Karamba Security Would Block Newly Reported Jeep Cherokee Attack if Performed Remotely by Malicious, Black Hat Hackers

Black Hat—LAS VEGAS, Aug. 04, 2016 (GLOBE NEWSWIRE) -- Karamba Security's Carwall would have blocked the Jeep Cherokee hack being presented by researchers Charlie Miller and Chris Valasek at Black Hat today, if it were conducted remotely by actual malicious hackers.

WIRED reported that this latest attack is, well, wired—as in a physical intrusion—unlike last year's remote wireless attack. In this case, Miller and Valasek directly plugged a laptop into the vehicle's CAN network through a port beneath the dashboard.

As told to WIRED, "Instead of merely compromising one of the so-called electronic control units or ECUs on a target car's CAN network and using it to spoof messages to the car's steering or brakes, they also attacked the ECU that sends legitimate commands to those components, which would otherwise contradict their malicious commands and prevent their attack." They then demonstrated how to physically gain control over and manipulate the Jeep's steering, braking and acceleration systems.

The attack skipped the remote access phase altogether and physically connected to the CAN bus. While Miller and Valasek's CAN message injection demonstration represents a valid risk, it is an unlikely scenario in the real world because hackers would need to be physically present by the car or in the car to successfully carry out the attack.

A realistic scenario is for hackers to compromise the car's externally connected ECUs communicating wirelessly and use them to exploit capabilities available via the bus. In this real-world scenario, Karamba Security Carwall would detect those hacking attempts and block them from compromising the externally connected ECUs, preventing the hacker from reaching the bus.

"More than anything else, this presentation demonstrates that protecting at the bus level is too late, and to prevent these hacks, we must block the ability to gain access to the bus," said David Barzilai, Karamba Security's chairman and co-founder.

"Karamba Security's Carwall software hardens the car controllers according to factory settings," said Barzilai. "When Chris and Charlie, or any other cyber hacker, wish to attack the car remotely (and not by connecting their laptop physically to the car's CAN bus), they must compromise one of the car's externally connected controllers and run operations or files that are not part of factory settings. Carwall inspects the controllers in real time, detecting and blocking such operations from running."

"The bottom line is, to actually perform a cyberattack on the car, you must compromise one of the externally connected controllers. Carwall detects and blocks such hacks at the controller level, keeping the car safe," Barzilai concluded.

In June, Karamba Security was selected by Forbes Israel as one of Israel's Top 10 Most Promising Cybersecurity Companies— a distinction made even more significant in a nation with more cyber companies per capita than anywhere in the world, and having only exited stealth two months earlier, in April 2016.

About Karamba Security
Karamba Security is a pioneer in electronic control unit (ECU) endpoint security to protect the connected car. The company seals and secures the ECUs within automobiles to detect and protect them from cyberattacks and ensure the car's safe, ongoing operations. To learn more, please visit www.karambasecurity.com.

Media Contact
Montner Tech PR
Deb Montner
+1-203-226-9290 x110
dmontner@montner.com