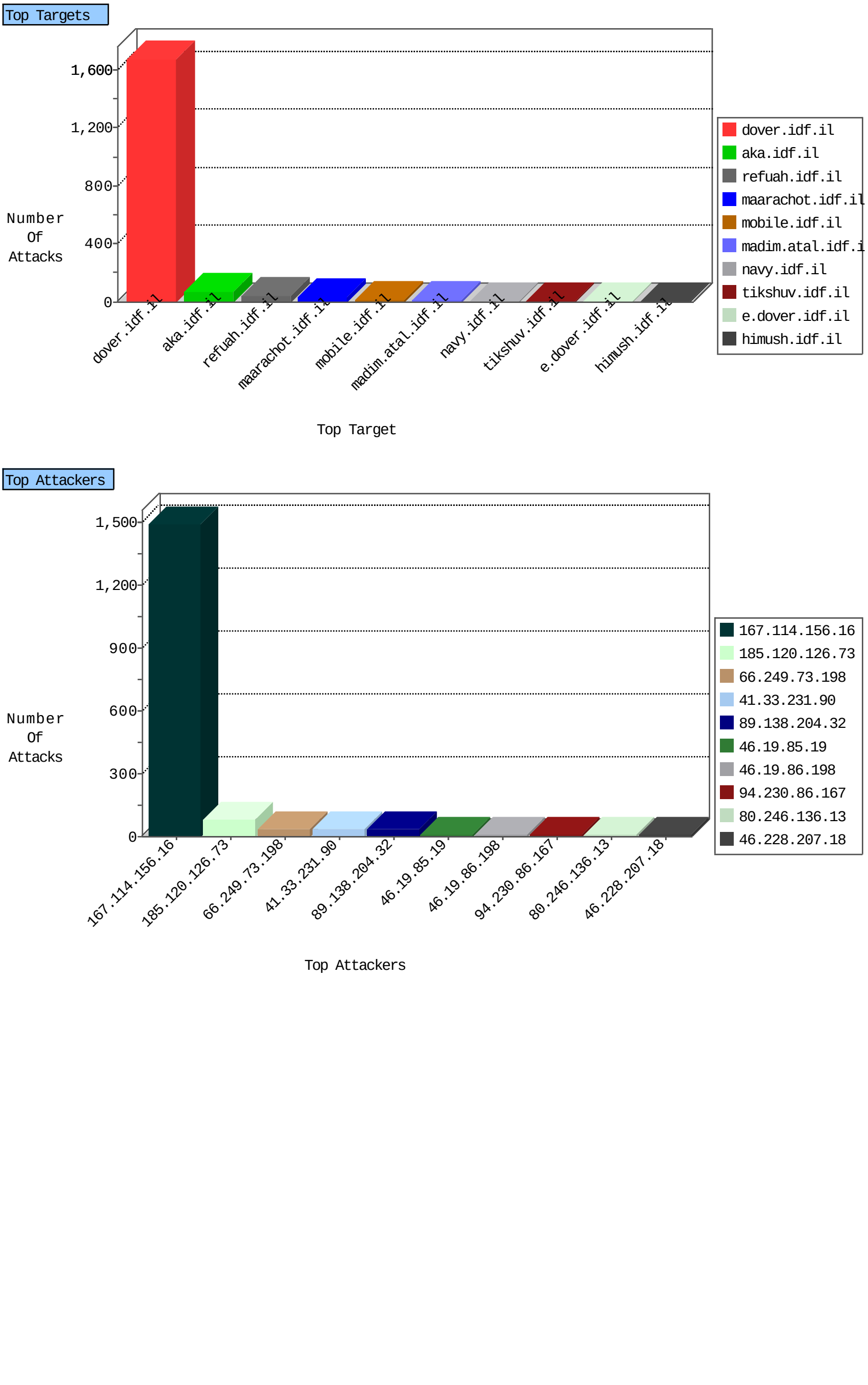
01-06-2016-01:05:18 to 01-06-2016-02:05:18

# IDF Under Attack Daily Report



01-06-2016-01:05:18 to 01-06-2016-02:05:18

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.73.198 | Israel | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 19221 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3153 |
| 66.249.78.146 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 790 |
| 79.181.57.33 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 6 |
| 124.232.150.230 | China | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 27.34.25.101 | Nepal | 147.237.76.44 | e.refuah.idf.il | Block_Udp_All_Nets | drop | 1 |

01-06-2016-01:05:18 to 01-06-2016-02:05:18

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 104.255.65.207 | | 147.237.77.19 | law-forum.idf.il | C003: HTTP: phpMyAdmin access | Block | 1 |
| 104.255.65.207 | | 147.237.76.200 | eitan.aka.idf.il | C003: HTTP: phpMyAdmin access | Block | 1 |

01-06-2016-01:05:18 to 01-06-2016-02:05:18

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 46.228.207.18 | 147.237.76.31 | Germany | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.130.5.235 | 147.237.76.42 | | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.228.207.18 | 147.237.0.34 | Germany | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.130.5.235 | 147.237.0.15 | | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 167.114.156.198 | 147.237.77.216 | Canada | dover.idf.il | SERVER-APACHE Apache mod_proxy reverse proxy information disclosure attempt | 1 |
| 123.133.12.112 | 147.237.8.28 | China | e.mobile-ks.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 104.200.78.42 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.161.227.206 | 147.237.0.33 | China | idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 46.228.207.18 | 147.237.77.227 | Germany | e.hamaz.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 46.228.207.18 | 147.237.76.31 | Germany | nakchal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 200.63.163.131 | 147.237.77.243 | Argentina | mobile.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 46.228.207.18 | 147.237.72.14 | Germany | dover.idf.il(old) | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.130.5.235 | 147.237.8.28 | | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 27.41.244.38 | 147.237.76.30 | China | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 168.62.238.153 | 147.237.77.121 | United States | e.navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 167.88.9.227 | 147.237.76.148 | United States | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 104.200.78.42 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.200.78.42 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.228.207.18 | 147.237.77.233 | Germany | atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 46.228.207.18 | 147.237.76.34 | Germany | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

01-06-2016-01:05:18 to 01-06-2016-02:05:18

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 63 |
| 185.120.126.73 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 56 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 35 |
| 89.138.204.32 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 35 |
| 185.120.126.73 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 28 |
| 46.19.86.198 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 94.230.86.167 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 80.246.136.13 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.19 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 207.46.13.4 | United States | 147.237.77.212 | e.dover.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 6 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 94.121.47.160 | Turkey | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 85.65.124.18 | Israel | 147.237.72.167 | ishurim.aka.idf.i | drop | First packet isn't SYN | drop | 4 |
| 185.3.146.224 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 104.238.32.54 | | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.160.209.150 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.152.245 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.66.95 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 109.253.138.57 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 109.253.138.57 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 203.133.170.140 | Korea, Republic of | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 2 |
| 46.19.86.155 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 81.169.237.146 | Germany | 147.237.8.45 | e.eitan.idf.il | drop | SAM rule | drop | 2 |
| 46.19.86.155 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 81.169.237.146 | Germany | 147.237.8.46 | e.chinuch.idf.il | drop | SAM rule | drop | 2 |
| 46.19.85.145 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 46.19.86.127 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 203.133.169.72 | Korea, Republic of | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 141.212.122.186 | United States | 147.237.76.202 | e.halag.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 54.183.120.101 | United States | 147.237.8.14 | e.orchot.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.121.173 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 216.58.110.146 | Canada | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 46.19.85.207 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 2.54.185.231 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 85.64.72.228 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.122.223 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.155 | United States | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 54.186.248.49 | United States | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 1 |
| 46.19.86.128 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.121.171 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 203.133.170.140 | Korea, Republic of | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 46.19.85.19 | Israel | 147.237.0.19 | madim.atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 181.21.135.92 | Argentina | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 141.212.122.187 | United States | 147.237.76.202 | e.halag.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 54.183.120.101 | United States | 147.237.76.44 | e.refuah.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.121.174 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 46.19.85.240 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 188.120.148.141 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 8.37.228.77 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Response out of state | monitor | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.54.139.19 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 109.253.157.186 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 37.142.64.107 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 3 |
| 79.176.29.181 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 167.114.156.198 | Canada | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 167.114.156.198 | Block | 2 |
| 80.246.133.141 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 2 |
| 87.69.132.189 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il | Block | 2 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 2 |
| 46.120.140.58 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 2 |
| 46.210.198.76 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 54.183.120.101 | United States | 147.237.77.19 | law-forum.idf.il | Unauthorized URL Access to 147.237.77.19/ | Block | 1 |
| 217.132.3.13 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Illegal Parameter Encoding %uzR)!q* {Q^vCgAz4I)p-e( in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx | None | 1 |
| 84.109.106.197 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/himush | Block | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/resources/images/miluim-over.jpg | Block | 1 |
| 194.150.168.95 | Germany | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 46.19.86.155 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/ | Block | 1 |
| 8.37.70.44 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he/dover.aspx&usg=alkjrhgbykait3addbl34w54dkaamvkesq | Block | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 79.178.136.69 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 54.186.248.49 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1294-he/www.idf.il | Block | 1 |
| 217.132.3.13 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Multiple Illegal Parameter Encoding from 217.132.3.13 | None | 1 |
| 167.114.156.198 | Canada | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/ | Block | 1 |
| 39.158.119.169 | China | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi | Block | 1 |
| 85.65.25.95 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.246 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/resources/images/miluim.jpg | Block | 1 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 46.120.95.124 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 8.37.70.135 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/&usg=alkjrhjxn39o6xcqv6o6zgvhmhijejtyja | Block | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 66.249.66.136 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2431.jpg | Block | 1 |
| 176.10.104.240 | Switzerland | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 46.19.85.19 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew/organization/artillery | Block | 1 |
| 8.37.70.243 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1153-he/dover.aspx&usg=alkjrhjch8cv5mje3rrfmvfphsvzvlp0sq | Block | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 80.246.136.13 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.66.182 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/ | Block | 1 |
| 176.13.16.5 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.85.19 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 89.138.204.32 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/text.css | Block | 1 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 8.37.71.15 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1153-he/dover.aspx&usg=alkjrhijq0p22sz7fhxhxzyk2fgdsx36ha | Block | 1 |
| 82.113.121.233 | Germany | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to www.maarachot.idf.il/pdf/files | Block | 1 |
| 66.249.69.2 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/inservice-over.jpg | Block | 1 |
| 194.72.238.241 | United Kingdom | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 194.72.238.241 | Block | 1 |
| 46.19.85.140 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 2.54.175.33 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 107.178.194.79 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |