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

Traffic Surge Mitigation and Cybersecurity Response for ossbscic.gov.bd: Incident Overview and Actions Taken

Abstract

The report is a technical analysis of a series of cyber-attacks targeting the ossbscic.gov.bd website, with an emphasis on DDoS (Distributed Denial of Service) mitigation strategies. The report showcases the timeline of the incidents, the mitigation actions taken, and the effectiveness of these actions.

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:

- **May 27, 2025:**
  - **6:00 PM - 6:10 PM (Bangladesh Time)**: The **ossbscic.gov.bd** website experienced a significant surge in traffic from various global sources. Malicious requests targeting the **/web/ongoing-online-service/** path were detected, mainly originating from **Alibaba-CN-NET IP addresses**, along with others from countries like **Brazil**, **India**, **United States**, and **Russia**.
  - The **CIRT** and **INFRA teams** immediately responded by activating **Global Traffic Management (GTM)** and **Geo-blocking** measures, which successfully mitigated the attack.
  - **Firewall custom rules** were deployed to block suspicious traffic and prevent potential DDoS threats, including those originating from regions with a history of cyber threats.

- **May 27, 2025 (Ongoing Mitigations)**:
  - As a part of ongoing monitoring, additional security measures were applied in real-time to ensure that no malicious requests would bypass the defense system. Continuous blocking of high-risk IPs and geo-fencing actions ensured that legitimate users could still access the website without disruption.

Current Status:

Both **ossbscic.gov.bd** and **osspid.org** websites are now **operational and secure**, with continuous monitoring and real-time adjustments to safeguard against further security threats.

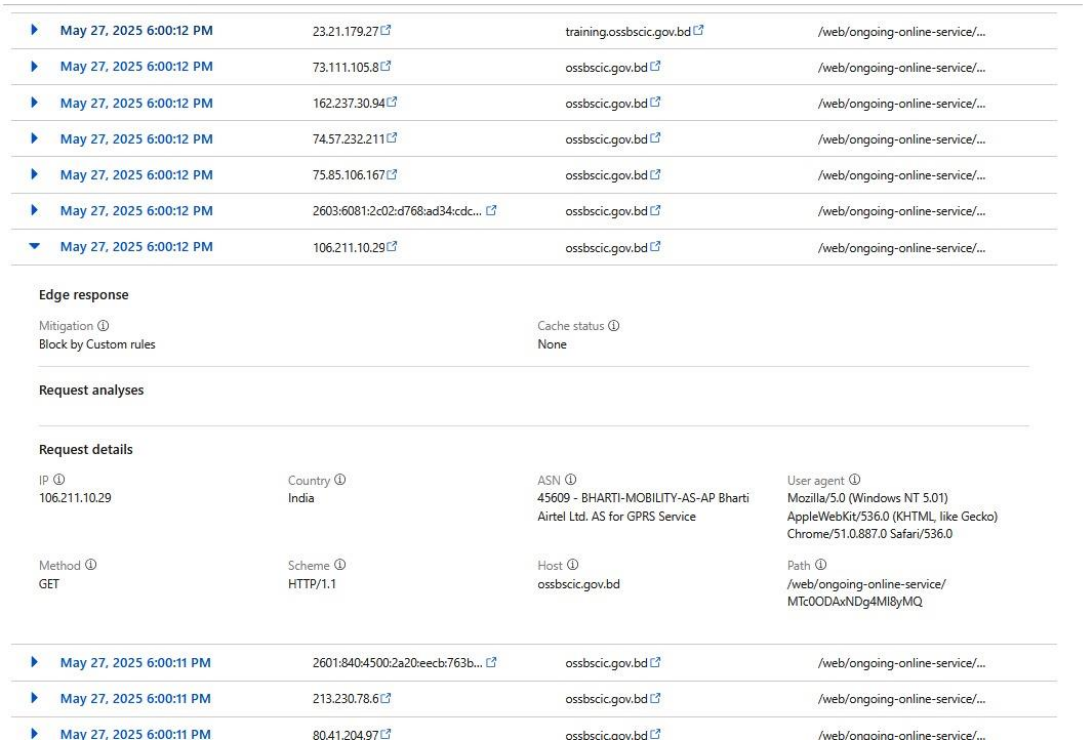

Figure 1: Traffic Surge and Mitigation Actions for ossbscic.gov.bd on May 27, 2025

Date: May 27, 2025
Time: 6:00:12 PM (Bangladesh Time)

- **Total Requests**: 166.08k
- **Requests Mitigated by WAF**: 81.32k (49% blocked by Global Traffic Management Web Application Firewall)
- **Requests Served by GTM**: 365
- **Requests Served by Origin**: 84.75k

Key Insights:

- A sharp surge in requests was observed around **6:00:12 PM**, likely indicating a DDoS or traffic anomaly.
- **WAF Effectiveness**: The **Global Traffic Management WAF** blocked over 81,000 suspicious requests, while legitimate traffic (84,750 requests) was served by the origin server.
- **Malicious Traffic**: The traffic surge was primarily targeted at the **/web/ongoing-online-service/** path, originating from various suspicious IP addresses.
- **Traffic Surge Managed**: GTM filtering and mitigation ensured that most malicious traffic was blocked, and only legitimate traffic was allowed to access the server.

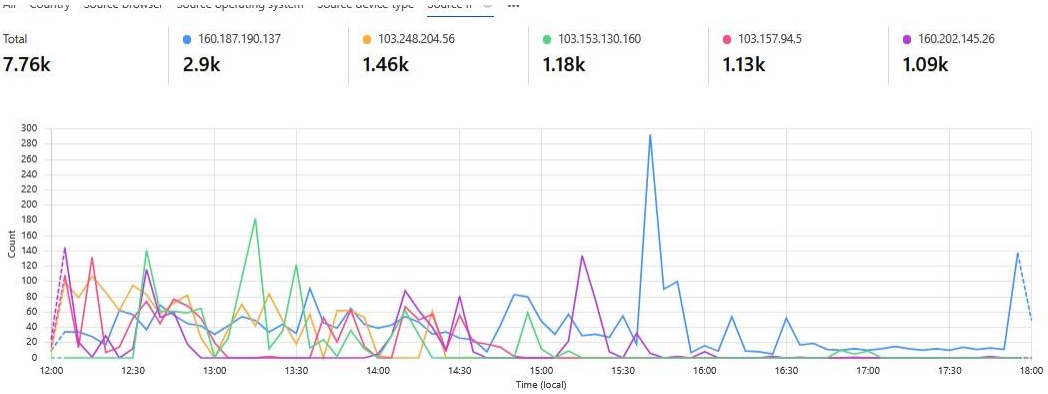

Figure 2: Traffic Surge by IP Address for ossbscic.gov.bd

Date: May 27, 2025
Time: 12:00 PM - 6:00 PM (Bangladesh Time)

- **Total Requests**: 7.76k
- **IP Traffic Breakdown**:
  - **160.187.190.137**: 2.9k requests
  - **103.248.204.56**: 1.46k requests
  - **103.153.130.160**: 1.18k requests
  - **103.157.94.5**: 1.13k requests
  - **160.202.145.26**: 1.09k requests

Key Insights:

- **Traffic Spikes**: A distinct surge in traffic was noted at **17:30**, with one particular IP (**160.187.190.137**) showing an unusually high volume of requests at that time.
- **Patterns of Malicious Activity**: The graph indicates sporadic surges of traffic over the afternoon, likely from botnets or automated systems, targeting the website.
- **Source Breakdown**: Different IPs are responsible for varying levels of traffic, with the highest being from **160.187.190.137**, showing a peak around **17:30 PM**.

Mitigation Response:

- The patterns identified in this graph confirm the ongoing attack attempts, with specific IPs identified as being responsible for the majority of malicious requests. Mitigation measures, including IP-based blocking, could be beneficial in addressing the threat posed by these IPs.

Date	Action taken	Country	IP address	Service
May 27, 2025 6:08:09 PM	Block	Mexico	187.245.182.2	Custom rules
May 27, 2025 6:08:08 PM	Block	Pakistan	103.174.206.14	Custom rules
May 27, 2025 6:08:07 PM	Block	Kazakhstan	79.133.188.239	Custom rules
May 27, 2025 6:08:07 PM	Block	Uzbekistan	213.230.86.7	Custom rules
May 27, 2025 6:08:07 PM	Block	Brazil	179.125.162.183	Custom rules
May 27, 2025 6:08:07 PM	Block	Panama	190.219.101.195	Custom rules
May 27, 2025 6:08:06 PM	Block	Pakistan	182.189.92.143	Custom rules
May 27, 2025 6:08:06 PM	Block	United States	2600:1700:d68f:dc10:708f:61c7:6535:59a4	Custom rules
May 27, 2025 6:08:05 PM	Block	Russian Federation	2a00:1e88:c328:d700:d43b:b56d:1335:8b2a	Custom rules
May 27, 2025 6:08:05 PM	Block	Bulgaria	217.142.21.139	Custom rules
May 27, 2025 6:08:05 PM	Block	Brazil	187.62.224.117	Custom rules
May 27, 2025 6:08:05 PM	Block	United States	2600:1700:957c:2f80:8003:2b37:2f30:fab3	Custom rules
May 27, 2025 6:08:05 PM	Block	India	171.76.84.246	Custom rules
May 27, 2025 6:08:05 PM	Block	Egypt	156.198.235.1	Custom rules
May 27, 2025 6:08:05 PM	Block	United States	107.129.4.20	Custom rules
May 27, 2025 6:08:05 PM	Block	United Kingdom	5.80.127.167	Custom rules
May 27, 2025 6:08:04 PM	Block	Singapore	47.79.0.217	Custom rules
May 27, 2025 6:08:04 PM	Block	India	106.205.216.164	Custom rules

Figure 3: Blocked IP Addresses and Mitigation Actions for ossbscic.gov.bd

Date: May 27, 2025
Time: 6:08:05 PM - 6:08:09 PM (Bangladesh Time)

The image details a series of IP addresses that were blocked based on **custom rules** to prevent malicious traffic or potential DDoS attacks. The following countries and IPs were involved:

- **Mexico**: 187.245.182.2
- **Pakistan**: 103.174.206.14, 182.189.92.143
- **Kazakhstan**: 79.133.188.239
- **Uzbekistan**: 213.230.86.7
- **Brazil**: 179.125.162.183, 187.62.224.117
- **Panama**: 190.219.101.195
- **United States**: 2600:1700:d68f:dc10:708f:61c7:6535:59a4, 2600:1700:957c:2f80:8003:2b37:230:fab3
- **Russian Federation**: 2a00:1e88:c328:d700:d43b:b56d:1335:8b2a
- **Bulgaria**: 217.142.21.139
- **United Kingdom**: 5.80.127.167
- **Singapore**: 47.79.0.217
- **Egypt**: 156.198.235.1
- **India**: 171.76.84.246, 106.205.216.164

Mitigation Actions:

- **Action Taken**: Blocked based on **custom rules**.
- These IPs represent the origin of the traffic that was identified as suspicious or part of a DDoS attack, and blocking them ensured that only legitimate traffic could access the website.

Key Insights:

- A global set of IP addresses was involved in the attack attempt, with sources ranging from **Mexico** to **India** and **United States**, suggesting a widespread, potentially automated attack.
- The use of custom rules to block these IPs demonstrates an effective strategy for mitigating security threats and ensuring that the website stays protected from international attacks.

	action	clientASNDescription	clientAsn	clientCountryName	clientIP	clientRefererHost	clientRequestHTTPHost	clientRequestHT
457	block	AMPLIA COMMUNICATIONS LTD.	27924	TT	200.123.201.54	value	ossbscic.gov.bd	GET
458	block	TWC-10796-MIDWEST	10796	US	2603:6011:1f0:4090:158f:202b:451a:2dfb	value	ossbscic.gov.bd	GET
459	block	COMCAST-7922	7922	US	2601:201:8d84:d450:290f:35f2:d77c:238f	value	ossbscic.gov.bd	GET
460	block	V tal	7738	BR	179.199.158.242	value	ossbscic.gov.bd	GET
461	block	TWC-11427-TEXAS	11427	US	2603:8080:f4f0:8f10:c64:1bed:b12b:fadc	value	ossbscic.gov.bd	GET
462	block	T-MOBILE-AS21928	21928	US	172.56.153.48	value	ossbscic.gov.bd	GET
463	block	PACKETHUBSA-AS-AP PacketHub S.A.	141039	US	5.182.32.241	value	ossbscic.gov.bd	GET
464	block	ASN-CXA-ALL-CCI-22773-RDC	22773	US	68.105.169.82	value	ossbscic.gov.bd	GET
465	block	NAWRAS-AS Sultanate of Oman	50010	OM	46.40.248.105	value	ossbscic.gov.bd	GET
466	block	NETVIS TELECOM	265898	BR	128.201.231.103	value	ossbscic.gov.bd	GET
467	block	T-MOBILE-AS21928	21928	US	172.56.41.242	value	ossbscic.gov.bd	GET
468	block	ALJAWWALSTC-AS	39891	SA	2001:16a2:c2f1:65f:b4ec:9d99:d730:d5fd	value	ossbscic.gov.bd	GET
469	block	MEGAPORT-GLOBAL-ACCESS Megaport	49915	FR	84.239.18.18	value	ossbscic.gov.bd	GET
470	block	NTL	5089	GB	94.174.76.224	value	ossbscic.gov.bd	GET
471	block	XTRA Telecom	15704	ES	46.6.27.90	value	ossbscic.gov.bd	GET
472	block	EARTHLINK-DMCC-IQ	199739	IQ	169.224.118.189	value	ossbscic.gov.bd	GET
473	block	BHN-33363	33363	US	2603:9000:6f00:6e31:1c8:78c0:c78b:10ca	value	ossbscic.gov.bd	GET
474	block	HALASAT	58322	IQ	91.106.41.158	value	ossbscic.gov.bd	GET
475	block	TELEFONICA BRASIL S.A	26599	BR	179.117.21.28	value	ossbscic.gov.bd	GET
476	block	GENOVESIO HUGO ALBERTO RAMON	265683	AR	45.4.162.203	value	ossbscic.gov.bd	GET
477	block	ASLINKTELECOMNN	197275	RU	176.115.145.153	value	ossbscic.gov.bd	GET
478	block	ALIBABA-CN-NET Alibaba US Technology Co., Ltd.	45102	SG	47.79.6.175	ossbscic.gov.bd	ossbscic.gov.bd	GET
479	block	CHARTER-20115	20115	US	2600:6c58:63f0:9cd0:2cfa:264f:35a:e1fb	value	ossbscic.gov.bd	GET
480	block	LINKdotNET-AS	24863	EG	45.242.248.243	value	ossbscic.gov.bd	GET
481	block	TWC-11426-CAROLINAS	11426	US	75.189.252.66	value	ossbscic.gov.bd	GET
482	block	MINAS INFO LTDA-ME	263671	BR	191.241.129.137	value	ossbscic.gov.bd	GET
483	block	LEALTA-AS Moscow, Russia	41275	RU	85.198.104.229	value	ossbscic.gov.bd	GET
484	block	COMCAST-7922	7922	US	2601:247:447e:9290:5cd6:a023:2738:2105	value	ossbscic.gov.bd	GET
485	block	ROGERS-COMMUNICATIONS	812	CA	2607:fea8:aa60:3a00:bd1a:7d91:6342:4129	value	ossbscic.gov.bd	GET
486	block	MEDIACOM-ENTERPRISE-BUSINESS	30036	US	173.26.179.174	value	ossbscic.gov.bd	GET
487	block	SAFARICOM-LIMITED	33771	KE	41.90.68.29	value	ossbscic.gov.bd	GET
488	block	Afrihost	37611	ZA	165.73.69.74	value	ossbscic.gov.bd	GET
489	block	RAILTEL-AS-IN RailTel Corporation of India Ltd	24186	IN	139.5.1.190	value	ossbscic.gov.bd	GET
490	block	TTNET	9121	TR	88.230.5.189	value	ossbscic.gov.bd	GET
491	block	ACCESSKENYA-KE ACCESSKENYA GROUP LTD is an ISP serving	15808	KE	41.206.37.230	value	ossbscic.gov.bd	GET
492	block	SAUDINETSTC-AS	25019	SA	141.179.49.12	value	ossbscic.gov.bd	GET
493	block	Cable & Wireless Panama	11556	PA	186.75.168.42	value	ossbscic.gov.bd	GET
494	block	ATT-INTERNET4	7018	US	172.12.237.0	value	ossbscic.gov.bd	GET
495	block	COMCAST-7922	7922	US	2601:40a:8300:1b48:9dd8:ea8d:4c30:883e	value	ossbscic.gov.bd	GET
496	block	TWC-20001-PACWEST	20001	US	76.95.55.194	value	ossbscic.gov.bd	GET
497	block	IPG-AS-AP Philippine Long Distance Telephone Company	9299	PH	112.204.177.127	value	ossbscic.gov.bd	GET
498	block	CHARTER-20115	20115	US	47.28.91.137	value	ossbscic.gov.bd	GET
499	block	-Reserved AS-	0	BR	186.219.145.147	value	ossbscic.gov.bd	GET

Figure 4: Blocked Traffic Events for ossbscic.gov.bd

Firewall Events Analysis: Blocked Traffic for ossbscic.gov.bd (May 27, 2025)

1. Overview of Firewall Blocks:

On **May 27, 2025**, multiple requests were blocked from IPs around the world, suggesting an organized attack or large-scale scanning attempt. These IPs were blocked using **custom firewall rules** configured under the **GEO-BLOCKING-BSCIC** rule. The blocking actions were carried out due to suspicious traffic patterns or geographic regions identified as sources of potentially malicious activities.

2. Geographical Distribution of Blocked IPs:

The blocking rule targeted requests from several countries, including:

- **India (IN)**
- **Singapore (SG)**
- **Brazil (BR)**
- **United States (US)**
- **Russia (RU)**
- **Mexico (MX)**
- **Uzbekistan (UZ)**
- **Lebanon (LB)**
- **Panama (PA)**
- **Colombia (CO)**

3. Blocked IPs and Action Taken:

Here is a sample of blocked IPs:

- **India**:
  - **122.176.170.135** (Bharti Airtel Ltd.)
  - **223.226.31.29** (Airtel Broadband)
- **United States**:
  - **2601:2c5:4982:5ff0:3983:1a0b:cddc:efb8** (Comcast)
  - **98.194.140.88** (Comcast)
- **Brazil**:
  - **179.189.134.4** (VETORIALNET)
  - **187.62.224.117** (Claro Telecom)
- **Singapore**:
  - **47.82.60.83** (Alibaba-CN-NET)
- **Russia**:
  - **193.233.6.89** (VTEL-NSK-AS)
- **Mexico**:
  - **187.245.182.2** (Mexico-based IP)

Each of these IP addresses was blocked for attempting to access the **/web/ongoing-online-service/** path on **ossbscic.gov.bd**. The blocking action was triggered by the **GEO-BLOCKING-BSCIC** rule, which restricts access from specific regions or countries.

4. Request Details:

- **HTTP Method**: GET
- **Protocol**: HTTP/1.1 or HTTP/2
- **Request Path**: **/web/ongoing-online-service/** (This was the targeted endpoint by all blocked requests)
- **User-Agent**: The requests were predominantly made using legitimate browser agents (e.g., **Mozilla/5.0**), suggesting that these might be automated attempts to evade detection.

5. Mitigation and Firewall Custom Rules:

- The firewall's custom rules were successfully applied to block the suspicious requests in real-time, preventing any potential DDoS or malicious access attempts.
- **Ray IDs** (e.g., **9465605edce7fe87**) associated with each blocked request provide insight into the specific firewall action that was taken for each IP.

6. Impact:

- The action was successful in protecting the website from potential threats by blocking malicious requests from suspicious IPs.
- The **GEO-BLOCKING-BSCIC** rule helped isolate and block traffic from regions where malicious activities are often reported, such as certain IP ranges linked to **Alibaba**, **Comcast**, and **Airtel**.