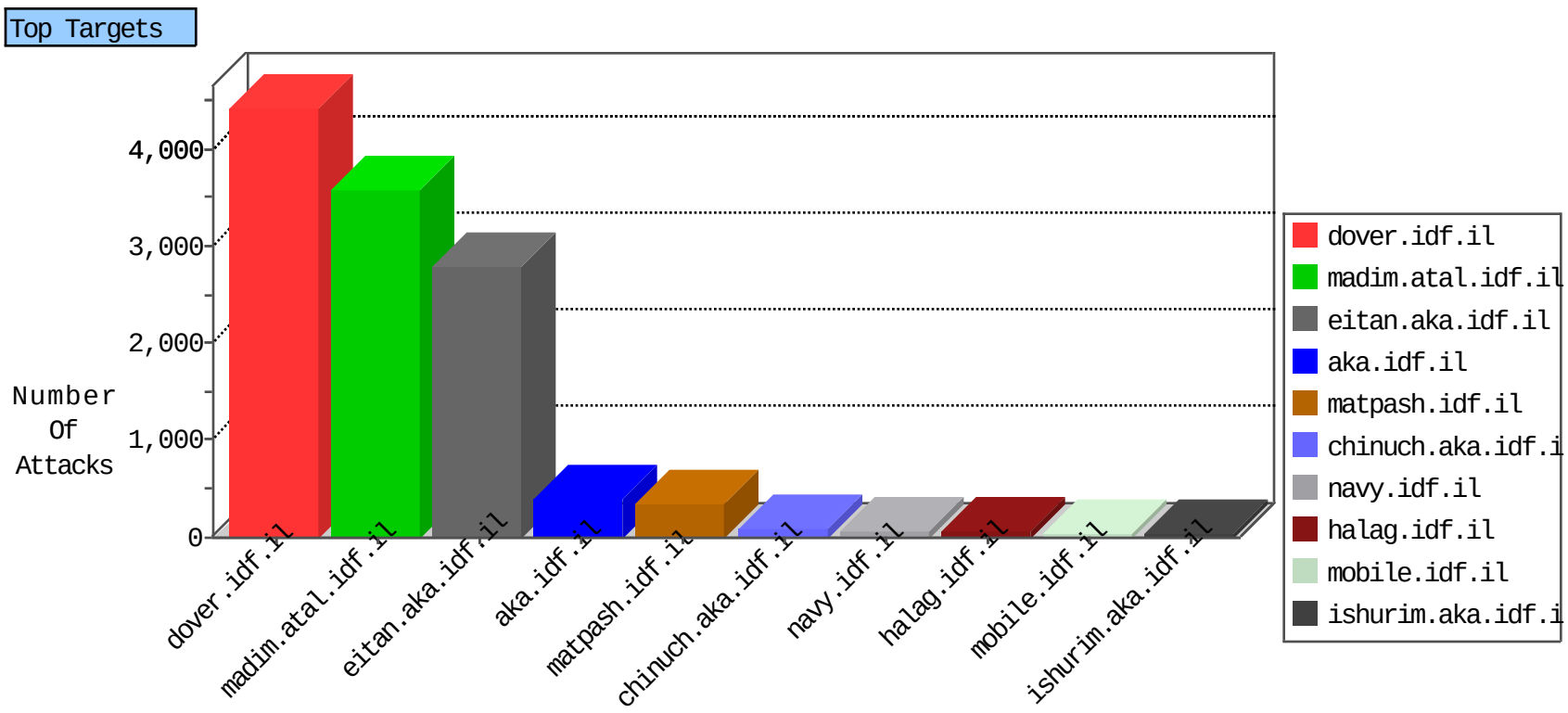
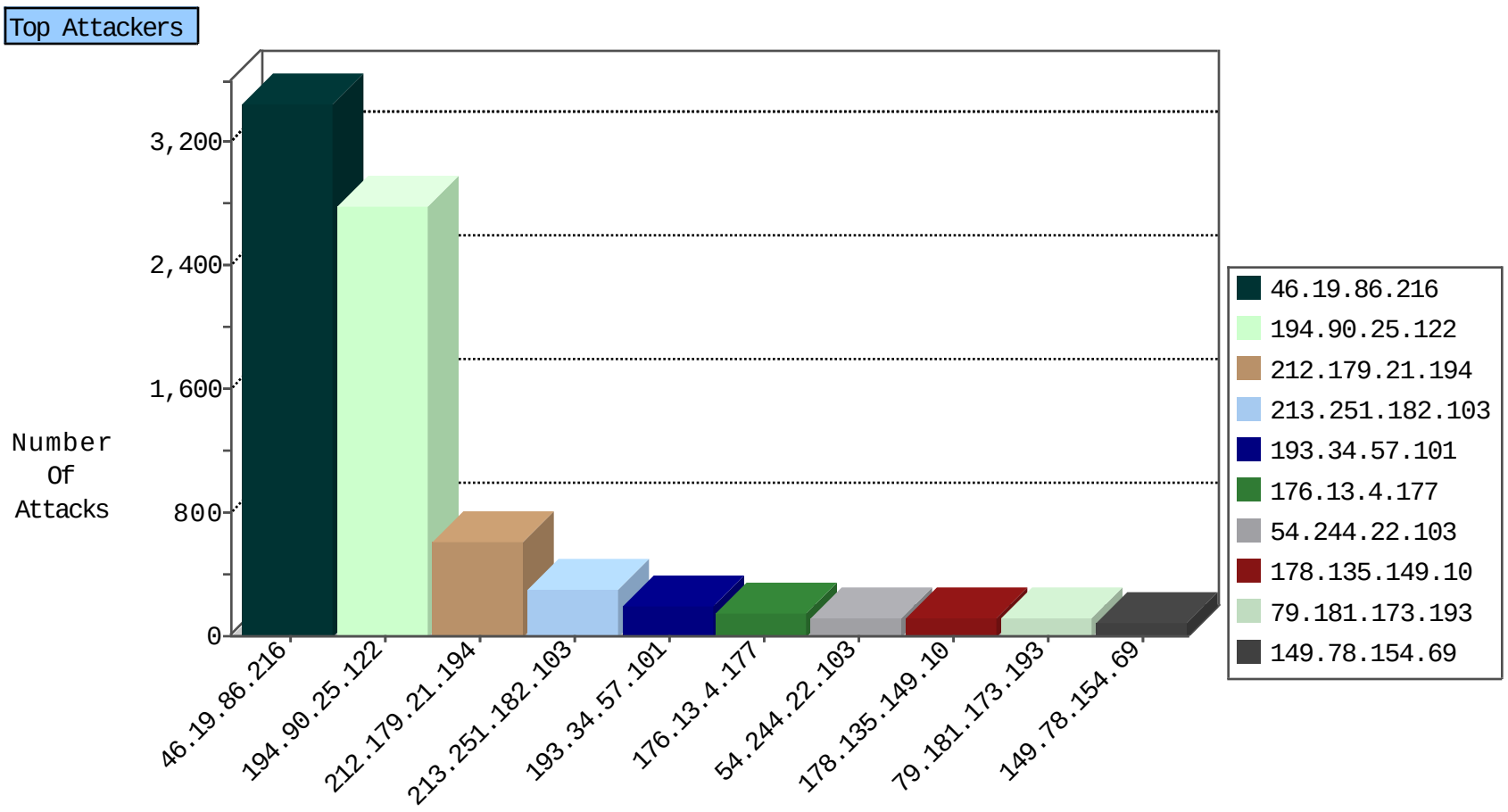
10-22-2015-08:04:07 to 10-22-2015-09:04:07

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



10-22-2015-08:04:07 to 10-22-2015-09:04:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 62 |
| 220.171.43.1 | China | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 12 |
| 81.218.48.37 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 11 |
| 82.213.48.225 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 46.19.85.118 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 9 |
| 37.26.146.203 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 176.13.21.105 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 84.253.54.97 | Switzerland | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 2.52.34.23 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 212.14.228.162 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 147.235.185.74 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 37.76.221.76 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 74.143.58.3 | United States | 147.237.76.44 | e.refuah.idf.il | Block_Udp_All_Nets | drop | 1 |
| 176.13.16.250 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 80.179.255.6 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 89.248.172.98 | Netherlands | 147.237.76.147 | chinuch.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 5.8.66.69 | Russian Federation | 147.237.76.202 | e.halag.idf.il | Block_Ntp_All_Net | drop | 1 |
| 89.248.172.98 | Netherlands | 147.237.76.176 | test.ncore.idf.il | Block_Udp_All_Nets | drop | 1 |
| 66.87.120.75 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |

10-22-2015-08:04:07 to 10-22-2015-09:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 212.179.197.2 | Israel | 147.237.76.42 | refuah.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 79.182.105.16 | Israel | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 1 |
| 84.228.127.150 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 1 |

10-22-2015-08:04:07 to 10-22-2015-09:04:07

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 |
| 27.75.168.255 | 147.237.0.34 | Vietnam | tikshuv.idf.il | ET SCAN Potential SSH Scan | 3 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 190.124.35.115 | 147.237.72.217 | Nicaragua | e.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 188.86.253.131 | 147.237.0.200 | Spain | m4u.idf.il | ET SCAN NMAP -f -sS | 1 |
| 172.8.58.186 | 147.237.77.19 | United States | law-forum.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 169.229.3.90 | 147.237.76.39 | United States | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 80.82.78.169 | 147.237.76.198 | Netherlands | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 77.126.117.20 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 222.186.58.131 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 190.124.35.115 | 147.237.77.226 | Nicaragua | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 190.124.35.115 | 147.237.72.217 | Nicaragua | e.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 188.86.253.131 | 147.237.0.200 | Spain | m4u.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 173.193.252.242 | 147.237.77.227 | United States | e.hamaz.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 172.8.58.186 | 147.237.77.19 | United States | law-forum.idf.il | ET SCAN NMAP -f -sS | 1 |
| 80.82.78.169 | 147.237.76.201 | Netherlands | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 80.82.78.169 | 147.237.76.176 | Netherlands | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.186.58.131 | 147.237.0.34 | China | tikshuv.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 2.52.33.187 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 190.124.35.115 | 147.237.77.226 | Nicaragua | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

10-22-2015-08:04:07 to 10-22-2015-09:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 569 |
| 193.34.57.101 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 191 |
| 54.244.22.103 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 122 |
| 178.135.149.10 | Lebanon | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 116 |
| 79.181.173.193 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 108 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 79 |
| 137.135.176.71 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 70 |
| 5.22.129.209 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 66 |
| 132.66.237.191 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 53 |
| 37.26.147.242 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 48 |
| 54.187.55.213 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 46 |
| 188.120.150.212 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 45 |
| 81.218.251.252 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 45 |
| 192.0.81.190 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 45 |
| 2.54.60.135 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 44 |
| 207.195.86.1 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 34 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 33 |
| 82.205.90.201 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 33 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 32 |
| 46.19.85.3 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 29 |
| 176.13.5.118 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 199.203.94.202 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 28 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 212.76.101.122 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 176.13.2.218 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 212.179.21.194 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 176.13.16.109 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 151.80.31.115 | Italy | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 64.233.172.163 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 192.117.150.233 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 93.172.0.25 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 54.224.21.23 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 194.90.25.122 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 22 |
| 46.19.85.16 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 213.8.68.217 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 207.46.13.178 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 80.246.130.35 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 93.172.184.58 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 46.19.86.162 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 79.176.199.101 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 37.26.146.203 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 81.218.48.37 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 46.19.86.216 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 100.100.58.97 |  | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 66.249.93.192 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 79.179.55.169 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.216 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.86.216 | Block | 3420 |
| 194.90.25.122 | Israel | 147.237.76.200 | eitan.aka.idf.il | Too Many of the Same Response Code (404) in Session from 194.90.25.122 | Block | 2720 |
| 213.251.182.103 | France | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src | Block | 294 |
| 176.13.4.177 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 140 |
| 2.54.136.36 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 42 |
| 188.143.232.11 | Russian Federation | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 42 |
| 151.80.31.115 | Italy | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 42 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 28 |
| 2.54.15.234 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 28 |
| 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 | 28 |
| 81.218.37.2 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/favicon.ico | Block | 28 |
| 192.114.23.210 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 28 |
| 188.143.232.22 | Russian Federation | 147.237.76.147 | chinuch.aka.idf.il | Multiple Unauthorized URL Access from 188.143.232.22 | Block | 28 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 28 |
| 62.90.99.139 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 28 |
| 194.90.25.122 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 28 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 66.249.64.37 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/ | Block | 14 |
| 176.13.7.69 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 14 |
| 81.218.34.242 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/size338x0/1564.jpg | Block | 14 |
| 203.160.125.53 | New Zealand | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 14 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.166 | Block | 14 |
| 188.143.232.22 | Russian Federation | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/900-he/ | Block | 14 |
| 157.55.39.50 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 14 |
| 212.143.186.129 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il./ | Block | 14 |
| 66.249.64.108 | Israel | 147.237.77.74 | law.idf.il | Distributed Unauthorized URL Access on 147.237.77.74/robots.txt | Block | 14 |
| 194.90.25.122 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/datatables.hebrew | Block | 14 |
| 185.32.179.228 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 14 |
| 207.46.13.35 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/miluim/hovot | Block | 14 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 61.135.190.71 | China | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to 147.237.0.19/ | Block | 14 |
| 157.55.39.51 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/ | Block | 14 |
| 74.82.47.2 | United States | 147.237.72.167 | ishurim.aka.idf.il | Unauthorized URL Access to 147.237.72.167/ | Block | 14 |
| 212.179.159.253 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif | Block | 14 |
| 199.16.156.125 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/17396.jpg | Block | 14 |
| 66.249.67.65 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 31.168.151.111 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 14 |
| 82.80.128.8 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 14 |
| 207.46.13.46 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/chinuch/ | Block | 14 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp | Block | 14 |
| 61.135.190.201 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Unauthorized URL Access on 147.237.0.17/ | Block | 14 |
| 192.117.150.233 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 14 |
| 157.55.39.200 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/ | Block | 14 |
| 79.180.174.107 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx | None | 14 |
| 199.16.156.126 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17396.jpg | Block | 14 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 14 |
| 46.19.85.144 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1880 | Block | 14 |
| 92.225.38.238 | Germany | 147.237.77.216 | dover.idf.il | Suspicious Response Code | Block | 14 |
| 207.46.13.119 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx | None | 14 |
| 81.218.34.242 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 14 |