Autonomous and Connected Vehicles Face 300,000 Attacks Per Month, According to Karamba Security

While self-driving cars take center stage at CES 2019, Karamba's ThreatHive cyber honey pots provides visibility about the scale of real hackers trying to attack connected automotive ECUs

LAS VEGAS and HOD HASHARON, Israel – January 8, 2019 – Karamba Security, a world-leading provider of end-to-end automotive cybersecurity prevention solutions, today unveiled vulnerability data in the autonomous and connected vehicle industry. Karamba Security has been attracting internet attacks on automotive electronic control units (ECUs) through its latest solution Karamba ThreatHive™. In the last three months alone, Karamba ThreatHive analysis concluded that each of the ECUs that Karamba had exposed to internet connectivity was subjected to as many as 300,000 attacks per month.

Karamba ThreatHive harnesses real-world hacking attempts to expose and pinpoint ECU vulnerabilities to be fixed before such vulnerabilities are exploited in real cars. A global system of data-generating "honeypots" runs continuously, collecting threat data to identify vehicle security gaps. According to the data, each of the automotive ECUs exposed by ThreatHive to the internet was attacked on average 300,000 times per month by 3,500 different hackers. Attackers come in different forms and are often bots searching for any ECU vulnerabilities they can expose to gain control of the connected system.

With ThreatHive, OEMs and tier 1s receive actionable security data to fix security bugs and logical errors before hackers actually exploit those vulnerabilities in real cars. The data enables them to close security gaps long time before hackers try to infiltrate the vehicle.

"The fact that each connected ECU gets attacked about 300,000 times every month illustrates just how creative and persistent hackers have become," said Ami Dotan, Karamba Security's co-founder and CEO. "As autonomous and connected vehicles become software driven, risks increase that hackers will find ways to take control of the vehicle by compromising ECUs and infiltrating cars to change their speed and direction. The automotive industry needs to take preventative measures and leverage technologies like ThreatHive that expose vulnerabilities for OEMS and tier 1s to address during the production stage, before the hackers identify and exploit such vulnerabilities in the car itself."

Data also uncovered that over 11 different types of attacks were attempted since Karamba ThreatHive's inception. Each simulated ECU was targeted by a different mode of attack, aiming to exploit different services in the ECU. Examples include attacks to the Telnet port – similar to the services targeted on the VW Golf white hat attack in April 2018 – to SSH (Subaru 2018) and to HTTP (Tesla 2017). Attacks were prevalent across geographies and service providers.

At CES 2019 attendees are invited to participate in a real car hacking demo or prevent cyberattacks launched at the car by scheduling an appointment here. Karamba Security executives will be available at CES 2019 Booth #929 to share ThreatHive insights, show a real-time view of vehicle attacks and discuss the partners ecosystem that is enhancing automotive cybersecurity.

About Karamba Security

Karamba Security provides industry-leading automotive cybersecurity solutions for autonomous and connected cars. Its Autonomous Security software products, including ThreatHive, Carwall, and SafeCAN, provide end-to-end in-vehicle cybersecurity for the endpoints and the internal messaging bus. Karamba Security's award-winning solutions prevent cyberattacks with zero false positives and secure

communications, including OTA updates, with negligible performance impact. Karamba is engaged with 17 OEM and tier-1 customers and received numerous industry awards. More information is available at www.karambasecurity.com and follow us on Twitter @KarambaSecurity.

Karamba Security Business Contact:
Amir Einav, VP of Marketing
amir.einav@karambasecurity.com
214-620-7320

Media Contact:
PAN Communications
Kyle Tildsley
Karamba@pancomm.com
617.502.4300