Hardware retailer nails aggressive price scrapers with advanced bot management

NETACEA

Hardware retailer nails aggressive price scrapers with advanced bot management

THE CHALLENGE | THE SOLUTION | THE OUTCOME

CUSTOMER PROFILE

- US based network of online hardware stores
- Operates over a dozen retail websites
- Provides ecommerce services to other home improvement businesses

RESULTS

- Without Netacea, the client would be serving up to 50% more traffic due to bots
- Competitors are now unable to scrape pricing data from the client's websites
- Server load related outages caused by bots are regularly mitigated by Netacea

THE CHALLENGE

The client is a US based online retailer operating dozens of ecommerce websites in the hardware industry. They also provide a suite of ecommerce services to other businesses within the home improvement sector.

The client was being inundated by web scraper bots, which were accounting for as much as 75% of their web traffic. Although some web scrapers are acceptable, such as search engine indexing, others are either too aggressive or were crawling the websites with malicious intent.

For example, consumers usually research home improvement purchases online to find the lowest possible price. Retailers use scraper bots to automatically undercut prices of their competitors and gain an advantage, damaging their rival retailers' profit margins.

Also, manufacturers frequently use minimum advertised price (MAP) agreements to prevent retailers selling their items below an agreed price floor. Breaking this agreement can lead to the manufacturer imposing restrictions on the seller. Competitors use pricing intelligence scraper bots to check whether retailers are adhering to MAP agreements, and report violations to the manufacturer, again to gain a competitive advantage.

Performance, infrastructure and forecasting issues

Bot activity on our client's websites had become extremely aggressive, especially in the wake of the global pandemic. With a variety of bots scraping the platform for different purposes at any given time, plus the day-to-day and sale traffic, the business was increasingly frustrated by performance degradation and outages. Customer experience was being affected negatively, leading to complaints and loss of customers to competitors.

The prevalence of these bots also made it challenging to forecast traffic levels. The business found that their projections had gone from being predictable and consistent to quadrupling above anticipated levels due to bot traffic. The result of this was budgets for third parties being missed by a significant margin. The business also did not want to provision additional infrastructure just to serve bots that were potentially designed to harm their business.

The business had previously attempted to block this kind of traffic using another bot management solution but found that most of the bots bypassed this layer of defense. They turned to Netacea's advanced AI-powered bot management solution for assistance.

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 was quickly put in place with an agentless implementation covering the entire estate of retail websites, removing the need to install and maintain individual JavaScript code on every site.

The client first wanted to get a better insight into what these bots were doing and how much of this traffic should be blocked. Netacea's Intent Analytics™ engine categorizes the intent behind every request made across their platform to determine whether it is non-human, and if so, whether it is part of a malicious attack.

This is done using a multilayered approach, combining data from past attacks across Netacea's user base with advanced machine learning algorithms to detect anomalous behavior. The output is also analyzed by Netacea's team of bot experts.

Combining these methods, attacks are quickly mitigated, either by passing suspected bad actors to a CAPTCHA challenge or by blocking them outright.

THE OUTCOME

Netacea keeps bad bots at bay, regularly detecting attempted scraping efforts and blocking them from accessing the client's websites with a high level of accuracy. Since implementing Netacea Bot Management, the business has reduced overall traffic by up to 50% by preventing scraper bots from crawling their sites.

Attack overview:

- 810,961 malicious requests mitigated by Netacea over the course of three days
- 100% "CAPTCHA incomplete" rate meaning extremely accurate mitigation
- Potential outages avoided and infrastructure costs saved

In just one attack attempt, scrapers attempted to flood one of the client's websites with over 810,000 requests over the course of three days. Without mitigation, the peaks of this activity could have easily caused outages and serving these requests would have had significant financial and operational implications.

Netacea's Intent Analytics™ engine rapidly evaluated the behavior of each request, blocking known bad actors immediately and passing suspected bad bots to CAPTCHA for verification.

None of the mitigated traffic completed CAPTCHA, confirming that they were indeed bots and that Netacea's suggestions were extremely accurate.

Fig 1: Several large-scale scraper bot attacks mitigated over the course of three days by Netacea Bot Management