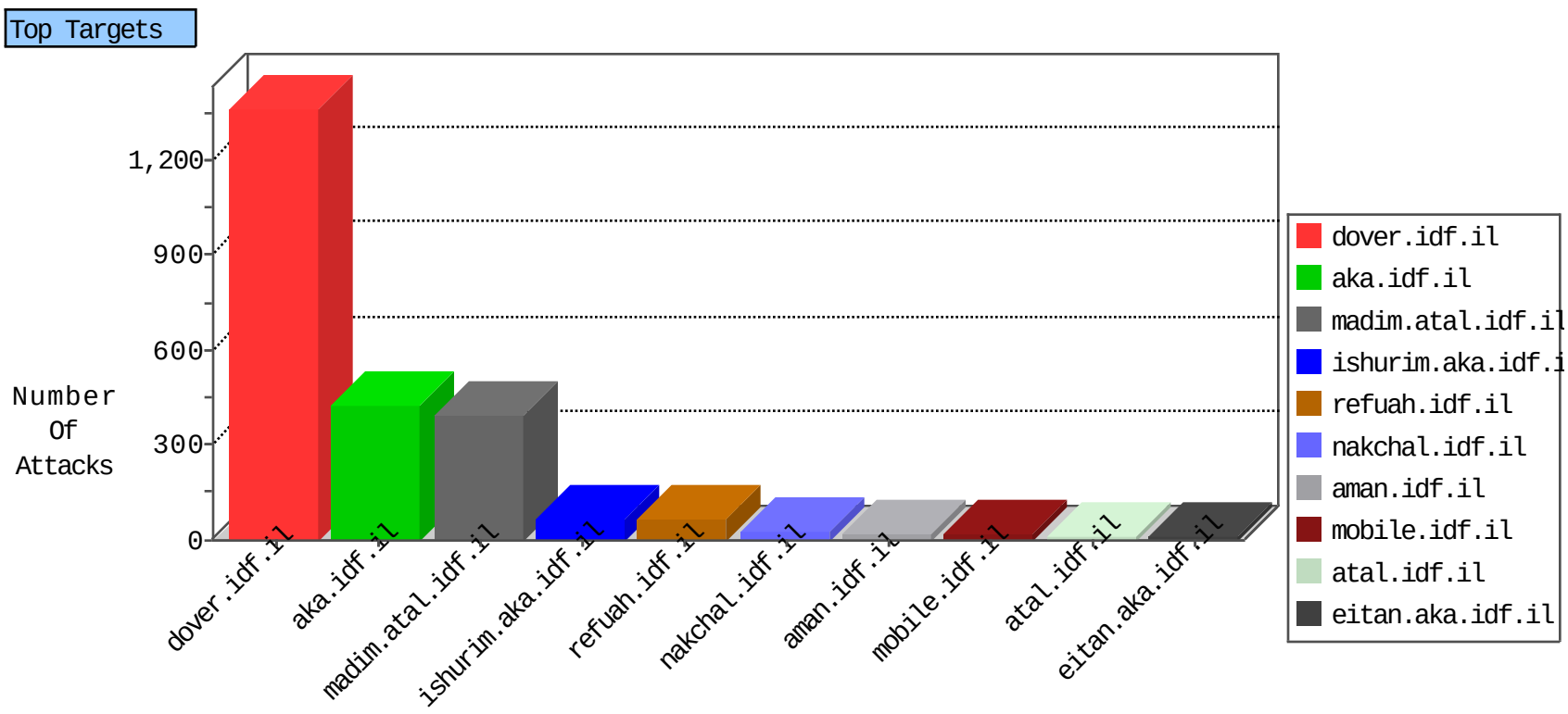
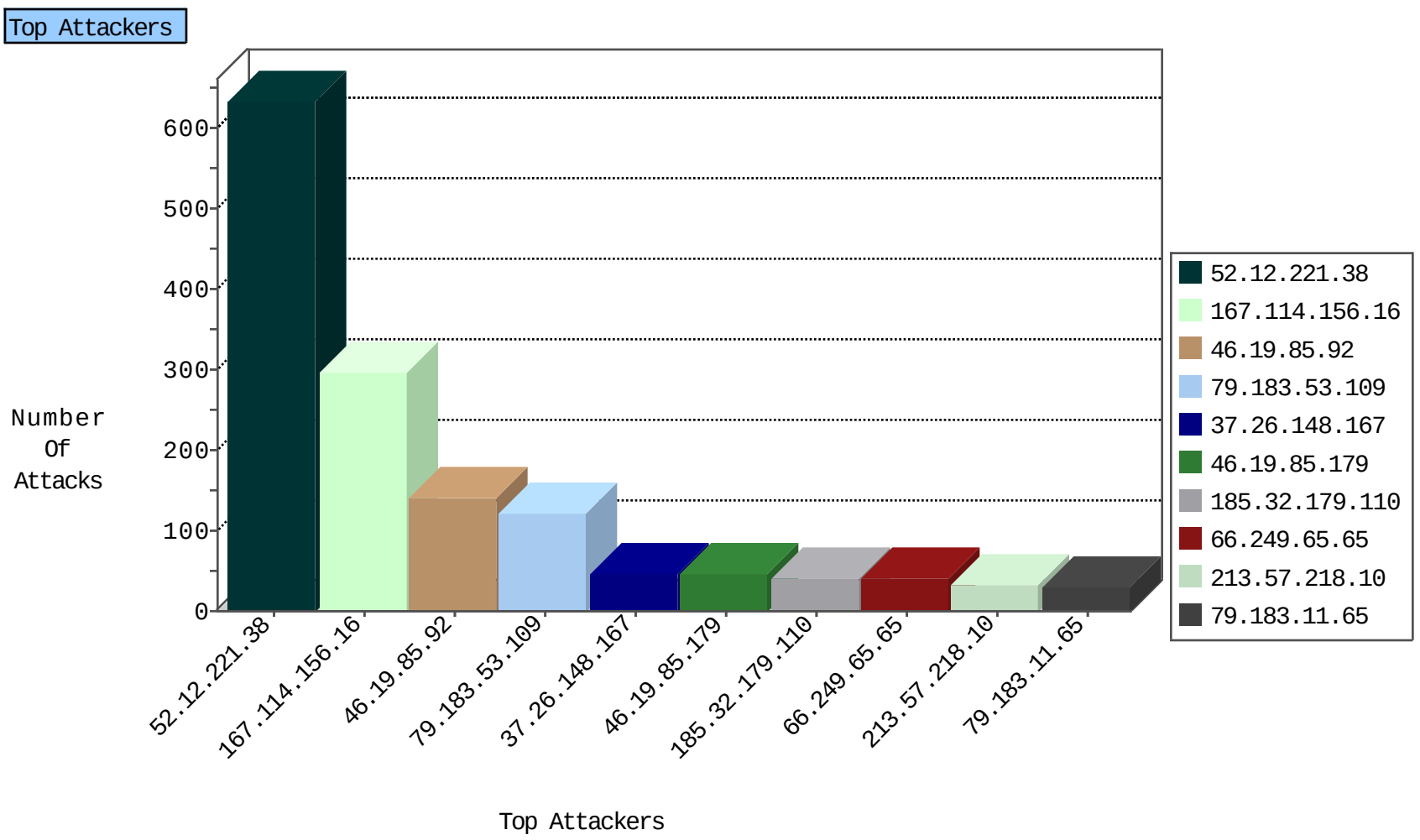
05-03-2016-16:04:01 to 05-03-2016-17:04:01

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



05-03-2016-16:04:01 to 05-03-2016-17:04:01

## 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 | HTTP-POST-Segmented-DoS | dest-reset | 10037 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 3377 |
| 81.218.65.210 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 115.29.167.133 | China | 147.237.76.176 | test.ncore.idf.il | JLM_Under_Attack_Con_Tcp | drop | 2 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 2 |
| 192.96.201.142 | United States | 147.237.76.201 | e.atal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 192.96.201.142 | United States | 147.237.76.202 | e.halag.idf.il | Block_Udp_All_Nets | drop | 1 |
| 82.221.105.6 | Iceland | 147.237.76.200 | eitan.aka.idf.il | Block_Ntp_All_Net | drop | 1 |
| 5.189.167.216 | Germany | 147.237.76.202 | e.halag.idf.il | Block_Udp_All_Nets | drop | 1 |
| 94.102.52.10 | Netherlands | 147.237.76.201 | e.atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 192.96.201.142 | United States | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 45.32.79.225 | Netherlands | 147.237.76.31 | nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |

05-03-2016-16:04:01 to 05-03-2016-17:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

05-03-2016-16:04:01 to 05-03-2016-17:04:01

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 77.127.85.137 | 147.237.76.86 | Israel | navy.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 82.80.125.206 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 217.132.47.54 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 208.100.26.228 | 147.237.8.14 | United States | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.85.10 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 198.20.69.74 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 193.43.246.250 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.88.34.207 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.135.50 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 104.219.238.10 | 147.237.76.177 | United States | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 84.228.92.71 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.179.18.40 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.129.15.245 | 147.237.77.205 | France | prisha.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.120.145.178 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 200.41.233.234 | 147.237.77.216 | Argentina | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 167.114.156.16 | 147.237.77.216 | Canada | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.78.168.55 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 104.219.238.10 | 147.237.77.234 | United States | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.139.236.141 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

05-03-2016-16:04:01 to 05-03-2016-17:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 52.12.221.38 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 633 |
| 37.26.148.167 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 47 |
| 66.249.65.65 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 39 |
| 79.183.11.65 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 80.246.130.146 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 25 |
| 203.133.168.86 | Korea, Republic of | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 46.19.86.29 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 19 |
| 82.166.57.32 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 15 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 213.57.253.213 | Israel | 147.237.76.31 | nakchal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 14 |
| 109.253.137.217 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 13 |
| 109.253.137.217 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 52.29.223.39 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 62.210.148.246 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 197.45.132.217 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 176.248.187.134 | United Kingdom | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 198.58.102.156 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 62.219.167.150 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 93.172.149.157 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 62.219.167.150 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 79.183.186.72 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 213.57.218.10 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.67.129.18 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 80.178.95.33 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.157 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 78.164.126.12 | Turkey | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 199.30.25.114 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 80.246.137.58 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.46.39.59 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 66.249.93.182 | Europe | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 149.78.230.201 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 213.57.218.10 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 46.19.85.251 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.96 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 213.57.218.10 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 6 |
| 84.108.125.84 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 66.249.79.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 213.57.218.10 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 213.57.218.10 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 213.57.218.10 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 212.199.224.24 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 4 |
| 132.70.66.10 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 64.135.44.66 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 197.164.102.165 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 80.178.157.105 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.156 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.92 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 140 |
| 79.183.53.109 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 121 |
| 46.19.85.179 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 46.19.85.158 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 28 |
| 199.30.24.171 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 24 |
| 80.246.136.142 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 20 |
| 109.64.108.233 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 109.64.108.233 | Block | 17 |
| 176.13.16.82 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 88.238.114.197 | Turkey | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 8 |
| 88.238.114.197 | Turkey | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/administrator/index.php | Block | 8 |
| 88.238.114.197 | Turkey | 147.237.77.216 | dover.idf.il | Multiple Admin Blocking from 88.238.114.197 | Block | 7 |
| 131.253.25.129 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 6 |
| 37.115.129.170 | Ukraine | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 6 |
| 2.55.159.93 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 37.115.129.170 | Ukraine | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 37.115.129.170 | Block | 5 |
| 64.107.201.150 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 37.26.148.154 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 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 | 3 |
| 109.253.128.236 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.139.111 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.1.188 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.2.33 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.15.6 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 199.30.25.114 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 80.179.9.115 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 176.13.19.153 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 131.253.25.158 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 131.253.25.214 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 187.234.103.129 | Mexico | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 2 |
| 85.64.216.111 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 85.64.216.111 | Block | 2 |
| 66.249.79.89 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 82.81.82.6 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 2 |
| 131.156.136.98 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 5.102.254.236 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/1043-he/displaycertufucates | Block | 2 |
| 80.179.9.7 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 46.19.85.63 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 192.117.175.194 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 88.238.114.197 | Turkey | 147.237.77.216 | dover.idf.il | Admin Blocking | Block | 1 |
| 80.246.137.58 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.182.124.117 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 93.172.149.157 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 207.46.13.22 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/ | Block | 1 |
| 185.3.144.33 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/favicon.ico | Block | 1 |
| 84.111.120.172 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile | Block | 1 |
| 157.55.39.89 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx | Block | 1 |
| 66.249.78.236 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2379.jpg | Block | 1 |
| 197.164.102.165 | Egypt | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/arr/ | Block | 1 |
| 2.53.5.206 | 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 |
| 79.183.25.72 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 101.226.33.217 | China | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |