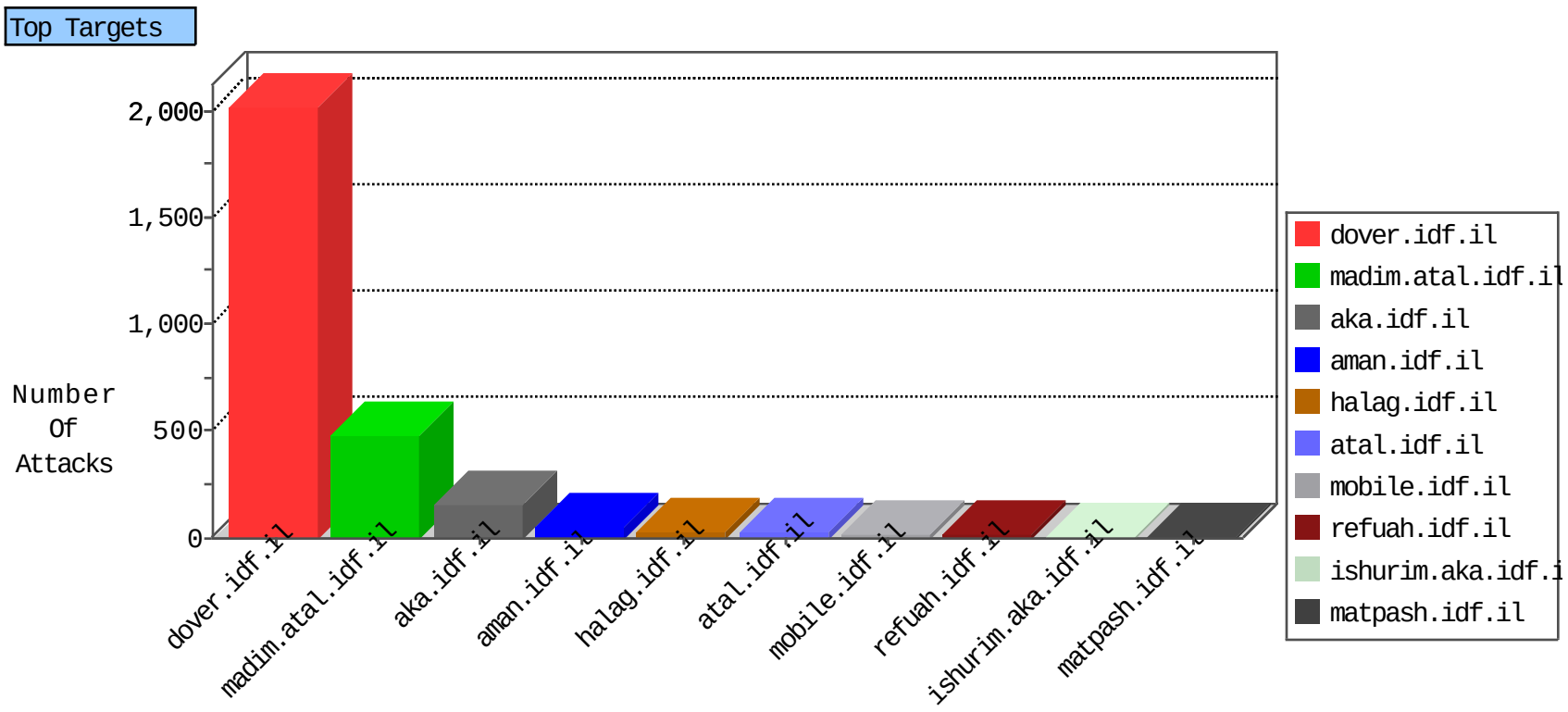
12-13-2015-23:04:07 to 12-14-2015-00:04:07

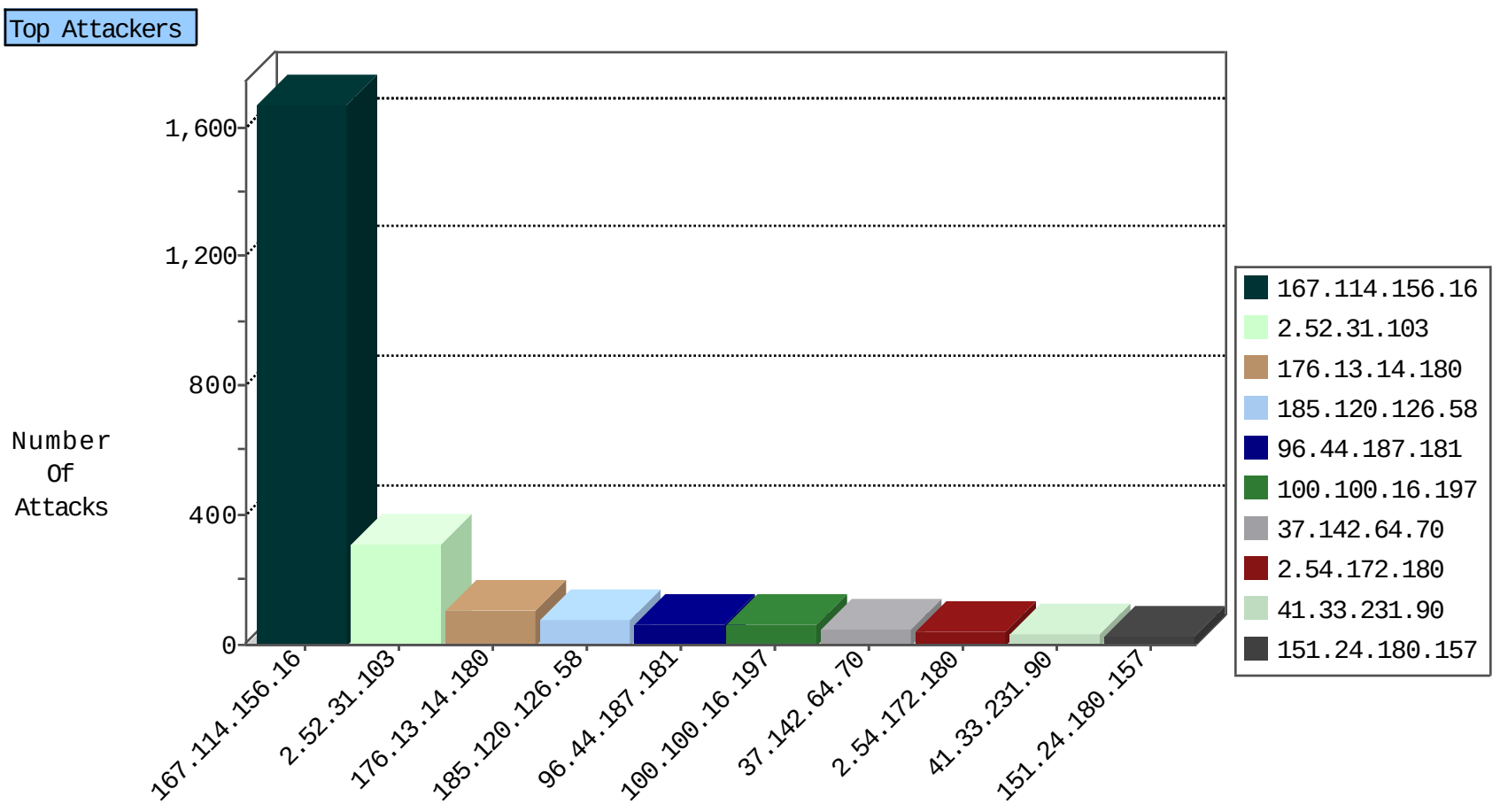
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

12-13-2015-23:04:07 to 12-14-2015-00:04:07

## 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 | 3731 |
| 66.249.64.190 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 155 |
| 109.64.200.16 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 6 |
| 115.230.124.164 | China | 147.237.77.216 | dover.idf.il | block-sp-traf1 | drop | 1 |
| 46.166.139.20 | Netherlands | 147.237.76.86 | navy.idf.il | Block_Ntp_All_Net | drop | 1 |
| 146.185.239.100 | Russian Federation | 147.237.72.166 | aka.idf.il | block-sp-traf1 | drop | 1 |

12-13-2015-23:04:07 to 12-14-2015-00:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 96.44.187.181 | United States | 147.237.77.216 | dover.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 26 |
| 96.44.187.181 | United States | 147.237.77.216 | dover.idf.il | 0854: HTTP: upload* Access | Block | 7 |
| 96.44.187.181 | United States | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 106.38.241.106 | China | 147.237.77.170 | maarachot.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 1 |

12-13-2015-23:04:07 to 12-14-2015-00:04:07

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 |
| 60.30.204.2 | 147.237.0.19 | China | madim.atal.idf.il | GPL SCAN nmap TCP | 2 |
| 69.54.59.231 | 147.237.76.31 | United States | nakchal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 58.253.96.122 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 58.253.96.122 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -f -sS | 1 |
| 58.253.96.122 | 147.237.76.42 | China | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.57.11.7 | 147.237.76.202 | China | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.20.69.98 | 147.237.76.44 | United States | e.refuah.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 104.219.238.10 | 147.237.76.148 | | gqcenter.aka.idf.i | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 94.102.48.195 | 147.237.72.217 | Netherlands | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.253.96.122 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.253.96.122 | 147.237.76.42 | China | refuah.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 218.57.11.7 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.155.65.247 | 147.237.8.28 | United States | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

12-13-2015-23:04:07 to 12-14-2015-00:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 185.120.126.58 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 52 |
| 2.54.172.180 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 40 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 100.100.16.197 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 151.24.180.157 | Italy | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 29 |
| 185.120.126.58 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 26 |
| 93.172.54.140 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 23 |
| 100.100.16.197 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 100.100.16.197 | | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 12 |
| 97.34.66.221 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 85.114.127.10 | Palestinian Territory, Occupied | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 7 |
| 79.178.160.105 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.177.17.39 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 97.34.66.221 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.67.100.73 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.178.3.135 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 85.64.130.142 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 82.80.128.110 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 93.173.158.215 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 93.173.158.215 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 5.102.254.178 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 84.111.182.95 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 37.142.192.120 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 84.111.182.95 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 85.114.127.10 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 176.13.5.233 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 62.90.203.73 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.183.1.143 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.66.141.235 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 157.55.39.69 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.215.241.103 | Denmark | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 37.46.39.84 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 79.180.23.81 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.142.192.120 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 5.255.253.188 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.183.229.161 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.52.170.243 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.176.16.40 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.67.51.166 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.49.162 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.12.147.165 | Israel | 147.237.77.243 | mobile.idf.il | drop | First packet isn't SYN | drop | 3 |
| 149.78.232.254 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 40.77.167.59 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.102.254.128 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 109.64.200.16 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.213 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 109.67.115.55 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 2 |
| 46.19.85.111 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 188.120.148.233 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.52.31.103 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 187 |
| 2.52.31.103 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 122 |
| 176.13.14.180 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 85 |
| 37.142.64.70 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 44 |
| 96.44.187.181 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 96.44.187.181 | Block | 26 |
| 176.13.14.180 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 19 |
| 147.251.43.64 | Czech Republic | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 147.251.43.64 | Block | 5 |
| 141.0.11.148 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/aman | Block | 4 |
| 207.241.226.39 | United States | 147.237.77.234 | halag.idf.il | Multiple Unauthorized URL Access from 207.241.226.39 | Block | 4 |
| 207.241.226.39 | United States | 147.237.77.234 | halag.idf.il | PHP Attempt | Block | 3 |
| 5.28.147.129 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.5.233 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.54.160.154 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 207.46.13.187 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/ | Block | 2 |
| 80.230.25.250 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 213.57.172.7 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.177.57.91 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 46.121.123.29 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 46.121.123.29 | Block | 2 |
| 37.142.64.70 | Israel | 147.237.0.19 | madim.atal.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx | Block | 2 |
| 80.246.136.242 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 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 | 2 |
| 79.178.107.201 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 79.178.107.201 | Block | 2 |
| 46.19.86.145 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | 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 |
| 176.12.142.4 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 84.95.116.55 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 109.186.188.37 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 66.249.64.13 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 46.19.85.105 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 107.178.195.163 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 178.74.239.104 | Ukraine | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 84.108.220.32 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.64.243 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/021904-1.stm, | Block | 1 |
| 147.251.43.64 | Czech Republic | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/896- | Block | 1 |
| 46.117.57.108 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.67.115.55 | Israel | 147.237.72.156 | aman.idf.il | Too Many Cookies in a Request - 101 cookies | Block | 1 |
| 96.44.187.181 | United States | 147.237.77.216 | dover.idf.il | Multiple Admin Blocking from 96.44.187.181 | Block | 1 |
| 2.52.10.7 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif | None | 1 |
| 66.249.64.23 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 46.19.86.68 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 107.178.195.171 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 5.28.136.235 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif | Block | 1 |
| 195.154.146.225 | France | 147.237.77.216 | dover.idf.il | Illegal HTTP Version HTTP/ | Block | 1 |
| 84.109.1.219 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 149.88.38.249 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 109.93.139.249 |  | 147.237.77.176 | matpash.idf.il | PHP Attempt | Block | 1 |
| 207.241.226.39 | United States | 147.237.0.15 | kosher-kravi.idf.il | Multiple Unauthorized URL Access from 207.241.226.39 | Block | 1 |
| 141.212.122.97 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to /x | Block | 1 |
| 66.249.64.131 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 46.19.86.130 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |