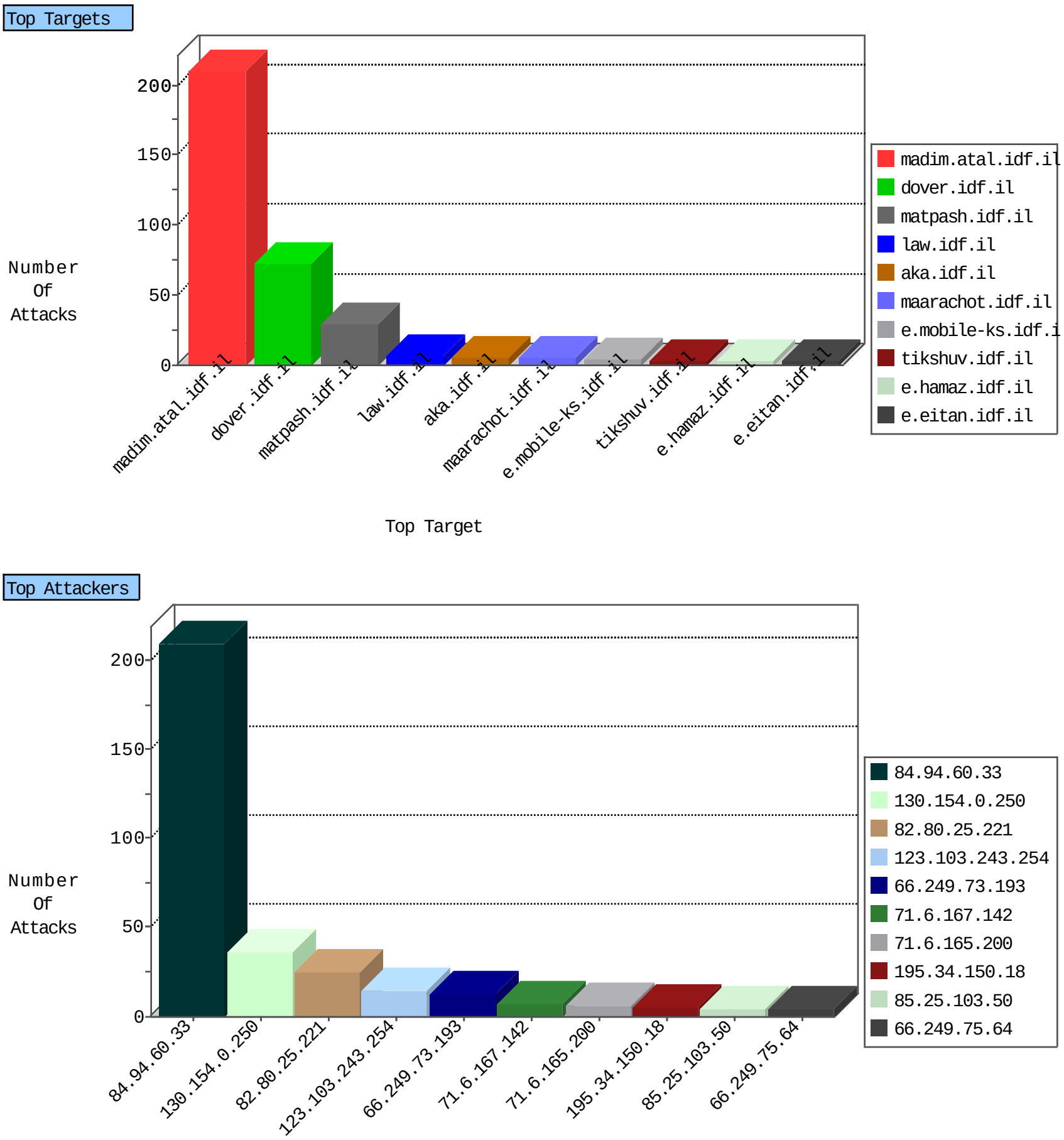
04-25-2015-02:03:07 to 04-25-2015-03:03:07

# IDF Under Attack
# 04-25-2015-02:03:07



04-25-2015-02:03:07 to 04-25-2015-03:03:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Web Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 220.181.108.154 | China | 147.237.76.42 | refuah.idf.il | TCP handshake violation, first packet not syn | drop | 402 |
| 220.181.108.181 | China | 147.237.76.86 | navy.idf.il | TCP handshake violation, first packet not syn | drop | 98 |

04-25-2015-02:03:07 to 04-25-2015-03:03:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 71.6.167.142 | United States | 147.237.76.42 | refuah.idf.il | DVRep_B-N_60_100 | Block | 2 |
| 85.25.103.50 | Germany | 147.237.76.198 | e.yohalan.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.77.243 | mobile.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.77.121 | e.navy.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.0.200 | m4u.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.76.201 | e.atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.8.24 | e.lifestyle.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.77.176 | matpash.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.72.14 | dover.idf.il(old) | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.77.179 | e.mazi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.8.27 | e.madim.atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 46.19.85.161 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 1 |
| 85.25.43.94 | Germany | 147.237.76.197 | e.himush.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.76.201 | e.atal.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 93.120.27.62 | Romania | 147.237.77.179 | e.mazi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 66.240.192.138 | United States | 147.237.72.167 | ishurim.aka.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 85.25.103.50 | Germany | 147.237.0.16 | my-kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.77.205 | prisha.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.167.142 | United States | 147.237.76.197 | e.himush.idf.il | DVRep_B-N_60_100 | Block | 1 |
| 71.6.165.200 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | DVRep_B-N_60_100 | Block | 1 |

04-25-2015-02:03:07 to 04-25-2015-03:03:07

## Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|---|---|---|---|---|---|
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 25 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 5 |
| 66.249.75.64 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 66.249.75.68 | United States | 147.237.77.74 | law.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 109.67.138.70 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 82.166.91.43 | Israel | 147.237.77.227 | e.hamaz.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.121 | e.navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.61 | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 193.107.16.206 | Russian Federation | 147.237.8.50 | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 119.90.139.71 | China | 147.237.76.199 | e.nakchal.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 61.240.144.67 | China | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.243 | mobile.idf.il | ET SCAN Potential SSH Scan | 1 |
| 117.74.137.59 | China | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 61.183.128.6 | China | 147.237.77.234 | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.234 | halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 117.74.137.59 | China | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN NMAP -f -sS | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.227 | e.hamaz.idf.il | ET SCAN Potential SSH Scan | 1 |
| 107.178.216.227 | United States | 147.237.76.148 | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.205 | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 88.204.187.90 | Kazakstan | 147.237.8.45 | e.eitan.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.178 | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 88.204.187.90 | Kazakstan | 147.237.8.45 | e.eitan.idf.il | ET SCAN NMAP -f -sS | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.170 | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 82.166.91.43 | Israel | 147.237.77.227 | e.hamaz.idf.il | ET SCAN NMAP -f -sS | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.74 | law.idf.il | ET SCAN Potential SSH Scan | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.19 | law-forum.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.67 | China | 147.237.76.30 | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 182.23.39.210 | Indonesia | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 119.90.139.71 | China | 147.237.76.199 | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.235 | sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 117.74.137.59 | China | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.233 | atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.216 | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 107.178.216.227 | United States | 147.237.76.148 | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.179 | e.mazi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 88.204.187.90 | Kazakstan | 147.237.8.45 | e.eitan.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 123.103.243.254 | Hong Kong | 147.237.77.176 | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |

04-25-2015-02:03:07 to 04-25-2015-03:03:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 130.154.0.250 | United States | 147.237.77.176 | matpash.idf.il | First packet isn't SYN | drop | drop | 27 |
| 66.249.73.193 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 10 |
| 130.154.0.250 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 9 |
| 37.48.120.214 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4 |
| 37.26.148.131 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1 |
| 141.170.211.247 | Algeria | 147.237.77.216 | dover.idf.il | Invalid ACK number | Bad TCP sequence | alert | 1 |

04-25-2015-02:03:07 to 04-25-2015-03:03:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.94.60.33 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 84.94.60.33 | Block | 209 |
| 66.249.73.201 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.201 | Block | 4 |
| 66.249.73.193 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.193 | Block | 3 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 2 |
| 66.249.73.185 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.73.185 | Block | 2 |
| 109.160.248.72 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.69.84 | Israel | 147.237.77.74 | law.idf.il | Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx | None | 1 |
| 185.71.141.23 | | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-ar | Block | 1 |
| 207.46.13.95 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/0205-4.stm | Block | 1 |
| 176.12.144.85 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 188.165.15.13 | France | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 188.165.15.13 | Block | 1 |
| 84.94.60.33 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many 404: Response Code per Session | Block | 1 |
| 5.28.141.232 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 176.12.151.118 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 188.165.15.95 | France | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/1498-he/atal.aspx ÐžÐ± Ñ?Ñ, Ð¾Ð¼ Ð¶Ðµ Ð² Ñ?Ð²Ð¾Ð¸ Ð¸ Ñ?Ñ?Ð»ÐµÐ´Ð¾Ð²Ð°Ð½Ð¸Ñ… Ð³Ð¾Ð²Ð¾Ñ€Ð¸Ñ‚ Ð±ÐµÐ·ÑƒÑ?Ð»Ð¾Ð²Ð½Ð¾ Ð Ð°Ñƒ,Ð¸Ð¾ | Block | 1 |
| 5.255.253.124 | Russian Federation | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 5.255.253.124 | Block | 1 |
| 180.76.4.170 | China | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to 147.237.0.34/ | Block | 1 |
| 194.72.238.241 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to / | Block | 1 |
| 104.131.147.112 | | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 5.255.253.124 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar | Block | 1 |
| 180.76.4.178 | China | 147.237.76.31 | nakchal.idf.il | Distributed Unauthorized URL Access on 147.237.76.31// | Block | 1 |
| 66.249.75.76 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/ | Block | 1 |
| 199.30.16.163 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |

04-25-2015-02:03:07 to 04-25-2015-03:03:07