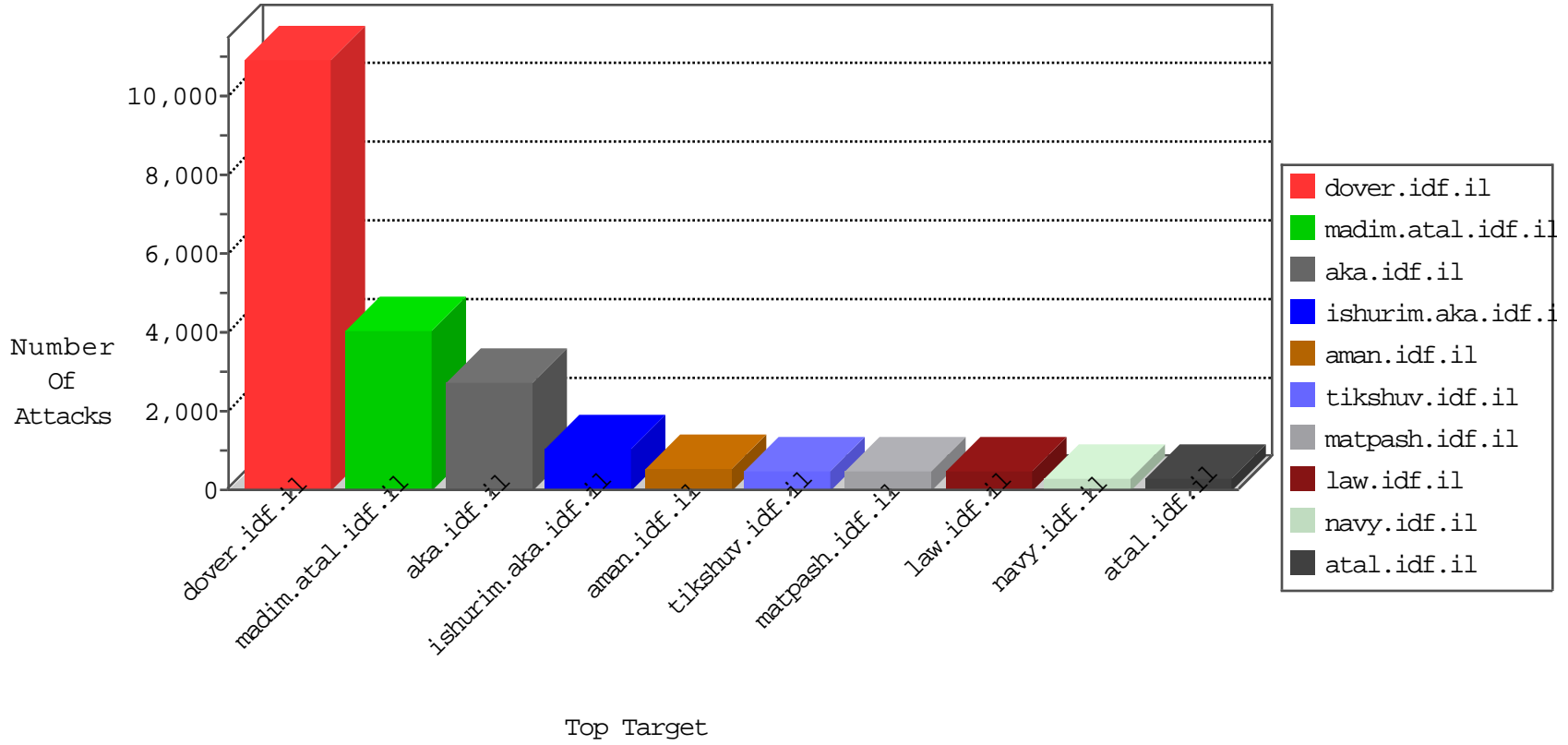


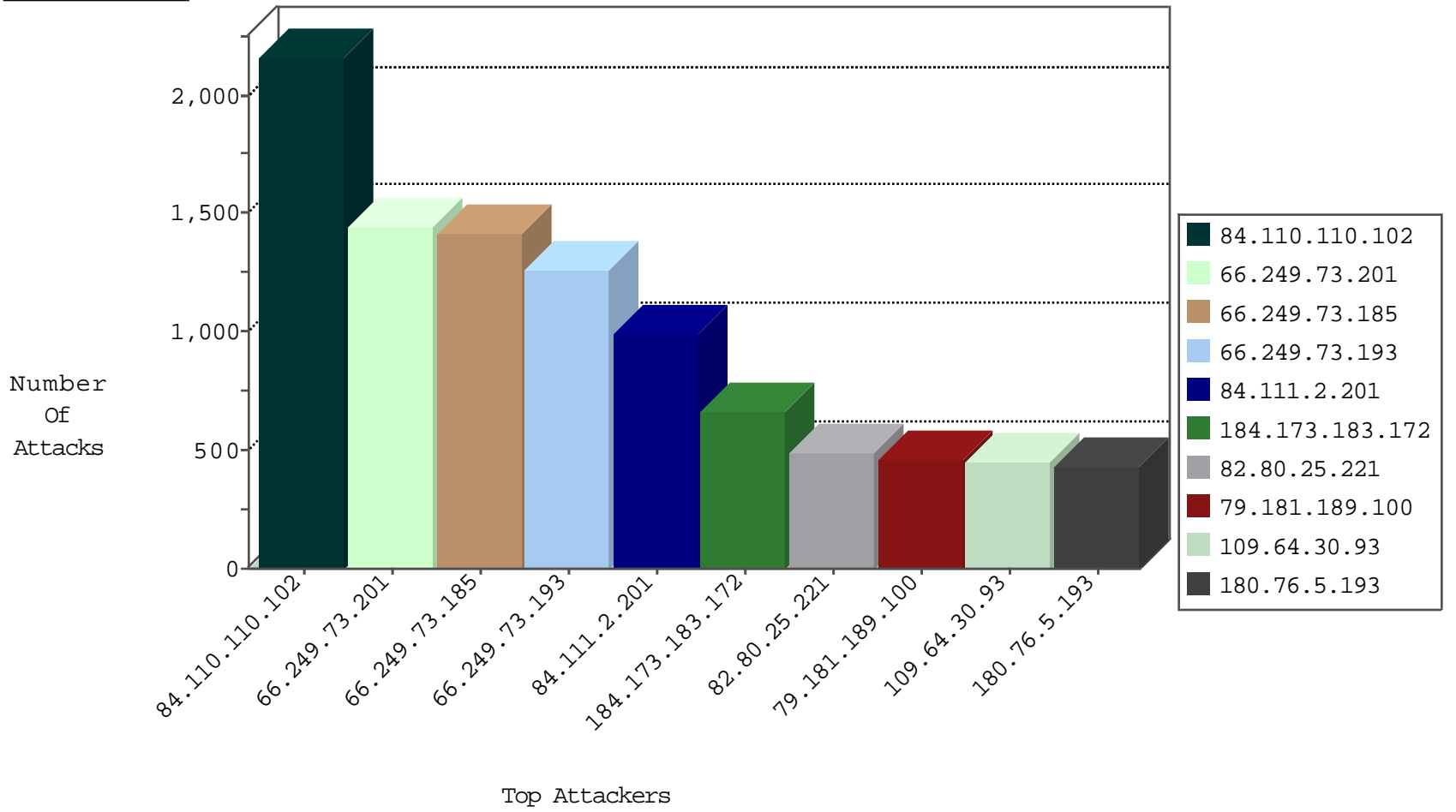
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|------------------|---------------------------------|----------------|------------------------|---|---------------|-------------------|
| 66.249.79.157 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 95057 |
| 66.249.79.42 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 45072 |
| 66.249.64.10 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 37241 |
| 66.249.79.5 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 36762 |
| 66.249.79.34 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 34949 |
| 66.249.79.50 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 32301 |
| 66.249.67.84 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 28923 |
| 66.249.79.13 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 27506 |
| 66.249.67.76 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 26606 |
| 66.249.78.82 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 26582 |
| 66.249.64.128 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 19715 |
| 66.249.78.93 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 19702 |
| 66.249.78.89 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 19517 |
| 66.249.81.206 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 17658 |
| 66.249.64.132 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 16510 |
| 66.249.64.191 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 13898 |
| 66.249.78.86 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 12316 |
| 66.249.81.253 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 12281 |
| 66.249.78.79 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 11275 |
| 66.249.64.14 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 10994 |
| 66.249.64.136 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 10658 |
| 66.249.81.209 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 10405 |
| 66.249.67.100 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 10279 |
| 66.249.81.239 | United States | 147.237.72.167 | ishurim.aka.idf.il | TCP handshake violation, first packet not syn | drop | 9804 |
| 194.169.221.236 | United Kingdom | 147.237.77.176 | matpash.idf.il | TCP handshake violation, first packet not syn | drop | 9603 |
| 66.249.81.196 | United States | 147.237.0.34 | tikshuv.idf.il | TCP handshake violation, first packet not syn | drop | 9435 |
| 66.249.81.172 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 9313 |
| 77.247.178.126 | Netherlands | 147.237.0.34 | tikshuv.idf.il | TCP handshake violation, first packet not syn | drop | 8181 |
| 77.247.178.126 | Netherlands | 147.237.0.16 | my-kosher-kravi.idf.il | TCP handshake violation, first packet not syn | drop | 7488 |
| 66.249.81.227 | United States | 147.237.77.176 | matpash.idf.il | TCP handshake violation, first packet not syn | drop | 7426 |
| 66.249.78.15 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 7234 |
| 66.249.64.183 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 7172 |
| 66.249.67.112 | United States | 147.237.77.234 | halag.idf.il | TCP handshake violation, first packet not syn | drop | 6788 |
| 85.28.114.69 | Belgium | 147.237.77.176 | matpash.idf.il | TCP handshake violation, first packet not syn | drop | 6644 |
| 66.249.78.96 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 5804 |
| 66.249.83.162 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 5452 |
| 66.249.88.137 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 4405 |
| 185.4.227.194 | Turkey | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 4280 |
| 74.89.82.190 | United States | 147.237.72.156 | aman.idf.il | TCP handshake violation, first packet not syn | drop | 4079 |
| 66.249.64.124 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 4008 |
| 66.249.81.154 | United States | 147.237.77.234 | halag.idf.il | TCP handshake violation, first packet not syn | drop | 3998 |
| 176.67.108.98 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 3981 |
| 66.249.78.60 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 3470 |
| 66.249.67.108 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 3439 |
| 66.249.81.234 | United States | 147.237.0.15 | kosher-kravi.idf.il | TCP handshake violation, first packet not syn | drop | 2991 |
| 66.249.67.92 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 2953 |
| 144.76.36.23 | Germany | 147.237.77.61 | e.cogat.idf.il | TCP handshake violation, first packet not syn | drop | 2907 |

02-20-2015-00:00:07 to 02-21-2015-00:00:07

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|------------------|------------------|----------------|----------------|---|---------------|-------------------|
| 66.249.64.6 | United States | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 2877 |
| 66.249.81.199 | United States | 147.237.0.34 | tikshuv.idf.il | TCP handshake violation, first packet not syn | drop | 2658 |
| 66.249.81.134 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 1964 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|------------------|------------------|----------------|--------------------------|---|---------------|-------|
| 84.110.110.102 | Israel | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 2162 |
| 84.111.2.201 | Israel | 147.237.72.166 | aka.idf.il | DVRep_P-N_40-59 | Permit | 990 |
| 184.173.183.172 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 385 |
| 180.76.5.193 | China | 147.237.77.176 | matpash.idf.il | DVRep_P-N_40-59 | Permit | 326 |
| 128.242.249.12 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 175 |
| 184.173.183.172 | United States | 147.237.76.86 | navy.idf.il | DVRep_P-N_40-59 | Permit | 163 |
| 184.173.183.172 | United States | 147.237.77.74 | law.idf.il | DVRep_P-N_40-59 | Permit | 113 |
| 180.76.5.193 | China | 147.237.0.34 | tikshuv.idf.il | DVRep_P-N_40-59 | Permit | 101 |
| 85.250.128.43 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 35 |
| 96.31.35.151 | United States | 147.237.77.74 | law.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 16 |
| 206.72.113.4 | United States | 147.237.77.74 | law.idf.il | 3808: HTTP: SQL Injection Variable Declaration Evasion | Block | 16 |
| 206.72.113.4 | United States | 147.237.77.74 | law.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 16 |
| 96.31.35.151 | United States | 147.237.77.74 | law.idf.il | 3808: HTTP: SQL Injection Variable Declaration Evasion | Block | 16 |
| 23.91.112.252 | United States | 147.237.77.74 | law.idf.il | 3808: HTTP: SQL Injection Variable Declaration Evasion | Block | 12 |
| 212.34.12.142 | Jordan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 12 |
| 37.187.150.125 | France | 147.237.77.216 | dover.idf.il | 13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability | Block | 9 |
| 37.187.150.125 | France | 147.237.77.216 | dover.idf.il | 13375: HTTP: Joomla Component JCE BOT for JCE | Block | 9 |
| 212.34.12.144 | Jordan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 79.176.24.230 | Israel | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 212.34.12.177 | Jordan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 46.19.85.112 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 85.25.103.50 | Germany | 147.237.77.74 | law.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 132.64.31.67 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 5 |
| 197.180.87.148 | Kenya | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 37.187.129.166 | France | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 93.120.27.62 | Romania | 147.237.8.46 | e.chinuch.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 198.20.70.114 | United States | 147.237.76.38 | e.e.meitav.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 46.19.85.220 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 84.111.141.136 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 153.31.113.20 | United States | 147.237.76.42 | refuah.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 89.31.57.5 | Italy | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 188.138.9.50 | Germany | 147.237.77.233 | atal.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 85.25.103.50 | Germany | 147.237.8.28 | e.mobile-ks.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 85.25.103.50 | Germany | 147.237.76.147 | chinuch.aka.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 198.20.70.114 | United States | 147.237.76.148 | ggcenter.aka.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 198.20.70.114 | United States | 147.237.72.156 | aman.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 198.20.70.114 | United States | 147.237.0.19 | madim.atal.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 188.138.9.50 | Germany | 147.237.0.17 | m.my-kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 85.25.103.50 | Germany | 147.237.76.176 | test.ncore.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 85.25.103.50 | Germany | 147.237.77.243 | mobile.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 85.25.103.50 | Germany | 147.237.0.33 | idf.il | DVRep_B-N_60_100 | Block | 3 |
| 213.57.178.212 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 188.138.9.50 | Germany | 147.237.76.38 | e.e.meitav.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 87.68.21.99 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 189.82.171.197 | Brazil | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 188.138.9.50 | Germany | 147.237.0.200 | m4u.idf.il | DVRep_B-N_60_100 | Block | 3 |
| 46.19.85.141 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 78.57.164.151 | Lithuania | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 188.138.9.50 | Germany | 147.237.77.170 | maarachot.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 46.19.85.241 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |

Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|------------------|---------------------------------|----------------|------------------------|---|-------|
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 487 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 141 |
| 176.67.108.98 | Palestinian Territory, Occupied | 147.237.0.19 | madim.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 15 |
| 176.67.108.98 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 7 |
| 37.187.150.125 | France | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 6 |
| 85.65.126.88 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 85.64.94.191 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 59.106.108.116 | Japan | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 115.28.48.188 | China | 147.237.0.16 | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 5.29.158.65 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 89.139.173.8 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 176.12.147.82 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.181.114.137 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 2.54.147.105 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 85.250.168.217 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.179.199.16 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 2.54.31.48 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.179.52.141 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.111.65.42 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 178.73.222.121 | Sweden | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP Mambo upload.php access | 2 |
| 79.176.42.164 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.120.17.162 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.108.101.120 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 122.228.207.199 | China | 147.237.0.16 | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 46.19.86.156 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 109.186.8.183 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 93.172.121.231 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 58.170.208.230 | Australia | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sS window 4096 | 2 |
| 5.29.50.126 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 87.69.165.138 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 176.12.136.26 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.180.39.112 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 122.228.207.199 | China | 147.237.76.38 | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 2.54.137.133 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 122.228.207.190 | China | 147.237.8.46 | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 2 |
| 85.65.131.185 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.179.174.50 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 1.93.34.235 | China | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 79.176.127.215 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.109.39.14 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 31.168.88.140 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.19.86.214 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.176.33.27 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.108.84.156 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 122.228.207.199 | China | 147.237.77.205 | prisha.idf.il | ET SCAN Potential SSH Scan | 2 |
| 109.186.154.26 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 77.125.98.7 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 89.248.160.167 | Netherlands | 147.237.8.45 | e.eitan.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 202.115.26.78 | China | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.66 | China | 147.237.77.121 | e.navy.idf.il | ET SCAN Potential SSH Scan | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|------------------|----------------------|----------------|-------------------|---|--|---------------|-------|
| 66.249.73.201 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 1380 |
| 66.249.73.185 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 1357 |
| 66.249.73.193 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 1196 |
| 38.111.147.86 | United States | 147.237.0.34 | tikshuv.idf.il | | drop | drop | 192 |
| 5.22.129.246 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 128 |
| 66.249.81.218 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 106 |
| 66.249.81.212 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 104 |
| 77.125.220.37 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 102 |
| 66.249.81.215 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 84 |
| 41.37.11.91 | Egypt | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 60 |
| 66.249.79.157 | United States | 147.237.72.166 | aka.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 54 |
| 212.199.109.234 | Israel | 147.237.76.42 | refuah.idf.il | First packet isn't SYN | drop | drop | 48 |
| 37.142.4.225 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 48 |
| 109.67.28.232 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 45 |
| 109.66.54.197 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 40 |
| 109.253.158.55 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 40 |
| 109.253.149.4 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 212.150.218.68 | Israel | 147.237.77.243 | mobile.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 134.191.232.71 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 109.66.141.111 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 34 |
| 192.249.47.206 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 34 |
| 157.55.39.119 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 34 |
| 131.137.245.209 | Canada | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 34 |
| 94.252.144.140 | Syrian Arab Republic | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 34 |
| 110.171.187.44 | Thailand | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 34 |
| 77.78.117.7 | Czech Republic | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 32 |
| 12.38.190.9 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 32 |
| 5.22.129.246 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid ACK number | Bad TCP sequence | monitor | 31 |
| 109.64.147.154 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 31 |
| 223.205.168.67 | Thailand | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 176.12.140.43 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 109.253.159.167 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |
| 176.12.151.103 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 28 |
| 109.66.51.168 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 27 |
| 109.65.21.39 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 25 |
| 109.66.159.158 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 25 |
| 110.227.80.121 | India | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 132.76.50.5 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 176.12.151.236 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 24 |
| 46.19.85.56 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid ACK number | Bad TCP sequence | monitor | 22 |
| 188.120.148.232 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 21 |
| 5.28.155.128 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 21 |
| 46.19.85.17 | Israel | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 20 |
| 85.65.157.223 | Israel | 147.237.77.243 | mobile.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 20 |
| 109.253.136.142 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 176.12.142.121 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 109.253.159.252 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 176.12.145.11 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 176.12.137.168 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 199.30.16.188 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|------------------|--------------------|----------------|--------------------|--|---------------|-------|
| 79.181.189.100 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 463 |
| 109.64.30.93 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 109.64.30.93 | Block | 440 |
| 2.54.54.163 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 416 |
| 149.88.3.221 | United States | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 304 |
| 87.69.182.190 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 87.69.182.190 | Block | 292 |
| 5.29.168.207 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 272 |
| 37.26.146.239 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 248 |
| 147.236.34.105 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 209 |
| 2.54.189.18 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 168 |
| 46.19.85.72 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 163 |
| 109.253.147.43 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 156 |
| 2.54.61.34 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 2.54.61.34 | Block | 102 |
| 147.236.34.105 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 147.236.34.105 | Block | 97 |
| 37.142.248.208 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 37.142.248.208 | Block | 91 |
| 46.19.86.177 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.86.177 | Block | 89 |
| 185.32.179.242 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 79 |
| 176.12.147.45 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 75 |
| 109.186.171.188 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 68 |
| 176.12.149.27 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 67 |
| 176.12.144.155 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 66 |
| 66.249.73.193 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.193 | Block | 64 |
| 66.249.73.185 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.185 | Block | 55 |
| 66.249.73.201 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.201 | Block | 53 |
| 85.64.163.22 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/ | Block | 48 |
| 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 | 40 |
| 2.52.20.85 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 23 |
| 77.125.29.101 | Israel | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 77.125.29.101 | Block | 18 |
| 24.12.146.120 | United States | 147.237.72.167 | ishurim.aka.idf.il | Distributed Too Many of the Same Response Code (404) | None | 18 |
| 95.86.108.118 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 18 |
| 79.181.119.184 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 79.181.119.184 | Block | 16 |
| 5.28.162.112 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 5.28.162.112 | Block | 14 |
| 94.159.132.67 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 14 |
| 5.29.119.150 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 13 |
| 68.180.228.117 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 68.180.228.117 | Block | 12 |
| 85.250.217.67 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined | Block | 12 |
| 83.130.111.210 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd | Block | 11 |
| 109.186.1.206 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd | Block | 10 |
| 109.160.216.54 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Distributed Too Many of the Same Response Code (404) | None | 9 |
| 187.114.106.220 | Brazil | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 187.114.106.220 | Block | 9 |
| 187.114.106.220 | Brazil | 147.237.77.216 | dover.idf.il | Suspicious Response Code | Block | 9 |
| 109.64.99.4 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined | Block | 8 |
| 23.95.138.218 | United States | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 8 |
| 84.109.20.101 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 8 |
| 83.130.107.14 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 7 |
| 77.126.215.98 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 7 |
| 208.81.36.90 | United States | 147.237.72.167 | ishurim.aka.idf.il | Distributed Too Many of the Same Response Code (404) | None | 7 |
| 31.44.136.32 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 7 |
| 80.2.81.194 | United Kingdom | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 7 |
| 95.108.158.233 | Russian Federation | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 95.108.158.233 | Block | 7 |
| 5.144.57.239 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd | Block | 6 |