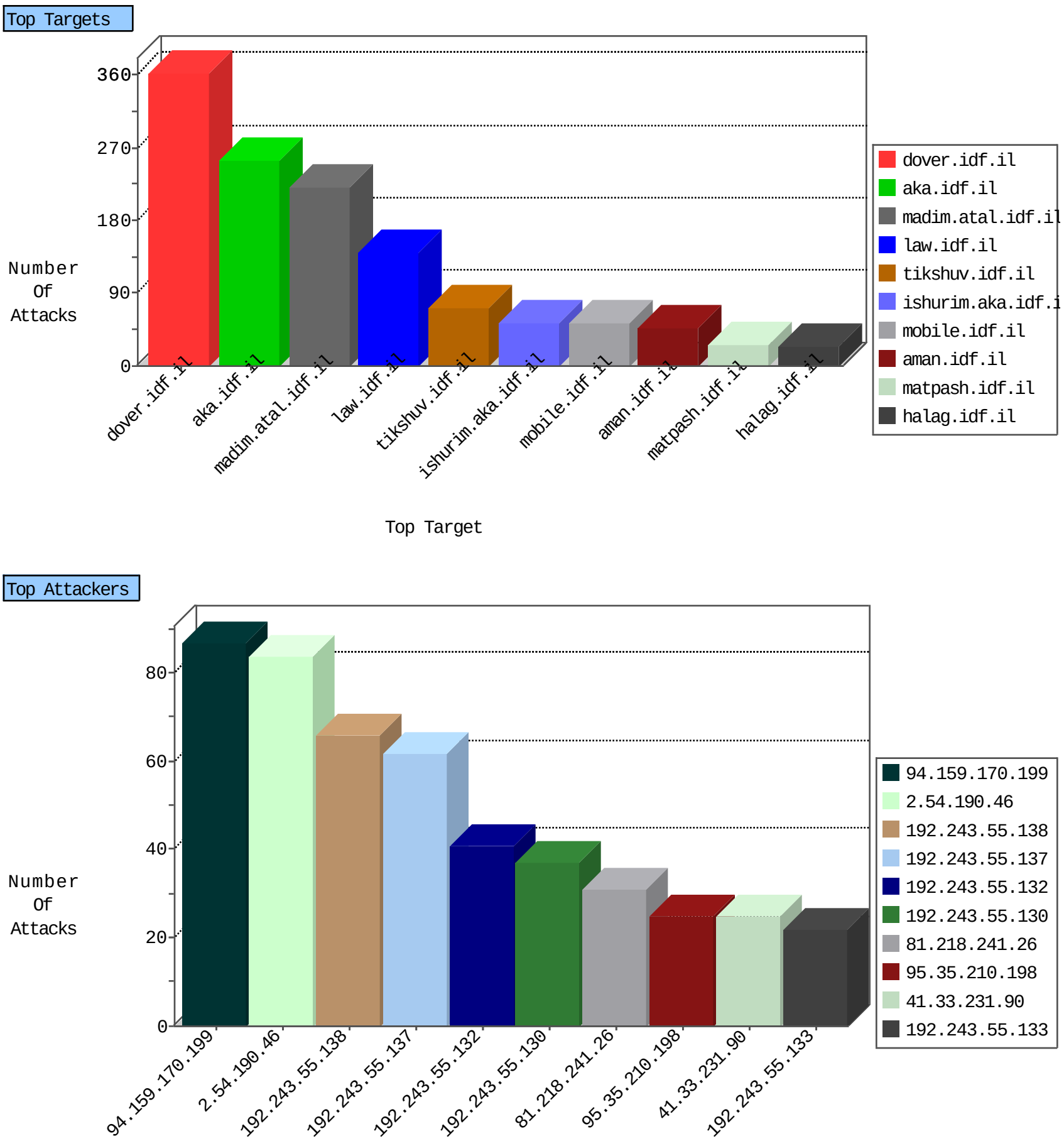
03-03-2016-13:04:09 to 03-03-2016-14:04:09

# IDF Under Attack Daily Report



03-03-2016-13:04:09 to 03-03-2016-14:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 6 |
| 81.218.65.210 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 6 |
| 82.145.217.215 | Europe | 147.237.72.167 | ishurim.aka.idf.il | Block_Ip_Web_In | drop | 5 |
| 124.244.180.73 | Hong Kong | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 2 |

03-03-2016-13:04:09 to 03-03-2016-14:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.180.153.13 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 19 |
| 2.54.132.5 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 18 |
| 81.218.56.171 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 12 |
| 176.13.7.45 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 123.126.113.154 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 5 |
| 80.178.195.147 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 185.106.92.164 | | 147.237.72.167 | ishurim.aka.idf.il | 20086: HTTP: Mueblackcat Security Scanner | Block | 2 |
| 157.55.39.210 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 212.150.78.2 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 176.13.19.79 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 93.173.248.117 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 136.243.103.92 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 207.46.13.96 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 185.106.92.164 | | 147.237.72.167 | ishurim.aka.idf.il | 20085: HTTP: Mueblackcat Security Scanner Initial Request | Block | 1 |

03-03-2016-13:04:09 to 03-03-2016-14:04:09

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 213.8.204.46 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 62.219.154.124 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 209.126.116.147 | 147.237.76.202 | United States | e.halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.151.52.139 | 147.237.72.167 | Ukraine | ishurim.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 202.71.25.29 | 147.237.8.45 | India | e.eitan.idf.il | ET SCAN NMAP -f -sS | 1 |
| 46.19.85.221 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.243.55.132 | 147.237.77.216 | Dominica | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.29.15.174 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.208.84 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 93.172.63.41 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.70.82.15 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.228.191.120 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 218.246.0.97 | 147.237.77.227 | China | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 66.249.64.50 | 147.237.72.166 | United States | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.235.98.139 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 62.90.88.104 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 202.71.25.29 | 147.237.8.45 | India | e.eitan.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 46.116.114.154 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 194.56.215.218 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.106.92.164 | 147.237.72.167 |  | ishurim.aka.idf.il | ET WEB_SERVER Muieblackcat scanner | 1 |
| 2.54.185.66 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.102.48.193 | 147.237.76.44 | Netherlands | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 87.71.18.150 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.250.65.36 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.180.228.150 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

03-03-2016-13:04:09 to 03-03-2016-14:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 22 |
| 149.20.63.13 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 22 |
| 2.54.175.53 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 18 |
| 95.35.210.198 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 17 |
| 81.218.241.26 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 12 |
| 79.183.55.68 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 81.218.241.26 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 2.52.173.72 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 46.19.86.75 | Israel | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 11 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 77.126.148.82 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 46.19.85.194 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 95.35.159.61 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 192.243.55.130 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 197.211.52.13 | Nigeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 46.19.86.176 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 192.243.55.130 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 41.35.128.77 | Egypt | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 7 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 46.19.85.102 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 5.22.131.44 | Israel | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 7 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 185.32.179.122 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 192.243.55.138 | Dominica | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.86.46 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 87.68.78.132 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 6 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 46.210.197.207 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 79.181.167.215 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 192.243.55.138 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 192.243.55.132 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 192.243.55.132 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 81.218.241.26 | Israel | 147.237.72.167 | ishurim.aka.idf.i | drop | First packet isn't SYN | drop | 6 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 192.243.55.136 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 2.52.175.40 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 192.243.55.132 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 192.243.55.130 | Dominica | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 192.243.55.129 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 192.243.55.130 | Dominica | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 5 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 94.159.170.199 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 87 |
| 2.54.190.46 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 84 |
| 80.246.137.40 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 14 |
| 109.253.209.206 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 109.253.156.101 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 79.176.149.221 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 4 |
| 176.13.14.196 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 62.219.236.190 | Israel | 147.237.77.176 | matpash.idf.il | Distributed Unauthorized URL Access on www.cogat.idf.il/templates/shared/usercontrols/promotioncube/ | Block | 3 |
| 82.80.131.234 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 168.63.200.167 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 2.54.160.185 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 65.55.210.90 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 199.30.25.13 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 176.13.6.202 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.58 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 65.55.210.198 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 95.35.210.198 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 95.35.210.198 | Block | 3 |
| 109.253.202.235 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 95.35.159.61 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 37.26.147.204 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 176.13.9.28 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 2.52.173.72 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.164 | Israel | 147.237.77.176 | matpash.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 108.4.143.45 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx | Block | 1 |
| 91.135.102.165 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif | Block | 1 |
| 46.19.85.36 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 212.76.106.172 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-21570-he/idfgdover.aspx&sa=u&ved=0ahukewir2dc-u6tlah uiz3ikhdqgdkgqfgglmae&usg=afqjcngkxkptobpol8pgxzxftd95sstiiw | Block | 1 |
| 79.177.100.69 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 37.26.148.192 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 2.54.25.85 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 1 |
| 95.35.210.198 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 46.19.85.124 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 1 |
| 37.26.148.254 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1283-13885-en/dov. | Block | 1 |
| 66.249.66.76 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp | Block | 1 |
| 31.168.113.60 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser | Block | 1 |
| 46.19.86.46 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 109.65.7.55 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 46.19.85.102 | Israel | 147.237.77.233 | atal.idf.il | Abnormally Long Request request version | Block | 1 |
| 212.76.121.224 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/&sa=u&ved=0ahukewjx4prju6tlahufyxikhcuyasqqfggnmaa&usg=afqjcnh4ucr3bqpmkvh4yz9t7jscutsloq | Block | 1 |
| 79.183.169.121 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 37.26.148.204 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 181.15.149.157 | Argentina | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.253.214.137 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 95.35.210.198 | Israel | 147.237.77.234 | halag.idf.il | Multiple Unauthorized URL Access from 95.35.210.198 | Block | 1 |
| 46.19.85.164 | Israel | 147.237.77.176 | matpash.idf.il | Distributed Abnormally Long Request | Block | 1 |
| 40.77.167.60 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/ | Block | 1 |
| 82.81.57.208 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/home/giyus.aspx | Block | 1 |
| 66.249.66.126 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/pdf/files/4/105744.pdf | Block | 1 |
| 37.26.146.205 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |