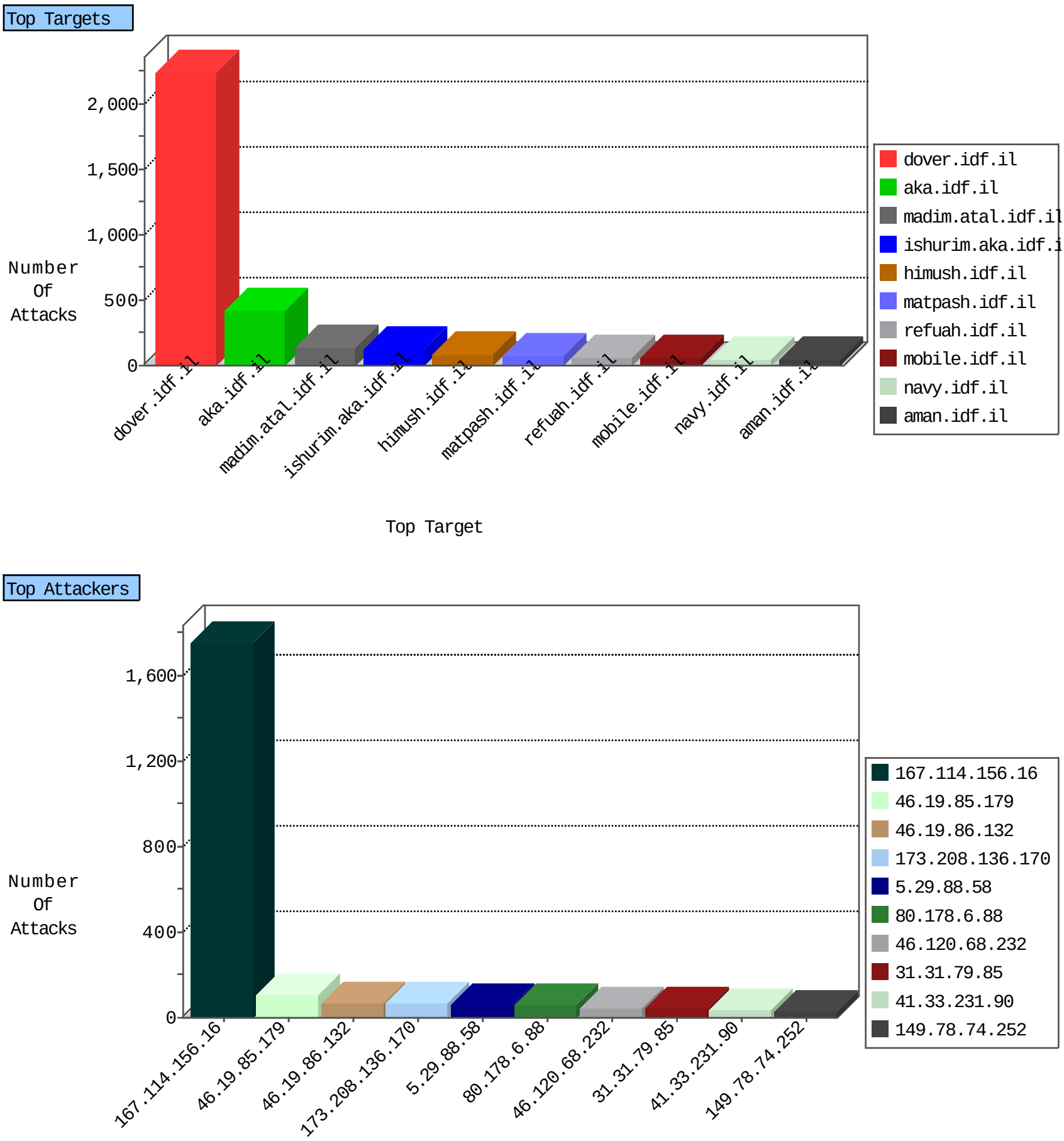
12-15-2015-22:04:06 to 12-15-2015-23:04:06

# IDF Under Attack
# Daily Report



12-15-2015-22:04:06 to 12-15-2015-23:04:06

## 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 | 3125 |
| 156.34.74.151 | Canada | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 4 |

12-15-2015-22:04:06 to 12-15-2015-23:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 2 |

12-15-2015-22:04:06 to 12-15-2015-23:04:06

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 |
| 66.102.9.28 | 147.237.72.167 | United States | ishurim.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 66.102.9.6 | 147.237.72.167 | United States | ishurim.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 42.118.12.100 | 147.237.0.200 | Vietnam | m4u.idf.il | ET SCAN NMAP -f -sS | 1 |
| 222.186.56.32 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 222.186.56.32 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 124.31.149.210 | 147.237.76.30 | China | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 85.65.192.211 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 62.90.77.221 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 42.118.12.100 | 147.237.0.200 | Vietnam | m4u.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 222.186.56.32 | 147.237.76.198 | China | e.yohalan.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 222.186.56.32 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 89.138.47.228 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.82.70.230 | 147.237.72.217 | Netherlands | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.101.92.39 | 147.237.0.35 | Russian Federation | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |

12-15-2015-22:04:06 to 12-15-2015-23:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.19.85.179 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 77 |
| 46.120.68.232 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 35 |
| 80.178.6.88 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 46.19.85.179 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 17 |
| 46.19.86.37 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 149.78.74.252 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 16 |
| 46.19.85.224 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 15 |
| 109.160.135.217 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 85.65.186.189 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 14 |
| 85.64.137.16 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 46.19.85.179 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 149.78.74.252 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 12 |
| 46.19.86.160 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 185.32.179.57 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 79.179.6.72 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 2.54.171.99 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 5.102.254.181 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 5.102.254.0 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 46.19.86.132 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 9 |
| 46.19.86.49 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 79.178.217.178 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 185.120.125.49 |  | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.86.132 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 79.177.183.25 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.86.132 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 66.249.93.113 | United States | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.86.132 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 8 |
| 46.19.85.46 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.86.132 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 185.120.125.49 |  | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 46.19.86.123 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 140.101.20.1 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 7 |
| 2.54.153.24 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 79.180.32.211 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.253.135.113 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.86.122 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.160.243.152 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 5.102.254.181 | Israel | 147.237.72.167 | ishurim.aka.idf.i | drop | First packet isn't SYN | drop | 6 |
| 2.52.160.167 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 132.66.222.127 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.148.191 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.160.243.152 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.180.129.104 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 84.108.104.229 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.65.41.19 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.64.0.246 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 93.173.12.90 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.67.41.105 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |

12-15-2015-22:04:06 to 12-15-2015-23:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 5.29.88.58 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 54 |
| 173.208.136.170 | United States | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 173.208.136.170 | Block | 43 |
| 31.31.79.85 | Czech Republic | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 41 |
| 80.178.6.88 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 80.178.6.88 | Block | 25 |
| 62.219.109.233 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 23 |
| 173.208.136.170 | United States | 147.237.77.176 | matpash.idf.il | Multiple Admin Blocking from 173.208.136.170 | Block | 19 |
| 79.179.122.78 | Israel | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 176.13.15.255 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 46.19.86.59 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 157.55.39.3 | United States | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 46.117.164.60 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 4 |
| 176.12.146.231 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 176.12.146.231 | Block | 3 |
| 82.81.3.200 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.103 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.238.140.177 | Iraq | 147.237.77.216 | dover.idf.il | Parameter Type Violation SortDir in www.idf.il/1133-he/dover.aspx | Block | 3 |
| 2.54.140.222 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 84.228.73.239 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Too Many of the Same Response Code (404) in Session from 84.228.73.239 | Block | 3 |
| 40.77.167.44 | United States | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.142.68.140 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 66.249.66.83 | Israel | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.4.126 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 95.90.251.149 | Germany | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 157.55.39.88 | United States | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 37.142.228.147 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.5.220 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 68.180.228.49 | United States | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.17.91 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 185.32.179.57 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 2 |
| 176.13.22.49 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 109.67.42.76 | Israel | 147.237.76.42 | refuah.idf.il | Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx | Block | 2 |
| 185.120.125.21 |  | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 207.46.13.135 | United States | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.228.128.6 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 46.19.85.20 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.220.156.120 | United States | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 176.10.99.208 | Switzerland | 147.237.77.216 | dover.idf.il | URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js | Block | 1 |
| 31.168.137.30 | Israel | 147.237.77.74 | law.idf.il | Parameter Type Violation prefixText in www.mag.idf.il/webservices/wscity.asmx/getcities | Block | 1 |
| 84.109.73.249 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 212.150.214.90 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 46.117.181.6 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.85.221 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 141.212.122.208 | United States | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to 147.237.0.19/ | Block | 1 |
| 185.120.126.73 |  | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnSave in www.aka.idf.il/main/giyus/faq.aspx | None | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.75.15 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-9628-he/refuah.aspx | Block | 1 |
| 54.153.32.246 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/ | Block | 1 |
| 173.208.136.170 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/administrator/siteenginemanager/components/editor/assetmanager/assetmanager.asp | Block | 1 |
| 85.65.186.189 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 213.204.101.26 | Lebanon | 147.237.76.30 | himush.idf.il | Distributed Suspicious Response Code | Block | 1 |

12-15-2015-22:04:06 to 12-15-2015-23:04:06