Karamba Security and Alpine Demonstrate at CES the Resiliency of In-vehicle Infotainment Systems to Ransomware Attack

BLOOMFIELD HILLS, Mich. And HOD HASHARON, Israel, Jan. 3, 2018 –Karamba Security, the world leader in automotive cyberattack prevention, today announced that Alpine Electronics, Inc. of Japan has selected its software to protect its infotainment systems against hackers in a demonstration that will take place during CES in Las Vegas, Jan. 9 – 12, 2018 in the by-invitation-only section of Alpine's booth at the Las Vegas Convention and World Trade Center (LVCC), North Hall, Meeting Room N102.

The resiliency of an infotainment system to malicious attacks and to ransomware hacks will be shown in the demo of how Karamba software protects against foreign code and buffer overflows. This is an attack vector that can allow attackers to take over connected and autonomous vehicles. Self-driving car ECUs protected by Karamba's Autonomous Security are not vulnerable.

To demonstrate this capability, the companies have introduced a ransomware exploit into the system which locks the system. The demo toggles between a vulnerable system and one with protection applied. The same exploit attempt will fail on the protected browser, and a detailed incident report is sent to Karamba's incident management server. By integrating Karamba's Carwall product, Alpine and Karamba assure that the infotainment system is resilient to such attempts to hack the system. The attack allows full remote code execution either to lock the device or to compromise it and send malicious commands to the car's safety systems, such as change the steering wheel while driving, or disable brakes.

Another interesting point is that in recent attacks such as BlueBorne, researchers were able to bypass a common defense method, memory address space layout randomization (ASLR), by exploiting the inherent weaknesses of the ASLR technology and by exploiting other information leak vulnerabilities.

As explained by the Karamba Security researchers, the best protection against buffer overflow and dropper type vulnerabilities is to harden the code in the components used in devices according to their factory settings, thus preventing the execution of any foreign code, which is the malware.

Karamba's Autonomous Security would prevent attacks, such as the BlueBorne Bluetooth flaws, and any other buffer overflow, whether known or unknown, by blocking the execution of foreign, malicious code at the component level.

This is just another example of why hardening sensors and electronic components according to factory settings is the only strategy that's going to prevent an attack. Karamba's software automatically hardens a car's electronic control units (ECUs), preventing hackers from compromising those ECUs and hacking into the car.

Alpine's selection was made after extensive evaluation of Karamba's solution.

Karamba will be at CES® 2018 to showcase its capabilities working with leaders in the global automotive supply chain. From its suite at the Bellagio Hotel, Karamba will conduct joint demonstrations with partners who include Honeywell, IAV, Alpine and FEV to engage with conference-goers on cybersecurity vulnerabilities and how organizations can work together to secure the automotive industry. To schedule a private demo email: ces@karambasecurity.com.

More information is available at www.karambasecurity.com.

Resources
Autonomous Security
Karamba Security Approach

About Karamba Security
Karamba Security provides industry-leading cybersecurity solutions for connected and autonomous vehicles. Its SafeCAN and Carwall software provide end-to-end in-vehicle security by authenticating communications, including OTA updates, with zero network overhead and by hardening the car's safety ECUs from attempts to manipulate or compromise their commands and hack into the car. Together, the products prevent cyberattacks with zero false positives, no connectivity requirements and negligible performance impact. In one year, Karamba has engaged with 16 OEM and tier-1 customers, received a total investment of $17 million. The company has been recognized in 2017 with TU-Automotive's Best Cybersecurity Product/Service and the North American Frost & Sullivan Award for Automotive New Product Innovation. More information is available at www.karambasecurity.com.

About Alpine Electronics
Alpine Electronics is an automotive electronics manufacturer that provides consumers and leading auto makers with audio, video, navigation and driver assistance products. The company specializes in system integration solutions with innovative vehicle entertainment and information technologies. Alpine's R&D and manufacturing facilities in Japan, China, Europe and North America ensure that all products address the real world requirements of drivers in each market. The company is committed to developing safe, comfortable and eco-friendly automotive electronics products. www.alpine.com.

Media Contact
Montner Tech PR
Deb Montner
dmontner@montner.com
203-226-9290 x110