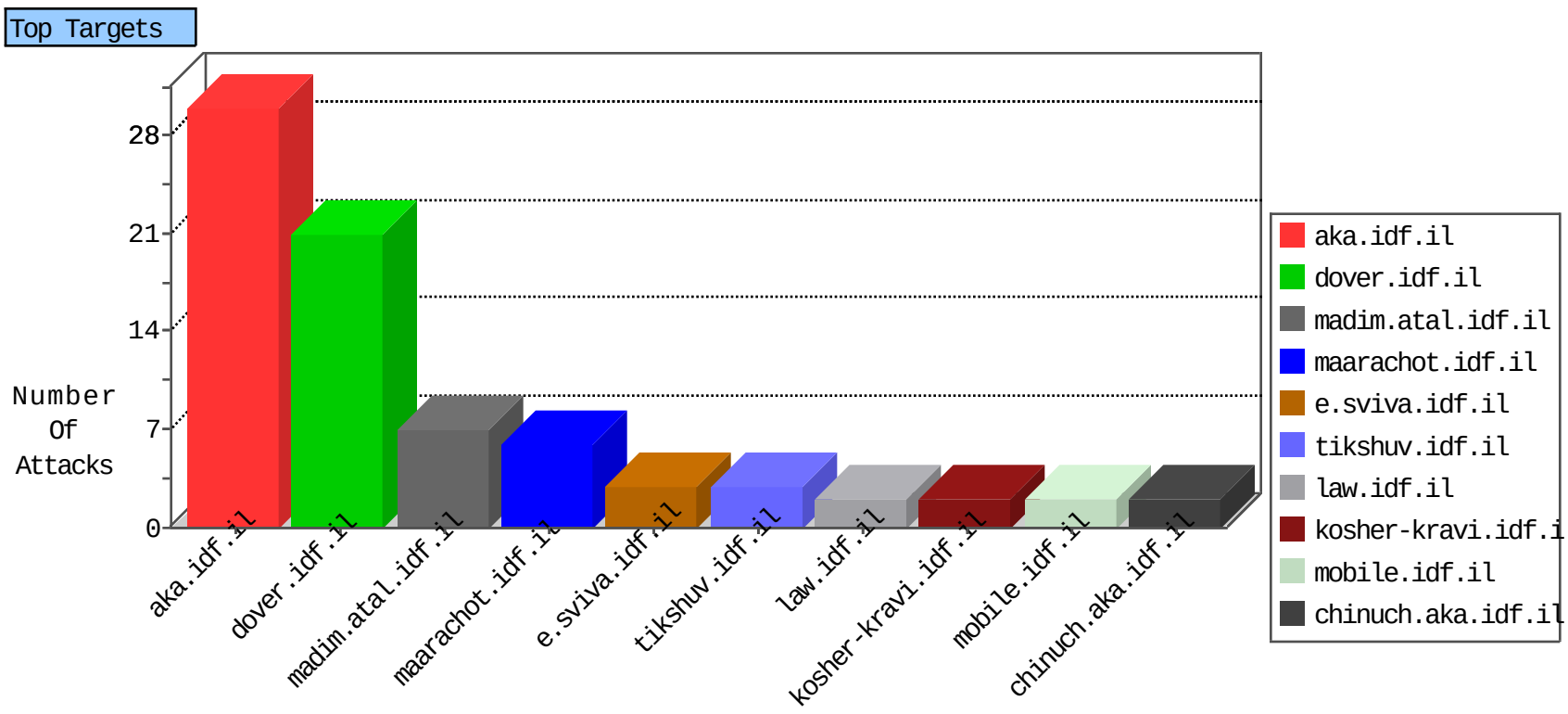
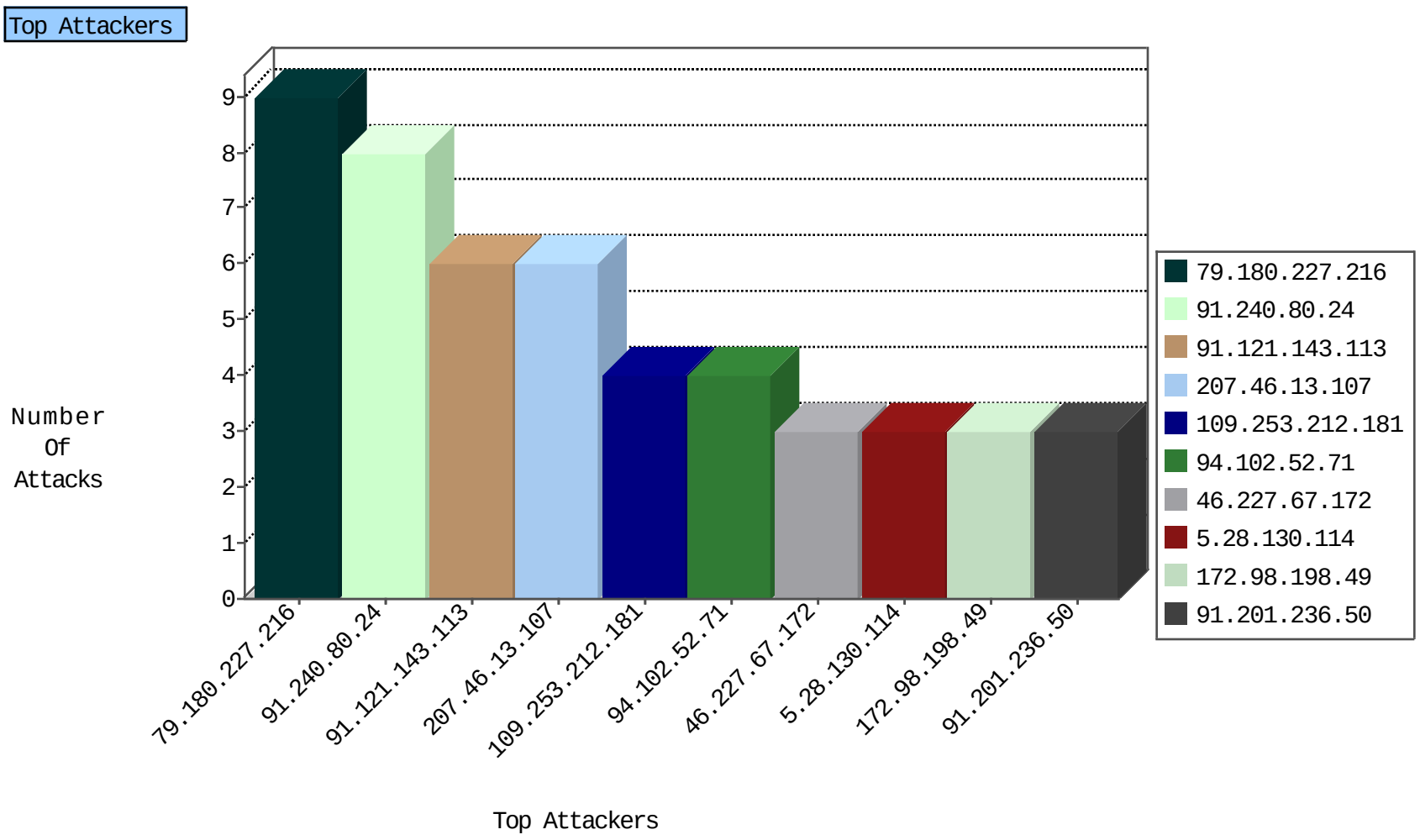
09-03-2016-01:08:02 to 09-03-2016-02:08:02

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-03-2016-01:08:02 to 09-03-2016-02:08:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 190.13.55.190 | Colombia | 147.237.77.170 | maarachot.idf.il | Invalid L4 Header Length | drop | 2 |
| 217.23.9.123 | Netherlands | 147.237.76.202 | e.halag.idf.il | Black List | drop | 1 |
| 115.230.125.146 | China | 147.237.77.216 | dover.idf.il | block-sp-traf1 | forward | 1 |
| 190.13.55.190 | Colombia | 147.237.77.170 | maarachot.idf.il | Invalid TCP Flags | drop | 1 |

09-03-2016-01:08:02 to 09-03-2016-02:08:02

## Top Attackers In IPS

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

09-03-2016-01:08:02 to 09-03-2016-02:08:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 91.121.143.113 | 147.237.72.166 | France | aka.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 6 |
| 195.154.184.122 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 46.227.67.172 | 147.237.76.34 | Sweden | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.169.150 | 147.237.0.15 | United Kingdom | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 5.255.90.133 | 147.237.0.19 | Netherlands | madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 116.12.175.233 | 147.237.76.196 | Singapore | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 104.128.144.131 | 147.237.77.234 | Canada | halag.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 94.102.52.71 | 147.237.77.243 | Netherlands | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.52.71 | 147.237.77.216 | Netherlands | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.50 | 147.237.0.19 | Ukraine | madim.atal.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 183.82.106.200 | 147.237.76.147 | India | chinuch.aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 91.201.236.50 | 147.237.0.19 | Ukraine | madim.atal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 172.98.198.49 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 46.227.67.172 | 147.237.76.39 | Sweden | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 172.98.198.49 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -f -sS | 1 |
| 46.227.67.172 | 147.237.0.34 | Sweden | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 116.12.175.233 | 147.237.76.196 | Singapore | e.sviva.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 116.12.175.233 | 147.237.76.196 | Singapore | e.sviva.idf.il | ET SCAN NMAP -f -sS | 1 |
| 103.207.39.11 | 147.237.77.178 | Vietnam | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.52.71 | 147.237.77.226 | Netherlands | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.52.71 | 147.237.77.179 | Netherlands | e.mazi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 190.69.215.85 | 147.237.0.35 | Colombia | akaws.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 91.201.236.50 | 147.237.0.19 | Ukraine | madim.atal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 183.82.106.200 | 147.237.76.147 | India | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 172.98.198.49 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sS window 2048 | 1 |

09-03-2016-01:08:02 to 09-03-2016-02:08:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 79.180.227.216 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 9 |
| 91.240.80.24 | Lebanon | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 207.46.13.107 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.253.212.181 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 183.129.160.229 | China | 147.237.0.15 | kosher-kravi.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.0.16 | my-kosher-kravi.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 1 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

09-03-2016-01:08:02 to 09-03-2016-02:08:02

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 5.28.130.114 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.76.83 | Block | 2 |
| 46.117.131.183 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 84.111.42.118 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 1 |
| 66.249.64.105 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json | Block | 1 |
| 66.249.76.112 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/apple-app-site-association | Block | 1 |
| 84.111.42.118 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx | None | 1 |
| 66.249.64.245 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/templates/general/general.aspx | Block | 1 |
| 77.138.203.153 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx | Block | 1 |
| 46.4.15.197 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp | Block | 1 |
| 157.55.39.70 | United States | 147.237.77.243 | mobile.idf.il | Suspicious Response Code | Block | 1 |
| 66.249.76.75 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.76.75 | Block | 1 |
| 77.237.138.202 | Czech Republic | 147.237.77.235 | sviva.idf.il | Unauthorized Method HEAD for / | Block | 1 |
| 46.19.85.207 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx | Block | 1 |
| 82.81.10.63 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.76.112 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.76.112 | Block | 1 |

09-03-2016-01:08:02 to 09-03-2016-02:08:02