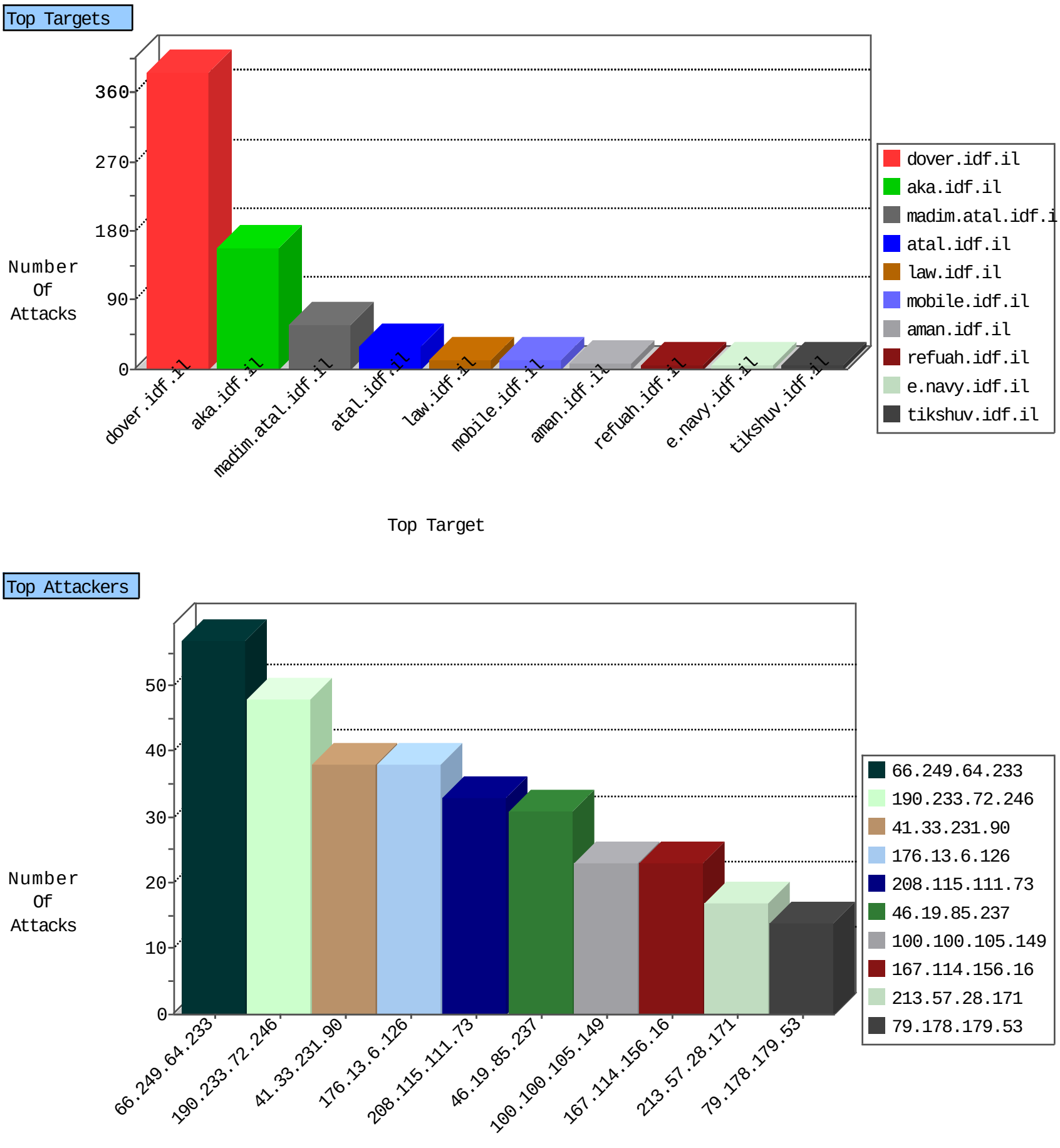
11-23-2015-00:04:03 to 11-23-2015-01:04:03

# IDF Under Attack
# Daily Report



11-23-2015-00:04:03 to 11-23-2015-01:04:03

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.67.67 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 3361 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 1776 |
| 115.239.228.8 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | Frk_Under_Attack_Con_Http | drop | 2 |
| 115.231.222.40 | China | 147.237.76.200 | eitan.aka.idf.il | JLM_Under_Attack_Con_Http | drop | 2 |
| 142.4.193.203 | United States | 147.237.76.176 | test.ncore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 176.123.0.4 | Moldova, Republic of | 147.237.76.176 | test.ncore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 142.4.193.203 | United States | 147.237.76.201 | e.atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 115.239.228.8 | China | 147.237.0.17 | m.my-kosher-kravi.idf.il | Frk_Purple_Con_Limit_Http | drop | 1 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 1 |

11-23-2015-00:04:03 to 11-23-2015-01:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.240.213.93 | United States | 147.237.72.166 | aka.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

11-23-2015-00:04:03 to 11-23-2015-01:04:03

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 |
| 66.249.64.233 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.66.125 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 104.219.238.10 | 147.237.77.226 | | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.219.238.10 | 147.237.77.121 | | e.navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.219.238.10 | 147.237.76.39 | | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.219.238.10 | 147.237.0.16 | | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 74.117.209.136 | 147.237.8.27 | United States | e.madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.228.207.18 | 147.237.77.243 | Germany | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 188.214.128.12 | 147.237.77.216 | Romania | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 124.167.55.106 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 104.219.238.10 | 147.237.77.178 | | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.219.238.10 | 147.237.77.61 | | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.219.238.10 | 147.237.0.17 | | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.219.238.10 | 147.237.0.15 | | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 66.240.213.93 | 147.237.76.30 | United States | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 188.214.128.12 | 147.237.77.226 | Romania | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.86.226 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.214.128.12 | 147.237.77.212 | Romania | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

11-23-2015-00:04:03 to 11-23-2015-01:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.249.64.233 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 52 |
| 190.233.72.246 | Peru | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 48 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 32 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 32 |
| 46.19.85.237 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 31 |
| 100.100.105.149 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 213.57.28.171 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 16 |
| 79.178.179.53 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 14 |
| 46.19.86.125 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 130.203.136.75 | United States | 147.237.77.74 | law.idf.il | Web Server Enforcement Violation | Web Servers Slow HTTP Denial of Service | reject | 8 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 77.126.195.155 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 46.19.85.229 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 66.249.64.238 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 185.120.126.82 | | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 167.114.156.198 | Canada | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 89.139.38.167 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 157.55.39.112 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.64.3.103 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.193 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 66.249.64.190 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.22.237 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 84.226.110.21 | Switzerland | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 46.19.86.91 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 70.27.242.67 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 109.186.12.30 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 79.178.114.109 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 73.36.177.185 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | | drop | 4 |
| 84.226.110.21 | Switzerland | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 79.179.187.25 | Israel | 147.237.77.243 | mobile.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 165.120.27.180 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 109.64.201.148 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.3.146.209 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 46.19.86.251 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 207.46.13.87 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 67.189.63.134 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 3 |
| 66.249.64.233 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 100.100.123.235 | | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 3 |
| 2.54.163.157 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 80.178.13.60 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 54.224.21.23 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 109.64.188.157 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.171.181 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 199.30.25.178 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 37.26.148.193 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |

11-23-2015-00:04:03 to 11-23-2015-01:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.6.126 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 36 |
| 79.177.223.48 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 4 |
| 2.54.163.157 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.124 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 84.229.55.183 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 188.120.148.173 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 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 |
| 79.178.114.109 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 208.184.112.75 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 2 |
| 37.26.149.221 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 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 | 1 |
| 79.178.54.189 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/ | Block | 1 |
| 66.249.64.93 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter 5cf35968 in aka.idf.il/news/ | None | 1 |
| 192.99.39.235 | Canada | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.179.194.143 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 207.241.226.41 | United States | 147.237.76.42 | refuah.idf.il | PHP Attempt | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx | Block | 1 |
| 176.13.6.100 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.86.91 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 87.69.105.83 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.64.190 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx | None | 1 |
| 192.116.175.122 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 109.186.173.73 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/ | Block | 1 |
| 5.22.131.124 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 79.181.211.214 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 207.241.226.41 | United States | 147.237.77.233 | atal.idf.il | PHP Attempt | Block | 1 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 95.30.56.44 | Russian Federation | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/9/ | Block | 1 |
| 79.178.225.163 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 213.57.28.171 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 66.249.64.230 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-19372-he/idfgdover.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 |
| 109.186.187.227 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser | Block | 1 |
| 207.241.226.41 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/templates/departmentslobby/piwik.php | Block | 1 |
| 78.133.226.162 | Poland | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 46.116.223.40 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 185.32.179.10 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 107.178.194.79 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 79.179.53.84 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 207.241.226.41 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/error.htm | Block | 1 |
| 66.249.67.46 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx | Block | 1 |
| 117.78.13.18 | China | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/robots.txt | Block | 1 |
| 37.142.114.42 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 85.64.3.103 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 46.166.190.167 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | 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 |
| 79.179.187.25 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/ | Block | 1 |
| 207.241.226.41 | United States | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 207.241.226.41 | Block | 1 |

11-23-2015-00:04:03 to 11-23-2015-01:04:03