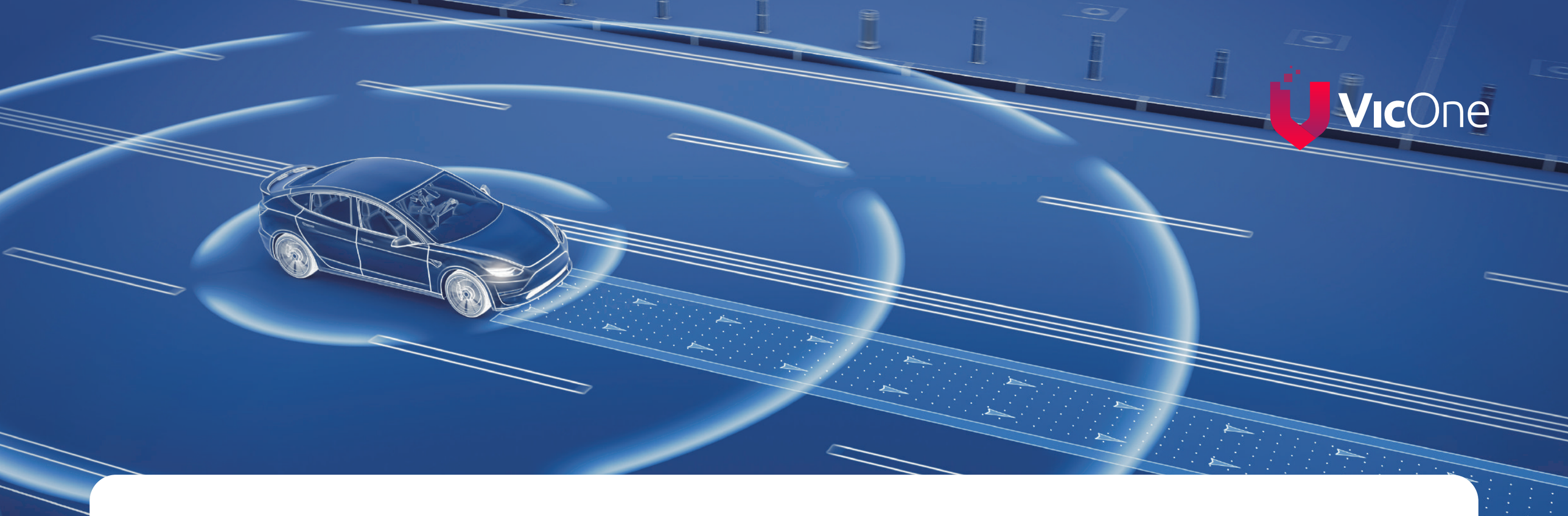
VicOne

USE CASE

Detecting Electronic Power Steering ECU Firmware Modification



Bypassing Lane Keeping Assist System restrictions to control a steering wheel

Lane Keeping Assist System (LKAS) helps steer you back to the marked lane if you stray away to prevent accidents caused by fatigue or distraction. In January 2022, an ethical hacker posted an article that explains how he modified the firmware of an Electronic Power Steering (EPS) ECU from a 2010 Volkswagen Golf Mk6 in order to use LKAS without restrictions.

How it's done

1. The hacker obtained the ECU of interest through its part number and established diagnostic communication with the ECU. Although the engineer mode is password protected, it can be accessed using a brute-force attack.

2. The hacker downloaded an update file containing the firmware he wanted to modify and reverse engineered the firmware to remove the restrictions of enabling LKAS: a six-minute timer of checking the steering wheel torque and a minimum speed of 50 km per hour. The relevant checksum in the firmware was also updated to pass the integrity check for data corruption.

3. In the end, the hacker successfully flashed the firmware back to an actual car, allowing him to take control of the steering wheel and use LKAS at any time.

How can VicOne help?

From the hacking journey, we learned that the researcher was able to make modifications to the firmware of an EPS ECU. In this section, we describe how VicOne xNexus can detect and alert manufacturers of these events.

- **xNexus detects unusual activity through vehicle profile comparison.**

  Although the specification of LKAS varies with the manufacturer, xNexus uses machine learning technology to compare vehicle profile and identify abnormal activity. In this use case, xNexus can detect the following issues: The vehicle has turned on LKAS but was driving below 50 km per hour, and the six-minute timer of checking the steering wheel torque has been disabled.

  After detecting abnormal activity, xNexus checks for modifications to the ECU configuration profile, looks up any connection event to the OBD-II port, and verifies if the firmware version matches the vehicle's current profile.

  xNexus can also detect more in-depth changes to the ECU firmware, such as the number of password retries, firmware integrity check, and firmware flashing, to help manufacturers identify the root cause more effectively.

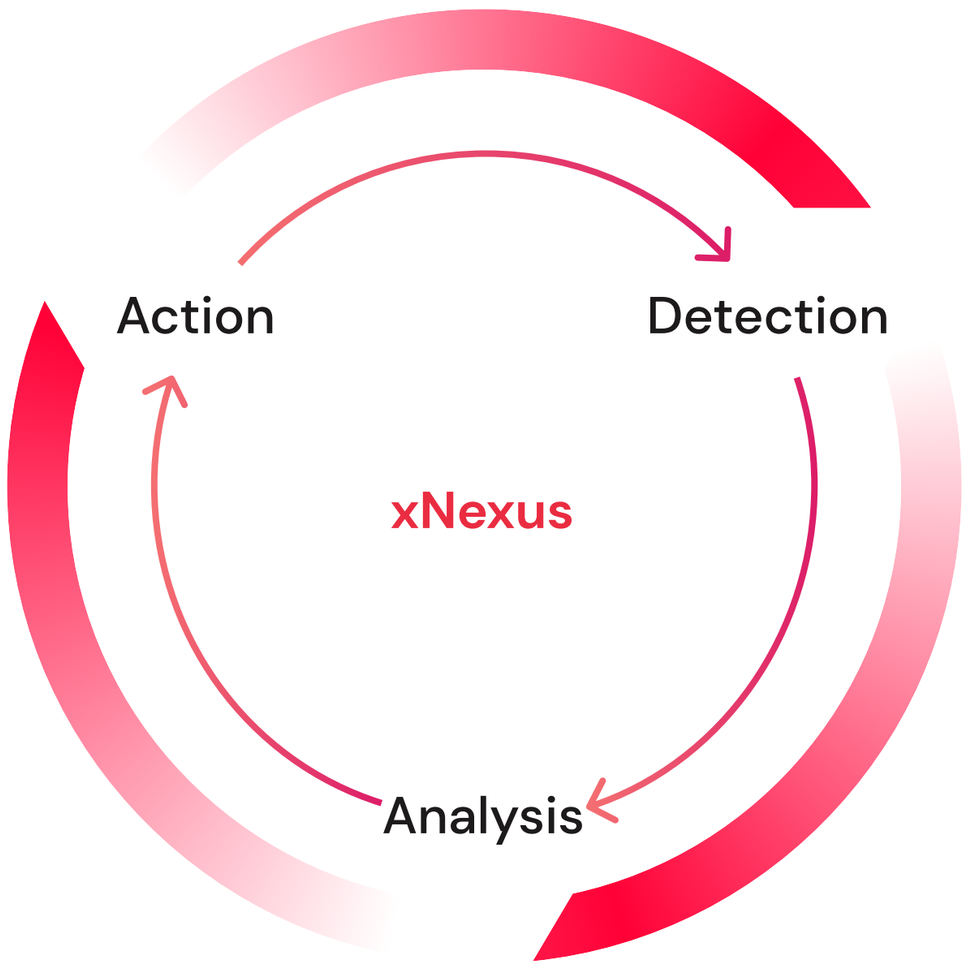
- **xNexus displays consolidated findings and violation alerts.**

  Manufacturers can use the information in further investigations to determine if the vehicle has been hacked, or if the modifications were due to a software upgrade through a third-party vendor.

  xNexus can map the identified activity to the VicOne Automotive Attack Matrix (inspired by MITRE ATT&CK®), which outlines tactics and techniques commonly used in automotive cyberattacks. In this use case, understanding the brute-force attack technique helps manufacturers consider securing the ECU by design, such as having stronger ECU authentication.

About VicOne Automotive Security

Our Automotive Security team offers comprehensive protection against cyberattacks targeting connected vehicles through xNexus, a cloud-based vehicle security operation center (VSOC). By leveraging extended detection and response (XDR) capabilities, automotive threat intelligence, OEM data, and xCarbon in-vehicle sensors, xNexus ensures compliance with UN Regulation No. 155 (UN R155), maps threats to the ATT&CK Matrix, highlights threats applicable to automotive cyberattacks, and keeps up with the latest automotive cybersecurity incidents.



Detection

Receives data or security notifications from various sources

Analysis

Conducts broad-spectrum correlation analysis of threats

Action

Visualizes analysis results in a unified view to assist in further investigations or mitigation

For more information:

Website:

https://www.vicone.com/

Contact:

https://www.vicone.com/contact-us