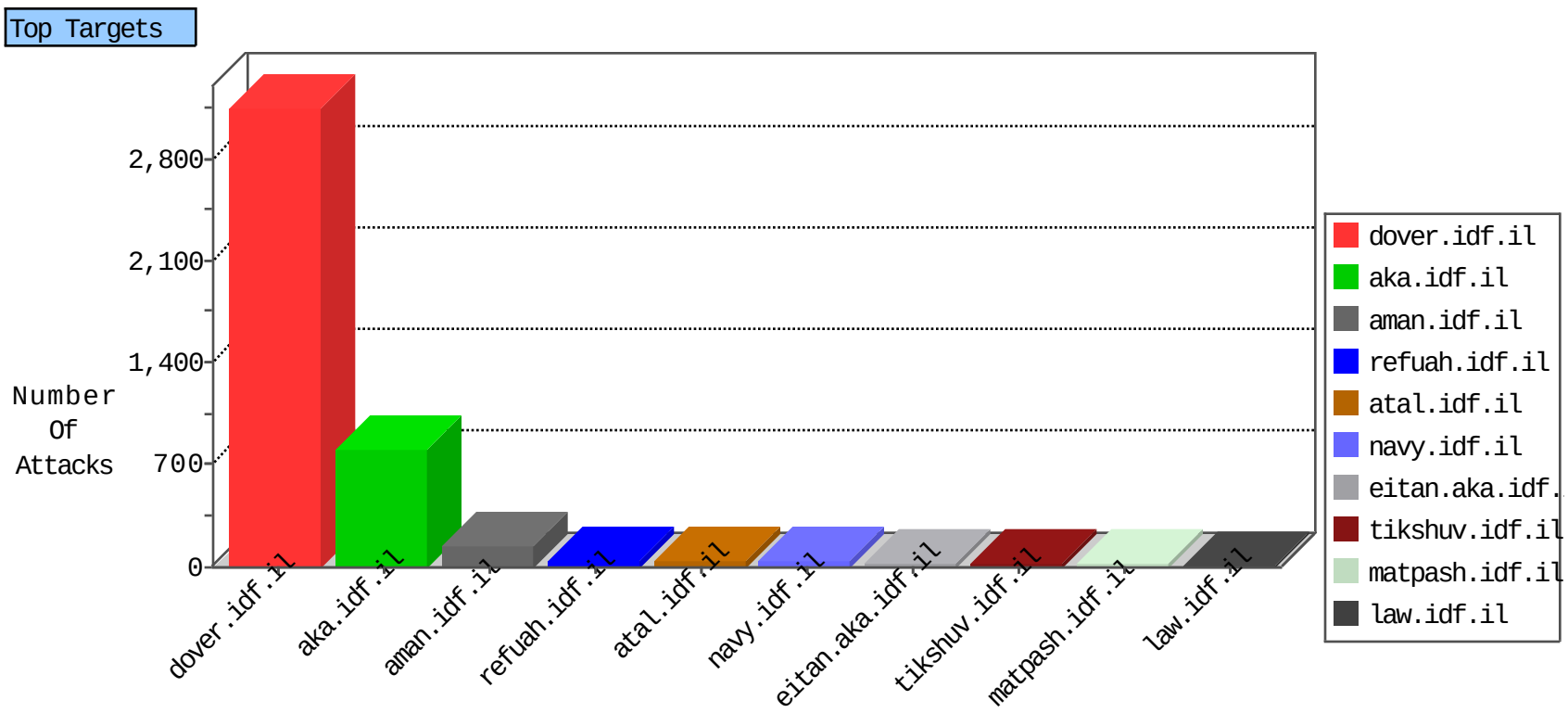
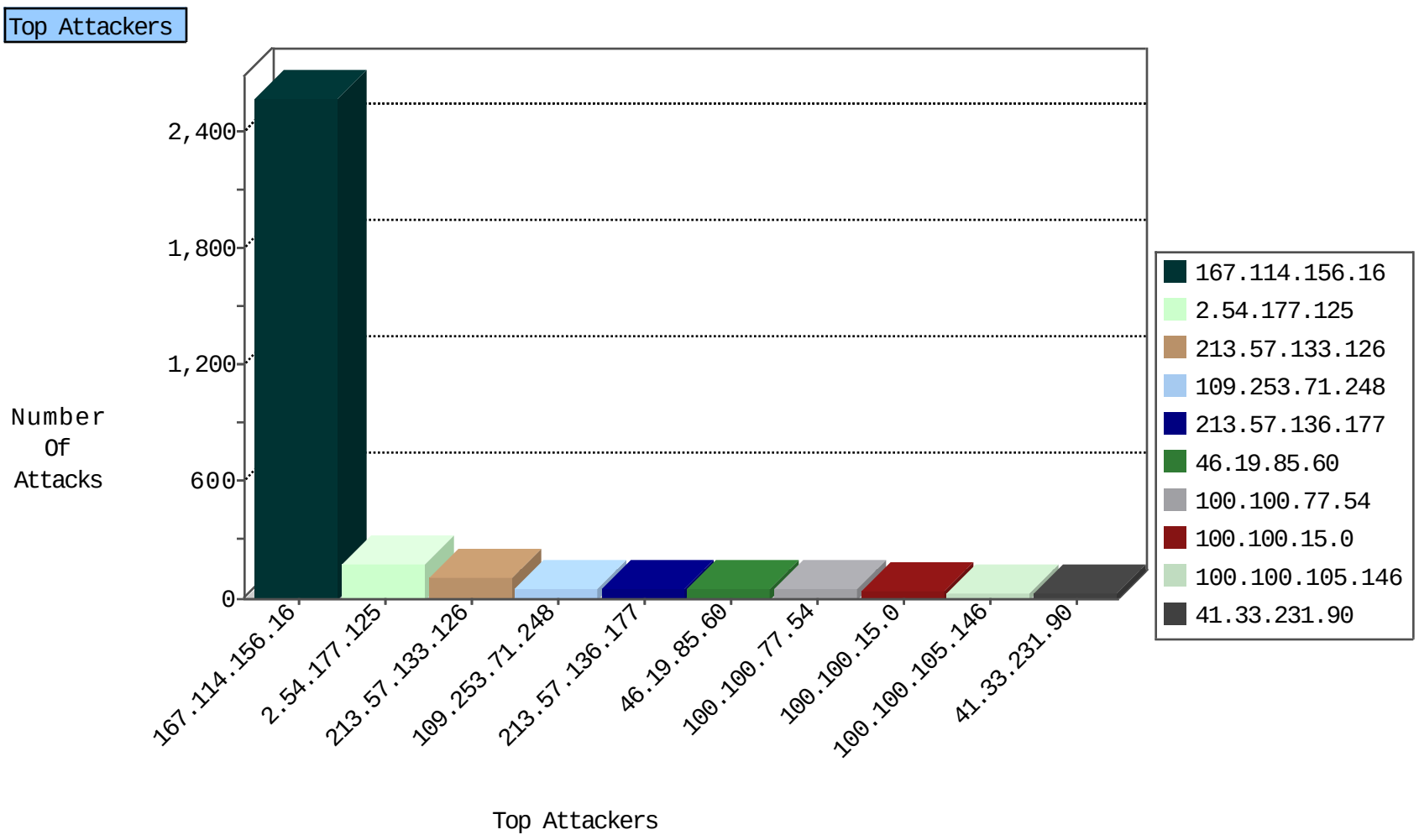
11-30-2015-19:04:01 to 11-30-2015-20:04:01

# IDF Under Attack Daily Report



11-30-2015-19:04:01 to 11-30-2015-20:04:01

## 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 | DOS-Tool-SwitchbladG | dest-reset | 3368 |
| 182.54.236.248 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 6 |
| 192.3.170.124 | United States | 147.237.76.202 | e.halag.idf.il | Block_Ntp_All_Net | drop | 1 |
| 115.230.124.164 | China | 147.237.77.216 | dover.idf.il | block-sp-traf1 | drop | 1 |

11-30-2015-19:04:01 to 11-30-2015-20:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 104.245.101.82 | | 147.237.72.166 | aka.idf.il | C025: HTTP: access to administrator/index.php -> Quarantine | Block | 1 |
| 77.126.225.170 | Israel | 147.237.72.166 | aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 1 |

11-30-2015-19:04:01 to 11-30-2015-20:04:01

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 | 4 |
| 66.249.66.78 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 109.66.191.107 | 147.237.72.156 | Israel | aman.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 43.229.53.89 | 147.237.0.16 | Japan | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 37.19.119.255 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.8.163.71 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.177.125 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.186.128.222 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 98.119.105.221 | 147.237.76.39 | United States | mobile.meitav.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 81.101.2.222 | 147.237.77.216 | United Kingdom | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.182.109.105 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 43.229.53.89 | 147.237.0.17 | Japan | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 37.46.39.48 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.29.98.29 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.150.201 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 95.86.97.142 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.246.136.79 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.176.214.209 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.117.64.6 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

11-30-2015-19:04:01 to 11-30-2015-20:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 2.54.177.125 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 108 |
| 213.57.133.126 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 66 |
| 213.57.133.126 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 49 |
| 100.100.77.54 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 47 |
| 109.253.71.248 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 34 |
| 46.19.85.60 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 33 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 213.57.136.177 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 27 |
| 100.100.105.146 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 27 |
| 100.100.34.212 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 26 |
| 213.57.136.177 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 25 |
| 100.100.10.209 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 25 |
| 100.100.45.233 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 100.100.77.33 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 24 |
| 100.100.62.61 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 23 |
| 66.249.81.175 | United States | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 21 |
| 109.253.71.248 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 20 |
| 212.235.98.139 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 18 |
| 100.100.15.0 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 18 |
| 100.100.15.0 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 18 |
| 2.54.177.125 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 17 |
| 2.54.177.125 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 46.19.85.62 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 17 |
| 2.54.177.125 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 17 |
| 79.178.119.35 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 66.249.75.94 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 14 |
| 149.88.104.116 | Israel | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 13 |
| 79.181.137.120 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 84.109.88.243 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 66.249.66.39 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 100.100.76.150 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 147.236.34.201 | Israel | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 100.100.97.114 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 11 |
| 2.54.177.125 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | | reject | 10 |
| 84.228.212.137 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 77.127.52.242 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 188.120.148.249 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 109.67.176.45 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 31.210.186.148 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 5.102.254.49 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 31.210.186.148 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 100.100.119.189 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 7 |
| 46.19.85.62 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 212.179.21.194 | Israel | 147.237.8.45 | e.eitan.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 37.26.149.157 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | | monitor | 6 |
| 84.95.198.7 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 217.132.4.120 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 77.127.193.41 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.65.26.59 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 84.95.198.7 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 146.185.234.48 | Russian Federation | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 146.185.234.48 | Block | 8 |
| 149.88.179.43 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword | Block | 7 |
| 46.116.99.214 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 4 |
| 207.241.226.41 | United States | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 207.241.226.41 | Block | 4 |
| 79.179.127.21 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 79.179.127.21 | Block | 4 |
| 176.13.10.91 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 176.13.10.91 | Block | 4 |
| 87.195.106.39 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 85.250.122.168 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Multiple Illegal Parameter Encoding from 85.250.122.168 | None | 3 |
| 87.106.179.206 | Germany | 147.237.76.200 | eitan.aka.idf.il | Distributed PHP Attempt | Block | 3 |
| 198.57.209.102 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 31.193.8.36 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 71.46.208.29 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 58.96.57.98 | Australia | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 74.220.215.245 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 83.170.118.9 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 213.57.173.101 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 3 |
| 31.193.8.36 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Admin Blocking | Block | 2 |
| 71.46.208.29 | United States | 147.237.77.216 | dover.idf.il | Distributed Admin Blocking | Block | 2 |
| 212.179.40.171 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/ufi/reaction/ | Block | 2 |
| 58.96.57.98 | Australia | 147.237.77.216 | dover.idf.il | Distributed Admin Blocking | Block | 2 |
| 74.220.215.245 | United States | 147.237.77.216 | dover.idf.il | Distributed Admin Blocking | Block | 2 |
| 83.170.118.9 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Admin Blocking | Block | 2 |
| 87.195.106.39 | Netherlands | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/index.php | Block | 2 |
| 79.176.65.145 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 71.46.208.29 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 71.46.208.29 | Block | 2 |
| 87.106.179.206 | Germany | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/index.php | Block | 2 |
| 198.57.209.102 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/index.php | Block | 2 |
| 31.193.8.36 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/index.php | Block | 2 |
| 176.12.139.183 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 58.96.57.98 | Australia | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/index.php | Block | 2 |
| 87.195.106.39 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Admin Blocking | Block | 2 |
| 74.220.215.245 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/index.php | Block | 2 |
| 83.170.118.9 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/index.php | Block | 2 |
| 87.106.179.206 | Germany | 147.237.76.200 | eitan.aka.idf.il | Distributed Admin Blocking | Block | 2 |
| 198.57.209.102 | United States | 147.237.77.216 | dover.idf.il | Distributed Admin Blocking | Block | 2 |
| 79.176.214.209 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 79.176.214.209 | Block | 2 |
| 66.249.66.75 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/tirkel.aspx | Block | 1 |
| 105.98.247.157 | Algeria | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 1 |
| 208.184.112.75 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 80.246.137.197 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 178.255.215.87 | France | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 2.52.168.245 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 79.179.127.21 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/d | Block | 1 |
| 176.12.150.67 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 62.90.147.211 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 202.112.51.96 | China | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.wooyun.org/ | Block | 1 |
| 185.35.62.11 | Switzerland | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 1 |
| 77.126.96.93 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/ | Block | 1 |
| 141.212.122.128 | United States | 147.237.77.216 | dover.idf.il | Malformed URL proxytest.zmap.io:80 | Block | 1 |
| 46.19.86.91 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |