Investigadores en ciberseguridad han revelado una serie de vulnerabilidades en vehículos Kia, que ya han sido corregidas, las cuales, de haberse explotado, habrían permitido el control remoto de funciones clave utilizando solo la matrícula del automóvil.

> *«Estos ataques se podrían haber realizado de forma remota en cualquier vehículo con hardware compatible en aproximadamente 30 segundos, sin importar si tenía una suscripción activa a Kia Connect»,* explicaron los investigadores de seguridad Neiko Rivera, Sam Curry, Justin Rhinehart e Ian Carroll.

Estas fallas afectaban a la mayoría de los vehículos fabricados a partir de 2013, lo que permitía a los atacantes acceder de forma discreta a información sensible como el nombre, número de teléfono, correo electrónico y dirección física de la víctima.

En resumen, los atacantes podrían aprovechar esta vulnerabilidad para añadirse a sí mismos como un segundo usuario «invisible» en el sistema del vehículo, sin que el propietario estuviera al tanto.

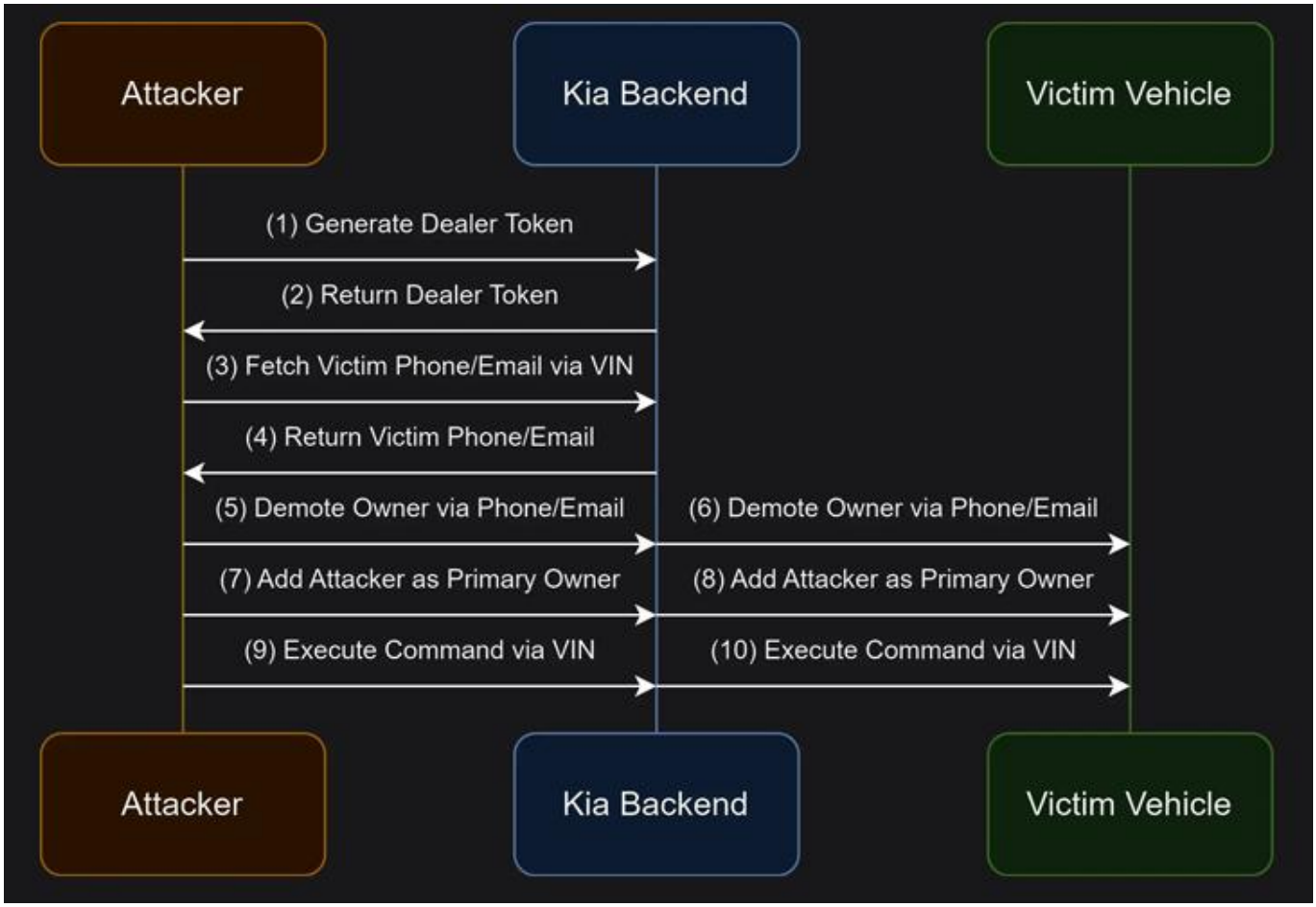
La investigación se centró en cómo estas vulnerabilidades explotan la infraestructura utilizada por los concesionarios Kia («kiaconnect.kdealer[.]com») para activar los vehículos. A través de una solicitud HTTP, los atacantes podían registrarse con una cuenta falsa y generar tokens de acceso.

Este token, junto con otra solicitud HTTP a un punto de acceso API del concesionario y el número de identificación del vehículo (VIN), se utilizaba para obtener el nombre, número de teléfono y correo electrónico del propietario del vehículo.

Además, los investigadores descubrieron que era posible acceder al vehículo de una víctima simplemente haciendo cuatro solicitudes HTTP, y finalmente ejecutar comandos de control del vehículo de manera remota:

1. Generar un token de concesionario y recuperar el encabezado «token» de la respuesta HTTP usando el método descrito anteriormente.
2. Obtener la dirección de correo electrónico y el número de teléfono de la víctima.
3. Usar el correo electrónico filtrado y el VIN para modificar el acceso del propietario y establecer al atacante como el titular principal de la cuenta.
4. Añadir al atacante como propietario principal del vehículo usando una dirección de correo electrónico bajo su control, permitiéndole ejecutar comandos arbitrarios.

> *«Desde la perspectiva de la víctima, no había notificaciones que indicaran que su vehículo había sido accedido o que los permisos de acceso habían sido modificados»,* explicaron los investigadores.
>
> *«Un atacante podría identificar la matrícula de un vehículo, ingresar el VIN en la API y luego rastrear pasivamente al propietario, enviando comandos activos como desbloquear, encender el motor o hacer sonar el claxon.»*



En un escenario hipotético, un atacante malintencionado podría ingresar la matrícula de un vehículo Kia en un panel de control personalizado, obtener la información del propietario y, en cuestión de 30 segundos, comenzar a ejecutar comandos sobre el vehículo.

Tras un informe de divulgación responsable en junio de 2024, Kia solucionó estas vulnerabilidades el 14 de agosto de 2024. No se ha encontrado evidencia de que estas fallas se hayan explotado en ataques reales.

> *«Los vehículos continuarán teniendo vulnerabilidades, ya que, de la misma manera que Meta podría introducir un cambio de código que permita a alguien tomar el*

> *control de tu cuenta de Facebook, los fabricantes de automóviles también podrían hacer algo similar con tu coche»,* advirtieron los investigadores.