CASE STUDY

Saas Based Bot Management Solution

ABSTRACT

- It's one of the organization which provides an online visa appointment scheduling platform for its clients, wherein the users log in to their web portal to book an appointment once the booking window is opened.
- A specific booking window has defined available slots and the booking window details are published to users in advance.
- Some of the visa appointment scheduling gets opened quarterly bases and hence huge amount of web traffic hit to their Application server.

KEY CHALLENGES

- Here the organization faced an issue with Bot attacks. As soon as the booking window gets opened, attackers send huge volume of bot traffic on the appointment booking web page that genuine users were not able to open the web page and successfully book the appointments.
- The attacker used to crawl and input the dummy data to fill in all the available booking slots. Also, they were using automated tools, scripts to generate the bad bot traffics.
- The backend Application server were not able to handle the bad bot traffic considering the huge volume and used to became non-responsive intermittently during the open booking window time.
- Customer also tried to apply the rate limit controls at the Application server level but that was not giving the desirable results.
- This was impacting the organization as it as a brand, revenue and financial damage.
- Wanted something immediately to protect the online brand from such attacks.
- Needed a solution which can handle this volume and block all the bad bot traffic, DDOS traffic at the perimeter level before reaching the Application server.
- Needed a solution which is scalable and highly available all the time.

STRATEGY & RECOMMENDED SOLUTION

- We have reviewed the Application work flow in detail and have come up with a strategic solution to address the problem. Below WAF policies were recommended.
- **BOT PRETENDER POLICY RULES:** Blocks bad bots which are pretending to be legitimate bots. This ensures genuine bots are not blocked but prevent any bots impersonating legit bots like fake search engine (Google, Baidu, Yandex) bots from crawling, stealing sensitive information, exploiting vulnerabilities, etc.
- **SECURITY SCANNER/EXPLOITATION TOOLS/ WEB CRAWLER/SCRAPER DETECTION RULES:** Block connection or IP based on checks User-Agent, request header, filename/argument etc. This is to block attacks from known vulnerability scanners (like Nessus, Nikto, Acunetix, etc.), exploitation tools (), etc. Also prevent from tools, scripting/generic HTTP clients which crawl the websites to scrape sensitive information by the attacker to perform further attacks.
- **IP REPUTATION RULES:** Block bad reputed IP based on the source IP is Spammer, Suspicious, Search Engine, Harvester, etc. The reputation of the IP address is analysed using the Project Honey Pot system which identifies the reputation through efficient DNS lookups, mail servers against various black lists.

INDUSFACE™

CASE STUDY

Saas Based Bot Management Solution

CLI AND/OR GUI BASED AUTOMATION DETECTION RULES

COOKIE CHALLENGE BASED POLICY RULES: Block non-browser based suspicious traffic. Block IP/User when WAF injected cookies are missing or mismatch detected. For eg:

- Without Cookie - Block IP for 5mins - 10 attempts without a cookie
- Cookie Mismatch - Block the IP for 5mins - Cookie mismatch detected
  - IP as Identity: Block IP if more than two session (different cookies) established
  - Email ID as Identity: Block IP if more than 2 registration attempts from different Email Id.

HTML WEB FORM CHALLENGE BASED POLICY\RULES: Block browser/web-GUI based suspicious traffic. Block IP/User when WAF injected form field value manipulation (Web Parameter Tampering) detected. For eg:

- Block IP for 3 mins when WAF injected form field manipulation detected

CAPTCHA PROTECTION BASED POLICY RULES: Block malicious bot traffic. Google Re-Captcha introduced for the first page. By default, it does not allow when wrong input provided. For eg: block IP for 5 mins for 3 incorrect attempts.

ADVANCED DDOS RATE LIMITING POLICY RULES: Block suspicious traffic by throttling incoming requests. Block IP/Cookie based on User and Non-User threshold-based rate limiting rules. For eg:

- Non-User based (CLI, bots) - to block IP for 3 mins if 200 requests (threshold) exceeds in 2 mins.
- User based (Cookie, browser, human bots) - to block Cookie for 3 mins if 25 requests (threshold) exceeds in 1 min

BRUTE-FORCE RATE LIMITING POLICY RULES: Block suspicious traffic using brute-force technique. Block IP/User based on Incorrect Login/Captcha attempts.

- Block IP/Identity for 3 mins for wrong Captcha - 3 attempts in a minute.
- Block IP/Identity for 3 mins for wrong login

INPUT VALIDATION POLICY RULES: Block suspicious user traffic. Block Connection based on Incorrect Login/Captcha attempts.

- Block Connection when invalid Email ID detected (wrong format).
- Block Connection when invalid password detected (based on password length)
- Block Connection if invalid captcha found (based on chars & length).

BLACKLISTING/WHITELISTING POLICY RULES: Block or control suspicious traffic based on real time monitoring. Block or Allow requests from IP/Geo-location/URI/Client based on configuration.

- Geo-location Blacklisting policy rules – to block or allow requests from a specific geo-location.

ANOMALY/ABNORMAL BEHAVIOR DETECTION RULES: Block IP based on abnormal behaviour in real time. Self-learning intelligence rules are written based on continuous monitoring of threat detection that incorporates threat intelligence to help protect from malicious attacks/suspicious activities. These rules are built based on the accumulated dataset, threat score to check unusual application traffic patterns grouped around common parameter over time period to identify anomalies.

RESULTS

The above WAF policies were built, simulated by our Security experts and were activated in the production. Below observations were concluded during actively running appointment booking window.

- All the bad bot traffic was successfully getting absorbed at the WAF. WAF was forwarding genuine user traffic to the Application server.
- Users were able to book the visa appointments seamlessly.
- Application servers were observed healthy considering the traffic handling got drastically reduce and were serving the web content faster for better user experience.

INDUSFACE™