Ransomware Attack of Fleet Vehicles? Yes, It Could Happen to You

Amundsen Davis Alert
August 3, 2018

The following scenario may sound familiar. It's a busy afternoon, and your operations manager gets a call from a driver. She's stuck in the middle of a highway, and her truck died without warning. Naturally, there's an important shipment deadline fast approaching. Scrambling ensues, and you're speed dialing your typical roadside supports.

Here's what may not sound so familiar—perhaps a scenario you discount as something straight out of Hollywood: the same scenario arises, but as your team's scrambling, the operations manager gets an email. It's a demand for two hundred fifty thousand dollars in bitcoin from an anonymous hacker. If payment isn't received, the truck stays dead.

You may have heard of bitcoin or read about ransomware attacks. But, likely, it's unclear whether this could ever *really* happen to *your* company. Wonder no more: it absolutely could.

Consider the ELD mandate set to go into full effect on December 16, 2019. Meant as a Congressional initiative to increase highway and transportation safety and to help monitor compliance with Hours of Service requirements, these electronic logging devices ("ELDs") will replace paper logbooks. To be in compliance, the new mandate requires all commercial vehicles to have an ELD hardwired into, and synchronized with, the vehicle's engine in order to electronically record driving segments and the driver's Record of Duty Status in real time. Yet, with just this requirement, your fleet's chances of suffering a ransomware attack will only continue to increase.

First, some background. A traditional ransomware attack looks like this: an employee receives what seems to be an innocuous email from a familiar name. He clicks on the attachment and his computer goes haywire. Other employees try to access files for their daily work, but they're prompted for a password, or 'key.' Another email is received wherein some hacker demands a large sum in bitcoin.

What likely happened? A hacker targeted an employee with access to all of the company's files with a phishing email. Opening that email opened a door for the hacker, who had malware at the ready. The hacker then encrypted, or locked-up,

PROFESSIONALS

Molly A. Arranz
Partner

RELATED SERVICES

Cybersecurity & Data Privacy

Transportation & Logistics

the network—and he had the only key.

Vehicle hacking could look very similar because today's vehicles have multiple electronic devices and units—each serving as a potential door to this infiltration. A vehicle's navigation system, communication channels and, now, ELD are all possible entry points.

A hacker need only open one of those multiple doors to access not only the vehicle's data—but possibly, the company's entire system—and to lock everything up. Stated another way, an intrusion into just one truck's system can have a domino effect resulting in cost of time and money for loss of use of the one truck and also, possibly, your company's entire network, which could be rendered inaccessible.

Rather than chalking up this possibility to it-will-never-happen-to-us, there are preventative measures to minimize your risk:

- Keep operating systems updated with the latest software updates
- Install and maintain programs to screen communications (anti-virus, firewalls, etc.)
- Evaluate the level and extent of access to your company's databases and networks that each driver and employee has
- Backup systems and critical data on an **offline** server (to use to restore after wiping impacted systems)
- Train, train, train. Make data security part of your onboarding orientation and regular training so that all employees and drivers learn how to identify and handle suspicious communications and react to ransomware attacks.

Ransomware Attack of Fleet Vehicles? Yes, It Could Happen to You