Are aftermarket smart car devices secure?

Kaspersky researchers analysed aftermarket connected car devices, designed to make vehicles smarter. This niche has proven to be more secure than other Internet of Things (IoT) accessories.

There are currently two ways for car enthusiasts to obtain a connected vehicle – purchase a ‘smart by design’ car from a dealer, or improve their existing car with a number of additional ‘smart-devices’.

While both scenarios create a greater driving experience, smart technology also represents a brand new area for malicious use, as the media and Kaspersky’s own research has repeatedly shown. This is inevitable – when a piece of technology becomes essential, related security issues tend to increase.

Source: pixabay.com

With this in mind, Kaspersky researchers set out to discover whether these reports on the security of IoT devices had any impact on manufacturers of smart devices for the automotive industry. The researchers analysed several randomly selected devices, including an OBD dongle scanning tool, tyre pressure and temperature monitoring system, a smart alarm system, a GPS tracker, and an app-controlled dashcam.

The findings were a pleasant surprise: while the IoT industry has often been considered vulnerable, these automotive-related smart and connected devices proved to be quite secure, with no major vulnerabilities exposed.

However, several security issues were also revealed: the ability to remotely access driving dynamics data via a scanning tool, the option to manipulate signals from the tire monitoring system, and, most alarmingly, the ability to open vehicle doors using the alarm system. However, all of these elements are either very hard to implement or bring no obvious or immediate outcome for a criminal.

Very few issues found

“The devices we examined met many security policies and were satisfactory, with the exception of a few small issues. This is partly due to the limited functionality of these devices and the lack of serious consequences in the event of a successful attack through these products – but also thanks to the vigilance of manufacturers.

We were glad to see that they have invested their efforts into making these devices more secure, a good sign overall for the automotive industry. Yet, this is still not a reason to relax: based on our experience, the smarter the device, the higher the chances that security issues will occur. That is why security should be considered more closely in the early stages of product development, especially as a new generation of smart devices come to the market,” notes Victor Chebyshev, a security expert at Kaspersky.

Victor Chebyshev, a security expert at Kaspersky

To keep smart automotive devices even more secure, we advise:

1. When choosing which part of your vehicle you're going to make a little bit smarter, first consider the security risks. Think twice if the device has something to do with the car telemetry or access to its 'brains'.

2. Before buying a device, search the internet for news of any vulnerabilities. It is likely that the device you are going to purchase has already been examined by security researchers and it is possible to find out whether any issues have been found in the device, or have already been patched.

3. It is not always a great idea to buy the most recent products released on the market. Along with the standard bugs often found in new products, recently-launched devices might contain security issues that haven't yet been discovered by security researchers. The best choice is to buy products that have already been worked on with several software updates.

4. Always consider the security of the 'mobile dimension' of the device, especially if you have Android devices – applications are often helpful and make life easier, but once a smartphone is hit by malware, a lot can go wrong.

5. To overcome the challenge of smart device cybersecurity, Kaspersky has invested in Kaspersky OS, widely used in customised manufacturing hardware and software. This system can be used across a variety of fields: on mobile devices and PCs, IOT devices, intelligent energy systems, industrial systems, telecommunications, and transportation systems. Kaspersky sees opportunities in the further development of KasperskyOS to meet the needs of our customers and ensure the highest levels of security can be achieved in all these fields, including the automotive industry. More information can be found here.