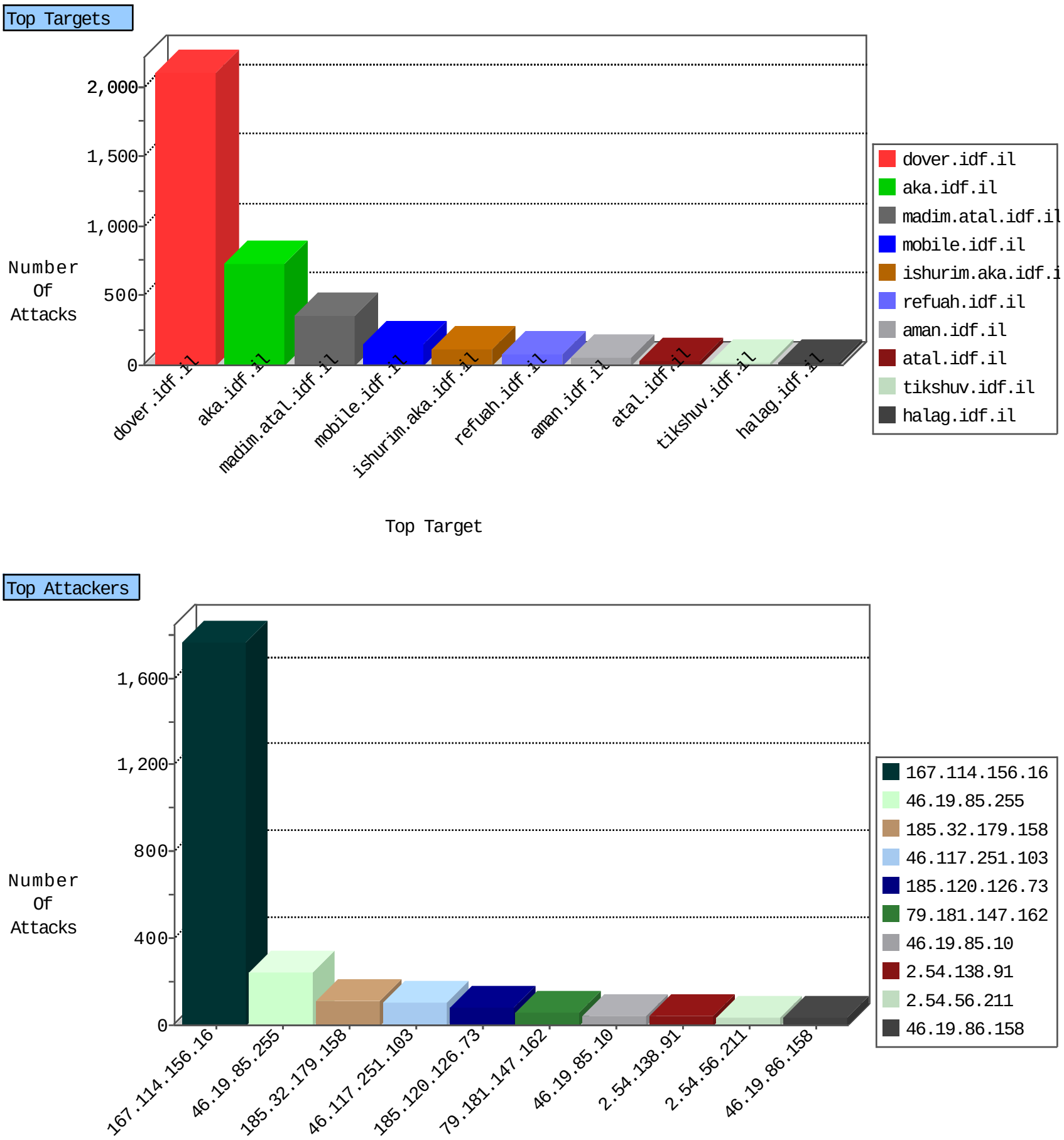
01-05-2016-13:04:02 to 01-05-2016-14:04:02

# IDF Under Attack Daily Report



01-05-2016-13:04:02 to 01-05-2016-14:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.75.214 | Israel | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 5279 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3008 |
| 66.249.75.198 | Israel | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 414 |
| 212.199.154.194 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 126 |
| 79.177.15.236 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 5 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 202.115.255.194 | China | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 71.6.216.36 | United States | 147.237.76.177 | ncore.idf.il | Block_Udp_All_Nets | drop | 1 |
| 132.72.227.31 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 61.152.150.138 | China | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 112.211.96.191 | Philippines | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 117.158.4.29 | China | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |

01-05-2016-13:04:02 to 01-05-2016-14:04:02

## Top Attackers In IPS

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

01-05-2016-13:04:02 to 01-05-2016-14:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 79.176.195.33 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 61.152.150.132 | 147.237.76.39 | China | mobile.meitav.idf.i | GPL SCAN nmap TCP | 1 |
| 52.90.147.148 | 147.237.76.31 | United States | nakchal.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 37.26.148.205 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.179.155.129 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 195.142.117.226 | 147.237.0.200 | Turkey | m4u.idf.il | ET SCAN NMAP -f -sS | 1 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 85.130.216.49 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.179.6.81 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 61.155.203.54 | 147.237.0.200 | China | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 58.246.10.65 | 147.237.76.39 | China | mobile.meitav.idf.i | GPL SCAN nmap TCP | 1 |
| 195.142.117.226 | 147.237.0.200 | Turkey | m4u.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 195.60.232.56 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 190.249.184.162 | 147.237.76.202 | Colombia | e.halag.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 79.181.68.220 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

01-05-2016-13:04:02 to 01-05-2016-14:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.117.251.103 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 91 |
| 46.19.85.255 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 84 |
| 46.19.85.255 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 84 |
| 46.19.85.255 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 76 |
| 79.181.147.162 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 60 |
| 185.120.126.73 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 56 |
| 46.19.86.158 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 36 |
| 185.120.126.73 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 28 |
| 109.253.206.187 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 79.177.212.238 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 23 |
| 2.52.130.163 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 2.54.24.220 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 15 |
| 46.19.86.31 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 176.13.17.51 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 2.52.19.79 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 13 |
| 46.19.85.234 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 12 |
| 66.249.64.250 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 46.117.253.186 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 46.19.85.234 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 109.253.221.28 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 11 |
| 149.50.93.96 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 84.228.170.165 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 9 |
| 79.182.254.8 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 109.253.204.183 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 79.182.254.8 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 79.180.249.204 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 176.58.68.34 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 9 |
| 79.182.254.8 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 9 |
| 46.19.86.143 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 62.0.197.105 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 7 |
| 94.230.86.252 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 84.228.170.165 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 7 |
| 79.181.202.91 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 157.55.39.208 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 213.8.204.20 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 212.199.154.194 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.54.60.7 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.131 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.66.34.193 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 149.78.228.34 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.184 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 213.8.204.20 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.119 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 62.0.219.1 | Israel | 147.237.76.31 | nakchal.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.86.241 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 2.54.191.168 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 46.19.86.103 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 185.32.179.158 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 96 |
| 46.19.85.10 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 43 |
| 2.54.56.211 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 38 |
| 2.54.138.91 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 37 |
| 109.253.132.231 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 29 |
| 109.253.211.94 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 27 |
| 109.253.144.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 21 |
| 185.32.179.158 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 185.32.179.158 | Block | 19 |
| 79.178.139.176 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 79.178.139.176 | Block | 13 |
| 176.13.5.2 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 11 |
| 46.19.85.111 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 79.178.176.170 | Israel | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx | Block | 7 |
| 80.178.186.27 | Israel | 147.237.0.34 | tikshuv.idf.il | Too Many of the Same Response Code (404) in Session from 80.178.186.27 | Block | 7 |
| 109.253.206.187 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 176.13.17.51 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 109.253.221.28 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 77.125.112.10 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.125.112.10 | Block | 5 |
| 46.19.86.48 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 2.52.130.163 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 216.35.195.247 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 4 |
| 109.253.204.183 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 194.114.146.227 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 3 |
| 109.65.157.81 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 138.134.102.16 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 46.19.86.2 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.119 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 2 |
| 46.19.85.79 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.54.160.45 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 46.19.86.94 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx | None | 2 |
| 46.19.85.255 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 212.179.159.253 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc | Block | 2 |
| 46.117.251.103 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Illegal Byte Code Character in Method :4Ã˜Ã¶}~Ã”ÂµÃŒjÃ–Ã¡Â-;MÃ‡Ã¸ HhÃœm 0Â³Â,Â ÃƒÂ¸R%[[#7]] | Block | 1 |
| 37.26.149.213 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 80.74.112.194 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 2.54.185.209 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 79.178.139.176 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/ | Block | 1 |
| 213.151.40.65 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 46.19.86.200 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.253.150.95 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 1 |
| 2.54.23.57 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/layout.css | Block | 1 |
| 67.212.175.138 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteykatava/ | Block | 1 |
| 195.154.227.118 | France | 147.237.77.216 | dover.idf.il | Distributed Illegal HTTP Version | Block | 1 |
| 95.35.165.165 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.85.27 | Israel | 147.237.76.42 | refuah.idf.il | Unknown HTTP Request Method 2bh3y155umfo5az0 in URL | Block | 1 |
| 80.246.136.133 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.117.251.103 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Too Many Headers per Request - 32 Headers | Block | 1 |
| 176.13.3.178 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 31.168.23.59 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/6599.jpg | Block | 1 |
| 79.181.147.162 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 46.117.251.103 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Abnormally Long Header Line request header name | Block | 1 |