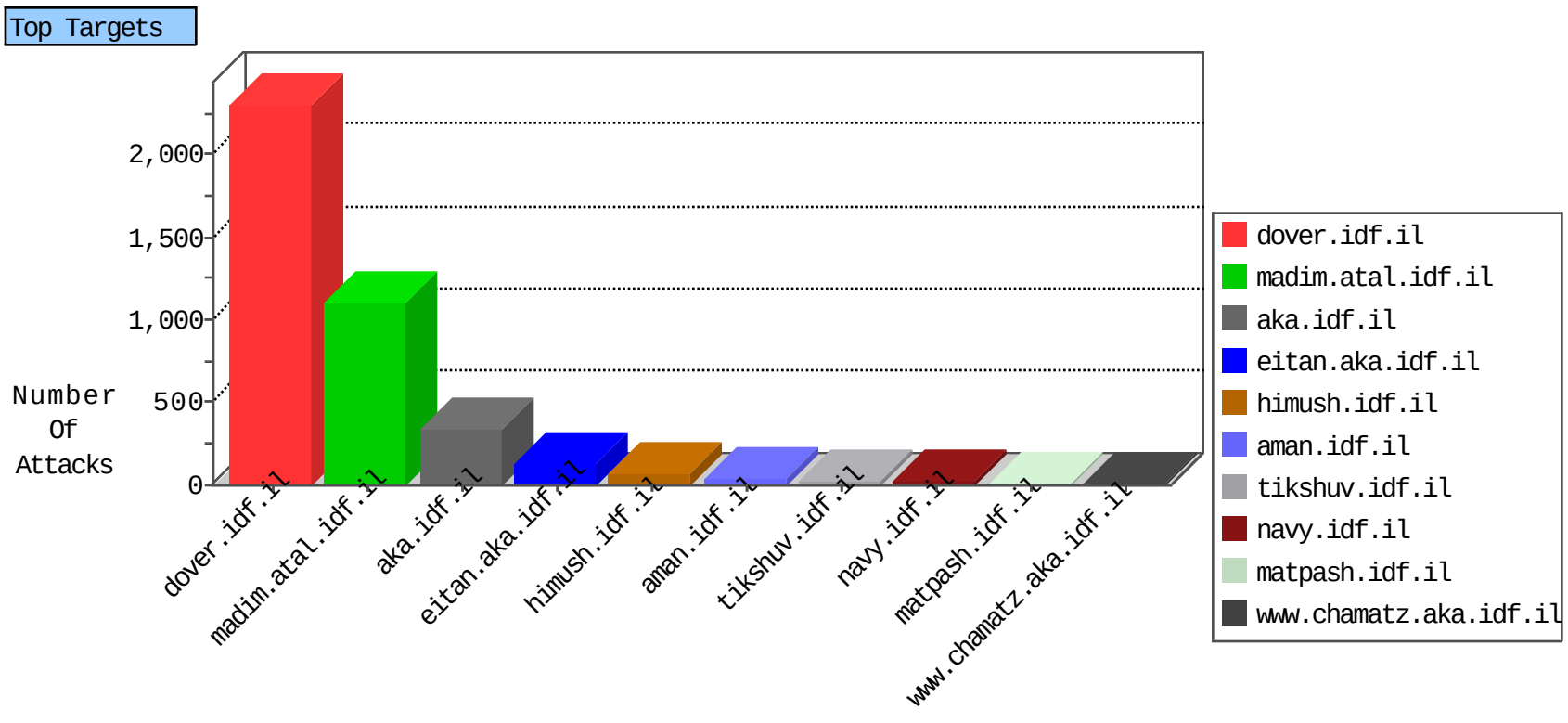
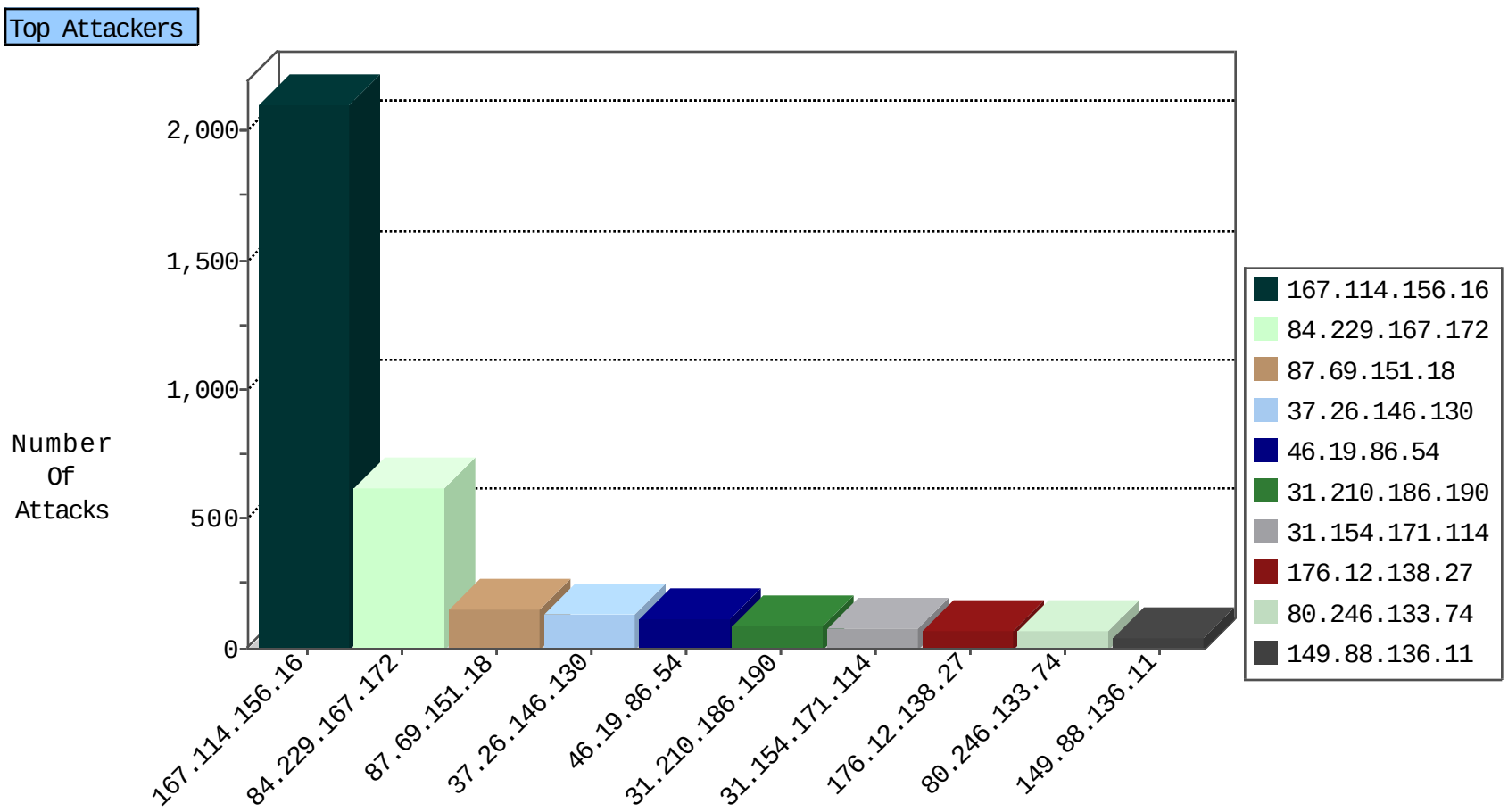
12-05-2015-22:04:08 to 12-05-2015-23:04:08

# IDF Under Attack Daily Report



12-05-2015-22:04:08 to 12-05-2015-23:04:08

## 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 | 3264 |
| 115.230.124.164 | China | 147.237.77.216 | dover.idf.il | block-sp-traf1 | drop | 1 |
| 118.193.21.98 | China | 147.237.76.197 | e.himush.idf.il | Block_Ntp_All_Net | drop | 1 |

12-05-2015-22:04:08 to 12-05-2015-23:04:08

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 222.106.222.147 | Korea, Republic of | 147.237.77.74 | law.idf.il | 9221: HTTP: PUT Method Execution over HTTP/WebDAV | Block | 1 |

12-05-2015-22:04:08 to 12-05-2015-23:04:08

## 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 |
| 80.246.133.74 | 147.237.76.30 | Israel | himush.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 4 |
| 66.249.66.61 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 210.117.121.60 | 147.237.72.167 | Korea, Republic of | ishurim.aka.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 187.245.55.214 | 147.237.72.14 | Mexico | dover.idf.il(old) | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 31.210.186.190 | 147.237.0.19 | Israel | madim.atal.idf.il | ET SCAN Possible SSL Brute Force attack or Site Crawl | 1 |
| 61.240.144.64 | 147.237.0.200 | China | m4u.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |

12-05-2015-22:04:08 to 12-05-2015-23:04:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 37.26.146.130 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 135 |
| 31.154.171.114 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 41 |
| 31.154.171.114 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 36 |
| 80.246.133.74 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 34 |
| 80.246.133.74 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | alert | 29 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 28 |
| 77.125.76.164 | Israel | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 22 |
| 188.48.9.209 | Saudi Arabia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 21 |
| 89.138.60.132 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 15 |
| 213.57.128.4 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 12 |
| 213.57.128.4 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 12 |
| 213.57.128.4 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 79.183.97.22 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 37.76.212.203 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 11 |
| 213.8.204.47 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 10 |
| 46.19.85.235 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 10 |
| 109.201.154.171 | Netherlands | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 10 |
| 173.252.88.249 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 8 |
| 66.249.74.6 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 46.19.86.206 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 109.65.129.112 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 87.69.43.248 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 79.181.125.152 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.46.39.2 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 37.26.149.176 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 5.102.254.152 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 188.120.148.238 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 5.102.254.210 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 181.30.36.5 | Argentina | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 5.102.254.82 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 85.250.59.182 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 181.30.36.5 | Argentina | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 94.230.86.172 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 173.252.88.244 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 4 |
| 185.3.144.52 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.85.17 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 173.252.88.250 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 4 |
| 149.88.136.11 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 46.19.86.206 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 80.179.143.201 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 2.54.187.209 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 185.27.105.129 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.68.157.100 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.229.131.173 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.146.239 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 188.48.9.209 | Saudi Arabia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 79.183.118.143 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

12-05-2015-22:04:08 to 12-05-2015-23:04:08

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.229.167.172 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 365 |
| 84.229.167.172 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 155 |
| 84.229.167.172 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 104 |
| 31.210.186.190 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 82 |
| 87.69.151.18 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 81 |
| 46.19.86.54 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 77 |
| 87.69.151.18 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 71 |
| 176.12.138.27 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 69 |
| 149.88.136.11 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 40 |
| 46.19.86.54 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 34 |
| 87.69.148.107 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 6 |
| 2.52.19.91 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 77.247.30.234 | Ukraine | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg | Block | 4 |
| 46.19.86.239 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.12.145.32 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 46.19.86.244 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 84.228.77.235 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 5.29.93.252 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â | Block | 2 |
| 54.159.13.0 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/main.asp | Block | 2 |
| 185.32.179.219 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 85.65.190.140 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 84.94.16.203 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â | Block | 2 |
| 77.126.68.43 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 2 |
| 2.54.176.198 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 87.69.202.26 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 51.254.33.64 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 85.65.67.60 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 1 |
| 84.108.237.116 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/images/1.he/email/mail_header.gif | Block | 1 |
| 41.237.138.113 | Egypt | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 1 |
| 107.178.194.79 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.66.31 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 5.22.129.87 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 86.104.162.55 | Romania | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php | Block | 1 |
| 46.166.186.231 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 199.16.156.126 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-ar | Block | 1 |
| 46.19.85.233 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx | Block | 1 |
| 109.67.217.139 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php | Block | 1 |
| 79.182.205.194 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 37.140.141.3 | Russian Federation | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 93.160.60.22 | Denmark | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english | Block | 1 |
| 66.249.78.236 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8847-he/refuah.aspx | Block | 1 |
| 54.81.211.131 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/newsite/hebrew/main.asp | Block | 1 |
| 213.151.40.186 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/&sa=u&ved=0ahukewjdspl7zcxjahwhxw8khs-udogqfgghmaa&usg=afqjcneeywysowwcocycbntx0qxav9lbkw | Block | 1 |
| 85.65.120.92 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/default.asp | Block | 1 |
| 178.154.243.114 | Russian Federation | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx | Block | 1 |
| 79.178.140.58 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 41.237.138.113 | Egypt | 147.237.77.176 | matpash.idf.il | Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php | Block | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |

12-05-2015-22:04:08 to 12-05-2015-23:04:08