INDUSFACE™

CASESTUDY

Mitigating a Botnet-Driven DDoS Attack on a Fortune 500 Company

SOLUTION HIGHLIGHTS:

8 million IPs

DDoS attacks were carried out from 8 million unique IPs for 14 days

3000X-14000X DDoS Traffic

The DDoS attack traffic ranged from 3000X – 14000X, the usual daily traffic

100% Availability

100% availability ensured while saving thousands of dollars in additional bandwidth expenditure

ABOUT THE CUSTOMER:

The customer is a Fortune 500 company with a presence in over 30 countries and has been running its businesses in a wide range of sectors for over 5+ decades.

The website provides details on various commodities that could be traded in bulk on a global scale.

KEY CHALLENGES:

- A targeted Distributed Denial of Service (DDoS) attack was launched by Botnets by flooding a series of HTTP requests against their application.
- The volume of this HTTP Flooding attack was 3000X – 14000X higher than the usual requests/min received on the site, and the attack used around 8 million unique IPs for 14 days.
- Rate-limiting could only counter some DDoS attacks, as some IPs were sending only one request per minute and there's no way to set the rate-limit to such a low level
- This high volume of traffic on the application led to slowness, increase bandwidth consumption, and disrupted legitimate users to access the services.
- This attack was unique because most were targeted on the base URLs, which were either non-existent or not publicly exposed (e.g.,/404, /admin, /config).
- Identifying the traces of vulnerability exploitation was also challenging, as there was no attack payload related to any platforms and no cookie details.
- The majority of attacks were seen to be coming from Android-based mobile devices using various data centers, anonymous proxies, Tor IPs, and IPs with bad reputation.

STRATEGY & RECOMMENDED SOLUTION:

Indusface reviewed all these details and strategically deployed a solution to address the above problem. Deployed custom policies to bring down these attacks to zero.

URI Blacklisting Policy:

All external requests to URLs that were not meant for public access were blocked. Only internal teams with specific internal IP addresses were permitted to access them.

Rate-Limiting Rules:

- IP-based rate limiting threshold was updated to 100 req/min & blocking duration as 60 mins.
- Implemented a rule to block an IP for a week if it accesses '/' URL more than 20 times in a minute.

Custom Rule to Allow Requests Only from Browsers

The system detected non-browser or headless requests when a WAF cookie was absent. The system only granted access to the origin when the request contained the WAF cookie.

Geo-Fencing Rules:

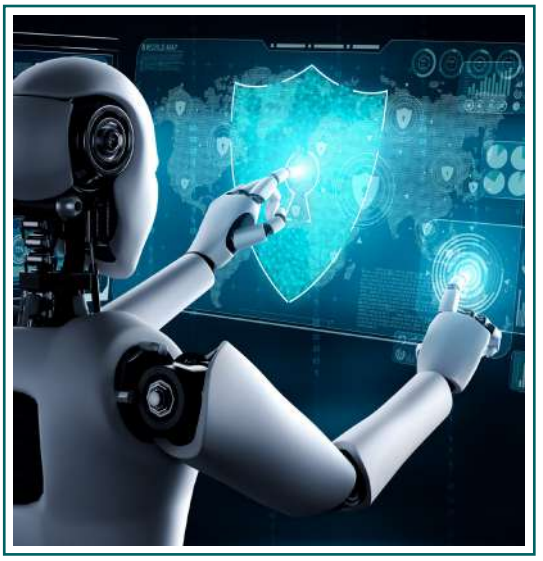
Block suspicious traffic from Nepal, Bangladesh, and Pakistan; as some requests were seen from these locations, the customer didn't have any scope for business in these locations.

Increased The Tolerance for Bot modules

- Updated tolerance level from High to Low.
- Enabled additional modules to detect and block requests concerning Tor nodes & data centers.

Deployed Custom Rules to Block Anonymous Proxy

A rule was implemented to detect and block harmful bot requests attempting to access the blacklisted URIs. This was done by analyzing the trend of attack requests over a period of time.

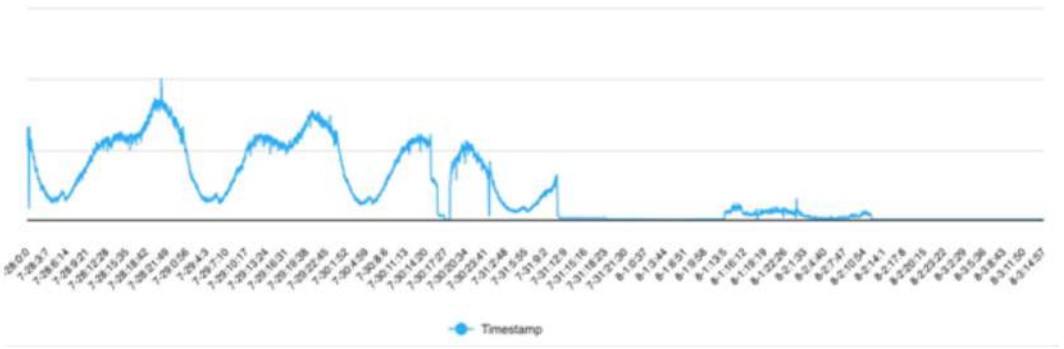


RESULTS:

- Successfully blocked all the bot traffic at the WAF level, and valid business users were forwarded to the application server.
- Users faced no lag in the website's usage and witnessed zero service disruptions.
- Saved thousands of dollars in additional bandwidth expenditure over the 14-day period

CHARTS:

Log/Block Chart



Incoming requests chart