Saving a top 3 telecoms provider £1 million by preventing streaming account theft

NETACEA

Saving a top 3 telecoms provider £1 million by preventing streaming account theft

THE CHALLENGE | THE SOLUTION | THE OUTCOME

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

- / £1 million saved by reducing customer support calls
- / On average over 1,000 and a peak of over 500k malicious login attempts blocked per hour
- / More than 350,000 account takeover attempts using stolen login details blocked in a under a year

THE CHALLENGE

The client is one of the top three largest multinational telecommunications companies based in the UK. They provide a wide range of services including fixed-line, broadband and mobile services to over 15 million customers.

Like most telecommunications businesses, their customers can access streaming media services, such as Netflix, Spotify and Apple TV, included in their broadband and television package subscriptions or as an add-on. These are bundled as part of partnership agreements between the business and the content providers.

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.

Once they gained access to the accounts, hackers 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. Customers would then be hit by unexplained add-on bills for these services or unexpectedly lose access to their accounts.

The impact of these account takeover attacks was wide reaching, requiring meetings across the client's fraud and security teams to triage, using up unnecessary infrastructure and licenses. The malicious activity also created a backlog of support calls from frustrated customers who were locked out of their stolen accounts.

The issue was also causing friction with the business's media streaming partners, who were frustrated that their services were being stolen, requiring their action to repatriate or cancel accounts. The client needed a solution to protect their reputation with streaming media partners.

Whilst our client knew this activity was caused by automated bots, any previous success at blocking them was short-lived as the adversaries quickly shifted tactics and hit back even harder.

The business initially asked Netacea to investigate web log data from a two-day period and identify malicious traffic during this time.

Attack overview: Two days of malicious activity

- / 18% of all login requests made by malicious bots
- / Bot attacks distributed across 11,000 IP addresses
- / 470,000 login attempts by bots across the two-day period

Netacea identified that over 18% of all login requests were made by malicious bots, accounting for nearly half a million attempts to compromise customer accounts in this 48-hour timeframe alone.

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.

FREE TRIAL

Find out how Netacea's unique approach to bot management can help your business keep bad bots at bay. Get a personalized demo of Netacea Bot Management for your business and get control over your website traffic.

These attacks were often highly distributed to evade detection from traditional defenses.

In one attack, each IP address made the exact same number of requests before stopping, indicating knowledge of the client's rate limiting and IP blocking rules. These defense measures were easily bypassed by continual 'low and slow' attacks using rotating IP addresses.

In all, Netacea identified 471,614 malicious login attempts originating from 1,799 data centers, 11,247 IP addresses and 116 countries in just two days' worth of data.

Based on these findings, the business engaged with Netacea to implement live analysis on real-time traffic in an ongoing engagement.

THE SOLUTION

Netacea worked closely to integrate into the authentication service for all the client's sites, apps and APIs, covering all potential bot attack vectors. Netacea investigates each request made on the platform, comparing every data point to distinguish between humans, benign bots and malicious bots. This allows for instant recommendations on whether to permit, challenge or block traffic.

Adapting to new and changing attacks with AI

Previous attempts by our client to block bot activity had limited success. The bot operators quickly identified rule-based blocking methods and found new ways to bypass defenses.

Netacea's next generation bot management technology, Intent Analytics®, detects complex attacks by using a combination of machine learning approaches that are invisible to attackers.

Firstly, we feed every user interaction into supervised machine learning models, which are trained by previously categorized bot activity. This flags any users who are behaving in the same ways as other known malicious users and can predict when attacks will occur based on previous patterns.

Then we detect emerging or changing threats without the need for trained data using unsupervised machine learning algorithms. With no requirement for predefined labels or human intervention, these models group users into clusters based on their behavior. Anomalous and malicious behavior is highlighted, and the clusters are continually reevaluated, moving users between them as new patterns of activity emerge.

This means that Netacea continually improves its bot detection technologies with each new attack type used against our clients, strengthening our defensive capabilities, and keeping our clients ahead of their adversaries.

THE OUTCOME

Over a period of nine months, Netacea has mitigated an average of 1,200 malicious login attempts per hour across the client's website, apps, and API. This peaked as high as 600,000 per hour during the most aggressive volumetric attack.

During this time, Netacea has also put a stop to over 120,000 account takeovers – attempts by bots to log in using valid but stolen username and password pairs.

By preventing over 350,000 user accounts from being stolen, and assuming a 10% call-in rate, Netacea has saved the client potentially £1 million to date in calls to their customer support call center alone, without taking into account the cost of investigation, analysis, refunds, and reputational damage.

More importantly, the client's customers are now protected against account theft. This removes disruption to their services, which is a key deliverable for the business, and allows the client to focus on their goal of improving the lives of their customers.