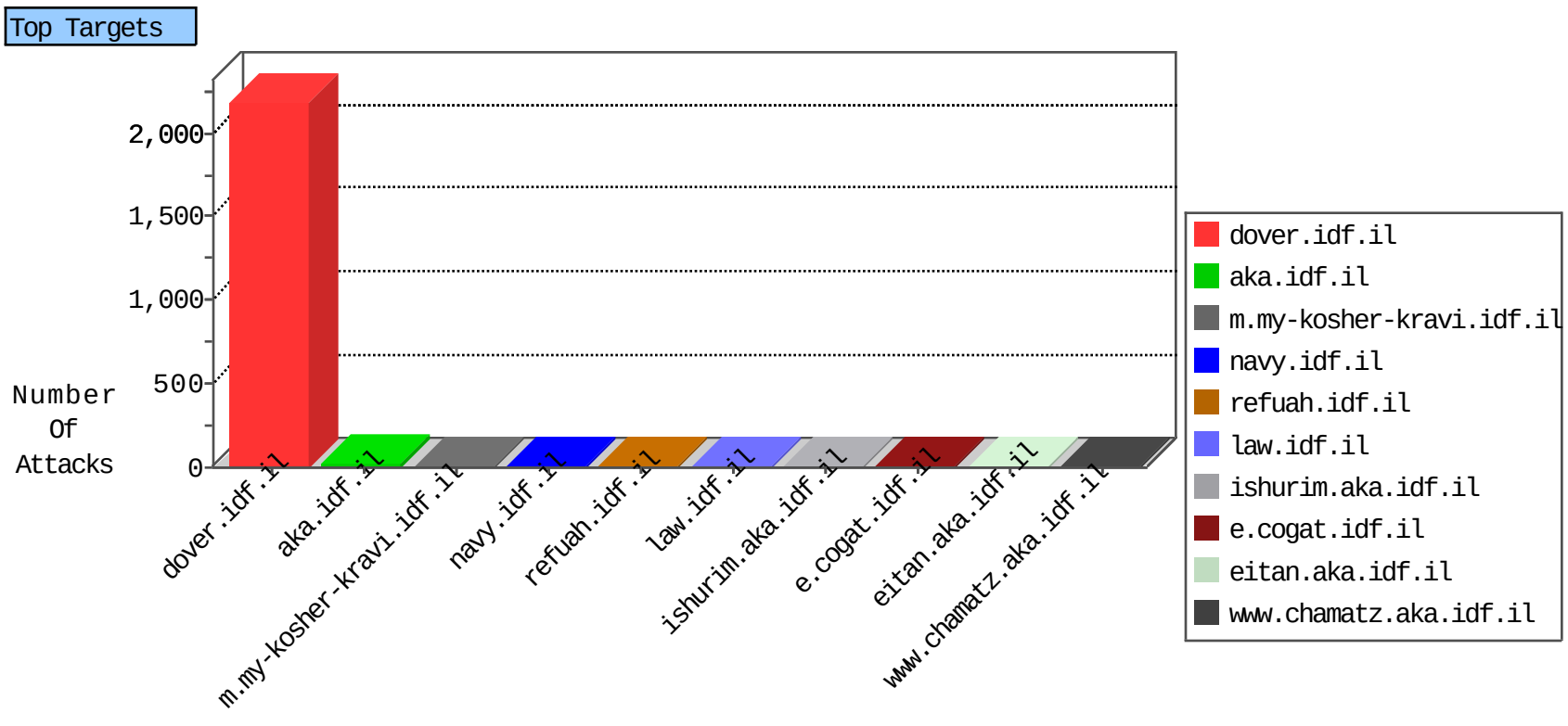
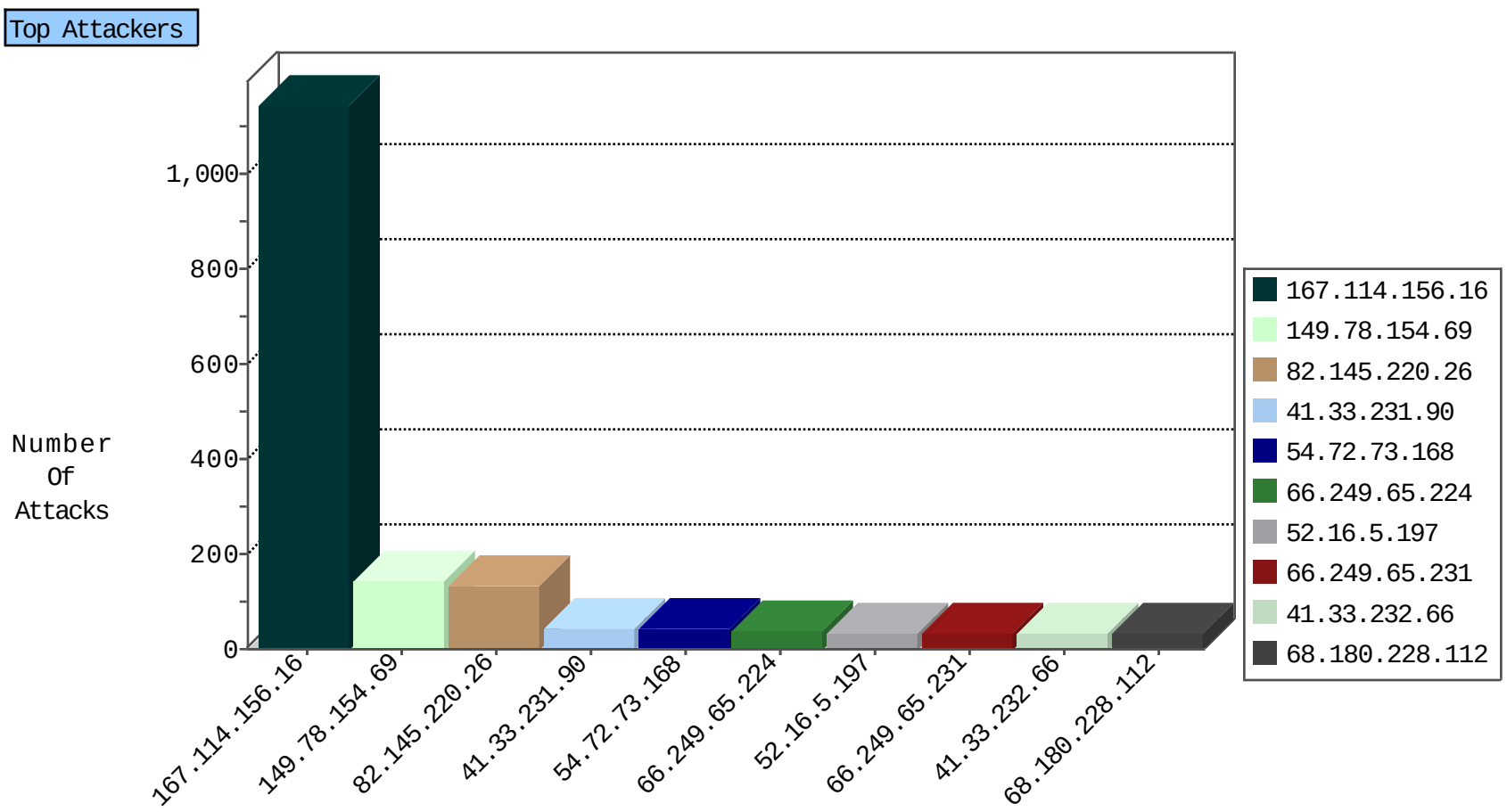
11-07-2015-05:04:04 to 11-07-2015-06:04:04

# IDF Under Attack Daily Report



11-07-2015-05:04:04 to 11-07-2015-06:04:04

## 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 | 2012 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 853 |
| 62.219.254.22 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 62.219.254.22 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 14.119.152.221 | China | 147.237.76.177 | ncore.idf.il | Block_Udp_All_Nets | drop | 1 |
| 83.5.244.118 | Poland | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |

11-07-2015-05:04:04 to 11-07-2015-06:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 195.154.180.63 | France | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 195.154.211.150 | France | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 195.154.188.186 | France | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 195.154.216.122 | France | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 195.154.211.20 | France | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 195.154.216.123 | France | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 195.154.211.30 | France | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 195.154.217.38 | France | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |
| 195.154.211.147 | France | 147.237.77.216 | dover.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |

11-07-2015-05:04:04 to 11-07-2015-06:04:04

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 8 |
| 192.35.222.17 | 147.237.77.216 | United States | dover.idf.il | ET DOS SSL Bomb DoS Attempt | 5 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 95.45.254.123 | 147.237.72.166 | Ireland | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 3 |
| 113.160.150.62 | 147.237.77.179 | Vietnam | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.248.174.106 | 147.237.8.28 | Netherlands | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 78.142.19.47 | 147.237.77.216 | Bulgaria | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.186.21.195 | 147.237.76.39 | China | mobile.meitav.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 46.151.52.8 | 147.237.76.38 | Ukraine | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.186.21.195 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 40.115.58.160 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 210.61.150.154 | 147.237.77.61 | Taiwan | e.cogat.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 188.138.9.51 | 147.237.8.14 | Germany | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 113.160.150.62 | 147.237.77.179 | Vietnam | e.mazi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 82.117.208.243 | 147.237.0.17 |  | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.186.21.195 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 78.142.19.47 | 147.237.76.147 | Bulgaria | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.186.21.195 | 147.237.0.33 | China | idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 210.61.150.154 | 147.237.77.61 | Taiwan | e.cogat.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 5.110.58.153 | 147.237.77.216 | Saudi Arabia | dover.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 210.61.150.154 | 147.237.77.61 | Taiwan | e.cogat.idf.il | ET SCAN NMAP -f -sS | 1 |
| 180.223.40.254 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |

11-07-2015-05:04:04 to 11-07-2015-06:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 145 |
| 82.145.220.26 | Europe | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 134 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 41 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 35 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 34 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 32 |
| 66.249.65.224 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 32 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 29 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 29 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 27 |
| 66.249.65.231 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 26 |
| 46.117.32.199 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 26 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 23 |
| 66.249.65.238 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 20 |
| 195.154.211.26 | France | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 18 |
| 195.154.211.20 | France | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 14 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 12 |
| 198.58.103.160 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 12 |
| 80.178.11.190 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 12 |
| 40.77.167.39 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 11 |
| 207.46.13.11 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 11 |
| 195.154.216.123 | France | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 11 |
| 188.165.15.14 | France | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 10 |
| 5.110.58.153 | Saudi Arabia | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 10 |
| 75.126.221.55 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 10 |
| 131.253.25.145 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 10 |
| 195.154.211.30 | France | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 9 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 9 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.i | drop | SAM rule | drop | 8 |
| 157.55.39.63 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8 |
| 65.19.138.34 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8 |
| 195.154.194.59 | France | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 8 |
| 66.249.65.231 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 7 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 7 |
| 5.255.253.157 | Russian Federation | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 7 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 7 |
| 209.133.111.211 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 6 |
| 157.55.39.180 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 6 |
| 66.249.67.13 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 199.30.24.94 | United States | 147.237.77.216 | dover.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 76.122.18.176 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 5 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.i | drop | | drop | 5 |
| 66.249.65.238 | Israel | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 5 |
| 129.184.84.40 | France | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 5 |
| 207.46.13.184 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 4 |
| 109.200.30.154 | United Kingdom | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 4 |
| 68.150.52.193 | Canada | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 4 |
| 128.242.249.10 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 4 |
| 66.249.65.238 | United States | 147.237.77.216 | dover.idf.i | drop | First packet isn't SYN | drop | 3 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 62.219.226.71 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 6 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 208.115.113.88 | Block | 4 |
| 195.154.211.20 | France | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 4 |
| 195.154.211.20 | France | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 195.154.211.20 | Block | 3 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 2 |
| 89.139.3.159 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 66.249.67.133 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/ | 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/8/size100x0/3238.jpg | Block | 1 |
| 181.47.177.97 | Argentina | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 75.102.8.33 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/ | Block | 1 |
| 66.249.67.13 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter pop in www.aka.idf.il/main/home/ | None | 1 |
| 195.154.211.20 | France | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/plus/mytag_js.php | Block | 1 |
| 62.210.88.201 | France | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to 51.254.206.142/httptest.php | Block | 1 |
| 95.45.254.123 | Ireland | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 66.249.67.249 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |
| 66.249.64.56 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/925-he/refuah.aspx | Block | 1 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp | Block | 1 |
| 184.168.27.42 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/ | Block | 1 |
| 85.64.202.120 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx | None | 1 |
| 66.249.67.13 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter utm_content in www.aka.idf.il/main/rabanut/general.aspx | None | 1 |
| 207.46.13.68 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/templates/news/ | Block | 1 |
| 62.210.88.201 | France | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to 51.254.206.142/httptest.php | Block | 1 |
| 129.184.84.40 | France | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx | Block | 1 |
| 68.180.230.167 | United States | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation PageNum in nakhal.idf.il/1117-he/nakhal.aspx | Block | 1 |
| 66.249.64.61 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3394.jpg | Block | 1 |
| 195.154.194.59 | France | 147.237.77.216 | dover.idf.il | Efone Config.INC Information Disclosure attempt | Block | 1 |
| 85.64.202.120 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Multiple Illegal Parameter Encoding from 85.64.202.120 | None | 1 |
| 66.249.67.59 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 208.115.111.73 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 157.55.39.221 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/robots.txt | Block | 1 |
| 66.249.65.238 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.67.65 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 65.99.237.154 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/ | Block | 1 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 162.254.149.38 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/ | Block | 1 |
| 74.82.47.3 | United States | 147.237.72.167 | ishurim.aka.idf.il | Unauthorized URL Access to 147.237.72.167/ | Block | 1 |
| 66.249.67.13 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 37.46.45.78 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 93.157.100.74 | Poland | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/wp-admin/ | Block | 1 |

11-07-2015-05:04:04 to 11-07-2015-06:04:04