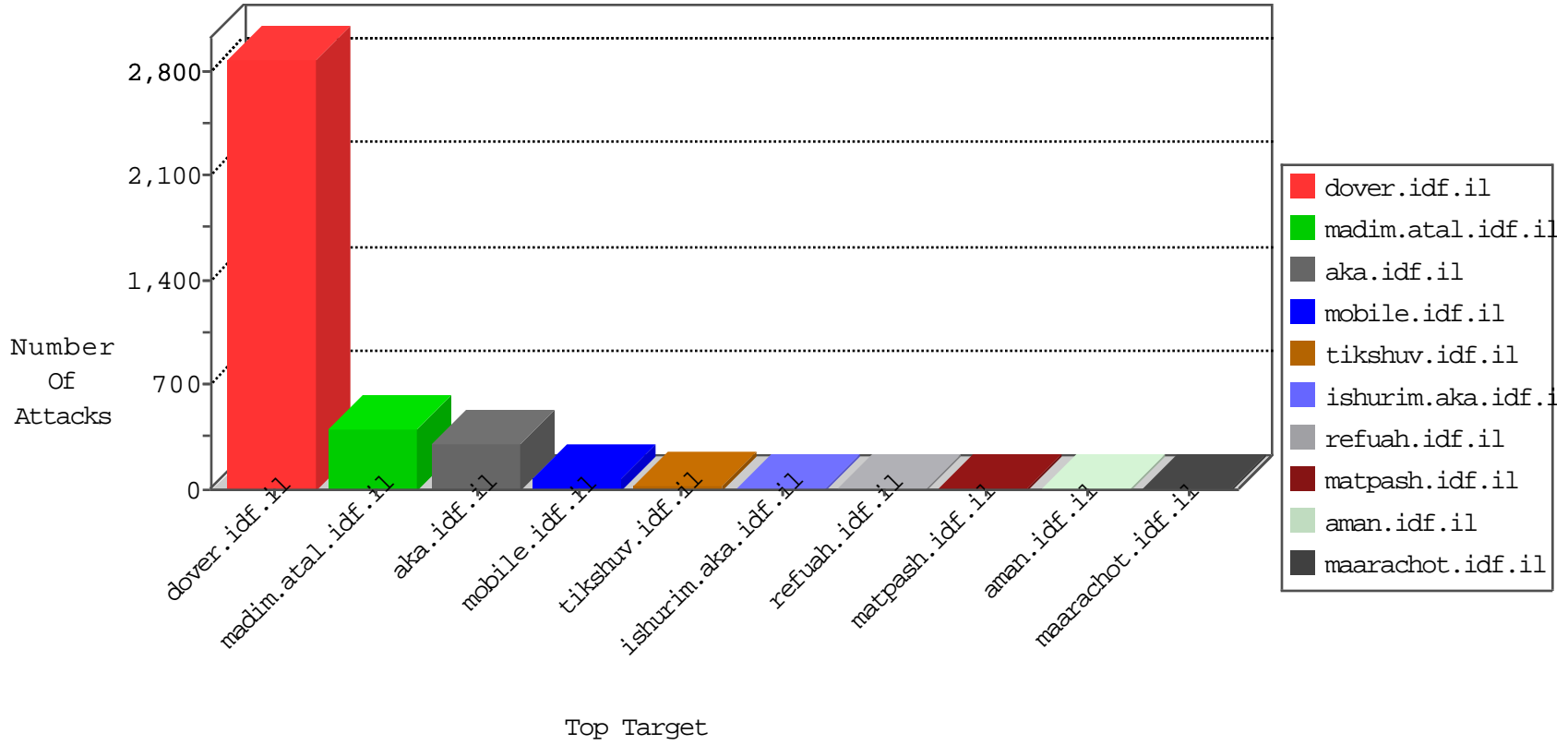


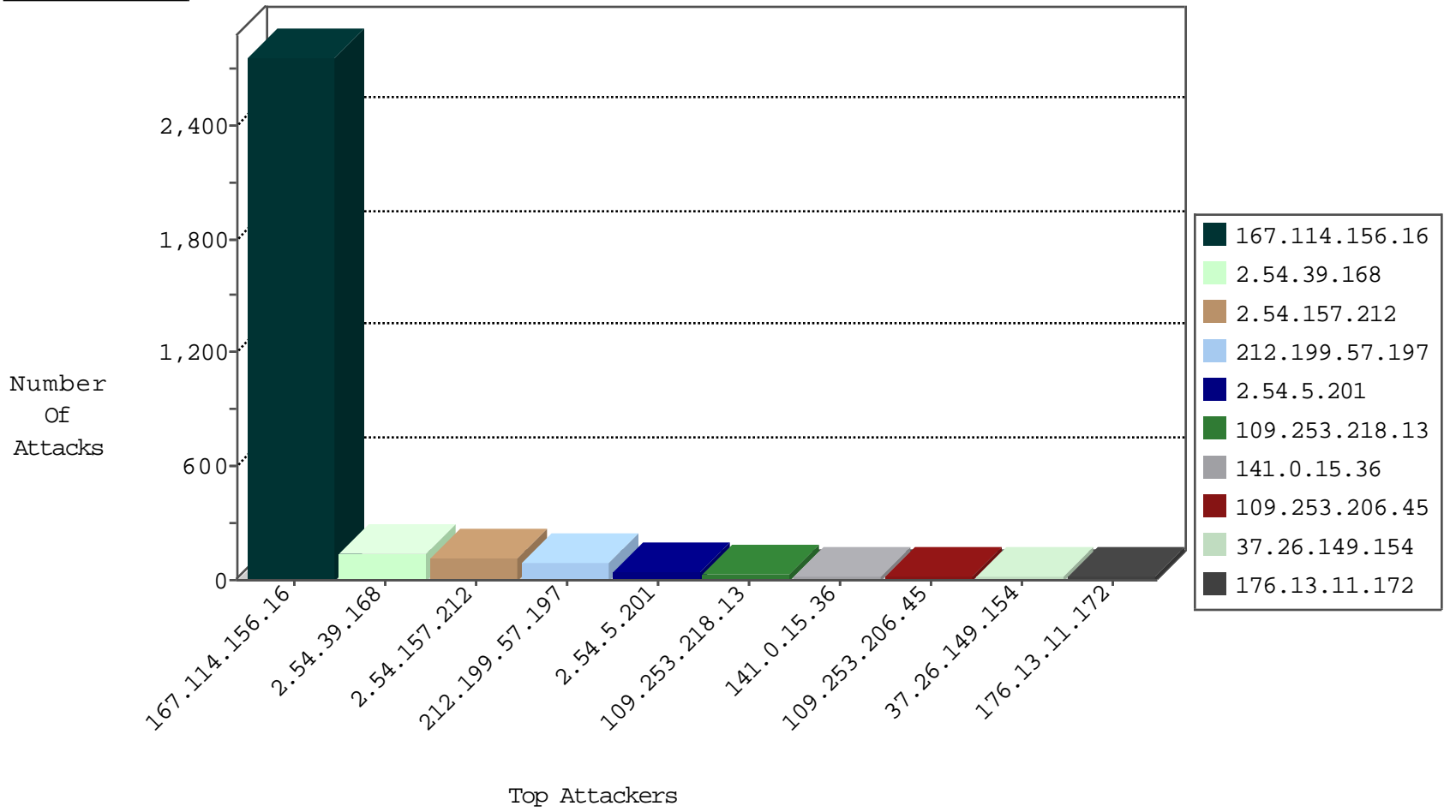
IDF Under Attack Daily Report



Top Targets



Top Attackers



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 | DOS-Tool-SwitchbladG | dest-reset | 3376 |
| 81.218.65.210 | Israel | 147.237.0.34 | tikshuv.idf.il | Block_Udp_All_Nets | drop | 3 |
| 81.218.65.210 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 66.249.64.190 | Israel | 147.237.72.166 | aka.idf.il | HTTP-Misc-BadBlue-Dir-Trave-2 | dest-reset | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|----------------|---|---------------|-------|
| 123.126.113.154 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 4 |
| 80.246.133.233 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 176.13.17.164 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 3 |
| 93.173.157.198 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 3 |
| 108.59.8.80 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|------------------|----------------|------------------|--------------------------|--|-------|
| 197.163.25.104 | 147.237.77.216 | Egypt | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.187.104.202 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 176.13.10.197 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.176.61.157 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.56.170 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 188.120.148.150 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.67.163.189 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.176.11.229 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------|----------------|--------------------|--|---|---------------|-------|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 74 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 39 |
| 141.0.15.36 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 109.253.206.45 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 176.13.11.172 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 109.253.218.13 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | | reject | 19 |
| 176.13.20.78 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 176.13.10.192 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 147.236.33.7 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 79.176.43.224 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 81.218.66.107 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 109.253.158.21 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 37.26.149.154 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.86.186 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 37.26.147.176 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 80.246.136.171 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 77.127.87.149 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.149.154 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 62.219.230.79 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.167.208 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 87.71.25.120 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.149.221 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 5.22.135.137 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 178.63.105.85 | Germany | 147.237.8.45 | e.eitan.idf.il | drop | SAM rule | drop | 5 |
| 178.63.105.85 | Germany | 147.237.8.46 | e.chinuch.idf.il | drop | SAM rule | drop | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 87.69.36.210 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 37.26.149.154 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 31.210.186.157 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 37.26.149.154 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 4 |
| 46.19.85.126 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 188.120.154.95 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 217.194.203.52 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 84.109.24.41 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 31.168.87.253 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.65.213.164 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.179.3.227 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.32.179.92 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 37.26.149.221 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 37.26.146.208 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.13.8.200 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.219 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 80.179.9.2 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.4.63 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.71.31.75 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.13.20.225 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.32.179.92 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 132.64.26.198 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

03-14-2016-12:04:00 to 03-14-2016-13:04:00

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------|----------------|------------|--|--|---------------|-------|
| 109.64.213.126 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|------------------|---|---------------|-------|
| 2.54.39.168 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 139 |
| 2.54.157.212 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 120 |
| 212.199.57.197 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 86 |
| 2.54.5.201 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 39 |
| 109.253.218.13 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 46.19.85.239 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 4 |
| 31.168.11.194 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 4 |
| 46.19.86.152 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 37.26.148.252 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 85.116.228.4 | Italy | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg | Block | 3 |
| 207.46.13.105 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 63.121.77.30 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en | Block | 2 |
| 46.19.85.162 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 62.219.44.190 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/miluim | Block | 1 |
| 207.46.13.105 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 207.46.13.105 | Block | 1 |
| 157.55.39.112 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 37.26.148.201 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 81.199.120.27 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 217.194.207.24 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.65.115 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/2808.jpg | Block | 1 |
| 192.115.215.60 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 1 |
| 37.26.146.154 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.253.134.232 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1412-he/atal.aspx | Block | 1 |
| 67.212.188.11 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 207.46.13.160 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 207.46.13.160 | Block | 1 |
| 176.13.0.105 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/894-ar | Block | 1 |
| 37.26.148.220 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 82.36.3.46 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.65.179 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/894-he | Block | 1 |
| 199.30.25.81 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 37.26.146.208 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.253.211.69 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in Header Name If-Mo Mozillaf.il | Block | 1 |
| 68.180.230.189 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx | Block | 1 |
| 66.249.64.13 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 212.183.128.164 | United Kingdom | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 176.13.10.192 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif | None | 1 |
| 5.156.118.205 | Romania | 147.237.77.176 | matpash.idf.il | PHP Attempt | Block | 1 |
| 66.249.75.8 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1238-he/refuah.aspx | Block | 1 |
| 46.19.86.206 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 207.46.13.65 | United States | 147.237.0.34 | tikshuv.idf.il | Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx | Block | 1 |
| 37.26.147.176 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 109.253.211.69 | Israel | 147.237.72.166 | aka.idf.il | Malformed HTTP Header Line 17 | Block | 1 |
| 77.75.77.11 | Czech Republic | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/page/28/ | Block | 1 |
| 2.52.191.217 | Israel | 147.237.76.42 | refuah.idf.il | Suspicious Response Code | Block | 1 |
| 66.249.64.37 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 185.49.14.190 | Poland | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php | Block | 1 |
| 5.156.118.205 | Romania | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php | Block | 1 |
| 87.69.62.227 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/ | Block | 1 |
| 66.249.75.16 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/3471.jpg | Block | 1 |
| 62.219.44.190 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 62.219.44.190 | Block | 1 |