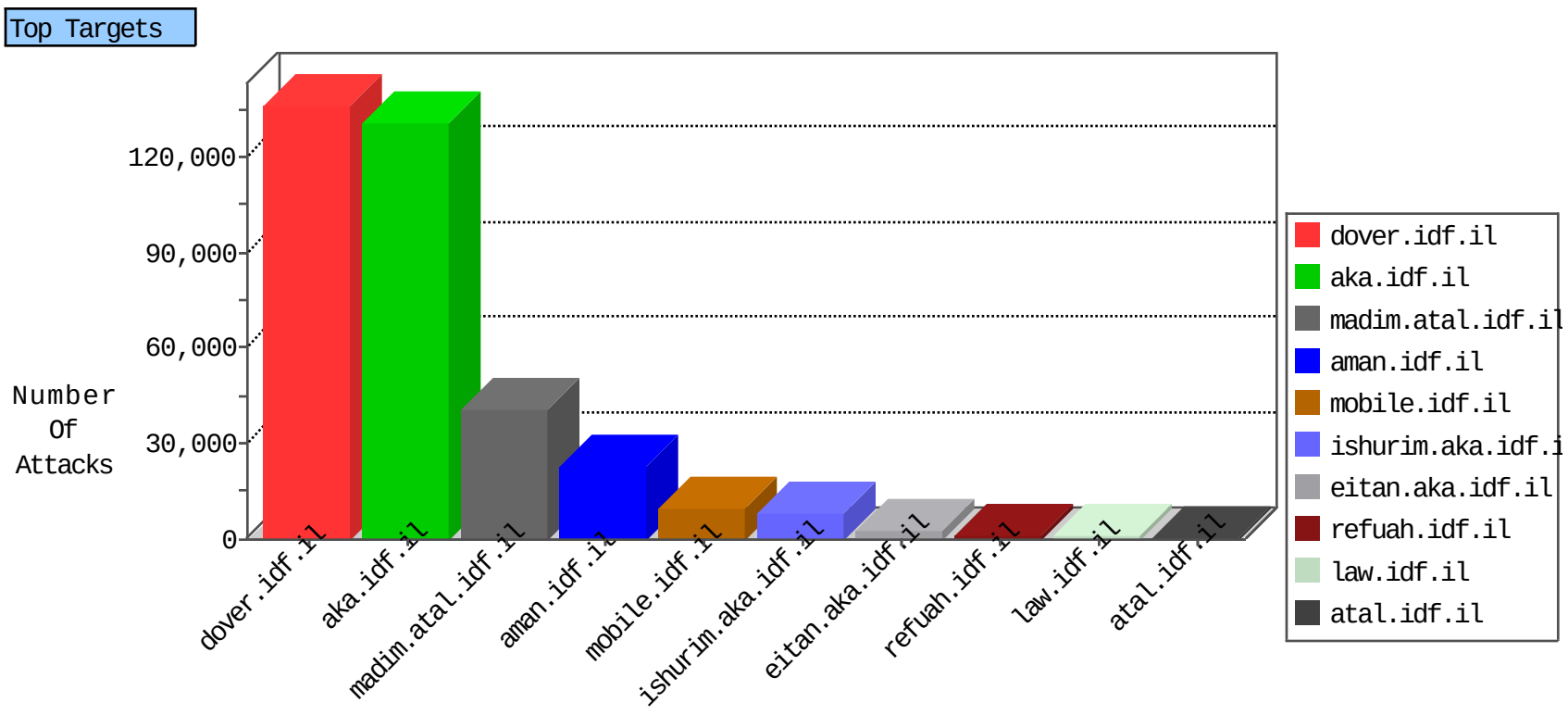
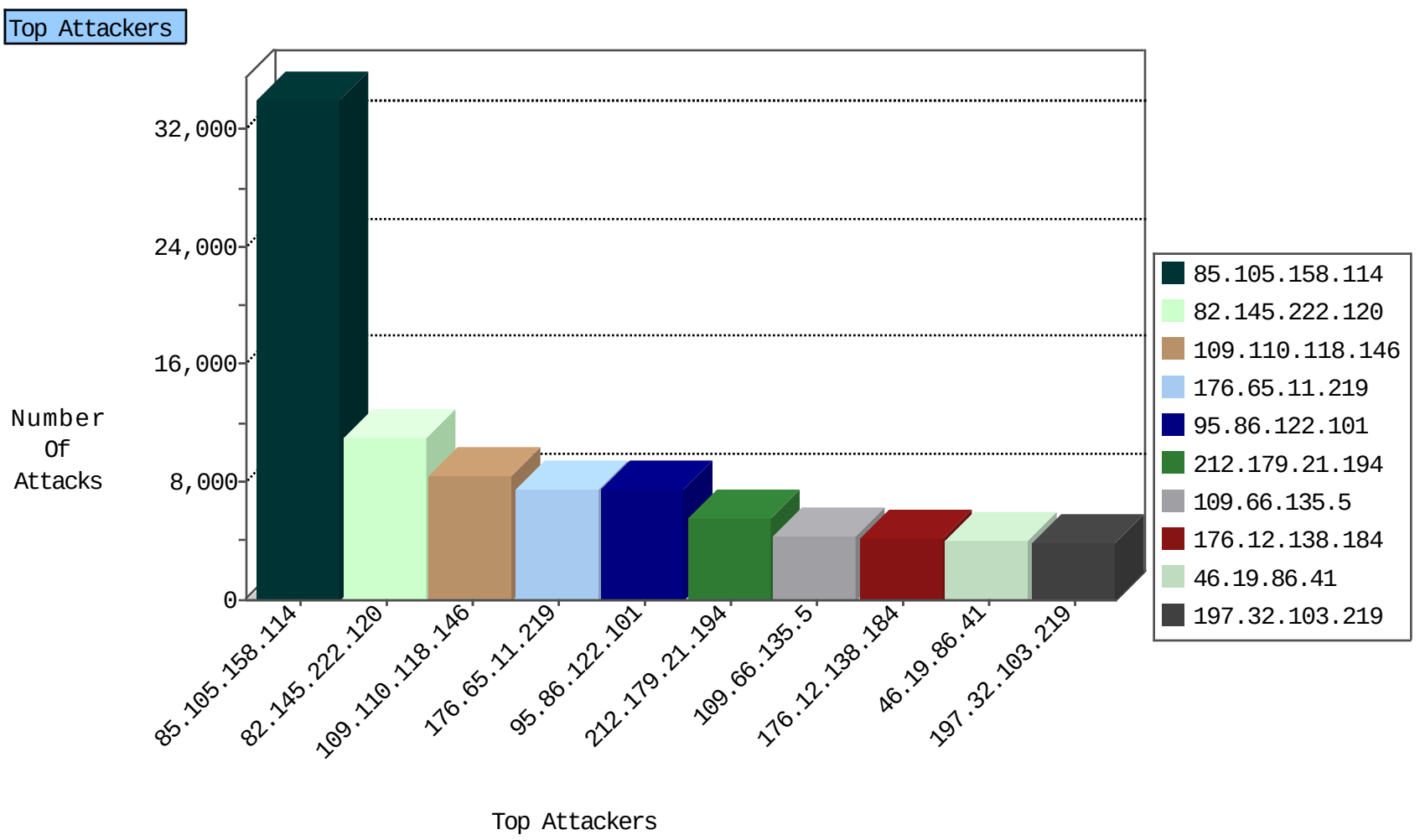
09-01-2015-00:00:02 to 09-02-2015-00:00:02

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-01-2015-00:00:02 to 09-02-2015-00:00:02

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|---|---|---|---|---|---|---|
| 66.249.64.173 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 6957 |
| 66.249.93.164 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3274 |
| 93.173.248.176 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3052 |
| 65.23.61.254 | United States | 147.237.77.176 | matpash.idf.il | TCP handshake violation, first packet not syn | drop | 2978 |
| 66.249.78.254 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 2974 |
| 66.249.78.160 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 2701 |
| 85.105.158.114 | Turkey | 147.237.77.216 | dover.idf.il | DOS-HTTP-fireflood | dest-reset | 1339 |
| 141.0.12.179 | Norway | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 587 |
| 66.249.69.96 | Israel | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 262 |
| 81.218.241.26 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 253 |
| 81.218.241.26 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 156 |
| 192.118.30.102 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 146 |
| 116.14.122.176 | Singapore | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 115 |
| 80.246.137.127 | Israel | 147.237.0.19 | madim.atal.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 112 |
| 81.218.241.26 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | forward | 71 |
| 87.69.160.199 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 48 |
| 77.126.151.170 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 39 |
| 46.19.86.91 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 38 |
| 80.246.136.55 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 35 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 30 |
| 46.19.85.184 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 27 |
| 46.19.85.184 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 27 |
| 85.65.197.159 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 25 |
| 46.19.85.0 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 25 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 24 |
| 46.19.86.233 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 24 |
| 212.143.3.44 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 23 |
| 37.142.111.20 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 23 |
| 66.249.78.153 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 23 |
| 71.77.132.192 | United States | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 20 |
| 66.249.78.254 | Israel | 147.237.72.166 | aka.idf.il | SYN Flood unverified cookie | drop | 19 |
| 46.19.86.176 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 18 |
| 107.150.52.82 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | TCP Scan (vertical) | drop | 18 |
| 176.13.23.140 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 18 |
| 212.199.107.106 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 18 |
| 212.76.124.6 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 18 |
| 84.228.4.150 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 16 |
| 212.143.3.44 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 15 |
| 176.12.151.189 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 15 |
| 95.86.127.231 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 15 |
| 176.12.151.189 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 15 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 13 |
| 212.143.122.2 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 13 |
| 176.12.143.64 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 12 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 12 |
| 84.109.16.50 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 12 |
| 176.13.15.164 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 12 |
| 109.67.132.195 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 12 |
| 194.114.146.227 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 12 |
| 37.26.146.226 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 11 |

09-01-2015-00:00:02 to 09-02-2015-00:00:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.106.226.2 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 20 |
| 138.134.102.15 | Israel | 147.237.76.31 | nakchal.idf.i | C1000004: HTTP: options method (Microsoft) | Block | 18 |
| 81.109.24.132 | United Kingdom | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 18 |
| 46.19.85.76 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 17 |
| 84.109.87.102 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 15 |
| 176.106.227.80 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 13 |
| 41.238.232.194 | Egypt | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 12 |
| 46.120.237.71 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 11 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | C091: HTTP: Access to - admin.asp | Block | 11 |
| 109.66.105.179 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 10 |
| 138.134.102.16 | Israel | 147.237.76.31 | nakchal.idf.i | C1000004: HTTP: options method (Microsoft) | Block | 8 |
| 87.68.16.10 | Israel | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 8 |
| 176.106.226.142 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 7 |
| 176.106.227.4 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 7 |
| 79.182.186.230 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 7 |
| 176.106.226.189 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 7 |
| 5.29.210.158 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 7 |
| 80.178.219.37 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 213.57.38.219 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 37.142.243.64 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 176.106.227.66 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 82.80.84.168 | Israel | 147.237.77.74 | law.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 5 |
| 46.120.132.144 | Israel | 147.237.76.31 | nakchal.idf.i | C1000004: HTTP: options method (Microsoft) | Block | 5 |
| 176.106.226.4 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 46.19.85.128 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 176.106.227.199 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 212.24.149.38 | Czech Republic | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | C014: HTTP: Fuck in url | Block | 5 |
| 184.64.9.210 | Canada | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 79.180.24.64 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 46.19.85.181 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 170.51.53.179 | Paraguay | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 87.69.39.95 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 176.106.227.185 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 5.29.58.45 | Israel | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 4 |
| 176.106.226.7 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 84.228.242.229 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 87.68.31.219 | Israel | 147.237.76.31 | nakchal.idf.i | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 37.26.149.235 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 46.19.85.92 | Israel | 147.237.0.34 | tikshuv.idf.i | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 176.106.227.162 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 212.235.62.200 | Israel | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 176.106.226.4 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 77.125.142.182 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 109.65.163.93 | Israel | 147.237.76.31 | nakchal.idf.i | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 213.8.123.108 | Israel | 147.237.76.31 | nakchal.idf.i | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 176.106.227.5 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 82.166.22.192 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 212.64.228.100 | Europe | 147.237.76.31 | nakchal.idf.i | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 2.54.154.239 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |

09-01-2015-00:00:02 to 09-02-2015-00:00:02

## Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|---|---|---|---|---|---|
| 66.249.78.2 | United States | 147.237.72.166 | aka.idf.il | ET SCAN NMAP -sA (2) | 171 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 73 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Admin login page scan - Havij | 67 |
| 46.19.85.231 | Israel | 147.237.76.42 | refuah.idf.il | POLICY-OTHER TCP packet with urgent flag attempt | 55 |
| 144.76.206.245 | Germany | 147.237.77.74 | law.idf.il | Tehila - Perl LWP with fake user agent | 40 |
| 23.96.25.186 | United States | 147.237.72.166 | aka.idf.il | Tehila - Perl LWP with fake user agent | 22 |
| 172.56.19.175 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 10 |
| 176.12.138.184 | Israel | 147.237.0.19 | madim.atal.idf.il | ET SCAN Possible SSL Brute Force attack or Site Crawl | 9 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP login.htm access | 8 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP adminlogin access | 7 |
| 8.37.225.25 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | SERVER-APACHE Apache SSI error page cross-site scripting | 6 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP admin.php access | 3 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 3 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SERVER-IIS scripts-browse access | 3 |
| 31.184.242.17 | Russian Federation | 147.237.77.216 | dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 3 |
| 66.249.64.168 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 3 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP /cgi-bin/ access | 3 |
| 93.174.93.100 | Netherlands | 147.237.72.217 | e.idf.il | ET SCAN Potential SSH Scan | 2 |
| 109.253.132.202 | Israel | 147.237.72.166 | aka.idf.il | INDICATOR-SCAN myscan | 2 |
| 93.174.93.100 | Netherlands | 147.237.77.233 | atal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 86.92.83.226 | Netherlands | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 66.249.81.180 | United States | 147.237.77.233 | atal.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 93.174.93.100 | Netherlands | 147.237.0.200 | m4u.idf.il | ET SCAN Potential SSH Scan | 2 |
| 123.96.244.213 | China | 147.237.77.235 | sviva.idf.il | ET SCAN Potential SSH Scan | 2 |
| 46.19.86.131 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 109.67.1.132 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 109.253.132.202 | Israel | 147.237.72.166 | aka.idf.il | GPL SCAN myscan | 2 |
| 123.96.244.213 | China | 147.237.76.39 | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 93.174.93.100 | Netherlands | 147.237.77.121 | e.navy.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.93.160 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 193.105.134.220 | Sweden | 147.237.0.15 | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 66.249.78.153 | United States | 147.237.72.166 | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.64.173 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 5.29.228.18 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 37.237.116.246 | Iraq | 147.237.76.44 | e.refuah.idf.il | ET SCAN Potential SSH Scan | 2 |
| 91.220.163.43 | Ukraine | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 182.48.105.216 | China | 147.237.8.28 | e.mobile-ks.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 79.182.173.92 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 123.96.244.213 | China | 147.237.76.177 | ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.19.85.226 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.64.132.49 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 218.7.37.194 | China | 147.237.72.167 | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 2.54.37.9 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 193.105.134.220 | Sweden | 147.237.76.30 | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 84.110.210.169 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

09-01-2015-00:00:02 to 09-02-2015-00:00:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 85.105.158.114 | Turkey | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 33169 |
| 82.145.222.120 | Europe | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 11018 |
| 109.110.118.146 | Lebanon | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 8183 |
| 95.86.122.101 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 7462 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 5238 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1912 |
| 2.54.189.241 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1764 |
| 2.54.13.84 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1694 |
| 141.0.12.179 | Norway | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1298 |
| 93.173.248.176 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 975 |
| 8.37.225.25 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 844 |
| 66.249.64.173 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 841 |
| 208.109.97.62 | United States | 147.237.77.216 | dover.idf.il | SAM rule | drop | drop | 839 |
| 66.249.64.178 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 792 |
| 66.249.64.168 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 790 |
| 208.109.97.62 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 786 |
| 46.19.85.124 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 739 |
| 46.19.85.224 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 662 |
| 213.233.103.21 | Romania | 147.237.72.166 | aka.idf.il | First packet isn't SYN | drop | drop | 597 |
| 164.138.124.85 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 536 |
| 46.19.85.221 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 501 |
| 79.179.204.247 | Israel | 147.237.76.200 | eitan.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 492 |
| 54.187.55.213 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 471 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 464 |
| 192.249.64.249 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 456 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 452 |
| 54.72.0.55 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 448 |
| 79.182.98.106 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 444 |
| 95.86.103.20 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 428 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 417 |
| 66.249.93.164 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 406 |
| 213.57.138.75 | Israel | 147.237.72.166 | aka.idf.il | SYN+ACK retransmit with different window scale | Bad TCP sequence | monitor | 388 |
| 66.249.93.168 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 387 |
| 79.176.109.141 | Israel | 147.237.76.200 | eitan.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 384 |
| 2.54.62.182 | Israel | 147.237.76.200 | eitan.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 363 |
| 66.249.93.160 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 349 |
| 37.125.255.71 | Saudi Arabia | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 335 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Failed to handle connection data | Block HTTP Non Compliant | monitor | 327 |
| 46.19.85.132 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 312 |
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 305 |
| 41.33.231.86 | Egypt | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 302 |
| 77.127.184.41 | Israel | 147.237.76.200 | eitan.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 300 |
| 2.54.29.221 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 292 |
| 84.228.86.95 | Israel | 147.237.76.200 | eitan.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 285 |
| 195.250.54.4 | Poland | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 272 |
| 213.204.103.36 | Lebanon | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 270 |
| 46.19.86.161 | Israel | 147.237.76.200 | eitan.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 270 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 247 |
| 37.26.149.134 | Israel | 147.237.76.200 | eitan.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 243 |
| 84.228.86.63 | Israel | 147.237.76.200 | eitan.aka.idf.i | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 231 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 176.65.11.219 | Block | 4653 |
| 109.66.135.5 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 4324 |
| 176.12.138.184 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 4125 |
| 46.19.86.41 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 4008 |
| 197.32.103.219 | Egypt | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/homepage/undefined | Block | 3874 |
| 46.19.85.73 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 2596 |
| 2.54.169.12 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 2349 |
| 82.102.169.113 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1899 |
| 2.54.41.115 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1784 |
| 176.12.148.228 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1412 |
| 37.26.147.255 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1344 |
| 2.54.8.190 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1254 |
| 80.246.137.127 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1197 |
| 46.19.85.62 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1128 |
| 5.29.88.115 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1116 |
| 37.26.149.246 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 1098 |
| 2.54.28.76 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 2.54.28.76 | Block | 1072 |
| 46.19.86.11 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 990 |
| 80.246.139.24 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 988 |
| 2.52.165.124 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 906 |
| 2.54.60.61 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 883 |
| 46.19.86.172 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 768 |
| 176.13.17.75 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 726 |
| 176.13.9.6 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 709 |
| 109.253.138.100 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 539 |
| 46.19.85.181 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 528 |
| 46.19.86.178 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 470 |
| 2.54.11.75 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 441 |
| 176.65.11.219 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Multiple Admin Blocking from 176.65.11.219 | Block | 390 |
| 46.19.86.132 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 46.19.86.132 | Block | 378 |
| 144.76.206.245 | Germany | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 288 |
| 109.110.118.146 | Lebanon | 147.237.77.216 | dover.idf.il | Post Request - Missing Content Type from 109.110.118.146 | Block | 286 |
| 144.76.206.245 | Germany | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 144.76.206.245 | Block | 276 |
| 46.19.85.123 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 46.19.85.123 | Block | 266 |
| 109.253.139.20 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 258 |
| 66.249.78.254 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 246 |
| 66.249.78.2 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 240 |
| 66.249.78.216 | Israel | 147.237.77.243 | mobile.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 240 |
| 157.55.39.235 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 234 |
| 66.249.79.228 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 216 |
| 66.249.78.9 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 210 |
| 66.249.78.230 | Israel | 147.237.77.243 | mobile.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 210 |
| 66.249.79.214 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 204 |
| 66.249.78.62 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 198 |
| 66.249.78.76 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 192 |
| 66.249.79.157 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 192 |
| 66.249.79.221 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 192 |
| 66.249.79.150 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 186 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 208.115.113.88 | Block | 186 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 180 |