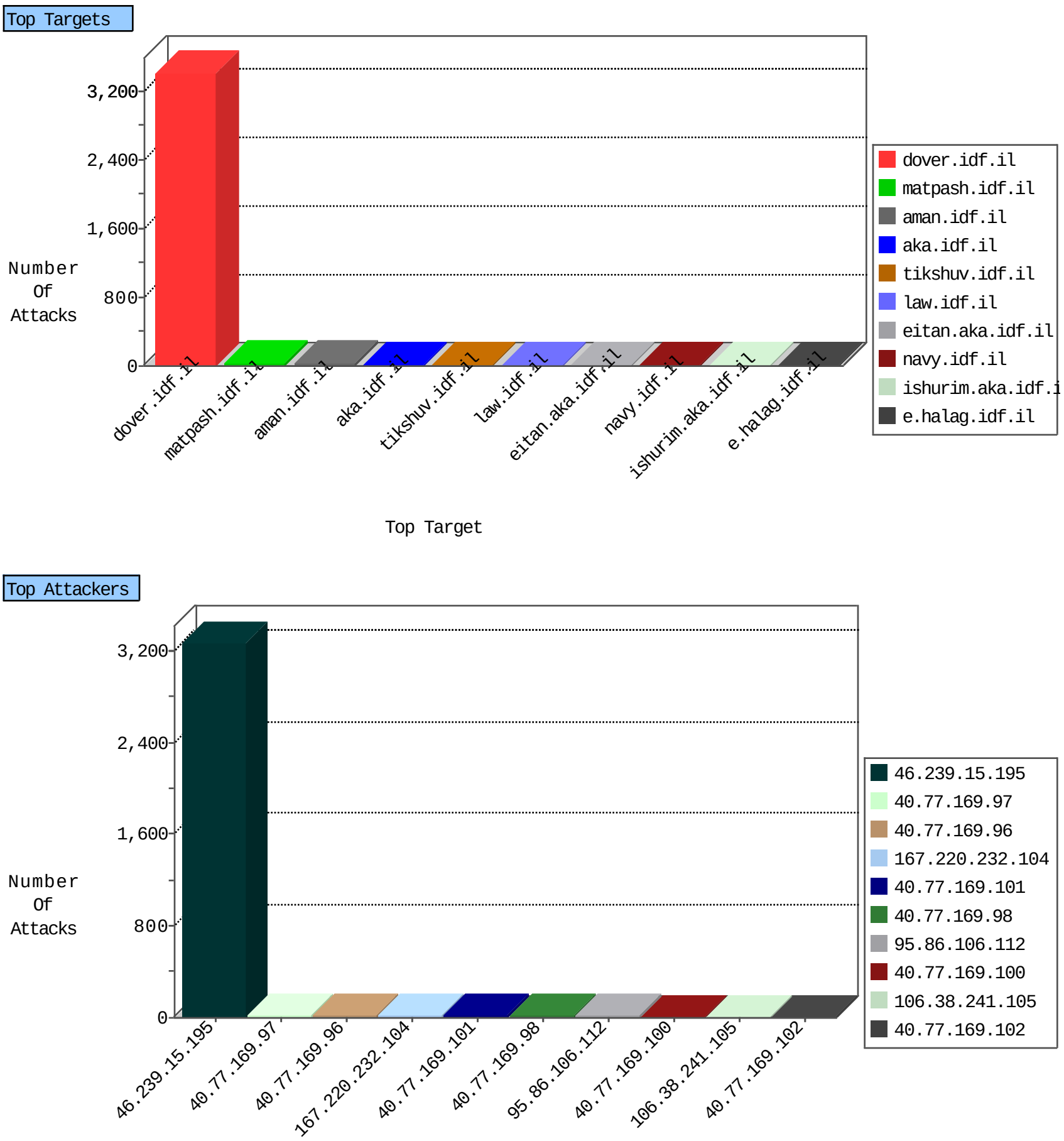
08-28-2016-03:04:08 to 08-28-2016-04:04:08

# IDF Under Attack Daily Report



08-28-2016-03:04:08 to 08-28-2016-04:04:08

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.239.15.195 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | Frk_Under_Attack_Con_Http | drop | 2 |
| 209.93.54.16 | United States | 147.237.76.198 | e.yohalan.idf.il | Black List | drop | 2 |
| 82.80.78.2 | Israel | 147.237.77.176 | matpash.idf.il | Black List | drop | 2 |
| 173.45.67.98 | United States | 147.237.72.167 | ishurim.aka.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |

08-28-2016-03:04:08 to 08-28-2016-04:04:08

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.165.197.142 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 111.202.102.76 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |
| 46.165.197.141 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 1 |

08-28-2016-03:04:08 to 08-28-2016-04:04:08

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 91.121.132.153 | 147.237.72.166 | France | aka.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 4 |
| 23.97.230.36 | 147.237.77.74 | Netherlands | law.idf.il | SQL Injection - Select From | 4 |
| 159.203.33.10 | 147.237.76.38 | Canada | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.176.80.201 | 147.237.77.233 | China | atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 123.176.80.201 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 193.201.225.149 | 147.237.76.44 | Ukraine | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 59.100.214.202 | 147.237.72.156 | Australia | aman.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 190.103.31.165 | 147.237.8.27 | Venezuela | e.madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.84.213.146 | 147.237.76.200 | United States | eitan.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 178.217.189.112 | 147.237.72.167 | Poland | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 23.97.231.138 | 147.237.77.74 | Netherlands | law.idf.il | SQL Injection - Select From | 1 |
| 177.200.192.50 | 147.237.76.202 | Brazil | e.halag.idf.il | ET SCAN NMAP -f -sS | 1 |
| 163.172.169.150 | 147.237.8.27 | United Kingdom | e.madim.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 159.203.33.10 | 147.237.77.61 | Canada | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 125.77.28.26 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 123.176.80.201 | 147.237.77.176 | China | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 193.201.225.149 | 147.237.76.39 | Ukraine | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.84.213.146 | 147.237.76.200 | United States | eitan.aka.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 188.19.144.78 | 147.237.77.179 | Russian Federation | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.84.213.146 | 147.237.76.200 | United States | eitan.aka.idf.il | ET SCAN NMAP -f -sS | 1 |
| 177.200.192.50 | 147.237.76.202 | Brazil | e.halag.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 163.172.169.150 | 147.237.8.50 | United Kingdom | e.tikshuv.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 159.203.33.10 | 147.237.77.226 | Canada | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

08-28-2016-03:04:08 to 08-28-2016-04:04:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.239.15.195 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3126 |
| 46.239.15.195 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | | drop | 150 |
| 167.220.232.104 | Japan | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 20 |
| 40.77.169.97 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 17 |
| 40.77.169.96 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 15 |
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 13 |
| 40.77.169.101 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 11 |
| 40.77.169.98 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 10 |
| 40.77.169.102 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 9 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 9 |
| 40.77.169.97 | United States | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 8 |
| 40.77.169.96 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 7 |
| 40.77.169.104 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 6 |
| 40.77.169.103 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 5 |
| 40.77.169.98 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.35 | Israel | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 4 |
| 40.77.169.103 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 3 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 106.38.241.105 | China | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 2 |
| 39.48.121.73 | Pakistan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 106.38.241.105 | China | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 2 |
| 77.139.157.173 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 106.38.241.105 | China | 147.237.76.86 | navy.idf.il | drop | SAM rule | drop | 1 |
| 46.165.197.141 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 128.232.110.28 | United Kingdom | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 106.38.241.105 | China | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 1 |
| 106.38.241.105 | China | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 1 |
| 159.203.33.10 | Canada | 147.237.0.35 | akaws.idf.il | drop | | drop | 1 |
| 106.38.241.105 | China | 147.237.77.170 | maarachot.idf.il | drop | SAM rule | drop | 1 |
| 40.77.169.98 | United States | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 1 |
| 106.38.241.105 | China | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 1 |
| 173.45.67.98 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 106.38.241.105 | China | 147.237.72.167 | ishurim.aka.idf.il | drop | SAM rule | drop | 1 |
| 106.38.241.105 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |

08-28-2016-03:04:08 to 08-28-2016-04:04:08

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 95.86.106.112 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/modiin/undefined | Block | 14 |
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.76.83 | Block | 3 |
| 131.253.25.231 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 213.151.35.214 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx | Block | 2 |
| 66.249.82.94 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 40.77.169.99 | United States | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 66.249.88.157 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 46.121.63.50 | Israel | 147.237.76.42 | refuah.idf.i | Unauthorized URL Access to 147.237.76.42/images/shared/mailthis.gif | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 77.138.202.217 | France | 147.237.76.42 | refuah.idf.i | Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx | Block | 1 |
| 66.249.64.12 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/ | Block | 1 |
| 92.37.189.52 | Russian Federation | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/drushim/ | Block | 1 |
| 66.249.64.240 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/navy/navy/articles.aspx | Block | 1 |
| 216.244.66.242 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 1 |
| 66.249.82.88 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 24.20.173.169 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1570-en/dover.aspxi volunteered twice | Block | 1 |
| 95.86.106.112 | Israel | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 95.86.106.112 | Block | 1 |
| 66.249.65.51 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp | Block | 1 |
| 66.249.69.249 | Israel | 147.237.0.34 | tikshuv.idf. | Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx | Block | 1 |

08-28-2016-03:04:08 to 08-28-2016-04:04:08