Netacea Client Stories

NETACEA

Saving A Top 3 Telecoms Provider £1 Million By Preventing Streaming Account Theft

Challenge

A top three telecommunications provider offers access to premium streaming services as part of product bundles, which 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.

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.

Results

Netacea bot management saved the client more than £3 millions by reducing the number of customer support calls. We saw a peak of 500,000 malicious login attempts blocked per hour and saw more than 100,000 account takeover attempts using stolen login details blocked in a nine-month period.

American Big Box Retailer Cuts API Abuse By 84%

Challenge

A big box American retailer has an eCommerce website generating revenues of more than $15 billion annually. Adversaries were exploiting its API by feeding custom-written scripts into scraper 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.

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. Volumes of traffic are extremely high, peaking at over 200,000 requests per second during the initial proof-of-concept phase.

Results

Using Netacea Bot Management meant API requests were reduced by 84%, representing more than 10 billion requests per day on the site. As a result, price and content scraping massively decreased, infrastructure requirements were reduced, and future attacks avoided.

Global Sportsbook Protects Odds IP And Maximizes Event Capacity

NETACEA

Challenge

A large global bookmaker was facing high levels of automated traffic on its website. Bots were being used to scrape data and odds from the customer's website and this large volume of unpredictable traffic was threatening website availability for everyday customers and increasing infrastructure costs across the business.

This malicious activity increased in the lead up to and during peak sporting events. Worse yet, the scraped data was being used to exploit imbalances in the odds across multiple operators.

Despite having several solutions such as WAFs and fraud tools in place, the business lacked visibility of bot traffic and was dependent on manual analysis to block and mitigate attacks.

Solution

Netacea identified how much of the traffic was malicious bots. Recommendations were then sent to the internal client's SIEM solution. Depending on how aggressive the scraping was, the operator took automated actions including requesting further verification, CAPTCHA, Blackhole or limiting account functionality.

Results

The client has experienced an 85% reduction in unwanted automated betting by bots. CPU usage has reduced by 7%, bandwidth by 5.2% and the number of requests by approximately 40%. Netacea is helping the client deliver an estimated saving of £3m per year and allowing for an increased capacity of real customers at critical times.

Protecting A Growing Fintech Against Credential Stuffing Attacks

Challenge

A fast-growing global FinTech organisation was frequently observing large spikes in automated bot traffic on its login pages and APIs. The business was concerned about the risk the traffic posed to its customers.

Tackling this traffic put strain on the internal SOC team, which was regularly required to carry out late-night manual blocking of suspicious traffic to minimise the threat to customer accounts.

Despite having a WAF and CDN solution in place, the increasing necessity for manual blocking and risk of exposure of customer data made it abundantly clear that sophisticated bots were continually bypassing traditional security measures.

Solution

Netacea's Data Science team identified that malicious bots were persistently bombarding login pages using automated credential stuffing techniques. The business quickly deployed Netacea Bot Management into its CloudFlare CDN using pre-built CloudFlare Workers.

Netacea's automatic blocking, autoscaling and proactive monitoring enables the solution to meet demand during periods of peak usage, taking the pressure off the customer's internal SOC team.

Results

Netacea's dashboards quickly illustrated the extent of the bot attacks. After six months, Netacea blocked an average of 250,000 credential stuffing attacks per week, protecting more than 10 million accounts. The client has seen a 5% reduction in traffic to login pages while internal resource is preserved.