TRAFFIC MITIGATION AND CYBER ATTACK RESPONSE ANALYSIS FOR OSSBSCIC.GOV.BD

Effective Defense Against DDoS and Malicious Traffic Surges

Abstract

This report analyzes recent cyber-attacks on the ossbscic.gov.bd website, where abnormal traffic spikes indicated potential DDoS attempts. GTM's Web Application Firewall (WAF) successfully mitigated over 81,000 suspicious requests, allowing 84,750 legitimate requests to be served by the origin server. Despite the surge, the mitigation measures ensured minimal disruption to users. The findings highlight the effectiveness of proactive security tools in defending against high-volume attacks and maintaining website stability.

CIRT AND INFRA TEAM, BUSINESS AUTOMATION LTD.

Version: 1.1

Analysis Conducted by: **Bhabatush Debnath Apu** and **Khandakar Rabbi Ahmed Sanjid**

Incident Timeline & Mitigation Actions:

- **April 9, 2025:**
  - **10:30 AM - 11:45 AM:** The **ossbscic.gov.bd** website faced a surge in requests, leading to temporary unavailability.
  - The **CIRT and INFRA team** immediately implemented **Global Traffic Management (GTM)** and **Nginx-level** mitigations to filter malicious traffic.
  - Traffic was primarily targeting the **/web/ongoing-online-service/** path, with requests originating from **Alibaba-CN-NET IP addresses** located in **Singapore**.

- **April 8, 2025 (Yesterday):**
  - The **osspid.org** website continued to experience a high volume of suspicious hits, which were mitigated using similar strategies. Both sites were **brought back online** and are under continuous observation to ensure security. We have identified this as a cyber-attack, which resulted in a disruption to the https://ossbscic.gov.bd login functionality.

Current Status:

*Both websites are now **operational and safe**, with monitoring ongoing to prevent further disruptions.*

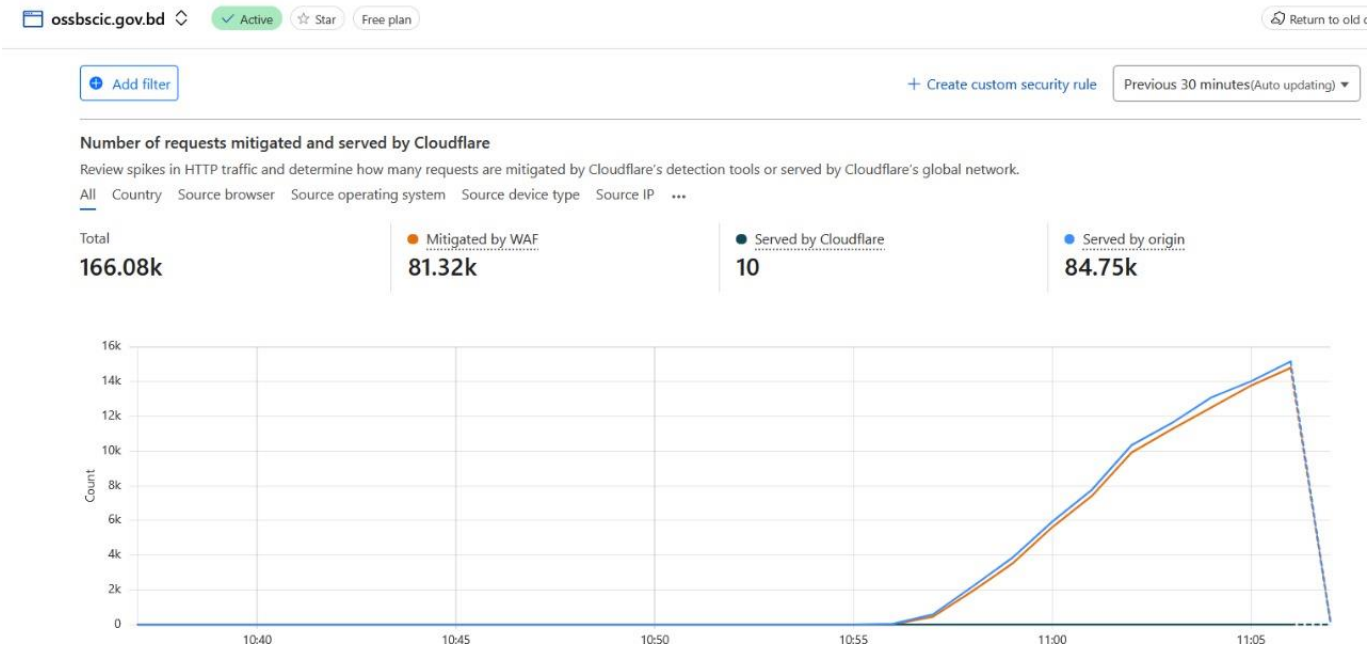

Figure 1: Traffic Data

Traffic Analysis Summary:

- **Total Requests:** 166.08k
- **Requests Mitigated by WAF:** 81.32k (49% blocked by Global Traffic Management Web Application Firewall)
- **Requests Served by GTM:** 10 (Indicates most traffic was filtered by GTM)
- **Requests Served by Origin:** 84.75k (Legitimate traffic processed by the origin server)

Key Insights:

- **Traffic Spike:** A sharp increase in requests was observed around **10:55 AM**, likely indicating a DDoS or traffic anomaly.
- **Mitigation Success:** Global Traffic Management WAF blocked a large portion of malicious requests (**81.32k**), while legitimate requests (**84.75k**) were served by the origin server.

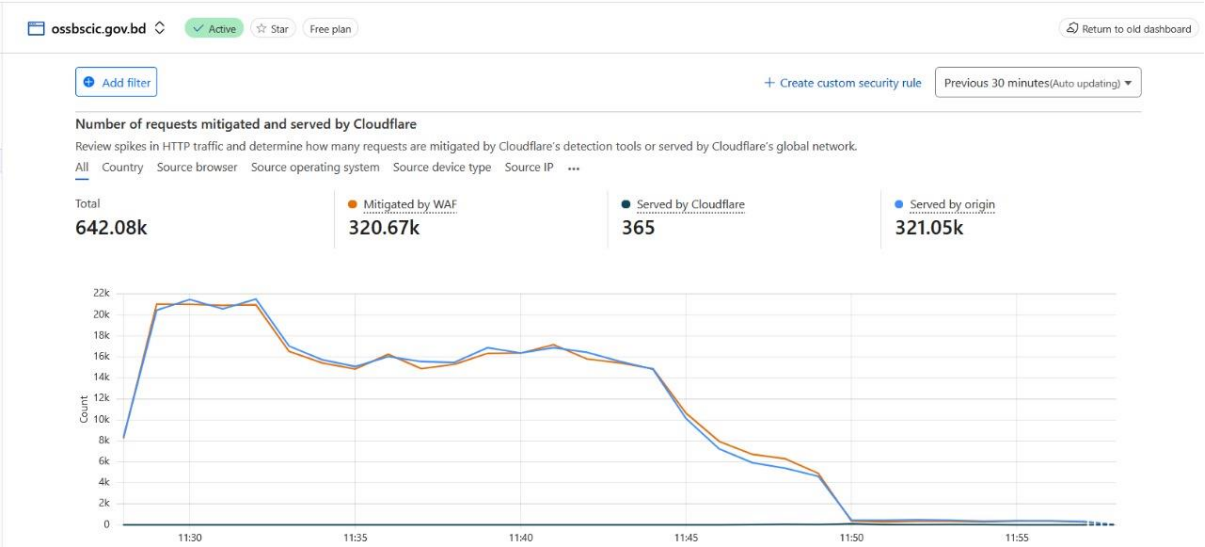

Figure 2: Traffic Flow and Mitigation Efforts

Traffic Mitigation Summary for ossbscic.gov.bd

- **Total Requests:** 642.08k
  A significant surge in traffic, likely due to a **DDoS attack**, was observed starting at **11:30 AM**.
- **Requests Mitigated by WAF:** 320.67k
  Global Traffic Management Web **Application Firewall (WAF)** successfully blocked over **50%** of incoming requests, preventing harmful traffic from reaching the server.
- **Requests Served by GTM:** 365
  Only a minimal number of requests (**365**) were processed and served by GTM after filtering out malicious traffic.
- **Requests Served by Origin:** 321.05k
  The **origin server** handled the legitimate requests, confirming the effectiveness of the mitigation measures in safeguarding the site.

Key Insights:

- **Traffic Surge (11:30 AM - 11:35 AM):** A sharp spike, likely caused by the attack, was immediately detected and mitigated.
- **Effective Mitigation:** The WAF and filtering measures significantly reduced the malicious traffic, ensuring smooth operation with **321.05k legitimate requests** processed.
- **Minimal Impact:** The gap between requests served by GTM and the origin shows successful filtering, minimizing disruption.

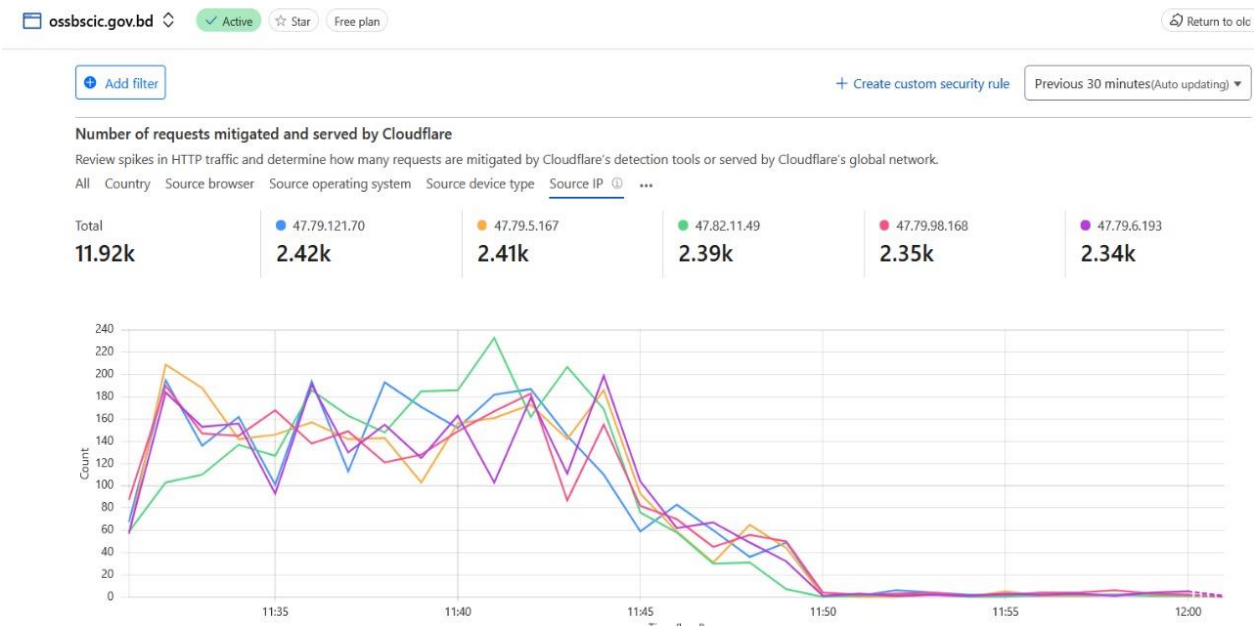

Figure 3: Traffic Data with Source

Traffic Mitigation Summary for ossbscic.gov.bd

- **Total Requests:** 11.92k
  Represents the overall traffic observed between **11:30 AM - 12:00 PM**, including both legitimate and suspicious traffic.
- **Requests Mitigated by GTM:** 2.42k - 2.34k
  Global Traffic Management mitigation tools blocked **suspicious traffic** originating from several source IP addresses, ensuring they did not reach the origin server.

  IP Breakdown:

  * **47.79.121.70:** 2.42k requests
  * **47.79.5.167:** 2.41k requests
  * **47.82.11.49:** 2.39k requests
  * **47.79.98.168:** 2.35k requests
  * **47.79.6.193:** 2.34k requests

Traffic Surge & Mitigation:

- **Spikes:** Multiple spikes in traffic observed, indicating potential malicious attempts from specific IPs.
- **Reduction:** After these peaks, the traffic reduced significantly, confirming that GTM effectively blocked the malicious requests.

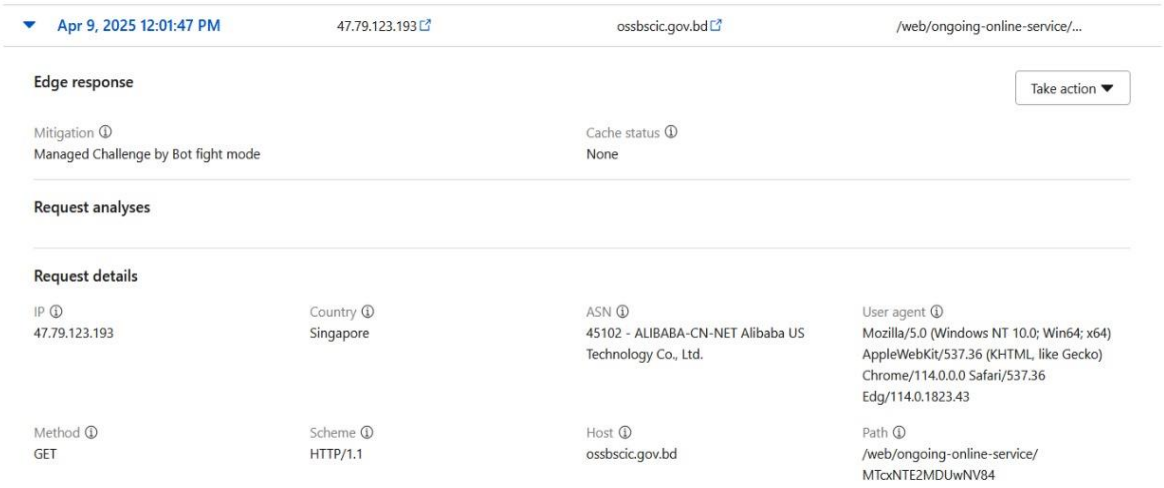

Figure 4: Source Path and Location

Request Analysis Summary:

- **Timestamp:** April 9, 2025, at 12:01:47 PM
- **IP Address: 47.79.123.193** (Located in Singapore, associated with Alibaba-CN-NET)
- **Request Path: /web/ongoing-online-service/** (Targeted endpoint during the attack)
- **Method: GET** (Standard HTTP method for retrieving data)
- **User Agent:** Chrome on **Windows 10** (Spoofed or automated traffic)
- **Bot Mitigation:** GTM **Managed Challenge in Bot Fight Mode** detected and blocked the request as suspicious.
- **Cache Status: None** (Request was not cached, processed dynamically)
- **ASN: 45102** (Linked to Alibaba US Technology Co., Ltd.)

Key Insights:

- The request was identified as potentially automated and mitigated by Global Traffic Management Bot **Fight Mode**.
- Originating from **Alibaba-CN-NET**, the IP is likely involved in bot-related activities.
- The targeted path aligns with previous attack patterns, confirming ongoing malicious attempts.