Trend Micro Helps Connected Car Stakeholders Manage Cyber Risk

Research details and prioritizes key attack vectors including future scenarios

DALLAS, Sept. 2, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, is committed to managing cyber risk no matter where it occurs. Today's new research report is designed to help manufacturers, suppliers, government bodies and service providers successfully manage cyber risk while implementing a key United Nations regulation on connected vehicle cybersecurity.

To read a full copy of the report, *Identifying Cybersecurity Focus Areas in Connected Cars Based on WP.29 UN R155 Attack Vectors and Beyond,* please visit: *https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/a-roadmap-to-secure-connected-cars*.

"Cyber risk is everywhere – even in your car. Vehicles are gaining intelligence, computing power, and connectivity, creating new attack scenarios for cybercriminals," said William Malik, vice president of infrastructure strategies for Trend Micro. "Understanding these cybersecurity recommendations and regulations will help manufacturers future-proof mobility. Our latest research report helps interpret and implement the WP.29 regulation by prioritizing the threats to the connected car industry."

To help stakeholders prioritize all the threats and attack vectors outlined by WP.29, Trend Micro experts calculated the severity levels of these attack vectors using the industry standard DREAD threat model.

These attack vectors should be given the highest priority, according to the research:

- Back-end servers used to attack a vehicle or extract data
- Denial of service attacks via communication channels to disrupt vehicle functions
- Hosted third-party software (e.g. entertainment apps) used to attack vehicle systems

Researchers also recalculated the DREAD threat model to show how threat severity will evolve over the next 5-10 years and highlighted new and emerging vectors not included in the WP.29 regulation.

The United Nations Economic Commission for Europe World Forum for Harmonization of Vehicle Regulations (WP.29) regulates vehicle safety around the world. The regulation contains seven high-level and 30 sub-level descriptions of vulnerabilities and threats, including 69 attack vectors. The regulations along with Trend Micro's findings will support the connected car industry's understanding of cyber risks to best prioritize their defense.

This latest Trend Micro report follows on from a February 2021 study on connected car security in which explored risks with connected vehicles interconnected with 5G, Cloud, and other connected technologies.

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

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

---