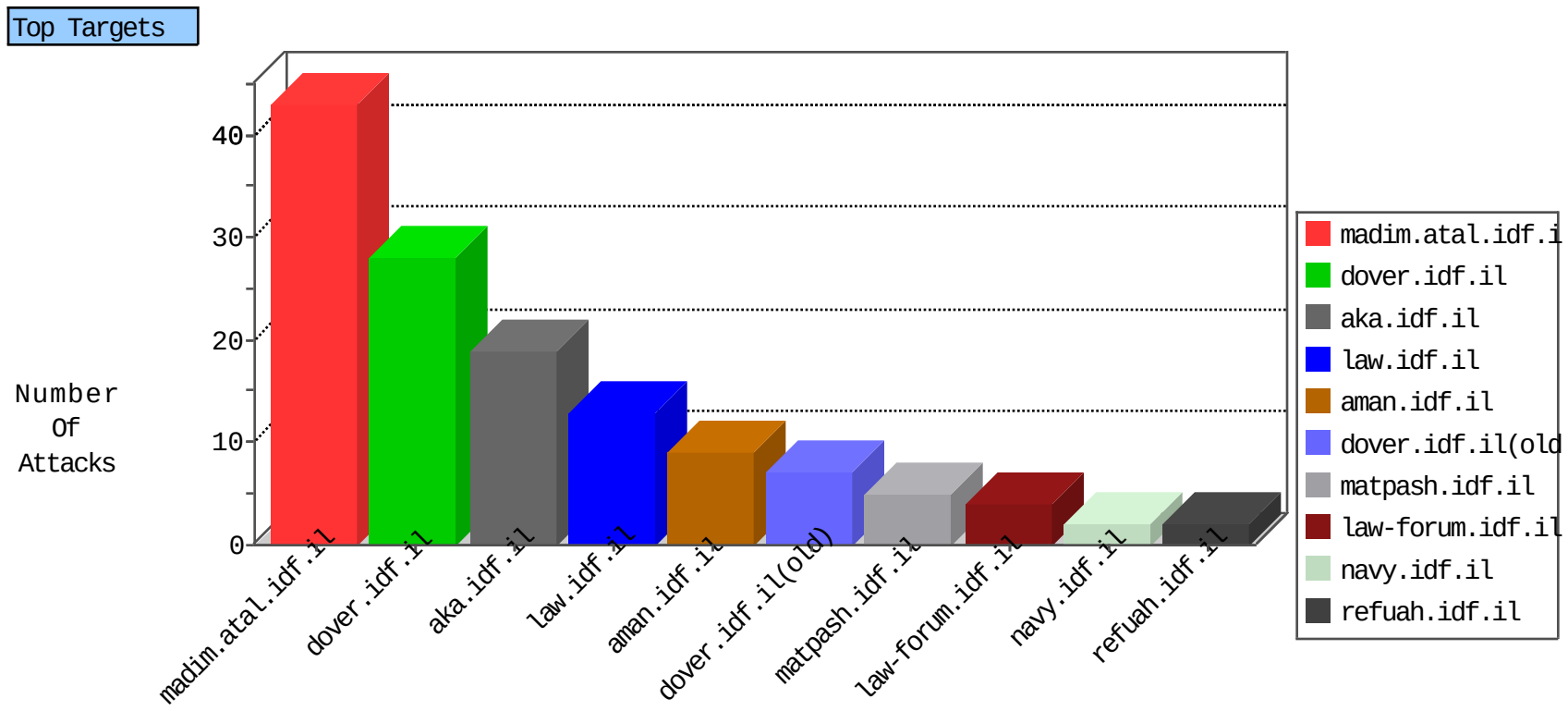
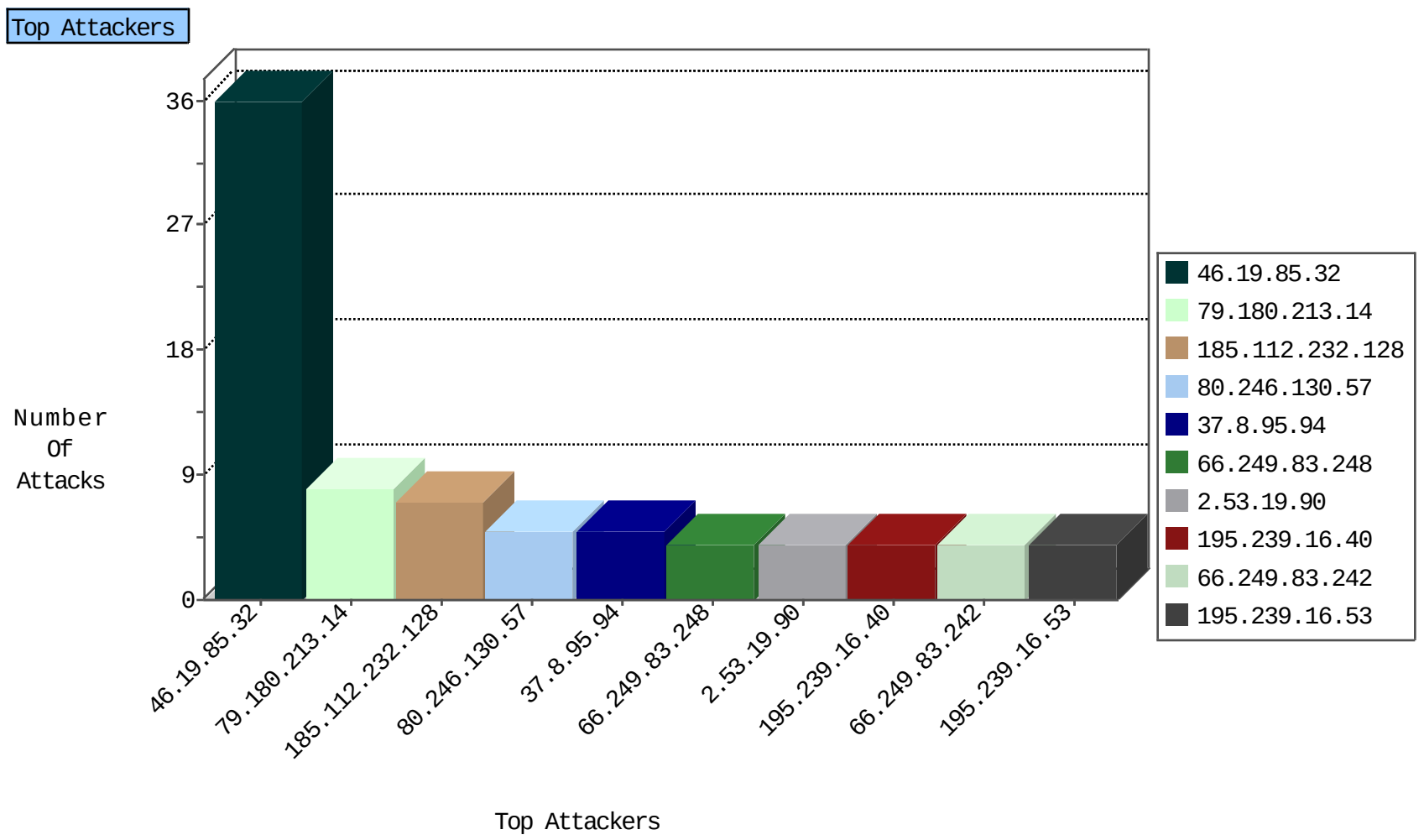
08-18-2016-00:04:06 to 08-18-2016-01:04:06

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



08-18-2016-00:04:06 to 08-18-2016-01:04:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.66.61.87 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3 |
| 186.112.15.122 | Colombia | 147.237.77.243 | mobile.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 82.80.78.2 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 1 |
| 89.248.171.2 | Netherlands | 147.237.76.201 | e.atal.idf.il | Black List | drop | 1 |
| 82.80.78.2 | Israel | 147.237.72.166 | aka.idf.il | Black List | drop | 1 |
| 82.80.78.2 | Israel | 147.237.76.86 | navy.idf.il | Black List | drop | 1 |

08-18-2016-00:04:06 to 08-18-2016-01:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 195.154.185.20 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 163.172.49.61 | United Kingdom | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 151.80.31.163 | France | 147.237.76.42 | refuah.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |

08-18-2016-00:04:06 to 08-18-2016-01:04:06

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 37.8.95.94 | 147.237.77.176 | Palestinian Territory, Occupied | matpash.idf.il | ET SCAN NMAP -sA (2) | 5 |
| 115.47.12.162 | 147.237.76.177 | China | ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 113.108.10.31 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 94.102.48.195 | 147.237.76.86 | Netherlands | navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.158 | 147.237.72.156 | Ukraine | aman.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 91.201.236.158 | 147.237.72.156 | Ukraine | aman.idf.il | ET SCAN NMAP -f -sS | 1 |
| 72.252.249.125 | 147.237.77.233 | Jamaica | atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 220.231.195.122 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 186.118.222.34 | 147.237.0.33 | Colombia | idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 123.206.85.139 | 147.237.77.233 | China | atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 113.108.10.31 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 99.184.21.78 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 94.102.48.195 | 147.237.76.39 | Netherlands | mobile.meitav.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.158 | 147.237.72.156 | Ukraine | aman.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 87.236.194.161 | 147.237.72.156 | Czech Republic | aman.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 220.231.195.122 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 46.227.67.169 | 147.237.76.199 | Sweden | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 220.231.195.122 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN NMAP -f -sS | 1 |
| 173.208.249.35 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

08-18-2016-00:04:06 to 08-18-2016-01:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 185.112.232.128 | Iraq | 147.237.72.14 | dover.idf.il(old) | drop | First packet isn't SYN | drop | 7 |
| 79.180.213.14 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 195.239.16.40 | Russian Federation | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 4 |
| 195.239.16.53 | Russian Federation | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 89.243.33.231 | United Kingdom | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 3 |
| 109.253.218.212 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 3 |
| 176.13.6.223 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.166.213.55 | Romania | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 1 |
| 109.253.206.85 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.3.179 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |

08-18-2016-00:04:06 to 08-18-2016-01:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.32 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 36 |
| 80.246.130.57 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 5 |
| 66.249.83.248 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 2.53.19.90 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 66.249.83.242 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 66.249.83.245 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 46.19.85.184 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.180.213.14 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 139.162.13.205 | Singapore | 147.237.76.31 | nakchal.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 77.138.225.167 | France | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/favicon.ico | Block | 1 |
| 50.74.27.82 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.167 | ishurim.aka.idf.i | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 77.139.109.13 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.78.123 | Israel | 147.237.76.30 | himush.idf.il | Unauthorized URL Access to www.tech.atal.idf.il/templates/shared/usercontrols/navmenu/undefined | Block | 1 |
| 109.64.177.151 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 68.180.228.99 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 180.76.15.145 | China | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/robots.txt | Block | 1 |
| 77.139.156.11 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.78.254 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 109.253.246.67 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 77.138.8.220 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar | Block | 1 |
| 213.172.183.61 | Poland | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/giyus/general/ | Block | 1 |
| 79.180.213.14 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb10452978 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 136.243.16.208 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx | Block | 1 |
| 77.138.14.205 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx | Block | 1 |

08-18-2016-00:04:06 to 08-18-2016-01:04:06