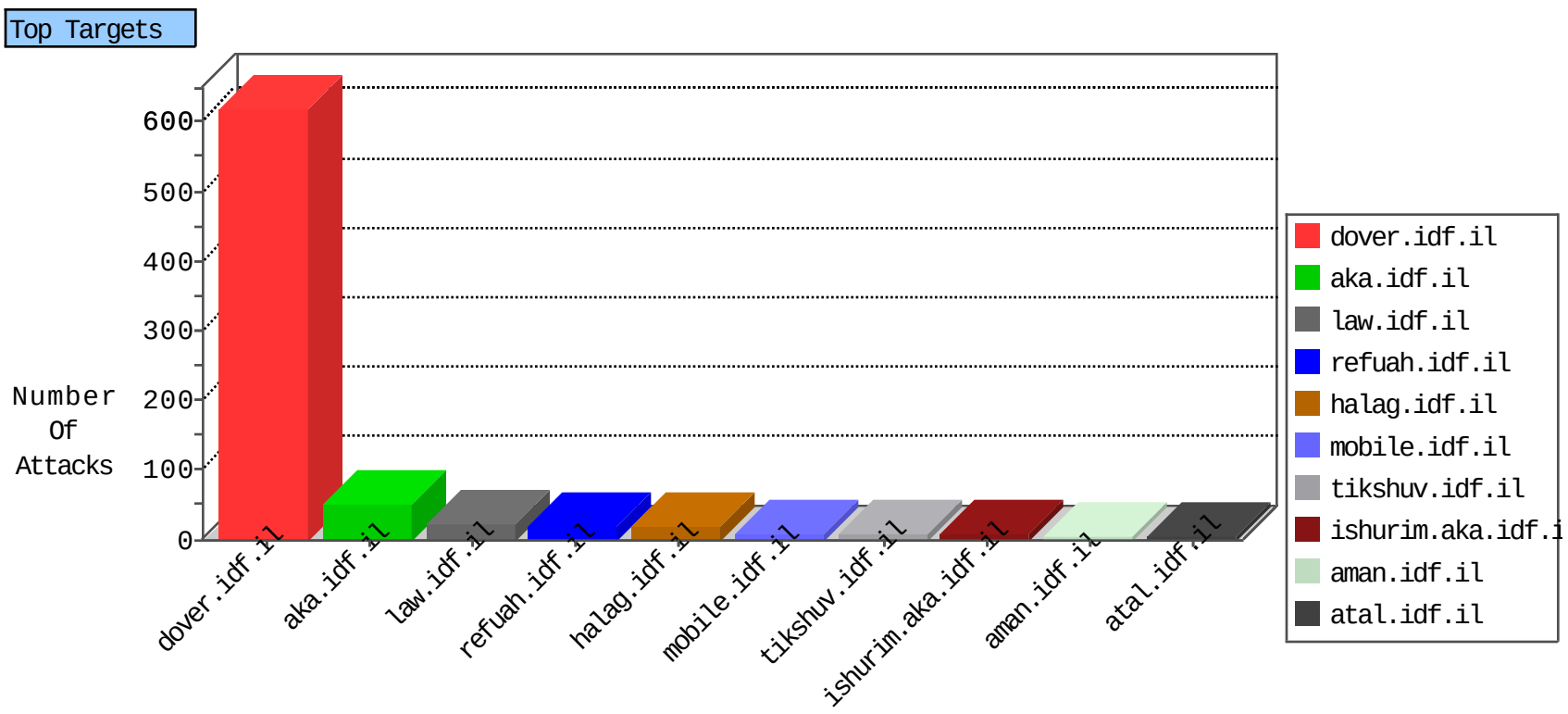
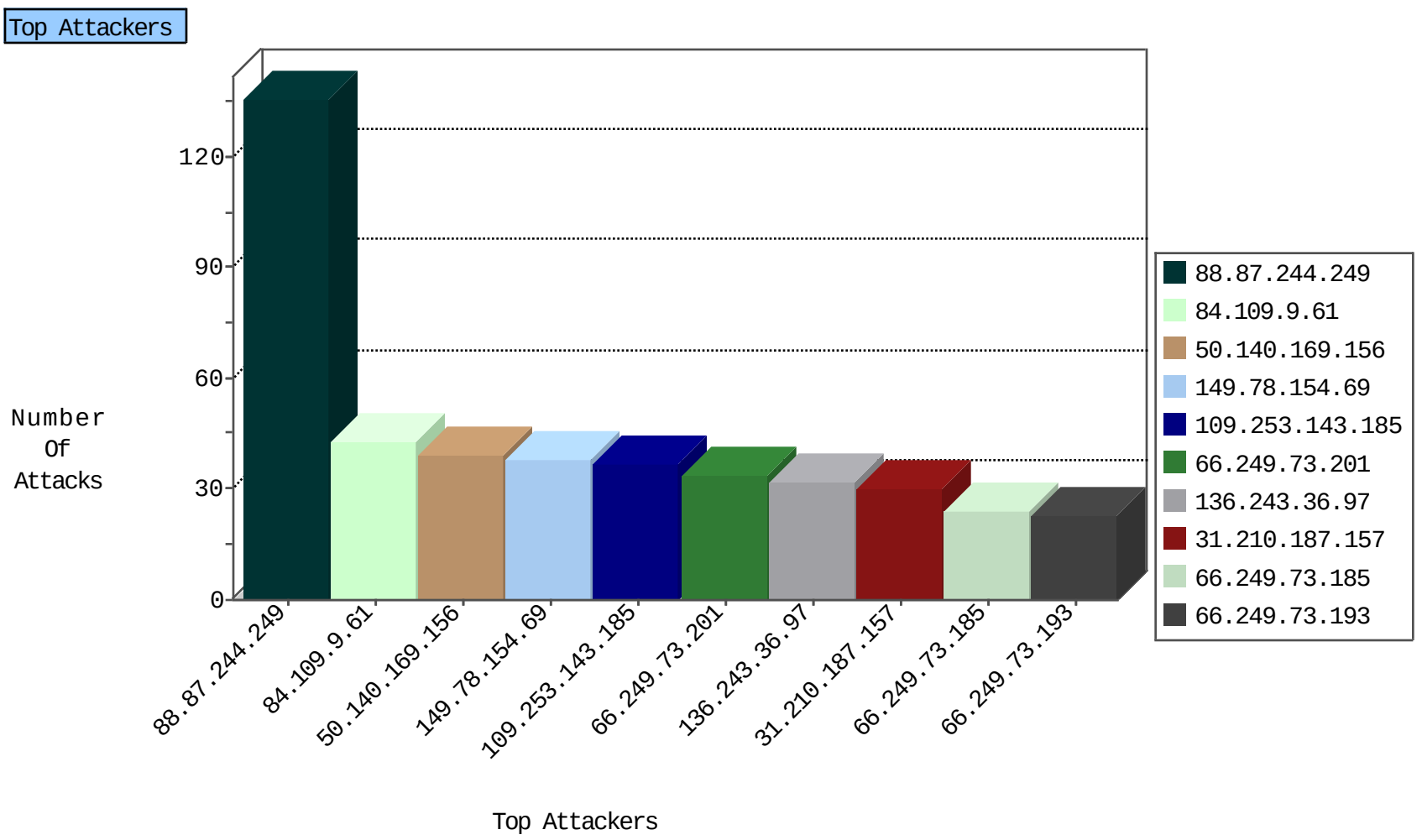
05-10-2015-01:03:05 to 05-10-2015-02:03:05

# IDF Under Attack
# 05-10-2015-01:03:05

Top Targets




Top Attackers



05-10-2015-01:03:05 to 05-10-2015-02:03:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Web Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 220.181.108.96 | China | 147.237.76.42 | refuah.idf.il | TCP handshake violation, first packet not syn | drop | 69 |
| 84.108.248.162 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 67 |
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 5 |
| 87.69.15.189 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 66.240.192.138 | United States | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 124.232.142.220 | China | 147.237.76.30 | himush.idf.il | Block_Udp_All_Nets | drop | 1 |

05-10-2015-01:03:05 to 05-10-2015-02:03:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 91.228.248.251 | Israel | 147.237.76.42 | refuah.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 12 |
| 66.240.192.138 | United States | 147.237.76.198 | e.yohalan.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 131.72.136.11 | | 147.237.77.235 | sviva.idf.il | EgovRep_B-N_70-99 | Block | 1 |
| 71.6.167.142 | United States | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.31 | nakchal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.192.138 | United States | 147.237.0.19 | madim.atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 87.68.31.243 | Israel | 147.237.72.167 | ishurim.aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 71.6.165.200 | United States | 147.237.77.233 | atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.192.138 | United States | 147.237.77.121 | e.navy.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.69.98 | United States | 147.237.8.24 | e.lifestyle.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.76.198 | e.yohalan.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.177 | ncore.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.192.138 | United States | 147.237.0.200 | m4u.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.0.15 | kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.0.34 | tikshuv.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.69.98 | United States | 147.237.76.177 | ncore.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.76.199 | e.nakchal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.196 | e.sviva.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.192.138 | United States | 147.237.8.24 | e.lifestyle.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 93.120.27.62 | Romania | 147.237.76.44 | e.refuah.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.0.35 | akaws.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.8.50 | e.tikshuv.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 46.19.85.143 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 198.20.69.98 | United States | 147.237.77.121 | e.navy.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.77.226 | www.chamatz.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.198 | e.yohalan.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.192.138 | United States | 147.237.76.148 | gqcenter.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.198 | e.yohalan.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.192.138 | United States | 147.237.76.148 | gqcenter.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 93.120.27.62 | Romania | 147.237.76.148 | gqcenter.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.77.121 | e.navy.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.30 | himush.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 46.116.210.130 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 198.20.69.98 | United States | 147.237.77.227 | e.hamaz.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.77.233 | atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.77.212 | e.dover.idf.il | DVRep_B-N_60_100 | Block | 1 |

05-10-2015-01:03:05 to 05-10-2015-02:03:05

## 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 |
| 2.52.155.8 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 187.11.121.110 | Brazil | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 128.199.238.136 | Singapore | 147.237.72.166 | aka.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 89.248.160.215 | Netherlands | 147.237.77.212 | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 81.200.91.2 | Russian Federation | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 61.240.144.67 | China | 147.237.76.201 | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.77.79.43 | China | 147.237.77.205 | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 187.11.121.110 | Brazil | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 187.11.121.110 | Brazil | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -f -sS | 1 |
| 104.167.117.197 |  | 147.237.77.233 | atal.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 81.200.91.2 | Russian Federation | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 61.240.144.67 | China | 147.237.77.234 | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.149.161.186 | China | 147.237.8.46 | e.chinuch.idf.il | GPL SCAN nmap TCP | 1 |

05-10-2015-01:03:05 to 05-10-2015-02:03:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 88.87.244.249 | Hungary | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 100 |
| 84.109.9.61 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 43 |
| 50.140.169.156 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 39 |
| 149.78.154.69 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 38 |
| 109.253.143.185 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 37 |
| 88.87.244.249 | Hungary | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 36 |
| 66.249.73.201 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 26 |
| 136.243.36.97 | Germany | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 20 |
| 66.249.73.193 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 16 |
| 66.249.73.185 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 14 |
| 136.243.36.97 | Germany | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 10 |
| 189.122.249.43 | Brazil | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 9 |
| 66.65.96.59 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 9 |
| 46.19.86.239 | Israel | 147.237.77.243 | mobile.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 9 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 8 |
| 114.125.41.235 | Indonesia | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 7 |
| 5.29.188.54 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 7 |
| 31.210.187.157 | Israel | 147.237.77.234 | halag.idf.il | Invalid ACK number | Bad TCP sequence | alert | 6 |
| 31.210.187.157 | Israel | 147.237.77.234 | halag.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 6 |
| 157.55.39.204 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 6 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 6 |
| 31.210.187.157 | Israel | 147.237.77.234 | halag.idf.il | First packet isn't SYN | drop | drop | 6 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 5 |
| 84.228.171.34 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 5 |
| 31.13.102.116 | Ireland | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 31.13.102.123 | Ireland | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 46.19.85.58 | Israel | 147.237.0.34 | tikshuv.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 4 |
| 31.13.102.117 | Ireland | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 31.210.187.157 | Israel | 147.237.77.74 | law.idf.il | First packet isn't SYN | drop | drop | 4 |
| 31.13.102.118 | Ireland | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 99.238.139.12 | Canada | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 188.227.238.173 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 37.187.162.184 | France | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 31.210.187.157 | Israel | 147.237.77.74 | law.idf.il | Invalid ACK number | Bad TCP sequence | alert | 4 |
| 41.33.231.86 | Egypt | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 37.140.141.37 | Russian Federation | 147.237.77.74 | law.idf.il | SAM rule | drop | drop | 4 |
| 54.72.0.55 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 75.61.140.216 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 31.210.187.157 | Israel | 147.237.77.74 | law.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 4 |
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 41.37.102.173 | Egypt | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 3 |
| 128.242.249.14 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 3 |
| 5.28.156.177 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 3 |
| 128.242.249.10 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 3 |
| 89.139.164.177 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2 |
| 81.218.208.248 | Israel | 147.237.76.42 | refuah.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 2 |
| 174.16.191.73 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2 |
| 37.187.162.126 | France | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2 |
| 109.253.132.185 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 80.178.2.98 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 10 |
| 66.249.73.185 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.185 | Block | 8 |
| 66.249.73.201 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.201 | Block | 7 |
| 62.90.235.246 | Israel | 147.237.72.156 | aman.idf.il | Distributed Unauthorized HTTP Method | Block | 6 |
| 37.139.52.23 | Germany | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/getfile/ | Block | 6 |
| 66.249.73.193 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.193 | Block | 5 |
| 207.46.13.26 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 3 |
| 157.55.39.136 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 2.52.7.153 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 213.151.35.218 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 2 |
| 149.78.114.200 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 2 |
| 77.127.184.105 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 86.67.9.220 | France | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 41.37.102.173 | Egypt | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 1 |
| 79.177.39.85 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx | Block | 1 |
| 66.249.78.146 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/portalmi | Block | 1 |
| 178.255.215.87 | France | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1129-he/kkkkkkk=55b3d697kkkkkkk_55b3d697 | Block | 1 |
| 66.249.67.79 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/261-6387-he/patzar.aspx | Block | 1 |
| 95.86.78.30 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/aman | Block | 1 |
| 66.249.78.240 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx | Block | 1 |
| 212.179.224.141 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 52.6.169.50 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm | Block | 1 |
| 157.55.39.137 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.78.160 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.78.160 | Block | 1 |
| 185.32.176.208 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.67.152 | Israel | 147.237.77.74 | law.idf.il | Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx | None | 1 |
| 136.243.36.97 | Germany | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 136.243.36.97 | Block | 1 |
| 75.131.150.100 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 66.249.75.34 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 213.151.32.163 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 1 |
| 157.55.39.137 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sachar/klali.aspx | Block | 1 |
| 84.108.65.245 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/ | Block | 1 |
| 66.249.78.160 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip.storage/files/4/ | Block | 1 |
| 185.32.177.206 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 136.243.36.97 | Germany | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy/ | Block | 1 |
| 77.125.164.23 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 1 |
| 66.249.78.2 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/m/ | Block | 1 |
| 157.55.39.161 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 64.79.85.205 | United States | 147.237.77.170 | maarachot.idf.il | URL is Above Root Directory maarachot.idf.il/../ | Block | 1 |
| 85.65.62.206 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 66.249.78.206 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/manilot | Block | 1 |
| 66.249.78.104 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx | Block | 1 |
| 157.55.39.162 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.67.65 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/71847-he/maarachot.aspx | Block | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp | Block | 1 |
| 207.46.13.26 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp | Block | 1 |
| 66.249.73.201 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |