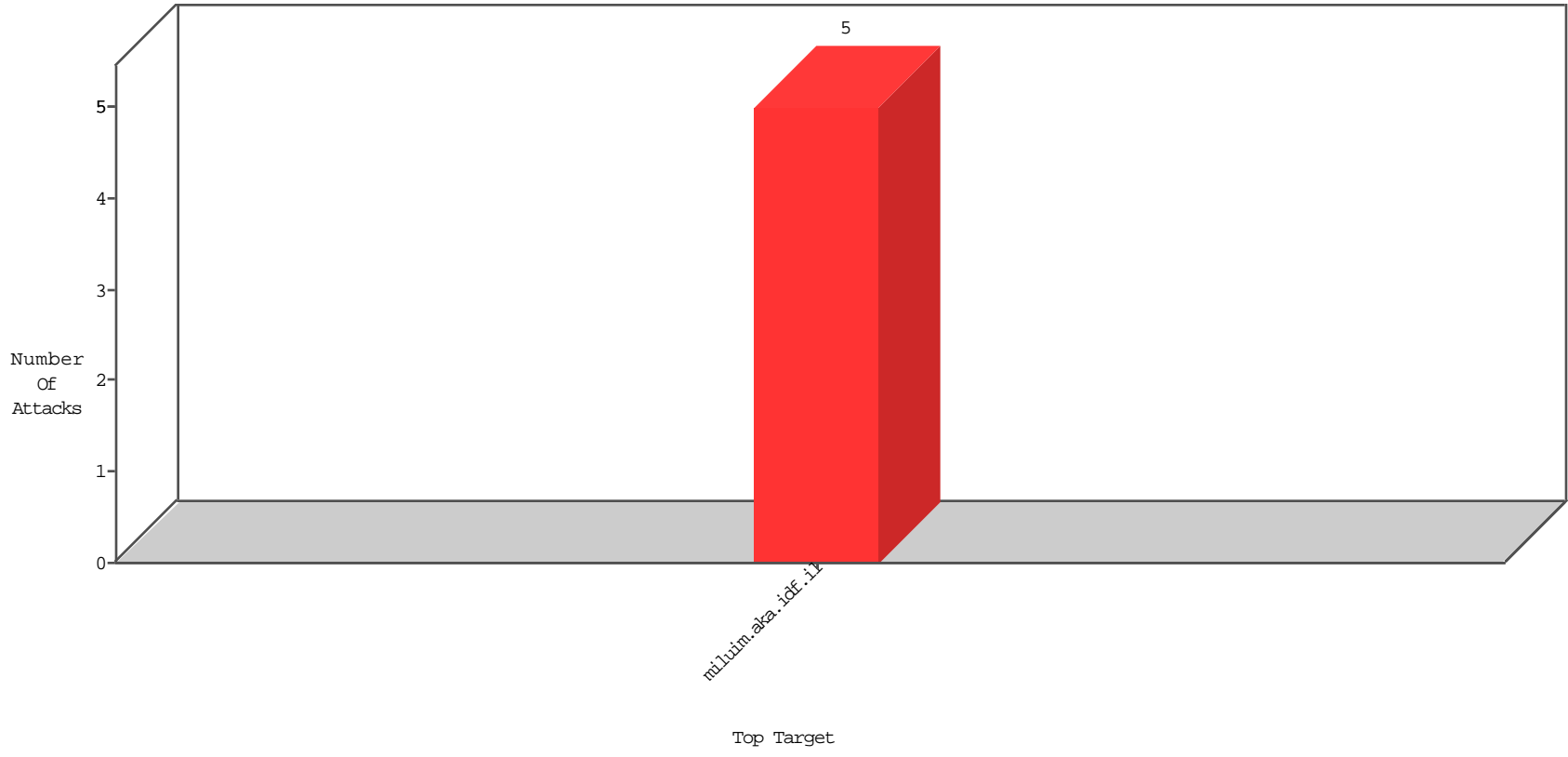


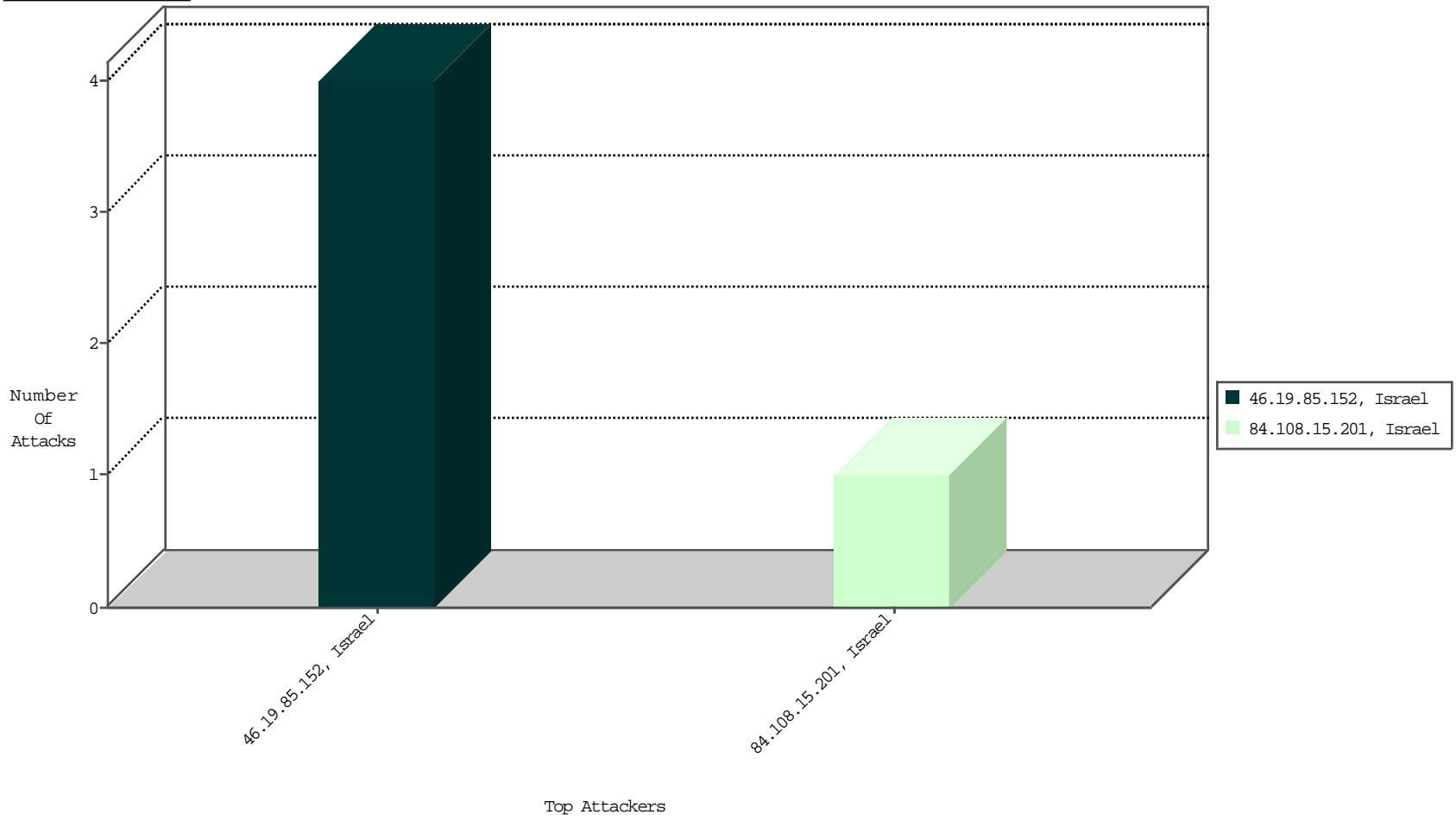
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

| Attacker Address | Attacker Geo | Target Address | Site              | Signature          | Device Action | DP_location.Location | Count |
|------------------|--------------|----------------|-------------------|--------------------|---------------|----------------------|-------|
| 84.108.15.201    | Israel       | 147.237.0.120  | miluim.aka.idf.il | Block_Udp_All_Nets | drop          | BEL-Israel           | 1     |

Top Attackers In IPS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|------------------|--------------|----------------|------|-----------|---------------|-------|
|------------------|--------------|----------------|------|-----------|---------------|-------|

Top Attackers In IDS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Count |
|------------------|--------------|----------------|------|-----------|-------|
|------------------|--------------|----------------|------|-----------|-------|

## Top Attackers In FW

| Attacker Address | Attacker Geo | Target Address | Site             | Name   | Signature   | Device Action | Count |
|------------------|--------------|----------------|------------------|--|---|---------------|-------|
| 84.95.252.68     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped.                         | drop          | 2304  |
| 2.55.14.117      | Israel       | 147.237.0.120  | miluim.aka.idf.i | SYN Attack                                   | SYN -> SYN-ACK -> RST   | reject        | 170   |
| 87.70.61.63      | Israel       | 147.237.0.120  | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped.                         | drop          | 144   |
| 62.219.198.6     | Israel       | 147.237.0.120  | miluim.aka.idf.i | SYN Attack                                   | SYN -> SYN-ACK -> RST   | reject        | 100   |
| 46.19.85.183     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 36    |
| 46.19.85.183     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | alert         | 36    |
| 2.55.27.9        | Israel       | 147.237.0.120  | miluim.aka.idf.i | SYN Attack                                   | SYN -> SYN-ACK -> RST   | reject        | 36    |
| 109.65.181.183   | Israel       | 147.237.0.120  | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped.                         | drop          | 27    |
| 37.26.146.170    | Israel       | 147.237.0.120  | miluim.aka.idf.i | SYN Attack                                   | SYN -> SYN-ACK -> RST   | reject        | 16    |
| 2.55.142.203     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | alert         | 4     |
| 46.19.85.218     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | alert         | 4     |
| 2.55.142.203     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 4     |
| 132.73.207.78    | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | SYN+ACK retransmit with different window scale                          | monitor       | 4     |
| 46.19.85.218     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 4     |
| 212.179.21.194   | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | SYN+ACK retransmit with different window scale                          | monitor       | 4     |
| 5.22.134.225     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 2     |
| 87.71.16.89      | Israel       | 147.237.0.120  | miluim.aka.idf.i | SYN Attack                                   | SYN -> SYN-ACK -> RST   | reject        | 2     |
| 213.57.55.205    | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | alert         | 1     |
| 85.64.136.61     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | alert         | 1     |
| 46.19.85.89      | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 1     |
| 23.101.61.176    | Ireland      | 147.237.0.120  | miluim.aka.idf.i | Instant Messengers                           | instant messenger pattern found, application: Skype                     | monitor       | 1     |
| 2.53.11.105      | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 1     |
| 213.57.55.205    | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 1     |
| 85.64.136.61     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 1     |
| 37.142.244.251   | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | alert         | 1     |
| 81.218.206.82    | Israel       | 147.237.0.120  | miluim.aka.idf.i | SYN Attack                                   | SYN -> SYN-ACK -> Timeout   | reject        | 1     |
| 46.19.85.152     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Block HTTP Non Compliant                     | illegal header format detected: Malformed HTTP protocol name in request | monitor       | 1     |
| 37.26.146.170    | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | alert         | 1     |
| 37.142.244.251   | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 1     |
| 2.55.142.203     | Israel       | 147.237.0.120  | miluim.aka.idf.i | SYN Attack                                   | SYN -> SYN-ACK -> RST   | reject        | 1     |
| 37.26.146.170    | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | monitor       | 1     |
| 46.116.31.111    | Israel       | 147.237.0.120  | miluim.aka.idf.i | SYN Attack                                   | SYN -> SYN-ACK -> RST   | reject        | 1     |
| 46.19.85.89      | Israel       | 147.237.0.120  | miluim.aka.idf.i | Bad TCP sequence                             | Invalid ACK number  | alert         | 1     |

05-04-2016-13:08:09 to 05-04-2016-14:08:09

Top Attackers In WAF

| Attacker Address | Attacker Geo | Target Address | Site             | Signature  | Device Action | Count |
|------------------|--------------|----------------|------------------|--|---------------|-------|
| 46.19.85.152     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Abnormally Long Request request version  | Block         | 1     |
| 46.19.85.152     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Illegal HTTP Version __atuvc=1%7C18; __atuvs=5729d17c3077ede0000; _pk_id.104.b624=963f5db6b63fe6ac.1462358217.1.1462358399.1462358217.; _pk_ses.104.b624=* | Block         | 1     |
| 46.19.85.152     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Malformed URL idf_cellular_redirect=tosite;  | Block         | 1     |
| 46.19.85.152     | Israel       | 147.237.0.120  | miluim.aka.idf.i | Unknown HTTP Request Method =ani4h3zehjtrlfavjolqdy2; in URL idf_cellular_redirect=tosite  | Block         | 1     |

05-04-2016-13:08:09 to 05-04-2016-14:08:09