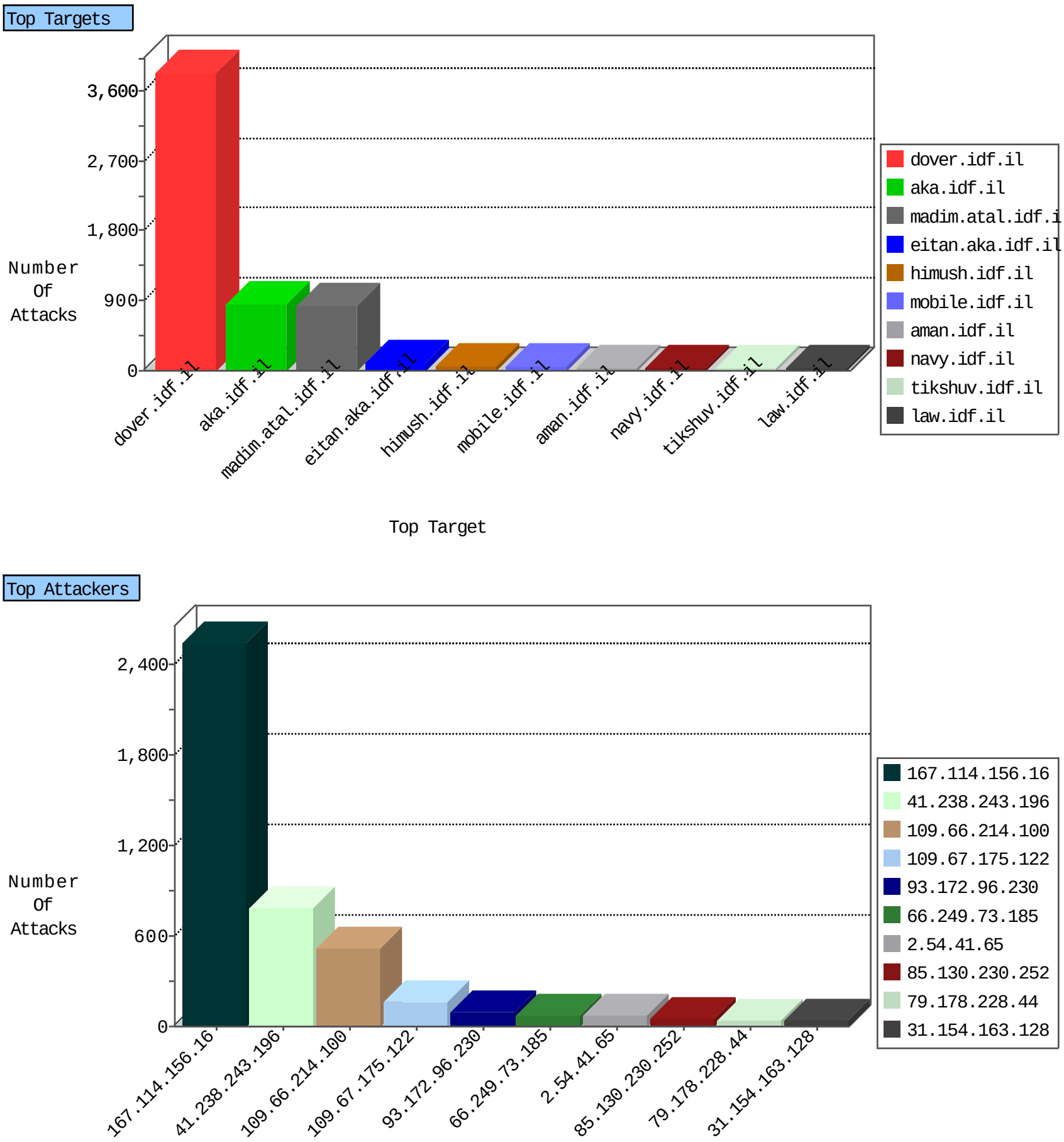
11-26-2015-17:04:07 to 11-26-2015-18:04:07

# IDF Under Attack Daily Report



11-26-2015-17:04:07 to 11-26-2015-18:04:07

## 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 | 3749 |
| 66.249.66.33 | Israel | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 1554 |
| 41.238.243.196 | Egypt | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 920 |
| 66.249.66.78 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 585 |
| 41.238.243.196 | Egypt | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 179 |
| 41.238.243.196 | Egypt | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 132 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 101 |
| 41.238.243.196 | Egypt | 147.237.77.216 | dover.idf.il | DOS-HTTP-fireflood | dest-reset | 53 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 22 |
| 79.177.183.157 | Israel | 147.237.72.156 | aman.idf.il | Block_Udp_All_Nets | drop | 6 |
| 82.166.184.140 | Israel | 147.237.76.31 | nakchal.idf.il | Block_Udp_All_Nets | drop | 4 |
| 178.214.66.201 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 146.185.57.7 | Israel | 147.237.72.156 | aman.idf.il | Block_Udp_All_Nets | drop | 3 |
| 114.161.225.244 | Japan | 147.237.76.39 | mobile.meitav.idf.i | Block_Udp_All_Nets | drop | 3 |
| 178.214.66.201 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 2 |
| 105.98.250.253 | Algeria | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 198.58.102.158 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 72.9.148.10 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 104.192.0.226 | United States | 147.237.76.147 | chinuch.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 146.185.239.100 | Russian Federation | 147.237.77.19 | law-forum.idf.il | block-sp-traf1 | drop | 1 |
| 198.20.70.114 | United States | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 93.174.93.151 | Netherlands | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 128.204.29.151 | Russian Federation | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |

11-26-2015-17:04:07 to 11-26-2015-18:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 212.199.63.46 | Israel | 147.237.77.216 | dover.idf.il | 1633: HTTP: WebDAV Protocol PROPFIND Method | Block | 5 |

11-26-2015-17:04:07 to 11-26-2015-18:04:07

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 | 2 |
| 66.249.78.130 | 147.237.76.86 | United States | navy.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.66.61 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 121.40.144.59 | 147.237.77.176 | China | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.172.71.252 | 147.237.76.31 | Ukraine | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 121.40.144.59 | 147.237.77.121 | China | e.navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 2.52.162.30 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 121.40.144.59 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN Potential SSH Scan | 1 |
| 115.47.52.157 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 198.20.69.98 | 147.237.77.235 | United States | sviva.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 109.65.173.129 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.106.94.91 | 147.237.76.38 |  | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.246.133.21 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 121.40.144.59 | 147.237.77.234 | China | halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 67.180.20.146 | 147.237.77.216 | United States | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 121.40.144.59 | 147.237.77.205 | China | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 66.249.73.201 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 121.40.144.59 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 66.249.66.1 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 121.40.144.59 | 147.237.77.170 | China | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 121.40.144.59 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 115.47.52.157 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 212.143.196.42 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 115.47.52.157 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 109.60.153.178 | 147.237.76.42 | Russian Federation | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 167.114.156.16 | 147.237.77.216 | Canada | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.178.1.190 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 121.40.144.59 | 147.237.77.226 | China | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 121.40.144.59 | 147.237.77.179 | China | e.mazi.idf.il | ET SCAN Potential SSH Scan | 1 |

11-26-2015-17:04:07 to 11-26-2015-18:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.238.243.196 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 340 |
| 109.66.214.100 | Israel | 147.237.0.19 | madim.atal.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 243 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 153 |
| 41.238.243.196 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 112 |
| 66.249.73.185 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 74 |
| 100.100.85.183 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 43 |
| 41.238.243.196 | Egypt | 147.237.77.216 | dover.idf.il | drop | | drop | 43 |
| 100.100.80.152 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 41 |
| 100.100.49.118 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 39 |
| 8.37.235.225 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 32 |
| 100.100.111.217 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 213.57.129.141 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 23 |
| 100.100.9.181 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 23 |
| 46.19.85.89 | Israel | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 22 |
| 93.172.96.230 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 22 |
| 31.154.163.128 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 22 |
| 31.154.163.128 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 21 |
| 100.100.61.164 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 21 |
| 66.249.81.212 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 20 |
| 66.249.81.215 | Russian Federation | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 100.100.33.240 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 100.100.36.68 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 100.100.76.150 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 100.100.96.236 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 17 |
| 213.57.143.49 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 16 |
| 213.57.143.49 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 16 |
| 46.19.85.89 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 15 |
| 100.100.12.40 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 14 |
| 2.54.26.168 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 14 |
| 100.100.87.240 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 13 |
| 147.114.44.208 | United Kingdom | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 147.114.44.208 | United Kingdom | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 12 |
| 85.130.216.252 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 85.130.230.252 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 185.120.126.49 | | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 85.130.230.252 | Israel | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 46.19.85.238 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 46.19.85.30 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 85.250.250.205 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 10 |
| 41.238.243.196 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 149.88.54.29 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 5.102.254.208 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 185.3.144.109 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 98.226.65.183 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 213.57.132.81 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 9 |
| 46.117.205.212 | Israel | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 46.19.85.182 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 66.249.66.61 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 85.130.230.252 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |

11-26-2015-17:04:07 to 11-26-2015-18:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.66.214.100 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 221 |
| 109.67.175.122 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 113 |
| 2.54.41.65 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 67 |
| 93.172.96.230 | Israel | 147.237.76.200 | eitan.aka.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 65 |
| 109.66.214.100 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 48 |
| 109.67.175.122 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 45 |
| 79.178.228.44 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword | Block | 44 |
| 185.120.125.15 | | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 41 |
| 46.19.86.45 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 24 |
| 46.121.123.29 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 46.121.123.29 | Block | 19 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 9 |
| 46.19.85.245 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 8 |
| 109.64.1.29 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 4 |
| 80.178.215.173 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/ | Block | 4 |
| 85.65.46.57 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 4 |
| 79.181.117.161 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 4 |
| 109.67.142.62 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 5.29.78.99 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 3 |
| 85.250.150.193 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 3 |
| 79.177.120.114 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 176.12.151.110 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 82.81.41.70 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/giyus | Block | 3 |
| 93.172.96.230 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx | Block | 3 |
| 85.64.152.65 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 3 |
| 95.86.90.164 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 3 |
| 2.52.162.30 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 212.199.63.46 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 212.199.63.46 | Block | 3 |
| 66.249.66.61 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 3 |
| 212.199.63.46 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 3 |
| 46.116.198.176 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 3 |
| 176.106.227.137 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 3 |
| 46.117.239.182 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 176.12.144.149 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 212.150.209.205 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59333&docid=68029 | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 2 |
| 2.54.48.198 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 176.13.5.250 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 80.246.130.33 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 2 |
| 46.116.84.54 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 46.121.123.29 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â | Block | 2 |
| 87.69.165.43 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 2 |
| 37.142.68.108 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 80.179.8.225 | Israel | 147.237.77.74 | law.idf.il | Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/657-he/patzar.aspx | Block | 2 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 176.12.143.89 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 212.117.157.74 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 81.218.151.130 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 5.22.134.149 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 82.166.237.150 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 157.55.39.129 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |

11-26-2015-17:04:07 to 11-26-2015-18:04:07