NETACEA / CASE STUDY

American Big Box Retailer Cuts API Abuse By 84%, Eliminating Billions of Malicious Requests Daily

NETACEA

American Big Box Retailer Cuts API Abuse By 84%, Eliminating Billions of Malicious Requests Daily

THE CHALLENGE | THE SOLUTION | THE OUTCOME

CUSTOMER PROFILE

- American big box retailer
- Online revenue over $15 billion
- Product categories include gaming consoles and clothing

RESULTS

- API requests reduced by 84%, representing over 10 billion requests per day
- Price and content scraping massively decreased
- Infrastructure requirements reduced
- Potential attacks such as scalping avoided

THE CHALLENGE

The client is a big box retailer with over 1,500 stores across the United States. Their ecommerce website generates revenues of over $15 billion annually, selling a wide range of products including high demand items like gaming consoles.

The eCommerce site sells a vast product range and is built on a microservices architecture using several APIs; like most big box retailers, their product listing API provides information on each item they sell, including price, availability, and specifications.

Adversaries were exploiting this API by feeding custom-written scripts into bots to access product information at scale.

This high velocity of API calls was impacting customers browsing the site, both directly by clogging up the API and slowing down response times, and indirectly by facilitating other attacks, for example snatching the full inventory of high-demand products such as PlayStation 5 and Xbox Series X consoles within seconds.

The dangers of web scraping

Malicious web scraping can help competitors undercut prices, steal content, or collect information and resources to prepare other attacks. For example, bots aggressively scrape product pages and APIs many times each second, looking for an indication the product is available. Scalper bots then swoop in instantly and buy up all the stock before genuine customers can react, forcing consumers to buy the products from scalpers on secondary markets at an inflated cost.

Adversaries use scraping to gather information facilitating account takeover attacks, from which they can steal personal information and payment details. Content scraping is also a means for criminals to clone websites, facilitating fraud and scamming users out of login or payment details.

Even otherwise harmless scrapers like search engine crawlers and product availability trackers can damage websites if a high volume of requests overloads the service, which can impact performance and availability.

THE SOLUTION

Netacea captured every API request using a low friction, low latency integration via the client's CDN. This meant no changes to their applications were needed.

As the client is one of the biggest retailers in the United States, volumes of traffic are extremely high, even before factoring in aggressive scraping activity. This equates to billions of requests each day, peaking at over 200,000 requests per second during the initial proof-of-concept phase.

Using AI to mitigate evolving threats

These requests were then analyzed by Intent Analytics®, our real time threat detection platform, which uses AI and machine learning to categorize traffic by its intent and makes recommendations to permit, block or investigate in real time.

Generic API attacks are often high volume, come from a single or small batch of origins (IP addresses, datacenters, etc.) and are low complexity, making them easy to detect. More sophisticated attacks are built to target individual APIs and seek to avoid detection by more closely emulating human behavior.

Intent Analytics uses machine learning algorithms to continually analyze every single request and rapidly categorize all types of API attack, from broad to targeted, fast to slow, and simple to highly distributed.

Netacea's adaptive AI patches new vulnerabilities as quickly as adversaries introduce them. We continually assess how the client's API is being called, highlighting malicious activity, and taking corrective action instantly. Our machine learning algorithms constantly evaluate every API request by asking three questions:

How does the user profile compare to known bad actors on this platform?

Based on previously seen bot activity, our machine learning algorithms compare all traffic to all other user interactions.

How does this user compare to other users currently using the system?

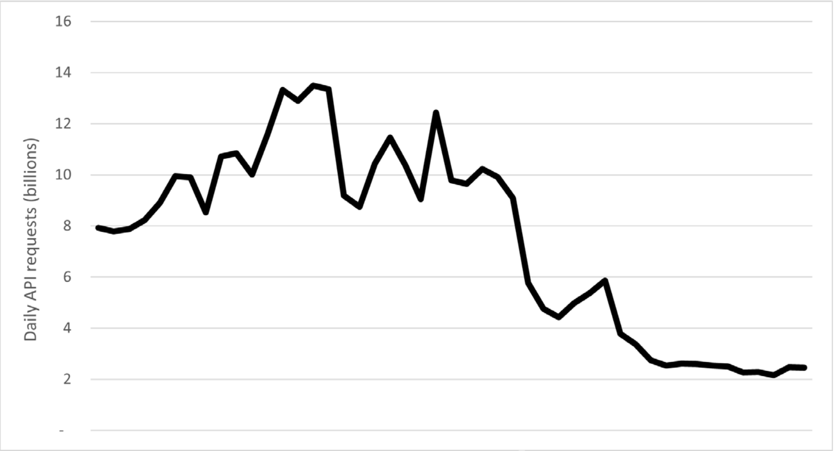
Using dynamic clustering to group similar users, Netacea's AI platform spots when new clusters are created, highlights atypical behavior, and constantly re-evaluates what 'normal' looks like.

Is overall activity unusual?

By utilizing recurrent neural networks and analyzing what has happened before and recently, we can predict what should happen in the next few minutes and highlight unexpected activity.

THE OUTCOME

Netacea's API Security reduced daily requests to the API by 84% (over 10 billion requests) within weeks of implementation. Mitigating API attacks has protected the client against content and price scraping, and scalper bots, as well as reducing infrastructure requirements.



Daily API requests dropped from nearly 14 billion to around 2 billion within weeks of Netacea mitigation

The three most popular requests during the peak trading season were to listings for the PlayStation 5, PlayStation 5 Digital Edition, and Xbox Series X console. Netacea's AI and Bot Experts team detected that half of these requests were made by automated bots with malicious intent.

It is likely that this scraping activity was just the first part of a larger attack, most likely scalping for resale on secondary markets. By blocking these requests, Netacea cut off the attackers' kill chain, preventing later threats from occurring.

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.