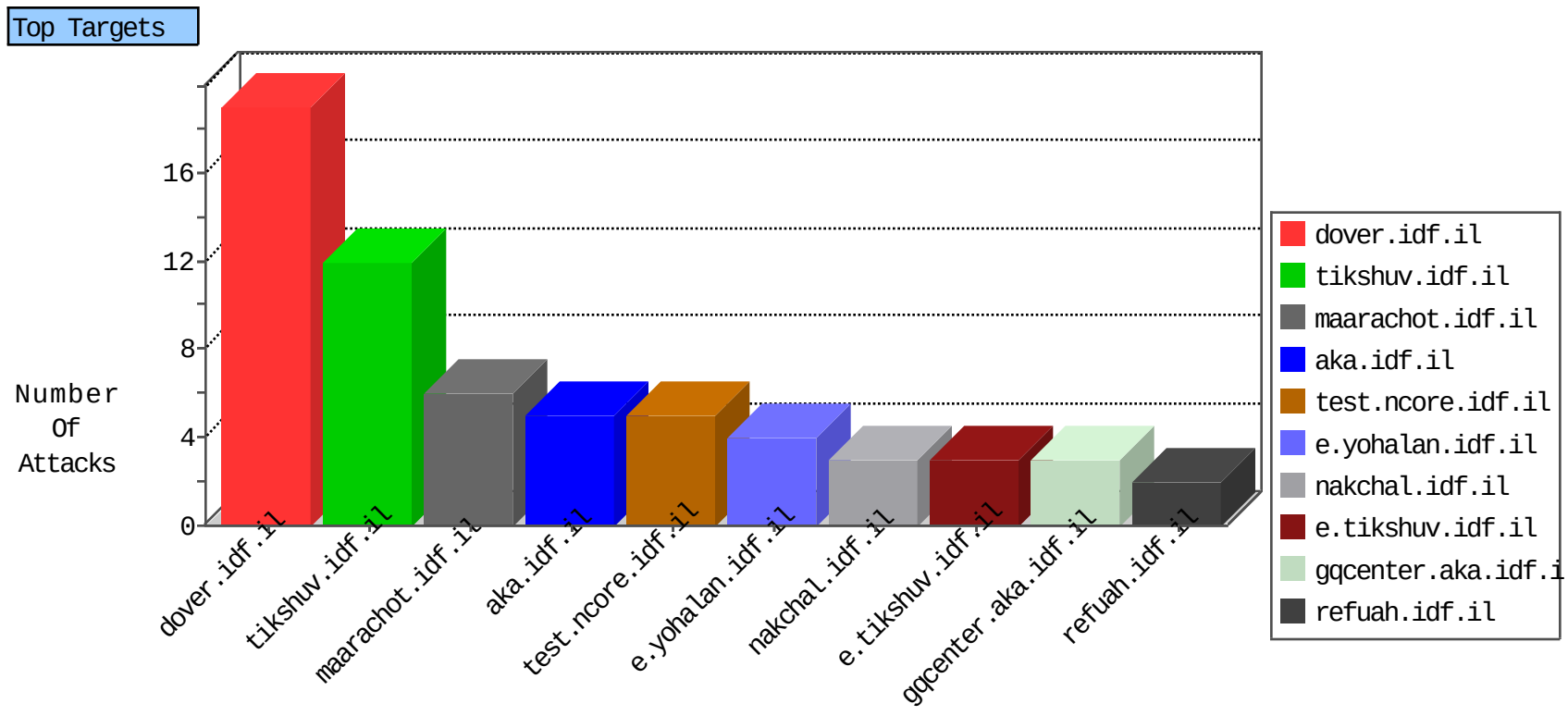
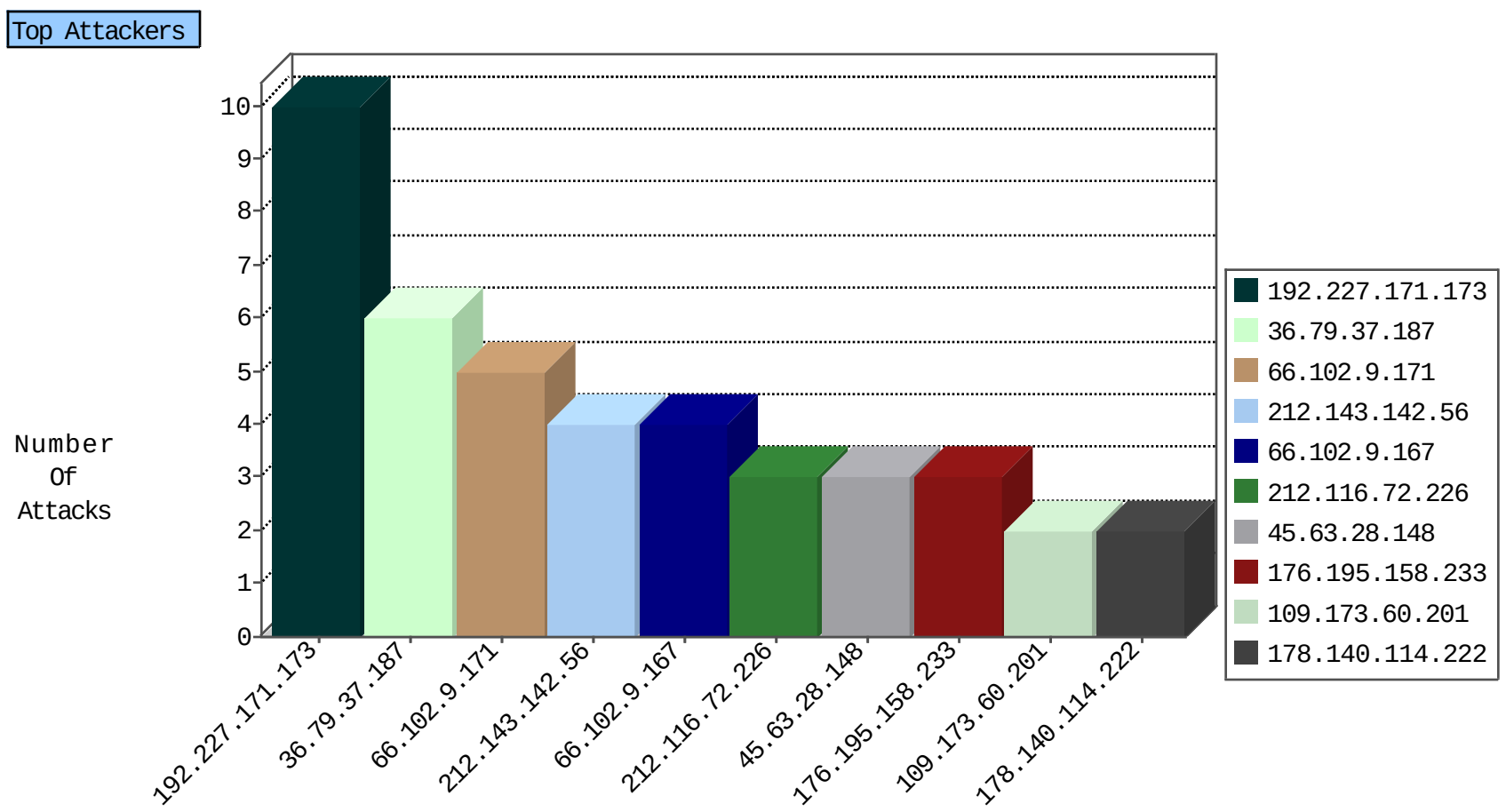
09-03-2016-04:04:08 to 09-03-2016-05:04:08

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-03-2016-04:04:08 to 09-03-2016-05:04:08

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 118.193.22.197 | Hong Kong | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |
| 204.42.253.132 | United States | 147.237.76.44 | e.refuah.idf.il | Black List | drop | 1 |
| 94.102.49.190 | Netherlands | 147.237.76.31 | nakchal.idf.il | Black List | drop | 1 |
| 118.193.22.198 | Hong Kong | 147.237.76.148 | gqcenter.aka.idf.il | Black List | drop | 1 |
| 217.23.9.123 | Netherlands | 147.237.76.148 | gqcenter.aka.idf.il | Black List | drop | 1 |
| 118.193.22.194 | Hong Kong | 147.237.76.148 | gqcenter.aka.idf.il | Black List | drop | 1 |
| 118.193.26.35 | Hong Kong | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |
| 118.193.22.196 | Hong Kong | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |
| 118.193.26.36 | Hong Kong | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |

09-03-2016-04:04:08 to 09-03-2016-05:04:08

## Top Attackers In IPS

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

09-03-2016-04:04:08 to 09-03-2016-05:04:08

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 36.79.37.187 | 147.237.77.170 | Indonesia | maarachot.idf.il | Tehila defacement attempt (-Hacked By- sent to Web Server) | 6 |
| 5.255.90.133 | 147.237.77.19 | Netherlands | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 192.227.171.173 | 147.237.76.196 | United States | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 192.227.171.173 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 192.227.171.173 | 147.237.0.200 | United States | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 192.227.171.173 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 119.142.202.43 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 221.204.249.157 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 45.63.28.148 | 147.237.8.50 | United States | e.tikshuv.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 212.116.72.226 | 147.237.76.198 | Sweden | e.yohalan.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 45.63.28.148 | 147.237.8.50 | United States | e.tikshuv.idf.il | ET SCAN NMAP -f -sS | 1 |
| 208.100.26.228 | 147.237.76.31 | United States | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 5.255.90.133 | 147.237.77.61 | Netherlands | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 192.227.171.173 | 147.237.76.198 | United States | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 192.227.171.173 | 147.237.76.147 | United States | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 192.227.171.173 | 147.237.76.38 | United States | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 192.227.171.173 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 192.227.171.173 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 221.204.249.157 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 87.236.194.161 | 147.237.77.205 | Czech Republic | prisha.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 212.116.72.226 | 147.237.76.198 | Sweden | e.yohalan.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 45.63.28.148 | 147.237.8.50 | United States | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 212.116.72.226 | 147.237.76.198 | Sweden | e.yohalan.idf.il | ET SCAN NMAP -f -sS | 1 |
| 192.227.171.173 | 147.237.76.201 | United States | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |

09-03-2016-04:04:08 to 09-03-2016-05:04:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.102.9.171 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 66.102.9.167 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 176.195.158.233 | Russian Federation | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 3 |
| 178.140.114.222 | Russian Federation | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 2 |
| 109.173.60.201 | Russian Federation | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 2 |
| 176.193.104.241 | Russian Federation | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 2 |
| 37.112.224.36 | Russian Federation | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 2 |
| 183.129.160.229 | China | 147.237.76.176 | test.ncore.idf.il | drop | SAM rule | drop | 1 |
| 31.13.110.110 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 31.13.110.126 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

09-03-2016-04:04:08 to 09-03-2016-05:04:08

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.76.83 | Block | 2 |
| 148.251.179.145 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp | Block | 1 |
| 66.249.64.41 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/63577.doc | Block | 1 |
| 66.249.76.112 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/האתר | Block | 1 |
| 66.249.69.13 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/mobile/ | Block | 1 |
| 66.249.76.115 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1153-22261-he/dover.aspx | Block | 1 |
| 66.249.76.75 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 68.180.230.47 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy/ | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp | Block | 1 |
| 77.237.146.28 | Czech Republic | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to / | Block | 1 |

09-03-2016-04:04:08 to 09-03-2016-05:04:08