Seguridad del coche conectado – un enfoque holístico y proactivo

PABLO MONTOLIU ZUNZUNEGUI

Chief Information & Innovation Officer. AON España

A PESAR DE LA VASTA Y CAMBIANTE SUPERFICIE DE ATAQUE, CON UN ADECUADO "CIBERGOBIERNO" EL DESAFÍO (ATACANTES) PUEDE SER MITIGADO

Mucho antes de que Jeep sufriera un hackeo muy publicitado que llamó la atención y preocupación del C-suite y el Consejo sobre la ciberseguridad de los vehículos conectados, nuestra Firma fue contratada por un prominente fabricante de autos para realizar un ejercicio confidencial de "hacking ético". Montamos un ataque a la empresa tipo Estado-nación, y después de muchas semanas de trabajo con un gran equipo, logramos un control completo, de tal manera que hubiéramos podido interferir con sus redes corporativas y de fabricación y con las interacciones con los vehículos.

Bienvenidos al nuevo territorio del ciberdelincuente: la creciente y dinámicamente cambiante "superficie de ataque" del vehículo conectado, es decir, la totalidad de los potenciales puntos de entrada no autorizados. La buena noticia es que el *hacking* en este espacio requiere habilidades muy avanzadas e importantes, por lo que un "script kiddie" medio no se hará con el control de los coches conectados en un futuro próximo. Las malas noticias son que, adversarios bien financiados y capacitados, que han afectado ya a la mayoría de las otras industrias, pueden empezar a dirigir su atención a las compañías de automóviles.

En este momento, mientras la industria automotriz trabaja para entender mejor las amenazas cibernéticas contra los automóviles conectados, puede tomar tres medidas inmediatas para mitigar sus riesgos (y el peligro físico de los clientes): conocer la superficie de ataque, evaluar continuamente las amenazas y adoptar un cibergobierno holístico y dinámico.

Los automóviles están integrando rápidamente nuevas tecnologías digitales para mejorar la experiencia de conducción y las vidas conectadas de los ocupantes a bordo. Sin embargo, la desventaja de aumentar la conectividad y las funcionalidades es que al hacerlo se expande la superficie de ataque del automóvil. Esto crea una situación potencialmente peligrosa, dada la oportunidad para que los criminales ganen mucho dinero a través de ataques dirigidos a los coches conectados, a sus fabricantes, y a sus redes.

Hasta la fecha, han sido los profesionales de seguridad quienes han hackeado coches conectados. Por ejemplo, hackearon la aplicación móvil OnStar, explotando un fallo de seguridad para desbloquear coches y arrancar motores a distancia[1]. Otros responsables de seguridad utilizaron simuladores GPS disponibles públicamente para suplantar las señales débiles del GPS con una señal falsa de mayor potencia que podría haber desviado un vehículo o enviar información falsa a los rastreadores de vehículos, como por ejemplo los operadores de flotas.

En el hackeo de Jeep mencionado anteriormente, dos hackers éticos contratados por la revista Wired pasaron cuatro meses montando un ataque "zero-day"[3] contra el vehículo. Primero, se infiltraron en su conectividad móvil. Después, se movieron lateralmente para comprometer la columna vertebral de la electrónica del coche, llamada el área de control del bus de red (CANBus). Entonces, alteraron sistemas conectados al CANBus que controlan arranque, parada, aceleración y dirección. Esto permitió a los hackers controlar completamente el coche, mientras un editor de Wired conducía (o intentaba conducir) el vehículo[4].

A pesar de que los profesionales de seguridad no tienen intención maliciosa, la revelación pública de las vulnerabilidades que encuentran pueden resultar en enormes costes para las empresas de automóviles conectados. Por ejemplo, el hackeo de Jeep resultó en una retirada del mercado de aproximadamente 1,4 millones de vehículos, y la cotización bursátil de Chrysler

1 "Investigador dice que puede hackear la aplicación OnStar de GM, abrir el vehículo, arrancar el motor", Reuters.com, 30 de julio de 2015, © 2015 Thomson Reuters.
2 "La falacia de la seguridad: Siete mitos sobre la seguridad física", Laboratorio Nacional Argonne, 26 de octubre de 2010.
3 Un ataque de día cero es uno que nunca se ha visto antes.
4 "Jeep Hacking 101", IEEE Spectrum, 6 de agosto de 2015, © Copyright 2015 IEEE Spectrum.

cayó un 6,4% el día después de dicha retirada, para después rebotar.

En el futuro, los coches conectados sin duda serán blanco de criminales con motivación económica, hacktivistas, y otros delincuentes que quieran causar daños físicos a los conductores. Algo de esto ya ha comenzado a suceder. Por ejemplo, los hackers han descifrado un sistema de entrada sin llave usado por múltiples fabricantes[5]. La policía dice que el hackeo fue usado para robar aproximadamente 6.000 coches en Londres en 2014[6].

PASO 1: CONOCER LA SUPERFICIE DE ATAQUE

La gestión del riesgo cibernético de los vehículos conectados comienza aceptando que la superficie de ataque el vehículo conectado es amplia y cambia continuamente. La superficie de ataque incluye el coche conectado, las redes corporativas y de fabricación de la empresa, las aplicaciones móviles, los concesionarios y terceros con conexiones de confianza a esas redes, al propio vehículo y a aplicaciones de posventa que se conectan a los sistemas del coche conectado.

Esto proporciona una gran oportunidad para los atacantes y requiere que las empresas de automóviles adopten un enfoque integrado hacia la seguridad para gestionar el riesgo cibernético en todos estos entornos, en lugar de hacerlo en silos:

En el futuro, los coches conectados sin duda serán blanco de criminales con motivación económica, hacktivistas, y otros delincuentes que quieran causar daños físicos a los conductores

- **Redes corporativas:** Con sus múltiples componentes orientados al público (incluyendo conectividad a Internet, sitios web, correo electrónico remoto y puntos de acceso inalámbricos corporativos), las redes corporativas de los fabricantes de automóviles podrían representar la forma más fácil de entrar para los atacantes. En estas redes, se puede conseguir información de identificación personal sobre clientes, puertas de entrada a la red de fabricación, conectividad potencial a sistemas de seguridad y otros controles industriales, correo electrónico corporativo, conocimiento sobre fabricación, o información material no pública, por nombrar unos pocos. Las conexiones de terceros de confianza extienden la superficie de ataque a los socios y proveedores de una empresa, y en otros sectores este ha sido el canal de entrada de los hackers.
- **Redes de fabricación:** las redes de fabricación de automóviles pueden no tener conectividad directa a Internet, pero los atacantes buscarán acceder a los sistemas de fabricación mediante la obtención de una credencial en la red corporativa para luego moverse lateralmente hacia la red de fabricación. Una vez en la red de fabricación, los atacantes pueden buscar especificaciones de fabricación u otra propiedad intelectual valiosa, intentar interrumpir las operaciones o destruir equipos, o corromper el software con el fin de introducir puertas traseras que puedan usar para controlar remotamente los vehículos.
- **Coches:** los coches conectados tienen conectividad a través de tecnologías móviles, inalámbricas, Bluetooth e infrarrojos (tecla fob). Los atacantes intentarán conectarse al coche a través de una de esas tecnologías y luego pivotar a lo largo de la red del coche para alcanzar los componentes que les ayuden a ejecutar su plan, ya sea para controlar algún aspecto del coche, corromper la información que fluye hacia el coche (como la información GPS), o simplemente encontrar y dar a conocer un conjunto de vulnerabilidades.
- **Redes posventa:** Las numerosas aplicaciones alojadas en vehículos conectados presentan vulnerabilidades potenciales a través de las que los hackers pueden acceder y tomar el control de coches conectados. Los dispositivos y utilidades posventa expanden significativamente la superficie de ataque y aumentan su naturaleza dinámica. Móviles instalados o conectados por el consumidor y dispositivos adicionales de posventa a menudo tienen su propia conectividad a Internet y sus propias vulnerabilidades, completamente fuera del control del fabricante. No sólo estos complementos pueden ser pirateados, sino que su uso regular posibilita que los hackers puedan manipular a los propietarios de coches en tiempo real, por ejemplo, mediante técnicas de ingeniería social, haciendo que estos introduzcan en el vehículo dispositivos hackeados.

5 "Hack para robar coches con encendido sin llave: Volkswagen pasó 2 años escondiendo defectos", Computerworld, 17 de agosto de 2015, 2015 Computerworld, Inc.

6 "Hackers Force Carmakers to Boost Security for Driverless Era," Bloomberg Business, 4 August 2015, Bloomberg L.P.Ibid.

PASO 2: LLEVAR A CABO UNA EVALUACIÓN COMPLETA DE LA AMENAZA

Comprender los motivos de los hackers ayuda a los fabricantes de automóviles a conocer sus riesgos. Como uno de los hackers de Jeep dijo durante una presentación de la hazaña en una conferencia en agosto de 2015: "No voy a fanfarronear, pero hicimos que las acciones bajaran".

Del mismo modo, no es difícil imaginar a los "hacktivistas", es decir, a los hackers que tienen motivaciones ideológicas, realizando ciberataques por creencias del tipo antiglobalización, cambio climático u otras razones políticas. Los malos actores también pueden utilizar vehículos piratas como instrumentos para infligir daños de forma selectiva (en una venganza individual) o a una base amplia (en un ataque terrorista). Por último, está la motivación para conseguir "derecho a alardear", lo cual puede parecer frívolo, pero aún sigue sucediendo.

PASO 3: ADOPTAR UN CIBERGOBIERNO HOLÍSTICO Y DINÁMICO

El "gobierno" cibernético incluye no sólo las estructuras organizativas que subyacen al esfuerzo para mitigar el riesgo, sino los procesos que la empresa tiene que implantar para identificar los riesgos a los que se enfrenta. Al adoptar un enfoque holístico y dinámico del cibergobierno, los fabricantes de automóviles pueden llegar más lejos que los hackers. A pesar de una vasta y cambiante superficie de ataque, y mientras las motivaciones del atacante son innumerables, con un cibergobierno adecuado se puede mitigar el desafío que plantean.

El compromiso de la Dirección, combinado con las inversiones adecuadas, puede ayudar a la Organización en el camino a la resiliencia. A continuación, se presentan algunos pasos inmediatos a considerar:

- **"Cacería" proactiva:** Con la gama de potenciales motivos de los hackers claramente discernibles, los fabricantes de automóviles deben suscribirse a fuentes de información de inteligencia y compartir información sobre amenazas dentro de su sector que se alineen con estas amenazas.
- **Eliminar los silos del cibergobierno:** El ecosistema automotriz está altamente interconectado. Cualquier vulnerabilidad en un componente o departamento conectado puede afectar a todos los demás. Eso es porque los atacantes pivotarán de uno al otro. Los departamentos corporativos, fabricación, gestión de vehículos, cadena de suministro, y redes de posventa están detrás de cada coche conectado. Por eso, todos los implicados deben trabajar juntos para anticipar cómo pueden ocurrir ataques. Una función centralizada, como el CISO, debe ser responsable del riesgo en todos sus aspectos, componentes y departamentos afectados. Realizar ejercicios que simulan ataques avanzados puede aumentar la concienciación y reducir el comportamiento en silos.
- **Desafía tus defensas:** Inculcar una cultura de seguridad que valore el exponer rutinariamente vulnerabilidades. Por ejemplo, ejercicios de hacking ético –en los que los equipos inventan nuevas formas de tratar de piratear los coches, las empresas y redes de fabricación, y aplicaciones móviles– conduce a la identificación y remediación de vulnerabilidades, y así endurecer las defensas. Los terceros independientes pueden desempeñar un papel clave en ciberdefensas. Los ejercicios de "Read team" con expertos externos resultan especialmente útiles, puesto que estudian el comportamiento de los criminales, sin estar sujetos a las restricciones impuestas por las políticas y procedimientos corporativos que están dispuestos a romper o desafiar.
- **Anticipar las vulnerabilidades futuras:** los fabricantes de vehículos autónomos deben crear un ciclo de mejora continua: identificación, ruptura, remediación, y anticipación de la próxima ola de vulnerabilidades. Sólo porque un coche conectado sea seguro hoy, no significa que seguirá siendo seguro dentro de tres meses. Los escenarios son múltiples. Podría ser algo tan cotidiano como una aseguradora o una compañía de recambios que sale a la luz con un nuevo complemento. O, digamos que un fabricante implementa una actualización de software enviando físicamente por correo unidades USB a sus clientes, y los hackers se adelantan enviando sus propios USB infectados, empaquetadas para que se parezcan a los de verdad.

UN CIBERGOBIERNO RESILIENTE: MANTENER EL RITMO A TRAVÉS DEL CAMBIO

Las oportunidades y los desafíos que vienen con el aumento de la conectividad de los automóviles son sustanciales. Los clientes quieren claramente las ventajas que ofrece la conectividad a bordo, pero los delincuentes se benefician de ello y están muy motivados. La manera de mantenerse por delante de los hackers es adoptando un modelo de cibergobierno resiliente que unifique todos los actores de su ecosistema y tenga en cuenta continuamente las nuevas tecnologías de vanguardia a medida que evoluciona la tecnología de sus vehículos conectados. Este tipo de gobierno requiere un claro compromiso desde lo más alto de la Organización.