NETACEA / CASE STUDY

Protecting customers of leading baked goods brand from loyalty point theft

NETACEA

Protecting customers of leading baked goods brand from loyalty point theft

THE CHALLENGE | THE SOLUTION | THE OUTCOME

CUSTOMER PROFILE

/ Baked goods and coffee-house chain operating in over 1,000 locations across the UK

/ Online delivery and click-and-collect services available

/ Loyalty reward scheme available via mobile app

RESULTS

/ Highly distributed bot attacks mitigated using advanced machine learning techniques

/ Loyalty point theft attempts blocked in real time with high level of accuracy

/ Seamless integration with eCommerce platform and mobile app

THE CHALLENGE

The client is a world-famous American baked goods and coffeehouse chain operating in the UK. The premium food brand has over 130 dedicated stores nationwide, whilst also selling its freshly made produce in over 1,000 third-party locations.

Like many food businesses, the client had to quickly adapt when the pandemic hit in 2020, switching focus from in-store sales to accommodate delivery and click-and-collect services to satisfy its customers. This meant an increased reliance on technology, both for the business itself and for its customers.

To remain competitive and keep customers coming back for more sweet treats, the client offers a loyalty points scheme, whereby customers can earn rewards like free items and birthday gifts. New customers are also offered a free treat upon creating their account. The loyalty scheme is managed via their website and mobile app.

Unfortunately, any website or app with a login page or user account functionality is a target for account takeover attacks, especially where redeemable credits are stored. As a leader in their space, our client was at particular risk, especially as it looked to further expand its dominance of the market.

Account takeover: The risk of offering rewards

Account takeover (ATO) attacks are used by bad actors to compromise the victim company's customer accounts. Rather than hacking the client's systems, the criminal obtains either full or partial account login information, typically from a data leak elsewhere or the dark web, then uses automation to verify the validity of those details on the platform. If credentials like passwords are missing, they will often use credential stuffing bots to rapidly test large lists of common passwords to access the accounts with brute force.

Once the adversary has gained access to an account, they will quickly lock the legitimate owner out and use up any reward points and assets held within. Professional attackers use tools to aggregate these accounts, creating an opportunity to sell on loyalty points balances at a reduced rate to unscrupulous buyers on the dark web. Since most customers may not check their accounts until they are making a purchase themselves, attacks go undetected by the account owner until much later.

These attacks are difficult to prevent and require a different approach from traditional cybersecurity defenses, particularly because user accounts are being accessed via their legitimate login details, even if gained through wrongful means.

Credential stuffing attacks are also extremely aggressive in their volume and speed. As bots attempt hundreds or thousands of username and password combinations in a short amount of time, the victim website's infrastructure is strained. This leads to slower response times for legitimate customers, increased operational costs to fix the problem, and higher hosting fees.

ABOUT NETACEA

Netacea provides an innovative bot management solution that solves the complex problem of web scraping and malicious bot activity for its 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 to 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.

THE SOLUTION

Netacea Bot Management was quickly integrated with the client's Magento-based web environment. Netacea initially analyzed traffic on the user login page to detect any account access attempts made by malicious users and bots. Over the initial 28-day period, Netacea analyzed 89 million requests.

Bots typically attempt to avoid detection by mimicking human behavior or traffic origins. For example, requests may originate from multiple countries or data centers, or use different user agents, despite all acting in the same manner for a common malicious purpose.

Netacea's Intent Analytics™ engine looks past these easily spoofed signals to analyze the behavior of every request made, using advanced machine learning to group these together in real time and spot malicious bots amongst legitimate users. Recommendations are then passed to the client, either as a feed to their SIEM or actioned directly on their platform.

THE OUTCOME

Netacea found that a significant portion of the login attempts made on the platform were made by malicious bots.

Attack overview:

/ On a single day, over 4,000 attempts to compromise customer accounts were detected

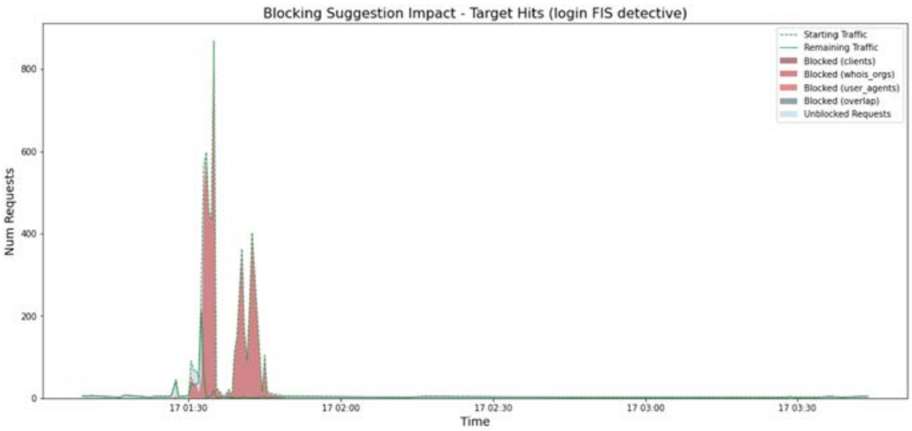
/ Malicious login attempts accounted for 23% of overall login requests

/ Login attacks were distributed across 10 countries

While several attacks were spotted over time, one attack saw over 4,000 attempts made to compromise customer accounts within the space of two hours. This accounted for nearly a quarter of all login attempts.

This was a highly distributed attack, likely designed to avoid detection by spreading request origins across 10 countries and multiple data centers. However, Netacea's multilayered approach was able to identify and group these malicious requests together.

The suspicious traffic was served a CAPTCHA challenge, with 100% of these challenges failed, indicating an extremely high level of bad bot detection accuracy. As a result, the attack was mitigated successfully, protecting customer accounts from unwanted access.


Blocking Suggestion Impact - Target Hits (login FIS detective)
Starting Traffic
Remaining Traffic
Blocked (clients)
Blocked (whois_orgs)
Blocked (user_agents)
Blocked (overlap)
Unblocked Requests
Num Requests
17 01:30
17 02:00
17 02:30
17 03:00
17 03:30
Time