New Cybercriminal Group Targeting Transportation and Logistics Industry – How to Protect Your Organization

Insights
10.22.25

A new cybercrime threat actor calling itself "Coinbase Cartel" has begun targeting transportation, logistics, and adjacent sectors – and you should act quickly to shore up your defenses. Their model is simple: they steal data at scale and then threaten public release to force payment. This new "leak-only" model represents a major evolution in ransomware, one that exposes businesses to reputational and legal risk without ever locking down their systems. What do you need to know about this new threat and what steps can you take to minimize your chances of suffering an attack?

What is Happening?

Coinbase Cartel surfaced in mid-September as a new cybercriminal group focused exclusively on data exfiltration rather than encryption, marking a strategic shift from traditional ransomware tactics. Investigations by several media sources (see here and here) reveal that the group operates with a "business-like" professionalism, emphasizing staged leaks, evidence packages, and even partnership programs for insiders and other criminals.

The group's initial wave of attacks has focused on transportation and logistics businesses, with confirmed or claimed victims spanning several continents.

In one high-profile case from last month, Japanese IT company NTT Data was listed on Coinbase Cartel's darknet leak site. The company denied confirmed data leakage and suggested the breach may have actually involved Vectorform, a US subsidiary acquired in 2022.

Coinbase Cartel's modus operandi relies on:

- Exploiting exposed or hard-coded credentials in cloud or source code repositories (e.g., AWS, Bitbucket, GitHub).
- Using insider-assisted access or weak segmentation to reach sensitive systems.
- Conducting staged data leaks to apply pressure during negotiations.
- Advertising for "strategic collaboration opportunities" with people who have legitimate access to corporate systems – effectively crowdsourcing insider threats.

Because the group does not encrypt files or disrupt operations, companies can continue functioning normally even as stolen data is weaponized against them. This stealthier model means victims may not realize a breach has occurred until extortion threats appear publicly.

Why Transportation and Logistics Are Prime Targets

The transportation and logistics industry has become a top target because it handles high-value operational and shipment data, often shared through complex supply chains of brokers, carriers, and IT vendors.

- Many organizations rely on integrated Transportation Management Systems (TMS), Warehouse Management Systems (WMS), and EDI links, which can serve as soft entry points for attackers.
- The need for constant uptime makes companies more likely to pay quickly to avoid reputational fallout.
- The industry's reliance on third-party vendors – from customs agents to 3PLs – creates a wide attack surface and multiple potential points of compromise.

What Steps Can You Take?

The good news is that there are some proactive steps your company can take to reduce your threat exposure.

1. Reduce the Blast Radius: Limit how much damage attackers can do if they gain access. Make sure employees and vendors only have the access they truly need. The fewer people with administrative privileges, the better.

- Enforce least privilege for TMS, WMS, EDI, and brokerage systems.
- Require phishing-resistant multi-factor authentication (MFA), and disable legacy email protocols (IMAP/POP3) that bypass MFA.

2. Block Easy Exfiltration: Prevent data from walking out the virtual door. Set up alerts and restrictions so sensitive files can't be mass-downloaded or emailed externally without authorization.

- Implement Data Loss Prevention (DLP) controls for Microsoft 365, Google Drive, and email platforms.
- Monitor and block mass downloads using service and integration accounts, and consider behavioral analytics to flag anomalies.

3. See the Real Signals: Spot the subtle signs of compromise before data leaves your network. Watch for red flags like sudden creation of large ZIP files or automatic email forwarding rules.

- Configure alerts for mailbox forwarding rules, suspicious OAuth grants, and bulk compression activities.
- Ensure Endpoint Detection and Response (EDR) coverage includes administrative and remote management hosts.

4. Strengthen Contracts: Hold your vendors and service providers to higher cybersecurity standards. Make sure contracts require prompt breach notification and data-handling transparency.

- Add clauses mandating 24-hour incident notice, log retention, evidence preservation, and minimum telemetry obligations for 3PLs, brokers, customs agents, and IT providers.

What Can FP's Data Protection and Cybersecurity Team Can Do For Your Organization

Our Data Protection and Cybersecurity team helps companies prepare for, respond to, and recover from leak-only extortion campaigns.

- **Rapid readiness review** – Evaluate your current exposure to data-only extortion and identify immediate defensive gaps.
- **Contract uplift** – Update vendor and carrier agreements to add breach notification, logging, and cooperation duties.
- **Incident response counsel** – Provide privileged coordination with regulators, law enforcement, and affected customers.
- **Industry-specific tabletop exercises** – Simulate attacks involving freight operations, service disruptions, and sensitive shipment data to improve resilience.

Conclusion

Make sure you are subscribed to Fisher Phillips' Insight system to get the most up-to-date information directly to your inbox. If you have questions, contact your Fisher Phillips attorney, the author of this Insight, or any attorney on our Transportation and Supply Chain Industry Team or our Data Protection and Cybersecurity team.

Related People

Daniel Pepper, CIPP/US
Partner
303.218.3661
Email

Service Focus

Privacy and Cyber

Data Protection and Cybersecurity

Industry Focus

Transportation and Supply Chain