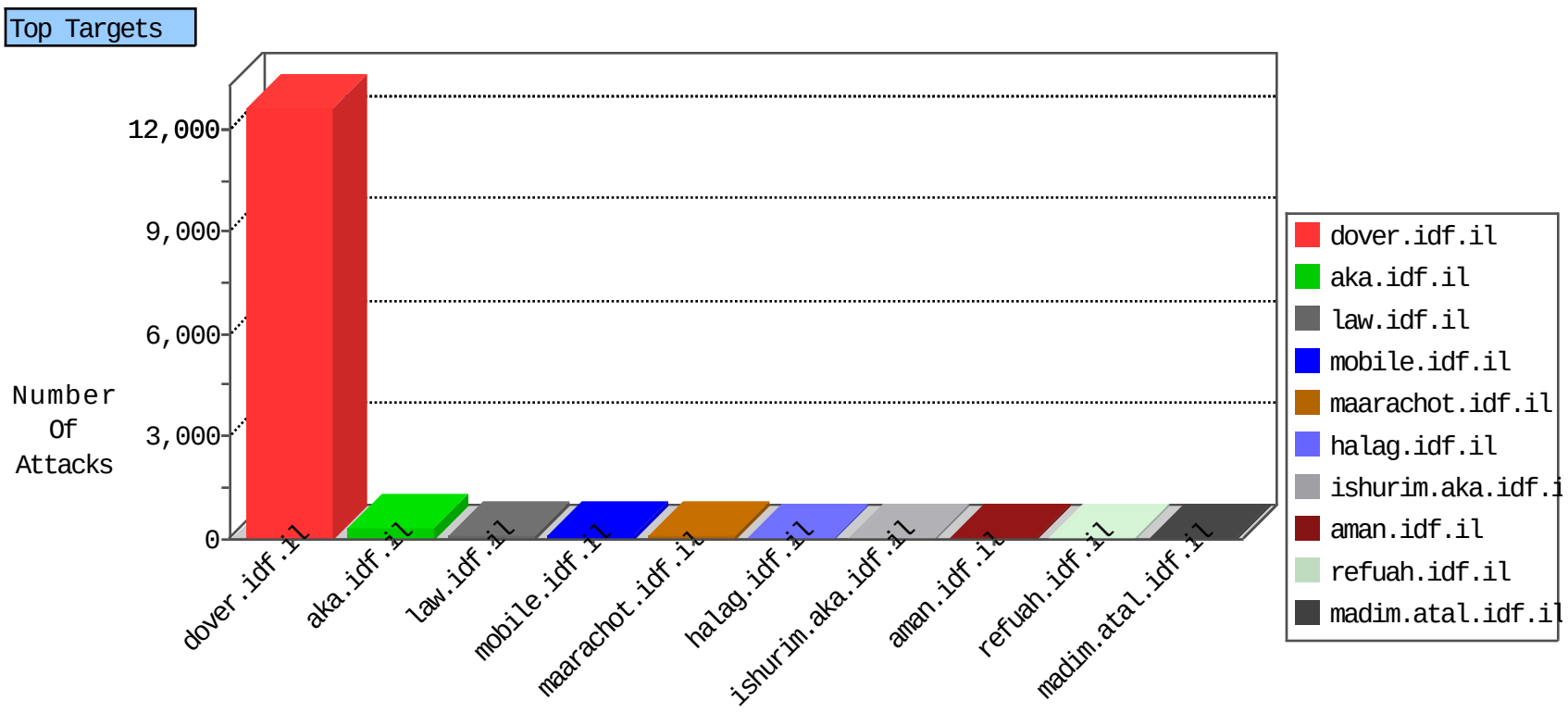
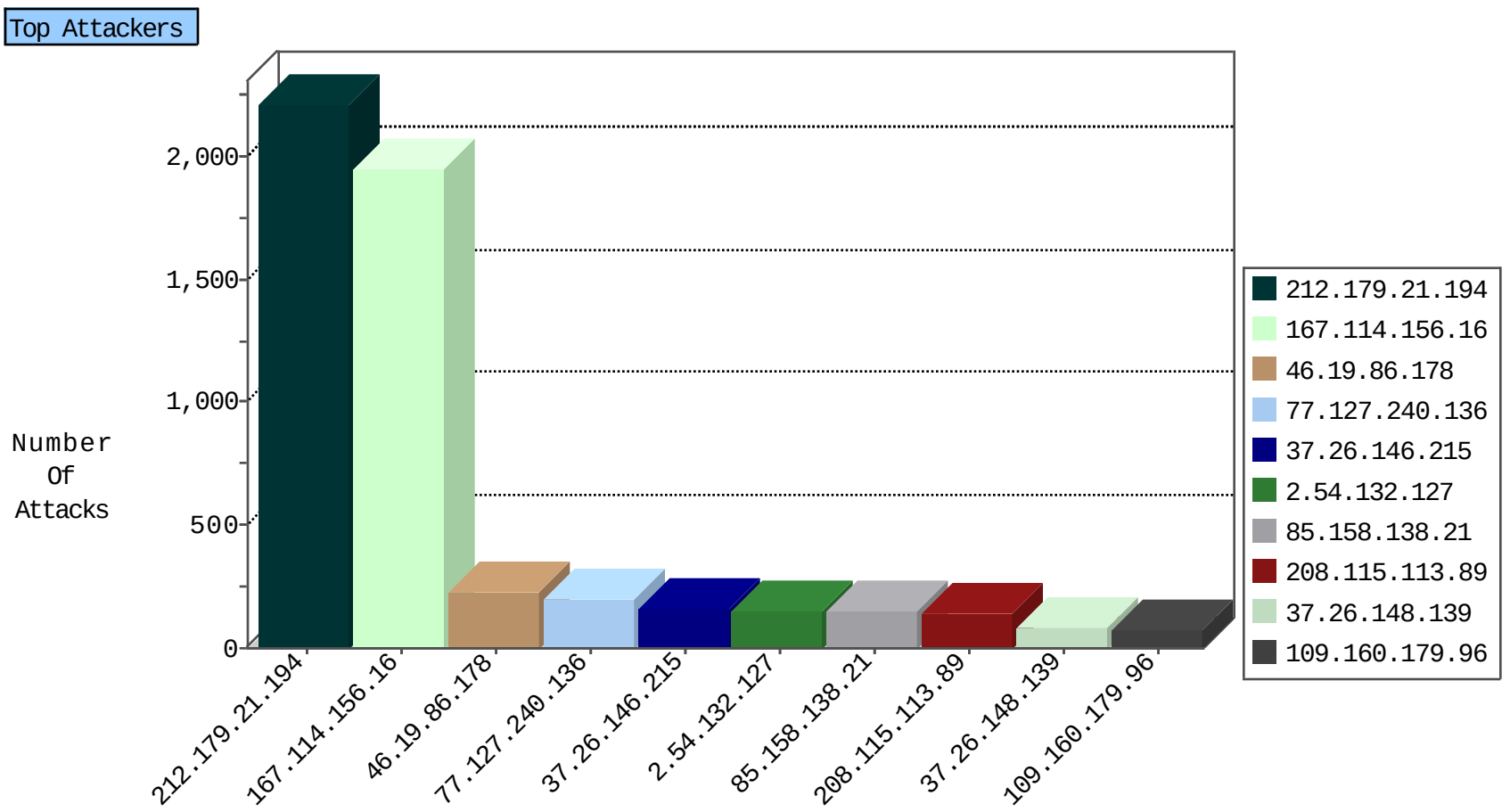
11-04-2015-12:04:06 to 11-04-2015-13:04:06

# IDF Under Attack Daily Report

Top Targets




Top Attackers



11-04-2015-12:04:06 to 11-04-2015-13:04:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.79.43 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 8193 |
| 66.249.69.34 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 7453 |
| 66.249.67.79 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 4627 |
| 66.249.67.67 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 4412 |
| 136.0.99.10 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3737 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3169 |
| 66.249.67.73 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 2472 |
| 66.249.79.45 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 2087 |
| 64.233.172.171 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1881 |
| 66.249.93.203 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 1584 |
| 66.249.67.6 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 865 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 783 |
| 185.7.121.0 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 287 |
| 0.0.0.0 |  | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 268 |
| 66.249.67.202 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 198 |
| 66.249.79.41 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 82 |
| 37.26.146.215 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 59 |
| 46.19.86.231 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 53 |
| 37.26.147.150 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 31 |
| 2.54.18.159 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 24 |
| 84.108.222.42 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 12 |
| 46.19.86.199 | 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 | 10 |
| 84.111.36.127 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 10 |
| 81.101.122.99 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-MISC-Slowloris-DOS-Var1 | dest-reset | 8 |
| 82.145.209.17 | Europe | 147.237.76.42 | refuah.idf.il | Block_Ip_Web_In | drop | 7 |
| 192.118.11.120 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 6 |
| 199.203.176.50 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 62.90.163.78 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 54.244.22.103 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 2.54.57.188 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 79.180.177.187 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 91.221.58.25 | Germany | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 80.246.136.237 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 192.118.11.120 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 93.172.0.25 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 66.249.69.26 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4 |
| 46.116.200.75 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 80.246.136.235 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 192.116.94.67 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 176.13.4.208 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 81.218.206.82 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 46.19.86.198 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 146.185.57.7 | Israel | 147.237.72.156 | aman.idf.il | Block_Udp_All_Nets | drop | 3 |
| 80.246.137.51 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 2.54.14.159 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 66.249.67.122 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 165.228.200.225 | Australia | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |

11-04-2015-12:04:06 to 11-04-2015-13:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 217.12.204.163 | Ukraine | 147.237.72.166 | aka.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 1 |
| 31.154.91.48 | Israel | 147.237.72.166 | aka.idf.il | C1000098: Block - dns poisoning | Block | 1 |
| 58.180.228.110 | Korea, Republic of | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 1 |

11-04-2015-12:04:06 to 11-04-2015-13:04:06

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 |
| 85.64.120.24 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.80.126.182 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.28.166.23 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.138.9.51 | 147.237.72.14 | Germany | dover.idf.il(old) | ET SCAN NMAP -sS window 1024 | 1 |
| 128.139.16.180 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.108.222.42 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.29.202.206 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.120.151.122 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

11-04-2015-12:04:06 to 11-04-2015-13:04:06

## 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 | 2207 |
| 46.19.86.178 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 219 |
| 77.127.240.136 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 200 |
| 37.26.146.215 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 153 |
| 2.54.132.127 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 149 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 143 |
| 85.158.138.21 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 141 |
| 37.26.148.139 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 84 |
| 37.76.199.227 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 69 |
| 46.19.86.199 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 50 |
| 85.158.139.101 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 49 |
| 62.219.99.130 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 48 |
| 109.160.179.96 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 46 |
| 66.249.93.192 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 44 |
| 119.224.26.199 | New Zealand | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 44 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 44 |
| 213.8.90.250 | Israel | 147.237.77.243 | mobile.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 39 |
| 192.114.23.209 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 192.114.105.254 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 46.19.86.196 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 35 |
| 176.106.227.26 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 32 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 32 |
| 193.188.136.30 | Lebanon | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 31 |
| 66.249.69.26 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 31 |
| 136.0.99.10 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 165.228.200.225 | Australia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 81.218.251.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 29 |
| 37.26.147.150 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 192.114.23.210 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 79.179.135.119 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 46.19.86.20 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 84.109.81.118 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 185.35.48.1 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 46.19.86.90 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 25 |
| 66.249.69.42 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 25 |
| 81.218.101.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 31.168.13.78 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 46.19.85.163 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 109.160.179.96 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 192.114.23.208 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 109.200.30.154 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 79.176.20.197 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 79.176.24.185 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 82.166.22.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 5.29.2.199 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 185.120.126.63 |  | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 192.118.11.120 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 31.168.100.81 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.157 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unknown HTTP Request Method from 46.19.86.157 | Block | 16 |
| 40.77.167.90 | United States | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 6 |
| 176.13.4.208 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 4 |
| 212.179.5.3 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 212.179.5.3 | Block | 3 |
| 77.127.150.6 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 3 |
| 94.179.168.186 | Ukraine | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg | Block | 3 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 3 |
| 46.116.171.46 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.201 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.182.141.19 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.211 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.54.148.187 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 31.168.18.224 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 208.115.113.88 | Block | 2 |
| 46.98.73.71 | Ukraine | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser | Block | 2 |
| 46.19.85.225 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.14.221 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 2 |
| 46.19.86.4 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.169 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.54.170.93 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 212.117.140.158 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il | Block | 2 |
| 176.12.147.191 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.116.171.46 | Israel | 147.237.77.233 | atal.idf.il | Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx | Block | 2 |
| 66.249.67.13 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 5.29.107.44 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 192.116.190.74 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 46.19.86.251 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 141.212.122.64 | United States | 147.237.72.156 | aman.idf.il | Malformed URL proxytest.zmap.io:80 | Block | 1 |
| 66.249.67.190 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/1091-he/patzar.aspx | Block | 1 |
| 46.19.85.18 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.65.80 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm | Block | 1 |
| 46.19.86.157 | Israel | 147.237.72.166 | aka.idf.il | Unknown HTTP Request Method undefined in URL www.aka.idf.il/main/giyus/api/api/professiondescription/:id | Block | 1 |
| 81.218.116.129 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/ajax/pages/fan_status.php | Block | 1 |
| 46.19.85.177 | Israel | 147.237.77.216 | dover.idf.il | Illegal HTTP Version __atuvc=1%7C44; __atuvs=5639de15dcd6e8fe000 | Block | 1 |
| 213.8.90.250 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/sip_storage | 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 |
| 2.52.134.66 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 141.212.122.64 | United States | 147.237.76.31 | nakchal.idf.il | Distributed Malformed URL | Block | 1 |
| 79.182.147.172 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/aman | Block | 1 |
| 46.19.85.118 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 212.179.5.3 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/ | Block | 1 |
| 66.249.67.204 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/336-he/patzar.aspx | Block | 1 |
| 2.54.157.117 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.65.93 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 46.19.86.223 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 46.19.85.177 | Israel | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method bbqqqqqqq_bf2026bb; in URL asp.net_sessionid=wwdhaaqopetazai4gjyndjbe | Block | 1 |
| 217.194.206.200 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/main/giyus/ | Block | 1 |
| 79.177.145.189 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/ | Block | 1 |
| 66.249.67.65 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 37.26.146.232 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 1 |