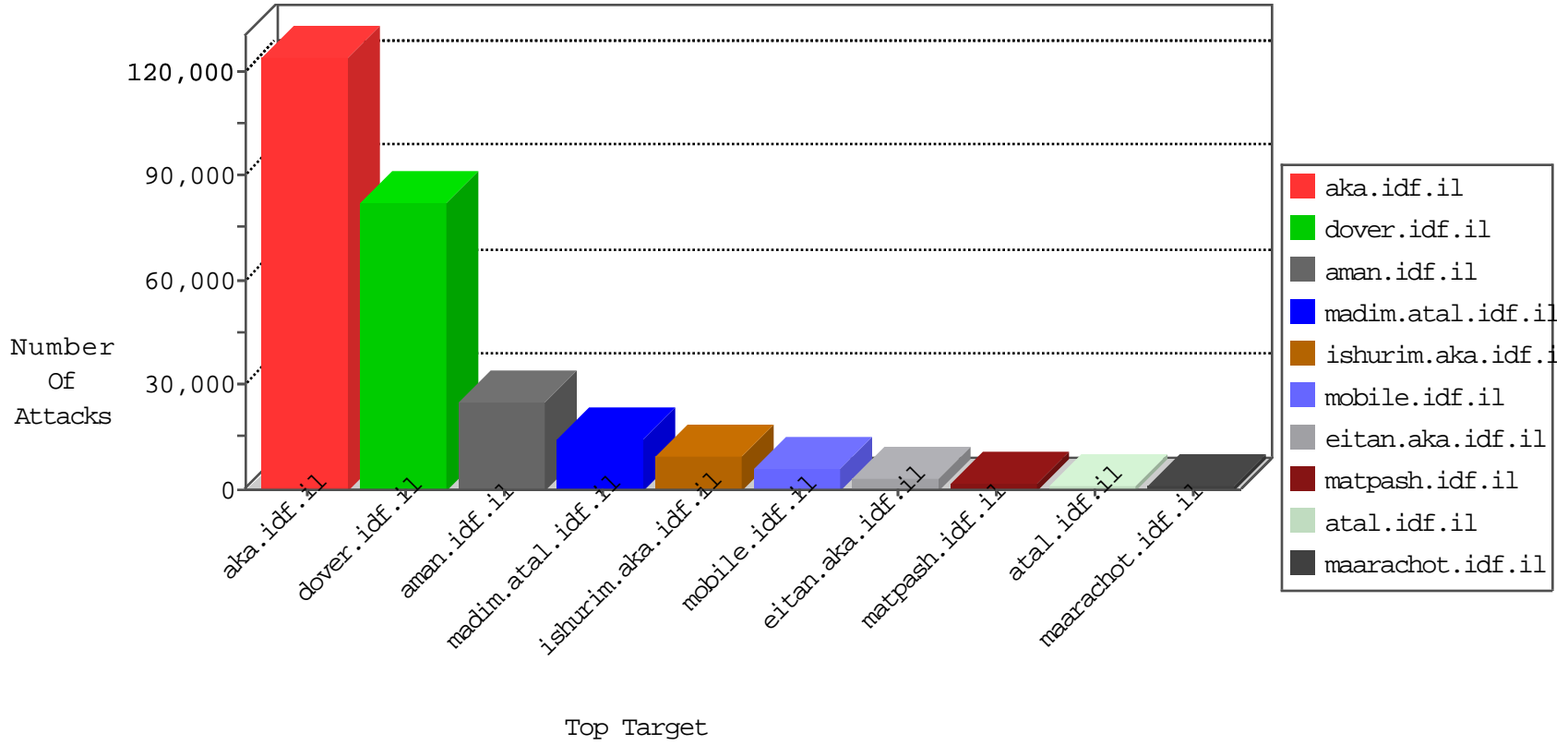


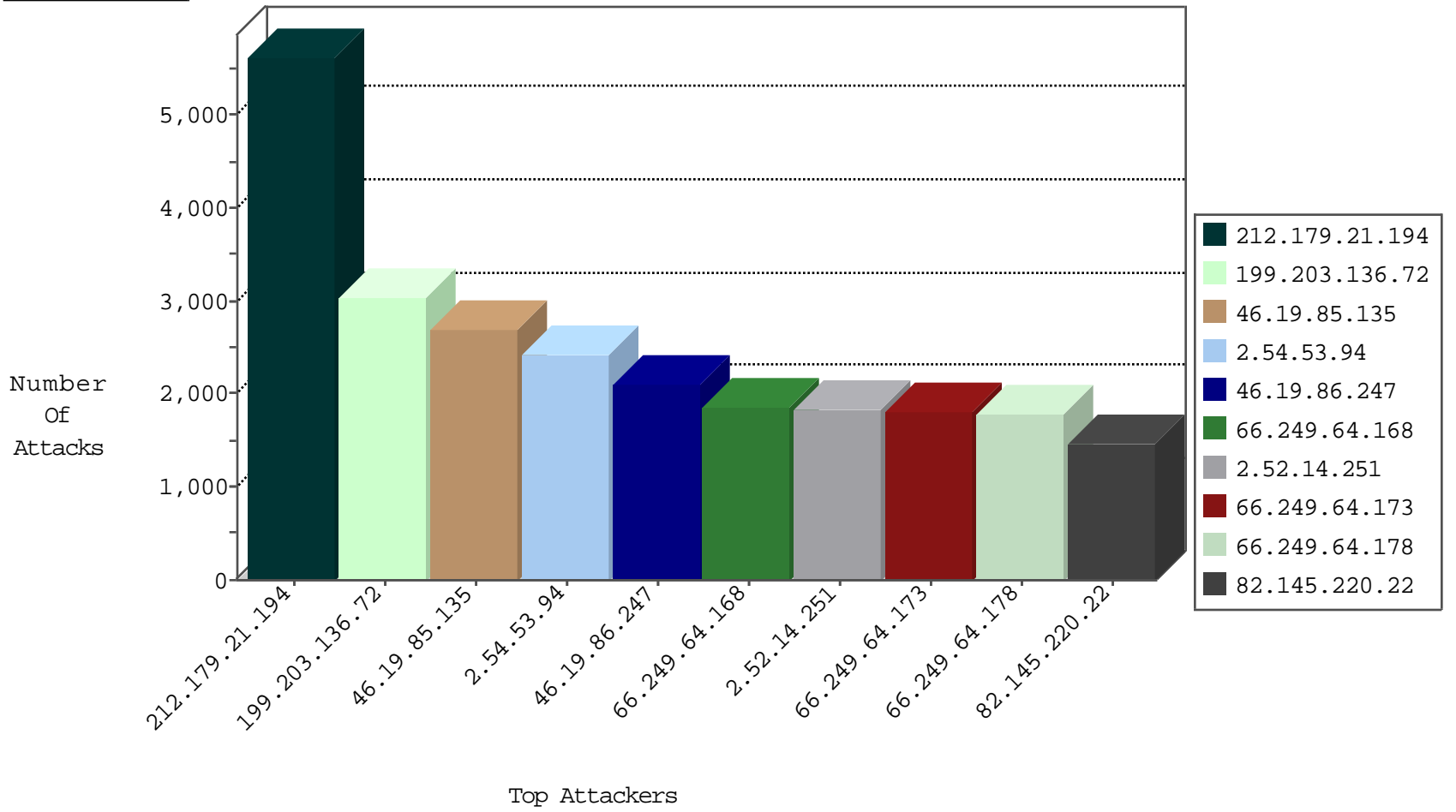
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|------------------|------------------|----------------|--------------------|---|---------------|-------------------|
| 2.52.150.102 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3110 |
| 66.249.78.2 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 2803 |
| 212.25.84.200 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2614 |
| 66.249.78.254 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 1069 |
| 123.125.71.30 | China | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 479 |
| 192.118.30.102 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 349 |
| 79.176.190.82 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 202 |
| 220.181.108.184 | China | 147.237.76.42 | refuah.idf.il | TCP handshake violation, first packet not syn | drop | 172 |
| 212.199.149.78 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 157 |
| 193.169.70.108 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 141 |
| 213.8.242.46 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 123 |
| 46.120.184.9 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 123 |
| 66.249.78.9 | Israel | 147.237.72.166 | aka.idf.il | TCP handshake violation, first packet not syn | drop | 116 |
| 192.118.30.102 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 105 |
| 220.181.108.83 | China | 147.237.76.42 | refuah.idf.il | TCP handshake violation, first packet not syn | drop | 93 |
| 46.120.208.54 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 71 |
| 176.12.150.173 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 50 |
| 80.230.16.215 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 43 |
| 5.102.224.76 | Israel | 147.237.77.216 | dover.idf.il | I4 Source or Dest Port Zero | drop | 42 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 33 |
| 109.67.132.195 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 32 |
| 199.203.170.158 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 30 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 26 |
| 37.26.146.147 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 22 |
| 79.183.35.128 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 22 |
| 80.246.140.110 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 21 |
| 176.13.8.74 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 20 |
| 2.54.174.117 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 19 |
| 213.151.52.191 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 18 |
| 95.86.107.36 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 18 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 18 |
| 109.67.132.195 | Israel | 147.237.77.233 | atal.idf.il | Block_Udp_All_Nets | drop | 16 |
| 176.13.8.74 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 15 |
| 46.19.85.193 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 15 |
| 37.26.147.134 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 15 |
| 176.13.18.193 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 15 |
| 176.12.151.228 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 15 |
| 46.19.85.82 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 14 |
| 176.13.9.100 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 13 |
| 46.19.85.254 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 13 |
| 176.106.227.1 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 12 |
| 2.54.14.235 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 12 |
| 176.106.227.2 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 12 |
| 70.115.195.75 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 12 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 12 |
| 85.250.38.242 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 12 |
| 84.228.217.177 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 12 |
| 192.168.1.200 | | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 11 |
| 37.26.147.233 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 10 |
| 188.120.148.196 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 10 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|------------------|--------------------|----------------|------------------------|---|---------------|-------|
| 80.178.157.40 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 231 |
| 194.114.146.227 | Israel | 147.237.76.42 | refuah.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 92 |
| 213.151.35.218 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 56 |
| 79.176.190.82 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 30 |
| 138.134.102.15 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 24 |
| 176.97.116.138 | Ukraine | 147.237.77.216 | dover.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 23 |
| 115.219.30.85 | China | 147.237.77.216 | dover.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 21 |
| 177.45.117.201 | Brazil | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 16 |
| 138.134.102.16 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 12 |
| 46.19.85.16 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 12 |
| 95.179.63.234 | Russian Federation | 147.237.77.170 | maarachot.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 11 |
| 77.125.80.141 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 11 |
| 31.154.85.167 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 11 |
| 115.219.30.85 | China | 147.237.77.216 | dover.idf.il | 0854: HTTP: upload* Access | Block | 10 |
| 176.97.116.138 | Ukraine | 147.237.77.216 | dover.idf.il | 0854: HTTP: upload* Access | Block | 10 |
| 46.19.85.123 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 9 |
| 85.64.19.133 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 8 |
| 93.173.185.156 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 7 |
| 176.106.226.238 | Israel | 147.237.72.167 | ishurim.aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 7 |
| 79.183.178.188 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 46.116.138.100 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 91.186.251.109 | Jordan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 79.178.176.13 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 6 |
| 46.19.85.5 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 84.108.123.220 | Israel | 147.237.72.166 | aka.idf.il | 15323: HTTP: User-Agent (MRSPUTNIK) | Block | 5 |
| 179.210.170.109 | Brazil | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 186.212.125.221 | Brazil | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 176.106.226.182 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 31.154.87.155 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 5 |
| 149.88.213.9 | United States | 147.237.77.233 | atal.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 46.120.78.152 | Israel | 147.237.72.167 | ishurim.aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 176.106.227.94 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 68.2.81.129 | United States | 147.237.77.234 | halag.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 37.26.147.134 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 207.232.27.5 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 4 |
| 88.132.201.187 | Hungary | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 149.78.80.165 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 188.72.59.190 | Iraq | 147.237.77.216 | dover.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 3 |
| 176.13.5.95 | Israel | 147.237.77.170 | maarachot.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 82.80.135.182 | Israel | 147.237.77.74 | law.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 176.106.226.7 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 82.80.198.164 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 154.101.175.209 | Sudan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 79.183.105.120 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 3 |
| 176.228.158.159 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 46.121.219.248 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 3 |
| 2.52.186.1 | Israel | 147.237.0.34 | tikshuv.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 46.120.77.148 | Israel | 147.237.72.156 | aman.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 197.251.16.132 | Sudan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |
| 89.139.63.34 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Permit | 2 |

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 | 58 |
| 82.145.53.206 | United Kingdom | 147.237.77.170 | maarachot.idf.il | Tehila - Perl LWP with fake user agent | 31 |
| 66.249.67.67 | United States | 147.237.77.74 | law.idf.il | ET SCAN NMAP -sA (2) | 12 |
| 105.103.106.188 | Algeria | 147.237.77.216 | dover.idf.il | SQL Injection - Select From | 10 |
| 104.207.147.244 | | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 10 |
| 66.249.67.27 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 10 |
| 195.160.240.11 | Israel | 147.237.72.166 | aka.idf.il | ET SCAN NMAP -sA (2) | 8 |
| 105.103.106.188 | Algeria | 147.237.77.216 | dover.idf.il | SQL generic sql with comments injection attempt - GET parameter | 8 |
| 105.103.104.132 | Algeria | 147.237.77.216 | dover.idf.il | SQL Injection - Select From | 7 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 5 |
| 105.103.104.132 | Algeria | 147.237.77.216 | dover.idf.il | SQL generic sql with comments injection attempt - GET parameter | 5 |
| 66.249.93.243 | United States | 147.237.77.233 | atal.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 66.249.67.32 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 66.249.93.176 | United States | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 212.199.205.68 | Israel | 147.237.77.233 | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 4 |
| 66.249.67.34 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 66.249.67.20 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 105.103.106.188 | Algeria | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP encoded cross site scripting HTML Image tag attempt | 3 |
| 66.249.78.9 | United States | 147.237.72.166 | aka.idf.il | ET SCAN NMAP -sA (2) | 3 |
| 109.253.144.211 | Israel | 147.237.77.233 | atal.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 3 |
| 66.249.78.254 | United States | 147.237.72.166 | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 93.174.93.100 | Netherlands | 147.237.76.30 | himush.idf.il | ET SCAN Potential SSH Scan | 2 |
| 132.64.142.38 | Israel | 147.237.77.170 | maarachot.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 66.249.64.178 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 115.219.30.85 | China | 147.237.77.216 | dover.idf.il | SERVER-WEBAPP Mambo upload.php access | 2 |
| 93.174.93.100 | Netherlands | 147.237.72.14 | dover.idf.il(old) | ET SCAN Potential SSH Scan | 2 |
| 66.249.64.168 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 61.148.116.114 | China | 147.237.77.216 | dover.idf.il | GPL SCAN nmap TCP | 2 |
| 212.106.70.216 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 220.191.15.105 | China | 147.237.76.176 | test.ncoore.idf.il | ET SCAN Potential SSH Scan | 2 |
| 188.68.250.151 | Russian Federation | 147.237.77.216 | dover.idf.il | Xenu Link Sleuth User Agent | 2 |
| 66.249.78.14 | United States | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 105.103.104.132 | Algeria | 147.237.77.216 | dover.idf.il | ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access | 2 |
| 79.180.219.125 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 93.174.93.100 | Netherlands | 147.237.76.44 | e.refuah.idf.il | ET SCAN Potential SSH Scan | 2 |
| 185.82.201.17 | | 147.237.77.216 | dover.idf.il | ET DOS SSL Bomb DoS Attempt | 2 |
| 199.127.54.213 | United States | 147.237.0.19 | madim.atal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 93.174.93.100 | Netherlands | 147.237.76.39 | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 2 |
| 105.103.106.188 | Algeria | 147.237.77.216 | dover.idf.il | XSS - IMG (POST) | 2 |
| 176.13.23.17 | Israel | 147.237.76.30 | himush.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 66.249.67.25 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.93.164 | United States | 147.237.77.233 | atal.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 115.248.138.98 | India | 147.237.72.217 | e.idf.il | ET SCAN Potential SSH Scan | 2 |
| 93.174.93.100 | Netherlands | 147.237.76.31 | nakchal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.64.242 | United States | 147.237.76.86 | navy.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.78.230 | United States | 147.237.77.243 | mobile.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 |
| 109.67.108.38 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 93.174.93.100 | Netherlands | 147.237.77.179 | e.mazi.idf.il | ET SCAN Potential SSH Scan | 2 |

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 | 4950 |
| 199.203.136.72 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 3024 |
| 2.54.53.94 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2393 |
| 82.145.220.22 | Europe | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1474 |
| 66.249.64.173 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 928 |
| 66.249.64.178 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 911 |
| 66.249.64.168 | United States | 147.237.77.216 | dover.idf.il | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 875 |
| 193.77.85.214 | Slovenia | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 848 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 790 |
| 79.179.104.189 | Israel | 147.237.76.200 | eitan.aka.idf. | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 705 |
| 168.235.197.144 | | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 688 |
| 109.64.2.178 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 687 |
| 54.72.0.55 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 661 |
| 212.143.41.138 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 618 |
| 192.249.64.249 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 617 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 615 |
| 41.77.11.186 | Malawi | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 593 |
| 62.90.107.178 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 583 |
| 54.72.73.168 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 580 |
| 37.60.42.226 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 579 |
| 208.109.97.62 | United States | 147.237.77.216 | dover.idf.il | SAM rule | drop | drop | 573 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 567 |
| 109.186.161.85 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 566 |
| 208.109.97.62 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 556 |
| 2.52.10.65 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 533 |
| 172.56.21.39 | United States | 147.237.77.176 | matpash.idf.il | First packet isn't SYN | drop | drop | 521 |
| 109.160.151.50 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 470 |
| 37.231.201.88 | Kuwait | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 461 |
| 37.26.147.213 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 441 |
| 46.19.85.60 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 419 |
| 192.115.248.2 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 408 |
| 185.4.252.171 | Lebanon | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 339 |
| 46.19.85.183 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 337 |
| 176.42.78.168 | Turkey | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 330 |
| 37.26.147.248 | Israel | 147.237.76.200 | eitan.aka.idf. | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 327 |
| 62.219.128.153 | Israel | 147.237.76.200 | eitan.aka.idf. | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 315 |
| 59.184.154.109 | India | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 305 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 303 |
| 46.19.86.110 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 301 |
| 54.187.55.213 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 300 |
| 95.86.88.33 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 295 |
| 212.143.3.44 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 292 |
| 46.19.86.204 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 292 |
| 77.125.100.240 | Israel | 147.237.76.200 | eitan.aka.idf. | Invalid segment retransmission. Packet dropped. | Streaming Engine: TCP Invalid Retransmission | drop | 276 |
| 41.33.232.65 | Egypt | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 263 |
| 109.110.118.146 | Lebanon | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 261 |
| 46.19.86.68 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 248 |
| 109.110.114.109 | Lebanon | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 246 |
| 128.6.36.137 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 243 |
| 2.54.168.236 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 239 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|------------------|------------------|----------------|-------------------|--|---------------|-------|
| 46.19.85.135 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 2703 |
| 46.19.86.247 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 2097 |
| 2.52.14.251 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 1831 |
| 2.54.130.213 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 1264 |
| 176.12.145.175 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 1210 |
| 176.13.10.91 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 1155 |
| 176.13.2.238 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 724 |
| 176.13.4.99 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 651 |
| 66.249.64.168 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.168 | Block | 625 |
| 46.19.85.241 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.85.241 | Block | 600 |
| 176.13.7.106 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 582 |
| 66.249.64.178 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.178 | Block | 550 |
| 46.116.172.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 540 |
| 109.253.149.147 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 483 |
| 66.249.64.173 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.173 | Block | 452 |
| 176.13.2.238 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 176.13.2.238 | Block | 408 |
| 79.179.104.189 | Israel | 147.237.76.200 | eitan.aka.idf.il | Too Many of the Same Response Code (404) in Session from 79.179.104.189 | Block | 384 |
| 66.249.67.37 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 341 |
| 82.145.53.206 | United Kingdom | 147.237.77.170 | maarachot.idf.il | Distributed PHP Attempt | Block | 336 |
| 82.145.53.206 | United Kingdom | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 82.145.53.206 | Block | 329 |
| 66.249.67.30 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 321 |
| 66.249.78.9 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 298 |
| 207.46.13.145 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 298 |
| 109.253.149.147 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 109.253.149.147 | Block | 294 |
| 66.249.67.44 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 284 |
| 66.249.78.230 | Israel | 147.237.77.243 | mobile.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 258 |
| 66.249.78.223 | Israel | 147.237.77.243 | mobile.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 253 |
| 66.249.78.2 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 250 |
| 66.249.78.134 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 247 |
| 66.249.78.216 | Israel | 147.237.77.243 | mobile.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 236 |
| 93.173.9.248 | Israel | 147.237.72.166 | aka.idf.il | Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/popups/markivsachar.aspx parameter | None | 234 |
| 192.169.196.179 | United States | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 234 |
| 66.249.78.141 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 233 |
| 66.249.78.254 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 228 |
| 192.169.196.179 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.169.196.179 | Block | 228 |
| 66.249.78.62 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 219 |
| 68.180.229.173 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 210 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 208.115.113.88 | Block | 205 |
| 66.249.78.69 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 204 |
| 66.249.78.148 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 201 |
| 66.249.93.174 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 188 |
| 66.249.93.170 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 170 |
| 82.145.53.206 | United Kingdom | 147.237.77.170 | maarachot.idf.il | Distributed Admin Blocking | Block | 168 |
| 66.249.78.76 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 166 |
| 157.55.39.36 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 166 |
| 157.55.39.146 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 156 |
| 66.249.93.166 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 149 |
| 79.178.211.166 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 145 |
| 157.55.39.147 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 139 |
| 157.55.39.80 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown Server Certificate | None | 134 |