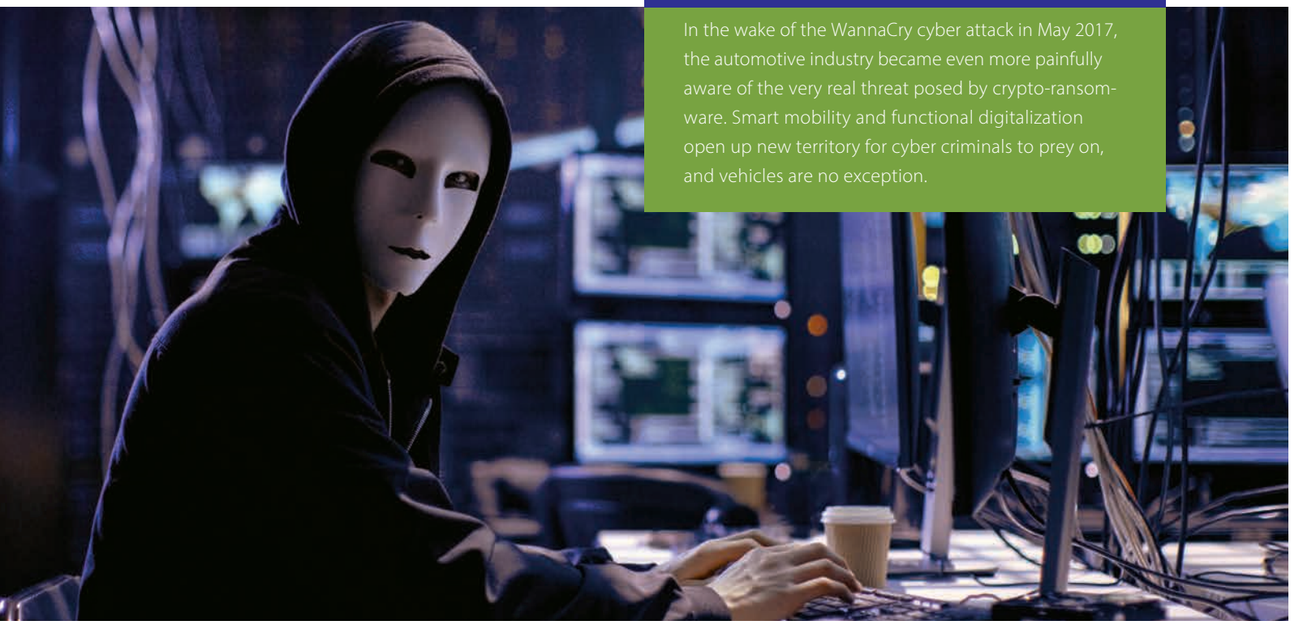
Dashboard demand for ransom payment

WannaDrive? Holistic IT security helps combat automotive ransomware

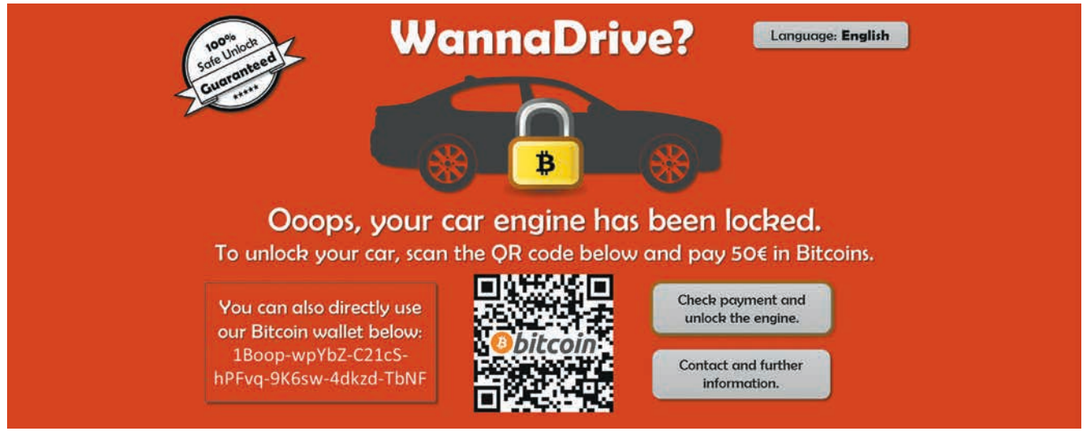


In the wake of the WannaCry cyber attack in May 2017, the automotive industry became even more painfully aware of the very real threat posed by crypto-ransomware. Smart mobility and functional digitalization open up new territory for cyber criminals to prey on, and vehicles are no exception.

Commercial vehicles and vehicle fleets are high on the list of targets for online extortionists. Potential victims include trucks transporting perishable goods on tight delivery schedules, bus companies, rental car fleets, car-sharing pools, expensive construction machinery, and special-purpose vehicles, to name just a few examples. If cyber attackers succeed in taking these vehicles as digital hostages using ransomware, their chances of coming away with the cash are pretty high.

Ransomware attacks take little effort to orchestrate

Although there are no known cases of ransomware attacks on vehicles to date, a look at real-world examples from other sectors make it easy to conceive a likely attack scenario. Cyber criminals usually rely on a ready-to-use ransomware kit or ransomware-as-a-service solutions, which include bot masters and bitcoin payment systems. Ransomware kits have thus far primarily targeted conventional desktop PCs and servers. But with the number of vehicles open to such attacks and fleet operators' vulnerability to extortion in the connected network increasing, ransomware variants for Automotive Linux or AUTOSAR will inevitably start to appear. There are already numerous potential access points for ransomware. Examples include infotainment systems that retrieve online content; in-vehicle reception of communications (such as emails, text messages, instant messenger services, digital radio); smartphones or navigation systems that are connected to a port in the vehicle; firmware updates over-the-air (FOTA); and cloud services or remote diagnostics from the vehicle manufacturer.



If ransomware successfully hijacks the system, it proves extremely difficult to free the car, a digital hostage, from the hands of the cyber criminals

Security engineers from ESCRYPT were able to simulate a ransomware attack using a test model. They took a Raspberry Pi computer running Linux OS and a touchscreen as the automotive infotainment system. The next step was to connect these to a genuine speedometer control unit with OEM firmware using a gateway ECU and a proprietary bus network – as would be the case in a normal vehicle. They subsequently exploited a USB port to "infect" the Raspberry Pi, or host ECU, with Python-based ransomware. As intended, the ransomware client then locked the speedometer and set it to display the top speed at all times. At the same time, a demand for a ransom payment to an anonymous bitcoin account flashed up on the infotainment system's touchscreen (see Figure). The ESCRYPT experts concluded that ransomware attacks on vehicles are easy to execute and pose a real threat – if IT security is not continuously upgraded to address the increasing connectivity of motor vehicles.

Holistic security approach prevents attacks from the outset

Despite their numerous vulnerabilities to attacks, vehicles on the road today often fail to provide backup for important data and functionalities. Nor do they receive regular security updates. What's more, most of today's vehicles have only very basic (gateway) firewalls and rarely feature automatic intrusion detection and prevention systems (IDPS) that provide proper protection. Upgrading these vehicles is usually difficult and costly. The most effective way to protect vehicle IT systems against ransomware and other forms of cyber attack lies in automotive manufacturers integrating comprehensive and effective information security into the development of their vehicle platforms from the outset. An all-encompassing security approach should address the entire vehicle system from end to end – including its IT infrastructure and the entire life cycle of the vehicle until it is scrapped. It should also cover the complete spectrum of organizational aspects such as defined security processes and security governance.

The comprehensive protection of vehicles therefore necessitates a series of interconnected security measures. In vehicles themselves, embedded security components can help defend against hacker attacks and malware with known signatures. Moreover, an intrusion detection and prevention system (IDPS) can detect and shut down critical anomalies in onboard network communications – including ransomware attacks. This can be achieved within the vehicle itself. Alternatively, a connected cyber security operations center (SOC) in the backend can distribute security updates to an entire fleet of vehicles to counteract a newly detected hacking pattern. But what if a ransomware attack succeeds? In such a case, the victim needs to respond quickly and effectively. A pre-defined incident response procedure, for example, can be used to specify countermeasures, one of which might even be payment of the ransom demand as a last resort in an emergency.

One thing is for sure: the potential threat that ransomware poses to vehicles calls for effective, end-to-end security – and this should not be seen as a costly burden, but rather as a key factor for success. After all, this security gives fleet operators and vehicle manufacturers the protection they need to ward off online blackmailers, and prevent product recalls and claims for damages. ■

Author

Dr.-Ing. Marko Wolf is Head of Consulting & Engineering at **ESCRYPT**.