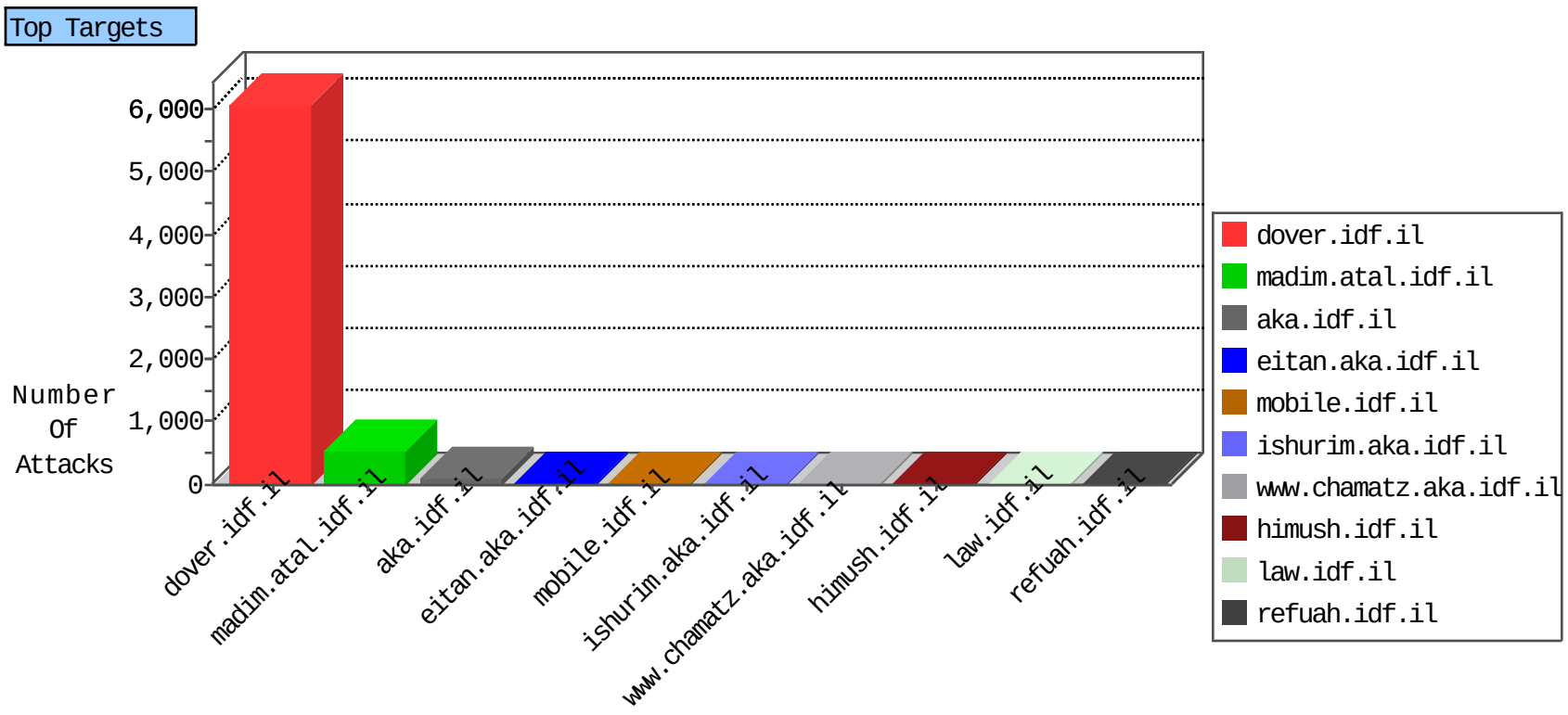
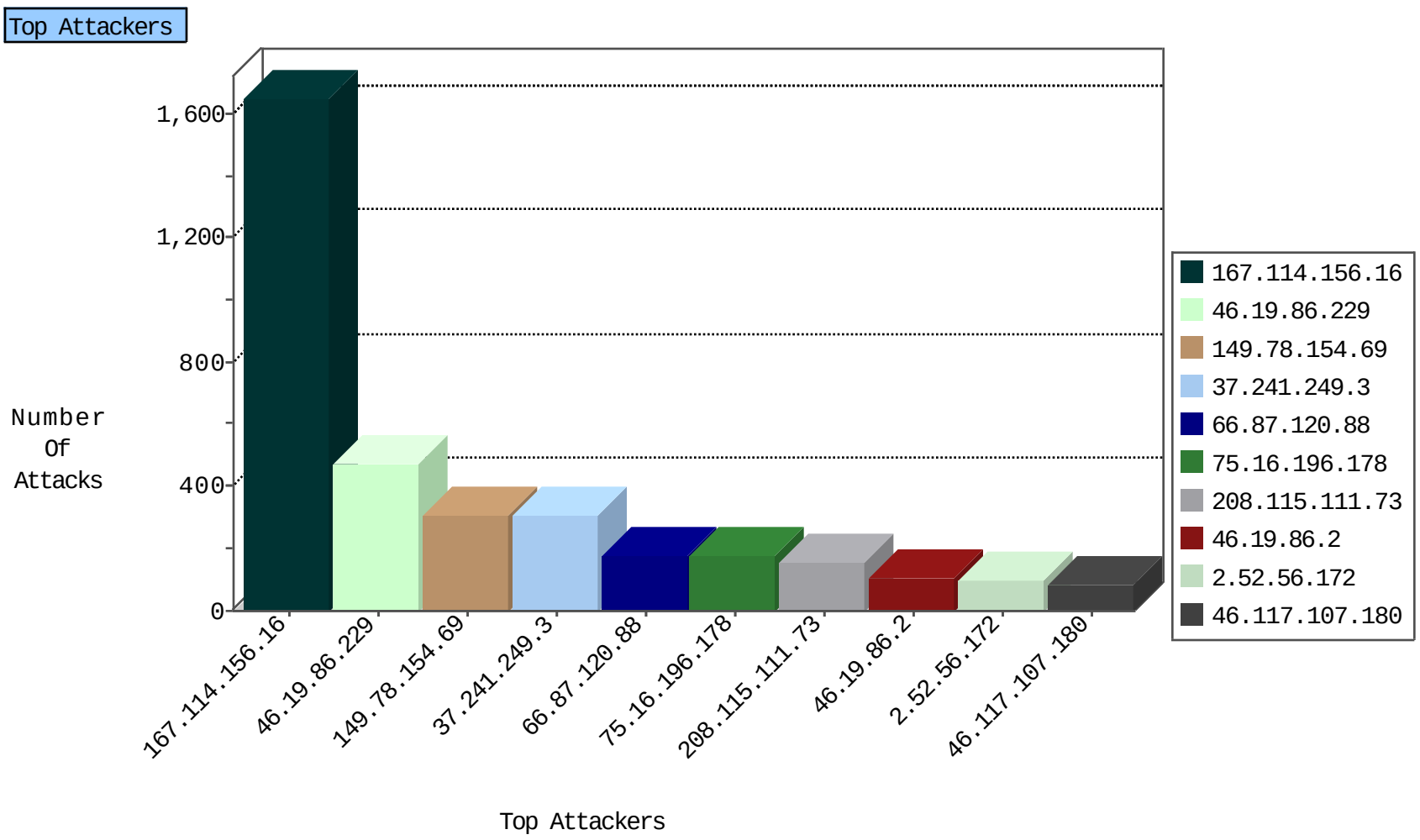
11-08-2015-00:04:08 to 11-08-2015-01:04:08

# IDF Under Attack
# Daily Report



11-08-2015-00:04:08 to 11-08-2015-01:04:08

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 2769 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2533 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 100 |
| 81.218.234.122 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 53 |
| 95.86.108.26 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 36 |
| 109.64.56.34 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 35 |
| 46.121.109.3 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 28 |
| 46.19.85.106 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 26 |
| 5.29.139.184 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 25 |
| 85.65.161.27 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 12 |
| 37.26.149.136 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 10 |
| 79.183.101.138 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 72.219.145.27 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 7 |
| 85.3.107.65 | Switzerland | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 77.125.163.144 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 46.19.86.165 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 76.111.69.2 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 109.67.183.195 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 109.64.15.57 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 82.132.230.81 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 5.22.129.230 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 87.69.94.218 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 149.78.30.224 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 37.241.249.3 | Saudi Arabia | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 79.179.175.179 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 5.29.92.80 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 62.219.254.22 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 46.19.85.106 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 3 |
| 37.142.211.223 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 79.176.27.25 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 84.228.197.215 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 185.32.179.88 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 87.69.165.146 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 176.12.137.253 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 2.52.56.172 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 10.0.0.1 | | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 176.12.149.94 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 109.67.183.195 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 167.114.82.227 | Canada | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 115.231.222.40 | China | 147.237.76.196 | e.sviva.idf.il | JLM_Under_Attack_Con_Http | drop | 1 |
| 37.60.44.78 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 109.67.54.163 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 66.249.65.224 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |

11-08-2015-00:04:08 to 11-08-2015-01:04:08

## Top Attackers In IPS

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

11-08-2015-00:04:08 to 11-08-2015-01:04:08

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 | 10 |
| 31.44.128.201 | 147.237.76.30 | Israel | himush.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 4 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 176.13.13.44 | 147.237.77.216 | Israel | dover.idf.il | INDICATOR-SCAN myscan | 2 |
| 176.13.13.44 | 147.237.77.216 | Israel | dover.idf.il | GPL SCAN myscan | 2 |
| 104.128.144.131 | 147.237.0.16 | Canada | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 76.111.69.2 | 147.237.77.216 | United States | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 222.186.34.238 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 46.151.52.8 | 147.237.72.217 | Ukraine | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.186.34.238 | 147.237.76.86 | China | navy.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 222.186.34.238 | 147.237.0.33 | China | idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 198.20.69.74 | 147.237.77.19 | United States | law-forum.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 193.105.134.220 | 147.237.77.243 | Sweden | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 167.114.156.16 | 147.237.77.216 | Canada | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 104.128.144.131 | 147.237.0.16 | Canada | my-kosher-kravi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 66.249.67.240 | 147.237.72.166 | United States | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 222.186.34.238 | 147.237.76.147 | China | chinuch.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 222.186.34.238 | 147.237.76.39 | China | mobile.meitav.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 210.7.18.87 | 147.237.76.30 | Fiji | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 188.138.9.51 | 147.237.0.33 | Germany | idf.il | ET SCAN NMAP -sS window 1024 | 1 |

11-08-2015-00:04:08 to 11-08-2015-01:04:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 305 |
| 37.241.249.3 | Saudi Arabia | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 303 |
| 66.87.120.88 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 180 |
| 75.16.196.178 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 176 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 154 |
| 46.19.86.2 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 108 |
| 2.52.56.172 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 93 |
| 46.117.107.180 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 80 |
| 41.248.58.68 | Morocco | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 77 |
| 108.59.253.71 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 74 |
| 99.58.197.15 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 73 |
| 72.219.145.27 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 64 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 58 |
| 46.120.116.86 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 53 |
| 99.224.238.30 | Canada | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 50 |
| 87.69.181.217 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 49 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 47 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 45 |
| 109.26.62.41 | France | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 45 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 44 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 44 |
| 84.108.16.62 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 43 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 42 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 38 |
| 41.90.249.241 | Kenya | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 37 |
| 131.253.25.203 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 33 |
| 79.114.205.60 | Romania | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 32 |
| 66.249.65.231 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 32 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 30 |
| 186.204.246.30 | Brazil | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 27 |
| 83.60.119.223 | Spain | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 27 |
| 134.191.232.70 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 26 |
| 66.249.65.238 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 26 |
| 40.77.167.67 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 26 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 25 |
| 66.249.65.224 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 149.78.255.141 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 23 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 22 |
| 66.249.65.238 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 22 |
| 37.142.250.24 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 22 |
| 82.132.230.81 | United Kingdom | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 21 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 21 |
| 79.180.127.76 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 21 |
| 157.55.39.1 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 20 |
| 46.60.46.103 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 20 |
| 79.181.5.146 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 20 |
| 5.102.254.30 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 20 |
| 77.125.108.210 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 19 |
| 93.173.161.26 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 19 |
| 157.55.39.31 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 19 |

11-08-2015-00:04:08 to 11-08-2015-01:04:08

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.229 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 261 |
| 46.19.86.229 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 151 |
| 46.19.86.229 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 46 |
| 2.54.176.187 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 26 |
| 79.176.0.41 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 16 |
| 46.117.167.240 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 2.52.36.227 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 46.121.109.3 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.54.170.23 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 95.86.68.10 | Israel | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 95.86.68.10 | Block | 1 |
| 66.249.67.122 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 46.19.86.229 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 1 |
| 157.55.39.7 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/894-he | Block | 1 |
| 66.249.69.49 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/ | Block | 1 |
| 66.249.64.56 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8867-he/refuah.aspx | Block | 1 |
| 95.86.117.26 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx | None | 1 |
| 66.249.67.147 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 195.154.227.118 | France | 147.237.77.216 | dover.idf.il | Illegal HTTP Version HTTP/ | Block | 1 |
| 2.52.16.177 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.64.108 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/robots.txt | Block | 1 |
| 104.167.101.113 | Canada | 147.237.72.167 | ishurim.aka.idf.il | Unauthorized URL Access to 147.237.72.167/xmlrpc.php | Block | 1 |
| 66.249.67.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 198.20.69.74 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 66.249.64.118 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/sip_storage/files/6/286.pdf | Block | 1 |
| 142.54.174.66 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.cloud.ph/ | Block | 1 |
| 66.249.67.240 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 62.219.193.62 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/ | Block | 1 |
| 2.54.36.230 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 85.64.113.88 | Israel | 147.237.77.216 | dover.idf.il | NULL Character in Method | Block | 1 |
| 66.249.67.13 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/family | Block | 1 |
| 151.80.31.136 | Italy | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-9064-he/refuah.aspx | Block | 1 |
| 66.249.69.41 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/robots.txt | Block | 1 |
| 66.249.64.51 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3365.jpg | Block | 1 |

11-08-2015-00:04:08 to 11-08-2015-01:04:08