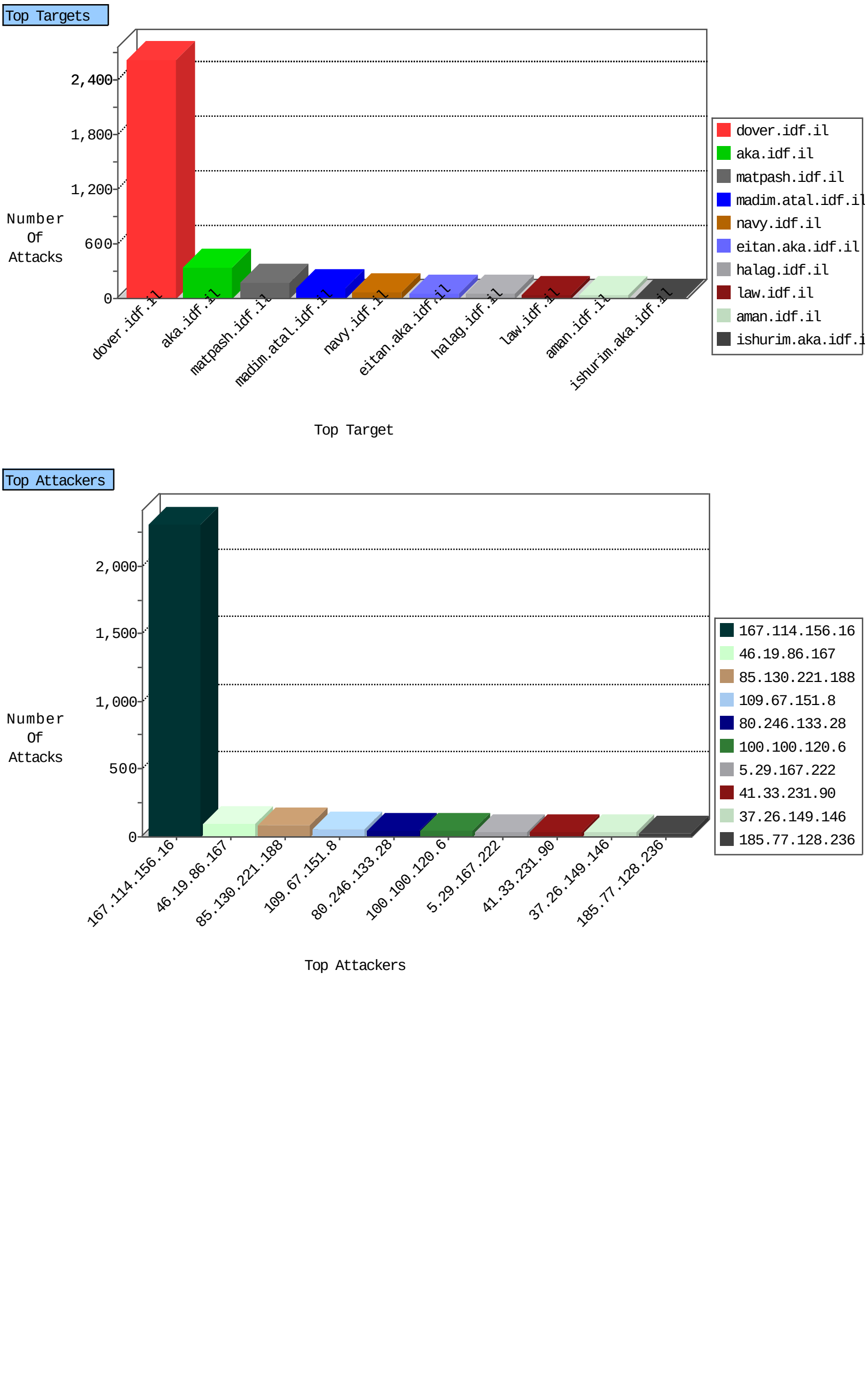
11-27-2015-21:04:06 to 11-27-2015-22:04:06

# IDF Under Attack Daily Report



11-27-2015-21:04:06 to 11-27-2015-22:04:06

## 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 | 3261 |
| 147.236.32.188 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |

11-27-2015-21:04:06 to 11-27-2015-22:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 52.1.90.117 | United States | 147.237.77.216 | dover.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 1 |

11-27-2015-21:04:06 to 11-27-2015-22:04:06

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 | 4 |
| 185.77.128.236 | 147.237.0.19 | | madim.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 185.77.128.236 | 147.237.76.148 | | gqcenter.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 185.77.128.236 | 147.237.8.28 | | e.mobile-ks.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 185.77.128.236 | 147.237.0.34 | | tikshuv.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 66.249.66.61 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 185.77.128.236 | 147.237.0.200 | | m4u.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.77.233 | | atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.77.178 | | e.matpash.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 167.114.156.16 | 147.237.77.216 | Canada | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.77.128.236 | 147.237.77.121 | | e.navy.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 94.102.48.195 | 147.237.72.14 | Netherlands | dover.idf.il(old) | ET SCAN NMAP -sS window 1024 | 1 |
| 185.77.128.236 | 147.237.76.198 | | e.yohalan.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 75.179.3.87 | 147.237.76.201 | United States | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.186.56.115 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 2.54.42.44 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 222.186.56.115 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.76.38 | | e.e.meitav.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 222.186.56.115 | 147.237.0.33 | China | idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.72.166 | | aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.77.235 | | sviva.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.77.205 | | prisha.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 182.50.130.133 | 147.237.77.216 | Singapore | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 1 |
| 185.77.128.236 | 147.237.77.170 | | maarachot.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 113.81.67.151 | 147.237.0.33 | China | idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 185.77.128.236 | 147.237.76.201 | | e.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 79.181.163.55 | 147.237.77.170 | Israel | maarachot.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 185.77.128.236 | 147.237.76.196 | | e.sviva.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 222.186.56.115 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.76.86 | | navy.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 222.186.56.115 | 147.237.76.30 | China | himush.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.76.31 | | nakchal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 222.186.56.115 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.72.156 | | aman.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 185.77.128.236 | 147.237.77.243 | | mobile.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |

11-27-2015-21:04:06 to 11-27-2015-22:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 109.67.151.8 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 51 |
| 80.246.133.28 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 43 |
| 100.100.120.6 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 42 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 5.29.167.222 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 85.130.221.188 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 26 |
| 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 |
| 85.130.221.188 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 18 |
| 85.130.221.188 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 18 |
| 46.19.86.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 100.100.19.209 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 15 |
| 100.100.57.52 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 14 |
| 46.19.85.17 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 14 |
| 100.100.28.106 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 100.100.101.41 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 100.100.0.45 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 37.26.149.146 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 11 |
| 37.26.149.146 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 11 |
| 85.130.221.188 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 5.29.124.105 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 85.130.221.188 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 85.130.221.188 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 46.19.85.184 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 100.100.66.25 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.46 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.50 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 100.100.24.78 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.52.129.120 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.86.129 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 79.178.102.107 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 2.52.129.120 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 66.249.73.185 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.66.134.56 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 37.26.149.146 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 37.26.149.146 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 92.253.82.23 | Jordan | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 46.19.86.17 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 100.100.0.64 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 5 |
| 188.120.148.144 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 213.57.185.155 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 46.19.86.129 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 188.120.148.200 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 2.54.165.39 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 185.120.126.48 | | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 4 |
| 66.249.66.61 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 46.19.86.26 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 31.154.91.120 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.125.242.203 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.67.19.196 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.181.98.181 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 78 |
| 176.13.22.57 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 8 |
| 2.54.159.36 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 67.222.12.77 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 91.92.198.5 | Bulgaria | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 91.92.198.5 | Block | 3 |
| 76.12.99.205 | United States | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 3 |
| 104.197.3.164 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 89.221.247.198 | Sweden | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 166.63.124.173 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 188.65.117.67 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 50.87.161.155 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 69.162.103.210 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 184.107.253.10 | Canada | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 91.92.198.5 | Bulgaria | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 50.87.161.155 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 50.87.161.155 | Block | 3 |
| 162.254.250.40 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 212.113.128.189 | United Kingdom | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 75.98.175.78 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 103.18.6.33 | Vietnam | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 91.209.72.79 | Russian Federation | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 50.22.252.18 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 198.1.94.242 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 46.32.230.183 | United Kingdom | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 162.144.248.125 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 209.204.64.36 | United States | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 3 |
| 128.192.22.58 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 69.162.103.210 | United States | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 69.162.103.210 | Block | 3 |
| 91.209.72.79 | Russian Federation | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 184.107.253.10 | Canada | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 184.107.253.10 | Block | 3 |
| 194.145.208.199 | United Kingdom | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 5.101.157.28 | Russian Federation | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 91.209.72.79 | Russian Federation | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 91.209.72.79 | Block | 3 |
| 188.65.117.67 | United Kingdom | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 109.66.62.75 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/ufi/reaction/ | Block | 3 |
| 91.109.15.16 | United Kingdom | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 3 |
| 216.120.237.104 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 72.52.219.191 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 46.19.86.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 3 |
| 70.38.37.185 | Canada | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 188.65.117.67 | United Kingdom | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 188.65.117.67 | Block | 3 |
| 194.145.208.199 | United Kingdom | 147.237.77.74 | law.idf.il | Distributed PHP Attempt | Block | 3 |
| 69.162.103.210 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 184.107.253.10 | Canada | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 83.172.144.20 | Netherlands | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 208.43.14.213 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 91.92.198.5 | Bulgaria | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 108.175.150.197 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |
| 194.145.200.135 | Netherlands | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 3 |
| 93.94.226.27 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 3 |
| 85.17.221.162 | Netherlands | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 3 |

11-27-2015-21:04:06 to 11-27-2015-22:04:06