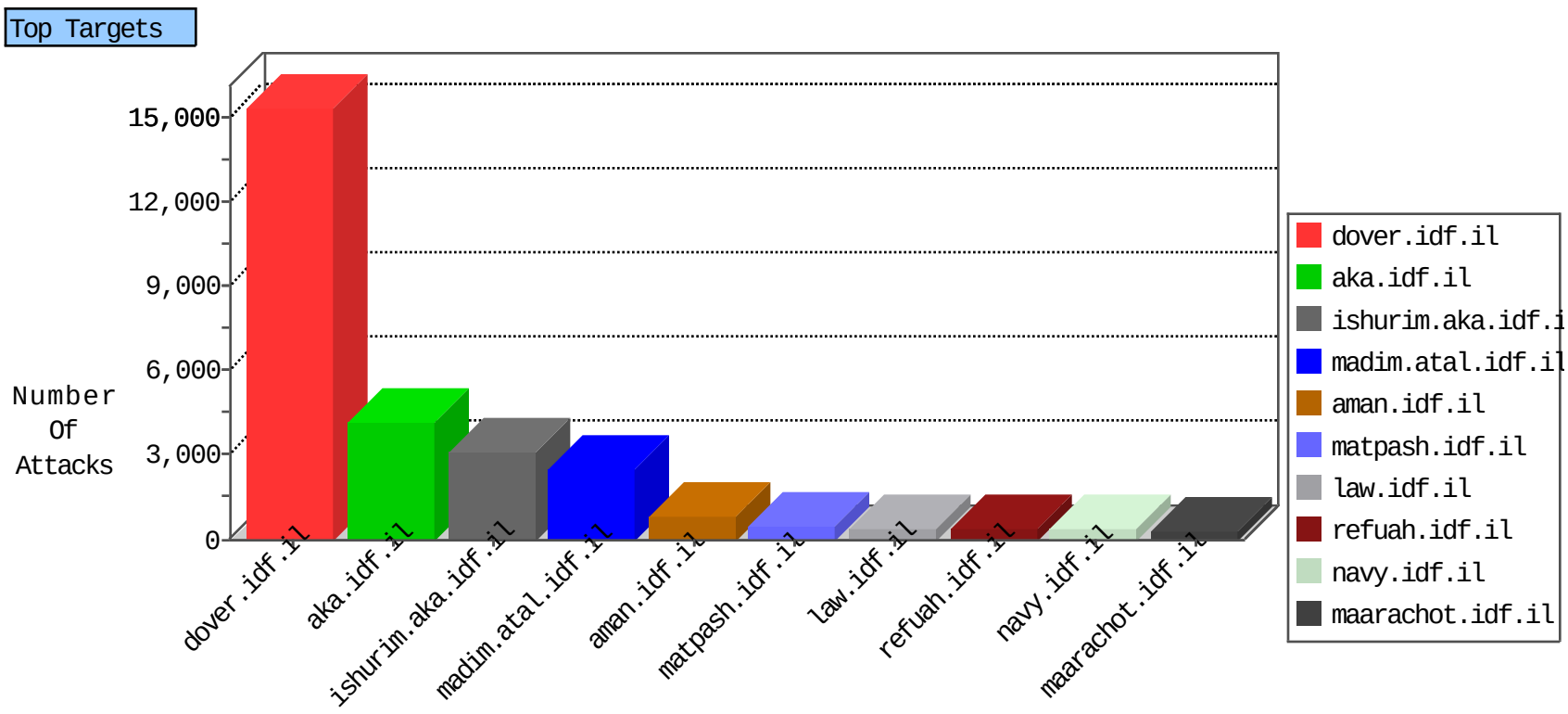
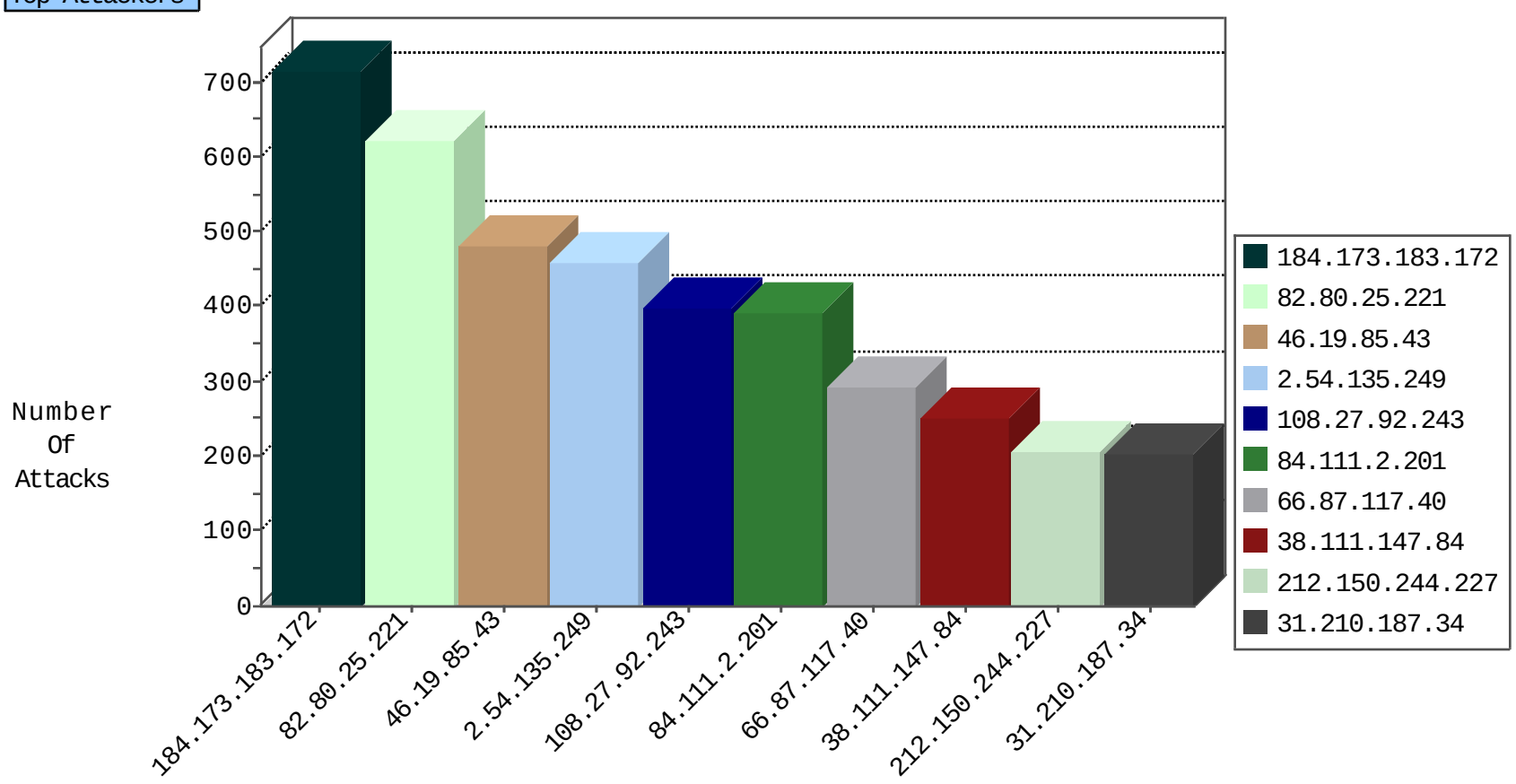
02-15-2015-00:00:00 to 02-16-2015-00:00:00

# IDF Under Attack Daily Report

Top Targets




Top Attackers



02-15-2015-00:00:00 to 02-16-2015-00:00:00

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|---|---|---|---|---|---|---|
| 46.120.17.33 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 1449 |
| 212.199.112.144 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 1094 |
| 79.178.147.53 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 751 |
| 84.108.245.74 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 588 |
| 66.249.64.136 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 537 |
| 5.102.193.48 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 485 |
| 66.249.78.190 | United States | 147.237.77.176 | matpash.idf.il | TCP handshake violation, first packet not syn | drop | 417 |
| 66.249.64.132 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 408 |
| 94.230.86.34 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 347 |
| 82.145.219.166 | Europe | 147.237.77.233 | atal.idf.il | TCP handshake violation, first packet not syn | drop | 336 |
| 46.121.195.172 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-SSL-renegotiation-Cli | dest-reset | 323 |
| 83.130.102.4 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 321 |
| 81.218.241.26 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 270 |
| 84.111.108.61 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 224 |
| 94.159.220.138 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 221 |
| 79.180.103.139 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 211 |
| 80.246.136.174 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-SSL-renegotiation-Cli | dest-reset | 202 |
| 109.186.6.116 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 198 |
| 109.160.242.98 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 178 |
| 84.110.60.205 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 177 |
| 46.19.85.82 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-SSL-renegotiation-Cli | dest-reset | 167 |
| 84.110.60.205 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 177 |
| 46.19.85.82 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-SSL-renegotiation-Cli | dest-reset | 167 |
| 46.116.151.246 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 167 |
| 2.54.21.74 | Israel | 147.237.0.19 | madim.atal.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 160 |
| 83.130.102.16 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 160 |
| 46.19.85.124 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-SSL-renegotiation-Cli | dest-reset | 158 |
| 84.109.4.151 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-SSL-renegotiation-Cli | dest-reset | 146 |
| 94.159.188.32 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 143 |
| 84.229.174.194 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 131 |
| 46.121.245.135 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 127 |
| 109.64.61.157 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 125 |
| 62.219.150.135 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 123 |
| 85.64.76.140 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 113 |
| 149.78.140.224 | United States | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 110 |
| 87.69.64.116 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 110 |
| 84.109.4.151 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 106 |
| 37.142.114.118 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 103 |
| 8.37.227.26 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | Frk_Purple_Con_Limit_Http | drop | 103 |
| 77.126.8.7 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 101 |
| 79.177.41.83 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 101 |
| 213.57.113.237 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 99 |
| 82.102.141.203 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 89 |
| 46.120.174.175 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 88 |
| 85.130.184.246 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 88 |
| 5.29.97.58 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 88 |
| 46.121.195.172 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 87 |
| 85.65.173.59 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 86 |
| 37.26.147.132 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 86 |
| 46.19.85.211 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 85 |
| 149.78.206.198 | United States | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 84 |
| 84.109.110.125 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 83 |

02-15-2015-00:00:00 to 02-16-2015-00:00:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.111.2.201 | Israel | 147.237.72.166 | aka.idf.il | DVRep_P-N_40-59 | Permit | 392 |
| 184.173.183.172 | United States | 147.237.77.176 | matpash.idf.il | DVRep_P-N_40-59 | Permit | 311 |
| 184.173.183.172 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 263 |
| 184.173.183.172 | United States | 147.237.76.86 | navy.idf.il | DVRep_P-N_40-59 | Permit | 142 |
| 128.242.249.12 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 127 |
| 180.76.5.193 | China | 147.237.77.74 | law.idf.il | DVRep_P-N_40-59 | Permit | 65 |
| 46.116.219.74 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 60 |
| 194.114.146.227 | Israel | 147.237.72.166 | aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 24 |
| 194.114.146.227 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 24 |
| 81.218.116.129 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 18 |
| 46.19.85.145 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 8 |
| 46.19.85.239 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 7 |
| 85.25.103.50 | Germany | 147.237.76.198 | e.yohalan.idf.il | DVRep_B-N_60_100 | Block | 6 |
| 192.116.105.90 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 46.19.85.230 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 81.218.251.250 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 46.19.85.214 | Israel | 147.237.77.74 | law.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.19.85.132 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.19.85.103 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.19.85.254 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.19.85.245 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 94.142.245.231 | Netherlands | 147.237.77.216 | dover.idf.il | 2023: HTTP: Cross Site Scripting in GET Request | Block | 5 |
| 72.186.5.22 | United States | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.19.85.57 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 85.25.103.50 | Germany | 147.237.0.33 | idf.il | DVRep_B-N_60_100 | Block | 5 |
| 79.178.216.62 | Israel | 147.237.77.74 | law.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 5 |
| 198.20.70.114 | United States | 147.237.77.61 | e.cogat.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 46.19.85.220 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.19.85.39 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.223 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 85.25.103.50 | Germany | 147.237.77.205 | prisha.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 46.19.85.235 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.22 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 198.20.70.114 | United States | 147.237.76.38 | e.e.meitav.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 14.14.149.22 | Japan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 79.180.11.168 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.168 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.237 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.158 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.136 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 85.25.103.50 | Germany | 147.237.72.14 | dover.idf.il(old) | DVRep_B-N_60_100 | Block | 4 |
| 46.19.85.246 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.207 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 207.232.27.5 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 84.110.213.162 | Israel | 147.237.72.167 | ishurim.aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.121 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.242 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 37.142.166.223 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 46.19.85.154 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 85.64.202.2 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |

02-15-2015-00:00:00 to 02-16-2015-00:00:00

## 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 | 622 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 130 |
| 91.185.202.85 | Slovenia | 147.237.72.166 | aka.idf.il | Tehila - Perl LWP with fake user agent | 48 |
| 97.74.24.210 | United States | 147.237.72.166 | aka.idf.il | Tehila - Perl LWP with fake user agent | 28 |
| 31.210.187.34 | Israel | 147.237.72.167 | ishurim.aka.idf.il | ET SCAN Possible SSL Brute Force attack or Site Crawl | 21 |
| 95.86.75.194 | Israel | 147.237.77.216 | dover.idf.il | POLICY-OTHER script tag in URI - likely cross-site scripting attempt | 19 |
| 46.120.198.230 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 8 |
| 59.106.108.116 | Japan | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 7 |
| 85.64.94.191 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 5 |
| 62.90.202.62 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 4 |
| 46.20.222.179 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | ET SCAN NMAP -sA (2) | 3 |
| 61.240.144.67 | China | 147.237.76.176 | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 66.249.75.136 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 2.54.187.191 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.116.94.88 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 37.142.39.194 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 80.246.130.115 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 2.54.164.189 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.180.198.248 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 176.12.151.209 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 89.248.162.228 | Netherlands | 147.237.0.16 | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 61.240.144.67 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 85.65.32.11 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 190.81.111.67 | Peru | 147.237.72.217 | e.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 82.102.141.223 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 2.54.9.40 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 85.64.14.26 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 66.249.93.160 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 149.78.213.9 | United States | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 5.29.128.172 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.121.140.102 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.228.128.67 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 212.129.52.90 | France | 147.237.0.35 | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 66.249.78.134 | United States | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.181.71.90 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.111.40.186 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 2.54.190.91 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 85.65.247.147 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.19.85.31 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.116.121.48 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 80.246.133.80 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 213.151.59.151 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.181.13.253 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.116.60.71 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 95.86.127.75 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.108.249.23 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 93.172.49.19 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 213.8.98.193 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.178.166.150 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.19.86.215 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |

02-15-2015-00:00:00 to 02-16-2015-00:00:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.87.117.40 | United States | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 293 |
| 108.27.92.243 | United States | 147.237.77.170 | maarachot.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 218 |
| 108.27.92.243 | United States | 147.237.77.216 | dover.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 163 |
| 31.210.187.34 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid ACK number | Bad TCP sequence | monitor | 96 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 94 |
| 85.250.175.164 | Israel | 147.237.72.166 | aka.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 90 |
| 46.116.97.201 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 72 |
| 31.210.187.34 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid ACK number | Bad TCP sequence | alert | 69 |
| 46.99.41.149 | Albania | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 68 |
| 66.249.81.215 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 62 |
| 176.12.136.86 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 60 |
| 2.54.51.42 | Israel | 147.237.76.42 | refuah.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 60 |
| 176.12.156.29 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 58 |
| 79.180.149.178 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 56 |
| 79.177.179.201 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 54 |
| 79.180.125.55 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 48 |
| 109.253.137.216 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 48 |
| 134.191.232.71 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 46 |
| 213.8.96.180 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 44 |
| 75.159.98.83 | Canada | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 44 |
| 134.191.232.69 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 42 |
| 176.12.142.15 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 42 |
| 109.253.145.86 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 42 |
| 109.253.140.27 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 42 |
| 80.179.9.104 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 42 |
| 176.12.136.200 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 42 |
| 79.178.53.138 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 41 |
| 109.253.157.55 | Israel | 147.237.77.234 | halag.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 40 |
| 176.12.139.148 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 38 |
| 176.12.148.226 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 38 |
| 176.12.141.115 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 38 |
| 176.12.149.91 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 38 |
| 190.31.111.43 | Argentina | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 37 |
| 109.253.141.103 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 109.226.18.249 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 109.253.128.75 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 109.253.158.217 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 109.253.158.39 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 84.95.251.243 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 134.191.232.70 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 34 |
| 176.12.156.4 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 34 |
| 109.253.158.87 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 34 |
| 2.54.18.100 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 34 |
| 109.253.133.248 | Israel | 147.237.77.216 | dover.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 34 |
| 80.178.184.3 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 33 |
| 85.250.174.96 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 32 |
| 213.8.96.180 | Israel | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 32 |
| 176.12.136.136 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 32 |
| 176.12.146.157 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 32 |
| 109.253.128.200 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 30 |

02-15-2015-00:00:00 to 02-16-2015-00:00:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.43 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 46.19.85.43 | Block | 472 |
| 2.54.135.249 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 400 |
| 38.111.147.84 | United States | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 38.111.147.84 | Block | 249 |
| 212.150.244.227 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 212.150.244.227 | Block | 205 |
| 2.54.21.74 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 143 |
| 176.12.147.239 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 126 |
| 176.12.139.6 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 112 |
| 46.210.236.195 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 46.210.236.195 | Block | 98 |
| 2.54.163.162 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 95 |
| 46.19.85.94 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 90 |
| 80.246.136.119 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 76 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.166 | Block | 76 |
| 46.19.86.7 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 67 |
| 2.54.135.249 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 2.54.135.249 | Block | 57 |
| 176.12.149.179 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 54 |
| 97.74.24.210 | United States | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 48 |
| 91.185.202.85 | Slovenia | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 48 |
| 46.19.85.249 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 46 |
| 46.19.85.19 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 45 |
| 46.19.86.106 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 42 |
| 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 | 31 |
| 46.19.86.76 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 46.19.86.76 | Block | 30 |
| 176.12.156.65 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 29 |
| 46.121.37.15 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 28 |
| 109.253.156.167 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 27 |
| 185.32.176.212 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 27 |
| 176.12.156.243 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 24 |
| 97.74.24.210 | United States | 147.237.72.166 | aka.idf.il | Multiple Admin Blocking from 97.74.24.210 | Block | 23 |
| 91.185.202.85 | Slovenia | 147.237.72.166 | aka.idf.il | Multiple Admin Blocking from 91.185.202.85 | Block | 23 |
| 176.12.148.92 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 23 |
| 176.12.149.245 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 20 |
| 46.19.86.108 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 20 |
| 85.130.249.3 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 20 |
| 95.86.116.122 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 19 |
| 95.86.75.194 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 95.86.75.194 | Block | 18 |
| 89.139.8.224 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 18 |
| 194.90.186.193 | Israel | 147.237.72.166 | aka.idf.il | Too Many of the Same Response Code (404) in Session from 194.90.186.193 | Block | 17 |
| 46.19.86.212 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 17 |
| 58.20.54.248 | China | 147.237.0.34 | tikshuv.idf.il | Multiple Illegal Byte Code Character in Method from 58.20.54.248 | Block | 17 |
| 58.20.54.248 | China | 147.237.0.34 | tikshuv.idf.il | Distributed NULL Character in Method | Block | 17 |
| 109.67.141.248 | Israel | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 109.67.141.248 | Block | 16 |
| 79.182.101.116 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 79.182.101.116 | Block | 16 |
| 85.250.215.149 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/sip_storage/files/1/71101.pdfâ€? | Block | 16 |
| 212.116.169.152 | 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 | 15 |
| 5.29.127.37 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 15 |
| 109.253.144.131 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 15 |
| 68.180.228.117 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 68.180.228.117 | Block | 14 |
| 80.246.136.74 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 14 |
| 89.139.56.146 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/modiin/undefined | Block | 13 |
| 85.130.206.34 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 13 |

02-15-2015-00:00:00 to 02-16-2015-00:00:00