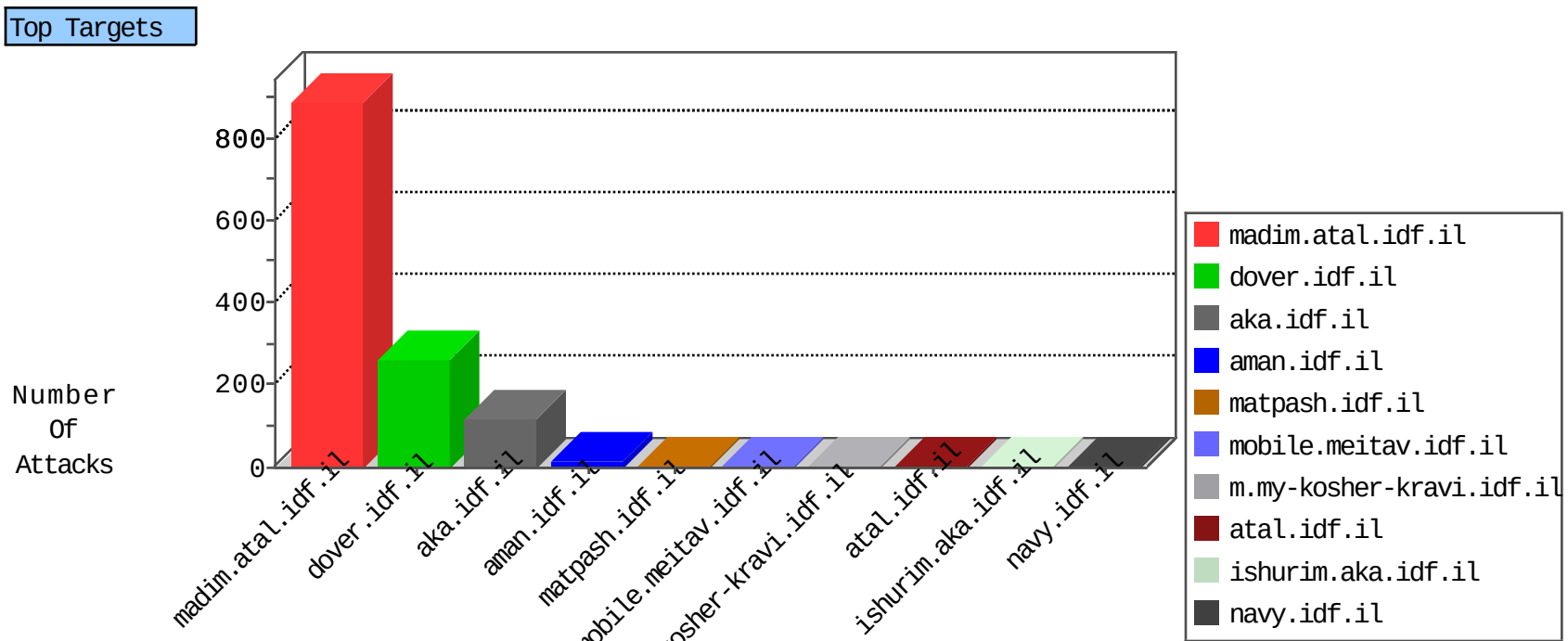
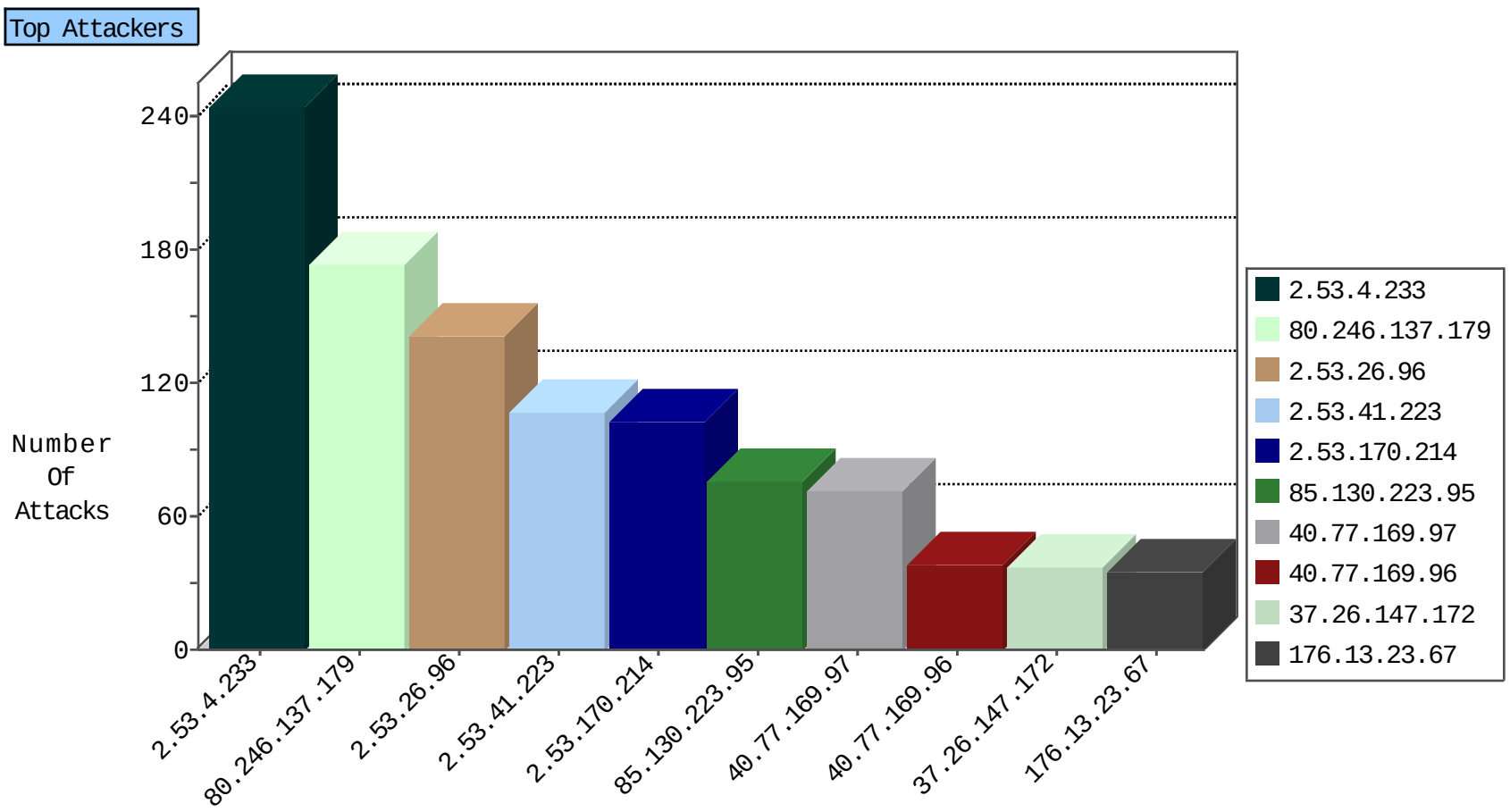
08-23-2016-14:04:00 to 08-23-2016-15:04:00

# IDF Under Attack Daily Report

Top Targets




Top Attackers



08-23-2016-14:04:00 to 08-23-2016-15:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 181.49.177.171 | Colombia | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4 |
| 137.74.157.88 | Hong Kong | 147.237.76.198 | e.yohalan.idf.il | Black List | drop | 1 |
| 176.13.23.67 | Israel | 147.237.0.19 | madim.atal.idf.il | DOSS-SSL-ClearText | drop | 1 |

08-23-2016-14:04:00 to 08-23-2016-15:04:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.165.197.141 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 162.210.196.130 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 199.58.86.209 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 199.58.86.211 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |

08-23-2016-14:04:00 to 08-23-2016-15:04:00

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 85.207.157.29 | 147.237.0.17 | Czech Republic | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 4 |
| 85.207.157.29 | 147.237.0.16 | Czech Republic | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 62.219.165.61 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.57.165.107 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.188.163.114 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 31.154.87.2 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.199.130.50 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 86.108.12.82 | 147.237.77.216 | Jordan | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 201.150.38.110 | 147.237.76.39 | Mexico | mobile.meitav.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 85.207.157.29 | 147.237.0.34 | Czech Republic | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 197.232.36.95 | 147.237.76.39 | Kenya | mobile.meitav.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 197.157.222.140 | 147.237.76.30 | South Africa | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 82.80.192.100 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.114.91.234 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.181.237.82 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 133.242.3.168 | 147.237.0.35 | Japan | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.176.26.223 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.136.133 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.212.179.106 | 147.237.77.234 | Canada | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 213.151.37.93 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 95.240.180.109 | 147.237.72.166 | Italy | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.19.85.238 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.57.138.132 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.236.194.161 | 147.237.77.235 | Czech Republic | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 202.155.58.28 | 147.237.76.31 | Indonesia | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 85.250.152.111 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 201.150.38.110 | 147.237.76.39 | Mexico | mobile.meitav.idf.il | ET SCAN NMAP -f -sS | 1 |
| 197.232.36.95 | 147.237.76.39 | Kenya | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 82.166.72.176 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.116.212.169 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.183.55.85 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 189.40.100.216 | 147.237.77.216 | Brazil | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.177.162.90 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 132.64.26.108 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 77.125.79.15 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 101.178.206.92 | 147.237.72.217 | Australia | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

08-23-2016-14:04:00 to 08-23-2016-15:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 85.130.223.95 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 76 |
| 40.77.169.97 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 66 |
| 40.77.169.96 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 38 |
| 40.77.169.98 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 26 |
| 40.77.169.99 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 23 |
| 40.77.169.103 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 15 |
| 91.231.192.149 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 10 |
| 62.0.210.1 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 10 |
| 40.77.169.98 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 9 |
| 94.153.147.142 | Ukraine | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 37.231.81.242 | Kuwait | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 6 |
| 40.77.169.100 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 6 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 5 |
| 40.77.169.102 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 5 |
| 209.133.111.211 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 192.117.188.130 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 40.77.169.97 | United States | 147.237.76.86 | navy.idf.il | drop | SAM rule | drop | 3 |
| 84.95.133.224 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 118.173.253.7 | Thailand | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 157.55.39.38 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 183.89.29.10 | Thailand | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 79.181.33.249 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 109.253.222.111 | Israel | 147.237.76.31 | nakchal.idf.il | drop | First packet isn't SYN | drop | 2 |
| 184.105.139.119 | United States | 147.237.0.200 | m4u.idf.il | drop |  | drop | 1 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 196.147.60.252 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.23.94 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 79.178.102.163 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 201.238.209.182 | Chile | 147.237.0.200 | m4u.idf.il | drop |  | drop | 1 |
| 202.155.58.28 | Indonesia | 147.237.76.148 | gqcenter.aka.idf.il | drop |  | drop | 1 |
| 46.32.126.32 | Jordan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

08-23-2016-14:04:00 to 08-23-2016-15:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.53.4.233 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 244 |
| 80.246.137.179 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 173 |
| 2.53.26.96 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 141 |
| 2.53.41.223 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 107 |
| 2.53.170.214 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 102 |
| 37.26.147.172 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 37 |
| 176.13.23.67 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 34 |
| 37.26.146.204 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 77.125.71.0 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 89.138.181.7 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 109.253.230.7 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 2.53.30.199 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 2.53.53.186 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.176.20.254 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.53.134.47 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.136.160 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.53.164.120 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.141 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 10.148.20.36 | | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim | Block | 2 |
| 66.249.79.37 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.79.37 | Block | 2 |
| 77.138.53.69 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.138.53.69 | Block | 2 |
| 77.125.24.194 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 194.90.99.193 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 194.90.99.193 | Block | 2 |
| 79.182.116.132 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/stylteversion=1.01 | Block | 2 |
| 213.57.201.161 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.102.9.95 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx | Block | 1 |
| 40.77.169.104 | United States | 147.237.77.216 | dover.idf.il | Illegal Byte Code Character in URL /1133-16898-he/dover.aspx idf spokesperson#011404 | Block | 1 |
| 80.246.133.162 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 77.126.26.126 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/labels.rdf | Block | 1 |
| 194.90.200.70 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/images/1.he/error.png | Block | 1 |
| 46.19.86.64 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Malformed URL | Block | 1 |
| 91.199.69.254 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/960.css | Block | 1 |
| 217.132.131.220 | Israel | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 41.141.167.138 | Morocco | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico | Block | 1 |
| 192.118.92.3 | Israel | 147.237.72.166 | aka.idf.il | Cookie Tampering on cookie wb48617274: Expected 72BF9966, Observed 6F503D84 | None | 1 |
| 212.179.27.26 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 46.19.86.64 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Unknown HTTP Request Method j4vlqo in URL | Block | 1 |
| 109.66.149.186 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc | Block | 1 |
| 79.181.235.211 | Israel | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 217.132.131.220 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/wp-login.php | Block | 1 |
| 46.19.85.59 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 192.243.55.133 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/information.aspx?docid=76754 | Block | 1 |
| 2.53.154.208 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 77.138.53.69 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunasmachta.aspx | Block | 1 |
| 213.57.42.201 | Israel | 147.237.72.156 | aman.idf.il | Suspicious Response Code | Block | 1 |
| 46.120.181.40 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc | Block | 1 |
| 79.181.235.211 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/wp-login.php | Block | 1 |
| 77.125.24.194 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152 | Block | 1 |
| 46.19.85.136 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 82.166.130.217 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |

08-23-2016-14:04:00 to 08-23-2016-15:04:00