CASE STUDY

ADVANCE DDOS PROTECTION FOR LEADING INSURANCE COMPANY

ABSTRACT

- A well known insurance company that provide varios insurance services in India was looking for robust WAF solution to protect their applications including Advance DDOS protection which can be customized as per their need.

KEY CHALLENGES

- Customer's Application was under DDOS attack which impacted the organization financially and damaged the brand reputation.
- As a first level of defense customer has applied the IP based rate limiting rules which helps them to get protection upto some extend against the attackers which were sending the requests more than the threshold value configured.

  However, there were few challenges observed-

  - Distinguishing between genuine and malicious traffic was a challenge. Some instances of false positive and false negative were getting observed.
  - They were not able to get comprehensive protection against bad traffic as attacker started changing the IP frequently and modulated the rate of the volumetric requests.
- The customer was looking for additional layer of defense that can address the above challenges and provide better protection against DDOS.

STRATEGY & RECOMMENDED SOLUTION

- We have reviewed the application work flow and suggested to implement a WAF DDOS policy with the combination of Average and Burst threshold. For eg:
  - Average threshold to be kept as 15 hits per second from a single ip in the period of 2 mins.
  - Burst threshold to be kept as 20 hits per second from a single ip in the period of 5 seconds.
  - **Rule logic:**
    - If the average threshold of 15 hits per second (during 2 mins period) is breached it will trigger advance monitoring mode, logs the traffic and immediate alert is triggered to customer's security team to review and take the action.
    - If the burst threshold of 20 hits per second (during 5 seconds period) is breached, it will immediately start blocking the request and the said IP address would be blocked for another 1 hour.
  - To further build the accuracy, we have tune up the rule to be consider GET|PUT|POST|HEAD HTTP request methods as a matching criteria.

RESULTS

- We have build the custom WAF policy and activated it in the production environment. After applying the custom policy customer's Application was stable and such bad traffic started getting absorbed at WAF level and we were successfully able to combat against such volumetric DDOS attacks.

INDUSFACE™