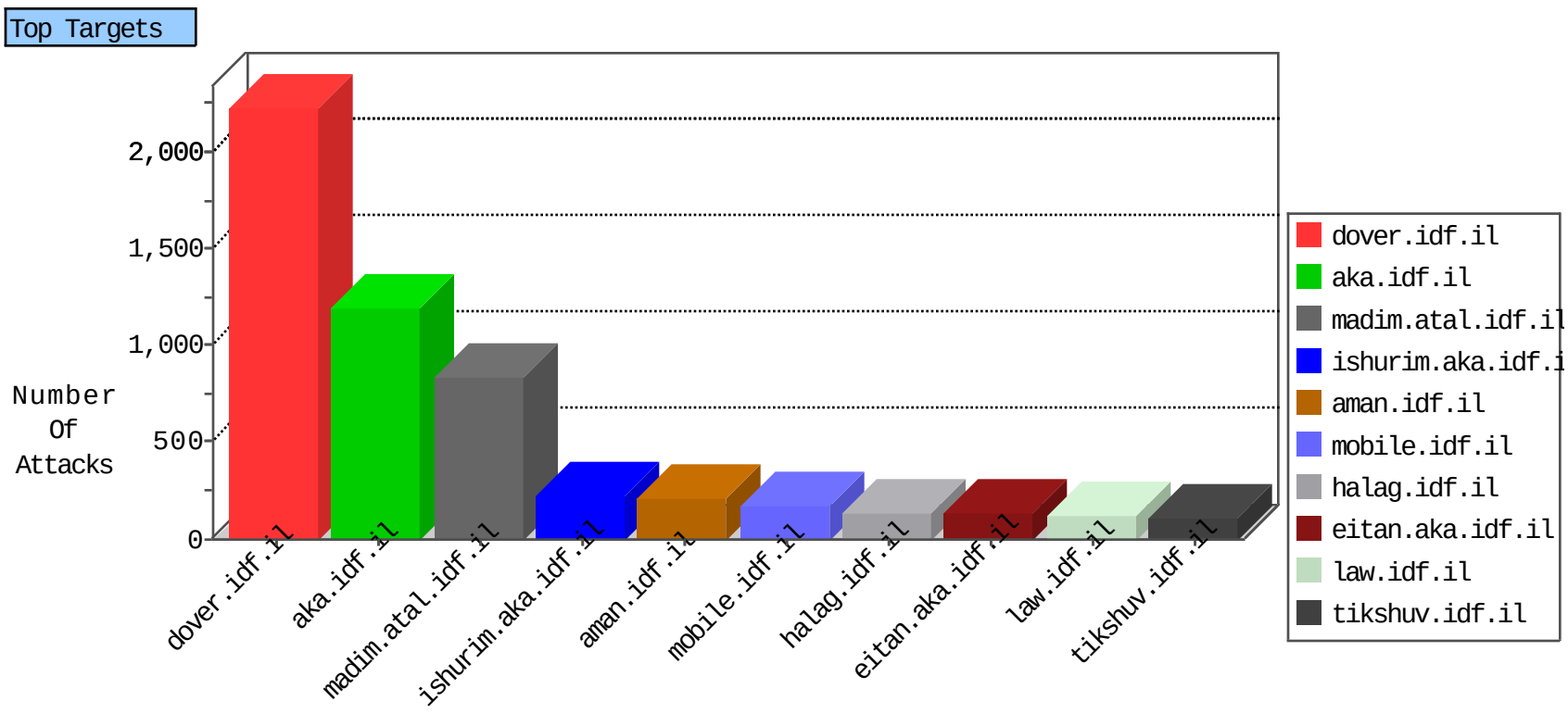
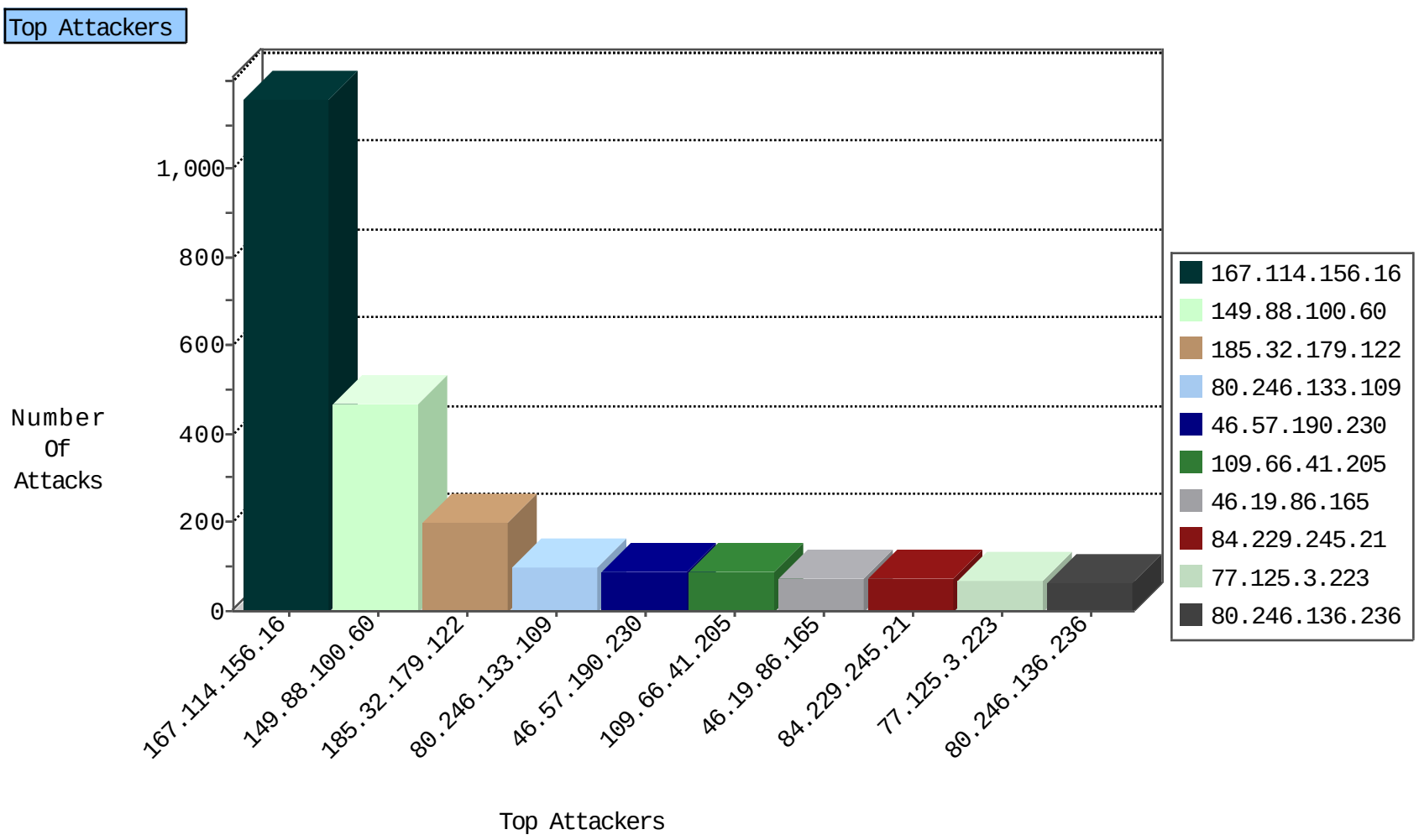
01-08-2016-11:04:01 to 01-08-2016-12:04:01

# IDF Under Attack
# Daily Report



01-08-2016-11:04:01 to 01-08-2016-12:04:01

## 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 | 3018 |
| 202.112.51.96 | China | 147.237.77.216 | dover.idf.il | block-sp-traf1 | drop | 1 |
| 146.185.239.100 | Russian Federation | 147.237.77.176 | matpash.idf.il | block-sp-traf1 | drop | 1 |
| 202.112.51.96 | China | 147.237.76.39 | mobile.meitav.idf.il | block-sp-traf1 | drop | 1 |
| 74.143.58.3 | United States | 147.237.76.44 | e.refuah.idf.il | Block_Udp_All_Nets | drop | 1 |
| 202.112.51.96 | China | 147.237.77.233 | atal.idf.il | block-sp-traf1 | drop | 1 |
| 202.112.51.96 | China | 147.237.76.86 | navy.idf.il | block-sp-traf1 | drop | 1 |
| 107.150.55.214 | United States | 147.237.72.167 | ishurim.aka.idf.il | block-sp-traf1 | drop | 1 |
| 202.112.51.96 | China | 147.237.0.19 | madim.atal.idf.il | block-sp-traf1 | drop | 1 |
| 202.112.51.96 | China | 147.237.77.170 | maarachot.idf.il | block-sp-traf1 | drop | 1 |
| 107.150.60.77 | United States | 147.237.77.74 | law.idf.il | block-sp-traf1 | drop | 1 |
| 202.112.51.96 | China | 147.237.72.167 | ishurim.aka.idf.il | block-sp-traf1 | drop | 1 |

01-08-2016-11:04:01 to 01-08-2016-12:04:01

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 136.243.103.92 | Germany | 147.237.76.86 | navy.idf.il | C1000106: HTTP: majestic bot | Block | 1 |
| 188.165.15.200 | France | 147.237.72.156 | aman.idf.il | C228: HTTP:  AhrefBot crawler | Block | 1 |

01-08-2016-11:04:01 to 01-08-2016-12:04:01

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 109.67.115.69 | 147.237.76.86 | Israel | navy.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 66.249.93.143 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.66.182 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 84.108.38.77 | 147.237.76.86 | Israel | navy.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 176.77.47.101 | 147.237.72.166 | Russian Federation | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.117.217.18 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 173.199.74.136 | 147.237.77.243 | United Kingdom | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.26.204.144 | 147.237.72.166 | Spain | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 131.109.15.15 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.142.236.56 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 104.128.144.131 | 147.237.8.45 | Canada | e.eitan.idf.il | ET SCAN NMAP -f -sS | 1 |
| 213.57.169.70 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.135.102.188 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 193.201.227.200 | 147.237.0.16 | Ukraine | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.64.93.15 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 183.61.109.189 | 147.237.72.166 | China | aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 80.230.25.18 | 147.237.77.233 | Israel | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 183.61.109.189 | 147.237.72.166 | China | aka.idf.il | ET SCAN NMAP -f -sS | 1 |
| 176.13.6.170 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.116.189.245 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 131.109.15.15 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 46.19.86.150 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.201.75 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 104.128.144.131 | 147.237.8.45 | Canada | e.eitan.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 218.77.79.38 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN Rapid POP3 Connections - Possible Brute Force Attack | 1 |
| 95.156.251.10 | 147.237.77.243 | Germany | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 87.69.204.68 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.32.179.122 | 147.237.0.19 | Israel | madim.atal.idf.il | ET SCAN Possible SSL Brute Force attack or Site Crawl | 1 |
| 183.61.109.189 | 147.237.72.166 | China | aka.idf.il | ET SCAN NMAP -sS window 2048 | 1 |

01-08-2016-11:04:01 to 01-08-2016-12:04:01

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 77.125.3.223 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 69 |
| 84.229.245.21 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 69 |
| 46.57.190.230 | Syrian Arab Republic | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 45 |
| 46.57.190.230 | Syrian Arab Republic | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 45 |
| 80.246.133.109 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 42 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 109.66.56.223 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 34 |
| 109.66.169.62 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 27 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 25 |
| 176.13.23.128 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 25 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 22 |
| 109.253.214.138 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 22 |
| 80.149.71.210 | Germany | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 22 |
| 46.19.86.72 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 104.236.203.68 | | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 21 |
| 2.54.34.132 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 80.149.71.210 | Germany | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 20 |
| 85.65.122.233 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 20 |
| 80.246.133.109 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 19 |
| 104.236.203.68 | | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 19 |
| 2.54.179.55 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 18 |
| 37.26.148.159 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 109.253.207.199 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 109.253.220.234 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 80.246.136.236 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 17 |
| 109.64.105.252 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 2.54.49.45 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 82.80.196.44 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 133.130.98.204 | Japan | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 16 |
| 2.54.63.131 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 109.64.105.252 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 15 |
| 133.130.98.204 | Japan | 147.237.76.200 | eitan.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 15 |
| 84.228.34.234 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 46.121.121.227 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 15 |
| 133.130.98.204 | Japan | 147.237.76.200 | eitan.aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 14 |
| 80.246.133.109 | Israel | 147.237.77.234 | halag.idf.il | drop | First packet isn't SYN | drop | 14 |
| 79.180.24.127 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 80.246.133.109 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | | monitor | 13 |
| 80.246.136.236 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 13 |
| 109.253.212.122 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 79.180.24.127 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 13 |
| 176.13.13.75 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 71.116.66.215 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 109.253.217.200 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 176.13.7.70 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 109.64.181.20 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 71.116.66.215 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 12 |
| 95.35.193.110 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 46.120.165.233 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 109.65.168.55 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 149.88.100.60 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 149.88.100.60 | Block | 222 |
| 149.88.100.60 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 116 |
| 149.88.100.60 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (403) in Session from 149.88.100.60 | Block | 114 |
| 185.32.179.122 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 102 |
| 109.66.41.205 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Too Many of the Same Response Code (404) in Session from 109.66.41.205 | Block | 81 |
| 185.32.179.122 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 74 |
| 46.19.86.165 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 62 |
| 185.32.179.122 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 19 |
| 176.13.20.147 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 79.177.177.236 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 10 |
| 194.90.89.5 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 80.246.140.118 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 8 |
| 87.69.172.57 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 80.246.137.130 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 164.138.115.62 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/1/113481.pdf&sa=u&ved=0ahukewi0xjtd-pnkahwhfhikhw07croqfggomam&usg=afqjcnhddnmcanx9goxshde6vmricrj_dq | Block | 4 |
| 80.246.138.31 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 109.66.169.62 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 2.54.3.113 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 95.35.193.110 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.146.243 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.3.252 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 212.76.110.143 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.148.159 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.233 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.140.149 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.180.53.202 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 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 | 2 |
| 77.125.2.105 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 80.246.139.2 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 2 |
| 2.54.58.111 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.7.70 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 91.200.12.139 | Ukraine | 147.237.77.176 | matpash.idf.il | PHP Attempt | Block | 2 |
| 79.180.24.127 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 87.69.170.120 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/ | Block | 2 |
| 46.19.85.29 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unknown HTTP Request Method from 46.19.85.29 | Block | 1 |
| 157.55.39.2 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp | Block | 1 |
| 37.142.64.112 | Israel | 147.237.72.166 | aka.idf.il | Malformed URL | Block | 1 |
| 121.241.127.12 | India | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/5/1475.png | Block | 1 |
| 208.80.194.126 | United States | 147.237.72.167 | ishurim.aka.idf.il | Unauthorized URL Access to 147.237.72.167/ | Block | 1 |
| 31.168.220.100 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 66.249.79.232 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |
| 185.130.5.216 | | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 46.19.86.165 | Israel | 147.237.0.19 | madim.atal.idf.il | Multiple Untraceable SSL Sessions from 46.19.86.165 (Open Mode) | None | 1 |
| 176.13.14.231 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 1 |
| 212.235.43.221 | Israel | 147.237.77.233 | atal.idf.il | Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx | Block | 1 |
| 40.77.167.74 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/yohalan/home/home.asp | Block | 1 |
| 149.88.100.60 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many 403: Response Code per Session | Block | 1 |