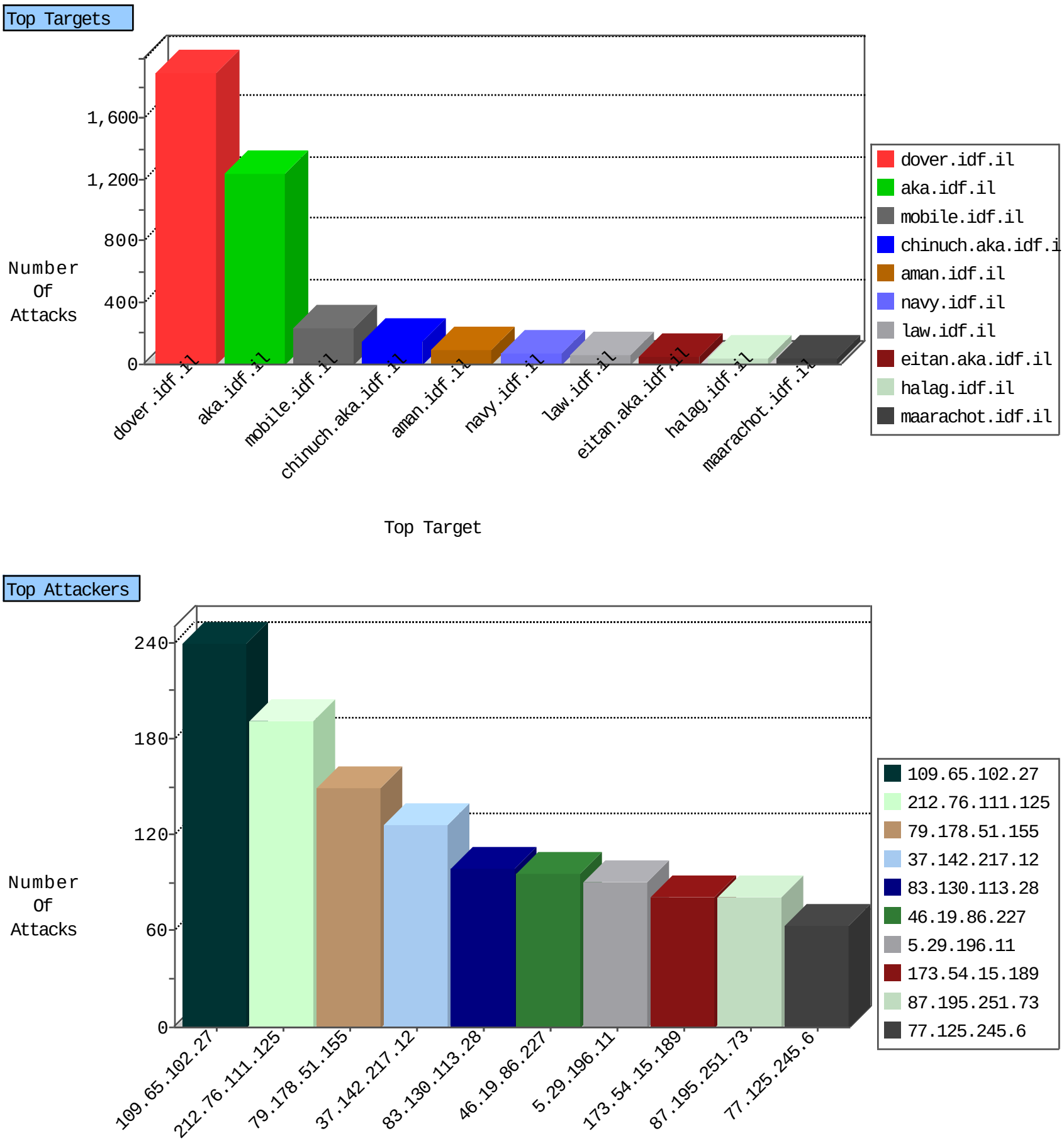
10-29-2015-22:04:08 to 10-29-2015-23:04:08

# IDF Under Attack
# Daily Report



10-29-2015-22:04:08 to 10-29-2015-23:04:08

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.102.7.240 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 193 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 135 |
| 66.249.67.27 | United States | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 72 |
| 84.229.161.187 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 38 |
| 79.181.192.73 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 21 |
| 79.178.194.28 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 17 |
| 89.173.43.248 | Slovakia | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 13 |
| 217.132.54.78 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 10 |
| 31.168.153.207 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 10 |
| 66.249.69.92 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 7 |
| 46.121.14.97 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 7 |
| 109.67.55.220 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Block_Udp_All_Nets | drop | 6 |
| 109.67.55.220 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 6 |
| 216.221.146.186 | United States | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 77.127.109.138 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 79.179.215.193 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 109.64.209.180 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 5.29.42.13 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 79.182.175.133 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 88.189.37.45 | France | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 62.219.254.22 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 79.179.59.9 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 176.12.149.82 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 188.120.134.119 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 5.102.254.167 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 213.151.55.207 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 176.13.0.91 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 176.13.20.115 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 83.211.5.111 | Italy | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 185.27.105.81 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 197.45.28.62 | Egypt | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 93.172.183.85 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 2 |
| 109.67.29.96 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 2 |
| 85.65.124.86 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 46.19.85.113 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 2.52.130.193 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 5.102.254.167 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 46.19.86.90 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 188.120.134.119 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 5.102.254.167 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 77.125.125.29 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 46.19.86.112 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 109.65.204.43 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 5.102.254.167 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 1 |
| 46.19.86.112 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 108.161.253.41 | United States | 147.237.8.45 | e.eitan.idf.il | L4 Source or Dest Port Zero | drop | 1 |
| 82.166.102.236 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 79.177.11.106 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 188.120.134.119 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 79.179.215.193 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |

10-29-2015-22:04:08 to 10-29-2015-23:04:08

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 89.139.191.39 | Israel | 147.237.72.166 | aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 1 |

10-29-2015-22:04:08 to 10-29-2015-23:04:08

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 66.249.65.40 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.78.190 | 147.237.77.176 | United States | matpash.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 93.120.243.175 | 147.237.8.28 | Russian Federation | e.mobile-ks.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |

10-29-2015-22:04:08 to 10-29-2015-23:04:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.76.111.125 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 191 |
| 87.195.251.73 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 81 |
| 173.54.15.189 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 81 |
| 37.142.217.12 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 73 |
| 77.125.245.6 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 63 |
| 69.85.243.50 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 45 |
| 31.154.144.117 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 42 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 37.142.217.12 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 190.24.146.71 | Colombia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 54.187.55.213 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 67.148.50.158 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 34 |
| 217.132.54.78 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 34 |
| 66.102.7.226 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 66.102.7.240 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 54.244.22.103 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 41.45.180.191 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 66.249.75.30 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 84.229.161.187 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 5.29.179.78 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 66.249.75.38 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 16 |
| 71.99.166.122 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 66.249.75.46 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 16 |
| 109.66.177.91 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 100.100.17.109 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 15 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 14 |
| 197.37.37.183 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 85.130.138.109 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 107.77.97.61 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 185.120.126.62 | | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 100.100.125.117 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 66.102.7.233 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 83.211.5.111 | Italy | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 79.177.11.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 216.221.146.186 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 54.244.22.103 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 10 |
| 100.100.114.235 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 10 |
| 5.102.254.167 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 84.108.175.1 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 83.130.113.28 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 79.178.194.28 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 176.13.6.238 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 206.169.227.78 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 207.46.137.200 | United States | 147.237.8.28 | e.mobile-ks.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 9 |
| 31.210.186.205 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |

10-29-2015-22:04:08 to 10-29-2015-23:04:08

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.65.102.27 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php | Block | 120 |
| 109.65.102.27 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 120 |
| 46.19.86.227 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 75 |
| 79.178.51.155 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 75 |
| 79.178.51.155 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php | Block | 75 |
| 66.249.69.16 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm | Block | 60 |
| 66.249.69.24 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm | Block | 45 |
| 2.54.162.70 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 45 |
| 5.29.196.11 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 45 |
| 83.130.113.28 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 45 |
| 5.29.196.11 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php | Block | 45 |
| 83.130.113.28 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php | Block | 45 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 30 |
| 109.66.81.202 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403 | Block | 30 |
| 62.90.167.68 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/popups/markivsachar.aspx | None | 30 |
| 79.179.32.95 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/giyu/ | Block | 30 |
| 66.249.69.8 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm | Block | 30 |
| 151.80.31.112 | Italy | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 30 |
| 207.46.13.78 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter docid in aka.idf.il/sites/klali/default.asp | None | 15 |
| 79.177.211.91 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx | None | 15 |
| 66.249.69.92 | Israel | 147.237.77.74 | law.idf.il | Distributed Illegal Parameter Encoding | None | 15 |
| 5.102.254.167 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 15 |
| 157.55.39.23 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter tablequery in aka.idf.il/eitan/listpage/default.asp | None | 15 |
| 84.109.144.206 | Israel | 147.237.72.166 | aka.idf.il | Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter | None | 15 |
| 66.249.67.234 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx | Block | 15 |
| 79.180.55.92 | Israel | 147.237.77.216 | dover.idf.il | Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx | Block | 15 |
| 66.249.67.6 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 15 |
| 46.19.85.156 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 15 |
| 176.118.79.146 | Russian Federation | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 15 |
| 66.249.67.71 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 15 |
| 84.94.96.198 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 15 |
| 46.116.144.127 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx | Block | 15 |
| 207.46.13.78 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter sorderby in aka.idf.il/iturim/asp/wars.asp | None | 15 |
| 66.249.75.83 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/page.asp | Block | 15 |
| 31.154.92.85 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 15 |
| 157.55.39.131 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/ | Block | 15 |
| 84.228.0.96 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx | Block | 15 |
| 66.249.67.247 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/pdf/files/4/112354.pdf | Block | 15 |
| 79.182.143.243 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 15 |
| 66.249.67.6 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.67.6 | Block | 15 |
| 46.19.85.170 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 15 |
| 200.100.221.82 | Brazil | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/en | Block | 15 |
| 77.125.122.147 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx | None | 15 |
| 66.249.69.24 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 15 |
| 66.249.67.122 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/giyus/[[#11]]general.aspx | Block | 15 |
| 84.95.117.160 | Israel | 147.237.77.216 | dover.idf.il | NULL Character in Method | Block | 15 |
| 207.46.13.140 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to 147.237.76.86/994-8862-he/navy.aspx | Block | 15 |
| 66.249.78.102 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-16789-he/dover.aspx | Block | 15 |
| 31.154.152.179 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx | None | 15 |
| 157.55.39.199 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/console/core/doc_mgr/undefined | Block | 15 |

10-29-2015-22:04:08 to 10-29-2015-23:04:08