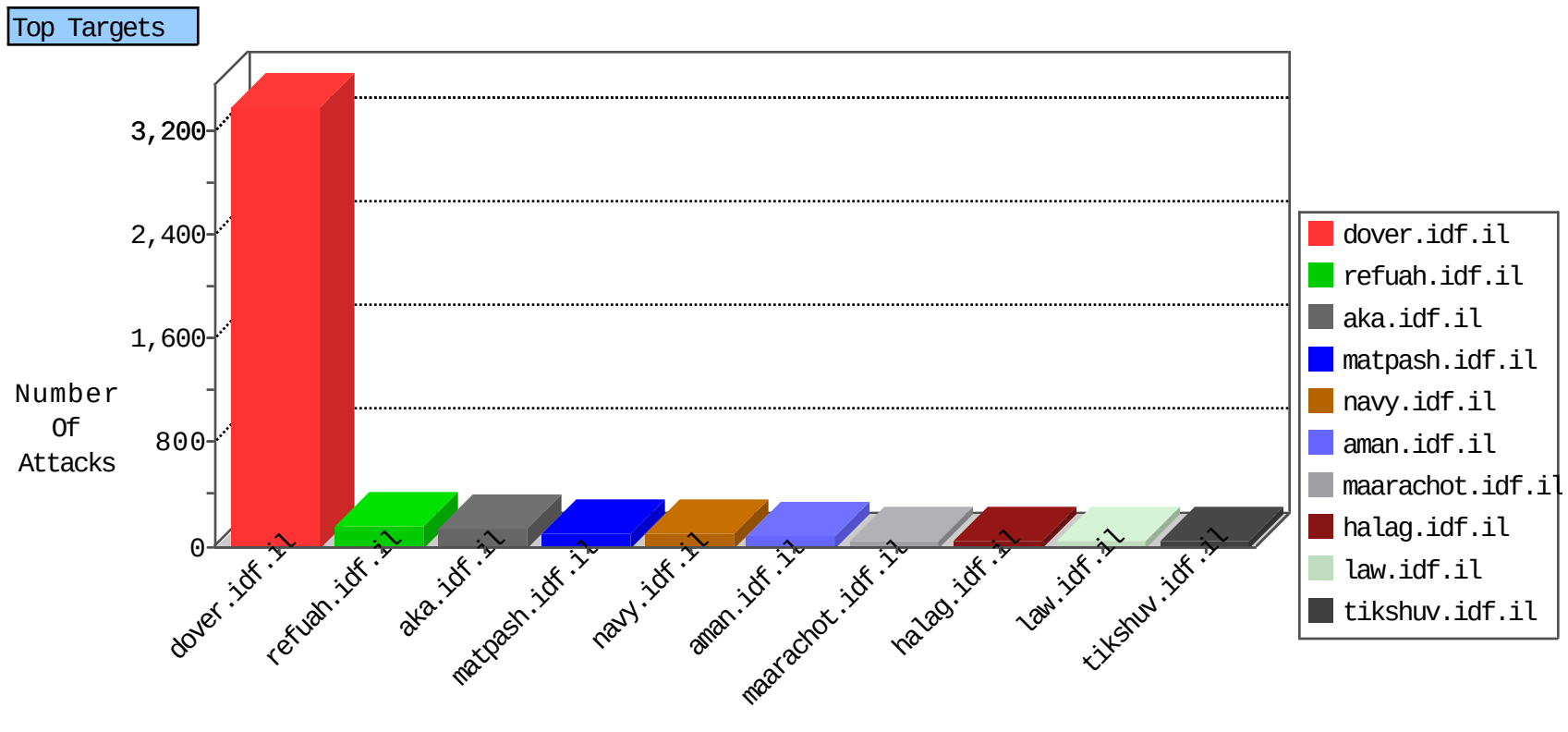
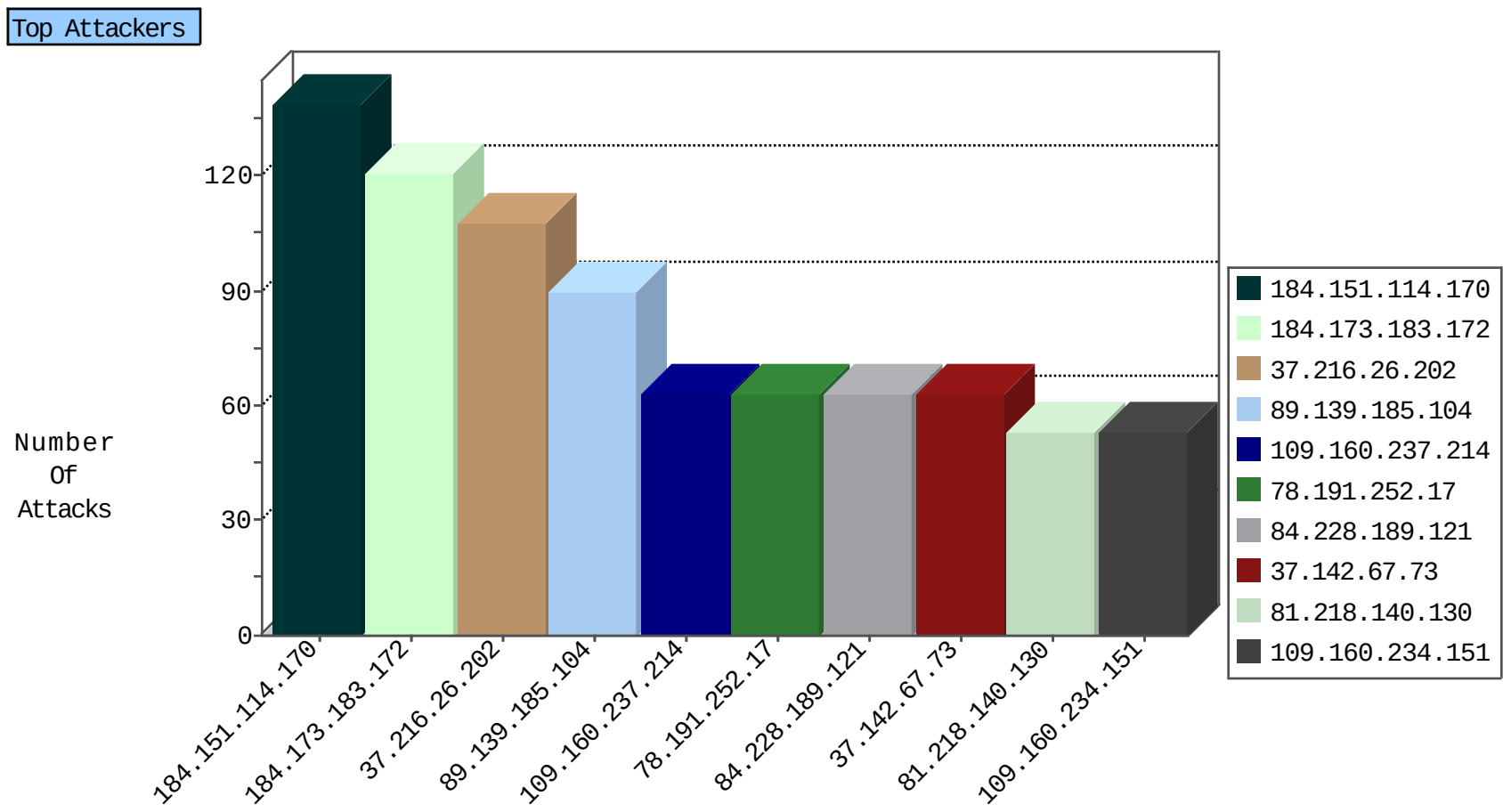
04-09-2015-21:03:06 to 04-09-2015-22:03:06

# IDF Under Attack
# 04-09-2015-21:03:06

Top Targets




Top Attackers



04-09-2015-21:03:06 to 04-09-2015-22:03:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Web Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 220.181.108.163 | China | 147.237.76.86 | navy.idf.il | TCP handshake violation, first packet not syn | drop | 6439 |
| 41.33.231.86 | Egypt | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1526 |
| 220.181.108.118 | China | 147.237.76.42 | refuah.idf.il | TCP handshake violation, first packet not syn | drop | 448 |
| 184.151.114.170 | Canada | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 187 |
| 213.8.240.168 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 147 |
| 46.19.86.100 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 144 |
| 84.108.33.230 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 99 |
| 84.94.189.118 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 77 |
| 66.249.78.167 | United States | 147.237.76.42 | refuah.idf.il | Block_Ip_Web_In | drop | 30 |
| 66.249.78.21 | United States | 147.237.76.42 | refuah.idf.il | Block_Ip_Web_In | drop | 28 |
| 66.249.78.190 | United States | 147.237.77.176 | matpash.idf.il | Block_Ip_Web_In | drop | 27 |
| 66.249.78.14 | United States | 147.237.76.42 | refuah.idf.il | Block_Ip_Web_In | drop | 23 |
| 66.249.78.104 | United States | 147.237.77.170 | maarachot.idf.il | Block_Ip_Web_In | drop | 21 |
| 66.249.67.30 | United States | 147.237.76.86 | navy.idf.il | Block_Ip_Web_In | drop | 21 |
| 66.249.75.96 | United States | 147.237.77.234 | halag.idf.il | Block_Ip_Web_In | drop | 20 |
| 66.249.78.82 | United States | 147.237.77.74 | law.idf.il | Block_Ip_Web_In | drop | 19 |
| 66.249.75.112 | United States | 147.237.77.234 | halag.idf.il | Block_Ip_Web_In | drop | 19 |
| 66.249.67.22 | United States | 147.237.76.86 | navy.idf.il | Block_Ip_Web_In | drop | 19 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 18 |
| 66.249.78.28 | United States | 147.237.76.42 | refuah.idf.il | Block_Ip_Web_In | drop | 18 |
| 66.249.78.204 | United States | 147.237.77.176 | matpash.idf.il | Block_Ip_Web_In | drop | 17 |
| 66.249.78.45 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Block_Ip_Web_In | drop | 17 |
| 66.249.78.197 | United States | 147.237.77.176 | matpash.idf.il | Block_Ip_Web_In | drop | 16 |
| 66.249.78.160 | United States | 147.237.76.42 | refuah.idf.il | Block_Ip_Web_In | drop | 16 |
| 66.249.78.97 | United States | 147.237.77.170 | maarachot.idf.il | Block_Ip_Web_In | drop | 13 |
| 66.249.78.89 | United States | 147.237.77.74 | law.idf.il | Block_Ip_Web_In | drop | 13 |
| 66.249.67.147 | United States | 147.237.76.86 | navy.idf.il | Block_Ip_Web_In | drop | 12 |
| 66.249.78.38 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Block_Ip_Web_In | drop | 12 |
| 66.249.78.174 | United States | 147.237.76.42 | refuah.idf.il | Block_Ip_Web_In | drop | 11 |
| 66.249.75.104 | United States | 147.237.77.234 | halag.idf.il | Block_Ip_Web_In | drop | 11 |
| 66.249.78.74 | United States | 147.237.77.233 | atal.idf.il | Block_Ip_Web_In | drop | 11 |
| 66.249.78.111 | United States | 147.237.77.170 | maarachot.idf.il | Block_Ip_Web_In | drop | 11 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 10 |
| 66.249.67.14 | United States | 147.237.76.86 | navy.idf.il | Block_Ip_Web_In | drop | 9 |
| 66.249.64.63 | United States | 147.237.76.31 | nakchal.idf.il | Block_Ip_Web_In | drop | 9 |
| 66.249.78.31 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Block_Ip_Web_In | drop | 8 |
| 66.249.78.127 | United States | 147.237.0.34 | tikshuv.idf.il | Block_Ip_Web_In | drop | 8 |
| 66.249.78.230 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | Block_Ip_Web_In | drop | 8 |
| 66.249.75.117 | United States | 147.237.72.166 | aka.idf.il | Block_Ip_Web_In | drop | 8 |
| 66.249.64.151 | United States | 147.237.72.156 | aman.idf.il | Block_Ip_Web_In | drop | 8 |
| 66.249.67.153 | United States | 147.237.0.15 | kosher-kravi.idf.il | Block_Ip_Web_In | drop | 8 |
| 66.249.67.155 | United States | 147.237.76.86 | navy.idf.il | Block_Ip_Web_In | drop | 8 |
| 66.249.78.134 | United States | 147.237.0.34 | tikshuv.idf.il | Block_Ip_Web_In | drop | 7 |
| 66.249.78.96 | United States | 147.237.77.74 | law.idf.il | Block_Ip_Web_In | drop | 7 |
| 66.249.81.212 | United States | 147.237.72.166 | aka.idf.il | Block_Ip_Web_In | drop | 6 |
| 66.249.64.155 | United States | 147.237.72.156 | aman.idf.il | Block_Ip_Web_In | drop | 6 |
| 66.249.78.151 | United States | 147.237.76.39 | mobile.meitav.idf.il | Block_Ip_Web_In | drop | 6 |
| 66.249.69.34 | United States | 147.237.72.166 | aka.idf.il | Block_Ip_Web_In | drop | 6 |
| 66.249.78.165 | United States | 147.237.76.39 | mobile.meitav.idf.il | Block_Ip_Web_In | drop | 6 |
| 66.249.78.67 | United States | 147.237.77.233 | atal.idf.il | Block_Ip_Web_In | drop | 6 |

04-09-2015-21:03:06 to 04-09-2015-22:03:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 184.173.183.172 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 121 |
| 46.19.85.201 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 46.19.85.211 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 93.120.27.62 | Romania | 147.237.76.34 | yohalan.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 93.120.27.62 | Romania | 147.237.76.199 | e.nakchal.idf.il | DVRep_B-N_60_100 | Block | 1 |

04-09-2015-21:03:06 to 04-09-2015-22:03:06

## Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|---|---|---|---|---|---|
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 6 |
| 84.108.29.151 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 61.240.144.64 | China | 147.237.0.15 | kosher-kravi.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 27.50.132.61 | China | 147.237.77.205 | prisha.idf.il | ET SCAN NMAP -f -sS | 1 |
| 218.77.79.43 | China | 147.237.76.197 | e.himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 94.102.56.231 | Netherlands | 147.237.8.46 | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.64 | China | 147.237.77.176 | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 27.50.132.61 | China | 147.237.77.205 | prisha.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 199.192.207.146 | United States | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 189.196.81.252 | Mexico | 147.237.76.42 | refuah.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 85.250.134.135 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

04-09-2015-21:03:06 to 04-09-2015-22:03:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 184.151.114.170 | Canada | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 128 |
| 37.216.26.202 | Saudi Arabia | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 108 |
| 89.139.185.104 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 90 |
| 37.142.67.73 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 63 |
| 109.160.237.214 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 63 |
| 84.228.189.121 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 63 |
| 78.191.252.17 | Turkey | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 54 |
| 109.160.234.151 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 53 |
| 81.218.140.130 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 53 |
| 198.103.167.20 | Canada | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 51 |
| 166.137.136.79 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 51 |
| 81.218.80.226 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 51 |
| 92.57.14.35 | Spain | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 45 |
| 64.53.187.88 | United States | 147.237.77.176 | matpash.idf.il | First packet isn't SYN | drop | drop | 44 |
| 85.65.6.217 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 43 |
| 46.19.85.184 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 37 |
| 37.237.192.23 | Iraq | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 36 |
| 67.253.18.17 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 33 |
| 149.78.154.69 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 32 |
| 176.12.142.162 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 32 |
| 188.49.117.99 | Saudi Arabia | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 31 |
| 176.12.141.247 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 30 |
| 157.55.39.6 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 30 |
| 41.97.62.200 | Algeria | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 29 |
| 109.253.137.93 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 29 |
| 54.72.0.55 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 28 |
| 37.48.120.214 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 23 |
| 46.19.85.219 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 22 |
| 197.202.234.151 | Algeria | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 22 |
| 162.254.149.195 |  | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 21 |
| 93.172.34.126 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 21 |
| 37.142.163.36 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 20 |
| 77.127.118.204 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 20 |
| 176.12.151.130 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 19 |
| 176.12.147.111 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 19 |
| 176.12.142.251 | Israel | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 150.212.112.17 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 18 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 18 |
| 172.8.181.109 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 18 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 17 |
| 80.246.130.82 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 17 |
| 173.209.211.219 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 16 |
| 82.114.169.88 | Yemen | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 15 |
| 173.209.211.245 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 15 |
| 46.19.86.111 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 14 |
| 95.187.180.208 | Romania | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 14 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 14 |
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 13 |
| 173.209.211.145 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 12 |
| 173.209.211.153 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 12 |

04-09-2015-21:03:06 to 04-09-2015-22:03:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.109.212.29 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/valtam | Block | 4 |
| 87.69.246.148 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 4 |
| 149.88.8.65 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 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 | 2 |
| 212.106.92.156 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 2 |
| 109.253.143.75 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 84.111.168.82 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 46.185.226.170 | Jordan | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-ar | Block | 1 |
| 180.76.5.60 | China | 147.237.72.166 | aka.idf.il | Unknown Parameter docid in www.aka.idf.il/iturim/asp/displayonesoldier.asp | None | 1 |
| 89.138.203.237 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152 | Block | 1 |
| 77.127.144.1 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __EVENTTARGET in www.aka.idf.il/main/sachar/ | None | 1 |
| 5.29.86.238 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 85.65.169.8 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 68.180.228.232 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/kamlar/home | Block | 1 |
| 180.177.159.111 | Taiwan | 147.237.0.34 | tikshuv.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 89.237.241.4 | Kyrgyzstan | 147.237.0.34 | tikshuv.idf.il | Unknown HTTP Request Method COOK in URL www.tikshuv.idf.il/1048-7888-he/tikshuv.aspx | Block | 1 |
| 77.127.144.1 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx | None | 1 |
| 37.237.192.23 | Iraq | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/klf/ | Block | 1 |
| 149.129.173.246 | United States | 147.237.0.15 | kosher-kravi.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 1 |
| 87.68.87.228 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 68.180.228.232 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx | None | 1 |
| 190.157.176.125 | Colombia | 147.237.77.74 | law.idf.il | Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx | Block | 1 |
| 93.172.45.126 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 80.246.140.90 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd | Block | 1 |
| 46.117.0.105 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/ | Block | 1 |
| 149.129.173.246 | United States | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 1 |
| 87.69.114.11 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm | Block | 1 |
| 109.64.42.49 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 46.121.121.184 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/ | Block | 1 |
| 149.129.173.246 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 1 |
| 77.125.121.29 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails | Block | 1 |
| 217.12.204.117 | Ukraine | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |

04-09-2015-21:03:06 to 04-09-2015-22:03:06