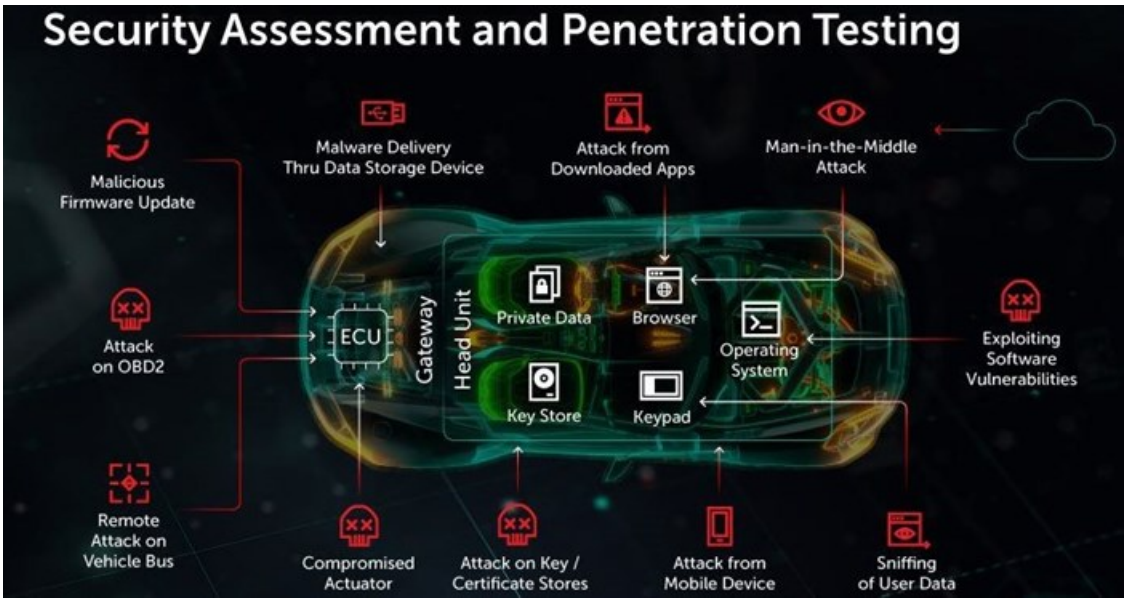
Kaspersky makes threat intelligence reports available for auto industry

Cybersecurity company Kaspersky recently announced that it has launched its tailored threat intelligence (TI) reporting tool for organisations working in the automotive industry - the tool was previously only available for a selected range of its customers.



Source: kaspersky.co.za

Kaspersky's reports reportedly provide car manufacturers with in-depth analysis of industry-specific security threats and identify information that could be utilised by malefactors to develop attacks on vehicles, connected vehicle infrastructure and other vehicle-related systems.

7 tips from Kaspersky on using Telegram privately and securely

13 Jan 2021

The company says numerous cases show an interest in automotive security. From independent researchers and enthusiasts to cybercriminals, the focus has moved on from the security of embedded devices and more attention is now being paid to the security of vehicles. This has resulted in a growing number of attack techniques and the introduction of new regulatory requirements that manufacturers must follow in order to stay protected against them.

An explanation by Kaspersky on the reports:

Each report includes an overview and analysis of technological trends related to cyberattacks in the automotive industry, such as cyber-incidents, recent security studies, conferences, talks, community forums, as well as information on potential attack vectors on the customer’s vehicle backend and services infrastructure.

The main service deliverables are the report with a high-level executive summary, threat descriptions and recommendations, as well as notifications on high-risk activities and vulnerabilities tailored for the OEM.

If the report finds a threat that needs to be resolved urgently, customers are notified immediately.

Sergey Zorin, head of Kaspersky transportation system security, says:

> *"With the growing number of technologies being used in modern vehicles, it is important to not only comply with the upcoming regulatory requirements but to also have information about all possible threats - from electronic control unit vulnerabilities to attacks on vehicle-to-everything components. By providing relevant threat intelligence, we do our part in helping car manufacturers manage these concerns."*