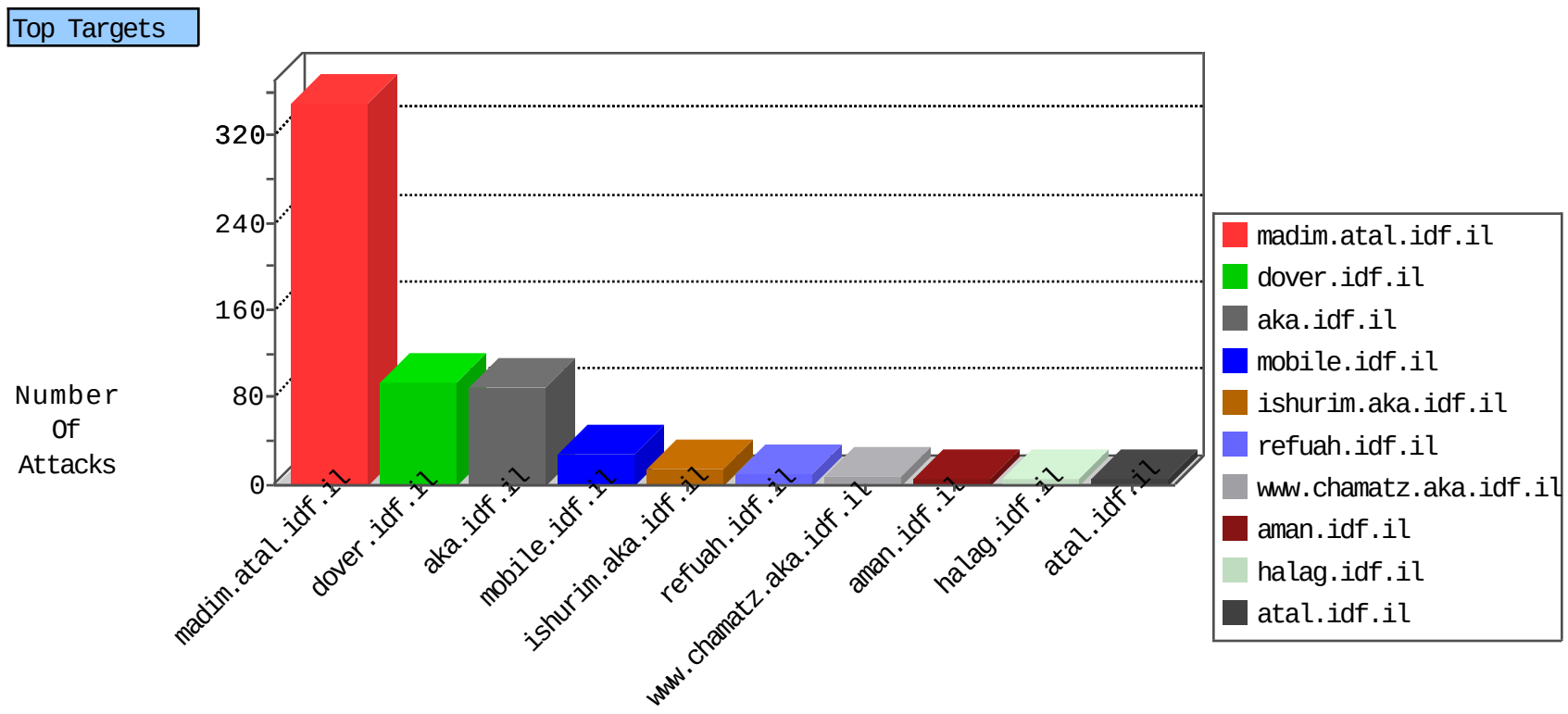
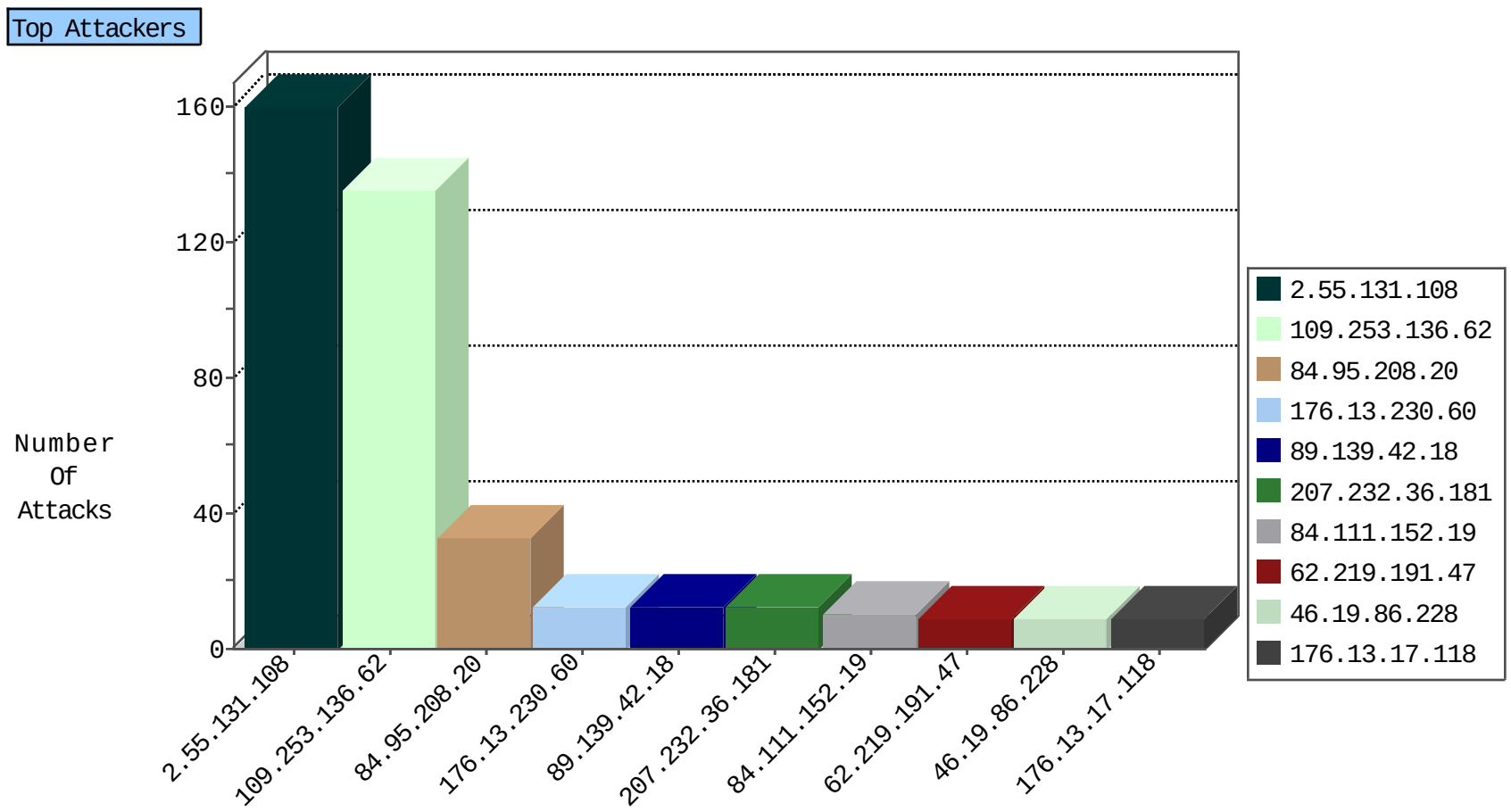
08-31-2016-09:04:04 to 08-31-2016-10:04:04

# IDF Under Attack Daily Report

Top Targets




Top Attackers



08-31-2016-09:04:04 to 08-31-2016-10:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 207.232.36.181 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 172 |
| 163.172.227.198 | United Kingdom | 147.237.76.147 | chinuch.aka.idf.il | Black List | drop | 1 |
| 80.82.70.230 | Netherlands | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |
| 163.172.216.36 | United Kingdom | 147.237.76.30 | himush.idf.il | Black List | drop | 1 |

08-31-2016-09:04:04 to 08-31-2016-10:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 162.210.196.100 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 4 |
| 199.58.86.206 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 4 |
| 199.58.86.211 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 83.149.126.98 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |

08-31-2016-09:04:04 to 08-31-2016-10:04:04

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 52.16.5.197 | 147.237.77.216 | Ireland | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.179.90.106 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.26.147.145 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.150.249.162 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.12.54.183 | 147.237.72.166 | Romania | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.217.127 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.53.44.91 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 95.35.33.46 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.102.60.173 | 147.237.0.19 | Netherlands | madim.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 85.65.245.94 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.178.84.185 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.176.107.251 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.199.106.194 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.19.86.139 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.179.21.194 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.8.103.142 | 147.237.77.176 | Palestinian Territory, Occupied | matpash.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 188.121.163.78 | 147.237.77.216 | Slovakia | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.55.151.214 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 106.5.93.10 | 147.237.72.166 | China | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.102.60.173 | 147.237.76.86 | Netherlands | navy.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 93.172.129.251 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.166.21.43 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.181.23.206 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.57.217.86 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

08-31-2016-09:04:04 to 08-31-2016-10:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 89.139.42.18 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.86.228 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 9 |
| 62.219.191.47 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 9 |
| 176.13.17.118 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 9 |
| 198.240.213.22 | Switzerland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 92.247.181.29 | Bulgaria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 77.75.76.161 | Czech Republic | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 192.169.7.223 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 4 |
| 123.63.190.165 | India | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 81.218.80.110 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 176.13.2.127 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 100.92.247.251 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 217.132.143.129 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 2.53.29.28 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 195.160.242.40 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 176.13.11.13 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 2.55.36.247 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 41.33.231.86 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 100.92.228.14 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 66.249.93.107 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 176.13.20.27 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.209.223 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 46.19.86.81 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 1 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 84.110.53.161 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.4.17 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.131.128 | Israel | 147.237.0.19 | madim.atal.idf.il | drop | First packet isn't SYN | drop | 1 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 137.116.71.170 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 62.0.204.92 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.134.63 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 79.178.233.71 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 1 |
| 141.212.122.85 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 109.253.141.171 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 81.218.80.110 | Israel | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 141.212.122.86 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |

08-31-2016-09:04:04 to 08-31-2016-10:04:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.55.131.108 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 160 |
| 109.253.136.62 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 135 |
| 176.13.230.60 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 84.111.152.19 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 10 |
| 37.26.148.128 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 109.253.192.116 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 66.249.64.22 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.22 | Block | 5 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 5 |
| 31.168.85.251 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/ | Block | 5 |
| 80.246.136.177 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 84.95.208.20 | Israel | 147.237.77.234 | halag.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 4 |
| 176.13.3.32 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 4 |
| 5.29.1.29 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 2.53.146.145 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword | Block | 4 |
| 77.138.109.205 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar | Block | 4 |
| 207.46.13.109 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 84.95.208.20 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 3 |
| 109.253.143.177 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 192.116.232.69 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 192.116.232.69 | Block | 3 |
| 46.19.86.192 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.194.92 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 84.95.208.20 | Israel | 147.237.0.15 | kosher-kravi.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 3 |
| 85.250.220.93 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.147.130 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.53.150.217 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 2.53.150.217 | Block | 3 |
| 84.95.208.20 | Israel | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 2 |
| 5.102.242.5 | Israel | 147.237.72.156 | aman.idf.il | Suspicious Response Code | Block | 2 |
| 80.246.133.36 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 84.95.208.20 | Israel | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 37.26.148.163 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | PHP Attempt | Block | 2 |
| 213.57.73.192 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.53.137.111 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 77.139.65.94 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/main/sachar | Block | 2 |
| 109.253.131.128 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.234.240 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 84.95.208.20 | Israel | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 84.95.208.20 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 176.13.242.127 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 77.138.134.140 | France | 147.237.72.167 | ishurim.aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 93.172.234.61 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/aman | Block | 1 |
| 46.19.85.64 | Israel | 147.237.77.243 | mobile.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 138.134.102.16 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 87.71.12.38 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 176.114.250.9 | Czech Republic | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx | Block | 1 |
| 2.53.150.217 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/apple-touch-icon.png | Block | 1 |
| 109.253.208.66 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 77.138.247.23 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/ | Block | 1 |
| 98.162.183.242 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.234 | halag.idf.il | PHP Attempt | Block | 1 |

08-31-2016-09:04:04 to 08-31-2016-10:04:04