Bright Network Engineering Project

Jesse Luo

July 17, 2025

1 Findings

Upon analysis of the IP addresses of all requests from the logs, it was found that 36000 requests (8.33% of all requests over all logs) were sent from 4 distinct groups of IP addresses:

IP address group	Countries	Number of Requests
194.168.1.−	UK	14400
45.133.1.−	Russia	10800
185.220.10 − .−	Iran, DPRK, China, Russia	7200
35.185.0.156	US	3600

1.1 Group 1

4 requests per second were made from 12pm to 1pm on July 3rd. These were all GET requests for various content on the site. This could be considered as spamming.

1.2 Group 2

3 requests per second were made from 3pm to 4pm on July 2nd. These requests were of various types and mainly interacted with the API of the site, include DELETE methods which may have deleted particular resources on the site. This is most likely a form of malicious scanning / reconnaissance by a bad actor.

1.3 Group 3

Requests were made every second across 5 different IP addresses from 7pm to 9pm on July 4th. All were POST requests which attempted to brute force different combinations of usernames and passwords for the login page for different users, including the administrator.

It was found that there were not GET requests associated with the same IP addresses, which suggests that the brute force attack was not successful.

1.4 Group 4

2 requests per second were made from 5am to 5:30am on July 2nd. No requests from other IP addresses were recorded during this period. All requests were GET requests for various content on the site. This could also be considered as spamming, and it should be investigated whether the lack of other traffic was due to genuine low traffic or the website struggling with high volume.

2 Recommendations

- IP bans should be enacted immediately for IP addresses in group 2 and 3, and further investigation should be performed for these malicious actors.
- Implement rate limiting and temporary IP bans for IP addresses in group 1 and 4, and automatically for any future IP addresses that perform spamming.