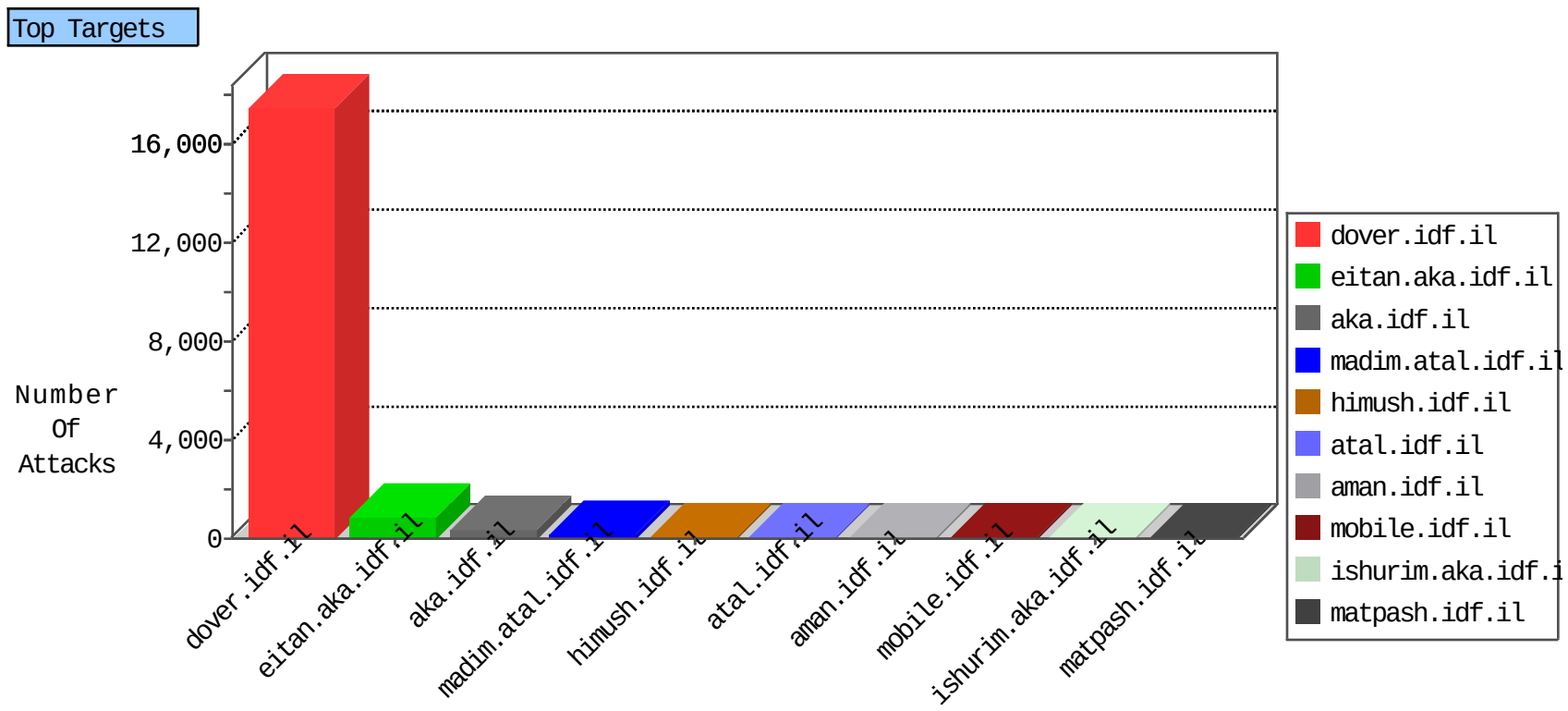
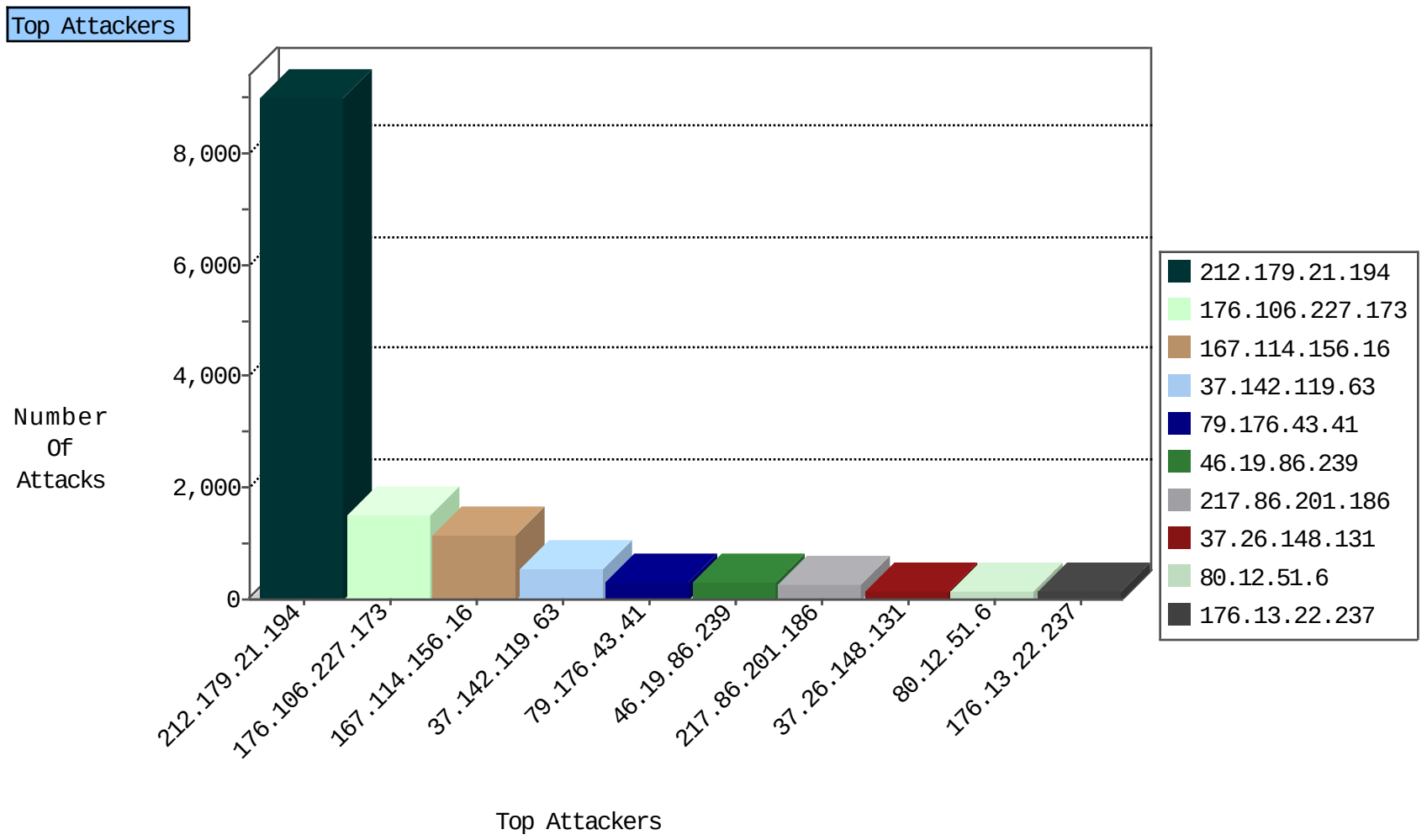
11-05-2015-17:04:00 to 11-05-2015-18:04:00

# IDF Under Attack Daily Report

Top Targets




Top Attackers



11-05-2015-17:04:00 to 11-05-2015-18:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 1864 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 904 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 502 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 389 |
| 66.249.67.202 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 85 |
| 79.177.195.251 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 59 |
| 46.19.86.253 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 55 |
| 84.108.132.157 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 36 |
| 77.126.205.232 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 27 |
| 109.66.127.252 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 26 |
| 176.53.193.18 | Russian Federation | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 25 |
| 95.86.119.38 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 25 |
| 2.52.55.234 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 22 |
| 37.26.149.208 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 18 |
| 37.26.146.243 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 17 |
| 46.19.86.33 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 15 |
| 176.13.15.91 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 12 |
| 80.246.136.219 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 10 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 79.235.16.150 | Germany | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 46.117.133.72 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 176.13.22.237 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 85.250.1.37 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 84.109.96.170 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 85.64.115.69 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 7 |
| 77.125.122.187 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 7 |
| 81.218.48.37 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 7 |
| 46.19.86.16 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 7 |
| 5.22.129.218 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 109.226.16.21 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 130.154.3.250 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 46.120.123.44 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 84.229.132.183 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 31.168.19.211 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 37.142.68.32 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 79.235.16.150 | Germany | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 5 |
| 89.138.46.89 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 84.109.114.97 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 83.150.36.3 | Switzerland | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 197.52.179.123 | Egypt | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 144.36.120.99 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 176.13.0.168 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 2.54.38.238 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 79.182.3.229 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 109.64.131.214 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 85.65.198.67 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 5.102.254.211 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 79.179.212.164 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 4 |
| 79.235.16.150 | Germany | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 4 |
| 191.223.171.52 | Brazil | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |

11-05-2015-17:04:00 to 11-05-2015-18:04:00

## Top Attackers In IPS

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

11-05-2015-17:04:00 to 11-05-2015-18:04:00

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |

11-05-2015-17:04:00 to 11-05-2015-18:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9007 |
| 176.106.227.173 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1528 |
| 79.176.43.41 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 315 |
| 46.19.86.239 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 285 |
| 217.86.201.186 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 147 |
| 37.26.148.131 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 137 |
| 80.12.51.6 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 132 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 112 |
| 176.13.22.237 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 111 |
| 132.73.196.41 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 89 |
| 105.168.16.186 | Angola | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 88 |
| 54.187.55.213 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 82 |
| 141.0.15.130 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 70 |
| 82.80.166.44 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 68 |
| 213.151.36.118 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 67 |
| 197.52.179.123 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 64 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 63 |
| 130.154.3.250 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 59 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 56 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 56 |
| 31.154.163.30 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 55 |
| 205.203.135.1 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 53 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 53 |
| 84.108.39.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 51 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 50 |
| 100.100.4.5 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 48 |
| 176.53.193.18 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 48 |
| 67.213.254.154 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 47 |
| 217.86.201.186 | Germany | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 46 |
| 100.100.98.113 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 43 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 41 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 41 |
| 2.54.21.190 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 40 |
| 213.151.60.219 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 39 |
| 87.69.73.222 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 146.255.183.211 | Estonia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 197.41.147.77 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 85.64.115.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 35 |
| 213.199.214.20 | Poland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 33 |
| 138.134.192.10 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 191.102.73.70 | Colombia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 37.26.146.243 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 87.68.243.99 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 46.19.85.162 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 29 |
| 217.86.201.186 | Germany | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | alert | 28 |
| 2.54.38.238 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 38.122.127.226 | United States | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 26 |
| 84.75.161.69 | Switzerland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 176.13.21.213 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |

11-05-2015-17:04:00 to 11-05-2015-18:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 37.142.119.63 | Israel | 147.237.76.200 | eitan.aka.idf.il | Too Many of the Same Response Code (404) in Session from 37.142.119.63 | Block | 536 |
| 149.78.76.243 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 40 |
| 2.52.145.216 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 31 |
| 84.228.57.92 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 19 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 4 |
| 79.179.169.247 | Israel | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 4 |
| 79.179.169.247 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php | Block | 4 |
| 77.125.119.198 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.125.119.198 | Block | 4 |
| 84.109.116.45 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 3 |
| 46.19.86.57 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.158 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 192.118.11.118 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 176.12.143.226 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.103 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 37.26.149.204 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 46.19.86.49 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 2 |
| 80.246.133.234 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 46.19.85.133 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 213.57.160.27 | Israel | 147.237.72.156 | aman.idf.il | Too Many Cookies in a Request - 109 cookies | Block | 1 |
| 66.249.69.42 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.69.42 | Block | 1 |
| 183.79.222.134 | Japan | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx | None | 1 |
| 109.64.29.55 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/favicon.ico | Block | 1 |
| 66.249.67.59 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 5.102.254.243 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/ | Block | 1 |
| 79.176.208.73 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/ | Block | 1 |
| 66.249.67.234 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 149.78.76.243 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index | Block | 1 |
| 66.249.67.6 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 86.59.68.62 | Austria | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg | Block | 1 |
| 81.218.140.112 | Israel | 147.237.77.176 | matpash.idf.il | E-mail collector robots 14 | Block | 1 |
| 46.19.85.167 | Israel | 147.237.77.216 | dover.idf.il | Malformed URL | Block | 1 |
| 216.223.27.31 | United States | 147.237.77.74 | law.idf.il | Distributed URL is Above Root Directory | Block | 1 |
| 66.249.69.48 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-20387-he/dover.aspx | Block | 1 |
| 2.52.145.216 | Israel | 147.237.0.19 | madim.atal.idf.i | Cookie Tampering on cookie _pk_ref.322.9cd2: Expected ["","",1446731938,"https://www.google.co.il/"], Observed ["","",1446736785,"https://www.google.co.il/"] | None | 1 |
| 183.79.223.73 | Japan | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in Header Name Â  HTTP/1.0 | Block | 1 |
| 141.212.122.64 | United States | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to /x | Block | 1 |
| 66.249.67.65 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/haredim/general.aspx | Block | 1 |
| 62.210.88.201 | France | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 51.254.206.142/httptest.php | Block | 1 |
| 84.111.54.98 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 188.165.15.235 | France | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 79.176.208.73 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.67.250 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 149.88.55.199 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.67.13 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 89.138.82.169 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 81.218.140.112 | Israel | 147.237.77.176 | matpash.idf.il | eMail Hoarding | Block | 1 |
| 46.19.85.167 | Israel | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method 2x4w45 in URL | Block | 1 |
| 183.79.223.73 | Japan | 147.237.72.166 | aka.idf.il | Illegal HTTP Version | Block | 1 |
| 141.212.122.96 | United States | 147.237.0.19 | madim.atal.idf.i | Unauthorized URL Access to /x | Block | 1 |
| 66.249.67.122 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |

11-05-2015-17:04:00 to 11-05-2015-18:04:00