CEQUENCE

Case Study

Ulta Beauty Reduces Costs by Blocking API-based Enumeration Attacks

ULTA BEAUTY

Executive Summary

Cequence Security assisted the Ulta Beauty CTI team to mitigate a persistent, high volume inventory API scraping attack. While the goal of the attack was uncertain, potential motivations include enabling real world shoplifting opportunities by mapping popular inventory. The attack was executed across a 3rd party local-inventory search API, and mitigating it saved Ulta Beauty significantly across infrastructure and inventory costs.

Enumeration Attack Against 3rd Party API

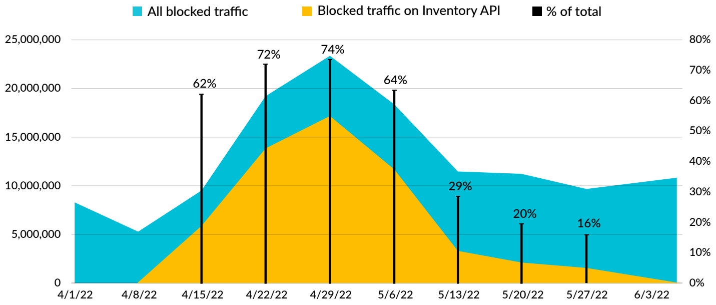
The attack unfolded as the volume of requests against local-inventory search API spiked at 700X normal volumes rotating through more than 153,000 unique product and SKU combinations while scraping 61,000 zip codes and 33,000 products. The local-inventory search API supplier notified the Ulta Beauty team of the sudden traffic surge and an investigation uncovered an enumeration attack with the following characteristics:

- High-quality, residential proxy IP addresses were used to make IP blocking at the edge difficult
- The attack enumerated through ZIP codes to find high concentration of particular products with higher retail values
- Initially, web API was targeted but that quickly pivoted to the analogous mobile API which provides similar information

Collaborative Efforts Save $80,000

Working together, the Ulta Beauty CTI and the CQ Prime Threat Research Team put policies in place that have successfully blocked 85.9M total requests since April 1st resulting in $80,000 saved in infrastructure and loss prevention. At the height of the attack, policies were blocking upwards of 17M requests as shown in the following chart.

Enumeration Attack on Local Inventory Check API



Policies block traffic that exhibit the following behaviors:

- **Direct-to-API:** The attack was designed to target the inventory API directly, without hitting any other app or web function. Normal behavior would show the user traversing multiple APIs.
- **Volumetric threshold:** The attacker used enumeration to rotate through the inventory at such a volumetric rate that it represented 90% of ALL the customer traffic at the time.
- **Outdated browser:** The attack was built to use very outdated or anomalous versions of Chrome.
- **Single cookie generation:** Each attack generated a single cookie whereas normal users would generate upwards of 40-50 cookies as they browsed the inventory.

A Win for All Parties

The rapid response and teamwork in blocking this attack resulted in a win for Ulta Beauty to the tune of $80,000 and a win for the local-inventory search API vendor, which no longer needed to bear the increased infrastructure costs. It's also a win for the CQ Prime Threat Research Team who mobilized quickly to identify the attack, motives, behaviors and respond with appropriate blocking policies.