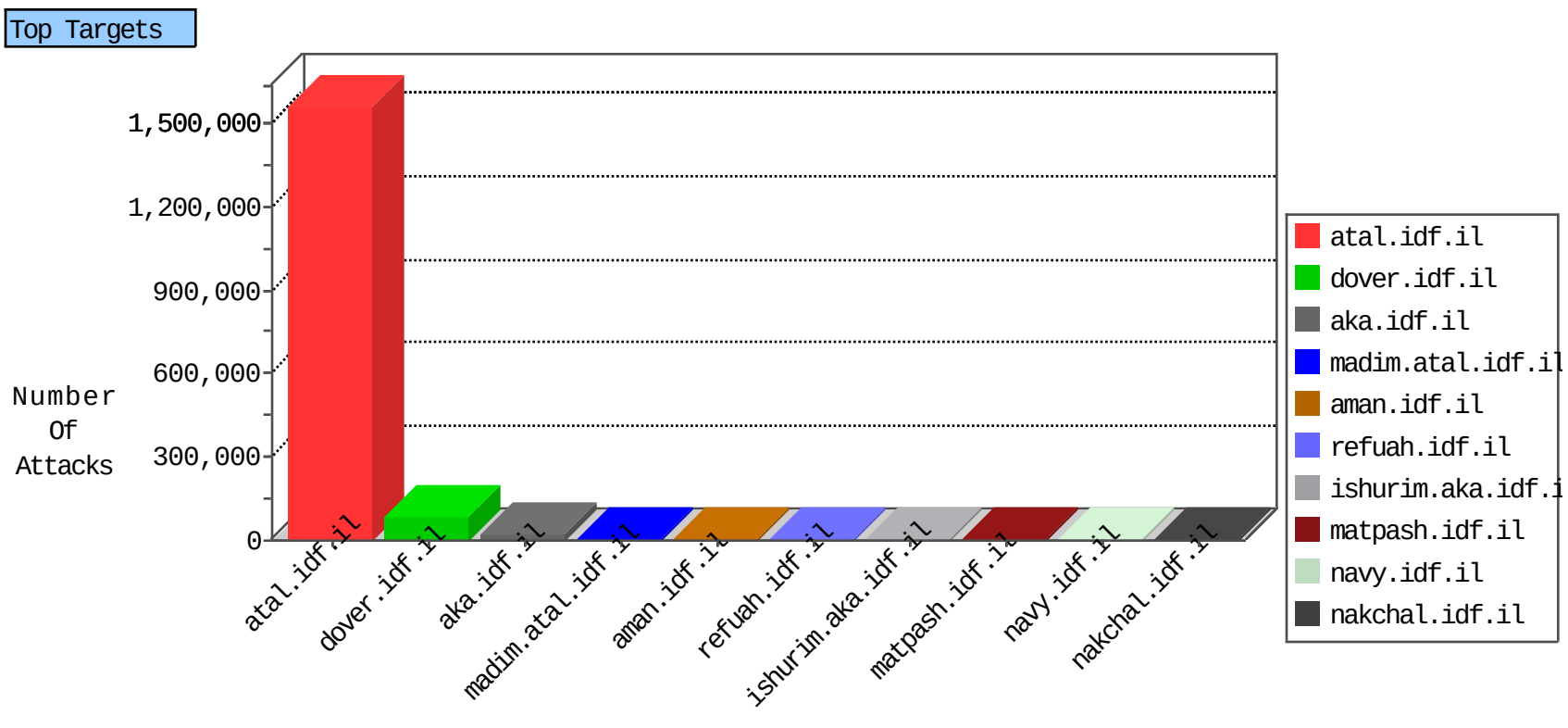
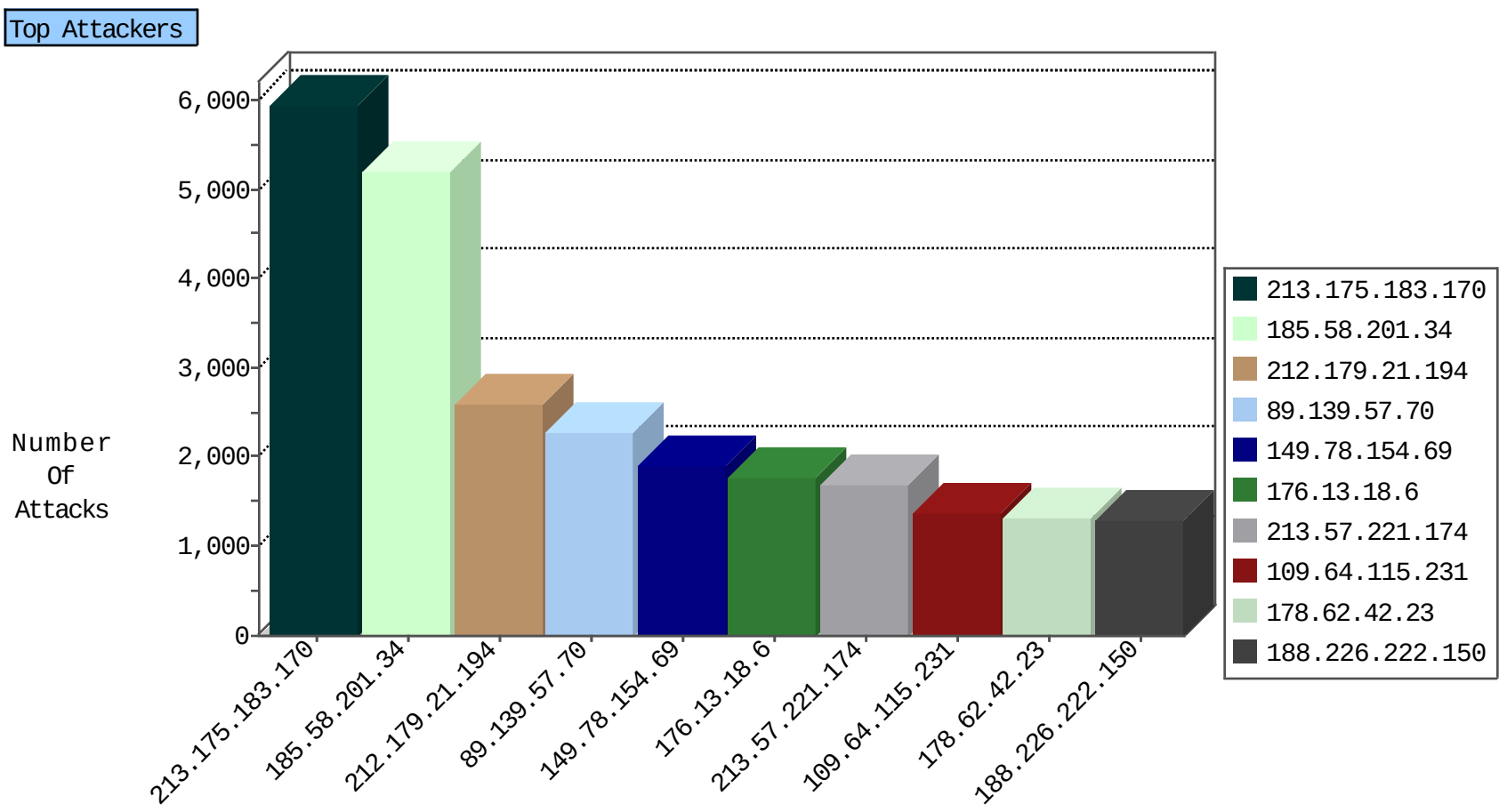
08-10-2015-00:00:09 to 08-11-2015-00:00:09

# IDF Under Attack Daily Report

Top Targets




Top Attackers



08-10-2015-00:00:09 to 08-11-2015-00:00:09

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|---|---|---|---|---|---|---|
| 98.251.102.247 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 269817 |
| 66.249.82.148 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | TCP handshake violation, first packet not syn | drop | 11317 |
| 64.233.173.188 | United States | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 10900 |
| 66.249.78.146 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 9058 |
| 200.48.200.103 | Peru | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 9018 |
| 17.142.152.85 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 5915 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4210 |
| 132.70.226.113 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 2756 |
| 77.127.95.156 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 1362 |
| 79.178.21.190 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 1112 |
| 46.117.157.61 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 731 |
| 109.65.134.161 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 631 |
| 109.64.176.100 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 621 |
| 92.22.1.173 | United Kingdom | 147.237.77.226 | www.chamatz.aka.idf.il | TCP handshake violation, first packet not syn | drop | 497 |
| 213.57.221.174 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 496 |
| 39.43.93.238 | Pakistan | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 423 |
| 84.109.127.76 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 395 |
| 85.250.132.209 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 374 |
| 178.135.80.196 | Lebanon | 147.237.72.166 | aka.idf.il | TCP Scan (vertical) | drop | 364 |
| 93.172.21.50 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 361 |
| 77.126.253.205 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 355 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 313 |
| 109.186.34.202 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 281 |
| 85.250.238.147 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 274 |
| 5.235.158.53 | Iran, Islamic Republic of | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 267 |
| 85.65.138.138 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 247 |
| 93.173.233.208 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 230 |
| 46.120.212.147 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 224 |
| 5.28.130.169 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 220 |
| 149.88.7.77 | United States | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 200 |
| 46.117.21.236 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 191 |
| 93.172.51.111 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 190 |
| 85.250.19.124 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 189 |
| 31.154.92.134 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 187 |
| 204.93.154.215 | United States | 147.237.72.166 | aka.idf.il | TCP Scan (vertical) | drop | 187 |
| 2.54.42.12 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 181 |
| 84.228.176.85 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 179 |
| 37.142.118.209 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 178 |
| 31.168.239.22 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 176 |
| 204.93.154.216 | United States | 147.237.77.233 | atal.idf.il | TCP Scan (vertical) | drop | 175 |
| 37.142.253.147 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 171 |
| 80.74.105.107 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 170 |
| 84.108.125.46 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 168 |
| 149.88.210.32 | United States | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 165 |
| 109.64.193.19 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 165 |
| 220.181.108.160 | China | 147.237.76.42 | refuah.idf.il | TCP handshake violation, first packet not syn | drop | 163 |
| 79.179.49.89 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 163 |
| 212.179.21.194 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 154 |
| 79.183.28.154 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 151 |
| 84.111.64.178 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 146 |

08-10-2015-00:00:09 to 08-11-2015-00:00:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 77.127.95.156 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 139 |
| 109.64.176.100 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 56 |
| 109.65.134.161 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 32 |
| 93.172.21.50 | Israel | 147.237.72.167 | ishurim.aka.idf.i | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 30 |
| 80.179.114.19 | Israel | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 23 |
| 194.114.146.227 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 21 |
| 91.228.248.251 | Israel | 147.237.76.42 | refuah.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 18 |
| 93.173.233.208 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 16 |
| 31.154.92.134 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 11 |
| 85.250.174.196 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 11 |
| 2.54.187.19 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 10 |
| 46.19.85.25 | Israel | 147.237.76.31 | nakchal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 46.19.85.32 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 79.102.141.240 | Sweden | 147.237.77.176 | matpash.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 31.168.114.74 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 46.19.85.32 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.117.253.158 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 5 |
| 46.19.85.204 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 37.26.146.200 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 37.26.147.134 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 46.19.85.236 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 109.186.96.61 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 2.54.155.105 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 192.115.29.222 | Israel | 147.237.77.176 | matpash.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 84.110.194.159 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 217.132.76.151 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 82.166.146.3 | Israel | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 109.67.51.138 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 80.246.137.163 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 93.172.137.137 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 212.143.43.173 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 109.64.189.24 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 46.120.25.42 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 3 |
| 79.183.37.131 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 46.121.199.25 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 84.108.224.120 | Israel | 147.237.0.34 | tikshuv.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 212.199.15.34 | Israel | 147.237.72.166 | aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 92.242.59.6 | Russian Federation | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 46.19.85.236 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 79.178.58.235 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 146.0.79.163 | Netherlands | 147.237.76.42 | refuah.idf.il | 12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability | Block | 2 |
| 84.109.235.74 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 192.114.2.36 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | 19691: HTTP: Microsoft IIS Web Server Information Disclosure Vulnerability | Block | 2 |
| 46.19.85.92 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 192.114.7.2 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 79.181.48.21 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 46.121.91.59 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 80.246.136.59 | Israel | 147.237.0.19 | madim.atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |
| 162.224.10.142 | United States | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 2 |

08-10-2015-00:00:09 to 08-11-2015-00:00:09

## 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 | 54 |
| 119.38.224.98 | China | 147.237.77.233 | atal.idf.il | GPL SCAN nmap TCP | 12 |
| 141.105.84.131 | Lebanon | 147.237.77.233 | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 9 |
| 62.221.75.244 | Moldova, Republic of | 147.237.72.166 | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 4 |
| 119.38.224.98 | China | 147.237.72.166 | aka.idf.il | GPL SCAN nmap TCP | 4 |
| 203.86.7.130 | China | 147.237.72.166 | aka.idf.il | GPL SCAN nmap TCP | 4 |
| 62.29.104.226 | Turkey | 147.237.77.216 | dover.idf.il | INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting | 3 |
| 83.233.208.235 | Sweden | 147.237.76.148 | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 2.94.80.138 | Russian Federation | 147.237.76.30 | himush.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.64.244 | United States | 147.237.77.233 | atal.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 167.114.156.198 | United States | 147.237.76.86 | navy.idf.il | SERVER-APACHE Apache mod_proxy reverse proxy information disclosure attempt | 2 |
| 184.154.1.124 | United States | 147.237.76.202 | e.halag.idf.il | ET SCAN Potential SSH Scan | 2 |
| 2.94.80.138 | Russian Federation | 147.237.77.179 | e.mazi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 213.204.103.36 | Lebanon | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 45.114.11.44 | | 147.237.77.227 | e.hamaz.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.67.7 | United States | 147.237.76.86 | navy.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.64.156 | United States | 147.237.77.233 | atal.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 2.94.80.138 | Russian Federation | 147.237.72.217 | e.idf.il | ET SCAN Potential SSH Scan | 2 |
| 83.233.208.235 | Sweden | 147.237.76.39 | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 94.102.48.193 | Netherlands | 147.237.76.147 | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 2.94.80.138 | Russian Federation | 147.237.77.235 | sviva.idf.il | ET SCAN Potential SSH Scan | 2 |
| 83.233.208.235 | Sweden | 147.237.76.200 | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 116.199.141.83 | China | 147.237.77.233 | atal.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 61.93.225.162 | Hong Kong | 147.237.76.44 | e.refuah.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 37.26.149.237 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 221.235.205.123 | China | 147.237.72.156 | aman.idf.il | ET SCAN NMAP -f -sS | 1 |
| 170.67.200.55 | United States | 147.237.77.233 | atal.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 45.114.11.46 | | 147.237.76.198 | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 186.227.79.12 | Brazil | 147.237.76.200 | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 199.230.97.117 | United States | 147.237.72.166 | aka.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 150.126.28.127 | United States | 147.237.72.166 | aka.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 45.114.11.44 | | 147.237.76.196 | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.7.99.61 | Brazil | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.52.174 | Netherlands | 147.237.0.17 | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.19.85.172 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 61.93.225.162 | Hong Kong | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 31.184.242.17 | Russian Federation | 147.237.77.216 | dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 218.65.30.107 | China | 147.237.77.74 | law.idf.il | ET SCAN Potential SSH Scan | 1 |
| 168.235.150.111 | | 147.237.76.196 | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 83.233.208.235 | Sweden | 147.237.76.42 | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 45.114.11.46 | | 147.237.72.167 | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 186.227.79.12 | Brazil | 147.237.8.45 | e.eitan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 113.240.250.157 | China | 147.237.8.46 | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 148.105.83.7 | United States | 147.237.72.166 | aka.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 66.231.164.142 | Puerto Rico | 147.237.0.19 | madim.atal.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 45.114.11.44 | | 147.237.76.148 | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 176.198.49.108 | Germany | 147.237.77.233 | atal.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.102.48.193 | Netherlands | 147.237.76.199 | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 45.114.11.47 | | 147.237.77.176 | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |

08-10-2015-00:00:09 to 08-11-2015-00:00:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2313 |
| 149.78.154.69 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1902 |
| 213.57.221.174 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1698 |
| 109.64.115.231 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1372 |
| 178.62.42.23 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1253 |
| 194.114.146.227 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1221 |
| 188.226.222.150 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1197 |
| 2.54.36.170 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 994 |
| 95.85.22.44 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 902 |
| 178.79.131.62 | United Kingdom | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 760 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 695 |
| 46.121.221.205 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 628 |
| 132.66.11.250 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 617 |
| 95.97.246.130 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 599 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 579 |
| 192.249.64.249 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 578 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 571 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 556 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 534 |
| 178.62.53.179 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 529 |
| 192.81.222.223 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 528 |
| 213.151.56.63 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 523 |
| 188.165.15.209 | France | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 522 |
| 54.72.0.55 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 518 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 494 |
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 458 |
| 37.60.41.200 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 445 |
| 185.58.201.34 |  | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 404 |
| 185.14.184.166 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 390 |
| 149.200.232.121 | Jordan | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 383 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 382 |
| 2.54.2.213 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 377 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 352 |
| 132.70.226.113 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 319 |
| 82.145.223.6 | Europe | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 294 |
| 45.56.73.98 |  | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 262 |
| 173.63.48.53 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 257 |
| 37.26.147.221 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 256 |
| 146.185.166.149 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 252 |
| 157.55.39.242 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 251 |
| 81.218.155.10 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 245 |
| 188.166.43.117 | Russian Federation | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 241 |
| 213.151.37.179 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 238 |
| 41.33.231.86 | Egypt | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 237 |
| 37.231.42.201 | Kuwait | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 222 |
| 212.103.99.24 | Russian Federation | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 222 |
| 207.46.13.82 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 206 |
| 68.180.230.29 | United States | 147.237.77.176 | matpash.idf.il | SAM rule | drop | drop | 204 |
| 37.228.105.109 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 201 |
| 104.131.181.129 |  | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 198 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 213.175.183.170 | Lebanon | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 4316 |
| 185.58.201.34 | | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 3240 |
| 89.139.57.70 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 89.139.57.70 | Block | 2270 |
| 176.13.18.6 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1764 |
| 185.58.201.34 | | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/templates/homepage/undefined | Block | 1437 |
| 213.175.183.170 | Lebanon | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/templates/homepage/undefined | Block | 1392 |
| 178.62.54.14 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 1194 |
| 80.246.136.28 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1065 |
| 46.19.86.126 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 717 |
| 109.228.19.161 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 588 |
| 46.101.178.105 | Russian Federation | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 576 |
| 46.19.86.113 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 46.19.86.113 | Block | 546 |
| 178.62.53.179 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 405 |
| 66.228.39.226 | United States | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 387 |
| 198.211.120.118 | United States | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 237 |
| 146.185.166.149 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 213 |
| 176.13.19.179 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 186 |
| 85.159.214.76 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 186 |
| 46.19.85.251 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unknown HTTP Request Method from 46.19.85.251 | Block | 168 |
| 176.13.19.3 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 168 |
| 45.56.73.98 | | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 135 |
| 162.216.17.96 | United States | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 129 |
| 185.58.201.34 | | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/homepage/undefined | Block | 120 |
| 176.13.10.160 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 117 |
| 198.199.65.243 | United States | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 117 |
| 207.106.190.2 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 207.106.190.2 | Block | 114 |
| 192.81.222.223 | United States | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 105 |
| 95.85.22.44 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 105 |
| 188.226.222.150 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 99 |
| 213.175.183.170 | Lebanon | 147.237.77.216 | dover.idf.il | Too Many of the Same Response Code (404) in Session from 213.175.183.170 | Block | 78 |
| 178.62.42.23 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 75 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.173 | Block | 63 |
| 178.79.131.62 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 57 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.166 | Block | 57 |
| 176.13.13.17 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 176.13.13.17 | Block | 51 |
| 212.179.21.194 | Israel | 147.237.76.200 | eitan.aka.idf.il | Distributed Unauthorized URL Access on www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx | Block | 45 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 42 |
| 213.251.182.103 | France | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src | Block | 42 |
| 81.218.241.26 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 81.218.241.26 | Block | 42 |
| 83.101.93.18 | Belgium | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 83.101.93.18 | Block | 39 |
| 85.159.211.56 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 36 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp | Block | 36 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 68.180.228.112 | Block | 36 |
| 62.128.48.84 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 62.128.48.84 | Block | 33 |
| 188.165.15.209 | France | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 188.165.15.209 | Block | 33 |
| 212.71.237.37 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 30 |
| 46.19.85.3 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 27 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp | Block | 24 |
| 46.116.140.218 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 24 |
| 2.54.150.202 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 24 |