Thieves Use CAN Injection Hack to Steal Cars

A hacking device can allow thieves to steal a wide range of car models using an attack method named CAN injection, researchers have revealed.

Automotive cybersecurity experts Ian Tabor of the EDAG Group and Ken Tindell, CTO of Canis Automotive Labs, started analyzing these attacks after Tabor had his 2021 Toyota RAV4 stolen last year.

The car was stolen after on two occasions Tabor found that someone had pulled apart his headlight and unplugged the cables. What initially appeared as vandalism turned out to be part of an attempt to steal the vehicle.

Specifically, the thieves pulled off the bumper and unplugged the headlight cables in an attempt to reach wires connected to an electronic control unit (ECU) responsible for the vehicle's smart key.

An investigation conducted by Tabor showed that the thieves likely connected a special hacking device that allowed them to unlock the vehicle and drive away.

Such hacking devices can be acquired on dark web sites for up to €5,000 ($5,500), and they are often advertised as 'emergency start' devices that can be used by vehicle owners who have lost their keys or automotive locksmiths. In the case of the device designed for Toyota cars, the electronics responsible for hacking the vehicle are hidden inside a Bluetooth speaker case.

The hacking device is designed to conduct what the researchers

call a CAN injection attack. These devices appear to be increasingly used by thieves. At least one theft was caught by CCTV cameras in London:

[embedded content]

The researchers analyzed diagnostics data from Tabor's stolen RAV4 and such a CAN injection device in an effort to see how they work.

Modern cars have several ECUs, each responsible for a different system, such as headlights, climate control, telematics, cameras, engine control, and the smart key that unlocks and starts the vehicle. ECUs are connected together through controller area network (CAN) buses.

The attacker does not need to directly connect to the smart key ECU. Instead, they can reach the smart key ECU from the wires connected to, for example, the headlight, as long as the headlight and the smart key ECU are on the same CAN bus.

The attacker connects the hacking device to the headlight wires and can send a specially crafted CAN message that tells the smart key receiver ECU that the key is validated. The attacker can then send a specially crafted CAN message to the door ECU to unlock the door. This allows the thieves to get in the car and drive away.

The attack can be carried out by connecting the hacking device to other CAN wires as well, but the ones in the headlight are often the most accessible and connecting to them does not involve causing too much damage to the car, which would lower its value.

While in this case the stolen vehicle was a Toyota and the hacking device tested by the researchers is specifically designed for Toyota cars, the problem is not specific to Toyota.

Similar hacking devices offered for sale to car thieves target many brands, including BMW, GMC, Cadillac, Chrysler, Ford, Honda, Jaguar, Jeep, Maserati, Nissan, Peugeot, Renault, and Volkswagen.

The researchers did report their findings to Toyota, but without much success due to the fact that it’s not an actual vulnerability disclosure. On the other hand, they believe all vehicle makers should read their report and take action to prevent CAN injection attacks. The report made public this week contains some recommendations that can be applied by manufacturers to prevent these types of attacks.

The security experts did manage to have a CVE identifier, CVE-2023-29389, assigned to the Toyota RAV4 hack.

Related: Tesla Hacked Twice at Pwn2Own Exploit Contest

Related: 16 Car Makers and Their Vehicles Hacked via Telematics, APIs, Infrastructure

Related: Unpatched Micodus GPS Tracker Vulnerabilities Allow Hackers to Remotely Disable Cars

Related: Honda Admits Hackers Could Unlock Car Doors, Start Engines

Thieves Use CAN Injection Hack to Steal Cars