S&P Journal of Commerce

Ocean carriers guarding their digital gates as visibility requests increase

Some carriers offer logistics providers and visibility vendors access to container status milestones via a paid monthly subscription. Photo credit: GreenOak / Shutterstock.com.

Eric Johnson, Senior Technology Editor | Jun 13, 2023, 12:03 PM EDT

Ocean carriers are aggressively preventing software vendors and third-party logistics providers (3PLs) from scraping container milestone data from their websites as demand for visibility continues to grow.

A number of visibility and shipment management software vendors told the *Journal of Commerce* that carriers are seeking to make it harder for those vendors to web scrape for status information, forcing vendors to create direct feeds with carriers or use carriers' application programming interfaces (APIs).

"Most of the carriers use some form of anti-bot managers," Akshay Dodeja, CEO of visibility provider Terminal49, told the *Journal of Commerce*. Those anti-bot programs,

such as Cloudfare and Akamai, detect scraping programs and prevent them from accessing the contents of a website.

"This is a moving target, and it's a cat-and-mouse game," Dodeja said. "It got worse during COVID when the volumes were high and there was more congestion. It makes it really challenging to monitor container milestone changes programmatically, especially for anyone who manages more than a few containers a month."

Attempts to access data from carrier websites come amid a long-simmering debate over whether container lines are owners or merely custodians of shipment information related to the cargo they move.

"We're not trying to resell the carriers' data," the chief information officer at one 3PL, who did not want to be identified, told the *Journal of Commerce.* "We're trying to give their own customers data about their shipments. But I get it, everybody and their mom is trying to scrape."

Most of a handful of carriers contacted by the *Journal of Commerce* didn't immediately respond to requests for comment on whether they are intentionally blocking third parties from accessing container status data on their websites.

But one, who did not want to be identified, said that virtually every carrier deploys programs to protect their sites, especially if they see specific third parties making several hundred or thousand hits per day in an attempt to scrape.

Pandemic drove more data requests

The more robust defenses are, in some sense, a defense against the number of data requests carriers' websites now receive on a continuous basis. With the proliferation of visibility vendors in the market over the past decade — both standalone providers and 3PLs offering visibility tools — container lines are essentially being asked dozens of times to provide information for the same status events.

The situation gets even more complicated when a large shipper with leverage asks a container line to create a direct feed with the shipper's visibility vendor of choice, forcing uneasy relationships between third-party companies that are seen by carriers to be monetizing carrier or shipper data.

Some carriers, in turn, are charging vendors a monthly fee — in the neighborhood of $1,700 per month — to subscribe to an API that gives them access to a certain number of container status "requests" monthly. Other carriers offer their API free to shippers but charge a "nominal" fee to third-party visibility providers, sources told the *Journal of Commerce.*

“The carriers were never really happy about [their websites being pinged for container status] because it is indecipherable from a denial-of-service attack,” said Bryn Heimbeck, CEO of Trade Tech, a logistics management software vendor. “A server you don’t know keeps running queries against your system. More and more of these online tracking, booking, and spot rates requests are login/password-protected and carriers are not giving this out to software companies.”

Heimbeck said Trade Tech has been able to secure electronic integrations with most of the major container lines and some smaller intra-Asia carriers by leveraging a customer’s need with a specific carrier.

“The days of having to go through a portal are numbered,” he said.

Different approaches among carriers

While all carriers are using tools to prevent scraping, including barriers such as captchas or bot detection and mitigation services, certain ones are being more aggressive than others.

“Usually, the less innovative carriers with poorer track and trace capability are the first to implement these, with no alternatives such as API or even [electronic data interchange] connections, being offered in place to customers,” said Tyler Hughes, chief technology officer at visibility provider Vizion.

Hughes said Vizion has focused on building API connections with carriers and terminals.

“But in other cases, we get our hands dirty and build out advanced crawlers that are able to bypass these checks,” he said. “Scrapers still play a role for our operations but more often as a fallback, as we've been able to uncover better and more well-hidden sources for data in carriers' underlying architecture.”

The CIO at the US-based 3PL said his company focuses on scraping behavior that doesn’t seem “too bot-like.” “We use a proxy to buy IP addresses and intelligence to ‘act like a human,’” he said. “And we make sure to ping the system intermittently.”

The 3PL uses a mixture of its own scraping and data from multiple visibility providers.

“We have a full-time person managing scrapes and we have all these analytics telling us how they’re performing,” the source said. “We’re also hitting the carrier APIs behind the scenes. The carriers are all recognizing it’s better to expose the data through APIs than having people blowing up their sites with status event requests.”

The impetus on getting the data has also changed, the 3PL CIO said, with the volume of status event requests rising as customer expectations for real-time visibility increase.

"Customers are expecting us to have 100% of the data," the CIO said. "It's on us. In the past we'd score the carriers for our customers. [For example] 'this carrier is only sending us 70% of the data.' Now, we say, we'll worry about how to get them the data."

The 3PL said carriers do respond when a large customer mandates the carrier create a direct data feed, but the terms of engagement are different in the mid-market, where most of his customers sit.

"The biggest challenge is on the [non-vessel-operating common carrier] side, because the shipper needs to give us the master bill of lading number and the container number," the CIO said. "We need those numbers to get events on the carrier websites because the carriers won't give us data off the NVO's house bill of lading. The APIs make a big difference because then I can get any milestone. We work with 200 NVOs and I'm not going to build EDI connectivity with 200 NVOs."

Contact Eric Johnson at eric.johnson@spglobal.com and follow him on Twitter: @LogTechEric.