NETACEA

REPORT

Refund fraud as a Service

The other RaaS threat for retailers

Netacea @Netacea_AI www.netacea.com hello@netacea.com

Contents

Introduction

Refund fraud is becoming increasingly impactful to e-commerce stores. Last December, a man pleaded guilty to defrauding a retailer for over $300,000 by performing refund fraud over a three-year period. With the cybercrime underground's continued shift to a service driven economy, interested parties can now outsource the process of refund fraud to groups of professional social engineers offering refund-fraud-as-a-service.

Refund-fraud-as-a-service poses a significant challenge to retailers. Previously legitimate customers with no history of fraud can enlist highly experienced fraudsters to perpetrate this fraud on their behalf. This makes identifying fraudulent activity difficult; fraud teams cannot rely on inexperience or prior account activity.

Refund fraud does not only affect e-commerce stores, but delivery carriers as well. Collaboration is needed to effectively detect and prevent fraudulent refunds, and both parties must understand the different methods and actors forming the refund-fraud-as-a-service market. Most actors use, or provide supporting services for, methods that either falsely claim the item did not arrive or pretend to send items back.

Once these methods and services are understood, processes can be put in place to mitigate specific methods, like using one-time-passwords (codes only provided to the recipient which must be validated by the delivery carrier at point of delivery), to prevent Did Not Arrive claims.

NETACEA

Background

Refund fraud is the act of abusing refund policies for financial gain, typically by requesting a refund when there is no intention of returning the item. It is not a new concept, but it is becoming increasingly impactful to e-commerce stores. For example, in December 2021, a man pleaded guilty to defrauding a retailer for over $300,000 by performing refund fraud over a three-year period.

Refund fraud has become more popular in recent years, due in part to the Covid-19 pandemic induced rise in e-commerce sales. However, professional adversarial groups offering refund-fraud-as-a-service have also emerged in the underground market.

Professionalisation of Refund Fraud

Refund-fraud-as-a-service allows individuals to outsource the process of refund fraud to groups of professional social engineers. These criminal groups facilitate and complete the fraudulent refund on behalf of the customer for a cut of the refunded value. The process proceeds as follows:

- A customer orders an item from an e-commerce store
- The customer provides their order details to the refund fraud service
- The refund fraud service initiates a refund request and socially engineers the e-commerce store into providing a refund, without returning the purchased item
- The customer receives a refund and pays the refund fraud service their cut

This service offering poses a new challenge to e-commerce fraud teams. One customer requesting multiple refunds against the same retailer generates a pattern that can be detected, as with the case of the $300,000 fraud referred to earlier. However, a group requesting refunds across multiple customer accounts and retailers, is less likely to cause suspicion. Similarly, a typically honest customer who suddenly decides to perform refund fraud is likely to be detected due to their inexperience in committing fraud. However, if that customer outsources the fraud to a professional refund fraud service, it will be perpetrated by skilled and experienced fraudsters.

Refund Fraud Services

Refund fraud services are publicly advertised, customer facing criminal organisations that take and fulfil requests from customers looking to obtain a fraudulent refund for their purchases. Refund fraudsters advertise their services by creating threads on hacker forums such as Cracked, Nulled and Sinisterly. These adverts highlight not only their skill, experience and success rates committing refund fraud, but also their customer service and response times to attract business in an increasingly crowded market. The Cracked and Nulled forums each have a dedicated section for refund fraud services, on which only members with upgraded memberships can create threads. Once a thread has been created, all forum members can post in the thread to vouch for the service and leave feedback.

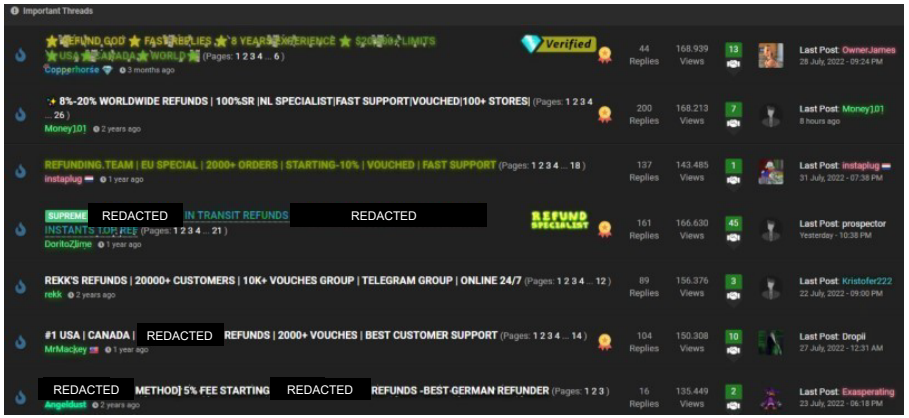


Figure 1 - Refunding services advertised on the hacker forum Cracked

The refund fraud service's hacker forum advert, serves to direct interested customers to their Telegram accounts, which are used to run the bulk of their operations and customer communication. Many refund fraud services use Telegram channels for announcements and vouches (i.e., evidence of successful refunds) and have a separate Telegram group for customer services.

Service request orders are taken through Google Forms. Potential customers are asked to provide a Telegram handle, the store they want to refund from and the details of the order they want to refund. The order details requested can include the total order amount, order and delivery date, payment method, and billing and delivery addresses. In many cases, the refund fraud service will also request the customer's credentials for the target store.

Fraudsters hold lists of stores and companies that their refund service can defraud on Google Sheets. These lists detail any limits on the number, type or value of items that can be fraudulently refunded, the refund processing time and fees for the refund fraud service. Refund fraudsters generally charge between 10% to 30% of the total refund value, and most only require payment following confirmation of the refund being initiated by the store.

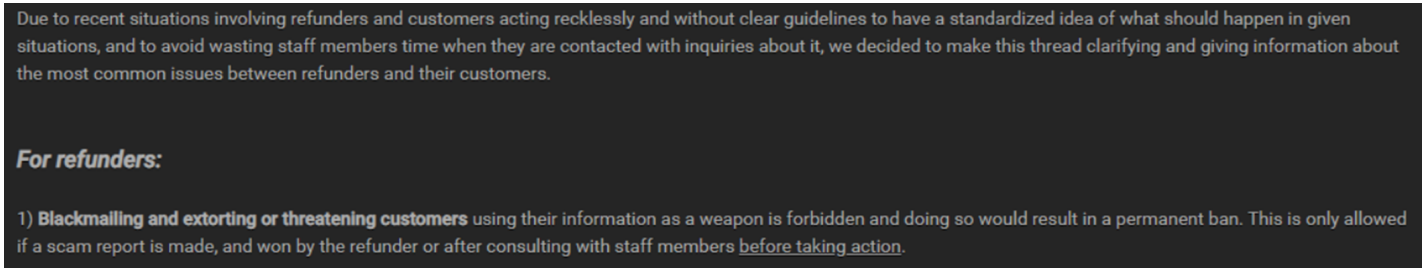
This is a relatively low risk monetisation model for the refund fraudster as the fraudulent refund is not requested from an account held by them. Therefore, with decent operational security (OPSEC) in place, there is little to link them to the fraud. Conversely, the customer outsourcing the fraud bears not only the risk of a failed refund, but also of providing personal information to the refund fraud service. Unsurprisingly, some refund fraud services have used their customer's information to extort them after completing the refund, or to discourage negative reviews being posted. This was so prevalent that an admin of the Nulled hacker forum had to set up guidelines for refund fraud services explicitly prohibiting such activity. Scam artists also take advantage of the interest in refund fraud, by creating lookalike profiles for prominent refund fraudsters to steal personal information or money from their customers.

ELECTRONICS & HOME

Stores	Price limits	Items limits	Fee (%)	Region	Approximately time	Notes
REDACTED	5000	10	25	UK/USA/NL	1-3 days	
	5000	5	30	USA/DE/DK	3-30 days	
	5000	10	25	Worldwide	1-20 days	USA instant refunds.
	3000	5	30	Worldwide	8-20 days	90-95% success rate
	600	1	25	USA	1-3 days	
	4000	3-4	25	USA/CA/UK	1-3 days	UK 80% success rate.
	5000	3	25	USA/UK/CA	7-20 days	
	7000	1	25	USA/CA	1-20 days	
	20000	Multiple	25	USA/CA/UK/DE	1-10 days	REDACTED not allowed.
	5000	Multiple	25	DE/NL/IT/FR	1-10 days	No specialized delivery.
	10000	Multiple	25	USA	1-3 days	Only items returnable REDACTED
	10000	10	30	USA	1-7 days	REDACTED
	5000	Multiple	25	USA	1-10 days	
	5000	Multiple	25	USA	3-14 days.	
	20000	Multiple	30	USA	1-15 days	Insider refunds.
	5000	3-4	25	USA	15-30 days	
	10000	10	25	USA	1-15 days	
	10000	10	25	USA	1-15 days	

Figure 2 - Excerpt of store list published by refund fraudster REKK

Once an order has been placed, the refund fraudster is responsible for socially engineering the e-commerce store into processing a refund without their customer returning the item. Refund fraudsters will use the customer's account to engage with the store's customer service representatives. Most refund fraudsters require customers to remove any multi-factor authentication from their account to enable easy access.


Due to recent situations involving refunders and customers acting recklessly and without clear guidelines to have a standardized idea of what should happen in given situations, and to avoid wasting staff members time when they are contacted with inquiries about it, we decided to make this thread clarifying and giving information about the most common issues between refunders and their customers.

For refunders:

1) **Blackmailing and extorting or threatening customers** using their information as a weapon is forbidden and doing so would result in a permanent ban. This is only allowed if a scam report is made, and won by the refunder or after consulting with staff members before taking action.

Figure 3 - Post on Nulled hacker forum by admin Lucas, prohibiting use of personal information for extortion

Refund Fraud Methods

Methods are the techniques used to fraudulently obtain a refund. Whilst there are many methods in use, they generally fall into two categories, non-arrival fraud methods and returns fraud methods.

Non-arrival Fraud Methods

Non-arrival methods are used by refund fraudsters to claim that the customer did not receive the items they purchased. This entitles the customer to a refund whilst at the same time removing the obligation to return the item. There are two main variants in use:

Did Not Arrive

The Did Not Arrive (DNA) method is simply claiming that the package was not delivered to the customer. Refund fraudsters will wait a few days after the delivery is made and initiate a refund, claiming not to have received the package. This method works best when packages are left outside the delivery address without being signed for; a standard question on refund fraud service request forms is whether this is the case.

The DNA method grew in popularity throughout the Covid-19 pandemic, as delivery carriers were more likely to make no-contact delivery. However, experienced refund fraudsters can still have success if an item is signed for, especially when a fake signature is used. In some cases, delivery drivers sign for the package themselves, making it easier for the refund fraudsters.

If stores can verify that the package was delivered to the address in question, they will often request a police report to be provided to corroborate the refund fraudster's story. Most refund fraudsters will comply with this and report the fictional crime, preferably through a digital channel, to the police to obtain a report. However, others will forge police reports instead, increasing the risk for the customer.

Requiring a one-time-password (OTP) to be provided on delivery is currently the most effective deterrent against the DNA method. If this is only communicated to the recipient of the package, and validated on delivery instead of, or in conjunction with a signature, refund fraudsters have little room to argue that the package was not received.

(Partially) Empty Box

The Partially Empty Box (PEB) method, also referred to as the missing item or empty box method, is a variant of DNA. The refund fraudsters claim that whilst the package was delivered, it was missing some or all of the items ordered. It is mostly used for lightweight, high value items in a larger order as the weight difference of the package with and without the item is marginal. Popular items are lightweight electronics such as mobile phones or smartwatches. To mitigate the method's effectiveness, e-commerce stores should flag such purchases as risky, especially when inconsistent with the customer's previous purchases, and purchased as part of a large heavy order.

Returns Fraud Methods

Returns Fraud methods are used by refund fraudsters to simulate returning an item, without actually doing so. These methods are used when the refund fraudster is claiming a refund for reasons such as receiving a wrong or damaged item, and the store requires the original item to be returned. After committing returns fraud, the fraudster will argue that since they have returned the item, the store should process their refund. Refund fraudsters generally employ third parties to assist them when using returns fraud methods, including Boxing and Scanning services:

Boxing Services

Boxing Services, or Boxers, perform label manipulation and postage for refund fraud services. The refund fraudster provides the original postage label and, if necessary for the delivery carrier, any weight and dimension requirements to the Boxer. Pricing for Boxing Services is typically under £50 per package.

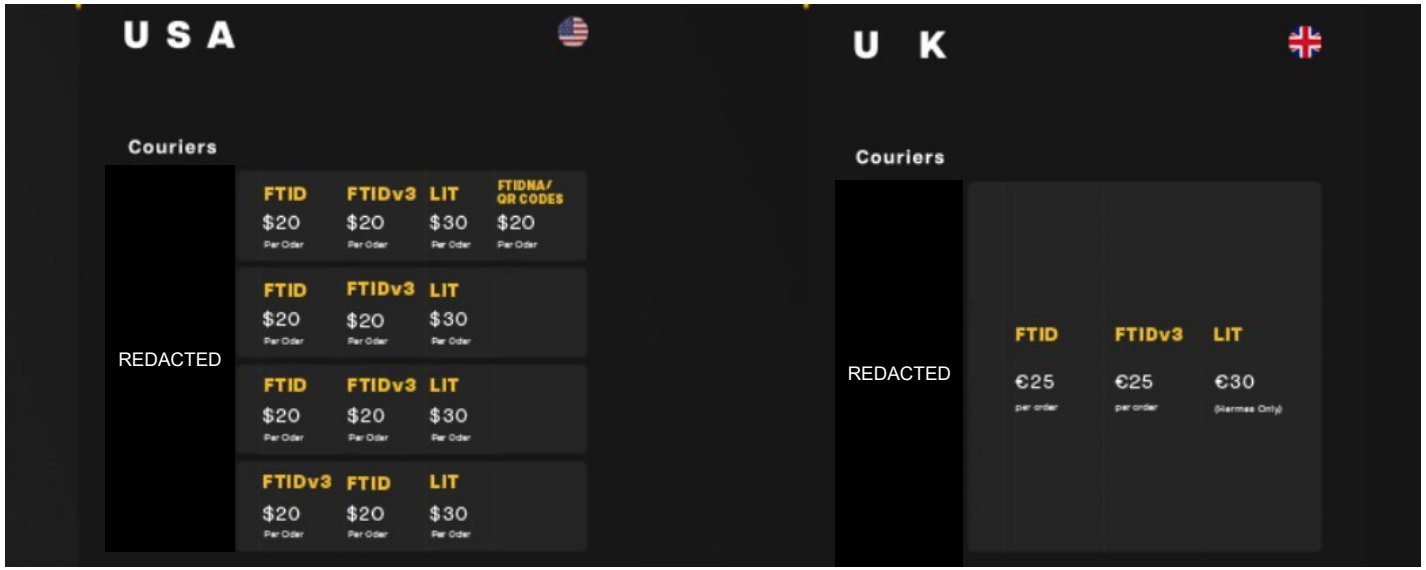


Figure 4 - USA and UK price list for HydraBoxing service

Fake Tracking ID

Boxers are primarily used for the Fake Tracking ID (FTID) refund fraud method. FTID is where the return postage label is altered and used to mail an empty or junk filled package instead of the item for which the refund has been requested. There are two dominating versions of FTID currently in use.

In the first, all information linking the package to the customer or order is removed. This is intended to cause the return centre to throw out the junk package and prevent them from tying it to the customer. At the same time, the delivery tracking will show the package as having been delivered, entitling the customer to their refund. In the second and more widely used method, the delivery address is also modified. Here, the intention is that the package is delivered to an unrelated address and the recipient throws out the junk package, removing evidence of the fraud. The delivery tracking will show that the package was delivered to the return centre, entitling the customer to their refund.

Lost in Transit

Refund fraud services may also employ Boxers when using the Lost in Transit (LIT) refund fraud method. Boxers print the postage labels using special disappearing ink, which fades over time. The postage label will be visible when the package is scanned in by the delivery carrier and tracking will record that the package is in transit. After some time, the label will fade and the delivery carrier will no longer be able to deliver the package, causing the tracking to eventually be marked as lost in transit. However, refund fraudsters currently prefer using scanning services for LIT refund fraud.

Scanning Services

Scanning Services assist refund fraud services by abusing inside access at delivery carriers to fraudulently manipulate tracking information. This allows packages to be marked as LIT, damaged, or returned to sender (RTS) however, in reality they have been delivered to the intended recipient. Pricing for these services ranges from £25 to £150 depending on the scan code requested, the service provider and the postal company.

Insider access to delivery carriers via access point accounts or sub-accounts is also traded on underground forums for between £100 and £750. Our research suggests that these accounts may be being taken over through credential stuffing, using tools such as OpenBullet. Once access to an account is obtained, many sellers will create multiple sub-accounts to be resold under that account.

Most refund fraud service providers now prefer to use scanning services over Boxers to lend weight to their social engineering attempts. For example, a scanning service can make it look like a package was refused and returned to the store it was purchased from by combining a RTS or damaged scan with a delivery scan, using the store's address and a fake signature. This strengthens the refund fraudster's case for a refund to be provided for their customer.

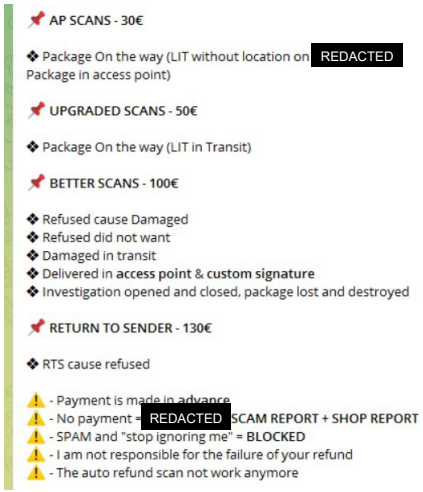


Figure 5 – Scanning service advert on Telegram from CristalineX

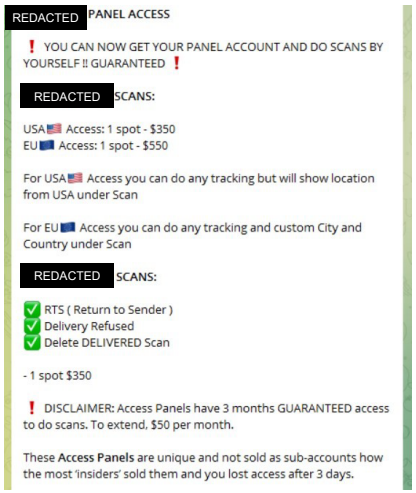


Figure 6 – Advert for insider access to multiple delivery carriers on Telegram channel FTID best service

Method Brokers

The popularity of refund fraud as a service has given rise to a number of underground vendors providing access to training courses and private methods. We will call them Method Brokers. These are typically refund fraud service providers looking for an additional income stream, however, some actors solely obtain and resell methods.

The most infamous of these method brokers goes by the alias Bob. Their refund fraud ebook was first advertised on the Nulled hacker forum in 2019. It has been regularly updated since, and is now on the fifth version. Purchasers could build their own ebook by selecting from available modules and services. Pricing ranged from €69 for the core ebook to €1,000 for the comprehensive version. This cost was also inclusive of one-to-one mentorship and access to the private Telegram group. The full version covers the DNA, PEB and FTID refund fraud methods, the latter of which Bob claims to have invented. It also includes guides for starting up a refund fraud service and OPSEC.

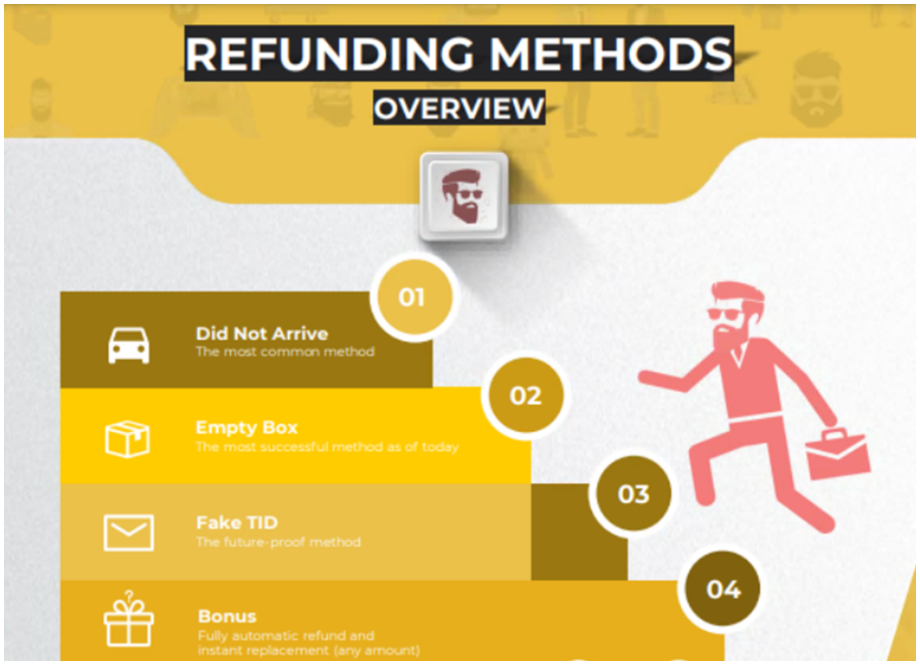


Figure 7 - Methods covered in Bob's refund fraud ebook

At time of writing, Bob seems to be no longer selling this ebook. They last posted to their public Telegram channel in December 2021 and their sales thread on the Nulled forum in April 2022. Their dedicated ebook sales website has also been down since May 2022. However, all versions of the ebook have been leaked and are widely available for use by threat actors looking to provide refund fraud services.

Another method broker offers lifetime access to the aptly named FraudBox, a repository which claims to have over 50,000 methods and resources for £2,000. Each method is a variant of the DNA, PEB, FTID or LIT methods, with instructions for using it on a particular e-commerce store. Similarly to Bob's offering, this comes with access to a private Telegram group for customers.

Figure 8 - Advertisement for the FraudBox refund fraud method repository

Mitigations

There are some general steps e-commerce stores can take to reduce their risk of refund fraud. Regardless of the method used, the refund fraudster will have to contact customer services to initiate the refund. Therefore, customer services employees should be educated on the methods and tactics that refund fraudsters may employ, to reduce their risk of being socially engineered. Where the refund is requested over a digital channel, the use of a third party to request the refund may also provide indicators to the e-commerce store. They should look for any inconsistencies between identifiers such as IP addresses and user-agents between the customer's usual sessions and their refund request. In addition, refund requests for items either above the value normally purchased by the customer, where multi-factor authentication has recently been removed from an account, or from newly created accounts should also be viewed as suspicious.

Delivery carriers should replace or complement signatures with one-time-passwords to prevent refund fraudsters from claiming that packages did not arrive. Any packages showing signs of label tampering should be reprinted to protect against the Fake Tracking ID method. Delivery carriers should also look to strengthen authentication processes for their access point accounts to prevent them being taken over and used for tracking manipulation. Bot management solutions can prevent credential stuffing attacks on these accounts. Multi-factor authentication should also be considered.

As refund fraud targets both e-commerce stores and delivery carriers, collaboration between the two is vital to tackle the issue. E-commerce stores and delivery carriers should look for patterns in their data sets that may indicate fraudulent activity. For example, e-commerce stores may be able to identify a disproportionate number of fraudulent refunds scanned at a certain access point. Similarly, delivery carriers may be able to identify an influx in items marked as lost in transit, and correlating the data points could provide useful insights.

Finally, in the instance that an e-commerce store identifies the claim to be fraudulent after a refund payment has been made, the store should rebill the customer's account. Refund fraud services take payment after refund confirmation and ironically don't offer refunds themselves if the refund fraud later fails. By rebilling the customer account, not only does the e-commerce store recover some of its losses but it serves to reduce the reputation of the refund fraud service. Reputation is power in the underground market. An influx of rebill complaints from customers may cause the refund fraud service to drop the retailer from their store list, to avoid negative reviews.

Start protecting your business against online fraud with Netacea

If your business operates online, it is a target for fraud.

Protecting your organization and your customers against online fraud and malicious threats requires real-time insights that ensure the efficacy of your security initiatives. Yet dedicated in-house threat intelligence with the ability to infiltrate criminal bot communities requires highly specialized skills that are prohibitively expensive to resource.

Netacea monitors billions of requests for the world's biggest sites, deconstructing automated threats continually. This gives us unmatched insights into their origins and tactics.

Netacea's Bot Intelligence Service is your secret weapon against even the most guarded threat groups. Our highly specialized professionals have successfully infiltrated criminal bot forums and communities, silently gathering intelligence about ongoing and new threats, and the adversaries responsible for them.

How we've helped our clients

- Tracking stolen user accounts on the dark web for a stock photo site
- Collecting evidence against adversaries in several ongoing legal cases
- Disassembling scalper bots so retail clients can detect their signals

Benefits of dedicated automated threat research

- Focus intelligence to pinpoint on the biggest threats to your business
- React quickly to attacks by monitoring dark web activity
- Disrupt threat actors and fight back against attacks
- Assess the effectiveness of your defenses
- Free internal teams from the burden of specialized threat intelligence

To find out more about Netacea's Bot Intelligence Service, contact the team today at hello@netacea.com.