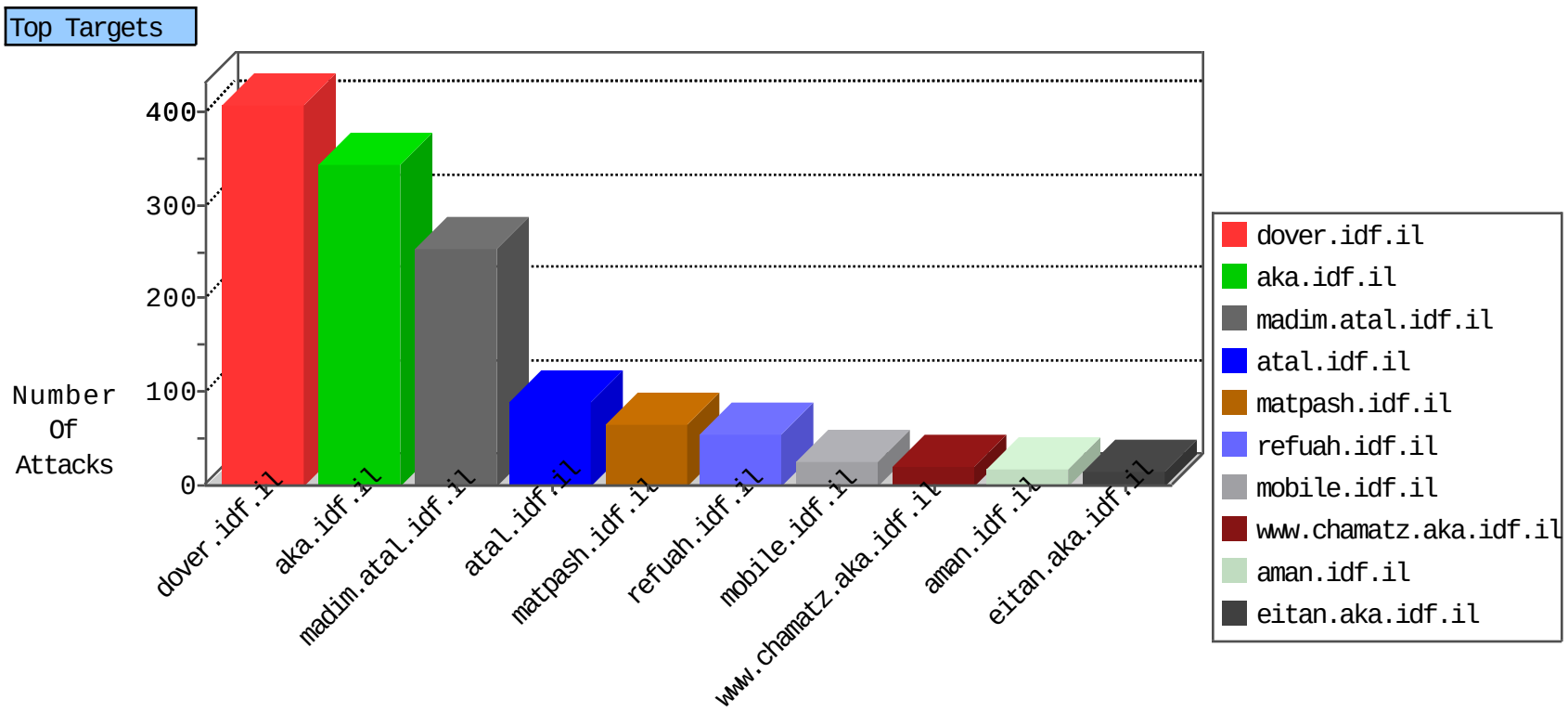
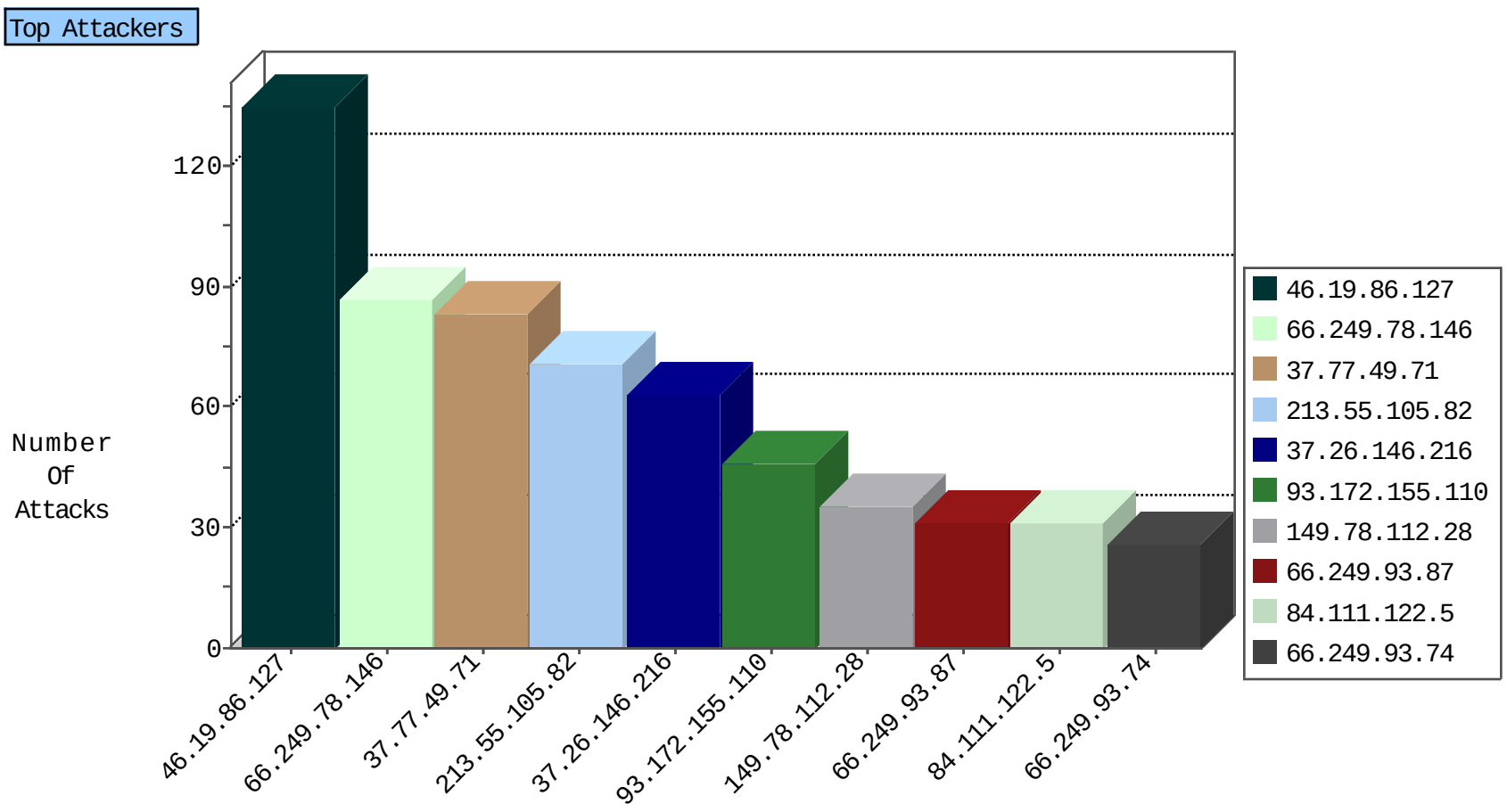
04-25-2016-14:04:09 to 04-25-2016-15:04:09

# IDF Under Attack Daily Report




Top Target




Top Attackers

04-25-2016-14:04:09 to 04-25-2016-15:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 107.77.70.46 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 467 |
| 81.218.65.210 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3 |
| 81.218.65.210 | Israel | 147.237.72.156 | aman.idf.il | Block_Udp_All_Nets | drop | 3 |
| 45.63.20.231 | United States | 147.237.76.197 | e.himush.idf.il | Block_Ntp_All_Net | drop | 1 |
| 94.102.52.10 | Netherlands | 147.237.76.39 | mobile.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-MISC-Slowloris-DOS-Var1 | dest-reset | 1 |
| 71.6.146.185 | United States | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |
| 94.102.52.10 | Netherlands | 147.237.76.198 | e.yohalan.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |

04-25-2016-14:04:09 to 04-25-2016-15:04:09

## Top Attackers In IPS

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

04-25-2016-14:04:09 to 04-25-2016-15:04:09

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 | 2 |
| 115.182.17.13 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.186.34.204 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.186.34.204 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.186.34.204 | 147.237.76.42 | China | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.186.34.204 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 213.57.234.252 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

04-25-2016-14:04:09 to 04-25-2016-15:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.249.78.146 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 87 |
| 213.55.105.82 | Ethiopia | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 50 |
| 37.77.49.71 | Iraq | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 47 |
| 66.249.93.87 | Europe | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 31 |
| 149.78.112.28 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 31 |
| 66.249.93.74 | Europe | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 24 |
| 188.32.242.200 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 66.249.93.79 | Europe | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 19 |
| 66.249.64.190 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 107.77.70.46 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 89.138.14.200 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 16 |
| 37.77.49.71 | Iraq | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 13 |
| 38.111.147.83 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 37.77.49.71 | Iraq | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 162.243.99.146 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 31.168.121.22 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 139.162.216.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 213.55.105.82 | Ethiopia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 84.111.122.5 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence |  | monitor | 10 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 207.46.13.11 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 87.70.79.196 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 79.177.43.199 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 9 |
| 46.19.85.91 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 207.46.13.34 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 216.218.147.195 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.86.207 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 207.46.13.173 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 84.94.208.75 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 185.3.147.190 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 52.29.223.39 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 89.139.188.30 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 185.37.12.200 | Palestinian Territory Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 6 |
| 79.180.176.118 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.77.49.71 | Iraq | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 66.249.65.20 | United States | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 81.218.201.79 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 45.35.64.142 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 84.111.122.5 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 84.111.122.5 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 84.111.122.5 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.86.207 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 84.110.35.154 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 157.55.39.148 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |

04-25-2016-14:04:09 to 04-25-2016-15:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.127 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 135 |
| 37.26.146.216 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 63 |
| 93.172.155.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 46 |
| 213.55.105.82 | Ethiopia | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 213.55.105.82 | Block | 7 |
| 212.179.21.194 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg | Block | 5 |
| 46.19.85.198 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.91 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 213.57.54.21 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 2 |
| 212.179.21.194 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 212.179.21.194 | Block | 2 |
| 82.102.169.113 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 192.198.151.45 | Europe | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 2 |
| 109.253.133.28 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 131.253.25.241 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 213.55.105.82 | Ethiopia | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 213.55.105.82 | Block | 2 |
| 207.46.13.34 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 217.66.251.153 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar | Block | 1 |
| 117.78.13.18 | China | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 212.68.153.94 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 84.197.247.146 | Belgium | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.233 | atal.idf.il | Illegal Byte Code Character in Method ÅÇµé§>ËÉ”ZTÊ:8J[[#22]]‹L£([[#15]]hEY)çsS¦#$ò•kÓ‹ð/!•Ð[[#25]]*#012=>R$XŽs±‡3š™#012ù | Block | 1 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 141.8.132.78 | Block | 1 |
| 2.53.17.106 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 80.246.133.177 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/ | Block | 1 |
| 207.46.13.121 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.31 | nakchal.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 66.249.64.235 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-20624-he/dover.aspx | Block | 1 |
| 119.156.54.17 | Pakistan | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 119.156.54.17 | Block | 1 |
| 84.197.247.146 | Belgium | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/wp-login.php | Block | 1 |
| 66.249.78.246 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.233 | atal.idf.il | Unknown HTTP Request Method ÅÇµé§>ËÉ”ZTÊ:8J[[#22]]‹L£([[#15]]hEY)çsS¦#$ò•kÓ‹ð/!•Ð[[#25]]*#012=>R$XŽs±‡3š™#012ù in URL | Block | 1 |
| 66.102.9.101 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english | Block | 1 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/daily | Block | 1 |
| 106.120.173.159 | China | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/robots.txt | Block | 1 |
| 5.102.173.71 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 213.57.54.21 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif | Block | 1 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.31 | nakchal.idf.il | Illegal Byte Code Character in Method 6Õàƒf9š'’àéÚÉ*[[#31]] | Block | 1 |
| 66.249.66.50 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/main/home/default.aspx | Block | 1 |
| 46.19.85.198 | Israel | 147.237.77.216 | dover.idf.il | Malformed URL | Block | 1 |
| 119.156.54.17 | Pakistan | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/ | Block | 1 |
| 85.65.116.235 | Israel | 147.237.72.156 | aman.idf.il | Too Many Cookies in a Request - 103 cookies | Block | 1 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx | Block | 1 |
| 149.78.112.28 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 66.249.64.181 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/m/templates/getfile/getfile.aspx | Block | 1 |
| 109.160.190.206 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 213.57.54.21 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 213.57.54.21 | Block | 1 |
| 208.115.113.82 | United States | 147.237.0.34 | tikshuv.idf.il | Parameter Type Violation catId in tikshuv.idf.il/site/story.aspx | Block | 1 |
| 84.108.149.78 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/modiin/default.aspx:80 | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.31 | nakchal.idf.il | Illegal Byte Code Character in URL | Block | 1 |

04-25-2016-14:04:09 to 04-25-2016-15:04:09