Karamba Security Introduces ThreatHive Solution for Expedited Detection of Automotive Cybersecurity Vulnerabilities

Karamba Security online service provides actionable insights on hacking attempts to electronic controller units (ECUs) of autonomous and connected vehicles

Bloomfield Hills, MI, Hod Hasharon, Israel – October 2, 2018 – Karamba Security, a world-leading provider of end-to-end automotive cybersecurity prevention solutions, today announced ThreatHive, which provides automobile OEMs and Tier-1 suppliers a view of actual, online attacks on their ECUs during development. This service offering enhances Karamba's ECU protection portfolio with Automotive Threat Intelligence, giving the automotive security industry a platform for early discovery of security vulnerabilities.

Karamba Security's ThreatHive implements a worldwide set of hosted automotive ECUs in simulation of a "car like" environment. These ECU software images are automatically monitored to expose automobile attack patterns, tools, and vulnerabilities in the ECU's operating system, configuration, and code. The real attacks on the ECU during the development lifecycle provide actionable insights into security vulnerabilities, including industry software (like OS, development tools, and common libraries), that benefit the automotive security community.

"Understanding the different attack vectors used against ECUs has always been a challenge for vehicle OEMs and Tier 1 suppliers. These stakeholders rightfully place a premium on learning how hackers might infiltrate a vehicle's system before the vehicle goes to production," said Patrick Daly, Analyst at 451 Research. "Karamba Security's offering is focused on providing the specific insights needed to keep connected and autonomous vehicles secure. If OEMs and Tier-1 suppliers can stay a step ahead of hackers they increase consumer safety and reduce the need for future Over-The-Air updates to remediate vulnerabilities once vehicles hit production."

By utilizing hackers' crowd effect, attacking the ECU software hosted in the honeypots, Karamba Security's offering expedites vulnerabilities discovery, and reduces OEMs' and Tier-1 suppliers' investment in penetration testing during product acceptance tests, in a narrow time window, which may limit vulnerabilities discovery. The findings from the threat analysis tool are shared in an aggregated and anonymized way to help vehicle OEMs and Tier-1 suppliers secure ECUs from hackers, as part of Karamba Security's strategic partnership with US Auto-ISAC.

"This new offering expands Karamba's ECU protection portfolio by providing actionable insights based on security research inputs to secure connected vehicles throughout their lifecycle," said Ami Dotan, Karamba Security's co-founder and CEO. "Customers need ways to test their products with real life security scenarios and our approach identifies and reports cyber-attacks, today, years and months before production, when there is enough time to fix those issues. By gaining insights on code vulnerabilities customers are able to update prevention technologies and fix vulnerabilities before they get into production, and not compromise time to market."

ThreatHive works with Karamba Security's Carwall, its in-vehicle security software that automatically secures connected cars against cyberattacks. Carwall keeps connected and autonomous cars safe by sealing the car's ECU software, so it automatically prevents cyberattacks from infiltrating the vehicle and compromise consumer safety. Together the products build out Karamba Security's ECU protection

portfolio to keep autonomous and connected cars safe from cyberattacks during development and in production.

Karamba Security recently announced it was selected by the Automotive Information Sharing & Analysis Center (Auto-ISAC) Board of Directors to join the Auto-ISAC Strategic Partnership Program to provide members analysis on attack activity and forensics data of such attacks against ECUs.

About Karamba Security
Karamba Security provides industry-leading automotive cybersecurity solutions for autonomous and connected cars. Its Autonomous Security software products, including 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.

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
617.502.4352