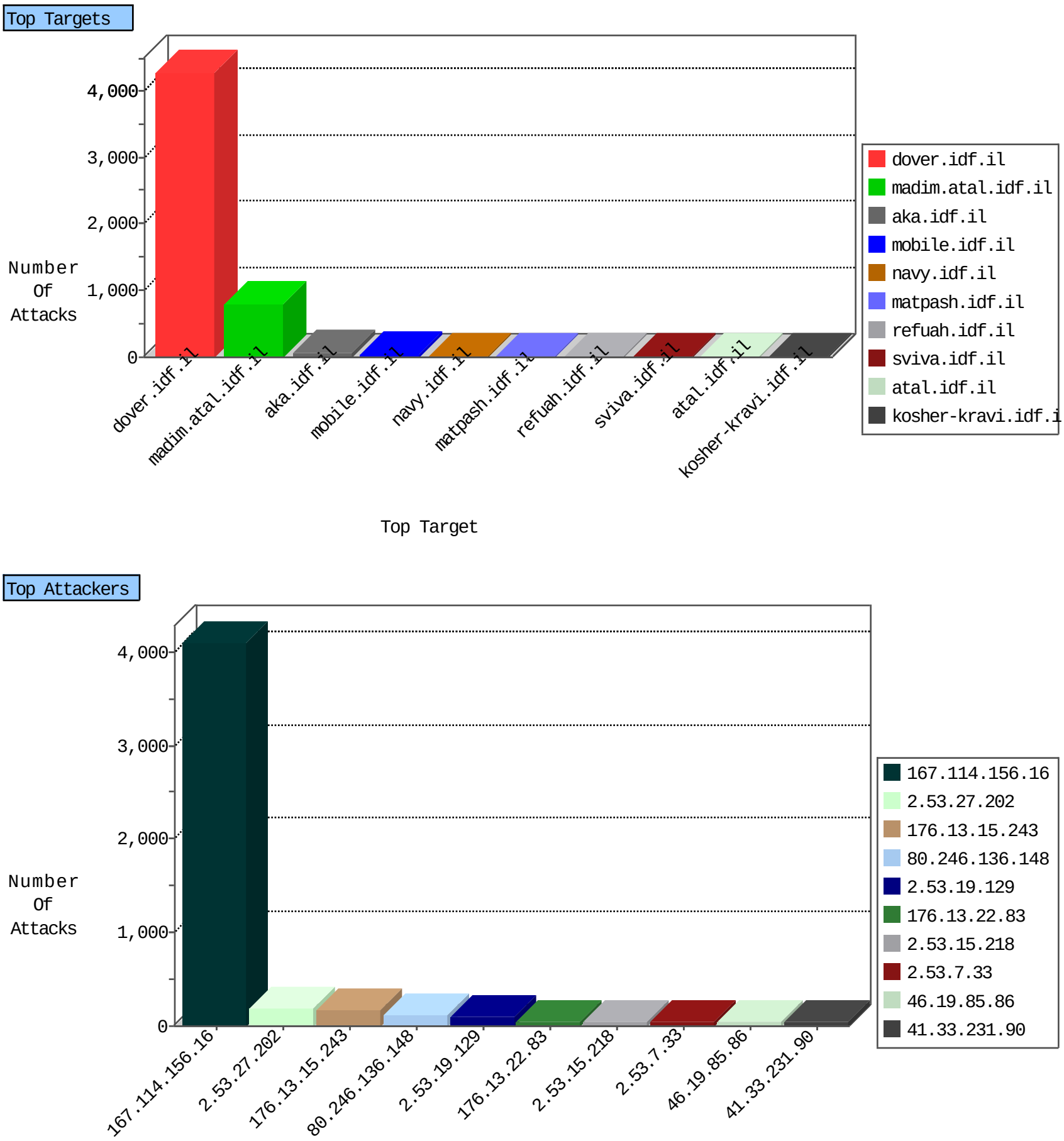
04-17-2016-07:04:07 to 04-17-2016-08:04:07

# IDF Under Attack Daily Report



04-17-2016-07:04:07 to 04-17-2016-08:04:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 4100 |
| 212.179.64.162 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 81.218.65.210 | Israel | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 3 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 180.153.235.242 | China | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 2 |
| 175.28.246.195 | Japan | 147.237.76.198 | e.yohalan.idf.il | Block_Udp_All_Nets | drop | 2 |
| 184.105.139.84 | United States | 147.237.77.233 | atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 81.17.30.220 | Switzerland | 147.237.0.16 | my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.81.157.165 | France | 147.237.8.24 | e.lifestyle.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.139.92 | United States | 147.237.8.27 | e.madim.atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 209.126.111.7 | United States | 147.237.77.121 | e.navy.idf.il | Block_Udp_All_Nets | drop | 1 |
| 184.105.139.67 | United States | 147.237.77.212 | e.dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 216.218.206.87 | United States | 147.237.0.33 | idf.il | Block_Udp_All_Nets | drop | 1 |
| 184.105.139.104 | United States | 147.237.77.227 | e.hamaz.idf.il | Block_Ntp_All_Net | drop | 1 |
| 209.126.111.7 | United States | 147.237.77.178 | e.matpash.idf.il | Block_Udp_All_Nets | drop | 1 |
| 184.105.139.84 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 216.218.206.115 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 184.105.139.124 | United States | 147.237.0.19 | madim.atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 209.126.111.7 | United States | 147.237.77.235 | sviva.idf.il | Block_Udp_All_Nets | drop | 1 |

04-17-2016-07:04:07 to 04-17-2016-08:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 136.243.5.87 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 4 |
| 106.38.241.106 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 66.249.66.184 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 174.139.251.164 | United States | 147.237.77.216 | dover.idf.il | C1000016: HTTP: administrator in URI | Block | 1 |
| 66.249.66.187 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |

04-17-2016-07:04:07 to 04-17-2016-08:04:07

## 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 |
| 113.240.250.154 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 113.240.250.154 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 107.158.255.194 | 147.237.0.15 | United States | kosher-kravi.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 84.111.138.75 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.80.86.86 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.177.252.87 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 210.117.121.60 | 147.237.0.16 | Korea, Republic of | my-kosher-kravi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 40.84.148.3 | 147.237.72.217 | United States | e.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 162.144.41.122 | 147.237.77.233 | United States | atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.142.235.101 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 113.240.250.154 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 31.204.128.186 | 147.237.0.15 | Netherlands | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 113.240.250.154 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.67.153.107 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 107.158.255.194 | 147.237.0.15 | United States | kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 84.109.230.232 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.82.78.38 | 147.237.0.33 | Netherlands | idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 210.117.121.60 | 147.237.0.16 | Korea, Republic of | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 63.142.161.25 | 147.237.76.200 | Canada | eitan.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 40.84.148.3 | 147.237.72.217 | United States | e.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 125.212.232.165 | 147.237.77.178 | Vietnam | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 31.204.128.186 | 147.237.0.34 | Netherlands | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |

04-17-2016-07:04:07 to 04-17-2016-08:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 2.53.4.45 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 37.26.146.174 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 46.19.85.181 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 2.53.140.87 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.181 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.66.29.188 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.146.174 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 79.182.179.120 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 73.171.202.86 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 46.19.85.181 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 79.176.130.195 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 46.19.85.181 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 79.176.130.195 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 66.249.66.15 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.227 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.13.4.246 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.168.123.7 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 3 |
| 46.19.85.234 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 37.26.146.196 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.25.76.207 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 3 |
| 31.168.123.7 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 79.178.123.228 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 82.166.94.67 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.55.143.21 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 132.66.62.239 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.168.123.7 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 79.181.129.158 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 172.56.7.240 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.53.29.236 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 149.78.255.164 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.102.254.200 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 79.177.205.42 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 2 |
| 5.102.195.23 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 213.244.119.251 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 2 |
| 185.3.144.70 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 46.19.85.24 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 85.65.107.49 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 199.203.215.1 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 31.168.123.7 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 184.105.139.112 | United States | 147.237.8.50 | e.tikshuv.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 5.39.222.159 | Netherlands | 147.237.77.19 | law-forum.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 162.144.41.122 | United States | 147.237.77.212 | e.dover.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.122.235 | United States | 147.237.8.14 | e.orchot.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 213.244.118.251 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 80.250.150.95 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 192.118.12.102 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |

04-17-2016-07:04:07 to 04-17-2016-08:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.53.27.202 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 183 |
| 176.13.15.243 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 171 |
| 80.246.136.148 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 125 |
| 2.53.19.129 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 100 |
| 2.53.15.218 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 52 |
| 176.13.22.83 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 51 |
| 2.53.7.33 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 41 |
| 46.19.85.86 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 39 |
| 46.19.85.22 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 29 |
| 131.253.25.241 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 5 |
| 199.30.25.142 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 109.253.140.49 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 65.55.210.226 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 199.30.24.5 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 109.253.144.216 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.10 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 65.55.210.96 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 199.30.24.1 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 2 |
| 174.139.251.164 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 2 |
| 2.53.4.45 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 104.36.236.140 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/article/src="http:/www.youtube.com/v/0mwqtcld1fe | Block | 2 |
| 68.180.230.45 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-9235-he/refuah.aspx | Block | 1 |
| 5.153.233.130 | Sweden | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/wp-login.php | Block | 1 |
| 2.55.175.221 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx | Block | 1 |
| 157.55.39.188 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/miluim/hovot/templates/main.asp | Block | 1 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy/ | Block | 1 |
| 24.218.80.94 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/homepage/mobile | Block | 1 |
| 65.55.210.240 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 5.44.174.93 | Russian Federation | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 1 |
| 199.30.24.50 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 77.237.146.28 | Czech Republic | 147.237.77.235 | sviva.idf.il | Unauthorized Method HEAD for / | Block | 1 |
| 213.254.241.6 | France | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx | None | 1 |
| 184.105.247.196 | United States | 147.237.72.167 | ishurim.aka.idf.i | Unauthorized URL Access to 147.237.72.167/ | Block | 1 |
| 109.253.202.53 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.78.234 | Block | 1 |
| 5.44.174.93 | Russian Federation | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php | Block | 1 |
| 199.30.24.70 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 174.139.251.164 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 174.139.251.164 | Block | 1 |
| 2.53.173.9 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 2.53.173.9 | Block | 1 |
| 126.57.122.131 | Japan | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 66.249.78.236 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2306.jpg | Block | 1 |
| 5.153.233.130 | Sweden | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 199.30.25.77 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 174.139.251.164 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 1 |
| 2.53.173.9 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/templates/newslobby/mobile | Block | 1 |

04-17-2016-07:04:07 to 04-17-2016-08:04:07