Dark Arts: Why some OTAs fool hotels with fake prices

It's well known that major hotel chains routinely check the rates being offered for their properties through online travel agencies (OTAs). The information helps hotels decide which rates to set on their own branded websites.
What's less well known is how and why some OTAs feed hotels false rates.

Malgorithms

OTAs use rate-scanning bots to "identify the rate spy software and feed it false information, to manipulate the rival's decision-making without busting it openly," said Roman Peskin, vice president of hospitality consulting at custom software shop DataArt.
An OTA knows that if it catches a bot scraping its rates and stops it from scraping, the "other side" will know that it has been caught, said Peskin. The other side might make efforts to enhance and cloak the scraping bot to elude detection.
Feeding a mix of false and true rates is more effective.

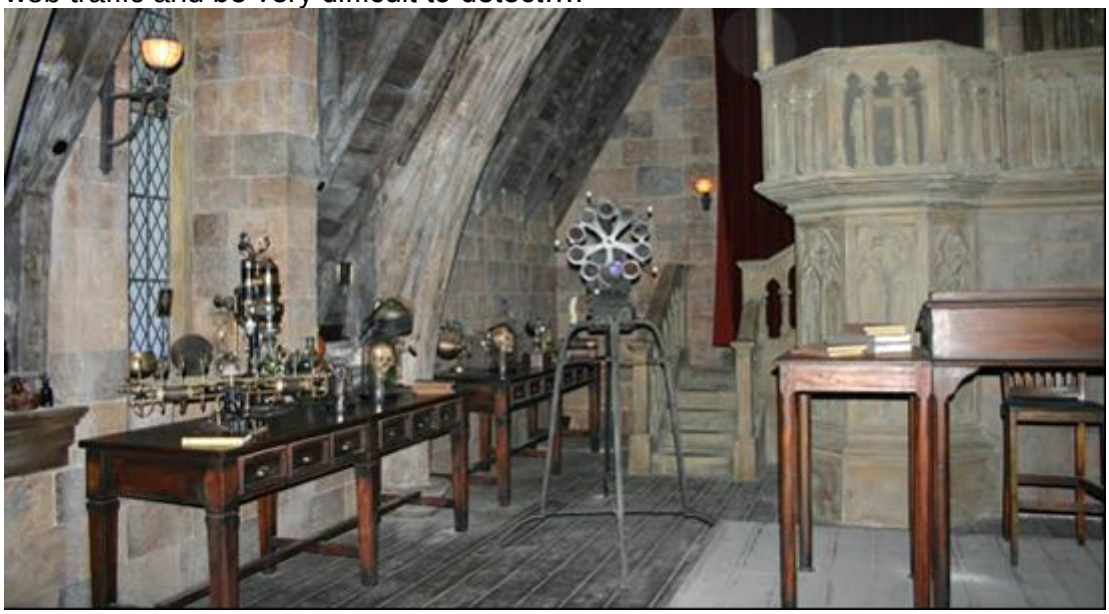
Counter-intelligence effort

Robert Cole of the consultancy RockCheetah agreed that the practice is happening:
"It is relatively simple to add some special code to return invalid rates or inventory – ideally, intermixing bad data with good data, so the bot owner wastes time and money trying to figure out why their data is bad.
Plus, messing with them is much more fun."
Patrick Landman, CEO of hotel management company Xotels, said:
"It's an emerging field, but it's very difficult to detect sophisticated bots since they can mimic a real user by going slowly and changing the identifying Internet Protocol (IP) addresses. This will be a tech battle that will play out over the next few years."

With feeds like these, who needs enemies?

Cole added context in an email interview:
"The scanning of published retail rates is fairly basic – and widespread. Using advanced methods to collect information on private rates and inventory management policies a much different adventure….
The key issue here is unauthorized screen-scraping processes that are typically forbidden by a website's terms of service (not just for OTAs, but also for airlines, hotels, car rental, cruise lines, etc.)….
Some price comparison bots can be exceptionally aggressive – especially those that are checking for pricing variations based on day of arrival and length of stay by room category, rate plan and party size over extended booking and stay windows.
A single arrival date could be searched for 1, 2, 3 and up to 14 day lengths of stay – normally requiring 14 different searches.
The next question is what range of dates are being scanned? The next 90 days, perhaps? Capturing up to a 14-day length of stay would trigger 1,260 queries.
As hotel rates may be changed multiple times throughout the day, some competitive scans may take place several times per day or week.
If an IP address is found to trigger lots of systematic searches over long periods of time, but not yield any bookings, it's probably a bot.

However, if the group running the bot is clever, they will make the searches look like typical web traffic and be very difficult to detect…."



Why scrape?

Scraping could provide valuable insights, such as tracking competitive pricing moves, while bypassing ineffective caching processes.

Said Bill Carroll, a professor at the Cornell School of Hotel Administration:

"For example, say I'm a hotel manager. Scraping to see my position on the Expedia display — how far up I am in search results — will give me some indications about how an Expedia market manager may be establishing a default position for my hotel, relative to my competitors.

The more that becomes obvious, that better I can decide how much to cooperate with the OTA, how much inventory to give, etc."

Which companies may the OTAs be trying to fool?

If you Google "hotel rate comparison software" or "hotel revenue management software", you'll find the names of dozens of vendors – most offering some form of competitive price tracking capability. Any of these could be a target of deception.

Dark bots: An open secret?

Ironically, some OTAs may use rate-scraping bots themselves.

For instance, an OTA might scan rates on a hotel's branded direct site and on rival OTAs to validate a hotel's compliance with its contractual terms, such asguaranteed parity with rates offered anywhere online.

If an OTA finds out that a hotel has given a better rate to one of its OTA competitors, it will call or email it to say it is not compliant with rate-parity agreements — known to consumers as Best Rate Available guarantees.

More precisely, some OTAs tap third-party vendors to do the work via web data harvesting and extraction solutions.

To respond to the OTA scraping, hotel chains could theoretically use similar "Dark Arts" to feed false information.

There's yet another twist in this game between bots and false feeds, and that's between the OTAs themselves. Peskin explained this with an example:

Let's say Booking.com is tracking to see if the Ritz Hotel is giving Expedia cheaper rates than the hotel is giving it. (Neither Peskin nor Tnooz is saying either company specifically engages in such practices. Using names is just to make the example easier to understand.)

In this case Booking.com may use bots to check what rates are available for the Ritz Hotel at other sites. But Expedia, in turn, may try to feed Booking.com's bot false information. After all, it wouldn't want its rival to know that it beat it on price.

Industry denials

Expedia Inc had no comment for this story. Neither did Priceline Group. A few well known vendors of rate management software and web data harvesting and extraction solutions also declined to speak for this story.

An executive at one major OTA group said anonymously that its brands do not engage in such practices, but that it is familiar with seeing competitor brands do this.

Original article — http://www.tnooz.com/article/bots-otas-hotels-rate-scraping/