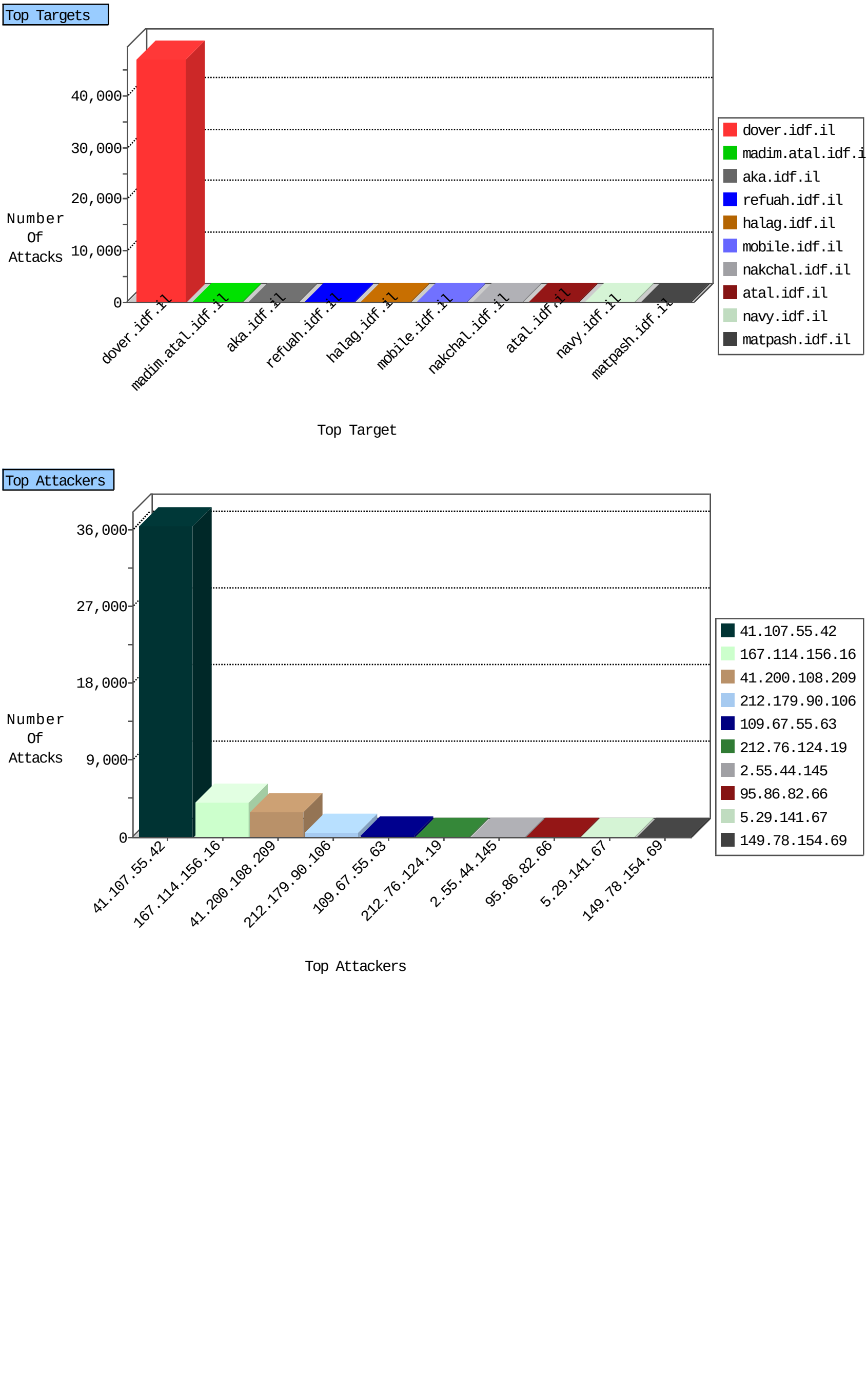
04-16-2016-22:04:07 to 04-16-2016-23:04:07

# IDF Under Attack Daily Report



04-16-2016-22:04:07 to 04-16-2016-23:04:07

## 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 | Block_Ip_Web_In | drop | 4099 |
| 41.200.108.209 | Algeria | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 2920 |
| 41.107.55.42 | Algeria | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 2464 |
| 41.200.108.209 | Algeria | 147.237.77.216 | dover.idf.il | DOS-HTTP-fireflood | dest-reset | 286 |
| 41.107.55.42 | Algeria | 147.237.77.216 | dover.idf.il | DOS-LOIC-TCP-80-cat | dest-reset | 203 |
| 123.59.59.52 | China | 147.237.76.39 | mobile.meitav.idf.il | block-sp-traf1 | forward | 4 |
| 82.145.208.202 | Europe | 147.237.77.176 | matpash.idf.il | Block_Ip_Web_In | drop | 4 |
| 81.218.65.210 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 2 |
| 37.204.142.237 | Russian Federation | 147.237.76.86 | navy.idf.il | JLM_Under_Attack_Con_Http | drop | 1 |
| 45.32.95.13 | Netherlands | 147.237.76.38 | e.e.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |
| 87.70.16.48 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 179.43.141.194 | Switzerland | 147.237.77.216 | dover.idf.il | Block_Ntp_All_Net | drop | 1 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 94.102.49.116 | Netherlands | 147.237.0.15 | kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |

04-16-2016-22:04:07 to 04-16-2016-23:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.64.153.33 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 79.178.102.11 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 217.103.97.99 | Netherlands | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 3 |
| 217.103.97.99 | Netherlands | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 3 |
| 217.103.97.99 | Netherlands | 147.237.77.176 | matpash.idf.il | C1000074: HTTP: majestic bot | Block | 3 |
| 41.200.108.209 | Algeria | 147.237.77.216 | dover.idf.il | 12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack) | Block | 2 |
| 61.135.189.122 | China | 147.237.76.31 | nakchal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 2 |
| 10.0.0.2 | | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 106.38.241.106 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 66.249.66.187 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

04-16-2016-22:04:07 to 04-16-2016-23:04:07

## 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 | 7 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 218.57.11.7 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.66.33 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 203.197.205.118 | 147.237.76.177 | India | ncore.idf.il | ET SCAN NMAP -f -sS | 1 |
| 80.82.78.38 | 147.237.77.227 | Netherlands | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 124.65.231.114 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 124.65.231.114 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 124.65.231.114 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.167.131 | 147.237.77.121 | Netherlands | e.navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.57.11.7 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.167.131 | 147.237.76.200 | Netherlands | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.57.11.7 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.167.131 | 147.237.76.147 | Netherlands | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.167.131 | 147.237.72.156 | Netherlands | aman.idf.il | ET SCAN Potential SSH Scan | 1 |
| 203.197.205.118 | 147.237.76.177 | India | ncore.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 89.248.167.131 | 147.237.0.19 | Netherlands | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 124.65.231.114 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.29.72.179 | 147.237.72.166 | Israel | aka.idf.il | LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file | 1 |
| 124.65.231.114 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.167.131 | 147.237.77.234 | Netherlands | halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.167.131 | 147.237.76.202 | Netherlands | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.57.11.7 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.167.131 | 147.237.76.196 | Netherlands | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.57.11.7 | 147.237.76.198 | China | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.248.167.131 | 147.237.76.39 | Netherlands | mobile.meitav.idf.i | ET SCAN Potential SSH Scan | 1 |
| 203.197.205.118 | 147.237.76.177 | India | ncore.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 89.248.167.131 | 147.237.8.24 | Netherlands | e.lifestyle.idf.il | ET SCAN Potential SSH Scan | 1 |

04-16-2016-22:04:07 to 04-16-2016-23:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.107.55.42 | Algeria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30585 |
| 41.107.55.42 | Algeria | 147.237.77.216 | dover.idf.il | drop | | drop | 2501 |
| 41.107.55.42 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 707 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 577 |
| 109.67.55.63 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 221 |
| 212.76.124.19 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 103 |
| 95.86.82.66 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 74 |
| 5.29.141.67 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 69 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 58 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 51 |
| 80.246.133.202 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 49 |
| 41.107.55.42 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 44 |
| 84.108.69.193 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 44 |
| 45.35.64.142 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 84.228.109.235 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 35 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 34 |
| 66.249.93.111 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 31 |
| 109.186.49.99 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 29 |
| 79.181.20.53 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 66.249.79.75 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 66.249.79.89 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 79.177.179.177 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 46.19.86.12 | Israel | 147.237.77.243 | mobile.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 192.241.189.66 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 79.178.238.193 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 109.67.204.178 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 66.249.79.75 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 213.57.204.33 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 16 |
| 84.94.126.182 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 46.19.86.108 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 192.249.66.247 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 46.19.86.217 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 64.233.172.171 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 41.107.25.234 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 13 |
| 174.115.28.30 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 87.69.196.178 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 46.120.36.93 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 109.64.222.60 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 82.166.244.149 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 79.180.204.81 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 2.53.45.168 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 66.249.93.115 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 94.77.196.82 | Saudi Arabia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.85.90 | Israel | 147.237.76.42 | refuah.idf.i | Bad TCP sequence | Invalid ACK number | alert | 12 |
| 37.26.148.161 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 139.162.216.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.55.44.145 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 88 |
| 2.53.172.71 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 19 |
| 46.19.86.155 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 16 |
| 2.55.133.39 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 13 |
| 46.120.3.230 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 11 |
| 109.67.136.10 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 185.120.126.111 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 185.120.126.111 | Block | 6 |
| 185.120.126.111 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized HTTP Method | Block | 5 |
| 46.120.48.21 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.0.48 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.239 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 212.76.104.80 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 2.53.13.236 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 157.55.2.157 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 66.249.78.242 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3048.jpg | Block | 1 |
| 207.46.13.169 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf!»½¿|Т»½¿|Т¢»!»½¿|Т»½¿|Т-»½¿|Т»½¿|Т¢» | Block | 1 |
| 5.39.222.159 | Netherlands | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to 147.237.0.19/ | Block | 1 |
| 157.55.39.163 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/chinuch/ | Block | 1 |
| 94.159.129.161 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/templates/qsystemform/mobile | Block | 1 |
| 66.249.66.121 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2312.jpg | Block | 1 |
| 123.59.59.52 | China | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.mafengwo.cn/894-he/chinuch.aspx | Block | 1 |
| 66.249.78.248 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3384.jpg | Block | 1 |
| 46.121.37.114 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 5.39.222.159 | Netherlands | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/ | Block | 1 |
| 157.55.39.245 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/994-7826-he/nakhal.aspx | Block | 1 |
| 66.249.78.111 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/ | Block | 1 |
| 185.120.126.111 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/ | Block | 1 |
| 46.19.86.12 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 128.232.110.28 | United Kingdom | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 66.249.79.75 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 54.210.18.124 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/robots.txt | Block | 1 |
| 213.57.204.33 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 37.26.149.177 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 109.67.161.250 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/smalim/f | Block | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/70488.pdf | Block | 1 |
| 197.231.221.211 | Liberia | 147.237.77.216 | dover.idf.il | URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js | Block | 1 |
| 149.88.214.201 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 66.249.79.75 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp | Block | 1 |
| 54.220.100.122 | Ireland | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/1048-7888-he/tikshuv.aspx#.vxksqvkrkuk | Block | 1 |
| 185.32.179.180 | Israel | 147.237.77.216 | dover.idf.il | Multiple Untraceable SSL Sessions from 185.32.179.180 (Open Mode) | None | 1 |
| 37.46.39.203 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation Password in mobile.idf.il/sachar/login | Block | 1 |
| 109.160.191.189 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 66.249.78.236 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3379.jpg | Block | 1 |
| 207.46.13.157 | United States | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/894-7860-he | Block | 1 |
| 5.29.72.179 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 5.29.72.179 | Block | 1 |
| 79.178.191.27 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.64.131 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 41.107.55.42 | Algeria | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 123.59.59.52 | China | 147.237.76.39 | mobile.meitav.idf.il | Unauthorized URL Access to www.qyer.com/1428-he/meitav.aspx | Block | 1 |
| 2.53.171.228 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile | Block | 1 |