad a la industria de autos, adquirió a la compañía TowerSec, cuya casa matriz está en Israel y que se especializa en software de seguridad para autos.

Es solo cuestión de tiempo, para que los medios informen sobre el incremento de ciberataques a vehículos, tal cual ocurre con las redes de computadoras de organizaciones privadas y gubernamentales. Tenga presente que según la "Organisation Internationale des Constructeurs d'Automobiles (OICA)", de 2012 a 2015 se fabricaron cerca de 352 millones de autos y quizás, uno de esos, lo esté manejando usted.

***Fuentes utilizadas:**

Fire Eye – junio 2016, Connected cars: the open road for hackers
FBI - Motor vehicles increasingly vulnerable to remote exploits https://www.ic3.gov/media/2016/160317.aspx
Robert N. Charette, "This Car Runs on Code," IEEE Spectrum, February 1, 2009, http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

CONTACTOS

Antonio Ayala I.
t: 279-1410 Ext. 104
aayala@riscco.com

Raúl Lezcano
t: 279-1410 Ext. 108
rlezcano@riscco.com

riscco.com

Es una compañía panameña, independiente y dedicada, de manera exclusiva, a la consultoría en riesgo tecnológico, seguridad de información y auditoría interna, compuesta por profesionales con el conocimiento y credibilidad necesaria para traducir aspectos muy técnicos a un lenguaje simple y con sentido de negocio. Con (7) siete años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías privadas e Instituciones del Estado Panameño, líderes en su ramo.

Desarrollo Gráfico Bellator Creative SAS
bellatorgallery.com – info@bellatorgallery.com