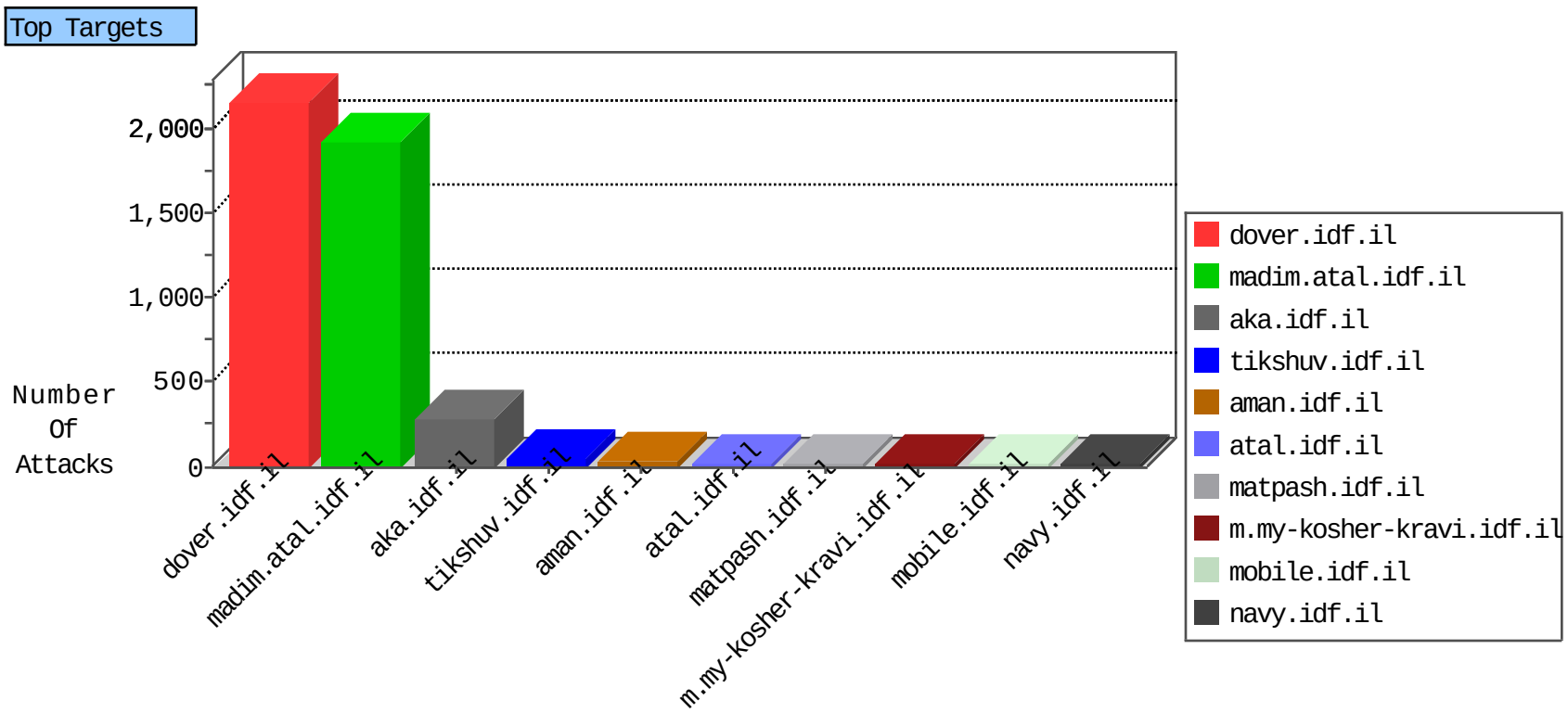
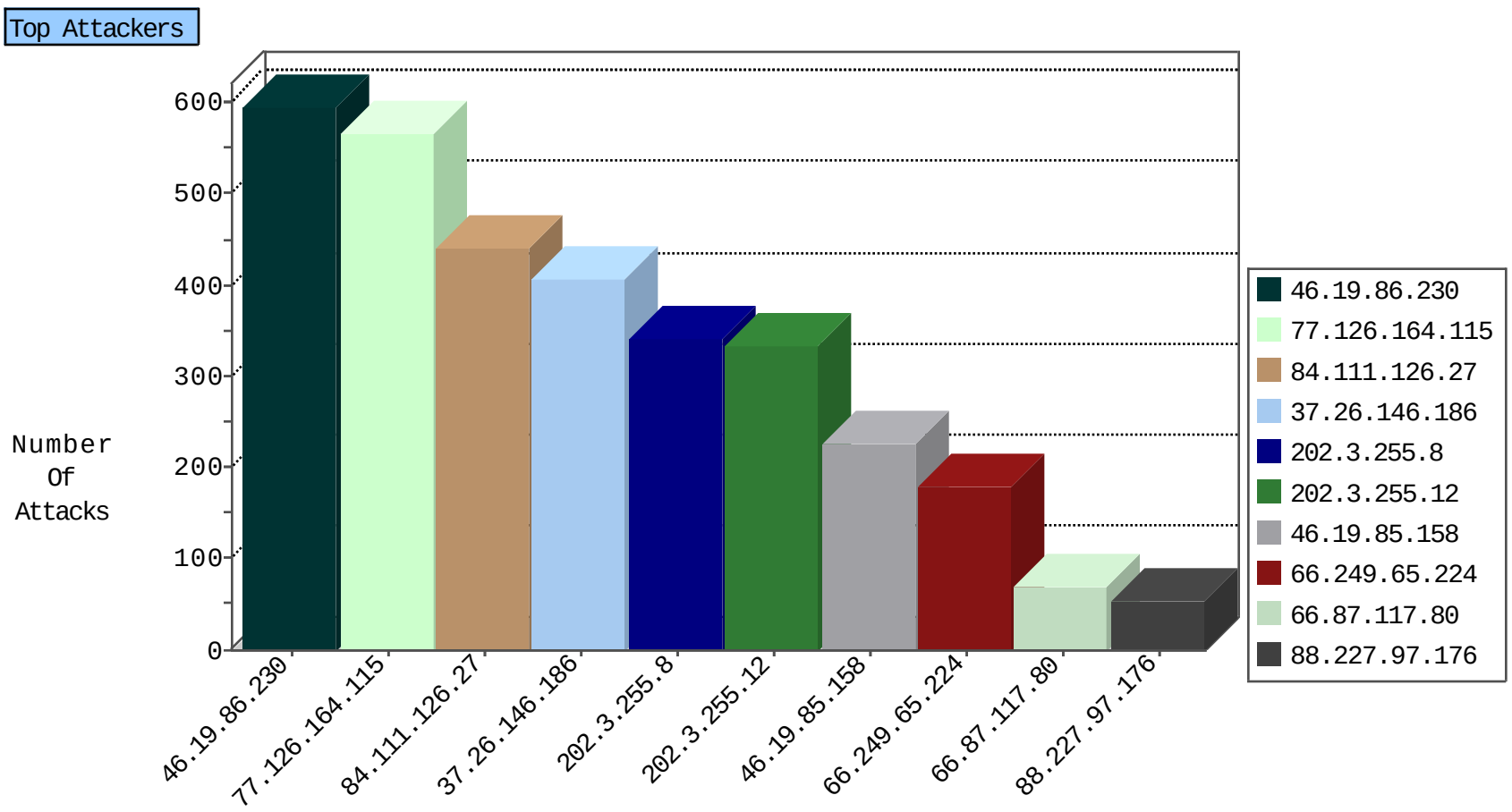
11-20-2015-16:04:00 to 11-20-2015-17:04:00

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



11-20-2015-16:04:00 to 11-20-2015-17:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 69.171.228.120 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 450 |
| 2.54.134.94 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 90 |
| 176.13.15.98 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 10 |
| 100.100.107.74 | | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 9 |
| 185.3.144.137 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 5 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 4 |
| 87.69.197.107 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 4 |
| 84.109.100.35 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 3 |
| 5.29.86.38 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 2 |
| 85.250.220.53 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 2 |
| 217.132.89.206 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 2 |
| 85.64.21.229 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 198.20.69.98 | United States | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 93.172.62.73 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |

11-20-2015-16:04:00 to 11-20-2015-17:04:00

## Top Attackers In IPS

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

11-20-2015-16:04:00 to 11-20-2015-17:04:00

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 202.3.255.8 | 147.237.77.216 | French Polynesia | dover.idf.il | GPL SCAN nmap TCP | 304 |
| 202.3.255.12 | 147.237.77.216 | French Polynesia | dover.idf.il | GPL SCAN nmap TCP | 298 |
| 66.249.78.31 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 74.117.209.135 | 147.237.76.34 | United States | yohalan.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 61.182.170.38 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 182.109.161.131 | 147.237.76.176 | China | test.ncore.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 182.109.161.131 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 61.182.170.38 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 182.109.161.131 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |

11-20-2015-16:04:00 to 11-20-2015-17:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 37.26.146.186 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 408 |
| 66.249.65.224 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 164 |
| 66.87.117.80 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 69 |
| 88.227.97.176 | Turkey | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 53 |
| 37.26.146.187 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 43 |
| 202.3.255.8 | French Polynesia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 202.3.255.12 | French Polynesia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 37 |
| 213.57.139.98 | Israel | 147.237.0.19 | madim.atal.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 37 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 50.153.146.200 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 84.242.121.62 | Czech Republic | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 27 |
| 72.9.148.10 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 100.100.87.240 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 23 |
| 100.100.122.42 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 100.100.101.107 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 31.186.228.31 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 31.186.228.57 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 79.181.100.157 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 213.57.129.8 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 17 |
| 213.57.129.8 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 100.100.127.240 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 17 |
| 31.186.228.32 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 100.100.120.7 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 14 |
| 213.57.143.80 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 14 |
| 208.115.111.73 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 12 |
| 31.186.228.95 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 100.100.33.240 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 31.186.228.60 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 199.30.24.2 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 100.100.107.74 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 198.58.103.91 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 100.100.61.147 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 100.100.101.107 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 11 |
| 31.186.228.58 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 216.223.27.54 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 50.153.146.200 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 173.252.89.58 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 8 |
| 31.186.228.94 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 149.78.131.40 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 173.252.89.55 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 8 |
| 84.111.110.211 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 66.249.78.37 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 66.249.64.221 | Israel | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 8 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 31.186.228.93 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 80.246.133.248 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 80.230.25.247 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 80.246.133.248 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |

11-20-2015-16:04:00 to 11-20-2015-17:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.230 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 393 |
| 77.126.164.115 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 335 |
| 84.111.126.27 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 268 |
| 46.19.85.158 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 133 |
| 77.126.164.115 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 122 |
| 84.111.126.27 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 113 |
| 46.19.86.230 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 107 |
| 77.126.164.115 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 107 |
| 46.19.86.230 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 94 |
| 46.19.85.158 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 69 |
| 84.111.126.27 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 61 |
| 46.19.85.158 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 24 |
| 109.160.172.56 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 18 |
| 85.65.239.24 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx | Block | 7 |
| 46.120.142.235 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 6 |
| 77.126.62.170 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 217.78.63.150 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg | Block | 4 |
| 2.52.53.138 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 46.19.86.109 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.142.159.13 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.181.48.190 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 199.30.25.114 | United States | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 3 |
| 46.19.86.9 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 84.111.115.134 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.178.161.229 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 149.78.250.223 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 80.246.137.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 87.69.193.30 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 84.95.255.154 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109455.pdf | Block | 2 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 2 |
| 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 | 2 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 84.109.115.60 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 85.65.239.24 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 77.127.232.165 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.179.66.166 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/ufi/reaction/ | Block | 1 |
| 46.185.221.230 | Jordan | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php | Block | 1 |
| 208.115.113.89 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 5.29.230.171 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |
| 66.249.67.122 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter pop in www.aka.idf.il/main/home/ | None | 1 |
| 66.249.65.223 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx | Block | 1 |
| 213.57.247.46 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 46.120.142.235 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx | Block | 1 |
| 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 | 1 |
| 79.176.20.194 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 69.243.91.188 | United States | 147.237.77.216 | dover.idf.il | E-mail collector robots 14 | Block | 1 |
| 46.19.85.165 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.66.72 | Israel | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 66.249.66.72 | Block | 1 |

11-20-2015-16:04:00 to 11-20-2015-17:04:00