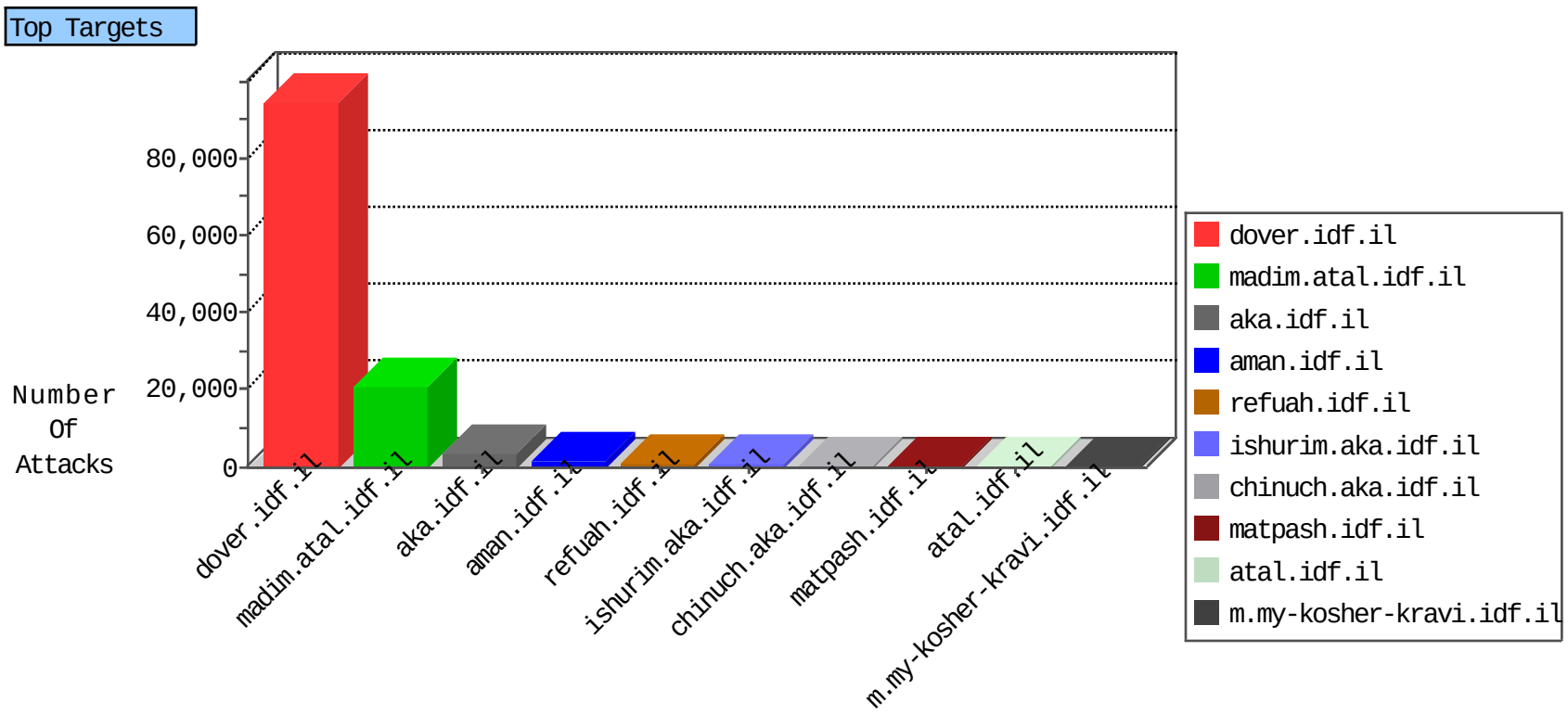
08-18-2015-00:00:00 to 08-19-2015-00:00:00

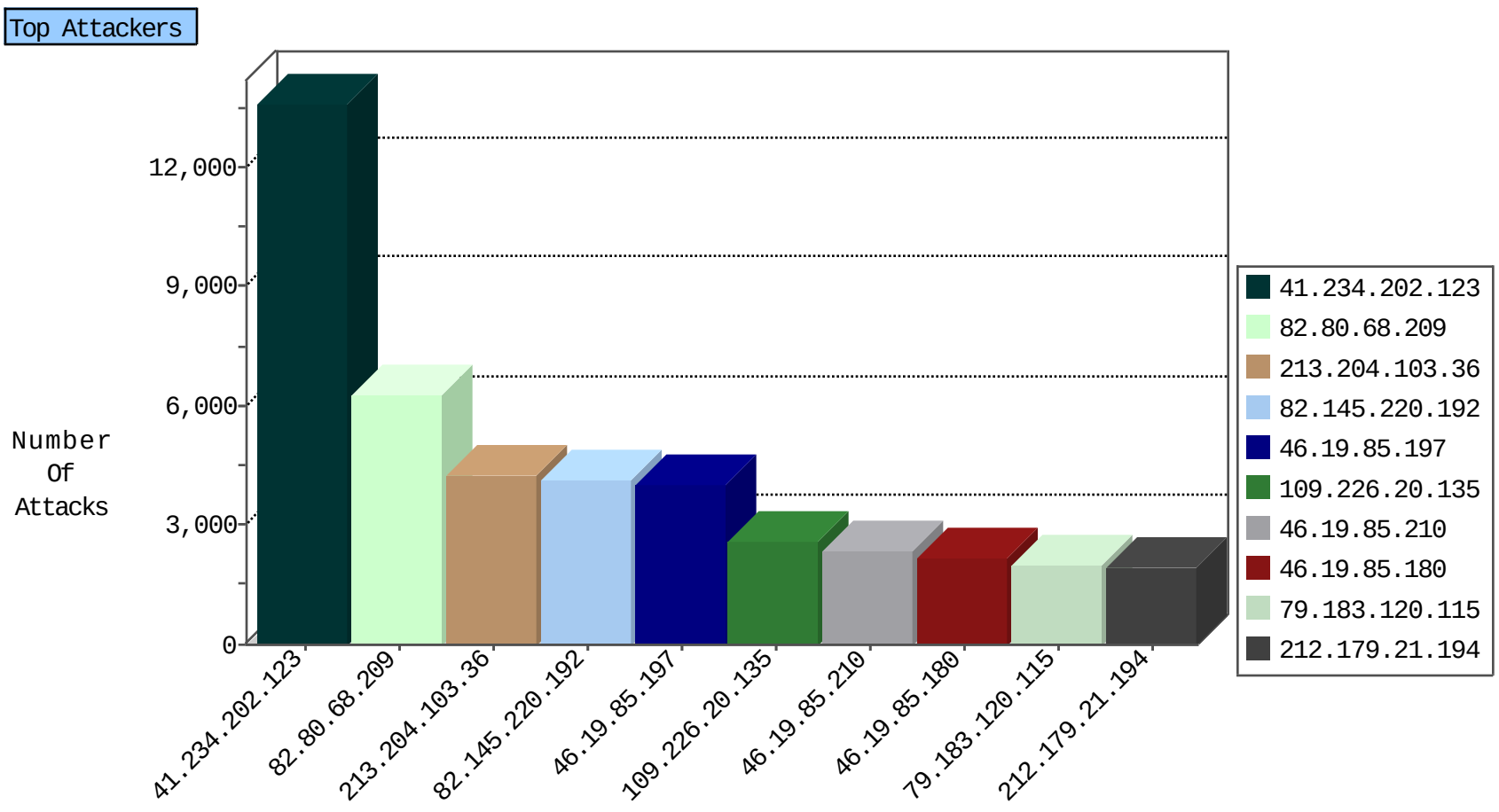
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

08-18-2015-00:00:00 to 08-19-2015-00:00:00

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|---|---|---|---|---|---|---|
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 7187 |
| 24.107.23.207 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2853 |
| 192.249.64.249 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 2840 |
| 212.143.121.19 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 2560 |
| 46.116.223.112 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 1236 |
| 109.160.243.10 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 745 |
| 93.173.180.116 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 635 |
| 104.172.224.157 | | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | forward | 547 |
| 81.218.241.26 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 509 |
| 109.65.185.14 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 418 |
| 79.179.60.37 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 326 |
| 79.179.138.32 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 324 |
| 37.142.143.239 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 315 |
| 89.138.43.67 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 292 |
| 77.125.72.193 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 289 |
| 212.25.84.200 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 288 |
| 149.88.107.165 | United States | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 285 |
| 213.57.160.27 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 268 |
| 149.78.253.225 | United States | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 248 |
| 109.64.59.210 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 214 |
| 213.57.173.7 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 203 |
| 85.250.11.35 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 202 |
| 109.186.190.161 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 191 |
| 85.250.136.172 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 190 |
| 46.120.34.43 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 181 |
| 87.69.231.160 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 179 |
| 79.180.206.238 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 171 |
| 81.218.51.66 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 168 |
| 84.108.82.117 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 165 |
| 84.94.49.44 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 164 |
| 66.249.64.151 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | TCP handshake violation, first packet not syn | drop | 163 |
| 46.117.73.249 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 158 |
| 77.125.247.70 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 150 |
| 109.160.136.240 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 149 |
| 94.230.86.205 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 149 |
| 176.12.148.242 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 146 |
| 164.138.115.214 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 146 |
| 46.121.243.123 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 144 |
| 2.54.134.92 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 132 |
| 93.173.185.254 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 131 |
| 109.65.109.50 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 129 |
| 93.173.245.68 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 125 |
| 81.218.241.26 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 122 |
| 46.120.104.109 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 121 |
| 89.139.36.241 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 114 |
| 109.64.184.70 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 113 |
| 176.12.149.225 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 110 |
| 5.29.117.206 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 110 |
| 84.109.200.204 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 104 |
| 79.177.199.102 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 96 |

08-18-2015-00:00:00 to 08-19-2015-00:00:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 197.38.62.254 | Egypt | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 71 |
| 91.228.248.251 | Israel | 147.237.76.42 | refuah.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 18 |
| 212.143.66.6 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 13 |
| 194.114.146.227 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 12 |
| 85.65.52.53 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 10 |
| 109.65.11.83 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 9 |
| 81.218.48.37 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 8 |
| 84.108.244.94 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 8 |
| 82.102.170.163 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 7 |
| 78.108.161.226 | Lebanon | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 7 |
| 79.182.189.153 | Israel | 147.237.72.167 | ishurim.aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 7 |
| 176.13.15.55 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 37.142.64.120 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 37.142.202.172 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 151.80.155.141 | Italy | 147.237.77.74 | law.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 5 |
| 79.177.107.186 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 151.80.155.141 | Italy | 147.237.77.235 | sviva.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 5 |
| 83.244.49.119 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 87.117.204.159 | United Kingdom | 147.237.77.19 | law-forum.idf.il | 16907: HTTP: FHScan Core Scanner Usage | Block | 4 |
| 80.178.187.210 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 79.177.25.130 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 86.168.121.211 | United Kingdom | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 109.64.184.70 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 81.218.48.37 | Israel | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 185.22.224.96 | United Kingdom | 147.237.77.74 | law.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 212.150.203.146 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 91.54.17.6 | Germany | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 79.180.60.138 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 85.158.137.195 | Europe | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 77.242.202.244 | France | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 213.8.41.250 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 46.19.85.45 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 213.8.46.230 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 109.65.106.122 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 197.0.103.210 | Tunisia | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 91.121.196.94 | France | 147.237.77.74 | law.idf.il | 19863: HTTP: WordPress Revslider/Showbiz PHP File Upload | Block | 3 |
| 46.117.40.12 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 84.228.111.23 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 84.108.122.94 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 2.52.140.44 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 82.81.250.69 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 109.188.125.23 | Russian Federation | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 87.117.204.159 | United Kingdom | 147.237.77.205 | prisha.idf.il | 16907: HTTP: FHScan Core Scanner Usage | Block | 2 |
| 46.19.85.112 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 46.121.73.60 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 46.19.85.31 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 87.117.204.159 | United Kingdom | 147.237.76.86 | navy.idf.il | 16907: HTTP: FHScan Core Scanner Usage | Block | 2 |
| 111.237.174.126 | Japan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 95.172.74.63 | United Kingdom | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 2 |
| 46.19.85.225 | Israel | 147.237.77.74 | law.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |

08-18-2015-00:00:00 to 08-19-2015-00:00:00

## 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 | 55 |
| 149.200.220.132 | Jordan | 147.237.77.216 | dover.idf.il | POLICY-OTHER TCP packet with urgent flag attempt | 43 |
| 41.234.202.123 | Egypt | 147.237.77.216 | dover.idf.il | WEB-FRONTPAGE /_vti_bin/ access | 9 |
| 24.225.8.5 | United States | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 9 |
| 202.78.217.116 | Japan | 147.237.72.166 | aka.idf.il | SERVER-WEBAPP backup access | 8 |
| 182.50.130.198 | Singapore | 147.237.77.74 | law.idf.il | Tehila - Perl LWP with fake user agent | 8 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 5 |
| 45.114.11.49 | | 147.237.8.45 | e.eitan.idf.il | ET SCAN Potential SSH Scan | 4 |
| 45.114.11.49 | | 147.237.76.30 | himush.idf.il | ET SCAN Potential SSH Scan | 3 |
| 41.234.202.123 | Egypt | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP backup access | 3 |
| 45.114.11.49 | | 147.237.76.176 | test.ncore.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.49 | | 147.237.0.35 | akaws.idf.il | ET SCAN Potential SSH Scan | 3 |
| 41.234.202.123 | Egypt | 147.237.77.216 | dover.idf.il | Tehila defacement attempt (-Hacked By- sent to Web Server) | 3 |
| 45.114.11.44 | | 147.237.72.156 | aman.idf.il | ET SCAN Potential SSH Scan | 3 |
| 45.114.11.49 | | 147.237.76.42 | refuah.idf.il | ET SCAN Potential SSH Scan | 2 |
| 80.82.64.127 | Netherlands | 147.237.76.34 | yohalan.idf.il | ET SCAN Potential SSH Scan | 2 |
| 37.161.249.160 | France | 147.237.72.166 | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 89.139.41.171 | Israel | 147.237.76.30 | himush.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 45.114.11.49 | | 147.237.77.178 | e.matpash.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.49 | | 147.237.0.19 | madim.atal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 201.76.127.72 | Brazil | 147.237.0.15 | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.49 | | 147.237.77.74 | law.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.44 | | 147.237.76.38 | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 31.44.138.118 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 41.234.202.123 | Egypt | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 45.114.11.49 | | 147.237.76.200 | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 71.34.89.145 | United States | 147.237.0.15 | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.49 | | 147.237.76.44 | e.refuah.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.49 | | 147.237.77.212 | e.dover.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.48 | | 147.237.0.16 | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.78.104 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 45.114.11.49 | | 147.237.0.33 | idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.44 | | 147.237.76.196 | e.sviva.idf.il | ET SCAN Potential SSH Scan | 2 |
| 71.34.89.145 | United States | 147.237.77.176 | matpash.idf.il | ET SCAN Potential SSH Scan | 2 |
| 109.67.164.253 | Israel | 147.237.77.216 | dover.idf.il | GPL SCAN nmap TCP | 2 |
| 45.114.11.49 | | 147.237.76.34 | yohalan.idf.il | ET SCAN Potential SSH Scan | 2 |
| 37.142.64.100 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 45.114.11.49 | | 147.237.0.16 | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 189.202.241.84 | Mexico | 147.237.76.34 | yohalan.idf.il | ET SCAN NMAP -sS window 4096 | 2 |
| 199.203.59.121 | Israel | 147.237.76.34 | yohalan.idf.il | ET SCAN Potential SSH Scan | 2 |
| 41.234.202.123 | Egypt | 147.237.77.216 | dover.idf.il | LOCAL_RULES - Request with the string install.php in it | 2 |
| 45.114.11.49 | | 147.237.72.166 | aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 80.82.64.127 | Netherlands | 147.237.77.170 | maarachot.idf.il | ET SCAN Potential SSH Scan | 2 |
| 61.188.189.4 | China | 147.237.76.31 | nakchal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 45.114.11.44 | | 147.237.76.31 | nakchal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 213.57.180.231 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 45.114.11.49 | | 147.237.76.199 | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 193.106.54.32 | Israel | 147.237.77.233 | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 45.114.11.49 | | 147.237.8.27 | e.madim.atal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 24.88.125.53 | United States | 147.237.77.216 | dover.idf.il | ET SCAN Potential SSH Scan | 2 |

08-18-2015-00:00:00 to 08-19-2015-00:00:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 82.80.68.209 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 6275 |
| 213.204.103.36 | Lebanon | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4258 |
| 82.145.220.192 | Europe | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 4105 |
| 109.226.20.135 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 2613 |
| 41.234.202.123 | Egypt | 147.237.77.216 | dover.idf.i | Failed to handle connection data | Block HTTP Non Compliant | monitor | 2305 |
| 41.234.202.123 | Egypt | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 2031 |
| 79.183.120.115 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 1971 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 1721 |
| 149.78.154.69 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 1678 |
| 70.39.185.182 | Satellite Provide | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 1075 |
| 180.253.243.202 | Indonesia | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 963 |
| 208.109.97.62 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 877 |
| 82.145.222.190 | Europe | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 813 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 791 |
| 208.109.97.62 | United States | 147.237.77.216 | dover.idf.i | SAM rule | drop | drop | 777 |
| 162.128.69.140 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 581 |
| 192.249.64.249 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 572 |
| 54.72.0.55 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 544 |
| 212.179.180.30 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 538 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 533 |
| 85.16.133.93 | Germany | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 527 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 523 |
| 212.76.96.156 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 477 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 471 |
| 79.179.102.141 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 438 |
| 66.249.78.173 | United States | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 434 |
| 81.17.16.253 | Switzerland | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 399 |
| 66.249.78.166 | United States | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 392 |
| 84.94.34.42 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 361 |
| 41.33.231.86 | Egypt | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 343 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 339 |
| 2.54.182.41 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 321 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 310 |
| 213.204.103.26 | Lebanon | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 308 |
| 190.177.249.76 | Argentina | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 298 |
| 197.149.88.190 | Nigeria | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 297 |
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 297 |
| 124.124.244.211 | India | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 294 |
| 207.46.13.70 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 266 |
| 213.151.37.24 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 264 |
| 207.46.13.119 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 250 |
| 207.46.13.126 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 247 |
| 54.187.55.213 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 246 |
| 212.243.165.114 | Switzerland | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 241 |
| 66.87.127.59 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 239 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 237 |
| 108.4.0.51 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 208 |
| 66.87.81.187 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 206 |
| 212.25.84.200 | Israel | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 198 |
| 66.249.93.160 | United States | 147.237.77.216 | dover.idf.i | First packet isn't SYN | drop | drop | 197 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 41.234.202.123 | Egypt | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 41.234.202.123 | Block | 9131 |
| 46.19.85.197 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.85.197 | Block | 4022 |
| 46.19.85.210 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 2318 |
| 46.19.85.180 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 2184 |
| 46.19.86.151 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 1667 |
| 149.88.217.7 | United States | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 1656 |
| 2.54.40.217 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 1533 |
| 2.54.22.99 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 971 |
| 176.13.6.235 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 176.13.6.235 | Block | 885 |
| 46.19.86.254 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.86.254 | Block | 871 |
| 2.54.167.226 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 2.54.167.226 | Block | 714 |
| 46.19.85.4 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 548 |
| 46.19.86.254 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 444 |
| 2.54.4.45 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 427 |
| 176.12.149.92 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 388 |
| 2.54.13.240 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 372 |
| 185.32.179.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 185.32.179.110 | Block | 336 |
| 176.12.140.91 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 278 |
| 193.201.224.126 | Ukraine | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 193.201.224.126 | Block | 264 |
| 2.54.155.219 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 252 |
| 46.19.86.82 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 236 |
| 66.249.78.128 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 236 |
| 2.54.168.179 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 232 |
| 46.19.86.109 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 142 |
| 2.54.171.62 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 136 |
| 176.12.149.243 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 128 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 64 |
| 66.249.78.166 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.166 | Block | 60 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 68.180.228.112 | Block | 52 |
| 202.78.217.116 | Japan | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 202.78.217.116 | Block | 48 |
| 46.19.85.153 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 48 |
| 46.19.86.118 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation Email in mobile.idf.il/sachar/createaccount | Block | 44 |
| 176.12.151.10 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 36 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.173 | Block | 36 |
| 176.13.13.146 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 36 |
| 212.179.21.194 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 36 |
| 46.19.86.128 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 32 |
| 41.234.202.123 | Egypt | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 28 |
| 202.78.217.116 | Japan | 147.237.72.166 | aka.idf.il | Multiple signatures from 202.78.217.116 | Block | 28 |
| 193.106.206.10 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 28 |
| 176.13.8.75 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 24 |
| 185.32.179.83 | Israel | 147.237.76.39 | mobile.meitav.idf.il | Cookie Tampering on cookie .ASPNETAUTH: Expected 0102CE810D90C6A7D208FECEF94E5BC9A7D208000932003000380036003400350039003700380000012F00FF, Observed 0102E282414E92A7D208FEE2FA821995A7D208000932003000380036003400350039003700380000012F00FF | None | 24 |
| 176.12.151.228 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 176.12.151.228 | Block | 24 |
| 176.12.151.10 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 24 |
| 79.176.16.8 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 20 |
| 89.138.201.32 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 20 |
| 80.246.136.132 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 20 |
| 66.249.78.52 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 20 |
| 182.50.130.198 | Singapore | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 182.50.130.198 | Block | 20 |
| 109.64.193.35 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/gius | Block | 20 |