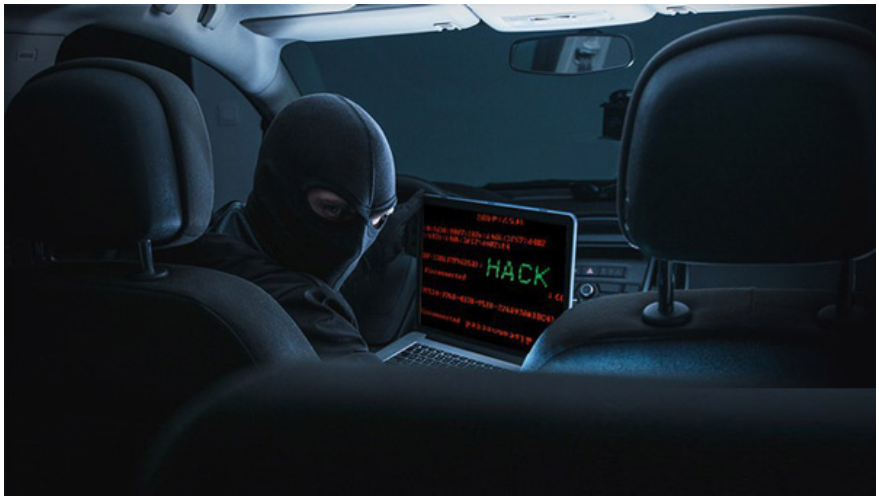
Hackers claim to be able to 'shutdown' 25,000 cars in a single note

Not you, it's the hacker who owns the car.

IoT devices and wireless networking technology are giving people a lot of convenience in life. One of them is the Immobilizer, which is equipped with a car to help millions of users around the world feel more secure.

Smart anti-theft technology ensures that only the key holder can start the car, the owner can track and locate the vehicle, can connect and turn off the vehicle engine (remotely) when detected. strangers intend to steal. However, this technology is gradually becoming a security threat.



Recently, a hacker announced that he could "shutdown" 25,000 cars at the same time, with a single operation. Taking advantage of a security vulnerability on SmarTrackdo tracking and anti-theft device, Global Tememetrics produces, although thousands of kilometers away, the hacke can easily bypass the vehicle owner to take control of the remote Smart anti-theft device, does not allow the driver to start his car engine.

This security vulnerability was discovered by a team from network security company Pen Test Partners. According to the research team, through this security hole, the attack and hijacking of the car is extremely simple, even if the owner is not aware of it.

To prove it, the team tried to "hack" the car equipped with an employee's SmarTrack device to work with the same company. Sitting in England, the group has successfully overthrown the colleague's car in remote Greece.

At the DEF CON conference in Las Vegas, Ken Munro, a researcher and cyber security partner of the Pen Test Parners, said he discovered how to turn on / off a car's anti-theft device with just one line of code. Simple commands through the browser. The anti-theft device was activated after only a second when Munro entered the command.

Munro also warned that the driver would not be able to restart the engine that was turned off when the anti-theft system was attacked and hijacked by hackers. Meanwhile, the new hacker is the owner of the car. Now, completely removing the intelligent anti-theft device is the only thing the owner can do.

Hackers taking control of an anti-theft device can lead to extremely dangerous situations. If the vehicle is moving on a highway where a hacker activates anti-theft mode, your vehicle will suddenly stop because the engine is turned off. Meanwhile, a series of continuous accidents on the highway is absolutely possible.

Currently, Global Tememetrics has patched this serious security hole on SmarTrack system but it also shows that we have to pay more attention to the level of security in the context of IoT devices are gradually becoming popular thanks to 5G technology.

1. With this fake Lightning cable, hackers can remotely take over your computer in minutes

You finished reading the article "**Hackers claim to be able to 'shutdown' 25,000 cars in a single note**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
