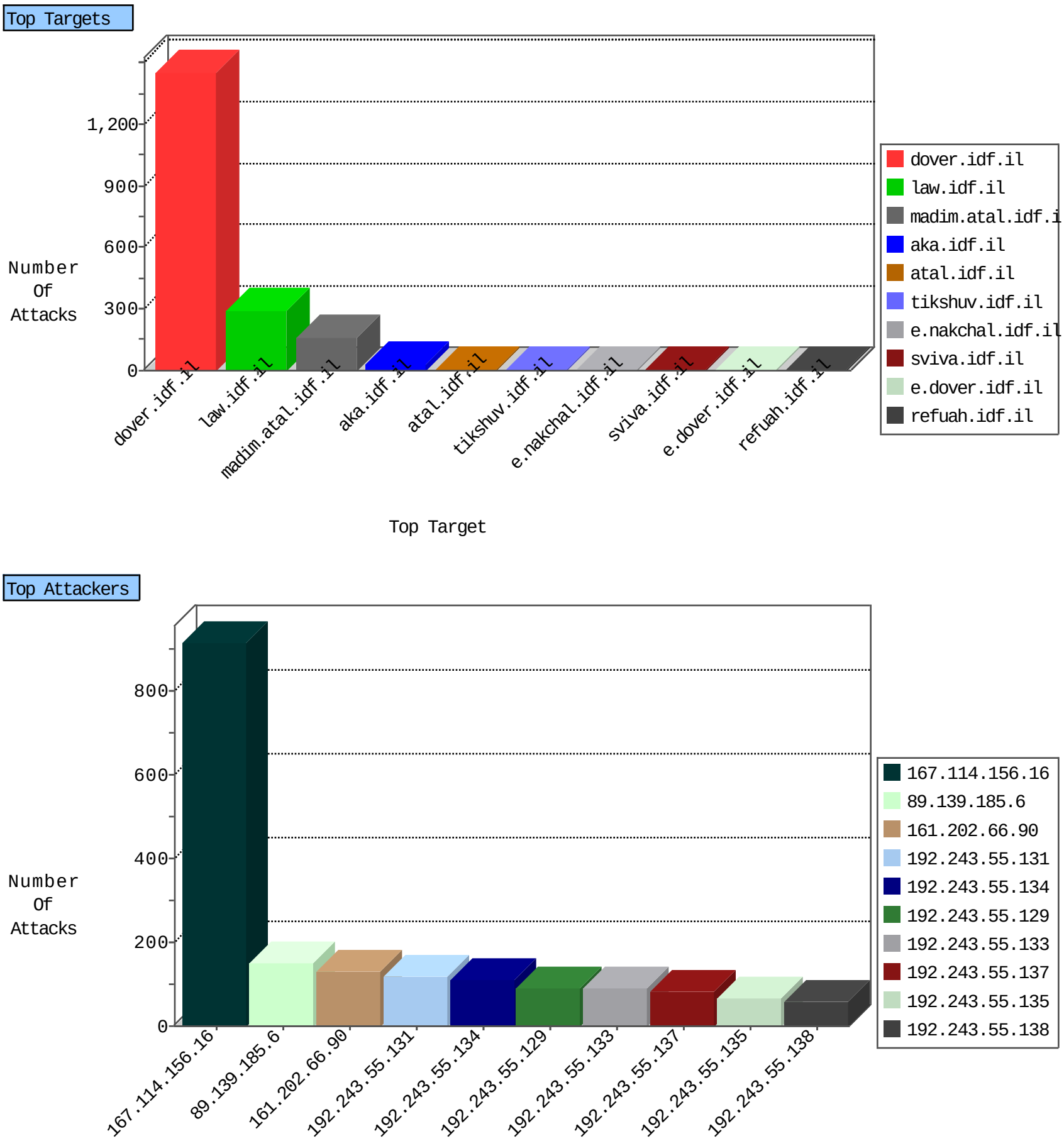
03-12-2016-03:04:07 to 03-12-2016-04:04:07

# IDF Under Attack Daily Report



03-12-2016-03:04:07 to 03-12-2016-04:04:07

## 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 | 3029 |
| 161.202.66.90 | Netherlands | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 450 |
| 82.145.220.162 | Europe | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 33 |
| 81.218.65.210 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 131.100.141.66 | El Salvador | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 5.189.172.102 | Germany | 147.237.76.30 | himush.idf.il | Block_Ntp_All_Net | drop | 1 |
| 184.105.247.198 | United States | 147.237.77.233 | atal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 5.189.172.102 | Germany | 147.237.77.178 | e.matpash.idf.il | Block_Ntp_All_Net | drop | 1 |
| 204.42.253.132 | United States | 147.237.76.34 | yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 5.189.172.102 | Germany | 147.237.77.179 | e.mazi.idf.il | Block_Ntp_All_Net | drop | 1 |
| 216.218.206.67 | United States | 147.237.0.35 | akaws.idf.il | Block_Udp_All_Nets | drop | 1 |
| 94.102.49.206 | Netherlands | 147.237.76.199 | e.nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 5.189.172.102 | Germany | 147.237.8.45 | e.eitan.idf.il | Block_Ntp_All_Net | drop | 1 |
| 182.155.113.90 | Taiwan | 147.237.76.44 | e.refuah.idf.il | Block_Udp_All_Nets | drop | 1 |

03-12-2016-03:04:07 to 03-12-2016-04:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 106.120.173.118 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 4 |
| 109.65.11.200 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 106.120.173.159 | China | 147.237.77.233 | atal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.120.173.102 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

03-12-2016-03:04:07 to 03-12-2016-04:04:07

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 161.202.66.90 | 147.237.77.216 | Netherlands | dover.idf.il | ET SCAN NMAP -sS window 1024 | 3 |
| 66.249.66.125 | 147.237.77.233 | United States | atal.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 104.196.98.22 | 147.237.77.61 | United States | e.cogat.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 104.196.98.22 | 147.237.77.61 | United States | e.cogat.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 50.102.242.22 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 217.147.86.61 | 147.237.77.235 | United Kingdom | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 178.63.11.208 | 147.237.77.235 | Germany | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

03-12-2016-03:04:07 to 03-12-2016-04:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 21 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 21 |
| 192.243.55.129 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 20 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 192.243.55.129 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 192.243.55.134 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 15 |
| 192.243.55.129 | Dominica | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 15 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 14 |
| 192.243.55.134 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 14 |
| 192.243.55.134 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 192.243.55.135 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 192.243.55.131 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 192.243.55.134 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 11 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 11 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 192.243.55.131 | Dominica | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 10 |
| 192.243.55.134 | Dominica | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 10 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 192.243.55.133 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 10 |
| 192.243.55.133 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 10 |
| 192.243.55.129 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 10 |
| 192.243.55.129 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 192.243.55.134 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 9 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 192.243.55.131 | Dominica | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 192.243.55.134 | Dominica | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 9 |
| 192.243.55.133 | Dominica | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 8 |
| 192.243.55.134 | Dominica | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 192.243.55.138 | Dominica | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 7 |
| 192.243.55.133 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 192.243.55.138 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 192.243.55.134 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 192.243.55.135 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 192.243.55.131 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 192.243.55.134 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 192.243.55.129 | Dominica | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |
| 192.243.55.135 | Dominica | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 192.243.55.135 | Dominica | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |
| 192.243.55.138 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 161.202.66.90 | Netherlands | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 192.243.55.131 | Dominica | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 89.139.185.6 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 152 |
| 2.54.140.36 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.65.50.141 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.66.23 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1409-he/atal.aspx | Block | 1 |
| 65.55.210.188 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 192.243.55.129 | Dominica | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/hebrew/0303-1.stm, | Block | 1 |
| 83.59.237.243 | Spain | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx | Block | 1 |
| 66.249.64.200 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/giyus/[[#11]]general.aspx | Block | 1 |
| 40.77.167.33 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 207.241.237.211 | United States | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 128.232.110.28 | United Kingdom | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/ | Block | 1 |
| 66.249.66.26 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx | Block | 1 |
| 66.249.64.51 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3467.jpg | Block | 1 |
| 192.243.55.133 | Dominica | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem | Block | 1 |
| 83.59.237.243 | Spain | 147.237.77.216 | dover.idf.il | Parameter Type Violation SortDir in www.idf.il/1398-en/dover.aspx | Block | 1 |
| 66.249.65.223 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/robots.txt | Block | 1 |
| 40.77.167.46 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/901-8504/tikshuv.aspx | Block | 1 |
| 128.232.110.28 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 66.249.69.30 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.64.131 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 83.59.237.243 | Spain | 147.237.77.216 | dover.idf.il | Parameter Type Violation lang in www.idf.il/1398-en/dover.aspx | Block | 1 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 46.19.86.27 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 157.55.39.17 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx | Block | 1 |
| 66.249.64.137 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 192.243.55.133 | Block | 1 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.224 | Block | 1 |
| 64.19.78.243 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/ | Block | 1 |
| 192.243.55.129 | Dominica | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 192.243.55.129 | Block | 1 |
| 68.180.229.31 | United States | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 1 |
| 66.249.64.180 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/ | Block | 1 |
| 38.111.147.88 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 1 |
| 192.243.55.133 | Dominica | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/igf | Block | 1 |