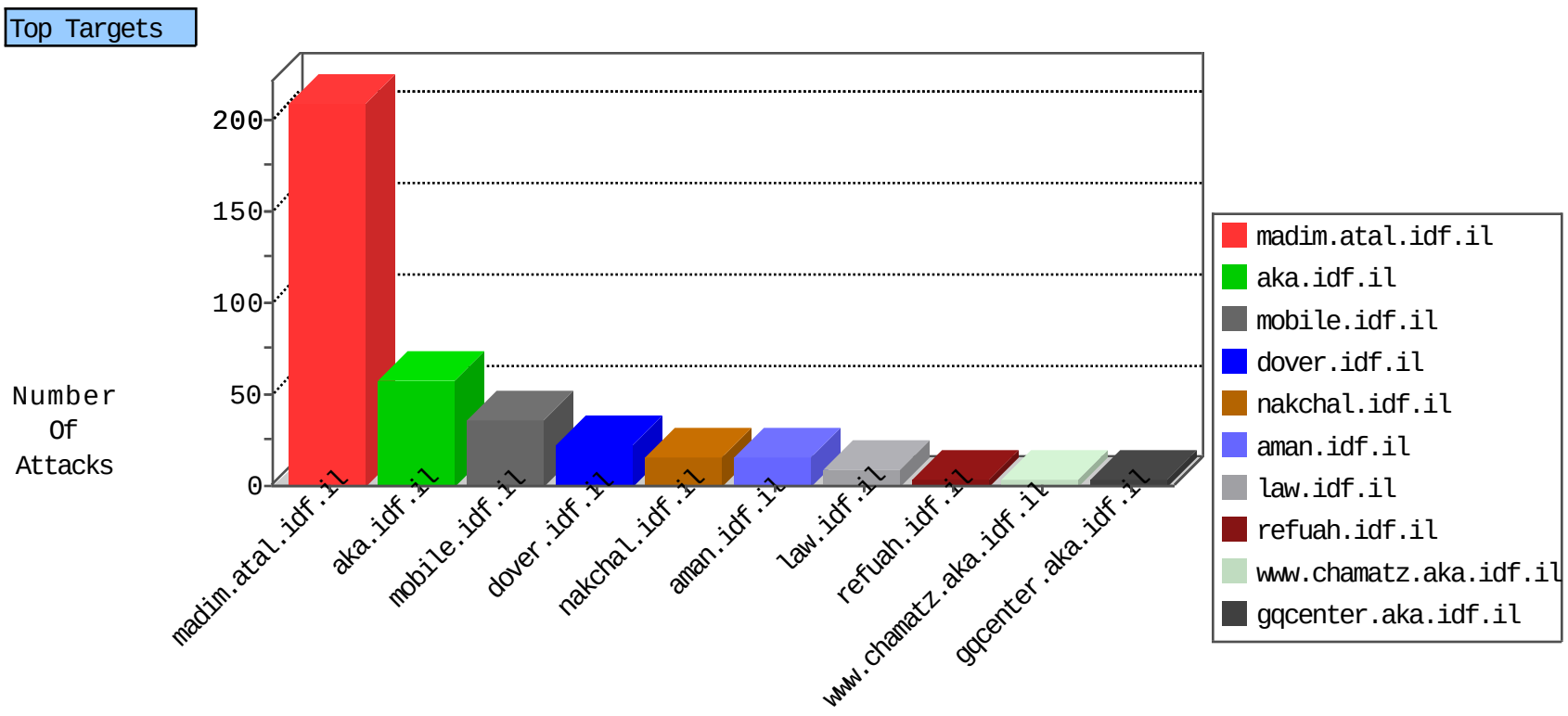
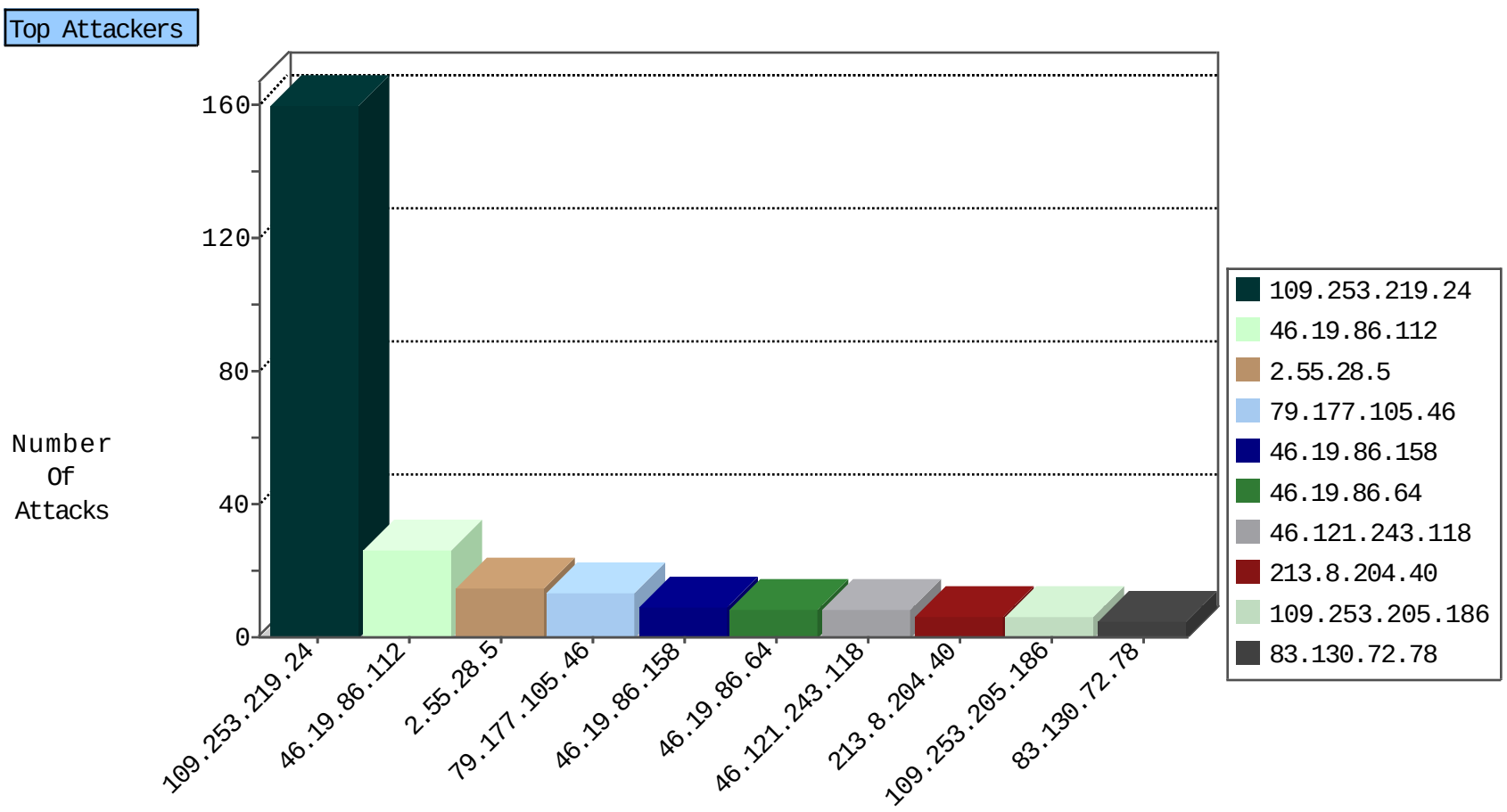
08-30-2016-21:04:05 to 08-30-2016-22:04:05

# IDF Under Attack Daily Report




Top Target




Top Attackers

08-30-2016-21:04:05 to 08-30-2016-22:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.64.19.86 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 185.94.111.1 | Russian Federation | 147.237.76.31 | nakchal.idf.il | Black List | drop | 1 |
| 46.105.96.223 | France | 147.237.76.44 | e.refuah.idf.il | Black List | drop | 1 |
| 91.230.107.174 | Russian Federation | 147.237.76.42 | refuah.idf.il | Black List | drop | 1 |

08-30-2016-21:04:05 to 08-30-2016-22:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

08-30-2016-21:04:05 to 08-30-2016-22:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 185.120.125.112 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.60.153.178 | 147.237.8.24 | Russian Federation | e.lifestyle.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 66.249.79.103 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 46.227.67.172 | 147.237.77.170 | Sweden | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.186.50.250 | 147.237.76.42 | China | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.52.97.86 | 147.237.77.74 | United States | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 1 |
| 115.47.12.162 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 88.249.106.23 | 147.237.76.34 | Turkey | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.116.123.135 | 147.237.76.38 | United States | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.186.50.250 | 147.237.76.202 | China | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 203.86.3.66 | 147.237.76.177 | China | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

08-30-2016-21:04:05 to 08-30-2016-22:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 2.55.28.5 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 14 |
| 83.130.72.78 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 5 |
| 176.12.160.1 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.85.47 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 192.169.7.223 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 3 |
| 79.176.28.14 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 176.13.246.180 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 2 |
| 93.172.202.50 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 176.13.231.94 | Israel | 147.237.0.19 | madim.atal.idf.il | drop | First packet isn't SYN | drop | 2 |
| 183.129.160.229 | China | 147.237.72.217 | e.idf.il | drop | SAM rule | drop | 1 |
| 83.130.68.219 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.147.28 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 1 |
| 185.120.125.111 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.9.137 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 178.146.49.116 | Greece | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.196.199 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.16.26 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 85.130.215.232 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 183.129.160.229 | China | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 1 |
| 109.253.198.245 | Israel | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 195.138.201.2 | Slovenia | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.17.136 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 183.129.160.229 | China | 147.237.72.167 | ishurim.aka.idf.il | drop | SAM rule | drop | 1 |
| 109.253.246.39 | Israel | 147.237.76.31 | nakchal.idf.il | drop | First packet isn't SYN | drop | 1 |
| 80.246.133.138 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 207.46.13.149 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.226.40.40 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

08-30-2016-21:04:05 to 08-30-2016-22:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.253.219.24 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 160 |
| 46.19.86.112 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 26 |
| 46.19.86.158 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 79.177.105.46 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized HTTP Method | Block | 7 |
| 109.253.205.186 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 213.8.204.40 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 46.121.243.118 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152 | Block | 5 |
| 79.177.105.46 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/ | Block | 4 |
| 46.121.243.118 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 109.253.215.112 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.71 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 213.8.204.64 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 2.53.168.77 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 213.57.135.38 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.182.132.85 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 86.245.145.126 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim/main/ | Block | 3 |
| 46.116.32.123 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 220.255.148.68 | Singapore | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 85.130.232.183 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 79.177.105.46 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 79.177.105.46 | Block | 2 |
| 66.249.85.221 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 176.13.230.200 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 80.246.133.94 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 207.46.13.93 | United States | 147.237.0.19 | madim.atal.idf.i | Unauthorized URL Access to madim.atal.idf.il/robots.txt | Block | 2 |
| 87.71.29.74 | Israel | 147.237.72.156 | aman.idf.il | Suspicious Response Code | Block | 2 |
| 79.178.140.64 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.64.122 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx | Block | 1 |
| 46.19.86.64 | Israel | 147.237.77.74 | law.idf.il | Unknown HTTP Request Method 1b9048e151f.1472582062.1.1472582062.1472582062.; in URL _pk_ses.115.5e0a=* | Block | 1 |
| 80.246.133.235 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 31.154.81.2 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx | None | 1 |
| 77.139.132.239 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/navy/navy/general.aspx | Block | 1 |
| 66.249.85.218 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 157.55.39.14 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/valtam | Block | 1 |
| 87.204.52.13 | Poland | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico | Block | 1 |
| 79.179.0.151 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/gen204 | Block | 1 |
| 46.19.86.64 | Israel | 147.237.77.74 | law.idf.il | Multiple Abnormally Long Request from 46.19.86.64 | Block | 1 |
| 2.53.37.222 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 185.110.110.37 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 77.126.8.138 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 1 |
| 66.249.66.107 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.66.107 | Block | 1 |
| 37.46.38.87 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 157.55.39.245 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 94.77.172.158 | Russian Federation | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx | Block | 1 |
| 79.179.149.21 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 46.19.86.64 | Israel | 147.237.77.74 | law.idf.il | Multiple Illegal HTTP Version from 46.19.86.64 | Block | 1 |
| 192.169.7.223 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized Method HEAD for 147.237.76.42/ | Block | 1 |
| 77.138.9.5 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx | Block | 1 |
| 66.249.66.107 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association | Block | 1 |
| 85.250.70.155 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 1 |
| 46.19.86.64 | Israel | 147.237.77.74 | law.idf.il | Abnormally Long Request method | Block | 1 |

08-30-2016-21:04:05 to 08-30-2016-22:04:05