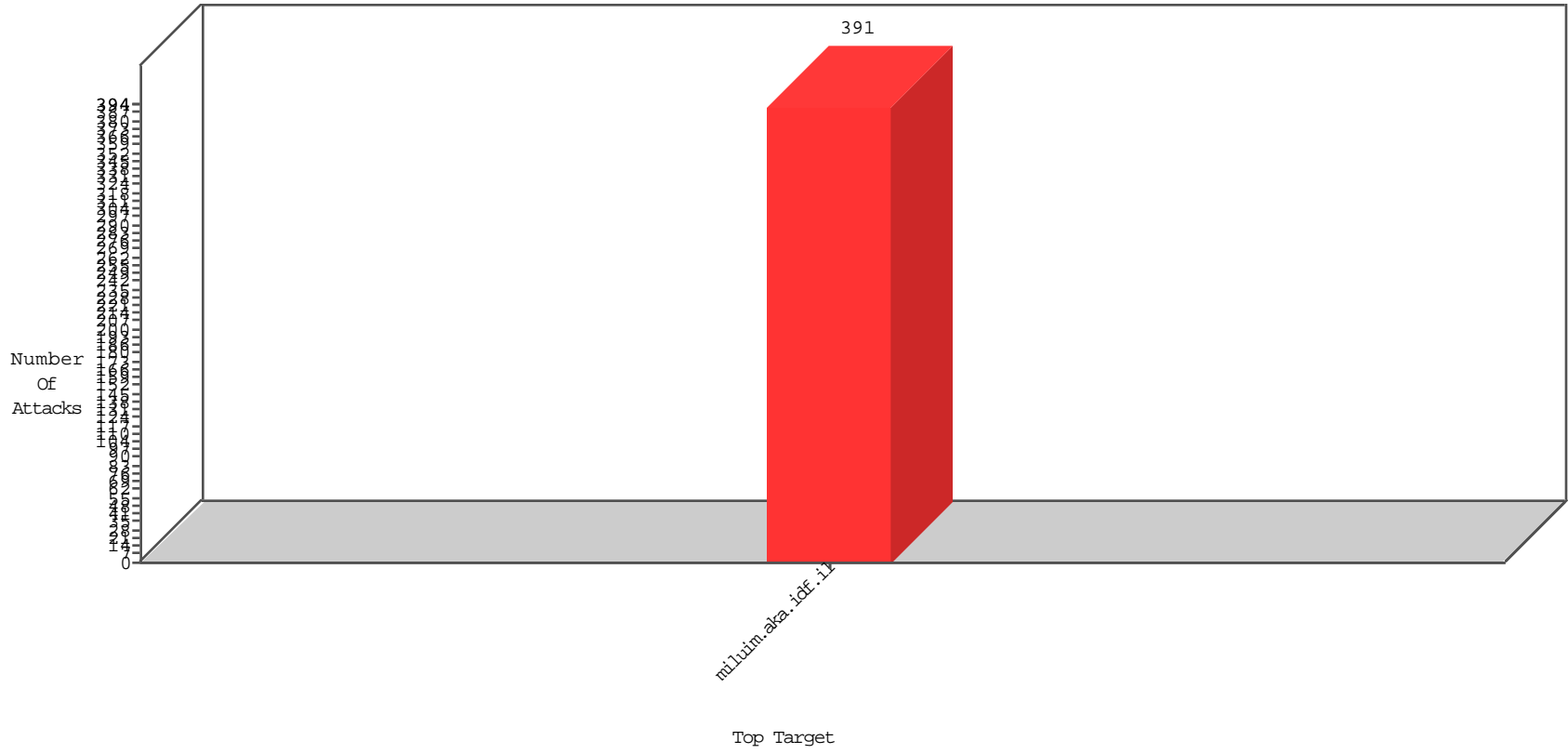


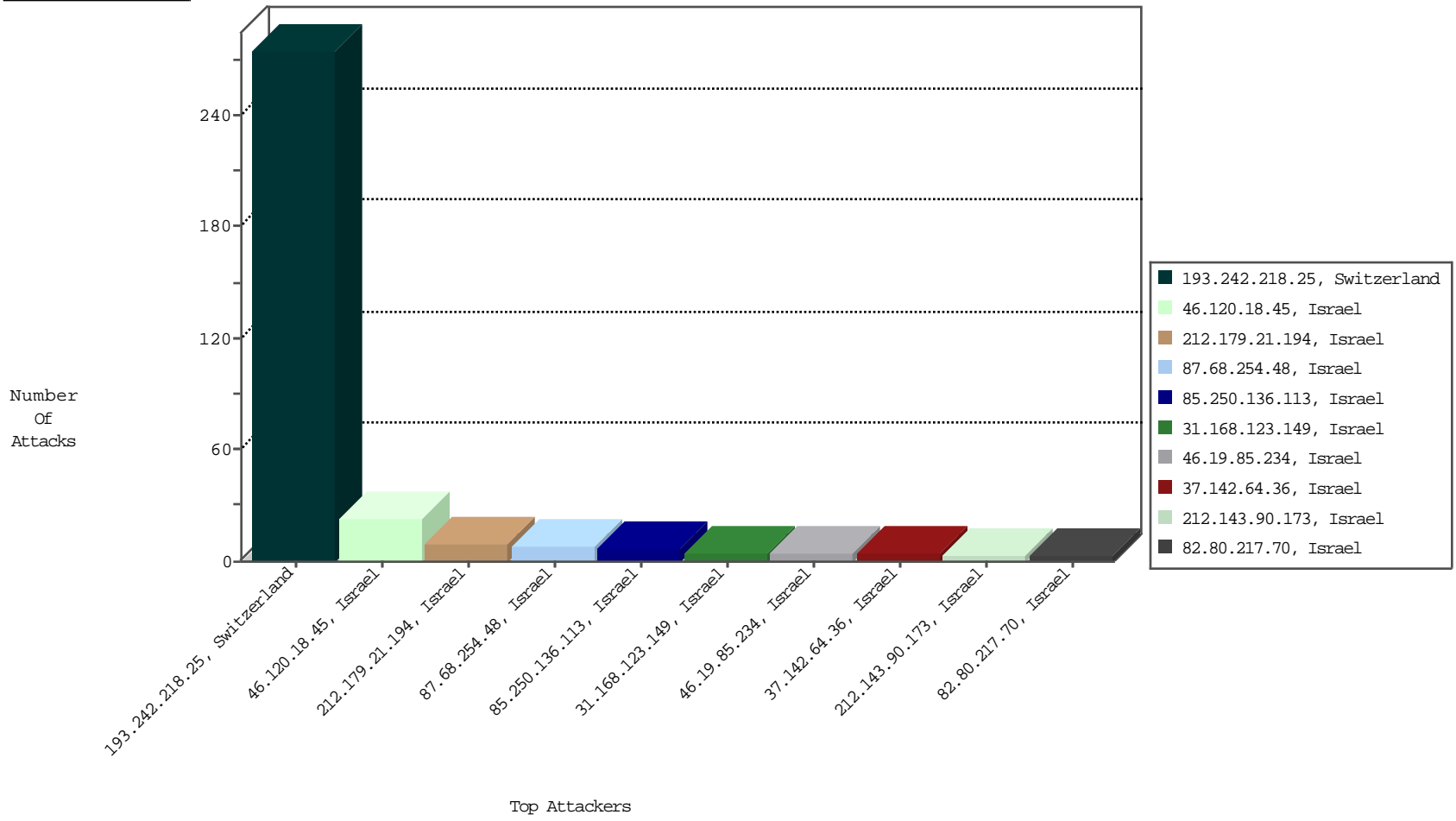
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | DP_location.Location | Count |
|------------------|--------------|----------------|-------------------|---|---------------|----------------------|-------|
| 193.242.218.25 | Switzerland | 147.237.0.120 | miluim.aka.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 275 |
| 82.80.217.70 | Israel | 147.237.0.120 | miluim.aka.idf.il | Block_Udp_All_Nets | drop | BBL-Israel | 3 |
| 79.176.4.235 | Israel | 147.237.0.120 | miluim.aka.idf.il | Block_Ntp_All_Net | drop | BBL-Israel | 1 |
| 185.89.217.227 | | 147.237.0.120 | miluim.aka.idf.il | TCP handshake violation, first packet not syn | drop | BBL-Frankfurt | 1 |

02-17-2016 to 02-18-2016

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 |
|------------------|--------------------|----------------|-------------------|------------------------------|-------|
| 66.249.93.215 | United States | 147.237.0.120 | miluim.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 185.130.5.240 | | 147.237.0.120 | miluim.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 190.216.146.151 | Chile | 147.237.0.120 | miluim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 194.63.140.74 | Russian Federation | 147.237.0.120 | miluim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 59.45.79.117 | China | 147.237.0.120 | miluim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 103.224.167.30 | Singapore | 147.237.0.120 | miluim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 188.64.169.106 | Russian Federation | 147.237.0.120 | miluim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 193.201.227.104 | Ukraine | 147.237.0.120 | miluim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.246.0.97 | China | 147.237.0.120 | miluim.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 36.72.228.72 | Indonesia | 147.237.0.120 | miluim.aka.idf.il | ET SCAN NMAP -sS window 4096 | 1 |

Top Attackers In FW

| Attacker Address | Attacker Geo | Target Address | Site | Name | Signature | Device Action | Count |
|------------------|--------------|----------------|------------------|--|--|---------------|-------|
| 149.78.3.164 | Israel | 147.237.0.120 | miluim.aka.idf.i | HTTP Format Sizes | 'User-Agent' header length exceeded maximum allowed length | monitor | 3230 |
| 62.90.45.1 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2870 |
| 79.183.137.203 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2304 |
| 79.178.0.149 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2304 |
| 81.218.201.231 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2304 |
| 2.52.160.41 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2304 |
| 109.67.107.92 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2304 |
| 87.68.41.74 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2160 |
| 84.228.36.252 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 1242 |
| 62.219.121.106 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 1224 |
| 79.176.184.210 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 576 |
| 79.180.160.132 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 468 |
| 77.127.205.203 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 225 |
| 79.181.118.105 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 153 |
| 2.54.141.22 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 144 |
| 79.182.180.175 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 144 |
| 79.181.179.57 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 144 |
| 82.81.33.15 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 121 |
| 46.19.85.203 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 82 |
| 46.19.85.105 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 81 |
| 2.54.132.9 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 81 |
| 149.78.54.234 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 64 |
| 2.52.163.69 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 64 |
| 37.26.148.247 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 64 |
| 109.64.204.102 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 49 |
| 84.109.126.246 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 49 |
| 46.19.85.203 | Israel | 147.237.0.120 | miluim.aka.idf.i | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 49 |
| 46.19.85.21 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 49 |
| 109.64.204.102 | Israel | 147.237.0.120 | miluim.aka.idf.i | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 49 |
| 37.26.146.145 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 49 |
| 46.19.85.179 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 49 |
| 37.26.147.229 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 49 |
| 46.19.85.237 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | | reject | 49 |
| 79.177.149.65 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 49 |
| 31.168.81.94 | Israel | 147.237.0.120 | miluim.aka.idf.i | Bad TCP sequence | Invalid sequence number | monitor | 40 |
| 37.26.147.137 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 36 |
| 2.54.146.12 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 2.52.5.77 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 46.19.85.108 | Israel | 147.237.0.120 | miluim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 36 |
| 79.178.225.178 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 37.26.149.213 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 36 |
| 46.16.142.100 | Cyprus | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 32 |
| 37.142.68.141 | Israel | 147.237.0.120 | miluim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 27 |
| 46.19.85.108 | Israel | 147.237.0.120 | miluim.aka.idf.i | Bad TCP sequence | Invalid ACK number | alert | 26 |
| 46.19.85.193 | Israel | 147.237.0.120 | miluim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 26 |
| 2.52.168.169 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 26 |
| 94.230.86.112 | Israel | 147.237.0.120 | miluim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 25 |
| 46.19.85.193 | Israel | 147.237.0.120 | miluim.aka.idf.i | Bad TCP sequence | Invalid ACK number | alert | 25 |
| 109.186.168.164 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 25 |
| 37.26.149.190 | Israel | 147.237.0.120 | miluim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 25 |

Top Attackers In WAF

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|------------------|---------------|----------------|------------------|--|---------------|-------|
| 46.120.18.45 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Unauthorized URL Access from 46.120.18.45 | Block | 13 |
| 46.120.18.45 | Israel | 147.237.0.120 | miluim.aka.idf.i | Distributed PHP Attempt | Block | 8 |
| 212.179.21.194 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Unauthorized URL Access from 212.179.21.194 | Block | 5 |
| 87.68.254.48 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized HTTP Method | Block | 4 |
| 87.68.254.48 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/ | Block | 3 |
| 31.168.123.149 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Redundant HTTP Headers in header Referer | Block | 3 |
| 212.179.21.194 | Israel | 147.237.0.120 | miluim.aka.idf.i | PHP Attempt | Block | 3 |
| 31.44.137.182 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Unauthorized URL Access from 31.44.137.182 | Block | 2 |
| 95.86.77.185 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewi6mb_olv7kahvgszokhrx_ay0qfggimaa&usg=afqjcne5p7m9pmcma58u2cjzfnfg7azoamw | Block | 2 |
| 2.54.39.100 | Israel | 147.237.0.120 | miluim.aka.idf.i | Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1442-he/miluim.aspx&?â€ž | Block | 2 |
| 212.143.90.173 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd | Block | 2 |
| 37.142.64.36 | Israel | 147.237.0.120 | miluim.aka.idf.i | Distributed PHP Attempt | Block | 2 |
| 46.120.18.45 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php | Block | 2 |
| 37.142.64.36 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php | Block | 2 |
| 5.22.135.196 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/1442-he/miluim.aspx&?â€ž | Block | 2 |
| 2.52.170.143 | Israel | 147.237.0.120 | miluim.aka.idf.i | Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1442-he/miluim.aspx&?â€ž | Block | 2 |
| 87.68.254.48 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Unauthorized URL Access from 87.68.254.48 | Block | 1 |
| 85.250.136.113 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Unauthorized URL Access from 85.250.136.113 | Block | 1 |
| 212.143.90.173 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/1935.gif | Block | 1 |
| 79.181.119.253 | Israel | 147.237.0.120 | miluim.aka.idf.i | Distributed PHP Attempt | Block | 1 |
| 176.13.18.104 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/1442-he/miluim.aspx&?â€ž | Block | 1 |
| 37.26.146.151 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/1431-he/miluim.aspx&?â€ž | Block | 1 |
| 85.250.136.113 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unknown Parameter Desk in www.miluim.aka.idf.il/894-he/miluim.aspx | Block | 1 |
| 85.64.93.168 | Israel | 147.237.0.120 | miluim.aka.idf.i | Distributed PHP Attempt | Block | 1 |
| 212.179.21.194 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php | Block | 1 |
| 192.116.232.69 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unknown Parameter wb48617274 in www.miluim.aka.idf.il/shared/ajax/createcaptchaimage.aspx | Block | 1 |
| 62.205.116.98 | Belgium | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/1442-he | Block | 1 |
| 149.88.73.50 | Israel | 147.237.0.120 | miluim.aka.idf.i | Distributed PHP Attempt | Block | 1 |
| 46.19.85.234 | Israel | 147.237.0.120 | miluim.aka.idf.i | Malformed URL http/1.1 | Block | 1 |
| 31.44.137.182 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewif8m3eup_kahkwkcwkhy1wbfoqfgghma&a&usg=afqjcne5p7m9pmcma58u2cjzfnfg7azoamw | Block | 1 |
| 85.250.136.113 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unknown Parameter D in www.miluim.aka.idf.il/894-he/miluim.aspx | Block | 1 |
| 79.181.119.253 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Unauthorized URL Access from 79.181.119.253 | Block | 1 |
| 185.35.62.11 | Switzerland | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to 147.237.0.120/ | Block | 1 |
| 120.141.193.113 | Malaysia | 147.237.0.120 | miluim.aka.idf.i | E-mail collector robots 14 | Block | 1 |
| 5.22.135.196 | Israel | 147.237.0.120 | miluim.aka.idf.i | Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1442-he/miluim.aspx&?â€ž | Block | 1 |
| 85.250.136.113 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unknown Parameter Deskt in www.miluim.aka.idf.il/894-he/miluim.aspx | Block | 1 |
| 85.64.93.168 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Unauthorized URL Access from 85.64.93.168 | Block | 1 |
| 198.204.249.34 | United States | 147.237.0.120 | miluim.aka.idf.i | URL is Above Root Directory www.miluim.aka.idf.il/./shared/usercontrols/footer/1230-he/miluim.aspx | Block | 1 |
| 66.249.66.55 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/shared/usercontrols/headerupper/ | Block | 1 |
| 46.19.85.234 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized HTTP Method | Block | 1 |
| 149.88.73.50 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Unauthorized URL Access from 149.88.73.50 | Block | 1 |
| 85.250.136.113 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unknown Parameter De in www.miluim.aka.idf.il/894-he/miluim.aspx | Block | 1 |
| 79.181.119.253 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php | Block | 1 |
| 185.89.217.233 | | 147.237.0.120 | miluim.aka.idf.i | URL is Above Root Directory www.miluim.aka.idf.il/./images/shared/hp/hp_icon.png | Block | 1 |
| 120.141.193.113 | Malaysia | 147.237.0.120 | miluim.aka.idf.i | eMail Hoarding | Block | 1 |
| 85.250.136.113 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unknown Parameter Deskto in www.miluim.aka.idf.il/894-he/miluim.aspx | Block | 1 |
| 85.64.93.168 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php | Block | 1 |
| 207.46.13.17 | United States | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/homepage.aspx | Block | 1 |
| 79.178.148.89 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/1442-he/miluim.aspx&?â€ž | Block | 1 |
| 46.19.85.234 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unknown HTTP Request Method luim.aspx in URL www.miluim.aka.idf.il/http/1.1 | Block | 1 |
| 149.88.73.50 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php | Block | 1 |
| 94.102.49.78 | Netherlands | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to savash.org/ | Block | 1 |
| 31.168.123.149 | Israel | 147.237.0.120 | miluim.aka.idf.i | Redundant HTTP Headers Referer | Block | 1 |
| 85.250.136.113 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unknown Parameter Des in www.miluim.aka.idf.il/894-he/miluim.aspx | Block | 1 |
| 79.181.147.208 | Israel | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.behatsdaa.org.il | Block | 1 |
| 61.135.190.72 | China | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to 147.237.0.120/ | Block | 1 |
| 192.116.232.69 | Israel | 147.237.0.120 | miluim.aka.idf.i | Multiple Unauthorized URL Access from 192.116.232.69 | Block | 1 |
| 141.212.122.193 | United States | 147.237.0.120 | miluim.aka.idf.i | Unauthorized URL Access to 147.237.0.120/ | Block | 1 |
| 46.19.85.234 | Israel | 147.237.0.120 | miluim.aka.idf.i | Illegal HTTP Version | Block | 1 |