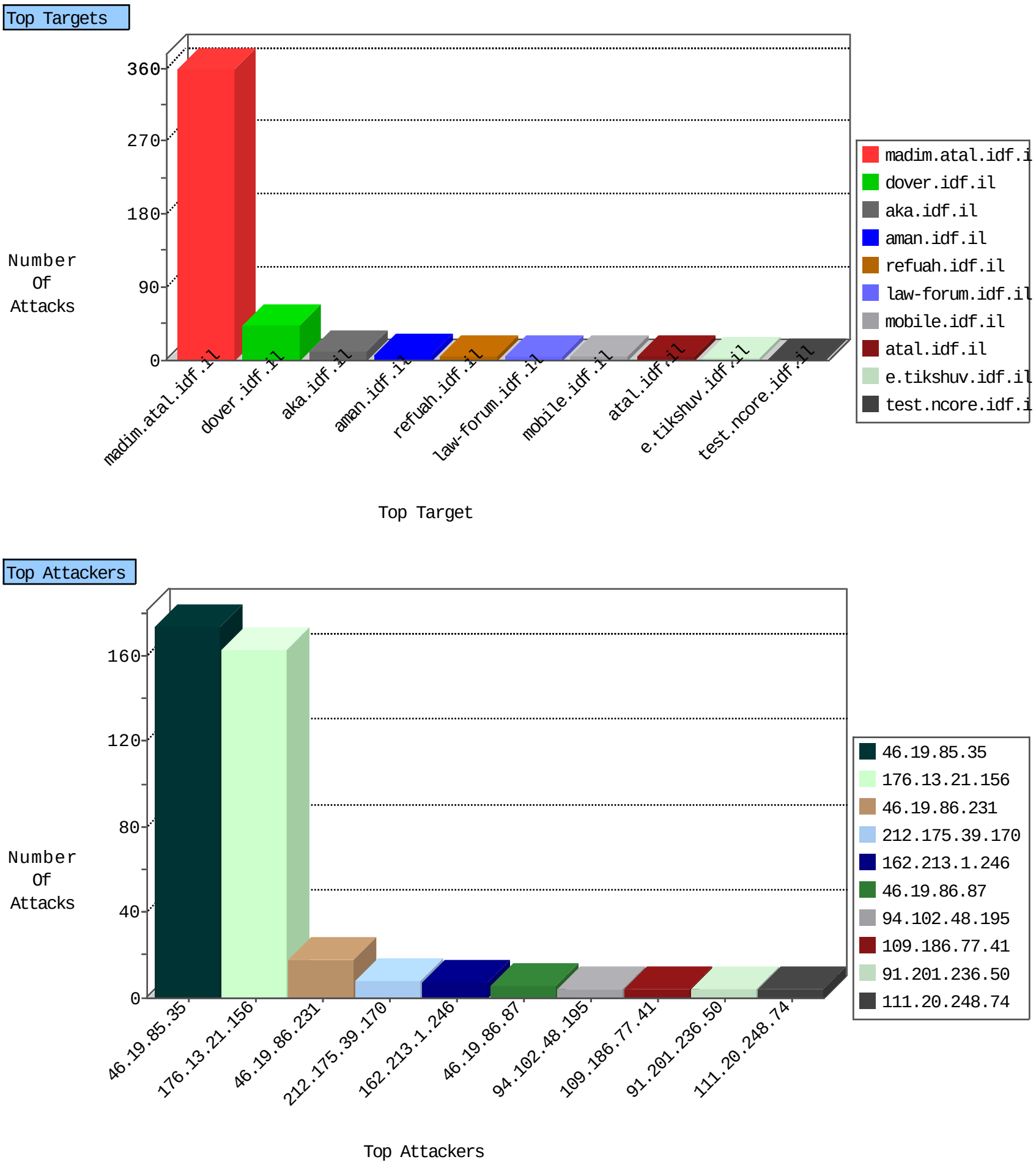
08-20-2016-15:04:01 to 08-20-2016-16:04:01

# IDF Under Attack Daily Report



08-20-2016-15:04:01 to 08-20-2016-16:04:01

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 104.148.55.162 | United States | 147.237.76.39 | mobile.meitav.idf.il | Black List | drop | 1 |
| 82.80.78.2 | Israel | 147.237.76.86 | navy.idf.il | Black List | drop | 1 |

08-20-2016-15:04:01 to 08-20-2016-16:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 197.231.221.211 | Liberia | 147.237.77.216 | dover.idf.il | 24910: HTTP: Python urllib User-Agent Header | Block | 1 |

08-20-2016-15:04:01 to 08-20-2016-16:04:01

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 162.213.1.246 | 147.237.77.216 | United States | dover.idf.il | Tehila - Perl LWP with fake user agent | 7 |
| 66.249.64.113 | 147.237.72.166 | United States | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 41.224.242.127 | 147.237.8.50 | Tunisia | e.tikshuv.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 187.171.212.187 | 147.237.76.30 | Mexico | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 129.56.2.38 | 147.237.72.167 | Nigeria | ishurim.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.48.195 | 147.237.77.19 | Netherlands | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.48.195 | 147.237.76.176 | Netherlands | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.50 | 147.237.77.19 | Ukraine | law-forum.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 91.201.236.50 | 147.237.77.19 | Ukraine | law-forum.idf.il | ET SCAN NMAP -f -sS | 1 |
| 66.249.76.117 | 147.237.72.166 | United States | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 41.224.242.127 | 147.237.8.50 | Tunisia | e.tikshuv.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 193.201.225.149 | 147.237.76.202 | Ukraine | e.halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 41.224.242.127 | 147.237.8.50 | Tunisia | e.tikshuv.idf.il | ET SCAN NMAP -f -sS | 1 |
| 117.135.131.60 | 147.237.76.176 | China | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.102.48.195 | 147.237.76.198 | Netherlands | e.yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.48.195 | 147.237.76.147 | Netherlands | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.50 | 147.237.77.19 | Ukraine | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.50 | 147.237.77.19 | Ukraine | law-forum.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |

08-20-2016-15:04:01 to 08-20-2016-16:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.175.39.170 | Turkey | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.86.87 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 6 |
| 111.20.248.74 | China | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 109.186.77.41 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 4 |
| 84.120.159.161 | Spain | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 108.59.8.70 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 84.94.123.153 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 216.243.31.2 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 109.253.128.191 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 212.241.3.81 | Kyrgyzstan | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 1 |
| 93.214.61.37 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.3.232 | Israel | 147.237.0.19 | madim.atal.idf.il | drop | First packet isn't SYN | drop | 1 |
| 216.218.206.118 | United States | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 184.105.247.208 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 216.243.31.2 | United States | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.35 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 174 |
| 176.13.21.156 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 163 |
| 46.19.86.231 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 46.19.86.231 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152 | Block | 4 |
| 131.253.27.64 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 2.55.180.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 156.211.96.245 | Egypt | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 37.26.146.252 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 80.246.130.55 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 77.139.104.116 | France | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.232.50 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 79.177.230.172 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.102.9.76 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 212.241.3.81 | Kyrgyzstan | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/favicon.ico | Block | 1 |
| 109.63.209.11 | Russian Federation | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/pniot.aspx | Block | 1 |
| 66.249.76.117 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 66.102.6.91 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 31.154.81.74 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.181.167.83 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.64.113 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 213.57.221.115 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 109.65.13.3 | Israel | 147.237.72.156 | aman.idf.il | Suspicious Response Code | Block | 1 |
| 68.180.228.231 | United States | 147.237.77.176 | matpash.idf.il | Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx | Block | 1 |
| 66.102.6.92 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 157.55.39.234 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1391-12626-en/dover.aspx | Block | 1 |
| 66.249.64.223 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx | Block | 1 |
| 46.121.96.74 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 109.67.197.208 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 66.102.6.131 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 40.77.167.32 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |
| 84.120.159.161 | Spain | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/history | Block | 1 |
| 66.249.64.227 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/robots.txt | Block | 1 |
| 46.121.96.74 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 2.53.9.117 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 109.186.86.71 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 77.139.104.116 | France | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/favicon.ico | Block | 1 |
| 66.102.6.191 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 90.80.227.59 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.76.115 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1841-22517-he/dover.aspx | Block | 1 |
| 65.49.68.197 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/71929-en/maarachot.aspx | Block | 1 |