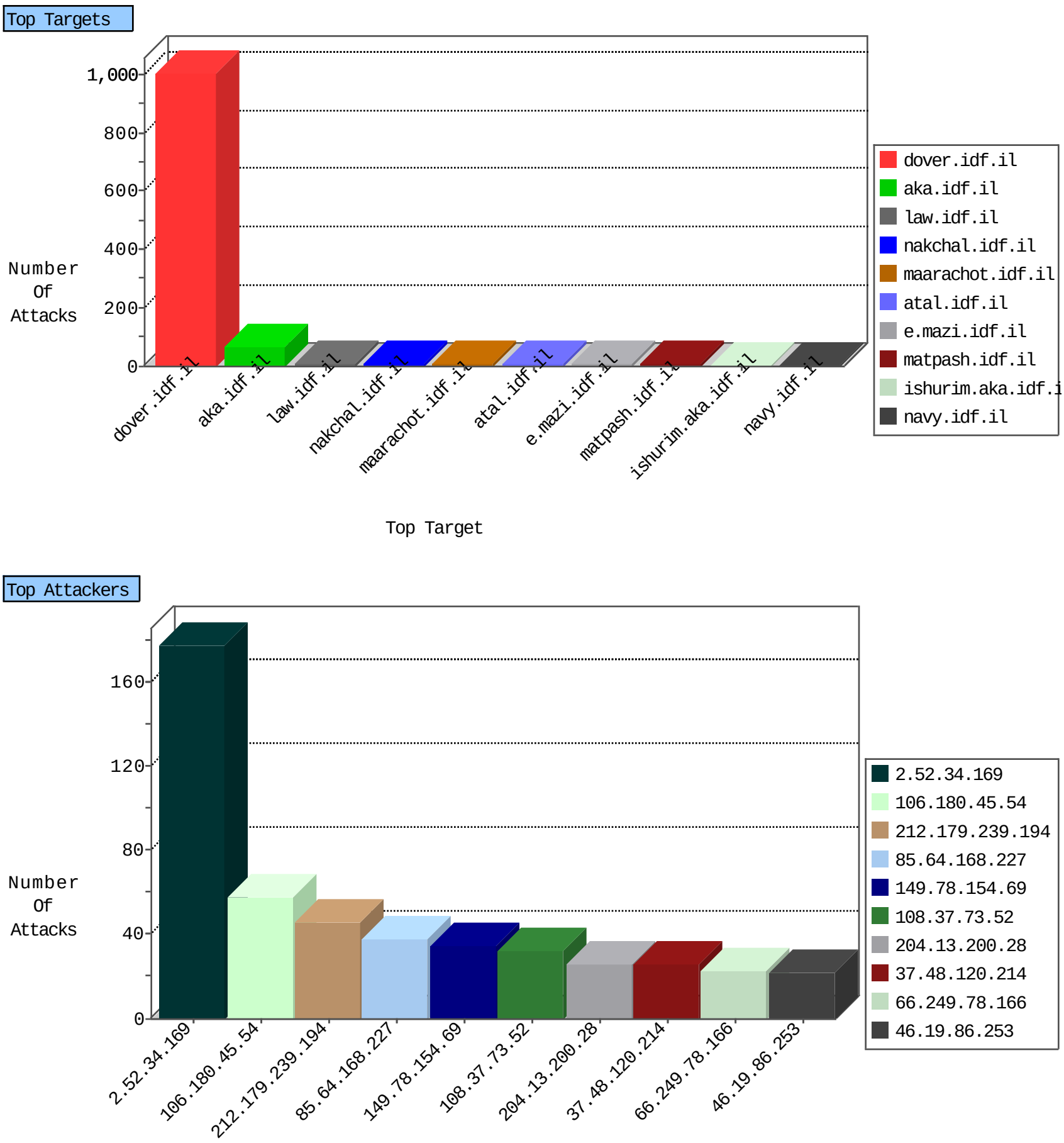
05-07-2015-07:03:02 to 05-07-2015-08:03:02

# IDF Under Attack
05-07-2015-07:03:02



05-07-2015-07:03:02 to 05-07-2015-08:03:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Web Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.78.29 | Israel | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 3340 |
| 204.13.200.28 | United States | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | forward | 370 |
| 2.52.34.169 | Israel | 147.237.77.216 | dover.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 83 |
| 84.94.54.130 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 77 |
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 192.115.248.2 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 2 |
| 185.32.176.57 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 185.32.178.168 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 2.54.160.236 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 212.179.239.194 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 111.202.66.66 | China | 147.237.0.19 | madim.atal.idf.il | L4 Source or Dest Port Zero | drop | 1 |
| 124.232.142.220 | China | 147.237.76.34 | yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 198.48.92.104 | United States | 147.237.76.86 | navy.idf.il | Block_Udp_All_Nets | drop | 1 |

05-07-2015-07:03:02 to 05-07-2015-08:03:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 192.116.94.74 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 128.242.249.12 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 6 |
| 46.19.85.170 | Israel | 147.237.77.74 | law.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 188.138.9.50 | Germany | 147.237.72.14 | dover.idf.il(old) | DVRep_B-N_60_100 | Block | 2 |
| 188.138.9.50 | Germany | 147.237.76.44 | e.refuah.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.76.148 | gqcenter.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.69.98 | United States | 147.237.76.202 | e.halag.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.0.35 | akaws.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.39 | mobile.meitav.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.70.114 | United States | 147.237.76.148 | gqcenter.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.76.196 | e.sviva.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.77.235 | sviva.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.135.131 | United States | 147.237.8.45 | e.eitan.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.69.98 | United States | 147.237.77.179 | e.mazi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.8.50 | e.tikshuv.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.72.14 | dover.idf.il(old) | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.76.201 | e.atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 76.185.192.18 | United States | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 71.6.135.131 | United States | 147.237.76.196 | e.sviva.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.69.98 | United States | 147.237.77.216 | dover.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.72.156 | aman.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.77.61 | e.cogat.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.77.121 | e.navy.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.135.131 | United States | 147.237.77.61 | e.cogat.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.69.98 | United States | 147.237.77.227 | e.hamaz.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.76.39 | mobile.meitav.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.76.31 | nakchal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.135.131 | United States | 147.237.77.233 | atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.70.114 | United States | 147.237.72.156 | aman.idf.il | DVRep_B-N_60_100 | Block | 1 |

05-07-2015-07:03:02 to 05-07-2015-08:03:02

## 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 | 4 |
| 66.249.78.82 | United States | 147.237.77.74 | law.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 192.115.83.5 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 80.246.133.150 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 1 |
| 222.69.94.13 | China | 147.237.77.179 | e.mazi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 69.12.92.137 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.89.137.3 | China | 147.237.76.44 | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 66.249.78.134 | United States | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 1 |
| 203.194.234.109 | Hong Kong | 147.237.77.179 | e.mazi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 61.160.224.128 | China | 147.237.77.212 | e.dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.160.224.128 | China | 147.237.72.167 | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 188.138.9.51 | Germany | 147.237.76.176 | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 128.199.75.236 | Singapore | 147.237.72.156 | aman.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 124.228.9.32 | China | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.128.144.130 |  | 147.237.8.46 | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.69.94.13 | China | 147.237.77.179 | e.mazi.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 80.179.9.7 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 222.69.94.13 | China | 147.237.77.179 | e.mazi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 69.12.92.137 | United States | 147.237.76.202 | e.halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 212.179.239.194 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 203.194.234.109 | Hong Kong | 147.237.77.179 | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.160.224.128 | China | 147.237.77.205 | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.19.85.217 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 178.19.107.114 | Poland | 147.237.76.30 | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 124.228.9.32 | China | 147.237.8.45 | e.eitan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 124.228.9.32 | China | 147.237.8.14 | e.orchot.idf.il | ET SCAN Potential SSH Scan | 1 |

05-07-2015-07:03:02 to 05-07-2015-08:03:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 2.52.34.169 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 168 |
| 106.180.45.54 | Japan | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 58 |
| 212.179.239.194 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 44 |
| 85.64.168.227 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 38 |
| 149.78.154.69 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 35 |
| 108.37.73.52 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 32 |
| 37.48.120.214 | Netherlands | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 26 |
| 46.19.86.253 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 22 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 20 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 18 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 16 |
| 46.19.85.220 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 16 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 14 |
| 46.19.85.236 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 13 |
| 46.19.85.217 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 12 |
| 192.116.94.74 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 12 |
| 157.55.39.7 | United States | 147.237.72.166 | aka.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 12 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 12 |
| 212.28.230.202 | Lebanon | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 12 |
| 157.55.39.204 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 11 |
| 213.151.32.163 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 11 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 11 |
| 54.72.0.55 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 10 |
| 81.218.29.162 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 9 |
| 77.125.6.63 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 9 |
| 109.65.116.115 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 8 |
| 109.253.131.96 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 8 |
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 8 |
| 5.28.154.11 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 80.246.133.136 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 46.116.132.31 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 109.186.61.222 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 80.179.9.115 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6 |
| 80.246.133.133 | Israel | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 6 |
| 2.52.40.200 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6 |
| 138.134.102.15 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6 |
| 98.167.28.205 | United States | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 6 |
| 80.179.9.7 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 5 |
| 80.250.154.169 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 5 |
| 85.64.54.163 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 5 |
| 74.90.247.206 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 5 |
| 46.19.85.251 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4 |
| 93.172.175.246 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4 |
| 2.54.42.6 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4 |
| 79.180.7.173 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4 |
| 46.19.85.89 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4 |
| 109.253.133.89 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4 |
| 109.253.157.184 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4 |
| 66.249.64.238 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4 |
| 79.182.201.16 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4 |

05-07-2015-07:03:02 to 05-07-2015-08:03:02

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 91.121.79.180 | France | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 91.121.79.180 | Block | 2 |
| 212.143.225.135 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc | Block | 2 |
| 66.249.78.118 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/924-2336-he/patzar.aspx | Block | 1 |
| 54.186.248.49 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1294-he/www.idf.il | Block | 1 |
| 157.55.39.136 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 157.55.39.136 | Block | 1 |
| 71.190.204.235 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 1 |
| 66.249.69.20 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 31.193.51.84 | France | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 176.12.150.206 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd | Block | 1 |
| 138.134.102.15 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/milnet | Block | 1 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/hebrew/download.stm | Block | 1 |
| 54.215.43.237 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter docId in www.aka.idf.il/kamlar/klali/ | None | 1 |
| 157.55.39.136 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp | Block | 1 |
| 66.249.75.51 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 1 |
| 46.121.137.194 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/938-he/cogat.aspx | Block | 1 |
| 195.10.194.74 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd | Block | 1 |
| 138.134.192.10 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il//milnet | Block | 1 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1361-10625-he/dover.aspx-publisher=israel | Block | 1 |
| 66.162.42.131 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 157.55.39.137 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 91.121.79.180 | France | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper | Block | 1 |
| 66.249.78.109 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-14276-he/dover.aspx | Block | 1 |
| 50.97.52.131 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/&usg=alkjrhjnql_xvu0f45t5gysvxs0ys7tltg | Block | 1 |
| 207.46.13.26 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 142.54.161.131 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1283-16707-en/dover.aspx/trackback/ | Block | 1 |
| 66.249.93.179 | Israel | 147.237.77.176 | matpash.idf.il | URL is Above Root Directory www.cogat.idf.il/../favicon.ico | Block | 1 |
| 66.249.67.78 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/ | Block | 1 |
| 157.55.39.137 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/sites/home/def...78&catid=38978 | Block | 1 |
| 109.66.183.58 | Israel | 147.237.77.170 | maarachot.idf.il | CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME | Block | 1 |
| 66.249.78.111 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/261-6599-he/patzar.aspx | Block | 1 |
| 52.6.169.50 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/news/nifg.stm. | Block | 1 |
| 157.55.39.7 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 68.180.229.51 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 68.180.229.51 | Block | 1 |
| 66.249.67.92 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/261-6455-he/patzar.aspx | Block | 1 |
| 31.184.195.166 | Russian Federation | 147.237.77.216 | dover.idf.il | Suspicious Response Code | Block | 1 |
| 157.55.39.191 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/+idf units | Block | 1 |
| 109.253.141.200 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |

05-07-2015-07:03:02 to 05-07-2015-08:03:02