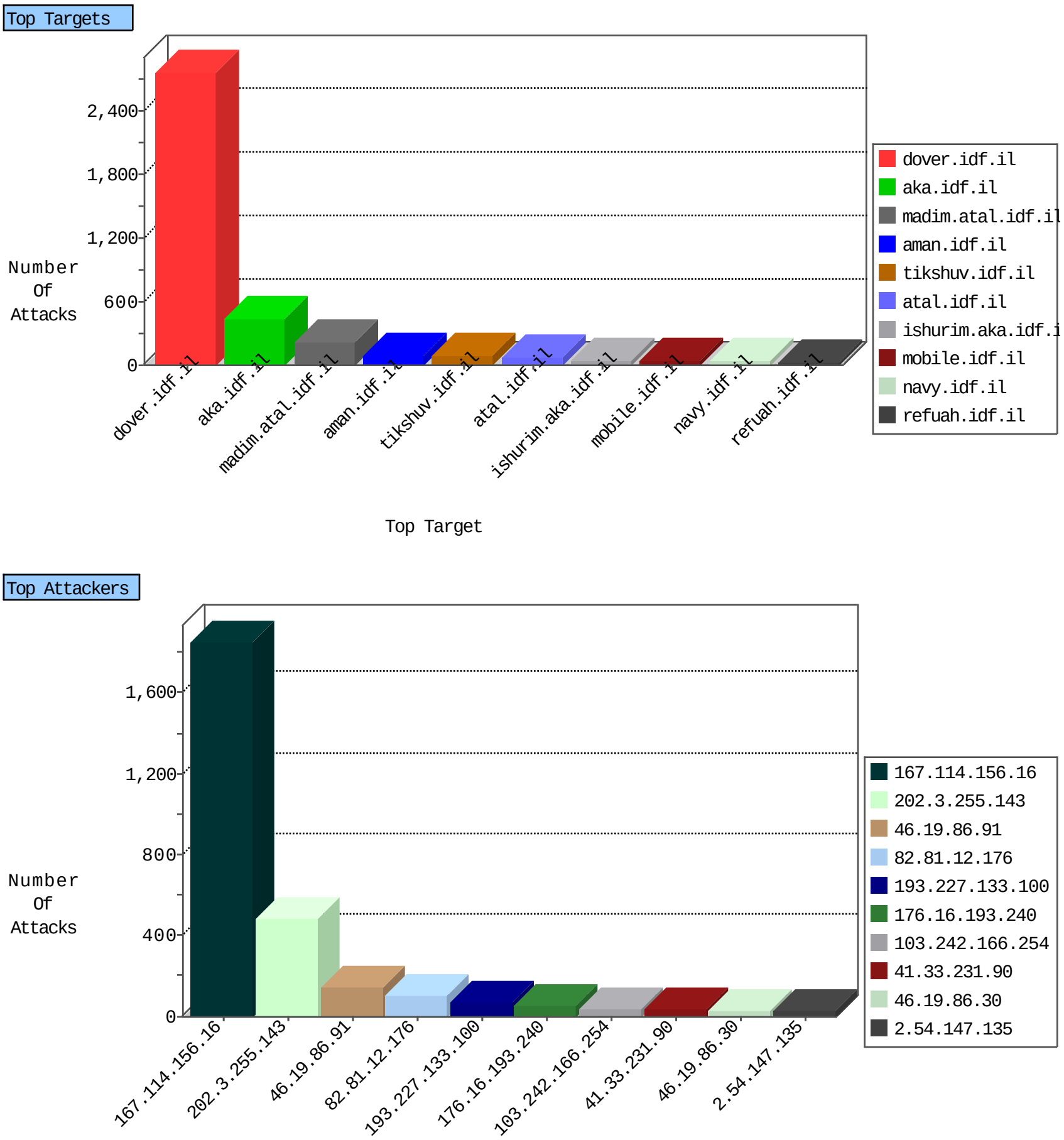
01-18-2016-19:04:05 to 01-18-2016-20:04:05

# IDF Under Attack Daily Report



01-18-2016-19:04:05 to 01-18-2016-20:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.78.2 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 8815 |
| 66.249.78.9 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 6464 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3177 |
| 82.81.12.176 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 101 |
| 193.227.133.100 | France | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 18 |
| 84.109.181.187 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 198.48.92.104 | United States | 147.237.76.148 | gqcenter.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 113.77.138.44 | China | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 58.97.111.9 | Thailand | 147.237.72.166 | aka.idf.il | Invalid TCP Flags | drop | 1 |
| 58.97.111.10 | Thailand | 147.237.72.166 | aka.idf.il | Invalid TCP Flags | drop | 1 |
| 113.77.138.44 | China | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |

01-18-2016-19:04:05 to 01-18-2016-20:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.183.50.175 | Israel | 147.237.0.34 | tikshuv.idf.il | C212: HTTP: prefix 1.01 in the URL | Block | 2 |
| 80.246.133.3 | Israel | 147.237.0.34 | tikshuv.idf.il | C212: HTTP: prefix 1.01 in the URL | Block | 2 |
| 82.165.24.123 | Germany | 147.237.77.233 | atal.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 1 |
| 188.165.15.119 | France | 147.237.0.15 | kosher-kravi.idf.il | C228: HTTP:  AhrefBot crawler | Block | 1 |

01-18-2016-19:04:05 to 01-18-2016-20:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 202.3.255.143 | 147.237.77.216 | French Polynesia | dover.idf.il | GPL SCAN nmap TCP | 443 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 82.165.24.123 | 147.237.77.233 | Germany | atal.idf.il | SQL Injection - Select From | 3 |
| 66.249.75.37 | 147.237.76.200 | United States | eitan.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 213.41.36.16 | 147.237.77.216 | United Kingdom | dover.idf.il | GPL SCAN nmap TCP | 2 |
| 66.249.81.175 | 147.237.77.233 | United States | atal.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 82.81.82.6 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 180.97.221.22 | 147.237.77.216 | China | dover.idf.il | SQL generic sql with comments injection attempt - GET parameter | 1 |
| 79.183.160.178 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 180.97.221.22 | 147.237.77.216 | China | dover.idf.il | SQL 1 = 1 - possible sql injection attempt | 1 |
| 180.97.221.22 | 147.237.77.216 | China | dover.idf.il | ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access | 1 |
| 46.161.40.120 | 147.237.77.74 | Russian Federation | law.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 168.62.238.153 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.86.255 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 163.172.13.173 | 147.237.76.42 | United Kingdom | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 2.52.58.94 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.136.41 | 147.237.77.216 | Israel | dover.idf.il | GPL SCAN myscan | 1 |
| 93.172.9.51 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.32.113.62 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.246.130.2 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 180.97.221.22 | 147.237.77.216 | China | dover.idf.il | SQL Injection - Select From | 1 |
| 180.97.221.22 | 147.237.77.216 | China | dover.idf.il | ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT | 1 |
| 50.56.221.222 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 180.97.221.22 | 147.237.77.216 | China | dover.idf.il | ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt | 1 |
| 46.121.28.6 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 168.62.238.153 | 147.237.77.176 | United States | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.142.211.25 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.136.41 | 147.237.77.216 | Israel | dover.idf.il | INDICATOR-SCAN myscan | 1 |
| 109.66.167.17 | 147.237.72.156 | Israel | aman.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.206.200.160 | 147.237.72.156 | Ukraine | aman.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 185.32.179.70 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

01-18-2016-19:04:05 to 01-18-2016-20:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 193.227.133.100 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 48 |
| 103.242.166.254 | Papua New Guinea | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 40 |
| 202.3.255.143 | French Polynesia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 46.19.86.30 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 29 |
| 107.167.116.130 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 23 |
| 176.16.193.240 | Saudi Arabia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 23 |
| 107.167.102.190 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 22 |
| 213.8.204.45 | Israel | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 18 |
| 176.16.193.240 | Saudi Arabia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 14 |
| 46.19.86.8 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 147.236.34.189 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 2.54.147.135 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 12 |
| 185.3.147.138 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 109.67.184.54 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 2.54.27.159 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 185.3.147.236 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 84.228.134.10 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 172.56.1.98 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 176.16.193.240 | Saudi Arabia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 85.65.109.210 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 176.16.193.240 | Saudi Arabia | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 66.249.81.175 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 7 |
| 109.253.209.202 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 67.11.183.117 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 2.54.147.135 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 2.54.174.152 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.66.184.31 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.86.101 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.147.135 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 193.227.133.100 | France | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 213.8.204.1 | Israel | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 6 |
| 2.54.147.135 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 31.210.188.98 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 185.3.147.138 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 67.11.183.117 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.253.209.202 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.177.142.233 | Greece | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.57 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 67.11.183.117 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 2.54.10.230 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 109.66.184.31 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.57 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 77.125.156.46 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 80.246.139.250 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 79.183.160.178 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 141.8.183.16 | Russian Federation | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.120.161.206 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 91.200.12.141 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.91 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 100 |
| 46.19.86.91 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.86.91 | Block | 40 |
| 84.228.99.132 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 25 |
| 31.168.77.168 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 20 |
| 94.230.86.205 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 16 |
| 2.54.169.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 11 |
| 109.253.140.148 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 80.246.136.165 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 85.65.120.140 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 2.54.27.159 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/sachar/index | Block | 3 |
| 176.13.22.125 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.85 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.220.164 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 202.45.154.42 | Australia | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 2 |
| 202.45.154.42 | Australia | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 2 |
| 217.132.123.12 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 41.33.241.154 | Egypt | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/894-ar | Block | 2 |
| 2.54.61.0 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 2 |
| 187.45.193.166 | Brazil | 147.237.72.167 | ishurim.aka.idf.il | Distributed PHP Attempt | Block | 2 |
| 109.67.59.85 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 46.19.86.178 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.54.154.141 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 93.136.123.70 | Croatia | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/resource/userfollowresource/create/ | Block | 2 |
| 2.54.26.209 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 2 |
| 46.19.85.175 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.46.167.71 | Canada | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 212.179.21.194 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Parameter Type Violation Master$ContentPlaceHolder1$captchaImage in my-kosher-kravi.idf.il/templates/login/login.aspx | Block | 1 |
| 14.1.194.250 | Malaysia | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 80.82.64.68 | Netherlands | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to alemara1.org/wp-content/themes/akhbar24/images/alemarah.jpg | Block | 1 |
| 186.202.127.85 | Brazil | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 182.50.155.2 | Singapore | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 50.62.208.106 | United States | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 95.211.0.114 | Netherlands | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 2.54.27.159 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.101.152.93 | | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 68.180.230.167 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp | Block | 1 |
| 176.13.7.62 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 46.19.85.190 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 91.206.200.160 | Ukraine | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 193.90.12.89 | Norway | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 31.154.35.244 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 82.80.37.238 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Distributed PHP Attempt | Block | 1 |
| 186.202.153.141 | Brazil | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 66.249.69.87 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx | Block | 1 |
| 132.66.223.9 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 213.251.182.102 | France | 147.237.72.167 | ishurim.aka.idf.il | Distributed PHP Attempt | Block | 1 |
| 79.181.103.151 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 79.181.103.151 | Block | 1 |
| 185.32.179.84 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 52.23.155.158 | United States | 147.237.76.86 | navy.idf.il | Directory Traversal - 16 | 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 |