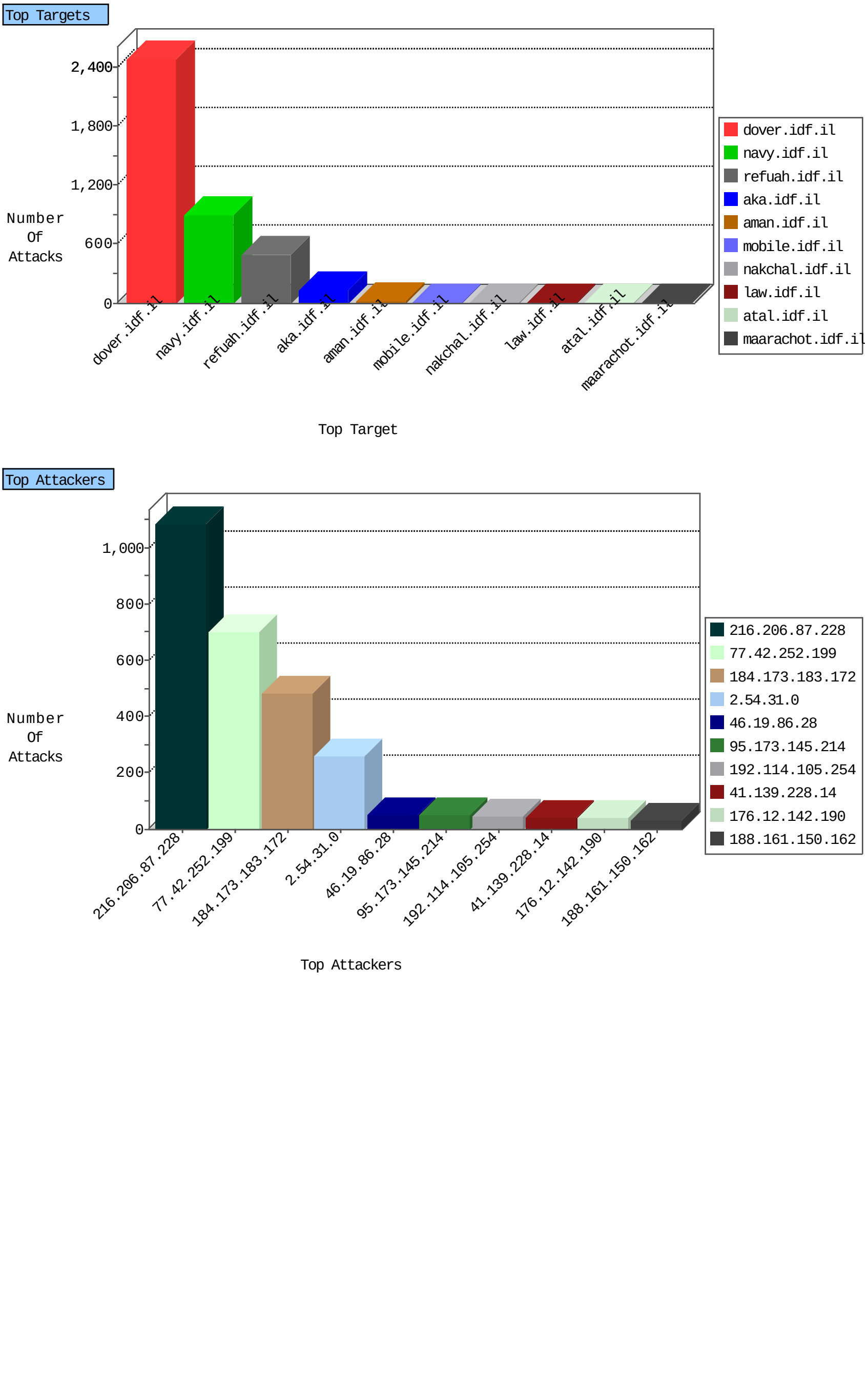
05-07-2015-09:03:04 to 05-07-2015-10:03:04

# IDF Under Attack
# 05-07-2015-09:03:04



05-07-2015-09:03:04 to 05-07-2015-10:03:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Web Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 147.235.236.1 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 291 |
| 204.13.200.28 | United States | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | forward | 282 |
| 192.115.116.25 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 106 |
| 79.182.103.60 | Israel | 147.237.77.216 | dover.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 86 |
| 79.182.103.60 | Israel | 147.237.77.216 | dover.idf.il | Anomaly-TLS-renegotiation-Cli | forward | 61 |
| 192.118.22.242 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 5 |
| 194.90.220.241 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 4 |
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 4 |
| 2.54.16.198 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 4 |
| 120.89.2.12 | Philippines | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 3 |
| 79.182.121.176 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 3 |
| 180.113.19.130 | China | 147.237.76.86 | navy.idf.il | Block_Udp_All_Nets | drop | 2 |
| 2.54.159.95 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 194.177.16.3 | Israel | 147.237.76.31 | nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 93.120.27.62 | Romania | 147.237.76.176 | test.ncore.idf.il | Block_Udp_All_Nets | drop | 1 |

05-07-2015-09:03:04 to 05-07-2015-10:03:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 216.206.87.228 | United States | 147.237.76.86 | navy.idf.il | DVRep_P-N_40-59 | Permit | 891 |
| 184.173.183.172 | United States | 147.237.76.42 | refuah.idf.il | DVRep_P-N_40-59 | Permit | 484 |
| 216.206.87.228 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 194 |
| 213.215.130.101 | Italy | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 10 |
| 85.250.24.69 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 151.90.254.205 | Italy | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 46.19.85.57 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 188.138.9.50 | Germany | 147.237.76.202 | e.halag.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 93.120.27.62 | Romania | 147.237.77.178 | e.matpash.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.70.114 | United States | 147.237.77.227 | e.hamaz.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.0.19 | madim.atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.76.30 | himush.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.0.15 | kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.77.243 | mobile.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 109.67.0.91 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 71.6.167.142 | United States | 147.237.0.200 | m4u.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.70.114 | United States | 147.237.77.233 | atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 188.138.9.50 | Germany | 147.237.76.31 | nakchal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.77.235 | sviva.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.8.14 | e.orchot.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 192.115.90.81 | Israel | 147.237.77.170 | maarachot.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 109.186.46.190 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 71.6.167.142 | United States | 147.237.76.30 | himush.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 212.179.46.23 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 188.138.9.50 | Germany | 147.237.76.38 | e.e.meitav.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.197 | e.himush.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.69.98 | United States | 147.237.76.198 | e.yohalan.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.77.74 | law.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 213.57.57.20 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 188.138.9.50 | Germany | 147.237.76.196 | e.sviva.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 93.120.27.62 | Romania | 147.237.77.176 | matpash.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 198.20.69.98 | United States | 147.237.76.200 | eitan.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.43.94 | Germany | 147.237.0.17 | m.my-kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.135.131 | United States | 147.237.77.212 | e.dover.idf.il | DVRep_B-N_60_100 | Block | 1 |

05-07-2015-09:03:04 to 05-07-2015-10:03:04

## Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|---|---|---|---|---|---|
| 221.235.189.244 | China | 147.237.76.177 | ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.89.137.3 | China | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 114.112.90.54 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.159.210.185 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.250.113.230 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.179.112.209 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 69.12.92.137 | United States | 147.237.8.24 | e.lifestyle.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 221.235.189.244 | China | 147.237.76.198 | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.66 | China | 147.237.0.34 | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 221.235.189.244 | China | 147.237.0.19 | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.89.137.3 | China | 147.237.8.27 | e.madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 188.138.9.51 | Germany | 147.237.8.46 | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.253.134.48 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.68.22.109 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 1 |
| 85.130.238.91 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.179.68.178 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.64.233 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 1 |

05-07-2015-09:03:04 to 05-07-2015-10:03:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 77.42.252.199 | Lebanon | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 700 |
| 2.54.31.0 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 262 |
| 46.19.86.28 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 52 |
| 95.173.145.214 | Russian Federation | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 50 |
| 192.114.105.254 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 46 |
| 41.139.228.14 | Kenya | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 42 |
| 176.12.142.190 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 40 |
| 188.161.150.162 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 31 |
| 149.78.154.69 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 28 |
| 157.55.39.204 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 23 |
| 141.90.9.62 | Germany | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 21 |
| 124.123.105.27 | India | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 20 |
| 2.52.32.254 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 18 |
| 79.177.116.198 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 17 |
| 37.26.147.252 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 16 |
| 193.33.2.112 | Spain | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 15 |
| 37.48.120.214 | Netherlands | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 13 |
| 130.86.75.28 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 13 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 13 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 12 |
| 207.46.13.26 | United States | 147.237.72.166 | aka.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 12 |
| 85.250.24.69 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 12 |
| 212.179.21.195 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 12 |
| 46.19.85.98 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 11 |
| 77.127.149.222 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 11 |
| 46.19.85.47 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 10 |
| 94.159.210.185 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 10 |
| 80.178.146.96 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 10 |
| 46.19.86.54 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 9 |
| 46.19.85.104 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 9 |
| 176.12.149.7 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 9 |
| 95.132.143.120 | Ukraine | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 9 |
| 84.229.175.252 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 9 |
| 81.218.251.250 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 9 |
| 46.19.86.78 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 9 |
| 46.19.85.57 | Israel | 147.237.72.166 | aka.idf.il | Invalid ACK number | Bad TCP sequence | monitor | 8 |
| 79.179.112.209 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 8 |
| 82.213.38.162 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 8 |
| 93.173.17.244 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 8 |
| 212.116.163.73 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 81.218.130.91 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 146.185.157.119 | Netherlands | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 46.19.86.207 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 7 |
| 109.253.149.9 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6 |
| 192.117.170.194 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6 |
| 93.173.132.16 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6 |
| 46.19.86.119 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6 |
| 46.19.86.11 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6 |

05-07-2015-09:03:04 to 05-07-2015-10:03:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.116.243.26 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 24 |
| 149.88.6.163 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd | Block | 13 |
| 37.140.141.39 | Russian Federation | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/mod | Block | 4 |
| 212.199.69.213 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/ | Block | 4 |
| 207.46.13.26 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 85.250.104.59 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.75.13 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/miluim/templates/ | Block | 1 |
| 31.168.230.82 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl74.x in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 203.133.170.17 | Korea, Republic of | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 109.253.157.123 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 66.249.78.147 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Unauthorized URL Access on tikshuv.idf.il//edim/yoman/enlarge.asp | Block | 1 |
| 46.120.25.119 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 157.55.39.162 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 157.55.39.162 | Block | 1 |
| 87.69.148.26 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.75.26 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx | Block | 1 |
| 37.26.147.195 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 1 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.166 | 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 |
| 157.55.39.191 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/021021.stm | Block | 1 |
| 94.159.167.181 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx | None | 1 |
| 66.249.75.109 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 212.25.70.199 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 149.129.152.239 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 85.65.239.207 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew/history/history.stm | Block | 1 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/homepage/ | Block | 1 |
| 185.32.178.74 | Israel | 147.237.77.243 | mobile.idf.il | Suspicious Response Code | Block | 1 |
| 5.102.254.211 | Israel | 147.237.77.216 | dover.idf.il | NULL Character in Method | Block | 1 |
| 109.67.17.119 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd | Block | 1 |
| 66.249.75.117 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 46.19.85.68 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx | Block | 1 |
| 157.55.39.136 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp | Block | 1 |
| 85.250.43.55 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.69.34 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 192.115.90.81 | Israel | 147.237.77.170 | maarachot.idf.il | CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME | Block | 1 |
| 5.157.42.212 | Luxembourg | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/main.asp | Block | 1 |
| 109.186.146.161 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 1 |
| 66.249.78.140 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp | Block | 1 |
| 157.55.39.162 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |

05-07-2015-09:03:04 to 05-07-2015-10:03:04