INDUSFACE™

CASESTUDY

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

SOLUTION HIGHLIGHTS:

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

The DDoS attack traffic went up by up to **14000X**, the usual daily traffic

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

Thousands of dollars saved in data-transfer costs as these were blocked on AppTrana

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
- Static rate-limiting (which was requested by the customer initially) could counter only some DDoS attacks, as many IPs were sending very few requests per minute or a request every few minutes. The tactic was to use millions of IPs to overwhelm the origin server while falling under the min threshold value for rate-limits
- However, the volume of this HTTP Flooding attack was 14000X higher than the usual requests/min received on the site, and the attack used around 8 million unique IPs for a couple of weeks
- Most attack 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

APPTRANA'S DDOS MITIGATION POWERED BY BEHAVIOURAL AI AND MANAGED SERVICES HELPED IN BRINGING DOWN THESE ATTACKS TO ZERO

AppTrana DDoS mitigation powered by behavioural AI capabilities and managed services, deployed default and custom policies to bring these attacks down to zero.

URI Blacklisting Policy:

The AI engine blocked all external requests to URLs that were not meant for public access as soon as the DDoS requests/ site traffic increase was witnessed. Only internal teams with specific internal IP addresses were permitted to access them.

Rate-Limiting Rules:

- The AI engine suggested keeping the IP-based rate limiting threshold at the lowest as well as the blocking duration for the IP for a higher amount of time, which was accepted and deployed by the managed services team
- The AI also blocked the IP for a set duration in case it witnessed any IP accessing the '/' URL higher times in a minute, as compared to the range of a normal user

Custom Rule to Allow Requests Only from Browsers

AI engine detected the headless requests. The system only granted access to the origin when the request contained the WAF cookie.

Geo-Fencing Rules:

The AI engine automatically detected suspicious traffic from countries where the customer didn't have any scope for business and blocked these requests. All the logs of the block requests were sent to the customer and the managed services team.

Automatic Reduction in the Bot Tolerance Levels by the AI Engine:

- Auto-updated the tolerance level from High to Low as soon as there were a higher number of requests and signs of Low-rate DDoS attack
- Auto enabling of additional modules to detect and block requests concerning Tor nodes & data centers

Deployed Custom Rules to Block Anonymous Proxy

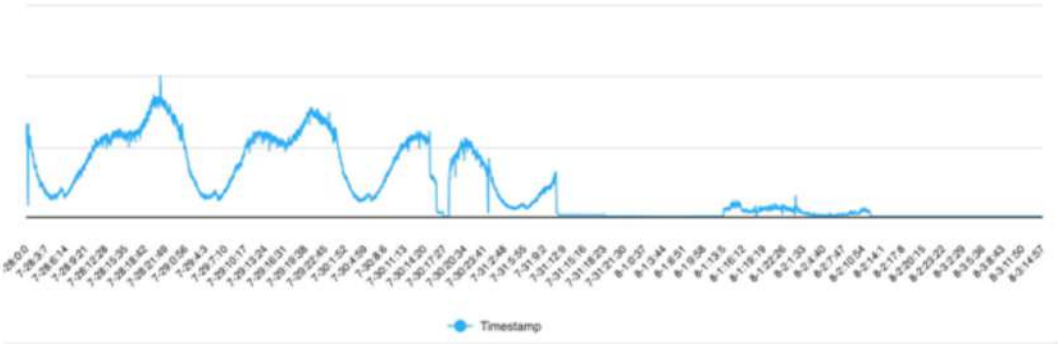
A rule was implemented by the managed services team to detect and block harmful bot requests attempting to access the blacklisted URIs. This was done by going through the notifications they received from the AI engine after analyzing the incoming traffic.

RESULTS:

- Successfully blocked all the bot traffic at the WAF level, and only 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
- All the rules were deployed within the SLA time frame provided to the customer, along with continuous monitoring and removal of false positives

CHARTS:

Log/Block Chart



Incoming requests chart