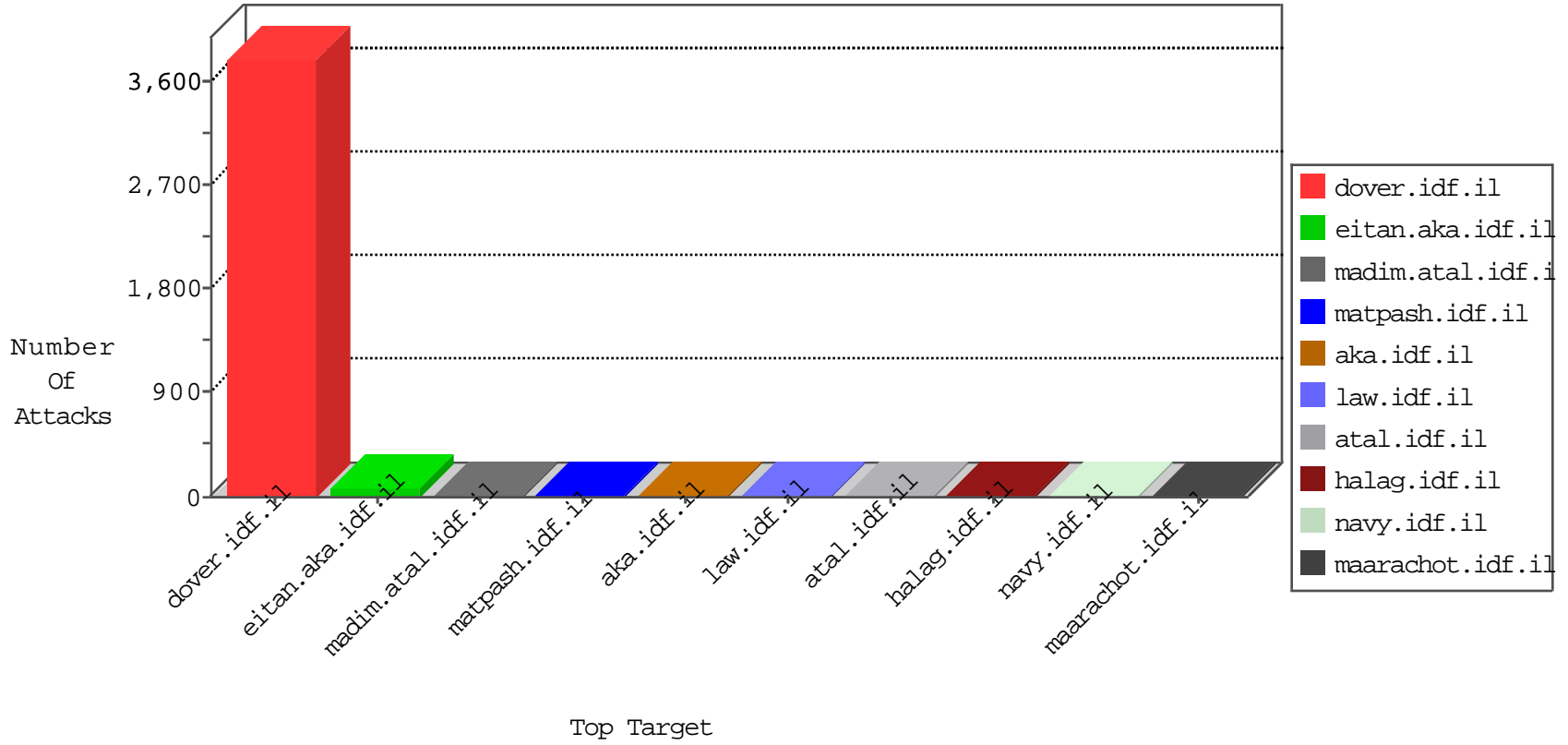


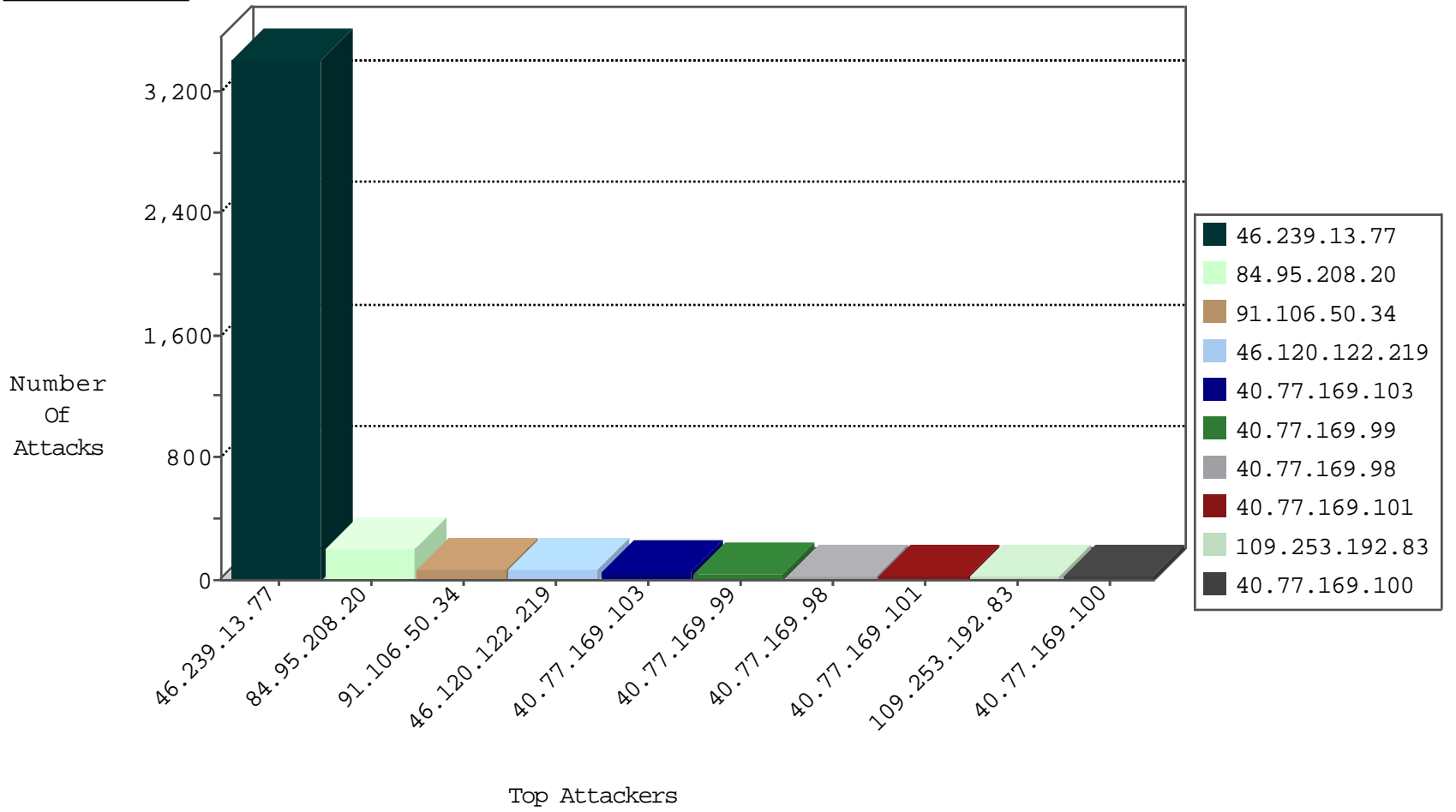
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|----------------------|------------|---------------|-------|
| 104.148.35.34 | United States | 147.237.76.39 | mobile.meitav.idf.il | Black List | drop | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|--------------|------------------------------|---------------|-------|
| 69.30.198.186 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 83.149.126.98 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 1 |

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|------------------|----------------|------------------|---------------------|------------------------------|-------|
| 46.120.122.219 | 147.237.77.216 | Israel | dover.idf.il | Xenu Link Sleuth User Agent | 31 |
| 46.120.122.219 | 147.237.77.74 | Israel | law.idf.il | Xenu Link Sleuth User Agent | 18 |
| 46.120.122.219 | 147.237.76.86 | Israel | navy.idf.il | Xenu Link Sleuth User Agent | 10 |
| 46.120.122.219 | 147.237.77.170 | Israel | maarachot.idf.il | Xenu Link Sleuth User Agent | 4 |
| 46.227.67.172 | 147.237.76.199 | Sweden | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 202.74.244.202 | 147.237.72.166 | Bangladesh | aka.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 142.54.191.210 | 147.237.76.147 | United States | chinuch.aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 106.186.20.183 | 147.237.0.15 | Japan | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 202.74.244.202 | 147.237.72.166 | Bangladesh | aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 202.74.244.202 | 147.237.72.166 | Bangladesh | aka.idf.il | ET SCAN NMAP -f -sS | 1 |
| 142.54.191.210 | 147.237.76.147 | United States | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------------|----------------|--------------------------|-----------|------------------------|---------------|-------|
| 46.239.13.77 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3163 |
| 46.239.13.77 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | | drop | 250 |
| 91.106.50.34 | Iraq | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 69 |
| 40.77.169.99 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 40 |
| 40.77.169.98 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 28 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 20 |
| 40.77.169.103 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 16 |
| 40.77.169.103 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 13 |
| 40.77.169.103 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 11 |
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 10 |
| 40.77.169.97 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 10 |
| 167.220.232.104 | Japan | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 10 |
| 40.77.169.100 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 6 |
| 40.77.169.102 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 6 |
| 40.77.169.102 | United States | 147.237.77.234 | halag.idf.il | drop | SAM rule | drop | 6 |
| 40.77.169.103 | United States | 147.237.77.234 | halag.idf.il | drop | SAM rule | drop | 5 |
| 104.158.35.213 | Canada | 147.237.77.216 | dover.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 |
| 183.129.160.229 | China | 147.237.77.19 | law-forum.idf.il | drop | SAM rule | drop | 1 |
| 128.232.110.28 | United Kingdom | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 183.129.160.229 | China | 147.237.77.61 | e.cogat.idf.il | drop | SAM rule | drop | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 169.229.3.91 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | drop | SAM rule | drop | 1 |
| 212.143.165.117 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 94.40.75.10 | Poland | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | drop | SAM rule | drop | 1 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|------------------------|---|---------------|-------|
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 103 |
| 84.95.208.20 | Israel | 147.237.76.200 | eitan.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 84 |
| 109.253.192.83 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 19 |
| 84.95.208.20 | Israel | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 8 |
| 84.95.208.20 | Israel | 147.237.77.233 | atal.idf.il | Distributed PHP Attempt | Block | 6 |
| 46.19.86.121 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 219.75.81.93 | Singapore | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 2 |
| 40.77.169.96 | United States | 147.237.77.216 | dover.idf.il | Multiple Illegal Byte Code Character in URL from 40.77.169.96 | Block | 2 |
| 66.249.75.24 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3480.jpg | Block | 1 |
| 46.19.86.4 | Israel | 147.237.77.216 | dover.idf.il | Abnormally Long Request request version | Block | 1 |
| 68.180.230.171 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx | Block | 1 |
| 65.55.210.119 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 2.53.133.110 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 46.19.86.4 | Israel | 147.237.77.216 | dover.idf.il | Illegal HTTP Version Safari/601.1 | Block | 1 |
| 220.255.145.120 | Singapore | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 84.95.208.20 | Israel | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 66.249.64.108 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/sfgsfdfs.aspx | Block | 1 |
| 37.214.21.221 | Belarus | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_ | Block | 1 |
| 46.19.86.4 | Israel | 147.237.77.216 | dover.idf.il | Malformed URL mobile/13g35 | Block | 1 |
| 66.249.75.8 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2388.jpg | Block | 1 |
| 40.77.169.96 | United States | 147.237.77.170 | maarachot.idf.il | Multiple Illegal Byte Code Character in URL from 40.77.169.96 | Block | 1 |
| 66.249.79.130 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx | Block | 1 |
| 46.19.86.4 | Israel | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method 0 in URL mobile/13g35 | Block | 1 |
| 66.249.75.16 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2367.jpg | Block | 1 |
| 176.126.252.12 | Romania | 147.237.77.176 | matpash.idf.il | Too Many Cookies in a Request - 223 cookies | Block | 1 |
| 66.249.79.138 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |