CASE STUDY

Saving a top 3 telecoms provider millions with Bot Attack Intelligence

Customer profile

- Top 3 telecommunications provider with over 15 million customers
- Serves fixed-line, broadband and mobile services, as well as subscription TV packages
- Customers have access to premium multimedia streaming services

Results

- Millions saved by reducing customer support calls, infrastructure demands and fraud cases
- On average over 1,000 and a peak of over 500k malicious login attempts blocked per hour
- More than 100,000 account takeover attempts blocked

NETACEA

Millions saved across multiple teams

500k attacks blocked in one hour

The challenge

The partner is one of the top three largest multinational telecommunications companies based in the UK, with over 15 million customers.

Their customers can access third party streaming media services, such as Netflix, Spotify and Apple TV, included in their broadband and television subscriptions or as add-ons. These are bundled as part of partnership agreements with the content providers.

Bundled streaming services targeted by criminals

These desirable assets made the business a frequent target for credential stuffing attacks. Netacea's Threat Research team found numerous credential stuffing configuration files on the dark web specifically written to target the client. Attackers used automated bots to validate credentials leaked from other sites on the client's authentication service, counting on users to reuse the same password across multiple sites.

Once they gained access to the accounts, adversaries would then sign up to the bundled streaming services via the telecommunication business's customer portal and sell the streaming account details on the dark web for a profit. Our Threat Research team uncovered hundreds of stolen accounts on sale for as little as £3 each.

NETACEA

A strain on time, resource and partnerships

The impact of these account takeover attacks was wide reaching, requiring meetings across the client's fraud and security teams to triage. Their SOC was dealing with attacks as they happened and deploying rules onto legacy firewalls based on the attack vectors they could analyze. Attacks were so persistent that their teams could only see spikes in traffic and not less volumetric attacks that persisted constantly at a low level.

The malicious activity also created a backlog of support calls from frustrated customers who were locked out of their stolen accounts or had been charged for streaming services they never signed up for.

The issue was also damaging the business's reputation with media streaming partners, who were frustrated that their services were being stolen, requiring them to repatriate or cancel accounts.

The solution

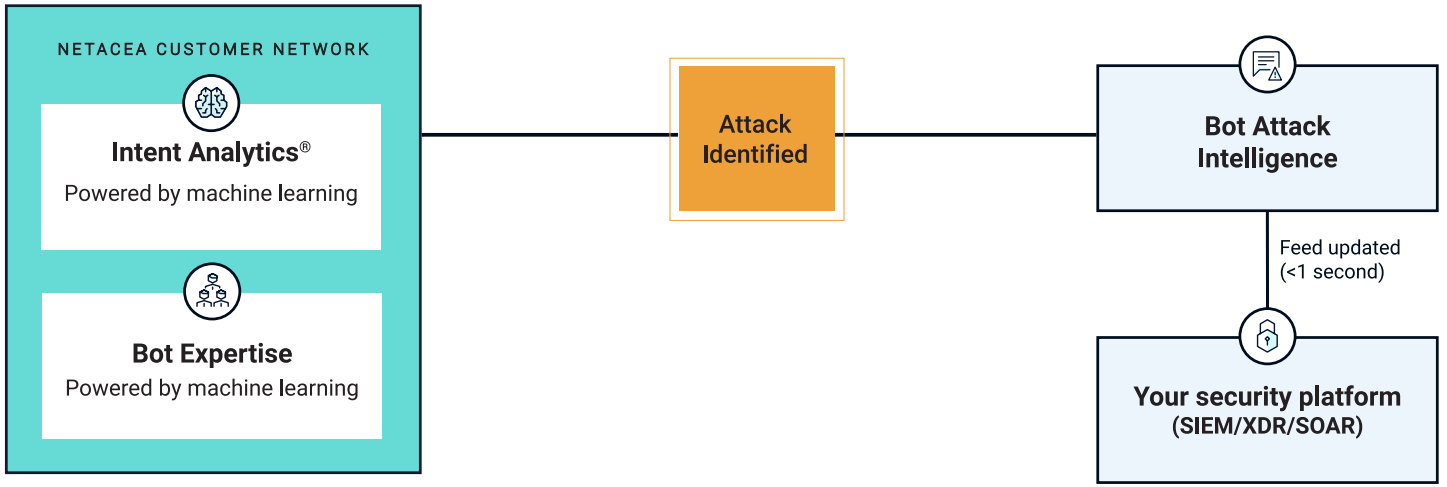
The partner needed an immediate solution to quickly gain control of access to their streaming services.

Netacea's Bot Attack Intelligence service was an ideal solution to get rapid results. Netacea analyzes billions of web requests across our network each day, analyzing every single one for malicious intent using our suite of machine learning algorithms. This data is augmented by our team of bot experts who analyze patterns and input intelligence from threat research gathered from breaching adversarial communities. The feed is constantly updated, with novel attackers added within a second of being identified within the Netacea platform.

This feed of over 11 million verified attacker datapoints was passed to the partner, who plugged the data directly into their existing risk engine and bot mitigation tooling.

The simplicity of the implementation meant the solution had an immediate impact, with the partner noticing a steep drop in the number of breached accounts reported by customers and seen on sale on the dark web.

The partner was also impressed by the extremely low false positive rate, with no reports of legitimate customers being erroneously blocked by the mitigation service.



The outcome

Netacea's Bot Attack Intelligence has provided highly accurate attacker information leading to the partner mitigating an average of over 1,000 malicious login attempts per hour across their website, apps, and API. This peaked at over half a million attempts per hour during the most aggressive attack.

By preventing user accounts from being stolen, Netacea has saved the partner millions in costs across several teams, including infrastructure, fraud, and risk. They have protected the organization's brand reputation with customers, regulators, and third-party streaming partners, whilst stemming calls to their customer support call center.

About Netacea

Netacea provides an innovative bot management solution that solves the complex problem of credential stuffing, account takeover and other malicious bot activity for our customers in a scalable, agile and intelligent manner, across websites, mobile apps and APIs.

Our Intent Analytics® engine is driven by machine learning to provide an in-depth analysis into all traffic on your site. This gives us an incredibly fast and comprehensive understanding of human and automated traffic behavior, enabling us to identify and block bots in real time with unparalleled accuracy.

With machine learning at the heart of our approach, our technology provides an innovative and profoundly effective solution that is configurable to your environment and adapts to changing threats.