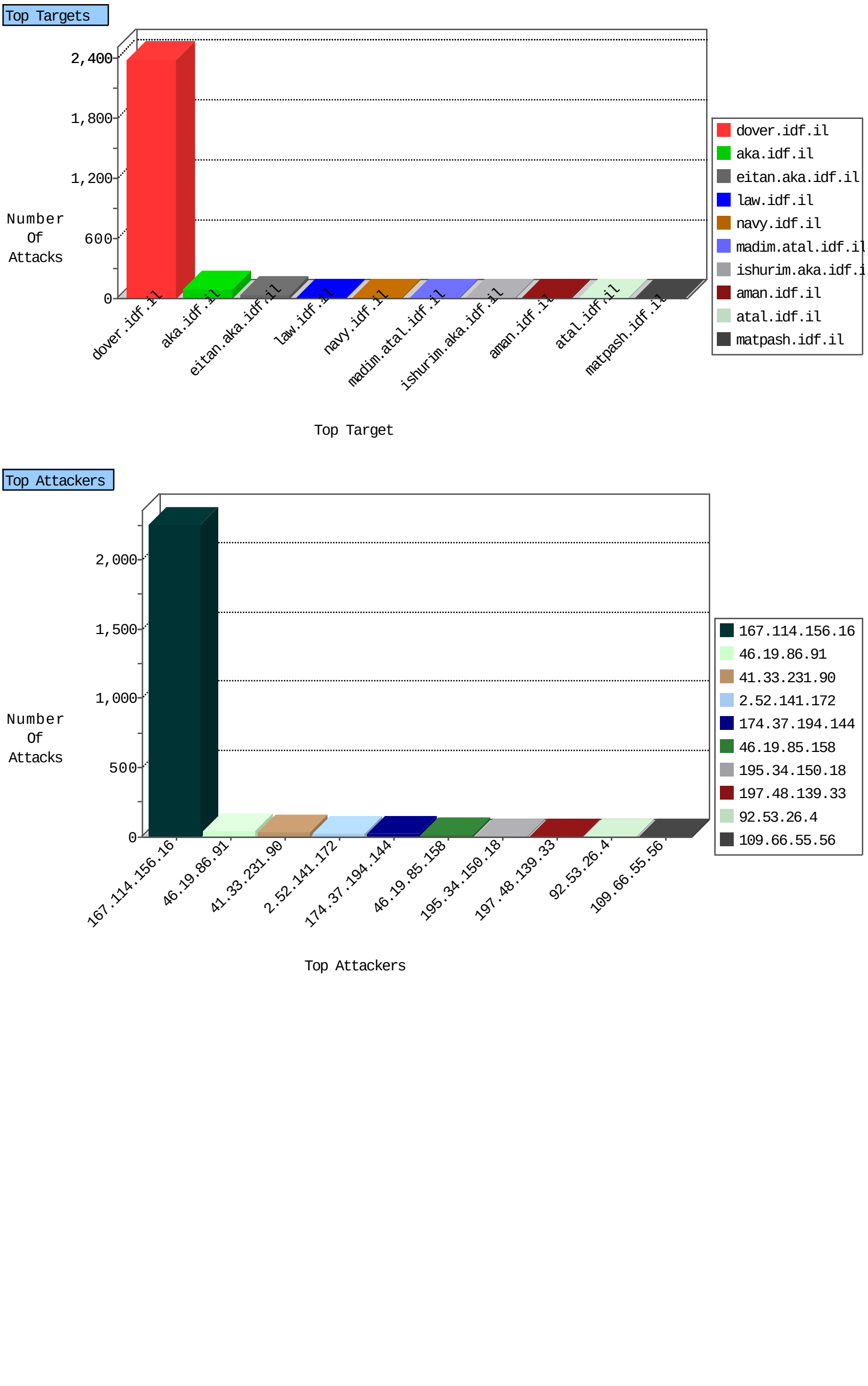
01-23-2016-00:04:01 to 01-23-2016-01:04:01

# IDF Under Attack Daily Report



01-23-2016-00:04:01 to 01-23-2016-01:04:01

## 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 | 3303 |
| 92.53.26.4 | Macedonia, the Former Yugoslav Republic of | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 115.230.124.164 | China | 147.237.77.216 | dover.idf.il | block-sp-traf1 | drop | 1 |
| 92.53.26.4 | Macedonia, the Former Yugoslav Republic of | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 92.53.26.4 | Macedonia, the Former Yugoslav Republic of | 147.237.76.198 | e.yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 8.8.8.8 | United States | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |
| 92.53.26.4 | Macedonia, the Former Yugoslav Republic of | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 92.53.26.4 | Macedonia, the Former Yugoslav Republic of | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 8.8.8.8 | United States | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 92.53.26.4 | Macedonia, the Former Yugoslav Republic of | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |
| 92.53.26.4 | Macedonia, the Former Yugoslav Republic of | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 74.91.28.58 | United States | 147.237.76.200 | eitan.aka.idf.il | block-sp-traf1 | drop | 1 |

01-23-2016-00:04:01 to 01-23-2016-01:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 172.245.218.130 | United States | 147.237.77.216 | dover.idf.il | 0543: HTTP: php.cgi Access | Block | 1 |
| 66.96.128.60 | United States | 147.237.77.233 | atal.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 1 |
| 93.89.16.110 | Turkey | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 1 |
| 115.163.56.112 | Japan | 147.237.77.216 | dover.idf.il | C008: HTTP: Xenu UserAgent | Block | 1 |

01-23-2016-00:04:01 to 01-23-2016-01:04:01

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.249.66.12 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 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 | 4 |
| 66.96.128.60 | 147.237.77.233 | United States | atal.idf.il | SQL Injection - Select From | 3 |
| 174.37.194.144 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 210.23.18.244 | 147.237.8.27 | Singapore | e.madim.atal.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 23.101.3.156 | 147.237.77.179 | Hong Kong | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 190.249.184.162 | 147.237.0.17 | Colombia | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 174.37.194.144 | 147.237.76.148 | United States | gqcenter.aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 159.8.109.19 | 147.237.72.167 | Netherlands | ishurim.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.48.195 | 147.237.77.179 | Netherlands | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.89.16.110 | 147.237.72.166 | Turkey | aka.idf.il | SQL Injection - Select From | 1 |
| 210.23.18.244 | 147.237.8.27 | Singapore | e.madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 23.101.3.156 | 147.237.77.234 | Hong Kong | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 190.249.184.162 | 147.237.0.17 | Colombia | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 177.240.82.146 | 147.237.8.14 | Mexico | e.orchot.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 174.37.194.144 | 147.237.76.197 | United States | e.himush.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 174.37.194.144 | 147.237.76.44 | United States | e.refuah.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 118.37.4.24 | 147.237.0.33 | Korea, Republic of | idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 94.102.48.195 | 147.237.77.170 | Netherlands | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

01-23-2016-00:04:01 to 01-23-2016-01:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.19.86.91 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 26 |
| 2.52.141.172 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 24 |
| 46.19.86.91 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 15 |
| 109.66.55.56 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 185.6.57.111 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 6 |
| 37.26.148.199 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 5.22.131.124 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.85.158 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 37.46.38.7 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 84.109.105.82 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 2.54.40.197 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 199.30.25.86 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 46.19.85.202 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 197.48.139.33 | Egypt | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 37.26.147.166 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 201.191.255.132 | Costa Rica | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.241 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.183.31.84 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.67.106.74 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 197.48.139.33 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 174.37.194.144 | United States | 147.237.76.196 | e.sviva.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 3 |
| 79.183.137.213 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.158 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 37.26.147.166 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.19.86.162 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 201.187.80.43 | Chile | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 84.108.92.161 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 174.37.194.144 | United States | 147.237.76.147 | chinuch.aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.19.86.91 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 84.228.97.68 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 174.37.194.144 | United States | 147.237.76.199 | e.nakchal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 46.19.86.162 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 46.19.86.91 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 174.37.194.144 | United States | 147.237.76.200 | eitan.aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 81.169.237.146 | Germany | 147.237.77.179 | e.mazi.idf.il | drop | SAM rule | drop | 2 |
| 31.210.188.16 | Israel | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 149.88.242.124 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 208.115.111.73 | United States | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 2 |
| 37.187.129.166 | France | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 84.108.92.161 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 174.37.194.144 | United States | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 2 |
| 149.88.242.124 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 84.228.97.68 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.20 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 89.139.15.104 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 172.245.218.130 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 172.245.218.130 | Block | 3 |
| 2.54.172.80 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.86.223 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 204.13.201.137 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 149.88.244.63 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 204.13.201.137 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.64.17 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/tutimprahim06012011.aspx | Block | 1 |
| 157.55.39.136 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1283-17060-en/dover.aspx>. | Block | 1 |
| 103.54.42.143 | | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 1 |
| 68.180.230.167 | United States | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx | Block | 1 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 178.255.215.87 | France | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-19779-he/kkkkkkk=34d19df9kkkkkkk_34d19df9 | Block | 1 |
| 109.66.209.136 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx | Block | 1 |
| 85.95.254.184 | Turkey | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 204.45.207.58 | United States | 147.237.77.216 | dover.idf.il | E-mail collector robots 14 | Block | 1 |
| 66.249.66.39 | Israel | 147.237.77.74 | law.idf.il | Distributed Illegal Parameter Encoding | None | 1 |
| 2.54.54.40 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 157.55.39.248 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx | None | 1 |
| 107.178.194.79 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 79.180.132.9 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hir | Block | 1 |
| 213.8.245.50 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/sip_storage/files/9/2749.jpg | Block | 1 |
| 46.19.85.250 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 197.35.61.65 | Egypt | 147.237.76.31 | nakchal.idf.il | Distributed PHP Attempt | Block | 1 |
| 121.222.7.103 | Australia | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 1 |
| 204.45.207.58 | United States | 147.237.77.216 | dover.idf.il | eMail Hoarding | Block | 1 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1589- en/dover.aspx | Block | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 83.134.123.55 | Belgium | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 197.35.61.65 | Egypt | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php | Block | 1 |
| 121.222.7.103 | Australia | 147.237.77.74 | law.idf.il | Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php | Block | 1 |
| 94.159.196.231 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 1 |
| 207.46.13.31 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 66.249.79.246 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/ | Block | 1 |
| 23.101.61.176 | Ireland | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-23118-he/dover.aspx/ | Block | 1 |
| 172.245.218.130 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/cgi-bin/php | Block | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 83.134.123.55 | Belgium | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 66.220.156.122 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 103.54.42.143 | | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 207.46.13.92 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-20786-he/dover.aspx. | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1841-he/dover.aspx | Block | 1 |
| 37.142.68.5 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx | Block | 1 |
| 176.13.3.248 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 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 |
| 84.108.81.227 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |