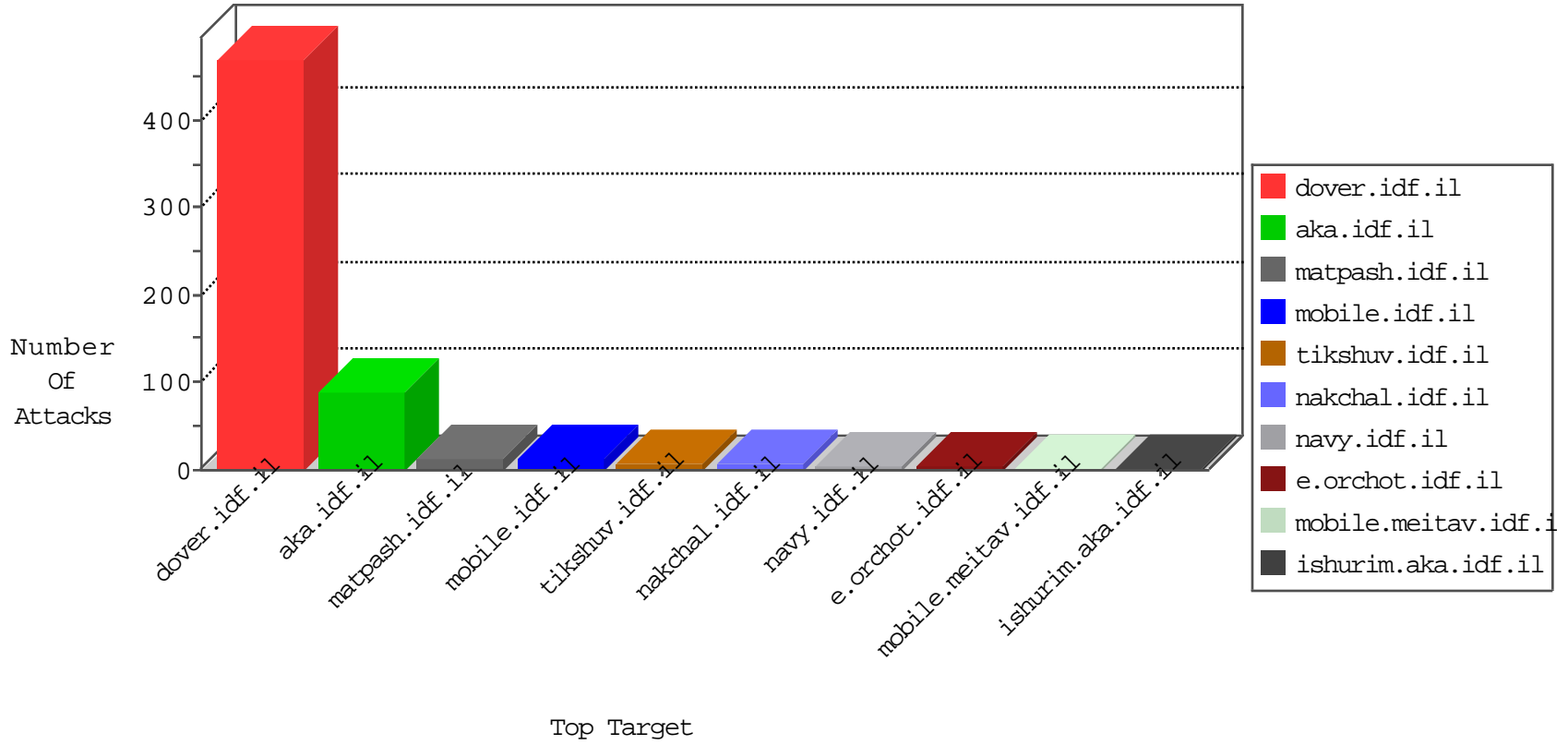


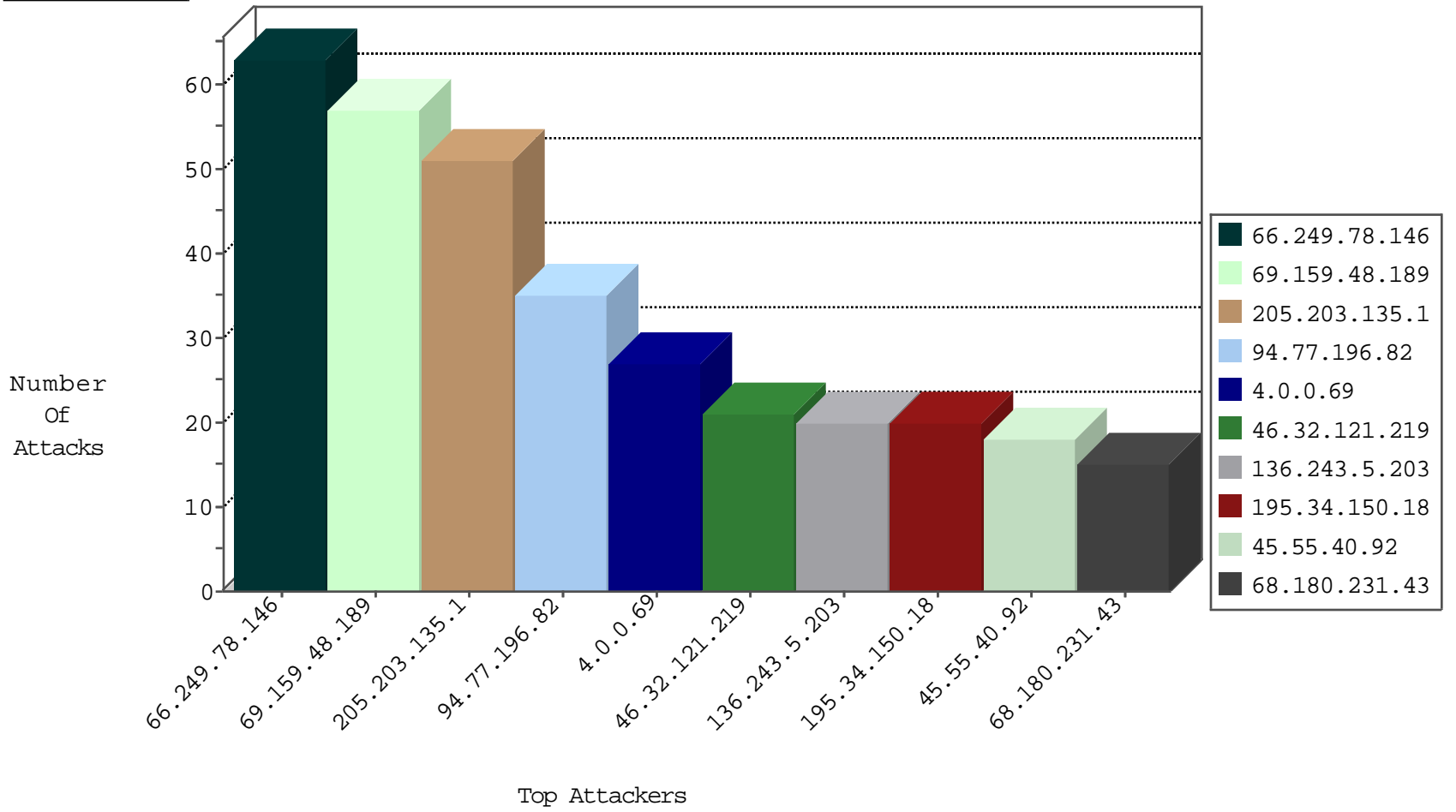
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|--------------------|----------------|----------------------|----------------------|---------------|-------|
| 5.135.17.28 | France | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.176 | test.ncore.idf.il | Block_Udp_All_Nets | drop | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|-------------|---|---------------|-------|
| 93.190.69.10 | Germany | 147.237.72.156 | aman.idf.in | 16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability | Block | 1 |

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|------------------|----------------|------------------|---------------|---|-------|
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 188.214.249.151 | 147.237.77.216 | Romania | dover.idf.il | Xenu Link Sleuth User Agent | 2 |
| 106.186.113.132 | 147.237.76.31 | Japan | nakchal.idf.i | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 2 |
| 93.190.69.10 | 147.237.72.156 | Germany | aman.idf.il | ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers | 1 |
| 80.82.78.38 | 147.237.77.121 | Netherlands | e.navy.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 |
|------------------|--------------------|----------------|-----------------|--|---|---------------|-------|
| 66.249.78.146 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 63 |
| 69.159.48.189 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 56 |
| 205.203.135.1 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 51 |
| 94.77.196.82 | Saudi Arabia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 35 |
| 4.0.0.69 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 46.32.121.219 | Jordan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 136.243.5.203 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 45.55.40.92 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 52.29.223.39 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 198.58.102.49 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 37.26.149.174 | Israel | 147.237.77.176 | matpash.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 198.58.102.156 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 37.204.108.99 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 87.203.102.200 | Greece | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 207.46.13.137 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 157.55.39.106 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 109.253.158.233 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 207.46.13.2 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 66.249.64.190 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 99.71.220.192 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 45.35.64.142 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 192.249.66.247 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 157.55.39.204 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 66.249.78.216 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.64.201.161 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.204.108.99 | Russian Federation | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 178.255.215.87 | France | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.93.247 | Europe | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.85.155 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 91.121.144.123 | France | 147.237.8.14 | e.orchot.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 3 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 66.249.66.184 | United States | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 156.198.197.8 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 128.242.249.12 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 156.199.62.223 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 199.30.24.164 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 66.249.64.41 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 106.186.113.132 | Japan | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 82.212.93.38 | Jordan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 142.4.217.162 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 203.6.69.2 | Australia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|--------------------|---|---------------|-------|
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp | Block | 2 |
| 208.115.113.82 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx | Block | 2 |
| 66.249.78.111 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 106.186.113.132 | Japan | 147.237.76.31 | nakchal.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 66.249.64.41 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atall/izkor/view_img.asp | Block | 1 |
| 66.249.78.246 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/sachar/default.aspx | Block | 1 |
| 184.105.247.195 | United States | 147.237.72.167 | ishurim.aka.idf.il | Unauthorized URL Access to 147.237.72.167/ | Block | 1 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/international_training | Block | 1 |
| 197.160.78.252 | Egypt | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-ar | Block | 1 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp | Block | 1 |
| 84.111.94.176 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 66.249.64.238 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp | Block | 1 |
| 106.186.113.132 | Japan | 147.237.76.31 | nakchal.idf.il | Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO)) | None | 1 |
| 66.249.64.18 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |