FD-2023-CS-0011

FLEET DEFENDER • ON-BOARD INTRUSION DETECTION

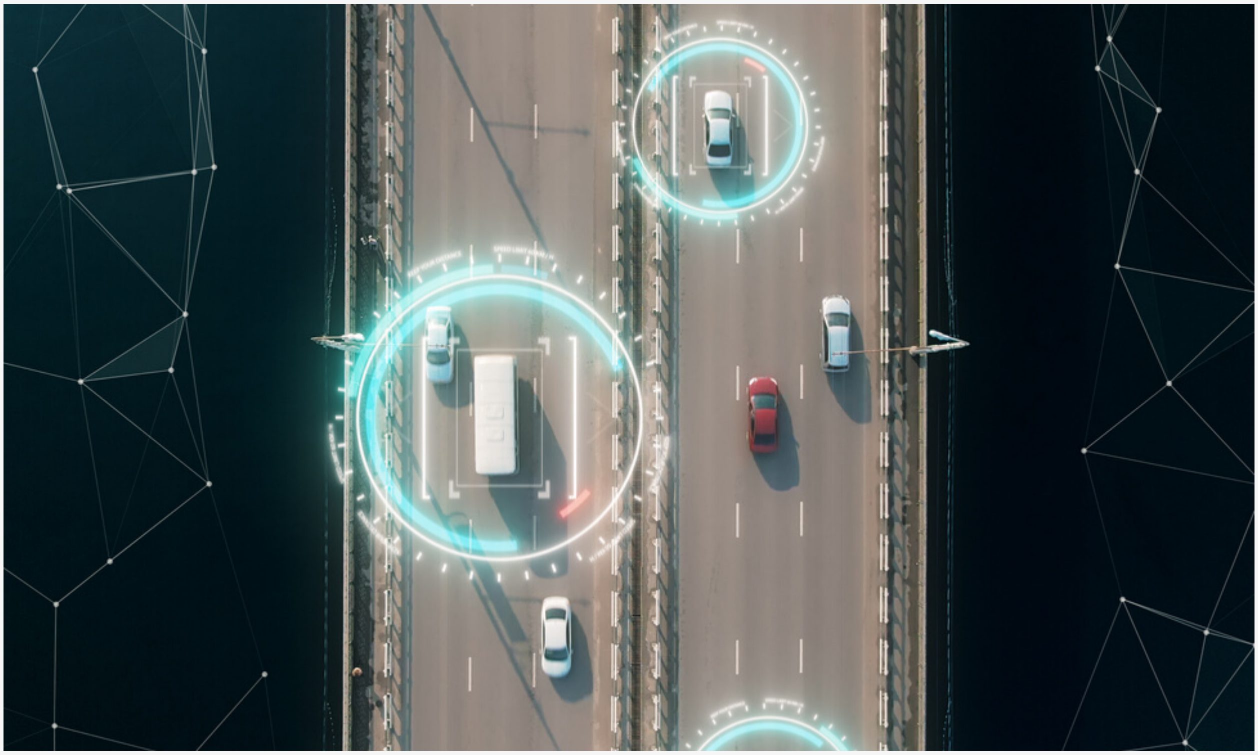
USE CASE

PROTECTING TRUCKS FROM REMOTE RANSOMWARE ATTACK

PREPARED AND PRESENTED BY

FLEET DEFENDER, INC.

A LOOK AT THE REMOTE ATTACK POSSIBILITIES ON OPERATIONAL TECHNOLOGY



INTRODUCTION

Trucks are a critical OT (Operational Technology) component of the global supply chain. These machines are now complex, interconnected systems with vulnerable digital infrastructures. As hackers refine their craft, they're setting their sights on OT devices and employing innovative ways to exploit cybersecurity weaknesses.

THE WORLD TAKES NOTICE

In the past few years we have seen regulations from the United Nations including United Nations Regulation Number 155 (R155): Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. This as well as ISO/SAE 21434 have become cornerstones for creating more robust vehicle cybersecurity at the OEM level.

RANSOMWARE RISK FOR FLEETS

The risks facing trucks today go beyond traditional vehicle and cargo theft — attackers can hijack the very digital systems that govern a trucks operation, turning a company's assets against itself in a high-stakes ransom game.

UKRAINIAN TRACTORS SHOW ATTACK POSSIBILITIES

In February 2022 Russian troops occupied and looted the city of Melitopol. Included in their looting was millions of dollars of John Deere farm equipment which were later transported to Chechnya. Tractors like John Deere utilize ISO 11783, a version of CAN based on SAE J1939 which is used in heavy duty vehicles. Ukrainian hackers were able to remotely disable the tractors making them unusable.

While this story is a win for the Ukrainians in their fight against Russia, it shines a light on the possible when it comes to remotely attacking heavy equipment. How could a hack like this affect the long-haul logistics space? Trucks and Tractors are similar in their use of a CAN protocol and external connections via GPS, bluetooth, and cellular networks. They have remote access which for bad actors, means attack vectors. Below is an outline of how trucks can be hacked remotely and held for ransom.

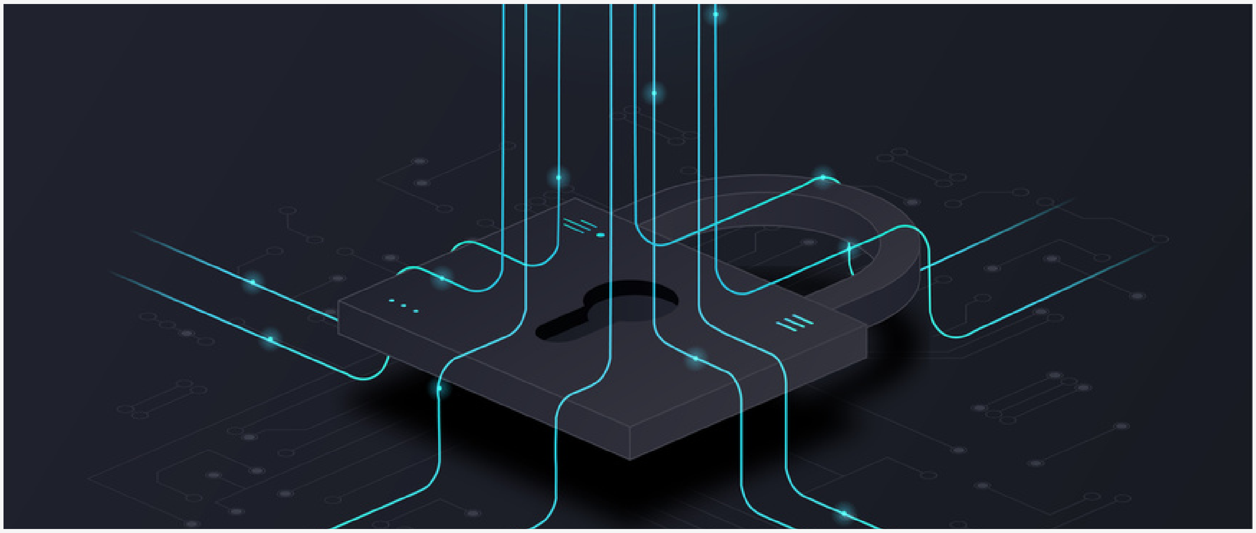
REMOTE ATTACK TO RANSOMWARE A TRUCK OR TELEMATICS SYSTEM

For this cyber kill chain, we are looking at the research conducted by Red Balloon Security whose research was focused on embedded systems. For modern vehicles, the ECUs that make up the nervous system are embedded systems. The kill chain for OT/ICS (industrial control system) can be weaponized against an embedded system in a vehicle.

UN REGULATION NO. 155

UN Regulation No. 155 (R155) relates to cybersecurity and cyber security management systems for road vehicles. Developed under the United Nations Economic Commission for Europe (UNECE), R155 came into force in mid-2020.

UN R155 requires vehicle manufacturers to establish and maintain a Cybersecurity Management System (CSMS), ensure their vehicles are protected against cyber attacks, and document any efforts taken to identify and mitigate vulnerabilities. The below tactics, techniques, and procedures (TTPs) can be tied to vulnerabilities or attack methods listed in R155. These vulnerabilities and attack methods are noted below.



RANSOMWARE KILL CHAIN

THIS IS AN EXAMPLE OF A CYBER KILL CHAIN TO REMOTELY ACCESS AND CONDUCT A RANSOMWARE ATTACK ON OPERATIONAL TECHNOLOGY SUCH AS HEAVY EQUIPMENT OR LONG-HAUL LOGISTICS VEHICLES

TACTICS, TECHNIQUES, AND PROCEDURES (TTP)	UN R155 VULNERABILITIES AND THREATS
INITIAL ACCESS Accessing a telematics system or infotainment head unit can be accomplished via multiple methods: • Phishing to gain hard-coded factory login credentials. • Hidden services and debugging utilities. • Communication protocol vulnerabilities discovered via fuzzing or static analysis.	**UN R155 4.3.1** Threats regarding back-end servers related to vehicles in the field **UN R155 4.3.2** Threats to vehicles regarding their communication channels

RANSOMWARE KILL CHAIN CONT.

TACTICS, TECHNIQUES, AND PROCEDURES (TTP)	UN R155 VULNERABILITIES AND THREATS
ELEVATING PRIVILEGES Bypass signature protection on the head unit via a memory corruption vulnerability. This provides root access and achieves remote code execution. Constructing an exploit utilizing a protocol parsing vulnerability to gain root access. Inject an arbitrary executable to a partition through a bypassed SMS client in the TCU.	**UN R155 4.3.7** Potential vulnerabilities that could be exploited if not sufficiently protected or hardened
CONDUCTING THE ATTACK Once access and privileges are obtained an attack can be conducted to either brick an embedded system or install malware that makes the vehicle inoperable or a safety risk to operate until a ransom is paid. This includes: 1. Changing access passwords (to prevent firmware update). 2. Accessing a fully privileged shell with credentials modified in the previous step. 3. Downloading additional material to be used in the ransomware. 4. Locating and modifying the protection function parameters. 5. Disabling protection functions. 6. Modifying the LCD screen.	**UN R155 4.3.6** Threats to vehicle data/code

HOW FLEET DEFENDER PROTECTS AGAINST OT RANSOMWARE

ON-BOARD INTRUSION DETECTION FOR UN R155 COMPLIANCE

Monitoring

Fleet Defender utilizes true AI & ML, not rule-based logic, on-platform to monitor CAN traffic for anomalous behavior.

Detection

Fleet Defender's on-board ML detects anomalous CAN traffic in real-time with zero false positives.

Alerting

Once detected the response follows our Threat Matrix to send alerts in-cab and to our Automotive Threat Intelligence and Analysis Center.

Fleet Defender's AI-based intrusion detection and monitoring system (IDS) gives drivers and back office personnel early insight into an attack so corrective action can be taken. Fleet Defender’s IDS ensures compliance with UN Regulation 155 (R155).

Fleet Defender’s technology uses on-board machine learning to detect anomalous behavior in the network traffic or control system data of a platform – including passenger vehicles, trucks, trains, boats, planes, space craft, and more. Our monitoring, detection, and alert system does not need a pre-defined catalog of attacks to alert for a cyber threat. Our proprietary models are able to catch zero-day attacks and because it’s on platform, it can do so in real-time.

Want to see a demonstration of Fleet Defender's AI detection system?

Schedule a Demo Today
www.fleetdefender.com

Contact Us
hello@fleetdefender.com

OPERATE YOUR FLEET PLATFORM ANYWHERE, ANYTIME WITHOUT FEAR OF COMPROMISE.