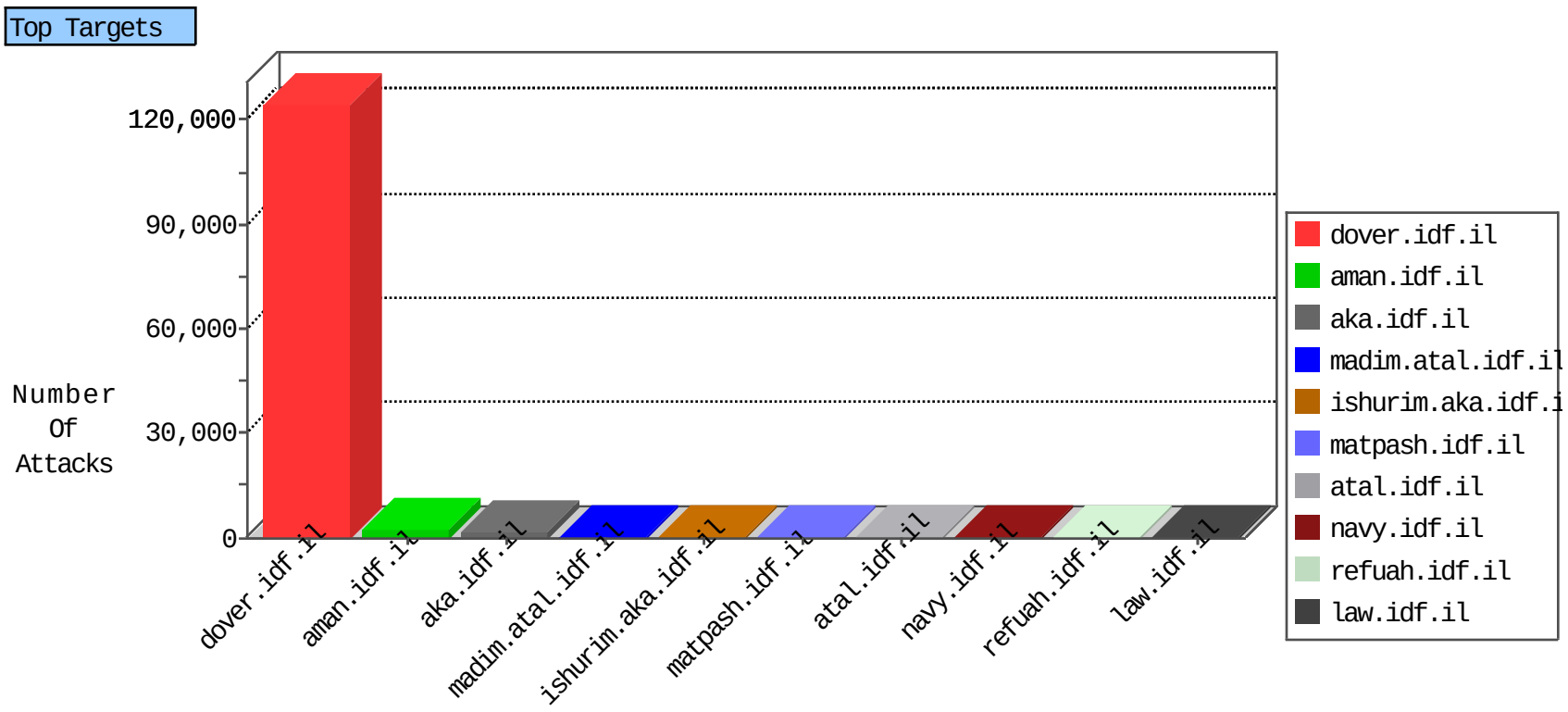
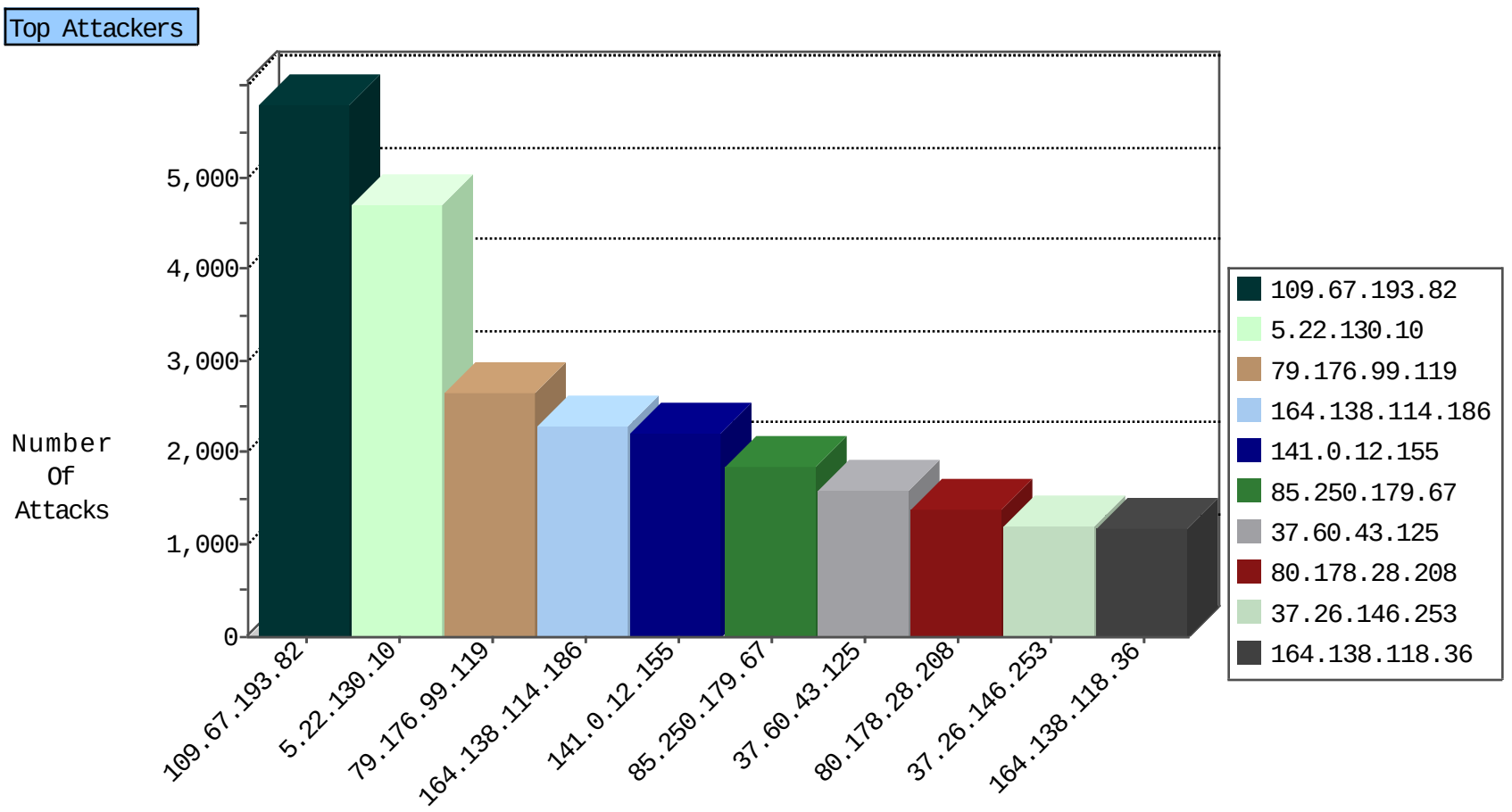
07-23-2015-00:00:06 to 07-24-2015-00:00:06

# IDF Under Attack Daily Report

Top Targets




Top Attackers



07-23-2015-00:00:06 to 07-24-2015-00:00:06

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|---|---|---|---|---|---|---|
| 212.235.60.161 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 3322 |
| 109.65.111.173 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 3223 |
| 5.29.169.50 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 3219 |
| 176.12.140.82 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 2631 |
| 141.0.12.155 | Norway | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 1925 |
| 66.249.83.158 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 1300 |
| 77.125.156.104 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 929 |
| 66.249.81.212 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 844 |
| 79.173.197.170 | Jordan | 147.237.77.216 | dover.idf.il | DOS-HTTP-fireflood | dest-reset | 773 |
| 109.64.157.21 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 672 |
| 84.108.119.124 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 624 |
| 37.142.64.152 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 588 |
| 66.249.93.168 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 538 |
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 506 |
| 82.80.165.174 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 474 |
| 85.65.121.128 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 463 |
| 81.218.241.25 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 426 |
| 85.65.121.128 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 463 |
| 81.218.241.25 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 426 |
| 31.210.186.218 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 408 |
| 109.66.57.238 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 379 |
| 46.121.81.86 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 348 |
| 79.180.135.139 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 329 |
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 320 |
| 109.186.128.144 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 310 |
| 81.218.37.2 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 294 |
| 213.8.71.26 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 291 |
| 77.125.139.60 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 276 |
| 5.29.242.230 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 276 |
| 87.69.8.26 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 254 |
| 109.67.127.65 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 215 |
| 46.121.24.56 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 196 |
| 86.108.93.249 | Jordan | 147.237.77.216 | dover.idf.il | DOS-HTTP-fireflood | dest-reset | 181 |
| 85.250.67.140 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 178 |
| 87.69.2.131 | Israel | 147.237.72.166 | aka.idf.il | TCP Scan (vertical) | drop | 168 |
| 207.232.36.181 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 167 |
| 79.176.5.139 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 166 |
| 77.126.10.176 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 164 |
| 46.120.21.70 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 163 |
| 95.86.72.161 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 160 |
| 84.108.67.228 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 146 |
| 47.70.44.186 | Germany | 147.237.77.216 | dover.idf.il | Anomaly-TLS-renegotiation-Cli | forward | 142 |
| 31.168.164.114 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 137 |
| 46.117.161.91 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 136 |
| 109.67.167.224 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 127 |
| 89.139.180.106 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 126 |
| 37.142.175.100 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Anomaly-TLS-renegotiation-Cli | dest-reset | 125 |
| 5.29.142.205 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 124 |
| 79.181.217.50 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 116 |
| 46.120.137.166 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 114 |
| 46.117.137.81 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 104 |
| 213.57.207.202 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 103 |

07-23-2015-00:00:06 to 07-24-2015-00:00:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.186.39.247 | Israel | 147.237.0.34 | tikshuv.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 19 |
| 194.114.146.227 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 18 |
| 5.29.46.228 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 7 |
| 217.55.173.153 | Egypt | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 7 |
| 46.19.85.106 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 5.22.130.244 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 196.206.91.153 | Morocco | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 178.77.130.73 | Jordan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 89.139.180.106 | Israel | 147.237.72.167 | ishurim.aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.19.85.177 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 85.65.111.60 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 5.29.213.9 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 79.183.163.101 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 93.172.132.230 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 43.224.85.161 | Japan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 103.242.20.225 | Bangladesh | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 77.125.12.232 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 109.64.184.16 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 89.138.241.113 | Israel | 147.237.77.74 | law.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 79.177.63.207 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 46.19.85.160 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 46.19.85.27 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 105.231.189.233 | Kenya | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 46.19.85.121 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 46.120.184.47 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 46.19.85.41 | Israel | 147.237.76.31 | nakchal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 79.183.3.198 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 93.172.50.56 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 81.218.171.206 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 5.102.254.20 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 46.19.85.249 | Israel | 147.237.77.176 | matpash.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 37.26.146.178 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 58.174.12.42 | Australia | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 89.139.174.127 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 157.166.167.129 | United States | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 79.183.166.240 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 132.70.57.47 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 46.19.85.176 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 46.19.85.88 | Israel | 147.237.76.31 | nakchal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 109.186.39.247 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 212.143.134.129 | Israel | 147.237.77.74 | law.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 46.19.85.127 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 62.210.251.69 | France | 147.237.77.74 | law.idf.il | 19791: HTTP: WordPress N-Media PHP File Upload | Block | 2 |
| 80.179.187.146 | Israel | 147.237.77.74 | law.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 2.52.137.224 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 62.210.251.69 | France | 147.237.77.74 | law.idf.il | 17031: HTTP: GetSimple CMS File Upload | Block | 2 |
| 93.172.42.107 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 212.179.4.21 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 46.19.85.136 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 84.109.90.140 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |

07-23-2015-00:00:06 to 07-24-2015-00:00:06

## Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|---|---|---|---|---|---|
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 91 |
| 2.54.0.4 | Israel | 147.237.77.216 | dover.idf.il | POLICY-OTHER TCP packet with urgent flag attempt | 58 |
| 91.121.85.219 | France | 147.237.76.86 | navy.idf.il | Tehila - Perl LWP with fake user agent | 27 |
| 2.54.168.11 | Israel | 147.237.76.30 | himush.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 9 |
| 212.199.57.205 | Israel | 147.237.77.233 | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 8 |
| 5.39.216.121 | Netherlands | 147.237.76.86 | navy.idf.il | SERVER-APACHE Apache SSI error page cross-site scripting | 7 |
| 37.237.192.37 | Iraq | 147.237.77.216 | dover.idf.il | SQL Injection - Select From | 5 |
| 66.249.64.244 | United States | 147.237.77.233 | atal.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 66.249.65.18 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 31.184.242.17 | Russian Federation | 147.237.77.216 | dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 4 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 4 |
| 5.39.216.121 | Netherlands | 147.237.77.170 | maarachot.idf.il | SERVER-APACHE Apache SSI error page cross-site scripting | 4 |
| 45.114.11.46 | | 147.237.77.74 | law.idf.il | ET SCAN Potential SSH Scan | 3 |
| 218.87.111.107 | China | 147.237.76.147 | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.47 | | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.46 | | 147.237.0.34 | tikshuv.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.49 | | 147.237.77.233 | atal.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.49 | | 147.237.72.166 | aka.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.49 | | 147.237.77.179 | e.mazi.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.47 | | 147.237.76.39 | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.46 | | 147.237.76.30 | himush.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.49 | | 147.237.77.121 | e.navy.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.47 | | 147.237.72.217 | e.idf.il | ET SCAN Potential SSH Scan | 2 |
| 221.203.3.117 | China | 147.237.76.176 | test.ncore.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.46 | | 147.237.76.202 | e.halag.idf.il | ET SCAN Potential SSH Scan | 2 |
| 5.39.216.121 | Netherlands | 147.237.0.15 | kosher-kravi.idf.il | SERVER-APACHE Apache SSI error page cross-site scripting | 2 |
| 45.114.11.46 | | 147.237.8.46 | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.67.120 | United States | 147.237.0.34 | tikshuv.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 37.237.192.37 | Iraq | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP encoded cross site scripting HTML Image tag attempt | 2 |
| 87.69.2.131 | Israel | 147.237.72.166 | aka.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 218.87.111.107 | China | 147.237.77.227 | e.hamaz.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.47 | | 147.237.76.201 | e.atal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 221.203.3.117 | China | 147.237.77.227 | e.hamaz.idf.il | ET SCAN Potential SSH Scan | 2 |
| 95.86.82.132 | Israel | 147.237.77.233 | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 218.87.111.107 | China | 147.237.77.212 | e.dover.idf.il | ET SCAN Potential SSH Scan | 2 |
| 212.106.76.87 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 218.87.111.107 | China | 147.237.0.200 | m4u.idf.il | ET SCAN Potential SSH Scan | 2 |
| 109.165.39.22 | Russian Federation | 147.237.0.16 | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 221.203.3.117 | China | 147.237.8.45 | e.eitan.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.46 | | 147.237.76.39 | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 5.39.216.121 | Netherlands | 147.237.77.226 | www.chamatz.aka.idf.il | SERVER-APACHE Apache SSI error page cross-site scripting | 2 |
| 45.114.11.47 | | 147.237.76.44 | e.refuah.idf.il | ET SCAN Potential SSH Scan | 2 |
| 218.87.111.107 | China | 147.237.0.34 | tikshuv.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.49 | | 147.237.8.45 | e.eitan.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.46 | | 147.237.76.31 | nakchal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 221.203.3.117 | China | 147.237.77.61 | e.cogat.idf.il | ET SCAN Potential SSH Scan | 2 |
| 5.39.216.121 | Netherlands | 147.237.77.19 | law-forum.idf.il | SERVER-APACHE Apache SSI error page cross-site scripting | 2 |
| 218.87.111.107 | China | 147.237.0.15 | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 89.248.174.100 | Netherlands | 147.237.8.24 | e.lifestyle.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 45.114.11.47 | | 147.237.76.30 | himush.idf.il | ET SCAN Potential SSH Scan | 2 |

07-23-2015-00:00:06 to 07-24-2015-00:00:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 109.67.193.82 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 5812 |
| 5.22.130.10 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 4727 |
| 79.176.99.119 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2667 |
| 164.138.114.186 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2310 |
| 141.0.12.155 | Norway | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2206 |
| 85.250.179.67 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1859 |
| 37.60.43.125 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1606 |
| 80.178.28.208 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1401 |
| 37.26.146.253 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1218 |
| 164.138.118.36 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1175 |
| 62.219.118.198 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1090 |
| 79.182.97.29 | Israel | 147.237.72.156 | aman.idf.il | SYN retransmit with different window scale | Bad TCP sequence | monitor | 1058 |
| 79.180.101.167 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1045 |
| 2.54.55.47 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1032 |
| 82.166.22.217 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1021 |
| 2.54.147.107 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1017 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1008 |
| 213.57.240.217 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 925 |
| 149.78.154.69 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 853 |
| 85.130.223.25 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 811 |
| 89.139.22.116 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 808 |
| 36.48.69.189 | China | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 783 |
| 213.57.63.198 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 669 |
| 84.229.33.188 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 656 |
| 2.54.178.38 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 648 |
| 95.86.126.245 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 647 |
| 109.65.158.49 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 629 |
| 5.29.208.55 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 623 |
| 149.88.40.184 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 618 |
| 84.108.39.1 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 608 |
| 85.250.174.144 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 586 |
| 31.44.140.42 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 577 |
| 89.138.61.151 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 574 |
| 80.123.167.25 | Austria | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 556 |
| 98.239.118.118 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 555 |
| 85.64.62.88 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 535 |
| 46.19.86.174 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 527 |
| 192.249.64.249 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 520 |
| 176.228.27.183 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 516 |
| 2.54.35.176 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 494 |
| 2.52.168.101 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 492 |
| 37.48.120.214 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 491 |
| 149.88.213.241 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 483 |
| 2.54.54.148 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 482 |
| 37.142.64.103 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 479 |
| 2.54.24.78 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 463 |
| 87.68.82.198 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 446 |
| 84.228.39.97 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 443 |
| 77.125.97.54 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 435 |
| 195.206.47.97 | Russian Federation | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 433 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 85.64.40.85 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 85.64.40.85 | Block | 142 |
| 66.249.64.173 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.173 | Block | 135 |
| 66.249.64.178 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.178 | Block | 134 |
| 66.249.64.168 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.168 | Block | 132 |
| 62.0.116.102 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 117 |
| 89.138.16.45 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 89.138.16.45 | Block | 85 |
| 46.19.85.71 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.85.71 | Block | 58 |
| 84.95.228.135 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 84.95.228.135 | Block | 51 |
| 91.121.85.219 | France | 147.237.76.86 | navy.idf.il | PHP Attempt | Block | 44 |
| 91.121.85.219 | France | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 91.121.85.219 | Block | 44 |
| 109.253.143.93 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 42 |
| 91.121.85.219 | France | 147.237.76.86 | navy.idf.il | Multiple Admin Blocking from 91.121.85.219 | Block | 22 |
| 176.13.12.81 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 176.13.12.81 | Block | 22 |
| 37.26.148.208 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 18 |
| 79.177.103.45 | Israel | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 79.177.103.45 | Block | 18 |
| 2.54.159.52 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 17 |
| 46.117.11.180 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 46.117.11.180 | Block | 16 |
| 79.173.197.170 | Jordan | 147.237.77.216 | dover.idf.il | Distributed Malformed URL | Block | 16 |
| 109.253.157.128 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword | Block | 12 |
| 148.163.2.234 |  | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 148.163.2.234 | Block | 12 |
| 81.218.241.25 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 81.218.241.25 | Block | 11 |
| 113.181.190.203 | Vietnam | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 113.181.190.203 | Block | 9 |
| 113.181.190.203 | Vietnam | 147.237.76.86 | navy.idf.il | PHP Attempt | Block | 9 |
| 176.12.140.242 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 8 |
| 84.108.15.130 | Israel | 147.237.72.156 | aman.idf.il | Suspicious Response Code | Block | 8 |
| 213.151.54.98 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 213.151.54.98 | Block | 8 |
| 82.81.6.25 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 82.81.6.25 | Block | 8 |
| 5.102.241.228 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp | Block | 7 |
| 2.50.182.224 | United Arab Emirates | 147.237.77.170 | maarachot.idf.il | Distributed PHP Attempt | Block | 6 |
| 31.154.91.253 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 6 |
| 2.54.184.206 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 6 |
| 46.118.155.4 | Ukraine | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1283-17155-en/ | Block | 5 |
| 188.165.15.121 | France | 147.237.76.30 | himush.idf.il | Unknown Parameter l in www.chimush.atal.idf.il/templates/sendtofriend/sendtofriend.aspx | None | 5 |
| 46.117.199.74 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/59452.swf | Block | 5 |
| 85.64.215.141 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 5 |
| 212.29.214.138 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/ | Block | 5 |
| 37.26.148.170 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword | Block | 5 |
| 95.86.65.159 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 5 |
| 212.199.224.24 | Israel | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 212.199.224.24 | Block | 5 |
| 192.116.94.209 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 5 |
| 109.67.167.159 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp | Block | 5 |
| 37.142.64.87 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 4 |
| 93.172.158.233 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 93.172.158.233 | Block | 4 |
| 132.66.222.230 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 4 |
| 109.67.2.152 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 109.67.2.152 | Block | 4 |
| 79.179.143.13 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 4 |
| 178.255.215.87 | France | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 178.255.215.87 | Block | 4 |
| 46.116.237.16 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 4 |
| 209.88.173.130 | Israel | 147.237.77.176 | matpash.idf.il | Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg | Block | 4 |
| 2.50.182.224 | United Arab Emirates | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 2.50.182.224 | Block | 4 |

07-23-2015-00:00:06 to 07-24-2015-00:00:06