Trend Micro report analyzes cyber attacks on the road and how to mitigate them

DALLAS, Feb. 16, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity, today announced a major new study into connected car security that describes multiple scenarios in which drivers could encounter attacks that threaten the safety of themselves and others.

Click here to access the full report, *Cyber Security for Connected Cars: Exploring Risks in 5G, Cloud and Other Connected Technologies*.

The report reveals the scope of the cybersecurity risks examined. Researchers evaluated 29 real-world attack scenarios according to the DREAD[1] threat model for qualitative risk analysis. These attacks could be launched remotely against and/or from victim vehicles. Examples and highlights include:

- DDoS attacks on Intelligent Transportation Systems (ITS) could overwhelm connected car communications and represent a high risk.
- Exposed and vulnerable connected car systems are easily discovered, making them at higher risk of abuse.
- Over 17% of all attack vectors examined were high risk. These require only a limited understanding of connected car technology and could be accomplished by a low-skilled attacker.

"Our research shows that there are ample opportunities for attackers looking to abuse connected car technology," said Rainer Vosseler, threat research manager for Trend Micro. "Fortunately, there are currently limited opportunities for attacks, and criminals have not found reliable ways to monetize such attacks. With the U.N.'s recent regulations requiring all connected cars to include cybersecurity, as well as a new ISO standard underway, now is the time for stakeholders across the industry to better identify and address cyber risk as we accelerate towards a connected and autonomous vehicle future." [2]

More than 125 million passenger cars with embedded connectivity are forecast to ship worldwide between 2018 and 2022, and progress continues to advance towards fully autonomous vehicles. This advancement will create a complex ecosystem comprising cloud, IoT, 5G and other key technologies. It also features an enormous attack surface comprising potentially millions of endpoints and end users.

As the industry develops, there will be multiple opportunities for monetization and sabotage for cybercriminals, hacktivists, terrorists, nation states, insiders and even unscrupulous operators, the report warns. Of all 29 attack vectors studied, the overall risk of successful cyber attacks was assessed as Medium. However, as SaaS applications become embedded in the Electrical/Electronics (E/E) architecture of vehicles and cybercriminals create new monetization strategies, an evolution in attacks will lead to higher risk threats.

To mitigate the risks outlined in the study, connected car security must be designed with an integrated view of all critical areas to secure the end-to-end data supply chain. Trend Micro has the following high-level guidance for protecting connected cars:

- Assume compromise and have effective alert, containment, and mitigation processes.
- Protect the end-to-end data supply chain across the car's E/E network, the network infrastructure, backend servers, and VSOC (Vehicle Security Operations Center).
- Apply lessons learned to further strengthen defenses and prevent repeat incidents.
- Relevant security technologies include firewall, encryption, device control, app security, vulnerability scanner, code signing, IDS for CAN, AV for head unit, and much more.

Trend Micro offers IoT cybersecurity solutions specific to connected cars. Learn more here: https://www.trendmicro.com/en_us/business/solutions/iot/connected-car.html.

About Trend Micro
Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers with connected solutions across cloud workloads, endpoints, email, IIoT, and networks. Our XGen™ security strategy powers our solutions with a cross-generational blend of threat-defense techniques that are optimized for key environments and leverage shared threat intelligence for better, faster protection. With over 6,700 employees in 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. www.trendmicro.com

[1] DREAD evaluates how great the damage is to assets; how easy the attack is to launch and replicate; how easy it is to find an exploitable weakness; and how many users might be affected.
[2] https://unece.org/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll-out-connected-vehicles

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

Additional assets available online: (1)

https://newsroom.trendmicro.com/2021-02-16-Connected-Cars-Technology-Vulnerable-to-Cyber-Attacks