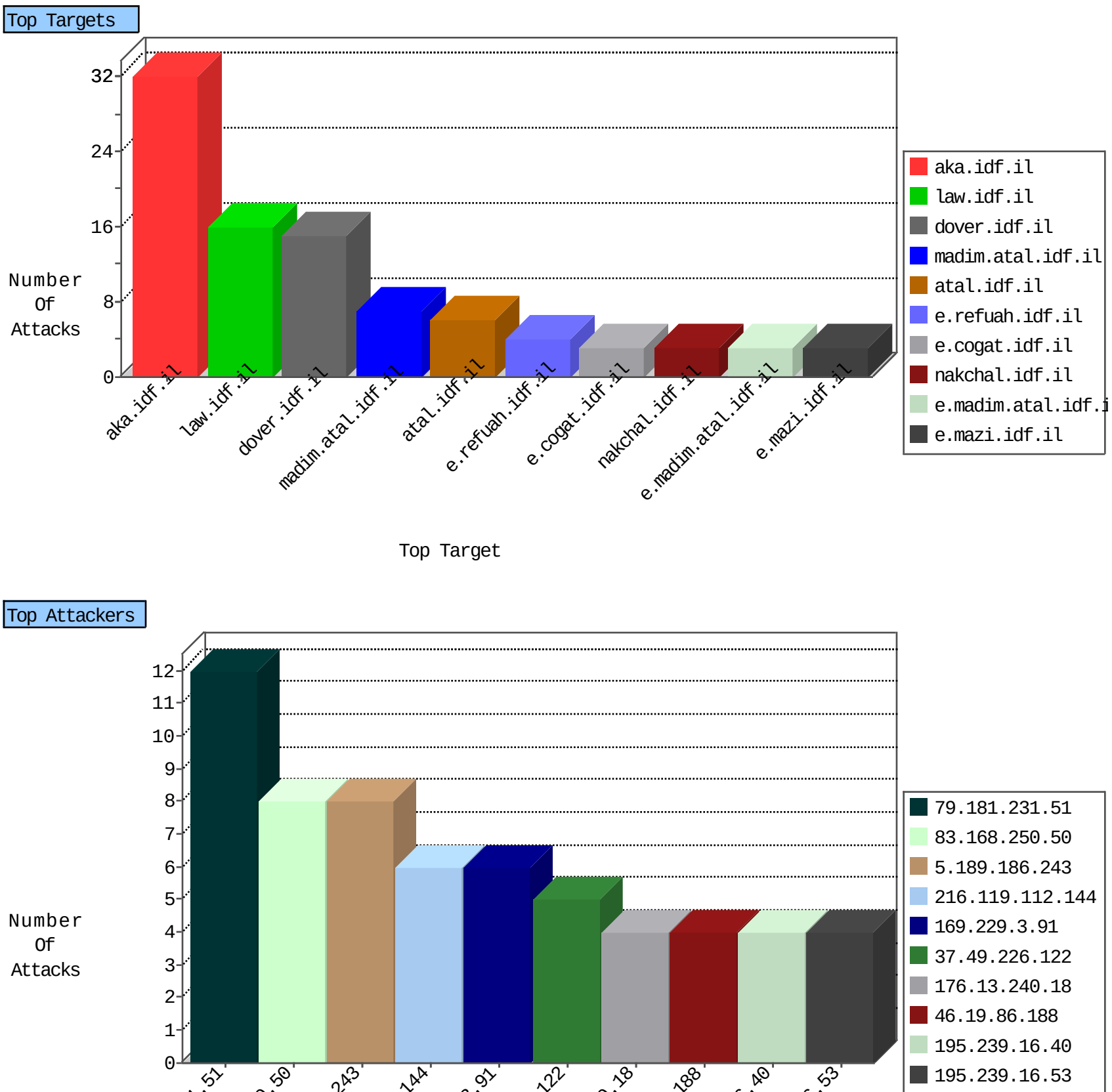
09-02-2016-00:04:07 to 09-02-2016-01:04:07

# IDF Under Attack
# Daily Report



09-02-2016-00:04:07 to 09-02-2016-01:04:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 218.92.147.81 | China | 147.237.0.34 | tikshuv.idf.il | Frk_Under_Attack_Con_Tcp | drop | 2 |
| 94.156.128.101 | Bulgaria | 147.237.76.38 | e.e.meitav.idf.il | Black List | drop | 1 |
| 5.189.186.243 | Germany | 147.237.76.147 | chinuch.aka.idf.il | Black List | drop | 1 |
| 185.25.33.140 | United Kingdom | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 1 |
| 5.189.186.243 | Germany | 147.237.76.201 | e.atal.idf.il | Black List | drop | 1 |
| 109.236.84.10 | Netherlands | 147.237.76.197 | e.himush.idf.il | Black List | drop | 1 |
| 5.189.186.243 | Germany | 147.237.76.148 | gqcenter.aka.idf.il | Black List | drop | 1 |
| 5.189.186.243 | Germany | 147.237.76.202 | e.halag.idf.il | Black List | drop | 1 |
| 5.189.186.243 | Germany | 147.237.76.30 | himush.idf.il | Black List | drop | 1 |
| 141.212.122.96 | United States | 147.237.76.44 | e.refuah.idf.il | Black List | drop | 1 |
| 5.189.186.243 | Germany | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |
| 93.115.28.125 | Romania | 147.237.76.147 | chinuch.aka.idf.il | Black List | drop | 1 |
| 5.189.186.243 | Germany | 147.237.76.31 | nakchal.idf.il | Black List | drop | 1 |
| 185.25.33.139 | United Kingdom | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 1 |
| 5.189.186.243 | Germany | 147.237.76.177 | ncore.idf.il | Black List | drop | 1 |

09-02-2016-00:04:07 to 09-02-2016-01:04:07

## Top Attackers In IPS

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

09-02-2016-00:04:07 to 09-02-2016-01:04:07

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 83.168.250.50 | 147.237.77.74 | Sweden | law.idf.il | SQL Injection - Select From | 8 |
| 46.120.122.219 | 147.237.77.176 | Israel | matpash.idf.il | Xenu Link Sleuth User Agent | 2 |
| 91.201.236.155 | 147.237.77.179 | Ukraine | e.mazi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 71.36.27.214 | 147.237.76.44 | United States | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.49.226.122 | 147.237.76.147 | Netherlands | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 190.196.178.78 | 147.237.77.61 | Chile | e.cogat.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 37.49.226.122 | 147.237.76.42 | Netherlands | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 190.196.178.78 | 147.237.77.61 | Chile | e.cogat.idf.il | ET SCAN NMAP -f -sS | 1 |
| 37.49.226.122 | 147.237.0.15 | Netherlands | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.197.206.193 | 147.237.8.27 | United States | e.madim.atal.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 104.197.206.193 | 147.237.8.27 | United States | e.madim.atal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 91.201.236.155 | 147.237.77.179 | Ukraine | e.mazi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 86.195.158.36 | 147.237.0.17 | France | m.my-kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 71.36.27.214 | 147.237.76.44 | United States | e.refuah.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 37.49.226.122 | 147.237.76.44 | Netherlands | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 190.196.178.78 | 147.237.77.61 | Chile | e.cogat.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 37.49.226.122 | 147.237.0.16 | Netherlands | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 122.224.250.234 | 147.237.76.38 | China | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 104.197.206.193 | 147.237.8.27 | United States | e.madim.atal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 91.201.236.155 | 147.237.77.179 | Ukraine | e.mazi.idf.il | ET SCAN NMAP -sS window 4096 | 1 |

09-02-2016-00:04:07 to 09-02-2016-01:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 216.119.112.144 | United States | 147.237.77.233 | atal.idf.il | drop | SAM rule | drop | 6 |
| 195.239.16.40 | Russian Federation | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 4 |
| 195.239.16.53 | Russian Federation | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.188 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 176.13.240.18 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 2.54.96.22 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 185.21.123.203 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 165.215.209.15 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 141.212.122.57 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.244.95 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 1 |
| 141.212.122.58 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 169.229.3.91 | United States | 147.237.76.196 | e.sviva.idf.il | drop | First packet isn't SYN | drop | 1 |
| 177.57.222.117 | Brazil | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 169.229.3.91 | United States | 147.237.76.201 | e.atal.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 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.il | drop | First packet isn't SYN | drop | 1 |
| 197.48.157.2 | Egypt | 147.237.77.243 | mobile.idf.il | drop | First packet isn't SYN | drop | 1 |
| 169.229.3.91 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 183.129.160.229 | China | 147.237.72.217 | e.idf.il | drop | SAM rule | drop | 1 |
| 169.229.3.91 | United States | 147.237.0.200 | m4u.idf.il | drop | First packet isn't SYN | drop | 1 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

09-02-2016-00:04:07 to 09-02-2016-01:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.181.231.51 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 8 |
| 77.138.43.198 | France | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 79.181.231.51 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 79.181.231.51 | Block | 4 |
| 108.211.201.46 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar | Block | 3 |
| 87.69.164.184 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 198.20.69.74 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 89.139.175.46 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/robots.txt | Block | 1 |
| 192.243.55.131 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/tizmoret/news | Block | 1 |
| 207.46.13.102 | 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 |
| 71.92.40.56 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/giyus/login/ | Block | 1 |
| 192.243.55.132 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/chinuch/gallery | Block | 1 |
| 79.183.117.75 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.69.14 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp | Block | 1 |
| 109.66.129.21 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc | Block | 1 |
| 192.243.55.133 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.133 | Block | 1 |
| 80.246.133.7 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 66.249.69.127 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 157.55.39.175 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/miluim/templa...172&docid=57698 | Block | 1 |
| 77.138.114.122 | France | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/favicon.ico | Block | 1 |
| 192.243.55.133 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/eitan/tmuna/?pictype=2&docid=32948 | Block | 1 |
| 66.249.76.39 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx | None | 1 |
| 192.198.151.45 | Europe | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim/main/ | Block | 1 |

09-02-2016-00:04:07 to 09-02-2016-01:04:07