NETACEA / WHITEPAPER

Travel in 2021: Are bots threatening the industry?

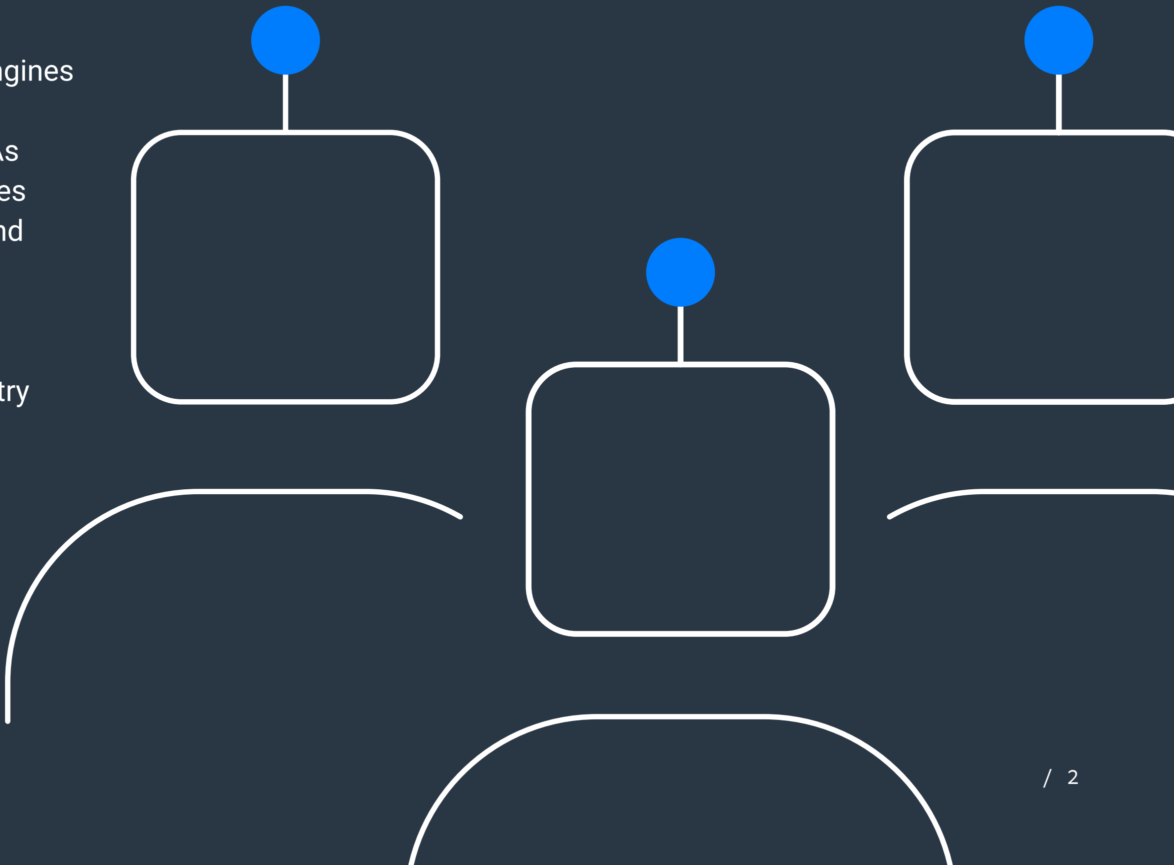
NETACEA

A BRIEF INTRODUCTION TO BOTS

Bot traffic is any request that is made by an automated process rather than triggered by a direct human action. While good bots are used daily by businesses across the globe, bad bots are automated processes that carry out legitimate activity to exploit business logic weaknesses within your website, mobile apps and APIs.

Travel websites regularly reap the rewards of good bots including search engines and SEO tools. They are used by airlines, hotel chains, holiday websites and third-party booking agents to gain competitive edge over rival companies. As with every industry, bad bot activity exposes travel and hospitality businesses to malicious automated threats such as denial of inventory attacks, price and availability scraping and various account takeover techniques.

In this whitepaper we explore how such attacks could damage the brand reputation, customer loyalty and profits of travel organisations as the industry prepares to open its doors once again.



THE REOPENING OF THE TRAVEL INDUSTRY IN 2021

In 2019, the travel and tourism industries contributed £106 billion to the British economy, supporting 2.6 million jobs.[1] Since then, the Covid-19 pandemic is estimated to have cost the international tourism market upwards of $1 trillion, while the percentage of the UK population reporting their primary employment as being in the travel and tourism industry during Q3 was 10.8% lower than the previous year, as international and domestic travel all but shut down due to government restrictions.[2]

When the pandemic hit in early 2020, tourism was brought to a halt across the globe as governments gave the order to stay at home and issued strict Covid travel restrictions. Flights were cancelled, and even domestic travel was limited, meaning international tourism arrivals dropped by 87% between January 2020 and 2021.[3] Accommodation businesses and travel agencies saw the sharpest decline in turnover during the first period of restrictions, falling to just 9.3% of their levels in February by May 2020.[4]

With lockdown restrictions now easing, preparations are already underway for the travel and tourism industry to reopen, beginning with household-only domestic trips, and leading to a traffic-lighted system of recreational international travel in the summer months. While the industry is gradually crawling back to where it left off in 2020, it is certainly not set to surge back to 2019 levels until later this year. For now, international travel remains uncertain, corporate bookings are almost redundant while the world continues to work from home, and the birth of the popular 'staycation' means only domestic travel has witnessed a boom in bookings during Q1. However, with more bookings comes more opportunity for malicious bots.

Sources:
1. Visit Britain: The Value of Tourism in Britain
2. Forbes: Tourism Industry Faces $1 Trillion Loss, 100 Million Jobs At Risk From Covid-19, UN Reports
3. UNWTO: International Tourism and Covid-19
4. ONS: Coronavirus and the impact on the UK travel and tourism industry

THE BOT PROBLEM IN THE TRAVEL INDUSTRY

The travel and tourism industries are no stranger to automated activity. In fact, a survey conducted by Tata Consultancy Services (TCS) found 85% of travel and hospitality service providers use artificial intelligence in their business.[5] But how bold are travel companies prepared to be in 2021? Budgets and priorities have shifted dramatically over the last year as cash flow issues left businesses struggling to survive when staff were furloughed, flights were cancelled, and refunds and credit vouchers were issued to millions of customers. Digital priorities were understandably neglected, but as the industry gets back on its feet, the challenge faced by travel companies is remaining agile in an unpredictable market. Investing in cybersecurity – and specifically a robust bot management solution – is key to achieving this ability to adapt to changing circumstances as the world reopens.

Netacea's Threat Research team predicts to see the same types of threats that have previously plagued the travel industry affect businesses again this season; what is set to change, however, is the volume, speed and sophistication of these attacks, with the increased demand for bookings meaning more traffic and subsequently more bots. As cybercriminals recover from the effects of Covid-19 in the same way as businesses, threat actors are keen to get old methodologies up and running rather than investing in new threat types or attack techniques. With financial gain from the travel industry a key driving force for criminal groups, Netacea expects to see a spike in bad actors making a profit as bookings increase.

> 26% of travel businesses surveyed by Netacea in 2020 said they'd had a full bot management solution operating for some time.[6]

Sources:
[5] Emerald Insight: Impact of AI and robotics in the tourism sector: a critical insight
[6] Netacea: The Bot Management Review 2020

PRICE AND AVAILABILITY SCRAPING

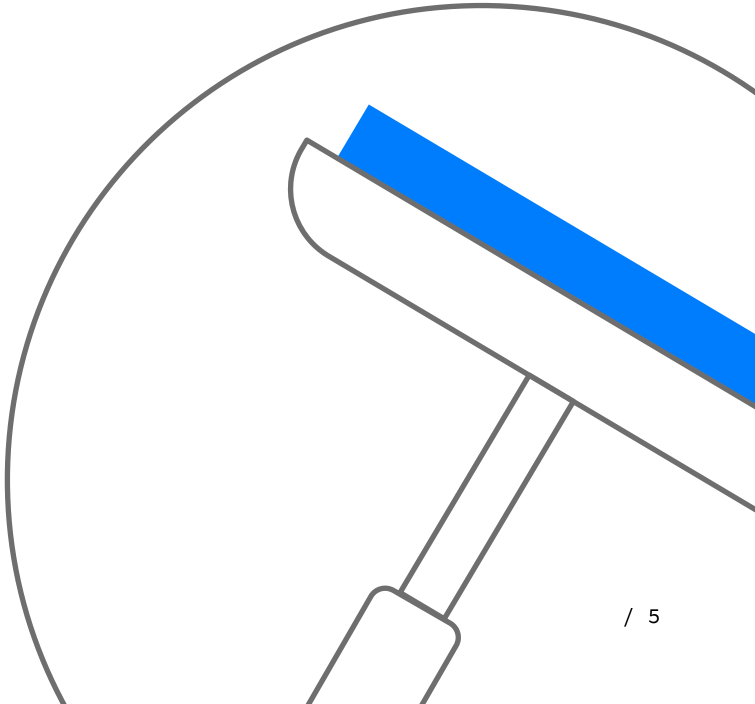
Web scraping in the travel industry

In travel, web scraper bots are mainly used to collect fare and availability information by rival companies and aggregator sites are used for price comparison. Travel sites are frequently affected by aggregation services that use scraper bots to discover and publicise the availability of products or services such as flights, hotels or car rentals. Threat actors advertise the scraped information at lower price points on a secondary site, motivated by the financial rewards of charging commissions, stealing personal data or generating advertising revenue. Due to the dynamic nature of travel pricing, this is fast becoming a top threat for the industry, exacerbated by increased competition driven by the pandemic.

What's the impact of price and availability scraping?

76% of travel businesses surveyed by Netacea in 2020 said that price scraping represented the greatest automated threat to their business.[7] Netacea's Threat Research team has observed travel sites with 90% scraper bot traffic, which can be useful, but if uncontrolled can impact top line revenue, bottom line profits and customer experience.

Price scraping on travel websites has the potential to not only damage website sales, but also user experience, marketing analytics and brand reputation. The technique is used by rival companies to gain competitive price advantage and has the potential to lose the affected website auxiliary sales such as car rental and insurance, as customers head elsewhere to source the cheapest deal. Look-to-book ratios, used by the travel industry to measure the number of people visiting a website compared to those who make a purchase, are regularly skewed by scraper bot traffic. Scraper bots can make excess web requests to an online travel agent which, in turn, negatively impacts your look-to-book ratio and significantly inflates prices on your website. This increased traffic also presents an inaccurate number of website viewers interested in a certain product or booking, leading to reduced conversions and misleading website analytics which are used as a basis for making business decisions. Scraping is also often used to gather the data used in more sophisticated or damaging threats such as spinner bots or denial of inventory bots, leading to future attacks. Stopping scraping can cut out these attacks early as the attackers do not have the data they need in order to progress.



Sources:
[7] Netacea: The Bot Management Review 2020

Fig. 1 shows the time series of human and scraper requests on a website between 3rd and 9th April. On generic eCommerce websites we would expect to see the underlying scraper bot traffic presented as a flat line, signifying a constant threat. On travel websites, there is generally a greater level of sophistication as scraper bots mimic human behaviour to appear as genuine users at peak times throughout the day, sometimes switching IP addresses to give the impression that the traffic originates from a human.

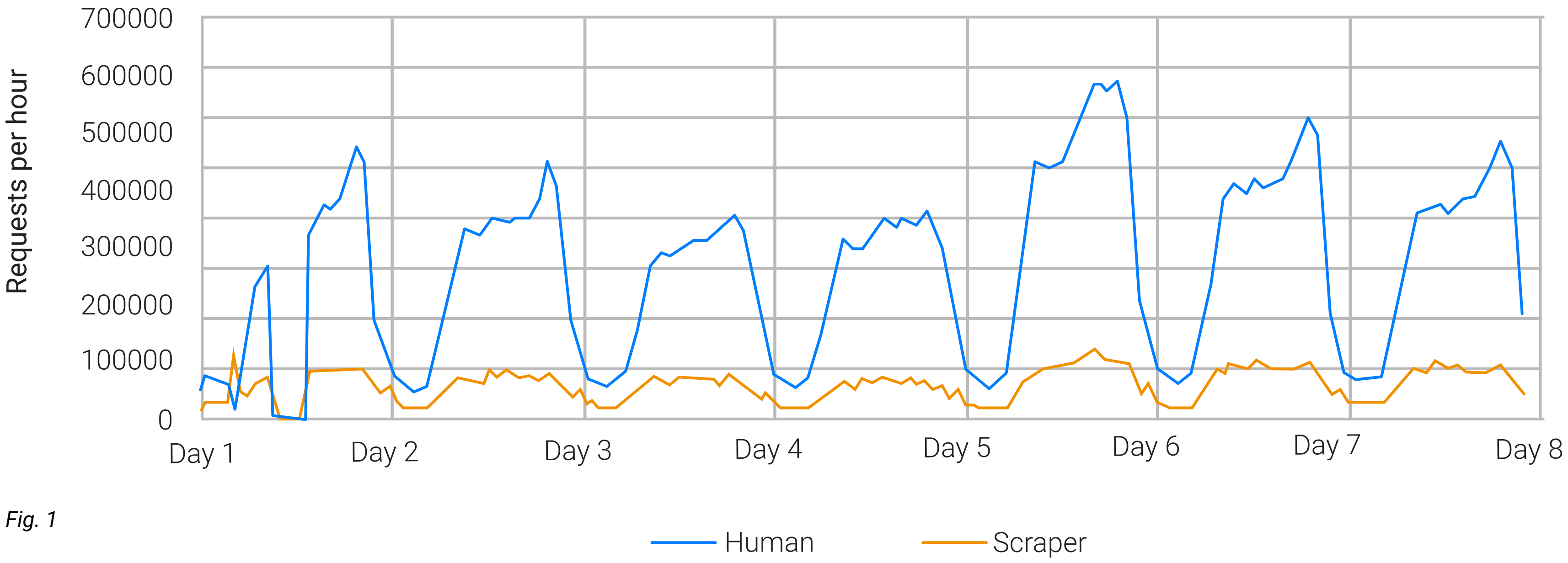


Fig. 1

DENIAL OF INVENTORY

What is a denial of inventory attack?

During a denial of inventory attack, bad actors use malicious hoarder bots to select and hold items from a limited inventory or stock in a shopping cart until the inventory is depleted. The items are held so that genuine users are unable to buy the items themselves. By hoarding high-demand products, bots keep it out of stock, leaving customers frustrated and reducing conversions and revenue for the business. The malicious actor then attempts to sell on the product for a profit. The transaction may be completed after the item has been resold elsewhere; by being held, it remains unavailable on the original site but available for sale on a secondary site.

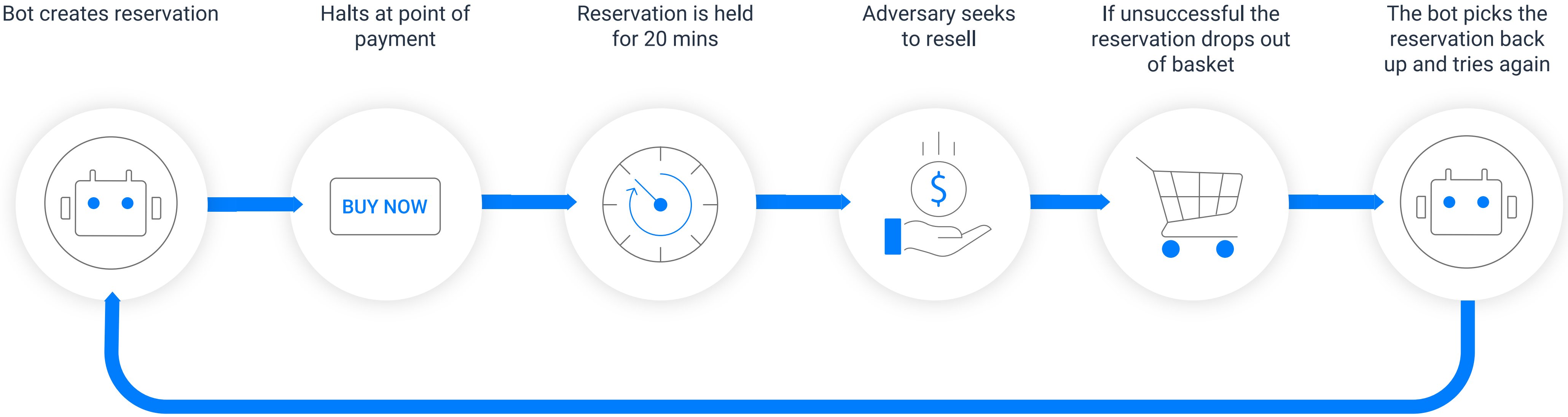
How does denial of inventory affect the travel industry?

Denial of inventory across travel websites involves making fake reservations for hotel rooms, restaurants, holidays and flights, holding these bookings until the ticket, room or booking becomes sold out, but never purchasing the item. Bad actors use bots to hoard inventory in various areas of the travel industry, and it is fast becoming a problem as demand for bookings increases at an unprecedented rate.

The objective of a denial of inventory attack on travel websites varies from:

- Generating high and fast profit; threat actors are commonly driven by the profitability of action, and acquiring inventory is a fairly low risk, high yield opportunity to make a fast profit
- Defeating the competition by sending customers to a rival website, enabling them to appear as the only vendor with availability and therefore able to charge a premium for in-demand items
- Disrupting availability by making an application unusable as part of an application-layer denial of service attack

Bots are programmed to carry out reservations up until the point of payment. For example, on an airline's or third-party online travel agent's website, bad actors use bots to reserve seats on flights. The bot reserves the seats for up to 20 minutes, during which time genuine customers perceive there to be no availability left on the flight, and the perpetrator attempts to sell the seats on for a profit. Once the website has cleared the basket of the held reservation, a new bot will pick up that availability and repeat the process until the inventory is successfully sold.


Bot creates reservation
Halts at point of payment
Reservation is held for 20 mins
Adversary seeks to resell
If unsuccessful the reservation drops out of basket
The bot picks the reservation back up and tries again
BUY NOW
$

ACCOUNT TAKEOVER

Why is account takeover used to target travel?

Credential stuffing, credential cracking and phishing techniques are used as the first step in attacks which result in account takeover across the travel industry. Such attacks give bad actors access to customer accounts. These accounts hold valuable items such as membership points, frequent flyer miles, loyalty programmes or cards that can be sold on for a profit, as well as saved payment details and personally identifiable information (PII) which have value across the dark web as they are sold on marketplaces to facilitate future attacks.

What are the risks of account takeover to travel businesses?

Credential stuffing has become an increasingly popular technique for threat actors across the travel industry over the past few years. In fact, 85% of travel businesses surveyed by Netacea in 2020 said a credential stuffing attack represented the greatest risk to their business.[8] During the pandemic, cybercriminals began circulating old credential lists in an effort to take advantage of personal and financial information on vulnerable accounts as the world's day-to-day activity moved online. As loyalty points in travel are often only checked by customers a handful of times a year, there is a huge window of opportunity for the threat actor before the genuine customer realises points have been stolen. This has a double-edged impact on the targeted travel company who must refund the points to the legitimate customer and pay for the goods or service that the threat actor has received using the stolen loyalty points.

The impact of losing saved payment details and PII to threat actors is both financially and reputationally damaging. While the organisation may not be directly at fault, if the customer has used the same login credentials across multiple accounts, ultimately it is the organisation who is responsible for the loss of such information, which has the potential to incur huge fines by the likes of the ICO in the UK or an equivalent in other territories. The organisation is left to pay the data breach fine, reimburse any affected customers and face the PR repercussions of publicly losing customer data.

Sources:

[8] Netacea: The Bot Management Review 2020

Fig. 2 shows the first step in the multi-step nature of an account takeover attack. Two large spikes of credential stuffing attacks against a travel booking site exhibit behavioural patterns that trend towards automated behaviour. After membership accounts were breached for approximately 17 minutes each, a separate attack then exploited these accounts, demonstrated by subsequent requests to the debit-transaction-request path on the website.*

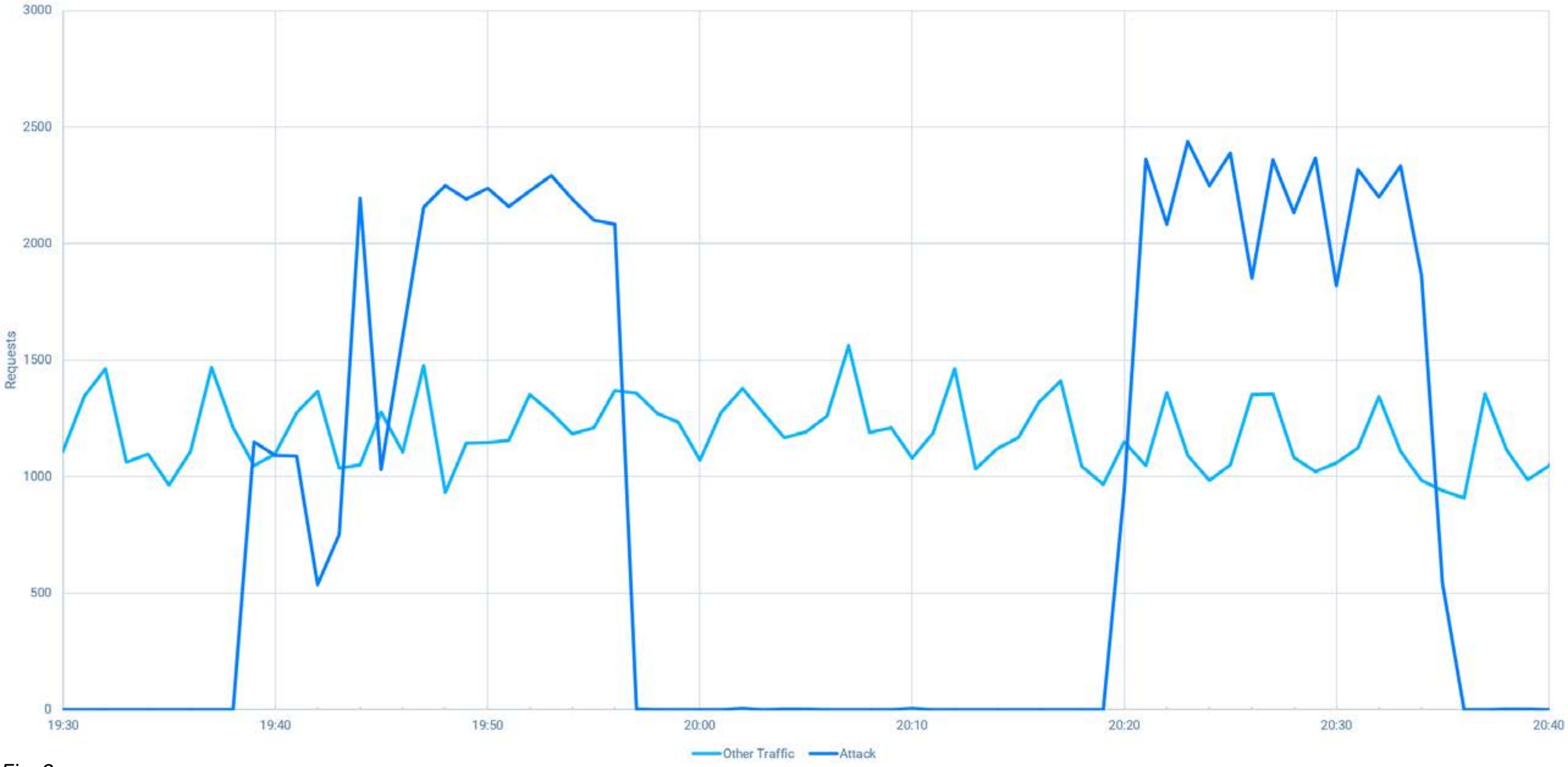


Fig. 2

* This was not a site that was under active protection by Netacea Bot Management. The graphs are based on analysis of historical data by Netacea's Threat Research team.

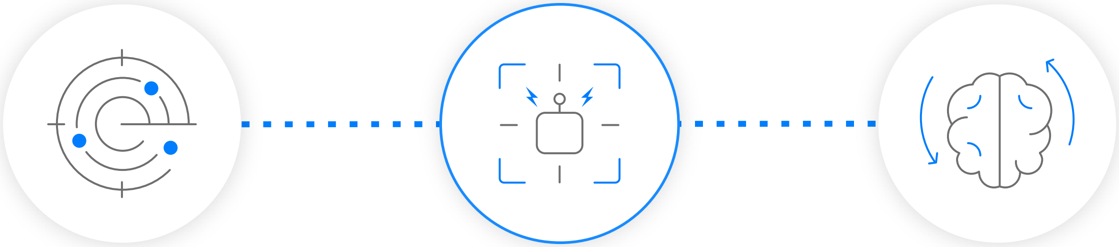
SUMMARY: HOW TO PROTECT YOUR TRAVEL BUSINESS IN 2021

Travel businesses should expect the bot threat to grow in volume and sophistication as threat actors capitalise on the demand for holiday bookings over the course of 2021, in line with Covid travel restrictions being lifted. As well as being prepared for the sudden rush of traffic expected to hit booking websites, now is the time to invest in cybersecurity services and put a dedicated bot management solution in place to deal with the most sophisticated threats. As attacks evolve, it’s critical for cybersecurity teams in the travel industry to adopt an advanced approach to bot detection.

CHOOSING THE RIGHT BOT MANAGEMENT SOLUTION

Netacea's revolutionary bot management technology is helping organisations across the travel and hospitality industry to detect and protect against malicious bot threats.

Choosing the right bot management solution is a significant decision for any business. At Netacea we take a consultative approach, working closely with you to understand not only the threats bots pose to your business, but how our solution fits into your wider strategy and organisation. This partnership, paired with our server-side approach and innovative Intent Analytics™ technology, allows us to seamlessly integrate with your business and deliver accurate, intelligent and effective bot mitigation.



DETECT MALICIOUS BOTS

RESPOND TO ATTACKS

EVOLVE AND ADAPT

To find out how much bots could be costing your travel organisation, try out Netacea's new bot calculator at www.netacea.com/impact-of-bots-calculator/

Or talk to our team today at hello@netacea.com.

- Real-time analysis powered by Intent Analytics™
- Best-of-breed anomaly detection
- Threat intelligence feed
- Insightful, data-rich dashboards
- Total control over response options
- Seamless and flexible integrations
- Dedicated bot experts with 24/7 support