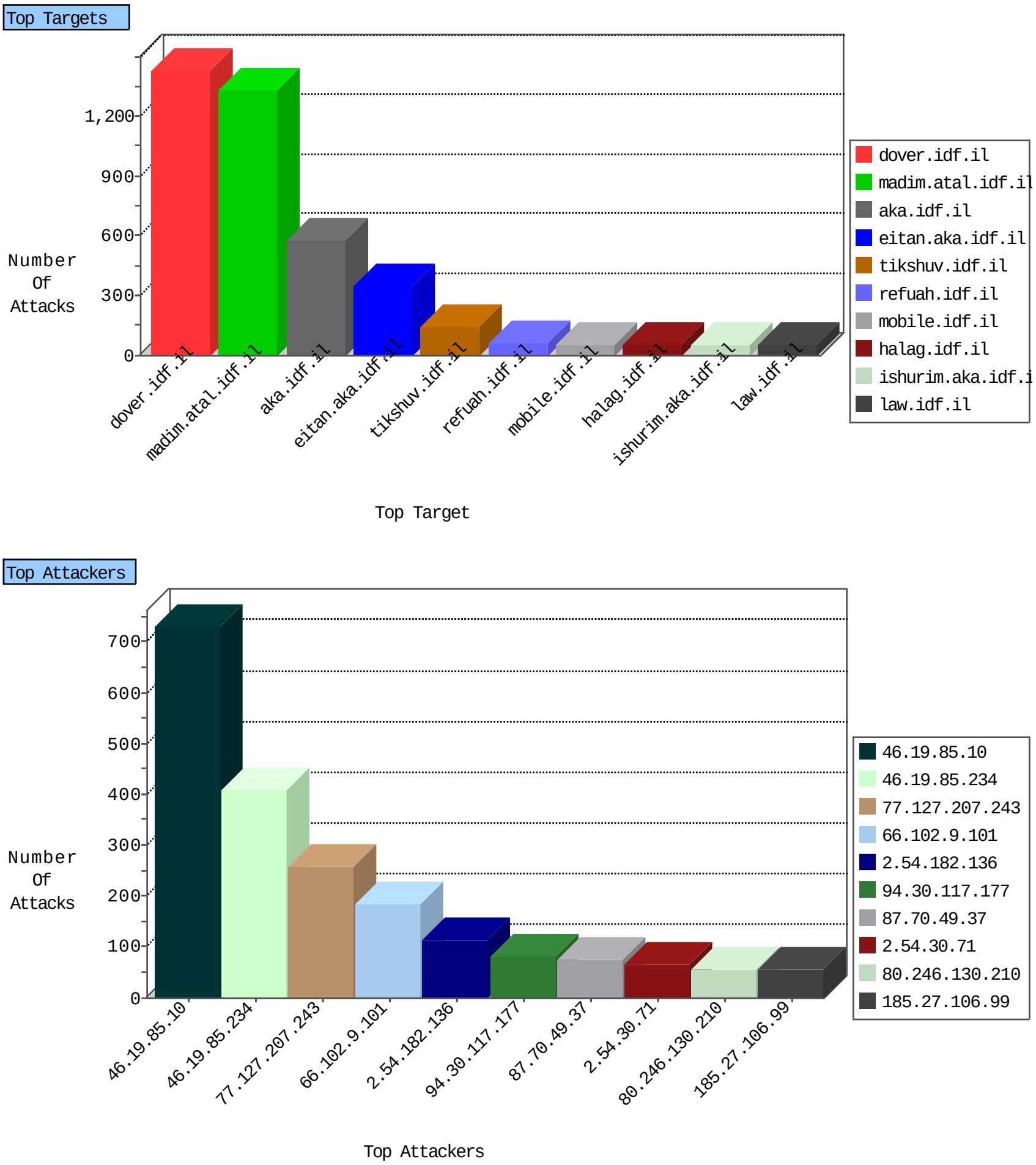
02-21-2016-19:04:07 to 02-21-2016-20:04:07

# IDF Under Attack
# Daily Report



02-21-2016-19:04:07 to 02-21-2016-20:04:07

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 221.1.74.86 | China | 147.237.76.199 | e.nakchal.idf.il | Invalid TCP Flags | drop | 2 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 192.99.58.235 | Canada | 147.237.76.201 | e.atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.130.5.224 | | 147.237.76.148 | gqcenter.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.130.5.224 | | 147.237.76.177 | ncore.idf.il | Block_Udp_All_Nets | drop | 1 |
| 192.99.58.235 | Canada | 147.237.76.148 | gqcenter.aka.idf.il | Block_Ntp_All_Net | drop | 1 |

02-21-2016-19:04:07 to 02-21-2016-20:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 5.29.193.165 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 10 |
| 84.111.29.9 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 109.66.3.182 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 93.173.169.48 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 182.50.130.133 | Singapore | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 1 |

02-21-2016-19:04:07 to 02-21-2016-20:04:07

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.102.9.101 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 185 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 84.94.45.226 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 208.67.1.109 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.183.106.112 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.114.91.244 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.26.149.144 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.181.124.241 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 119.81.107.18 | 147.237.76.200 | Singapore | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.28.132.173 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.93.249 | 147.237.72.166 | United States | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 119.81.107.18 | 147.237.0.33 | Singapore | idf.il | ET SCAN Potential SSH Scan | 1 |
| 62.219.128.187 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 119.81.107.18 | 147.237.0.17 | Singapore | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 59.45.79.117 | 147.237.76.44 | China | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 84.229.32.179 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 59.45.79.117 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 84.109.230.214 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 59.45.79.117 | 147.237.8.14 | China | e.orchot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 84.108.5.115 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.121.115.109 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.151.59.238 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.166.247.66 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.142.253.88 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.181.130.67 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.120.148.148 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.29.157.207 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.181.101.172 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 119.81.107.18 | 147.237.0.34 | Singapore | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 2.54.43.242 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 119.81.107.18 | 147.237.0.19 | Singapore | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 59.45.79.117 | 147.237.77.176 | China | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 109.64.53.79 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 59.45.79.117 | 147.237.72.14 | China | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 84.228.96.31 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 59.45.79.117 | 147.237.8.46 | China | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 84.109.194.9 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 59.45.79.117 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |

02-21-2016-19:04:07 to 02-21-2016-20:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 77.127.207.243 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 258 |
| 94.30.117.177 | United Kingdom | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 83 |
| 185.27.106.99 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 54 |
| 87.68.64.205 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 51 |
| 89.139.162.197 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 45 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 34 |
| 212.179.244.152 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 33 |
| 37.26.146.187 | Israel | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 20 |
| 89.138.177.140 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 19 |
| 46.19.85.19 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 46.19.85.33 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 14 |
| 2.52.48.211 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 13 |
| 192.243.55.134 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 13 |
| 46.19.85.186 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 80.246.139.86 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 46.19.85.23 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 46.19.85.177 | Israel | 147.237.76.147 | chinuch.aka.idf.il | drop | First packet isn't SYN | drop | 11 |
| 46.19.85.177 | Israel | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 10 |
| 2.52.181.108 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 46.19.85.177 | Israel | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 10 |
| 31.168.93.239 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.85.1 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 9 |
| 46.19.85.177 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.85.33 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 77.125.134.230 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 2.52.184.0 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 46.19.85.177 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 2.52.184.0 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack |  | reject | 8 |
| 130.193.50.33 | Russian Federation | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 8 |
| 2.52.184.0 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 2.52.184.0 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 2.52.184.0 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 8 |
| 192.243.55.134 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.218 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.165 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 82.80.144.24 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 7 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 80.246.139.86 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence |  | monitor | 7 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 7 |
| 84.108.180.242 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.53 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.79 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.36 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.165 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.66.157.187 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.130 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.176.100.108 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.10 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 551 |
| 46.19.85.234 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 263 |
| 46.19.85.10 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 180 |
| 46.19.85.234 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 146 |
| 2.54.182.136 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 59 |
| 80.246.130.210 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 56 |
| 2.54.182.136 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 54 |
| 213.57.174.198 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 48 |
| 2.54.30.71 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 40 |
| 2.54.30.71 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 23 |
| 213.8.204.83 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 213.8.204.83 | Block | 16 |
| 77.125.115.24 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.125.115.24 | Block | 13 |
| 213.8.204.57 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 12 |
| 213.8.204.83 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 8 |
| 109.66.157.187 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 8 |
| 176.13.15.5 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 176.13.15.5 | Block | 8 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Distributed Malformed URL | Block | 7 |
| 66.249.81.215 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 7 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 7 |
| 66.249.81.215 | Russian Federation | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 7 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Distributed Abnormally Long Request | Block | 7 |
| 95.172.233.91 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 94.230.86.153 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 6 |
| 213.57.147.221 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 66.249.81.212 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 5 |
| 66.249.81.218 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 5 |
| 66.249.81.212 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 5 |
| 66.249.81.218 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 5 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Multiple Illegal Byte Code Character in Method from 87.70.49.37 | Block | 4 |
| 46.19.85.160 | Israel | 147.237.77.216 | dover.idf.il | Distributed Malformed URL | Block | 4 |
| 185.89.217.233 |  | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 65.55.210.107 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 95.86.105.224 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1361-10648-he/dover.aspx&sa=u&ved=0ahukewie7f2esynlahxdca8khb0fdzcqfggemac&sig2=tjhluneq2ij-njoxlje2ka&usg=afqjcngzl-ikko4csdomsuq7twivb-8nig | Block | 4 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Multiple Abnormally Long Header Line from 87.70.49.37 | Block | 4 |
| 157.55.39.159 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 46.19.85.160 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 4 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Multiple Malformed HTTP Header Line from 87.70.49.37 | Block | 4 |
| 199.30.24.157 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 46.19.86.3 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 4 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Multiple Illegal Byte Code Character in Header Name from 87.70.49.37 | Block | 4 |
| 185.89.217.230 |  | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 4 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Multiple NULL Character in Header Name from 87.70.49.37 | Block | 4 |
| 199.30.25.146 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 185.89.217.234 |  | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 87.70.49.37 | Israel | 147.237.77.216 | dover.idf.il | Multiple Illegal Byte Code Character in Header Value from 87.70.49.37 | Block | 4 |
| 80.179.9.7 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 185.89.217.226 |  | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 46.19.86.66 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 4 |
| 66.249.83.161 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |