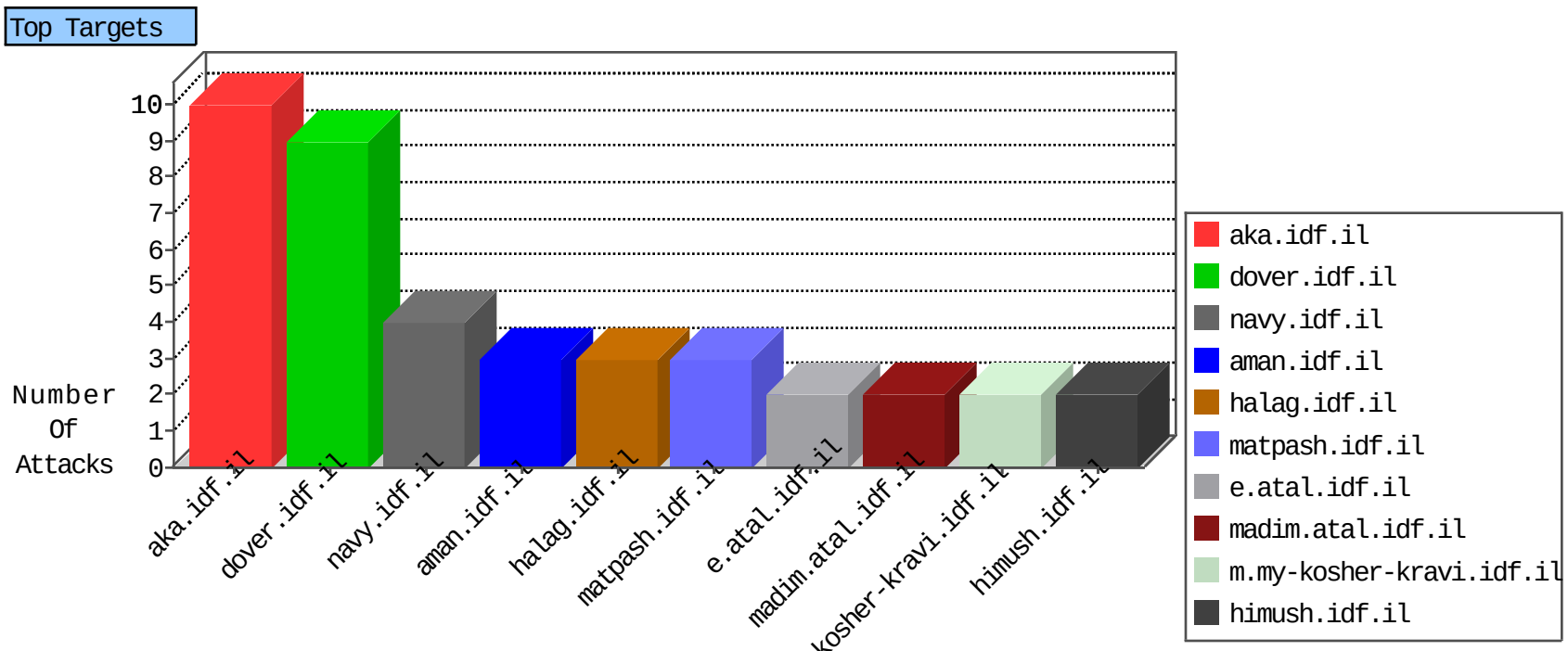
08-19-2016-06:04:00 to 08-19-2016-07:04:00

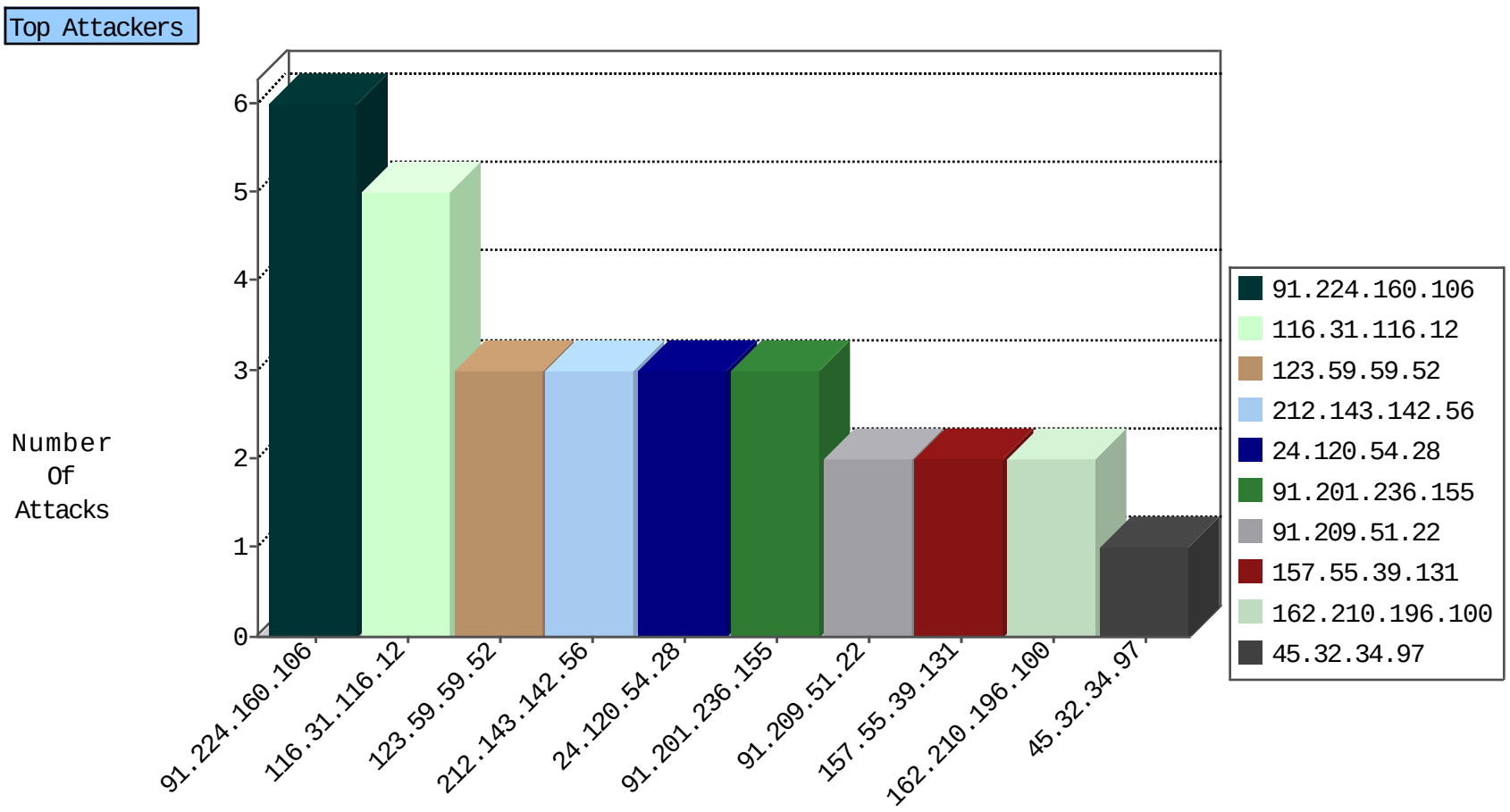
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

08-19-2016-06:04:00 to 08-19-2016-07:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 123.59.59.52 | China | 147.237.76.30 | himush.idf.il | block-sp-traf1 | forward | 2 |
| 116.31.116.12 | China | 147.237.76.201 | e.atal.idf.il | JLM_Under_Attack_Con_Tcp | drop | 2 |
| 123.59.59.52 | China | 147.237.77.216 | dover.idf.il | block-sp-traf1 | forward | 1 |
| 45.32.34.97 | Netherlands | 147.237.0.19 | madim.atal.idf.il | L4 Source or Dest Port Zero | drop | 1 |

08-19-2016-06:04:00 to 08-19-2016-07:04:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 162.210.196.100 | United States | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 94.102.49.193 | Netherlands | 147.237.72.166 | aka.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |
| 46.165.197.141 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 1 |
| 71.6.167.142 | United States | 147.237.8.28 | e.mobile-ks.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

08-19-2016-06:04:00 to 08-19-2016-07:04:00

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 116.31.116.12 | 147.237.76.86 | China | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.76.86 | Netherlands | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.76.31 | Netherlands | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.0.19 | Netherlands | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.155 | 147.237.77.234 | Ukraine | halag.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 91.201.236.155 | 147.237.77.234 | Ukraine | halag.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 116.31.116.12 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 116.31.116.12 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.76.34 | Netherlands | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.0.35 | Netherlands | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.160.106 | 147.237.0.17 | Netherlands | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.155 | 147.237.77.234 | Ukraine | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

08-19-2016-06:04:00 to 08-19-2016-07:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 24.120.54.28 | United States | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 3 |
| 91.209.51.22 | Ukraine | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 2 |

08-19-2016-06:04:00 to 08-19-2016-07:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 157.55.39.131 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 2 |
| 108.63.172.142 | Canada | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 204.79.180.54 | 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 |
| 66.249.76.47 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/giyus/hebrew/html/1 | Block | 1 |
| 131.253.27.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 204.79.180.231 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx | Block | 1 |
| 66.249.76.51 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp | Block | 1 |
| 66.249.64.176 | Israel | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 66.249.64.176 | Block | 1 |
| 66.249.76.52 | Israel | 147.237.72.166 | aka.idf.il | Double URL Encoding - parameter: catId%5Cu003d58624 in www.aka.idf.il/main/giyus/general.aspx | Block | 1 |
| 157.55.39.238 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/console/core/doc_mgr/undefined | Block | 1 |
| 66.249.64.183 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp | Block | 1 |
| 66.249.79.170 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 1 |
| 190.39.233.71 | Venezuela | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.69.253 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx | Block | 1 |

08-19-2016-06:04:00 to 08-19-2016-07:04:00