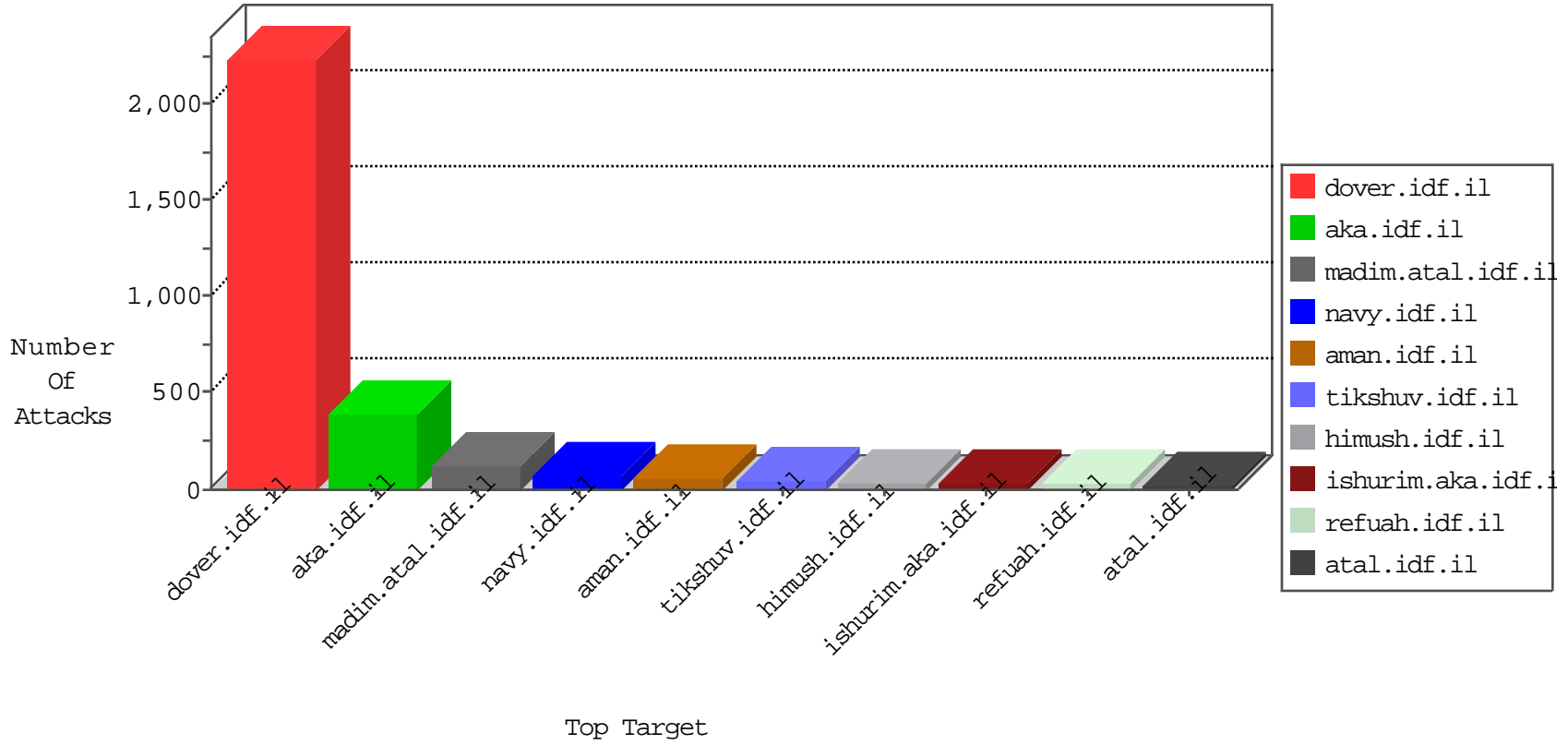


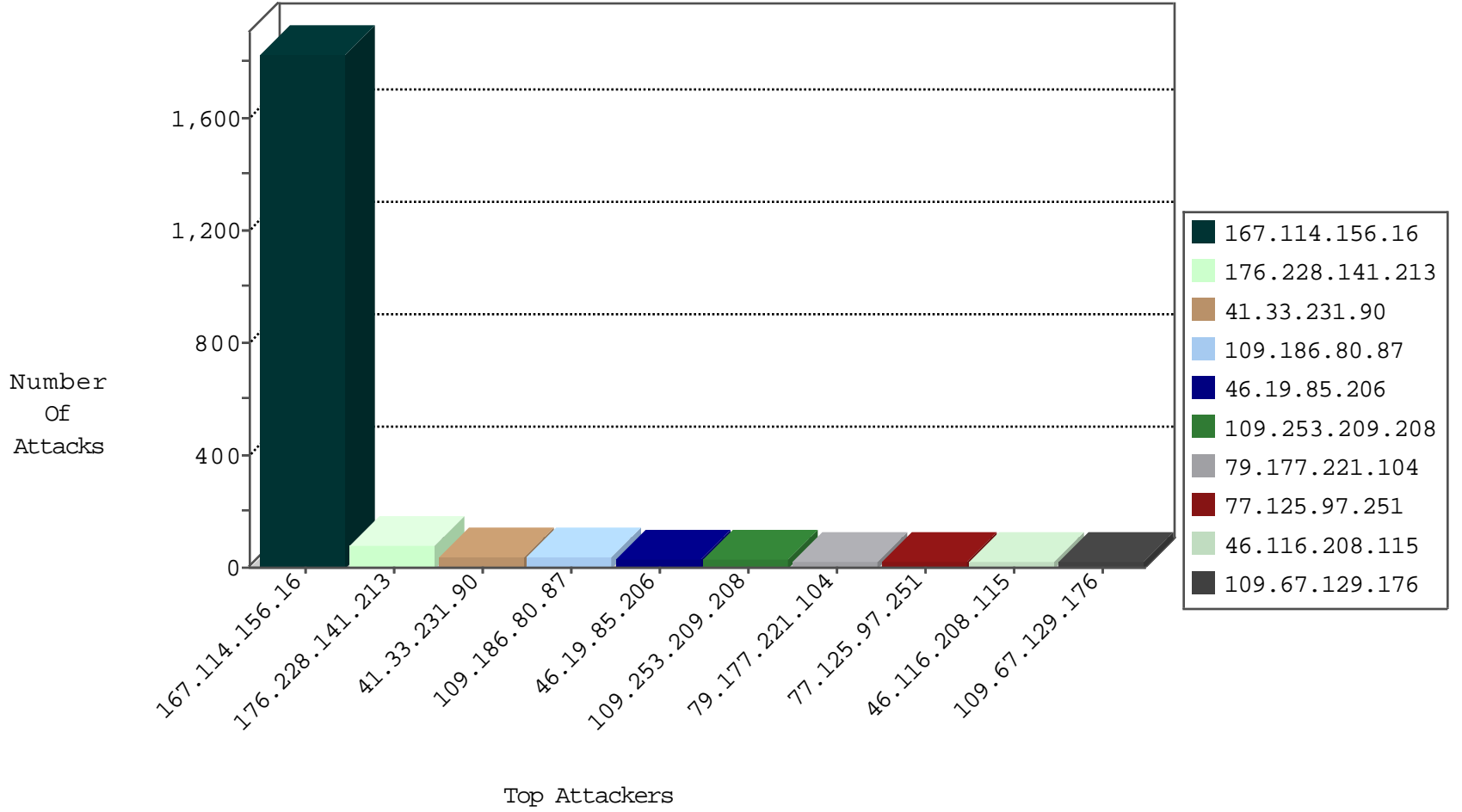
IDF Under Attack Daily Report



Top Targets



Top Attackers



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 | 3127 |
| 79.180.39.239 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 114.236.52.30 | China | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |

Top Attackers In IPS

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

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 |
| 37.142.230.95 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 162.242.245.138 | 147.237.77.179 | United States | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 149.78.141.47 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 104.192.0.18 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.173.140.87 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.69.191.155 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.60.48.25 | 147.237.76.198 | China | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 82.166.247.200 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.60.48.25 | 147.237.76.176 | China | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 79.179.97.63 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.60.48.25 | 147.237.0.34 | China | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.19.85.80 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 162.242.245.138 | 147.237.77.179 | United States | e.mazi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 149.88.10.129 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 121.201.27.61 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 95.86.122.37 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 89.138.194.187 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.60.48.25 | 147.237.77.216 | China | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 87.68.249.136 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.60.48.25 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 79.181.213.177 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.60.48.25 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 79.178.211.245 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.60.48.25 | 147.237.0.33 | China | idf.il | ET SCAN Potential SSH Scan | 1 |

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 | 34 |
| 79.177.221.104 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 109.67.129.176 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 109.253.209.208 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 46.19.86.141 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 13 |
| 109.186.185.69 | Israel | 147.237.72.156 | aman.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 109.253.209.208 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | alert | 12 |
| 85.130.171.23 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 77.127.217.15 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 46.116.208.115 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 10 |
| 46.116.208.115 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 77.125.97.251 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 10 |
| 77.125.97.251 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 82.166.158.156 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 46.19.86.58 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 79.178.5.200 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 46.19.85.206 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 194.230.159.162 | Switzerland | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 37.142.230.95 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 37.142.230.95 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.170 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 31.210.188.126 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.72 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.7 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.30 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.7 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.206 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.38 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.170 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.64.146.235 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.206 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 46.19.85.183 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.38 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.180.131.15 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.183 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.183.102.67 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.157 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.72 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 79.180.131.15 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 185.3.147.206 | Israel | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.157 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.136 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.85.193 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 41.249.75.249 | Morocco | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 79.181.184.138 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 31.210.188.126 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 37.26.149.165 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 46.19.85.193 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 5.102.254.229 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|---------------------------------|----------------|------------------|---|---------------|-------|
| 176.228.141.213 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 79 |
| 109.186.80.87 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 35 |
| 185.32.179.7 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 17 |
| 213.57.40.247 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 12 |
| 213.8.204.32 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 5 |
| 217.132.139.6 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/resource/userfollowresource/create/ | Block | 5 |
| 5.28.131.167 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 5.28.131.167 | Block | 4 |
| 79.181.147.157 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 79.181.147.157 | Block | 3 |
| 82.205.0.108 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-ar | Block | 3 |
| 62.219.115.220 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 77.125.78.87 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 80.246.136.73 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 46.121.77.180 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 109.253.145.76 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi | Block | 2 |
| 79.177.53.146 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Unknown SSL Session | None | 2 |
| 37.142.230.95 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 46.19.86.27 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 85.65.107.63 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/ | Block | 2 |
| 79.177.206.43 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 84.94.38.200 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationervice.asmx/getauthuser | Block | 2 |
| 23.31.9.105 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/ | Block | 2 |
| 109.65.197.24 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 77.125.97.251 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 194.90.15.61 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 84.108.184.84 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.86.114 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 174.129.228.67 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 46.19.85.106 | Israel | 147.237.76.86 | navy.idf.il | Illegal HTTP Version | Block | 1 |
| 217.132.156.67 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 207.46.13.193 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/newsflash/index.php | Block | 1 |
| 109.66.35.95 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.121.129.64 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 46.121.129.64 | Block | 1 |
| 185.32.179.74 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 8.37.70.141 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/&usg=alkjrhgvlfdbtv_7r3bjuzqzpxbsskknug | Block | 1 |
| 95.86.79.160 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 2.54.8.56 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 80.246.138.186 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.85.175 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 157.55.39.137 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 79.179.200.82 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.85.51 | Israel | 147.237.77.216 | dover.idf.il | Abnormally Long Request request version | Block | 1 |
| 109.253.209.4 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 31.168.148.218 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 109.65.68.222 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.69.34 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1513-en/dover | Block | 1 |
| 199.30.25.86 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 176.13.15.66 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 5.28.131.167 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 1 |
| 84.228.171.107 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |