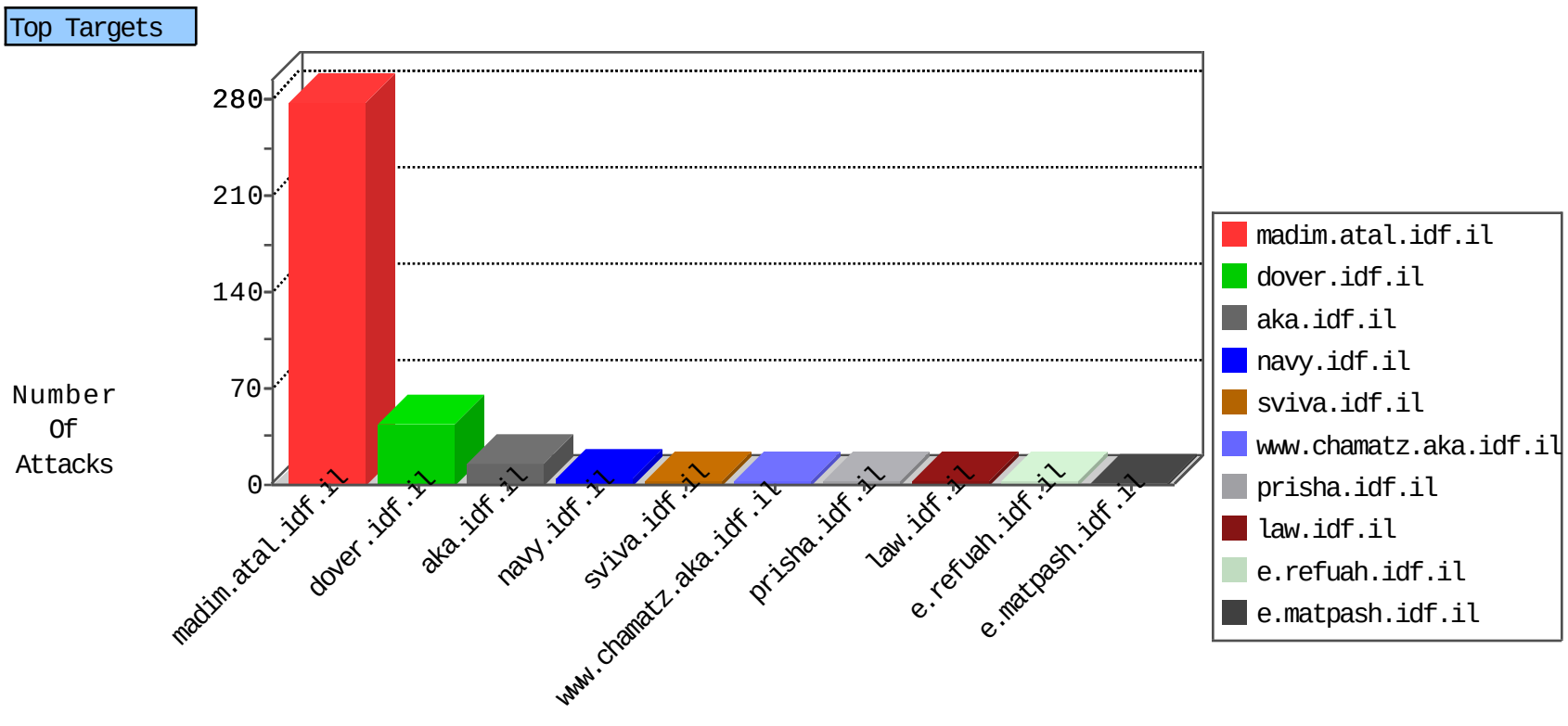
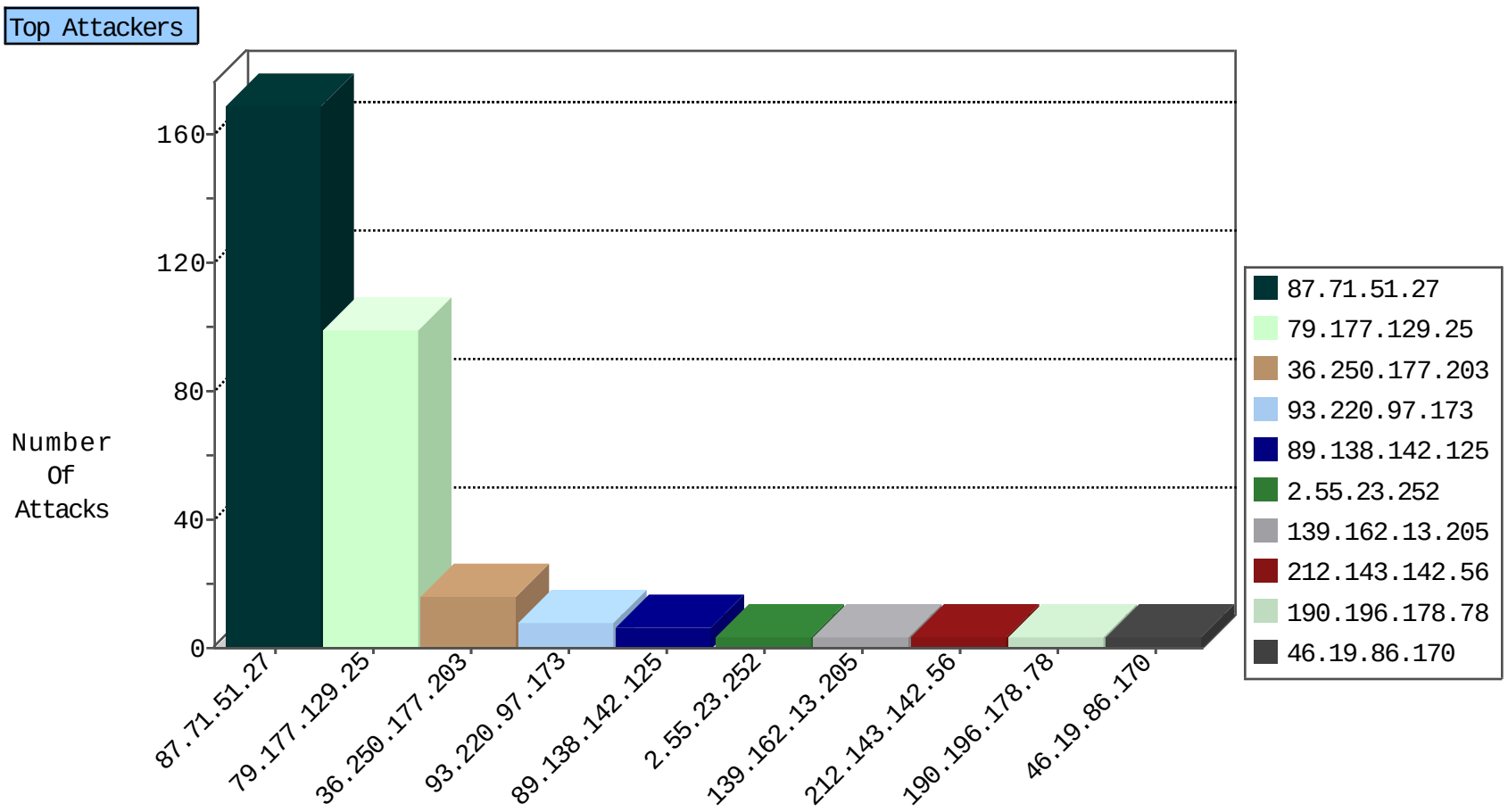
08-19-2016-14:04:08 to 08-19-2016-15:04:08

# IDF Under Attack Daily Report

Top Targets




Top Attackers



08-19-2016-14:04:08 to 08-19-2016-15:04:08

Top Attackers In DDoS-Defence

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

08-19-2016-14:04:08 to 08-19-2016-15:04:08

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 71.6.158.166 | United States | 147.237.76.196 | e.sviva.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |
| 91.217.244.214 | Ukraine | 147.237.76.86 | navy.idf.il | 12715: HTTP: Blind SQL Injection in URI | Block | 1 |

08-19-2016-14:04:08 to 08-19-2016-15:04:08

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 84.109.180.213 | 147.237.77.216 | Israel | dover.idf.il | Xenu Link Sleuth User Agent | 2 |
| 91.217.244.214 | 147.237.76.86 | Ukraine | navy.idf.il | SQL Injection - Select From | 1 |
| 87.236.194.161 | 147.237.0.15 | Czech Republic | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 71.86.124.86 | 147.237.76.44 | United States | e.refuah.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 2.53.58.221 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 190.196.178.78 | 147.237.77.205 | Chile | prisha.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 179.179.203.53 | 147.237.76.30 | Brazil | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 161.18.180.120 | 147.237.0.34 | Colombia | tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 139.162.13.205 | 147.237.77.235 | Singapore | sviva.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 87.236.194.161 | 147.237.76.197 | Czech Republic | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 71.86.124.86 | 147.237.76.44 | United States | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 190.196.178.78 | 147.237.77.205 | Chile | prisha.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 190.196.178.78 | 147.237.77.205 | Chile | prisha.idf.il | ET SCAN NMAP -f -sS | 1 |
| 173.208.249.37 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 152.173.172.251 | 147.237.0.33 | Chile | idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |

08-19-2016-14:04:08 to 08-19-2016-15:04:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 93.220.97.173 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 89.138.142.125 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 109.253.147.89 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 79.181.185.75 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 83.149.126.98 | Germany | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 188.120.154.215 | Israel | 147.237.76.31 | nakchal.idf.il | drop | First packet isn't SYN | drop | 1 |
| 139.162.37.147 | United States | 147.237.0.35 | akaws.idf.il | drop | | drop | 1 |
| 216.243.31.2 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 183.129.160.229 | China | 147.237.77.178 | e.matpash.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.77.243 | mobile.idf.il | drop | SAM rule | drop | 1 |

08-19-2016-14:04:08 to 08-19-2016-15:04:08

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 87.71.51.27 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 169 |
| 79.177.129.25 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 99 |
| 36.250.177.203 | China | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 36.250.177.203 | Block | 7 |
| 2.55.23.252 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.170 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.36.201.171 | Ireland | 147.237.77.74 | law.idf.il | Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/450-he/patzar.aspx | Block | 2 |
| 66.249.64.183 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 2.53.137.130 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 157.55.39.145 | United States | 147.237.0.19 | madim.atal.idf.il | Distributed Unauthorized URL Access on madim.atal.idf.il/robots.txt | Block | 2 |
| 36.250.177.203 | China | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 2 |
| 157.55.2.135 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.81.215 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 190.210.93.81 | Argentina | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/español | Block | 1 |
| 83.12.28.222 | Poland | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.76.47 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/default.asp | Block | 1 |
| 36.250.177.203 | China | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/index.asp | Block | 1 |
| 157.55.12.75 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 77.126.54.209 | Israel | 147.237.0.19 | madim.atal.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx | Block | 1 |
| 212.76.125.192 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 66.249.76.51 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter catId\u003d59116\u0026pageNum\u003d3 in www.aka.idf.il/edim/yoman/yoman.asp | None | 1 |
| 46.19.85.236 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Malformed URL | Block | 1 |
| 157.55.12.92 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 77.139.206.205 | France | 147.237.72.166 | aka.idf.il | Multiple Untraceable SSL Sessions from 77.139.206.205 (Open Mode) | None | 1 |
| 66.249.64.183 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.235 | sviva.idf.il | Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO)) | None | 1 |
| 66.249.79.173 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 66.249.79.173 | Block | 1 |
| 46.19.85.236 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Unknown HTTP Request Method 55pfxcsw3w in URL | Block | 1 |
| 77.139.206.205 | France | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.64.185 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.235 | sviva.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 66.249.79.173 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/main/smalim/showbig.aspx | Block | 1 |
| 178.63.101.134 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp | Block | 1 |
| 66.249.76.33 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |

08-19-2016-14:04:08 to 08-19-2016-15:04:08