COALFIRE LABS

CASE STUDY

Vulnerable to the hack

AT A GLANCE

To keep up with consumer expectations, automotive industry innovation is expanding from Detroit to Silicon Valley. Cars are now more than mere vehicles; they are mobile computers with a growing reliance on connectivity. Many of today's automobiles feature advanced electronic systems that share information with cloud solutions and put a smartphone at the center of the automotive user interface. But with every additional link comes a larger threat landscape, and therefore, increased risk. In this new reality, automobile security has gone high tech as well.

CLIENT CHALLENGE

For one major manufacturer, the system security of a new electric vehicle was a top priority. The vehicle's web and mobile platforms were designed to provide drivers with a convenient and easy-to-use interface to monitor and manage the eco-friendly car. While the development team knew the vehicle's platforms worked perfectly from a performance standpoint, they paused the development program to ensure the systems were not exposed to outside interference. They wanted to uncover any unknown vulnerabilities that might put the driver or the vehicle at risk.

APPROACH

Coalfire was retained to run a series of penetration testing scenarios, including specific tests focused on the mobile application programming interface (API) and the telematics control unit. Using the credentials from a test account, Coalfire pivoted outside of an assigned environment and was able to take control of other vehicles using only the VIN. By exploiting vulnerabilities discovered in hidden and undocumented interfaces, Coalfire was able to harness GPS functions to locate cars, lock and unlock vehicles, and perform other malicious tasks.

RESULTS

Coalfire provided specific technical recommendations to mitigate the risks identified during testing. Several third-party components

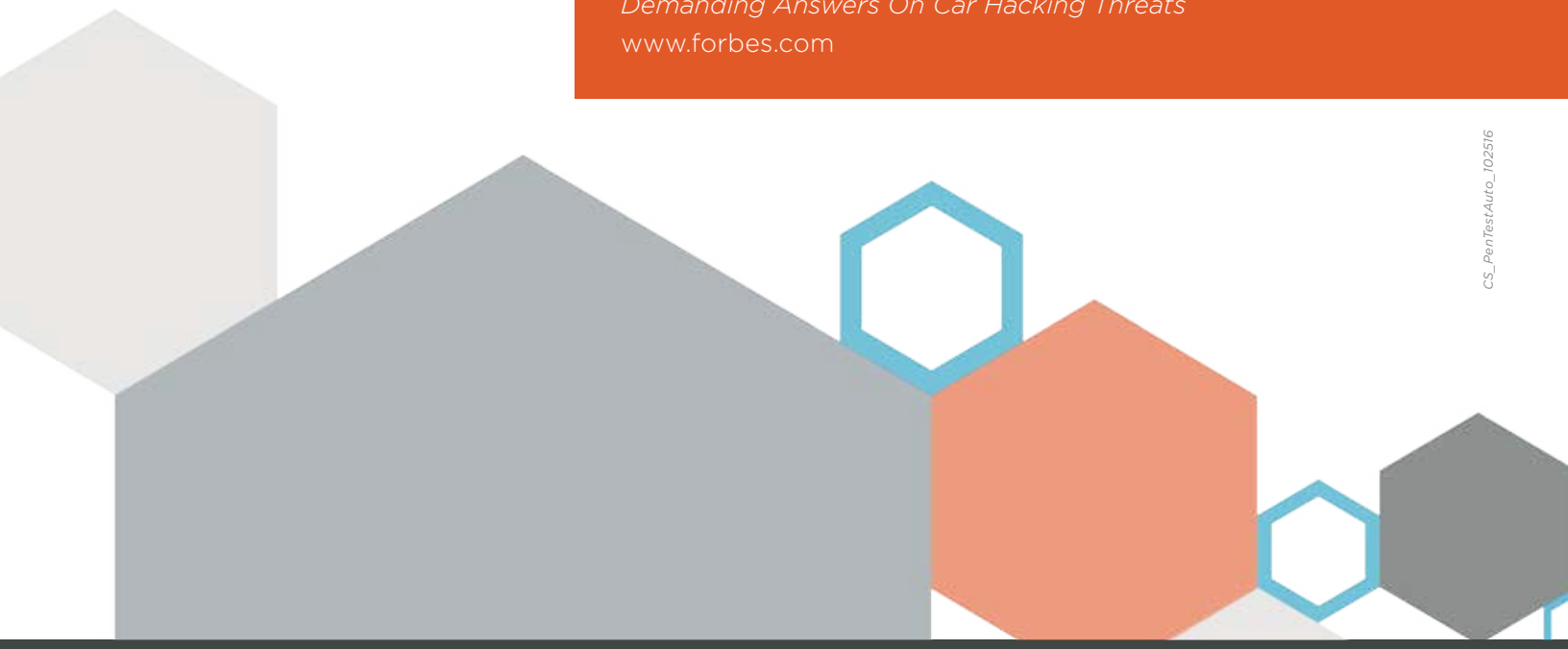
were found to have critical issues. Coalfire and the manufacturer collaborated with the third-party firm to patch the API, protect GPS coordinates, and enforce appropriate permissions across the solution. The software was updated and deployed, protecting the automobile manufacturer and millions of drivers worldwide.

"Our focus, and that of the entire automotive industry, is to prevent hacking into a vehicle's by-wire control system from a remote/wireless device outside of the vehicle."

TOYOTA SPOKESPERSON
Car Hackers Use Laptop To Control Standard Car
www.bbc.com

"As vehicles become more integrated with wireless technology, there are more avenues through which a hacker could introduce malicious code, and more avenues through which a driver's basic right to privacy can be compromised..."

SENATOR EDWARD MARKEY
Here's The Letter A Senator Sent To 20 Auto Makers Demanding Answers On Car Hacking Threats
www.forbes.com



CS_PenTestAuto_102516

About Coalfire

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client's specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. **www.coalfire.com**

COALFIRE