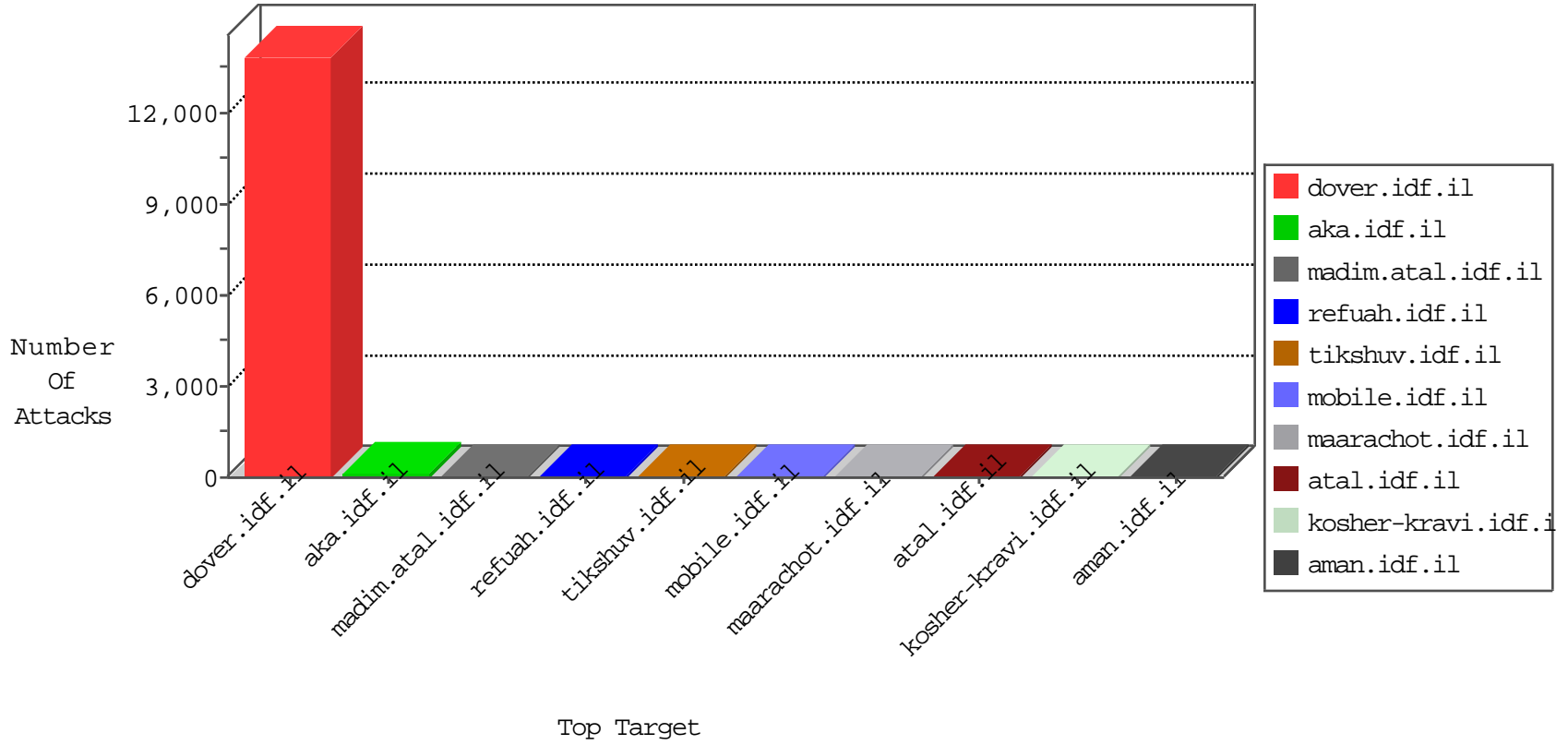


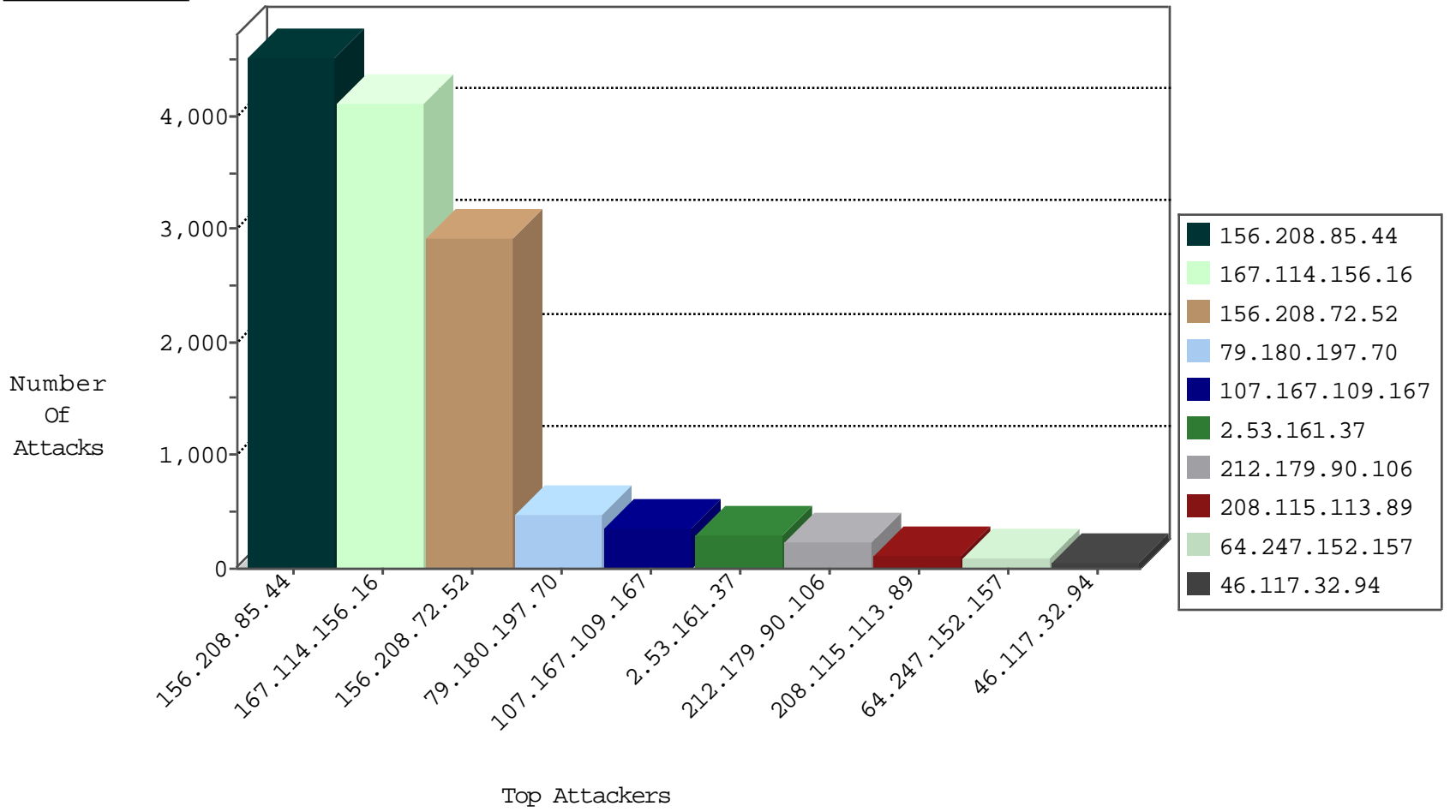
IDF Under Attack Daily Report



Top Targets



Top Attackers



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 | Block_Tp_Web_In | drop | 4102 |
| 156.208.85.44 | Egypt | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1944 |
| 156.208.72.52 | Egypt | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 341 |
| 81.218.65.210 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 134.147.203.115 | Germany | 147.237.76.86 | navy.idf.il | Block_Ntp_All_Net | drop | 2 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 94.102.49.116 | Netherlands | 147.237.72.167 | ishurim.aka.idf.il | Block_Ntp_All_Net | drop | 1 |
| 62.138.3.98 | Germany | 147.237.76.148 | ggcenter.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 94.102.49.116 | Netherlands | 147.237.77.243 | mobile.idf.il | Block_Udp_All_Nets | drop | 1 |
| 66.249.78.146 | Israel | 147.237.72.166 | aka.idf.il | HTTP-Misc-BadBlue-Dir-Trave-2 | dest-reset | 1 |
| 45.32.95.13 | Netherlands | 147.237.72.167 | ishurim.aka.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.70.184.164 | Netherlands | 147.237.72.14 | dover.idf.il(old) | JLM_Under_Attack_Con_Https | drop | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|----------------|---|---------------|-------|
| 79.178.223.238 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 5.102.242.252 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 66.249.66.187 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|------------------|----------------|------------------|--------------------------|---|-------|
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 66.249.79.75 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 76.181.249.213 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 201.175.108.99 | 147.237.77.205 | Mexico | prisha.idf.il | SERVER-WEBAPP bad HTTP/1.1 request, Potentially worm attack | 1 |
| 116.109.156.108 | 147.237.8.45 | Vietnam | e.eitan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 115.182.17.13 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 93.174.93.96 | 147.237.0.19 | Netherlands | madim.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 76.181.249.213 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 76.181.249.213 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 115.182.17.13 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 104.232.98.38 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 82.117.208.243 | 147.237.0.17 | | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------|----------------|--------------|--|---|---------------|-------|
| 156.208.85.44 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2452 |
| 156.208.72.52 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2424 |
| 79.180.197.70 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 475 |
| 107.167.109.167 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 354 |
| 2.53.161.37 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 300 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 228 |
| 156.208.72.52 | Egypt | 147.237.77.216 | dover.idf.il | drop | | drop | 129 |
| 156.208.85.44 | Egypt | 147.237.77.216 | dover.idf.il | drop | | drop | 114 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 110 |
| 64.247.152.157 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 91 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 46.19.85.163 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 25 |
| 156.208.72.52 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 22 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 192.249.66.247 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 45.35.64.142 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 46.19.85.91 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 156.208.85.44 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 81.218.106.146 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 79.181.218.142 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 109.160.149.29 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 109.186.49.99 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.85.40 | Israel | 147.237.76.42 | refuah.idf.i | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 84.109.30.239 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 46.19.85.40 | Israel | 147.237.76.42 | refuah.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 207.46.13.136 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 94.77.196.82 | Saudi Arabia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 207.35.33.162 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.23 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 46.119.112.23 | Ukraine | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 77.125.7.39 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 207.228.78.72 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 5.102.242.252 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 5.29.147.108 | Israel | 147.237.77.243 | mobile.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.64.222.60 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 178.7.201.147 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.67.150.19 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.64.81.245 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 79.176.71.126 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 84.228.211.143 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.64.147.124 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 94.230.86.32 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 5.28.174.222 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.120.131.74 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 79.176.39.147 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|------------------------|--|---------------|-------|
| 46.117.32.94 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 48 |
| 2.53.25.43 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 109.253.227.116 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 109.253.227.122 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.13.107 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.227.112 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.253.227.113 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.65.15.126 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.178.135.10 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/14-he | Block | 2 |
| 188.76.145.30 | Spain | 147.237.77.216 | dover.idf.il | Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx | Block | 2 |
| 89.138.65.172 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 207.46.13.82 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/... | Block | 1 |
| 66.249.78.248 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2370.jpg | Block | 1 |
| 156.208.85.44 | Egypt | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 62.210.254.52 | France | 147.237.72.166 | aka.idf.il | Unknown Parameter amp;w in www.aka.idf.il/main/giyus/captcha.ashx | None | 1 |
| 109.253.208.143 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter moduleTo tqGoTo in www.aka.idf.il/main/giyus/login.aspx | None | 1 |
| 81.111.195.163 | United Kingdom | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/wp-login.php | Block | 1 |
| 66.249.78.104 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 201.175.108.99 | Mexico | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 1 |
| 2.53.138.251 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 91.135.102.161 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile | Block | 1 |
| 207.46.13.117 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to www.maarachot.idf.il/pdf/files/ %2 x %2 %2 %2 %2 | Block | 1 |
| 68.180.230.45 | United States | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/robots.txt | Block | 1 |
| 66.249.64.131 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 159.226.95.66 | China | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 81.111.195.163 | United Kingdom | 147.237.76.86 | navy.idf.il | PHP Attempt | Block | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp | Block | 1 |
| 201.175.108.99 | Mexico | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 1 |
| 141.212.122.209 | United States | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to 147.237.0.19/ | Block | 1 |
| 2.55.29.161 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1682.doc | Block | 1 |
| 95.35.131.172 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 207.46.13.178 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/sites/hoshen | Block | 1 |
| 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 | 1 |
| 66.249.66.123 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3142.jpg | Block | 1 |
| 81.111.195.163 | United Kingdom | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/wp-login.php | Block | 1 |
| 201.175.108.99 | Mexico | 147.237.77.235 | sviva.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 1 |
| 66.249.78.236 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3469.jpg | Block | 1 |
| 149.78.230.79 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 23.80.147.64 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/ | Block | 1 |
| 66.249.66.125 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2977.jpg | Block | 1 |
| 84.109.205.40 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile | Block | 1 |
| 207.46.13.82 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 207.46.13.82 | Block | 1 |
| 66.249.78.242 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 156.208.72.52 | Egypt | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 109.66.77.215 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https://www.idf.il/ | Block | 1 |
| 81.111.195.163 | United Kingdom | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 66.249.78.97 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 188.247.72.52 | Jordan | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to ww.idf.il/arr/ | Block | 1 |
| 109.253.227.120 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 2.53.42.171 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |