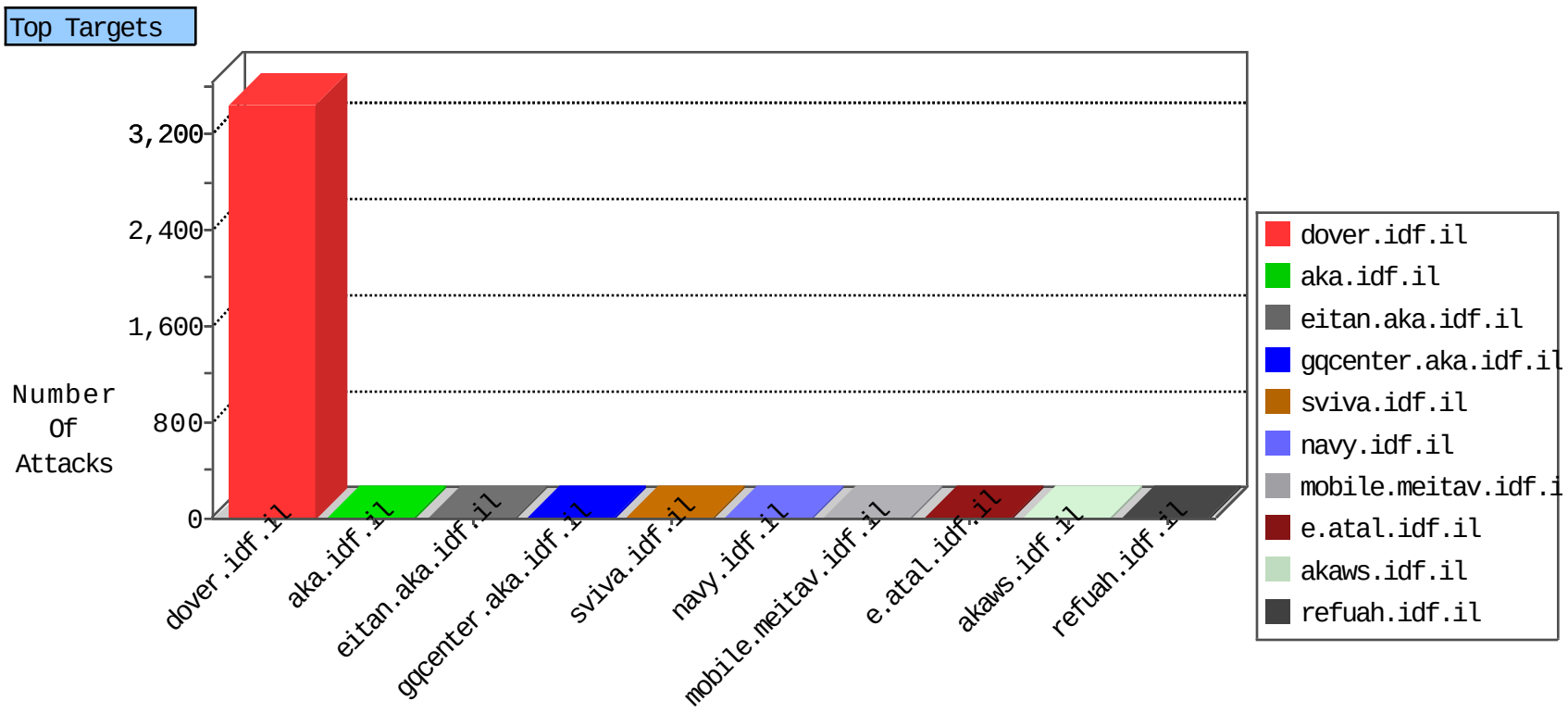
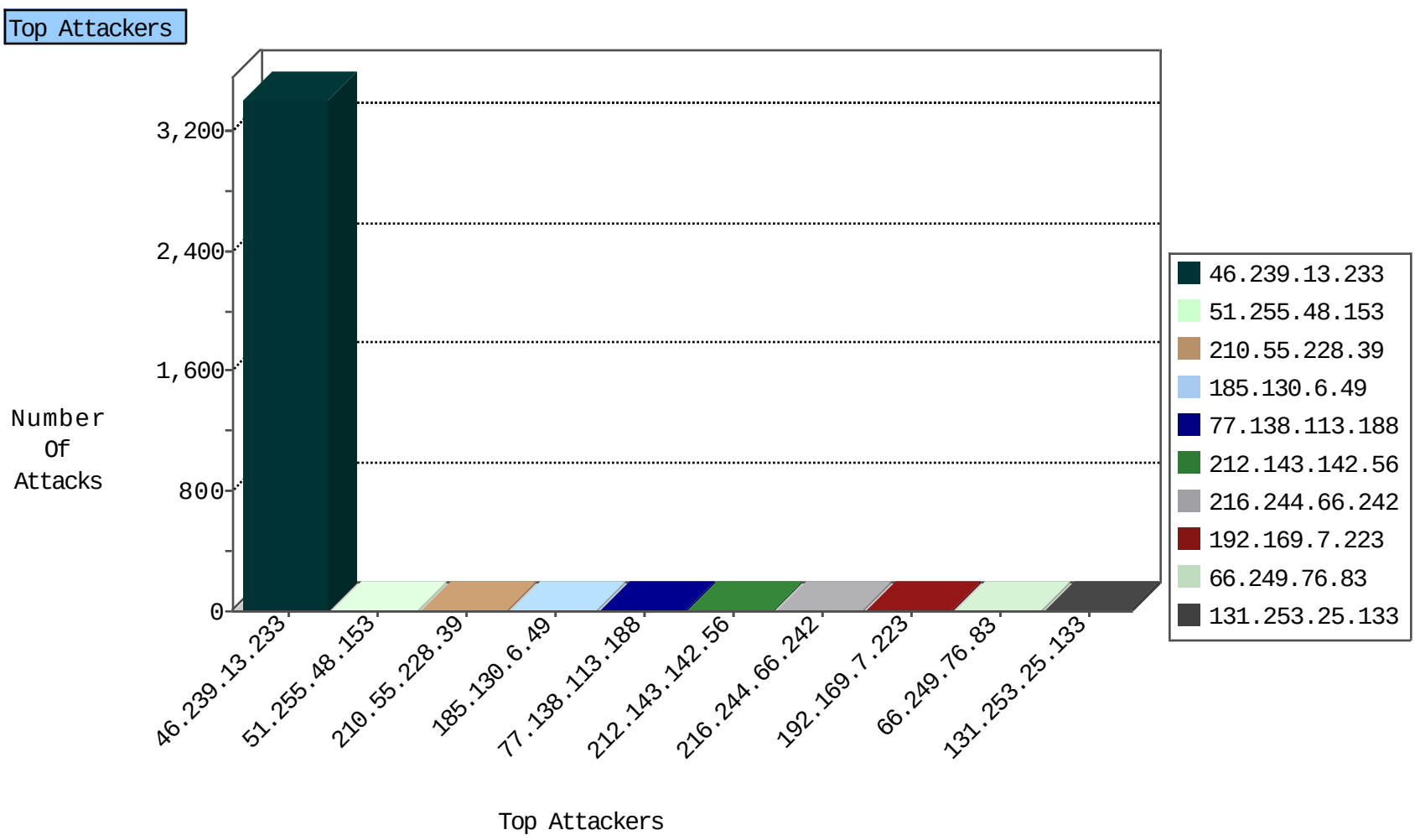
08-29-2016-03:04:06 to 08-29-2016-04:04:06

# IDF Under Attack Daily Report



08-29-2016-03:04:06 to 08-29-2016-04:04:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.239.13.233 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | Frk_Under_Attack_Con_Http | drop | 2 |

08-29-2016-03:04:06 to 08-29-2016-04:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 51.255.48.153 | France | 147.237.76.200 | eitan.aka.idf.il | C1000074: HTTP: majestic bot | Permit | 7 |
| 51.255.48.153 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 3 |
| 123.126.68.105 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |

08-29-2016-03:04:06 to 08-29-2016-04:04:06

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 123.206.73.185 | 147.237.76.38 | China | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 84.200.84.187 | 147.237.8.27 | Germany | e.madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.116.123.135 | 147.237.76.148 | United States | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 212.116.72.226 | 147.237.76.86 | Sweden | navy.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 186.137.157.66 | 147.237.76.201 | Argentina | e.atal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 163.172.169.150 | 147.237.72.156 | United Kingdom | aman.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 154.16.199.217 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 137.117.168.203 | 147.237.77.212 | United States | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.147.200.234 | 147.237.76.148 | Azerbaijan | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 66.249.64.141 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 222.45.173.82 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 201.238.202.219 | 147.237.0.19 | Chile | madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 186.137.157.66 | 147.237.76.201 | Argentina | e.atal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 159.203.33.10 | 147.237.76.31 | Canada | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 137.117.168.203 | 147.237.77.233 | United States | atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

08-29-2016-03:04:06 to 08-29-2016-04:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.239.13.233 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3263 |
| 46.239.13.233 | Bosnia and Herzegovina | 147.237.77.216 | dover.idf.il | drop | | drop | 150 |
| 210.55.228.39 | New Zealand | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 185.130.6.49 | Lithuania | 147.237.77.235 | sviva.idf.il | drop | SAM rule | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 192.169.7.223 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 4 |
| 198.58.100.99 | United States | 147.237.76.39 | mobile.meitav.idf.il | drop | SAM rule | drop | 3 |
| 106.38.241.105 | China | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 1 |
| 106.38.241.105 | China | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 1 |
| 46.120.122.219 | Israel | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 1 |
| 106.38.241.105 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 156.199.213.24 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 201.238.202.219 | Chile | 147.237.0.35 | akaws.idf.il | drop | | drop | 1 |
| 185.128.37.152 | Iraq | 147.237.77.227 | e.hamaz.idf.il | drop | First packet isn't SYN | drop | 1 |

08-29-2016-03:04:06 to 08-29-2016-04:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 77.138.113.188 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/sachar | Block | 4 |
| 66.249.76.83 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.76.83 | Block | 3 |
| 131.253.25.133 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 77.138.113.188 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined | Block | 2 |
| 216.244.66.242 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 216.244.66.242 | Block | 2 |
| 66.249.88.157 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 216.244.66.242 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 2 |
| 157.55.39.175 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter ismul in aka.idf.il/main/sachar/viewpayslip.aspx | None | 1 |
| 66.249.66.185 | Israel | 147.237.76.42 | refuah.idf.i | Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2418.jpg | Block | 1 |
| 207.46.13.64 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter slipid in aka.idf.il/main/sachar/viewpayslip.aspx | None | 1 |
| 2.53.170.164 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 157.55.39.252 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter ismul in aka.idf.il/main/sachar/viewpayslip.aspx | None | 1 |
| 207.46.13.109 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 79.178.199.111 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/ צור קשר | Block | 1 |
| 38.111.147.83 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 1 |
| 167.220.232.104 | Japan | 147.237.77.74 | law.idf.il | Illegal Byte Code Character in URL /163-4314-en/patzar.aspx#011200 | Block | 1 |
| 66.249.88.151 | Israel | 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 |
| 40.77.167.29 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp | Block | 1 |
| 167.220.232.104 | Japan | 147.237.77.216 | dover.idf.il | Multiple Illegal Byte Code Character in URL from 167.220.232.104 | Block | 1 |
| 66.249.64.11 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/229-he/faq.aspx | Block | 1 |
| 207.46.13.64 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter ismul in aka.idf.il/main/sachar/viewpayslip.aspx | None | 1 |

08-29-2016-03:04:06 to 08-29-2016-04:04:06