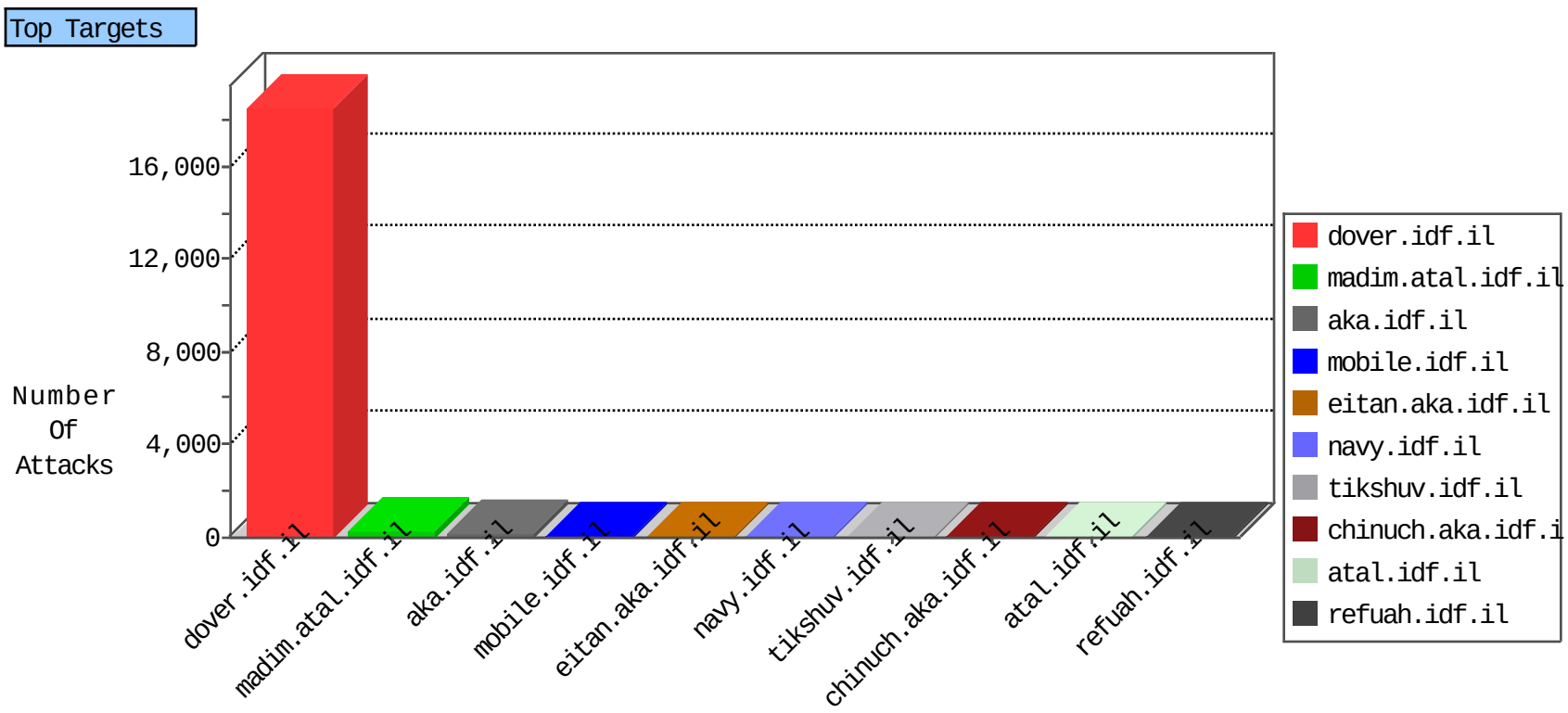
04-20-2016-22:04:04 to 04-20-2016-23:04:04

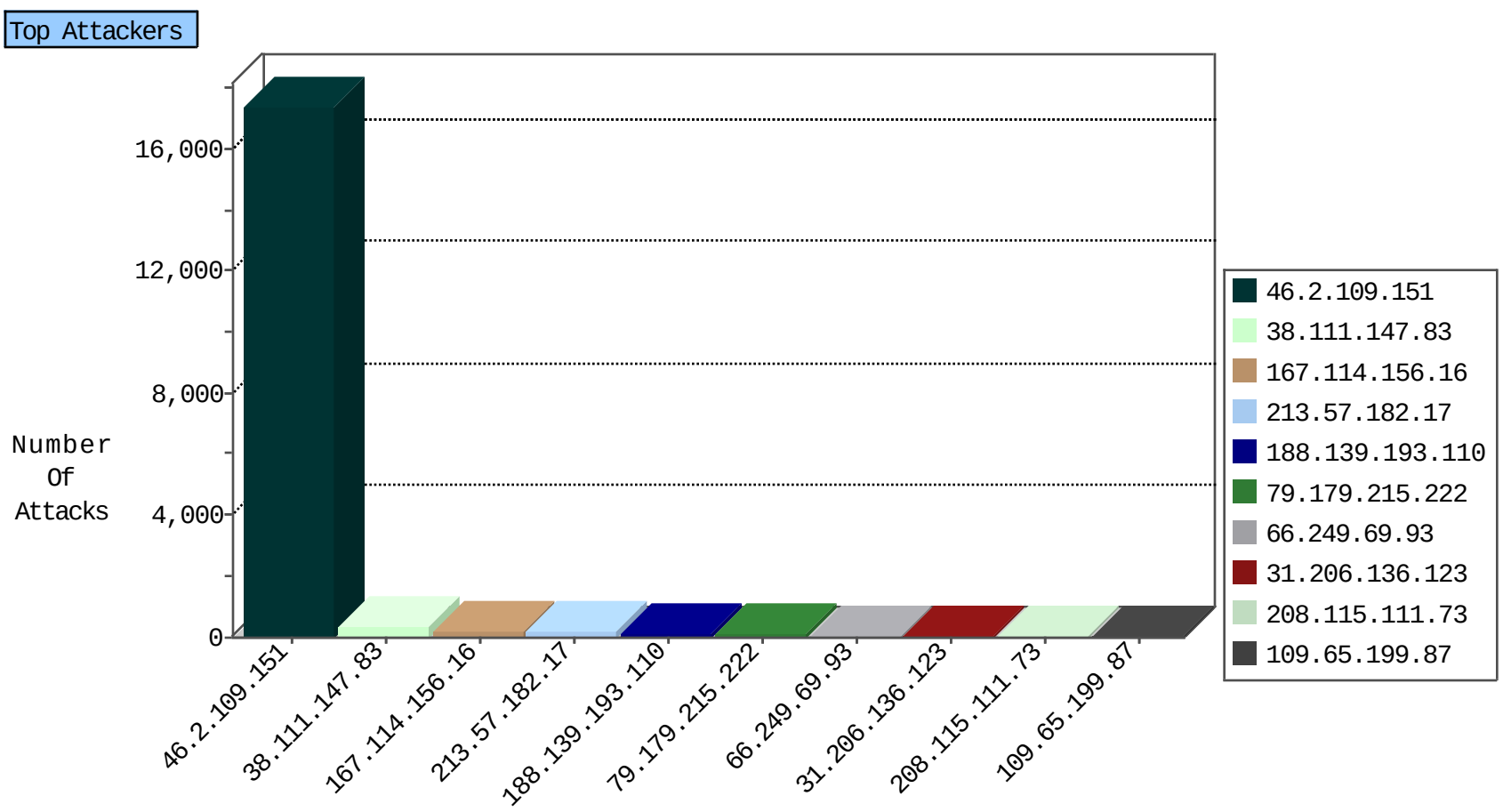
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

04-20-2016-22:04:04 to 04-20-2016-23:04:04

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 | HTTP-POST-Segmented-DoS | dest-reset | 12141 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 11860 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 5496 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-MISC-Slowloris-DOS-Var1 | dest-reset | 59 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 20 |
| 123.59.59.52 | China | 147.237.77.226 | www.chamatz.aka.idf.il | block-sp-traf1 | drop | 2 |
| 69.30.202.230 | United States | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | forward | 2 |
| 69.197.185.22 | United States | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | forward | 2 |
| 74.91.23.107 | United States | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | forward | 2 |
| 69.30.226.101 | United States | 147.237.76.200 | eitan.aka.idf.il | block-sp-traf1 | forward | 2 |
| 74.91.23.109 | United States | 147.237.76.42 | refuah.idf.il | block-sp-traf1 | forward | 2 |
| 69.197.185.22 | United States | 147.237.0.15 | kosher-kravi.idf.il | block-sp-traf1 | forward | 1 |
| 69.30.226.100 | United States | 147.237.0.19 | madim.atal.idf.il | block-sp-traf1 | forward | 1 |
| 69.30.202.228 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | block-sp-traf1 | forward | 1 |

04-20-2016-22:04:04 to 04-20-2016-23:04:04

## Top Attackers In IPS

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

04-20-2016-22:04:04 to 04-20-2016-23:04:04

## 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 | 2 |
| 104.130.70.221 | 147.237.77.179 | United States | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 85.131.208.140 | 147.237.77.178 | Germany | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.131.208.140 | 147.237.76.177 | Germany | ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.131.208.140 | 147.237.8.45 | Germany | e.eitan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.131.208.140 | 147.237.8.27 | Germany | e.madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.131.208.140 | 147.237.0.16 | Germany | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.20.69.74 | 147.237.77.179 | United States | e.mazi.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 80.82.78.38 | 147.237.77.19 | Netherlands | law-forum.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.12.184.172 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.43.68.142 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 173.65.154.27 | 147.237.0.15 | United States | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 85.131.208.140 | 147.237.77.226 | Germany | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.131.208.140 | 147.237.76.198 | Germany | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.131.208.140 | 147.237.76.39 | Germany | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.131.208.140 | 147.237.8.28 | Germany | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.131.208.140 | 147.237.0.33 | Germany | idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.131.208.140 | 147.237.0.15 | Germany | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 80.82.78.38 | 147.237.76.197 | Netherlands | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 173.65.154.27 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

04-20-2016-22:04:04 to 04-20-2016-23:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.2.109.151 | Turkey | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 13938 |
| 38.111.147.83 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 343 |
| 188.139.193.110 | Syrian Arab Republic | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 70 |
| 188.139.193.110 | Syrian Arab Republic | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 69 |
| 66.249.69.93 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 42 |
| 31.206.136.123 | Turkey | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 29 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 109.65.199.87 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 46.2.109.151 | Turkey | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 185.32.179.159 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 207.241.229.102 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 18 |
| 79.183.138.131 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 16 |
| 69.175.127.10 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 79.177.232.31 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 88.67.146.148 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 176.13.15.126 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 52.29.223.39 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 185.75.97.5 | Iraq | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 198.58.96.215 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 66.249.66.184 | United States | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 162.243.99.146 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 41.128.165.8 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 70.28.86.138 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 72.9.148.10 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 149.50.112.62 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 178.238.225.108 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 45.33.135.237 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 67.54.168.251 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 216.165.95.7 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 5.102.254.177 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 31.13.167.190 | Palestinian Territory Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 77.127.147.65 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.146 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 2.53.15.169 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.146 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.146 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 46.19.85.146 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 157.55.39.151 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 203.133.170.155 | Korea, Republic of | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 109.66.26.166 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 149.88.219.7 | Israel | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 107.77.70.121 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.2.109.151 | Turkey | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |
| 52.58.92.83 | Germany | 147.237.76.198 | e.yohalan.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 4 |
| 199.30.24.131 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.2.109.151 | Turkey | 147.237.77.216 | dover.idf.il | Automated Vulnerability Scanning V1 | Block | 3451 |
| 213.57.182.17 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 180 |
| 79.179.215.222 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 96 |
| 68.82.35.97 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 68.82.35.97 | Block | 16 |
| 213.57.246.79 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 188.139.193.110 | Syrian Arab Republic | 147.237.77.216 | dover.idf.il | Distributed Abnormally Long Request | Block | 5 |
| 84.109.160.102 | Israel | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 84.109.160.102 | Block | 5 |
| 46.19.86.88 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.23.241 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.177.232.31 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.136.96 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 5.248.253.133 | Ukraine | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1556-en/ | Block | 3 |
| 176.13.17.114 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 95.86.120.227 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 95.86.120.227 | Block | 2 |
| 131.253.25.160 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 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 |
| 109.65.134.23 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx | None | 1 |
| 79.180.53.240 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/ | Block | 1 |
| 207.46.13.118 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 69.30.226.100 | United States | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to www.369bs.com/ | Block | 1 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 88.67.146.148 | Germany | 147.237.77.216 | dover.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1283-en/dover.aspx | Block | 1 |
| 74.91.23.107 | United States | 147.237.76.147 | chinuch.aka.idf.il | Distributed Unauthorized URL Access on www.app-softwares.com/ | Block | 1 |
| 68.235.243.237 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 109.66.26.166 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 54.210.18.124 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/robots.txt | Block | 1 |
| 79.181.180.114 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb13148377 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 69.30.226.101 | United States | 147.237.76.200 | eitan.aka.idf.il | Distributed Unauthorized URL Access on www.369bs.com/ | Block | 1 |
| 178.137.89.21 | Ukraine | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 178.137.89.21 | Block | 1 |
| 68.235.243.237 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 188.161.97.118 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/894-ar | Block | 1 |
| 62.117.59.18 | Egypt | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/newsflash/mobile | Block | 1 |
| 69.197.185.22 | United States | 147.237.0.15 | kosher-kravi.idf.il | Unauthorized URL Access to www.ps780.com/ | Block | 1 |
| 68.82.35.97 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/homepage/mobile | Block | 1 |
| 178.137.89.21 | Ukraine | 147.237.77.216 | dover.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx | Block | 1 |
| 95.86.120.227 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 203.133.170.31 | Korea, Republic of | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx | Block | 1 |
| 69.30.202.228 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | Unauthorized URL Access to www.369bs.com/ | Block | 1 |
| 157.55.39.151 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 213.151.36.128 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 69.197.185.22 | United States | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.ps780.com/ | Block | 1 |
| 68.180.230.45 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 178.238.225.108 | Germany | 147.237.77.216 | dover.idf.il | URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js | Block | 1 |
| 109.64.25.109 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/rights/asp/inf...17&catid=22703 | Block | 1 |
| 79.180.53.240 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 1 |
| 204.79.180.159 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 69.30.202.230 | United States | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.369bs.com/ | Block | 1 |
| 66.249.75.44 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx | Block | 1 |
| 84.109.160.102 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile | Block | 1 |