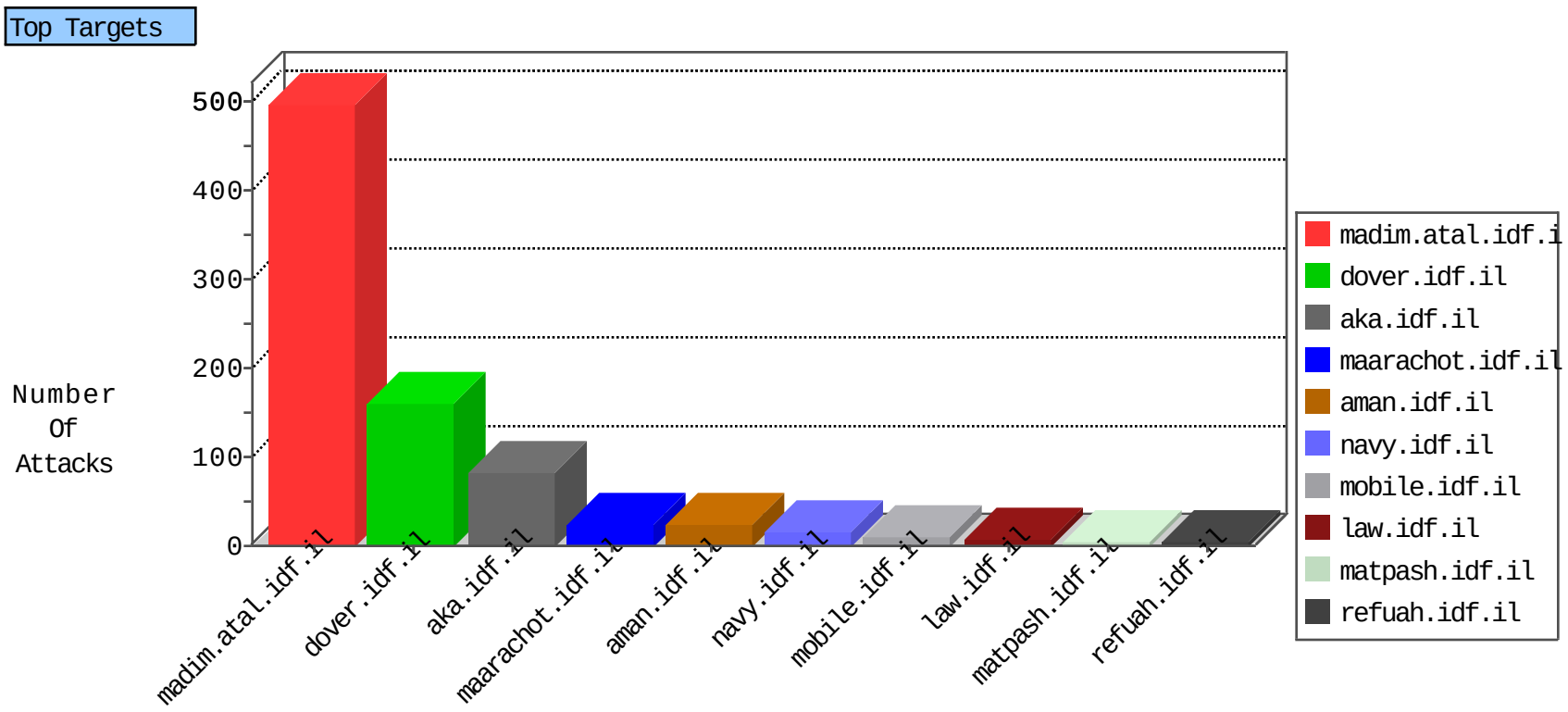
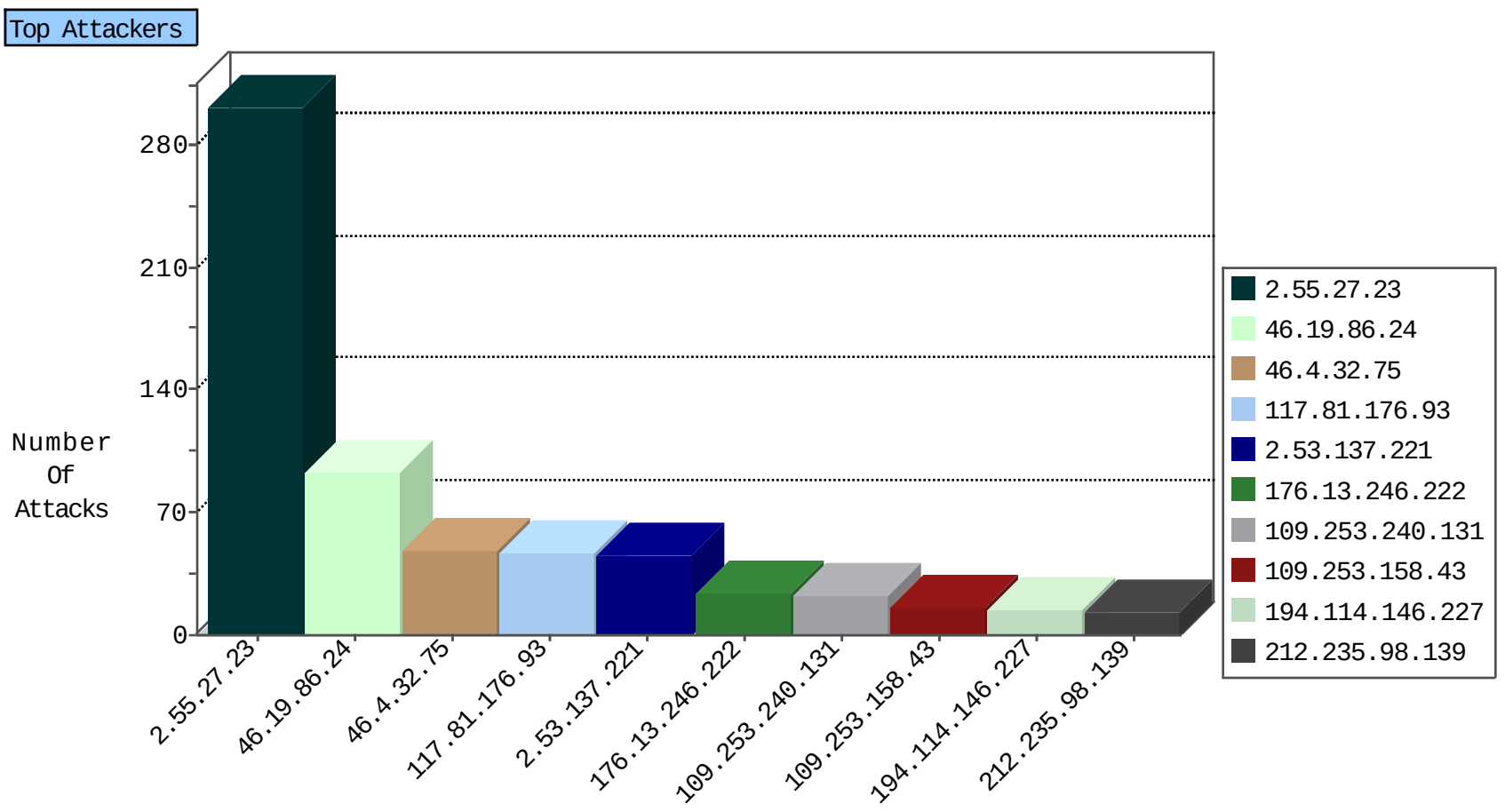
08-21-2016-15:04:02 to 08-21-2016-16:04:02

# IDF Under Attack Daily Report

Top Targets




Top Attackers



08-21-2016-15:04:02 to 08-21-2016-16:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.53.4.9 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 8 |
| 46.19.86.51 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 4 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 107.150.53.170 | United States | 147.237.76.148 | gqcenter.aka.idf.il | Black List | drop | 1 |
| 120.132.50.135 | China | 147.237.77.235 | sviva.idf.il | block-sp-traf1 | forward | 1 |
| 46.19.86.65 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 66.249.76.106 | Israel | 147.237.72.166 | aka.idf.il | HTTP-Misc-BadBlue-Dir-Trave-2 | dest-reset | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.30 | himush.idf.il | Black List | drop | 1 |
| 79.178.192.65 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 1 |
| 192.116.166.94 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 1 |

08-21-2016-15:04:02 to 08-21-2016-16:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.4.32.75 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 14 |
| 46.4.32.75 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 13 |
| 46.4.32.75 | Germany | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Permit | 7 |
| 46.4.32.75 | Germany | 147.237.76.86 | navy.idf.il | C1000074: HTTP: majestic bot | Permit | 4 |
| 46.4.32.75 | Germany | 147.237.77.176 | matpash.idf.il | C1000074: HTTP: majestic bot | Permit | 3 |
| 46.4.32.75 | Germany | 147.237.76.42 | refuah.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 69.30.198.186 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 46.4.32.75 | Germany | 147.237.76.200 | eitan.aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 162.210.196.129 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |

08-21-2016-15:04:02 to 08-21-2016-16:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 162.213.1.246 | 147.237.77.216 | United States | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 94.102.48.195 | 147.237.0.35 | Netherlands | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 5.102.242.75 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.111.57.42 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 193.201.225.149 | 147.237.0.200 | Ukraine | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 82.81.223.5 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.179.13.140 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 123.206.85.139 | 147.237.76.202 | China | e.halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.180.24.19 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 123.206.85.139 | 147.237.76.176 | China | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.176.10.129 | 147.237.77.216 | Israel | dover.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 123.206.85.139 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 77.126.35.131 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.226.17.72 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.228.207.18 | 147.237.76.148 | Germany | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 95.215.60.214 | 147.237.0.200 | Spain | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 41.104.6.249 | 147.237.77.216 | Algeria | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 89.139.140.232 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.29.114.113 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.57.87.62 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 82.166.85.204 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 193.201.225.138 | 147.237.72.156 | Ukraine | aman.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 82.81.161.50 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 141.226.162.32 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.180.243.207 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 123.206.85.139 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.178.52.45 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 123.206.85.139 | 147.237.76.86 | China | navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 77.138.88.199 | 147.237.72.166 | France | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 120.237.232.6 | 147.237.76.202 | China | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 66.249.76.106 | 147.237.72.166 | United States | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 95.215.60.214 | 147.237.72.166 | Spain | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.121.112.175 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

08-21-2016-15:04:02 to 08-21-2016-16:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 109.253.158.43 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 16 |
| 2.53.20.160 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 199.203.179.99 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.86 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 8 |
| 93.173.248.93 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 212.235.98.139 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 6 |
| 31.210.186.16 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 62.0.67.44 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 4 |
| 85.130.175.66 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.58 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 2.53.4.9 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.86.65 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 77.138.12.89 | France | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 2 |
| 109.186.91.117 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 169.229.3.91 | United States | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 1 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 46.117.199.96 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 176.13.14.241 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.137.89 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 216.218.206.120 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop |  | drop | 1 |
| 169.229.3.91 | United States | 147.237.76.86 | navy.idf.il | drop | SAM rule | drop | 1 |
| 80.246.130.161 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 66.249.69.105 | Israel | 147.237.0.33 | idf.il | drop |  | drop | 1 |
| 216.243.31.2 | United States | 147.237.0.33 | idf.il | drop |  | drop | 1 |
| 169.229.3.91 | United States | 147.237.76.147 | chinuch.aka.idf.il | drop | SAM rule | drop | 1 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.203.139 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 66.249.81.218 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 216.243.31.2 | United States | 147.237.0.35 | akaws.idf.il | drop |  | drop | 1 |
| 169.229.3.91 | United States | 147.237.76.177 | ncore.idf.il | drop | SAM rule | drop | 1 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.il | drop | SAM rule | drop | 1 |
| 169.229.3.91 | United States | 147.237.77.243 | mobile.idf.il | drop | SAM rule | drop | 1 |

08-21-2016-15:04:02 to 08-21-2016-16:04:02

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.55.27.23 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 293 |
| 46.19.86.24 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 93 |
| 2.53.137.221 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 46 |
| 176.13.246.222 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 24 |
| 117.81.176.93 | China | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 117.81.176.93 | Block | 19 |
| 109.253.240.131 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 19 |
| 117.81.176.93 | China | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 117.81.176.93 | Block | 15 |
| 194.114.146.227 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/ | Block | 8 |
| 2.55.27.23 | Israel | 147.237.0.19 | madim.atal.idf.i | Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx | Block | 7 |
| 117.81.176.93 | China | 147.237.77.170 | maarachot.idf.il | PHP Attempt | Block | 6 |
| 117.81.176.93 | China | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 6 |
| 194.114.146.227 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/ | Block | 5 |
| 220.249.249.11 | China | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 220.249.249.11 | Block | 5 |
| 176.13.3.43 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 2.53.167.4 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 4 |
| 66.249.76.112 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.76.112 | Block | 3 |
| 109.253.222.120 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 37.46.41.196 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 37.46.41.196 | Block | 3 |
| 212.29.203.226 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx | Block | 3 |
| 109.66.149.244 | Israel | 147.237.76.42 | refuah.idf.il | Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx | Block | 2 |
| 109.253.240.131 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 82.102.136.65 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 109.64.12.14 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/gius | Block | 2 |
| 66.249.76.35 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.76.35 | Block | 2 |
| 2.55.27.23 | Israel | 147.237.0.19 | madim.atal.idf.i | Untraceable SSL Sessions: Open Mode | None | 2 |
| 176.13.228.158 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 80.246.136.254 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 77.138.220.60 | France | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 77.138.220.60 | Block | 2 |
| 66.102.6.191 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 2.55.138.42 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 78.46.42.235 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp | Block | 1 |
| 220.249.249.11 | China | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 176.13.237.26 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 46.4.32.75 | Germany | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 46.4.32.75 | Block | 1 |
| 77.138.220.60 | France | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/4/110654.pdf | Block | 1 |
| 66.220.146.29 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to 147.237.0.34/sip_storage/files/8/size220x0/1738.jpg | Block | 1 |
| 109.67.240.192 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 31.168.65.25 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 79.180.112.73 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/ | Block | 1 |
| 176.13.239.66 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 66.249.82.218 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 46.4.32.75 | Germany | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/navy/ | Block | 1 |
| 89.149.88.121 | Moldova, Republic of | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx | Block | 1 |
| 77.138.237.81 | France | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 207.46.13.165 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/robots.txt | Block | 1 |
| 66.249.65.177 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.177 | Block | 1 |
| 157.55.39.40 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/main/giyus/giyus/general.aspx | Block | 1 |
| 79.181.186.42 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 1 |
| 220.249.249.11 | China | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1503-en/contact.php | Block | 1 |
| 66.249.82.224 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |

08-21-2016-15:04:02 to 08-21-2016-16:04:02