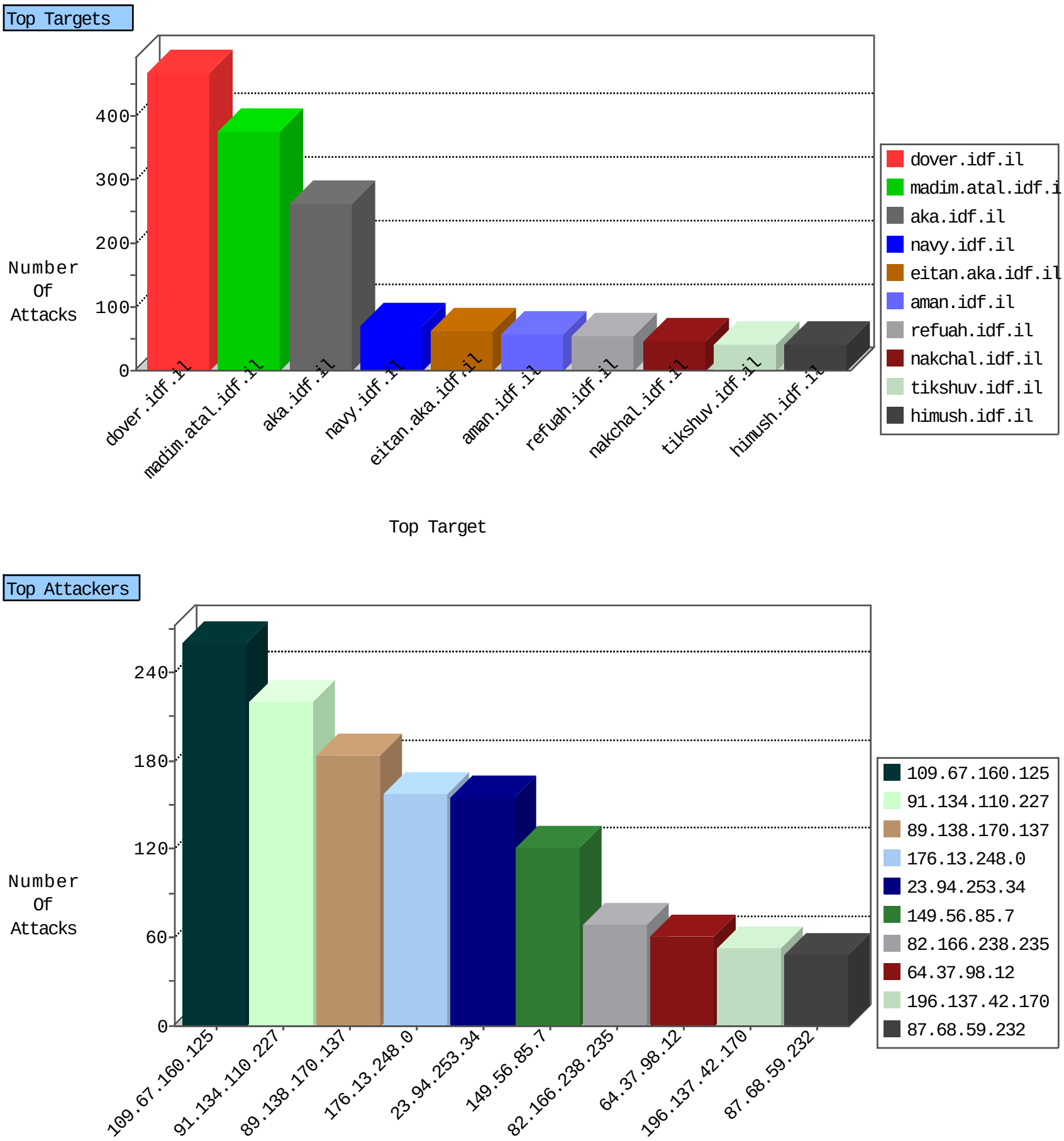
09-08-2016-22:04:07 to 09-08-2016-23:04:07

# IDF Under Attack
# Daily Report



09-08-2016-22:04:07 to 09-08-2016-23:04:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 94.102.60.21 | Netherlands | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2776 |
| 109.67.160.125 | Israel | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 2236 |
| 109.67.160.125 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 144 |
| 149.202.57.201 | France | 147.237.76.30 | himush.idf.il | Black List | drop | 1 |
| 149.202.57.201 | France | 147.237.76.34 | yohalan.idf.il | Black List | drop | 1 |
| 149.202.57.201 | France | 147.237.76.147 | chinuch.aka.idf.il | Black List | drop | 1 |
| 37.26.148.237 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 149.202.57.201 | France | 147.237.76.202 | e.halag.idf.il | Black List | drop | 1 |
| 82.221.105.6 | Iceland | 147.237.76.38 | e.e.meitav.idf.il | Black List | drop | 1 |

09-08-2016-22:04:07 to 09-08-2016-23:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.165.197.141 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 64.137.242.231 | Canada | 147.237.77.216 | dover.idf.il | 24910: HTTP: Python urllib User-Agent Header | Block | 1 |

09-08-2016-22:04:07 to 09-08-2016-23:04:07

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 77.138.22.23 | 147.237.77.216 | France | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 61.240.144.65 | 147.237.77.216 | China | dover.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 163.172.129.15 | 147.237.76.176 | United Kingdom | test.ncore.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 61.240.144.65 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 163.172.129.15 | 147.237.72.217 | United Kingdom | e.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 61.240.144.65 | 147.237.72.156 | China | aman.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 104.128.144.131 | 147.237.77.176 | Canada | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.8.45 | China | e.eitan.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 93.174.94.142 | 147.237.77.243 | Netherlands | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.172.71.251 | 147.237.76.148 | Ukraine | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.174.94.142 | 147.237.77.227 | Netherlands | e.hamaz.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 12.139.34.20 | 147.237.76.148 | United States | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 91.224.160.106 | 147.237.0.34 | Netherlands | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 12.139.34.20 | 147.237.76.148 | United States | gqcenter.aka.idf.il | ET SCAN NMAP -f -sS | 1 |
| 208.73.143.36 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.158 | 147.237.72.166 | Ukraine | aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 195.88.208.193 | 147.237.77.179 | Russian Federation | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 180.97.106.37 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 163.172.129.15 | 147.237.76.176 | United Kingdom | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.76.44 | China | e.refuah.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 109.60.153.178 | 147.237.77.243 | Russian Federation | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 94.102.48.195 | 147.237.77.74 | Netherlands | law.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.172.71.251 | 147.237.76.198 | Ukraine | e.yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.174.94.142 | 147.237.77.233 | Netherlands | atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 46.172.71.251 | 147.237.0.200 | Ukraine | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.174.94.142 | 147.237.77.61 | Netherlands | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 12.139.34.20 | 147.237.76.148 | United States | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 91.201.236.158 | 147.237.72.166 | Ukraine | aka.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 208.73.143.36 | 147.237.76.199 | United States | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.158 | 147.237.72.166 | Ukraine | aka.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 180.97.106.37 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |

09-08-2016-22:04:07 to 09-08-2016-23:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 196.137.42.170 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 53 |
| 46.117.56.42 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 30 |
| 82.166.238.235 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 27 |
| 87.68.59.232 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 18 |
| 23.94.253.34 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 18 |
| 87.68.59.232 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 18 |
| 23.94.253.34 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 18 |
| 23.94.253.34 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 23.94.253.34 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 23.94.253.34 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 23.94.253.34 | United States | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 23.94.253.34 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 23.94.253.34 | United States | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 109.64.95.53 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 14 |
| 176.13.234.63 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 14 |
| 41.254.0.106 | Libyan Arab Jamahiriya | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 37.26.148.237 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 12 |
| 87.68.59.232 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 12 |
| 46.19.85.171 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 82.166.238.235 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 11 |
| 91.134.110.227 | Bulgaria | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 82.166.238.235 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 91.134.110.227 | Bulgaria | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 91.134.110.227 | Bulgaria | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 82.166.238.235 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 80.246.133.70 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 11 |
| 91.134.110.227 | Bulgaria | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 46.19.85.171 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 91.134.110.227 | Bulgaria | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 91.134.110.227 | Bulgaria | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 91.134.110.227 | Bulgaria | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 91.134.110.227 | Bulgaria | 147.237.77.170 | maarachot.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 91.134.110.227 | Bulgaria | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 91.134.110.227 | Bulgaria | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 91.134.110.227 | Bulgaria | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 91.134.110.227 | Bulgaria | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 91.134.110.227 | Bulgaria | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 91.134.110.227 | Bulgaria | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 91.134.110.227 | Bulgaria | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 91.134.110.227 | Bulgaria | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 91.134.110.227 | Bulgaria | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 91.134.110.227 | Bulgaria | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 46.19.86.176 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 82.166.238.235 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 91.134.110.227 | Bulgaria | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 91.134.110.227 | Bulgaria | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 91.134.110.227 | Bulgaria | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 91.134.110.227 | Bulgaria | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 46.19.86.176 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 194.90.198.147 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |

09-08-2016-22:04:07 to 09-08-2016-23:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 89.138.170.137 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 184 |
| 176.13.248.0 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 154 |
| 176.13.5.191 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 80.246.138.160 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 87.70.107.211 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized HTTP Method | Block | 2 |
| 107.204.184.90 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 107.204.184.90 | Block | 2 |
| 46.116.98.156 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 107.204.184.90 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/kapatz/ | Block | 2 |
| 192.115.113.220 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 84.108.112.170 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 201.144.162.15 | Mexico | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/ishurim/main/ | Block | 2 |
| 80.246.133.70 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.69.127 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1394-he/refuah.aspx | Block | 1 |
| 79.182.45.153 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 207.46.13.76 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx | None | 1 |
| 46.116.32.126 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 80.246.133.221 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 68.180.228.240 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/robots.txt | Block | 1 |
| 87.70.107.211 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/ | Block | 1 |
| 79.183.87.175 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx | None | 1 |
| 73.150.254.9 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 2.53.45.49 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.183.96.178 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.102.9.2 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 157.55.39.133 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/templates/journalview/journalview.aspx | Block | 1 |
| 77.138.44.194 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx | Block | 1 |
| 198.20.87.98 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to 147.237.0.34/robots.txt | Block | 1 |
| 2.53.163.250 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc | Block | 1 |
| 94.230.84.67 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 80.178.218.253 | Israel | 147.237.77.74 | law.idf.il | Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/421-2258-he/patzar.aspx | Block | 1 |
| 66.249.64.45 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/templates/news/{"key":" | Block | 1 |
| 157.55.39.168 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/robots.txt | Block | 1 |
| 85.65.246.7 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx | Block | 1 |
| 77.138.141.148 | France | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/63578.doc | Block | 1 |
| 37.142.199.116 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/1325-he/refuah.aspx) | Block | 1 |
| 95.86.115.89 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized HTTP Method | Block | 1 |

09-08-2016-22:04:07 to 09-08-2016-23:04:07