case study

COMBATING THE BOT ATTACKS AGAINST AN E-COMMERCE COMPANY

THE BUSINESS:

This case study is about one of the large e-commerce platforms. The company has been the largest retail platform in Indonesia, with 139 stores in 77 cities across Indonesia, as well as an online presence. For over 60 years, the company has provided the growing Indonesian middle class with quality, fashionable and affordable apparel, beauty, and footwear products. The organization employs around 40,000 employees (including consignment SPGs) and partners with around 600 local and international suppliers.

It is one of the leading, most dynamic, and trusted companies in Indonesia.

Recently, they observed a few anonymous activities on their website as someone was continuously bombarding their registration form with the same and different details that were fake to choke the bandwidth of their website. They also noticed high spikes on their backend server due to these automated bot activities. These registration forms are used for the customers' ease-of-use and to identify themselves prior to purchasing the products, which help to avail the discount codes in the future.

Furthermore, their security team analyzed the traffic and confirmed the fake accounts' creation with the help of an automated bot threat used by cybercriminals to commit fraudulent acts such as influencing product reviews, distributing false information, or spreading malware to slow down the website.

CHALLENGES BEFORE INDUSFACE:

The various challenges this organization faced due to this bot attack were:

1. **Identity Source Data:** Before running the user registration process, bad actors would obtain the identified source data, either stolen data, fabricated data, or a combination of the two, and use the bulk data as inputs for their next fake profile attack phase, which impacted their database servers.

2. **Registration/User Enrollment Process:** Threat actors used automated bot attack scripts and APIs to sidestep new account registration forms and generate them behind the scenes in large quantities. Because of this, their servers got flooded with huge amounts of fake data.

3. **Business Impact:** This malicious bot attack attempts to scrape the retailer's proprietary product listings and pricing data, take over customer accounts using credential stuffing techniques, and place products into carts only to abandon them, which impacts their daily business with regular customers.

4. **Loss in Revenue:** All these bot attacks could potentially lead to considerable losses in revenue, operational expenses, and brand reputation.

This was certainly not a situation that any online retailer would want to confront on an ongoing basis.

STRATEGY & RECOMMENDATIONS BY INDUSFACE:

We analyzed the behavior of these bot attacks and suggested to them the below custom rules be applied to AppTrana:

1. Tracking the same IP of an intruder when filling up the registration form and blocking the IP for 1 day when more than 5 requests are received from the same IP within 30 mins.

2. Tracking the same IP/session of an intruder submitting multiple registrations and blocking the IP for 3 hours when more than 3 requests are received from the same IP in 10 mins.

3. When the same IP and same email address are being used, then blocking the IP for 1 day when we see hits more than 3 times in 30 mins.

4. When the intruder is using a different IP with the same email address, then we will block the IP for 1 day when we see hits more than 3 times in 30 mins.

5. Block requests based on a malicious user-agent as per the traffic analysis or organization's need.

IMPLEMENTATIONS:

The organization confirmed to proceed with the below 2 custom rules to see the behavior of the attacks blocked with the help of the policies applied through AppTrana.

1. Tracking the same IP of an intruder when filling up the registration form and blocking the IP for 1 day when more than 5 requests are received from the same IP within 30 mins.

2. Tracking the same IP/session of an intruder submitting multiple registrations and blocking the IP for 3 hours when more than 3 requests are received from the same IP in 10 mins.

RESULTS:

The custom policies now block an average of over 32000 bad bot requests trying to register the application on a single day and prevent them from carrying out a slew of harmful activities against the retailers and their customers, including

1. Stopping fake registration forms to protect the customer from fraud
2. Preventing systematic scrapping to help the retailer protect its competitive advantages
3. Ending the cart abandonment to increase the product availability to genuine shoppers
4. Blocking bad bots results in a better user experience and low infrastructure costs
5. Accurate traffic analytics to help the retailer optimize the operational and market strategy
6. Reduction of spikes on their server's traffic logs to increase the performance of the servers
7. Eliminating affiliate fraud (a win-win for both the retailer and its affiliates)

SPOTLIGHT

Customer

SOLUTIONS DEPLOYED

- Indusface AppTrana

ABOUT THE COMPANY

One of the largest E-Commerce platforms in Indonesia that provides apparel, beauty, and footwear products.

HEADQUARTERS

Tangerang, Indonesia

SIZE

40K Employees; 700 Suppliers

INDUSTRY

Retail & E-Commerce

HIGHLIGHTS

32K

The total number of bot attacks blocked through Apptrana

2

Custom rules applied through AppTrana

KEY HIGHLIGHTS

Blocking bad bots resulted in lower infrastructure costs and a better user experience.

Stopped fake registration forms to protect the customer from fraud

Prevented systematic scrapping to protect the competitive advantages

Decreased cart abandonment rate & increased the product availability to genuine shoppers