# How cybercriminals create turbulence for the transportation industry

intel471.com/blog/how-cybercriminals-create-turbulence-for-the-transportation-industry

When you break down how transportation companies actually work, you can find yourself looking at nothing but supply chains. From moving people or goods from one place to another, keeping track of the vehicles that are transporting those people or goods, the third parties that are responsible for the maintenance and operations of those vehicles, along with a list of other business-critical functions, it's easy to see how these companies would need to lean heavily on internet-connected technology in order to be successful.

However, since these companies are so reliant on the internet, they present a juicy target for the cybercrime underground. Transportation companies are constantly in the discussions on criminal forums, with nefarious actors attempting (and some succeeding) to attack companies' infrastructure along their supply chains for their own illegal gains.

Below are just some of the examples Intel 471 has observed when it comes to criminals going after transportation companies.

## Access to Networks

Intel 471 has long tracked criminals who specialize in selling access to compromised systems or stolen information. Some of those we have tracked have used their ability to target transportation companies as a way to stand out in the cybercrime underground. Here are some of the instances we have observed:

> In November 2020, an Iranian-based actor advertised unauthorized access to a system belonging to an Iranian-based airline. The actor shared a demonstration video which looked to be from an internal employee portal, which allowed people to access employee account numbers, national codes, passwords, payments, phone numbers, usernames and more. The advertisement was shared on a popular Telegram channel dedicated to cybercrime, with over 19,000 members.

In January 2021, Intel 471 observed a well-known cybercriminal selling network access to a number of companies they allegedly pulled from malware logs. Among the advertised access was a Citrix Gateway believed to be associated with a large, multinational aviation company. The platform detailed access to another aviation company based in Scandinavia, mainly showcasing programs designed for training. The actor is well-known for selling access to Citrix Gateways on various cybercriminal forums.

Also in January 2021, an actor offered to sell information on a remote code execution (RCE) vulnerability allegedly impacting a European-based cargo airline. The actor sought US $150 for the information about the vulnerability that allegedly could be exploited to exfiltrate several internal documents and access login credentials. The actor further claimed they also uploaded a web shell to the impacted server.

## Gift Cards

Gift cards have long been a staple of the cybercrime underground, utilized by criminals as a way to move money. Whether it be physical cards or solely online credits, numerous transportation companies use gift cards as a way from customers to buy flights. There are actors that have leveraged that ability for their own crimes.

- One actor Intel 471 has tracked has been in the gift card fraud business since at least 2017. The actor, who was previously engaged in selling compromised remote desktop protocol (RDP) credentials, bought ready-to-use gift cards from other actors, derived them from compromised accounts and sourced access from malware logs. The companies the actor expressed interest in included three well-known airlines based in the United States, along with one multinational hotel chain. The actor bought gift cards for half or a quarter of their value.
- Another actor Intel 471 has tracked allegedly claimed to have a large number of digital gift cards issued by three well-known airlines based in the United States for sale each day. The gift cards were not carded using compromised payment cards, but purchased with points from compromised accounts with rewards programs or cash-back services. The actor primarily obtained credentials for such accounts from malware logs purchased on forums.

## Ransomware

Ransomware is a top threat for all internet-connected businesses. The transportation sector is no different.

Intel 471 has observed numerous attacks on transportation-based organizations, including entities in both the public and private sector. These incidents have all the hallmarks of a ransomware-as-a-service attack, with crews “renting” software to launch the attack, hundreds of gigabytes in data stolen, and calls for million-dollar ransom payments.

- In March 2021, the operator or operators behind the NEFILIM ransomware-as-a-service affiliate program claimed the compromise of U.S.-based commercial airline Spirit Airlines, leaking 40GB of data with over 33,000 files. According to open source reporting, Financial data and other personal information of customers who purchased tickets to fly with the airline between 2006 and 2021 were posted on a name-and-shame blog.
- In April 2021, a group using the Mount Locker ransomware attacked the Santa Clara Valley Transportation Authority, stealing about 130 GB of corporate data. The responsible parties are likely an offshoot of those who developed the ransomware, as the organization’s data was posted on a name-and-shame blog operated by a different criminal group. Intel 471 also observed that the criminal crew applied a “double extortion” tactic by calling and threatening the victim’s employees.

## Conclusion

Transportation companies are as dependent on technology as any other company. With that trend likely to keep growing, is it imperative that these companies understand where their weak spots are when it comes to cybersecurity and how the cybercrime underground will exploit them if those weaknesses are left unchecked. Keys to a successful business often rely on the internet, just as cybercriminals rely on it to carry out their crimes. By being proactive in assessing risk and closing vulnerabilities, transportation companies will prevent their technology stacks from being a target for the cybercrime underground.