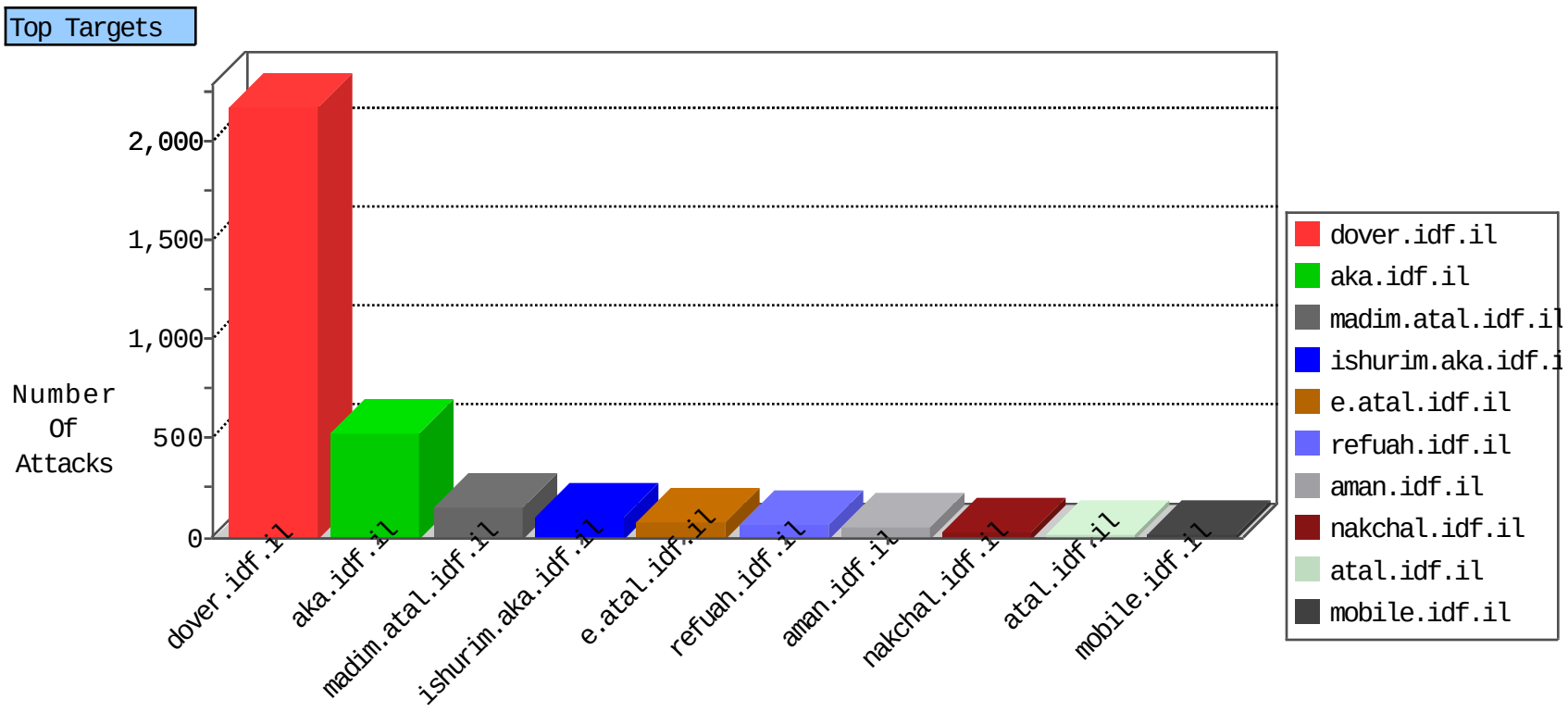
12-14-2015-13:04:01 to 12-14-2015-14:04:01

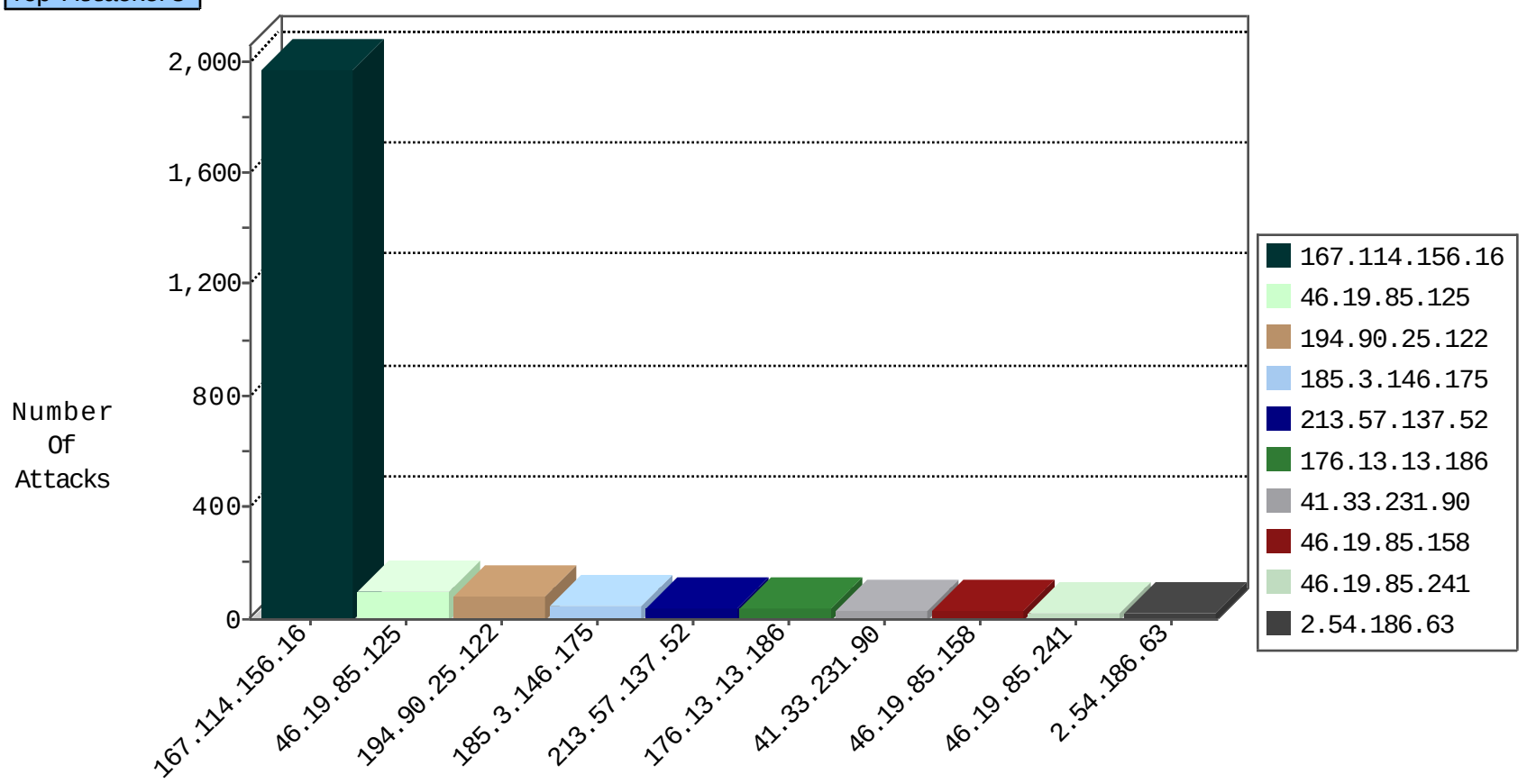
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

12-14-2015-13:04:01 to 12-14-2015-14:04:01

## 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 | 3227 |
| 81.199.122.185 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 12 |
| 46.120.68.8 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 2 |
| 185.130.5.201 | | 147.237.76.34 | yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 95.18.216.166 | Spain | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 79.183.175.91 | Israel | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |

12-14-2015-13:04:01 to 12-14-2015-14:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.64.243 | Israel | 147.237.77.216 | dover.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 1 |

12-14-2015-13:04:01 to 12-14-2015-14:04:01

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 | 1 |
| 156.170.244.162 | 147.237.77.216 | | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 119.10.114.32 | 147.237.76.39 | China | mobile.meitav.idf.i | ET SCAN NMAP -sS window 3072 | 1 |
| 95.86.107.130 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.218.246.103 | 147.237.76.201 | Russian Federation | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.218.246.103 | 147.237.76.197 | Russian Federation | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.176.206.174 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.52.168.4 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 208.115.113.89 | 147.237.77.216 | United States | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 176.228.133.128 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.78.252.208 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.67.212.169 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 93.174.89.113 | 147.237.76.34 | Netherlands | yohalan.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 91.218.246.103 | 147.237.76.199 | Russian Federation | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.179.223.31 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 62.219.229.79 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 222.186.56.32 | 147.237.77.216 | China | dover.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |

12-14-2015-13:04:01 to 12-14-2015-14:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 194.90.25.122 | Israel | 147.237.76.201 | e.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 81 |
| 185.3.146.175 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 42 |
| 46.19.85.158 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 33 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 32 |
| 213.57.137.52 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 23 |
| 213.57.137.52 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 18 |
| 213.57.128.210 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 16 |
| 84.109.93.196 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 15 |
| 107.178.195.133 | United States | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 14 |
| 79.183.103.6 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 13 |
| 62.219.182.75 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 11 |
| 46.19.85.221 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 46.19.86.109 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 107.178.195.128 | United States | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 10 |
| 31.168.14.94 | Israel | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 9 |
| 212.235.98.139 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 9 |
| 185.120.125.43 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 8 |
| 79.183.175.91 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 85.64.84.152 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 46.19.85.238 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.86.90 | Israel | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 8 |
| 2.54.38.113 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 62.219.228.172 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 84.108.57.254 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 7 |
| 77.125.106.209 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.13.5.122 | Israel | 147.237.0.19 | madim.atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.241 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 132.64.205.32 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.65.174.191 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.113 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 5.102.254.172 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 185.3.146.175 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 77.125.162.252 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.186.55.175 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 199.203.47.194 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 109.66.56.245 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 176.12.160.1 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.4 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 107.178.195.189 | United States | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.149 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 77.126.98.193 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 84.228.135.62 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.241 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.64.111.107 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.86.89 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 79.183.103.6 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 77.127.56.124 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 185.3.146.105 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 2.54.186.63 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |

12-14-2015-13:04:01 to 12-14-2015-14:04:01

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.125 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 77 |
| 176.13.13.186 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 39 |
| 46.19.85.125 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.85.125 | Block | 16 |
| 79.180.3.32 | Israel | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 79.180.3.32 | Block | 9 |
| 176.13.5.122 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 85.65.219.32 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/ | Block | 4 |
| 79.178.57.28 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 85.65.219.32 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/ | Block | 3 |
| 107.77.164.27 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 3 |
| 82.102.175.93 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 3 |
| 176.12.145.134 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.12.136.146 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.86.209 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 176.12.151.232 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 132.74.216.204 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp | Block | 2 |
| 176.12.140.10 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx. | Block | 2 |
| 2.52.46.54 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.12.143.219 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx. | Block | 2 |
| 85.65.124.150 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 2.54.22.26 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 93.173.36.168 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.20 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |
| 193.106.52.31 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 84.108.103.205 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 62.90.45.222 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/ | Block | 1 |
| 173.252.114.116 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 79.179.29.212 | Israel | 147.237.72.166 | aka.idf.il | Unknown HTTP Request Method %tÃ©Â€ 0Ã¡[[#0]][[#0]]~Â°[[#14]]Â'Ã²C3Â‡[[#16]]Ã²ÃŠÂ¸ fÂ®ÃŽwÃ¼ | Block | 1 |
| 79.177.4.165 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 207.46.13.187 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1283-18681-en/dover.aspx <a href= | Block | 1 |
| 5.29.62.214 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 107.178.195.167 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 185.32.179.159 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 79.183.103.6 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 46.19.86.73 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 176.12.148.57 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 130.193.50.36 | Russian Federation | 147.237.0.16 | my-kosher-kravi.idf.il | Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx | Block | 1 |
| 79.179.29.212 | Israel | 147.237.72.166 | aka.idf.il | Malformed URL | Block | 1 |
| 37.26.147.142 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 2.54.34.189 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 95.35.146.62 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 66.249.78.79 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/navmenu/ | Block | 1 |
| 195.154.168.82 | France | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 62.219.13.180 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 84.108.116.192 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.85.125 | Israel | 147.237.0.19 | madim.atal.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/mobile/1088-he/meretz.aspx | Block | 1 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 31.3.144.19 | Germany | 147.237.72.166 | aka.idf.il | Unknown Parameter amp;t in www.aka.idf.il/main/smalim/scriptresource.axd | None | 1 |
| 109.65.54.167 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 66.249.64.243 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp | Block | 1 |

12-14-2015-13:04:01 to 12-14-2015-14:04:01