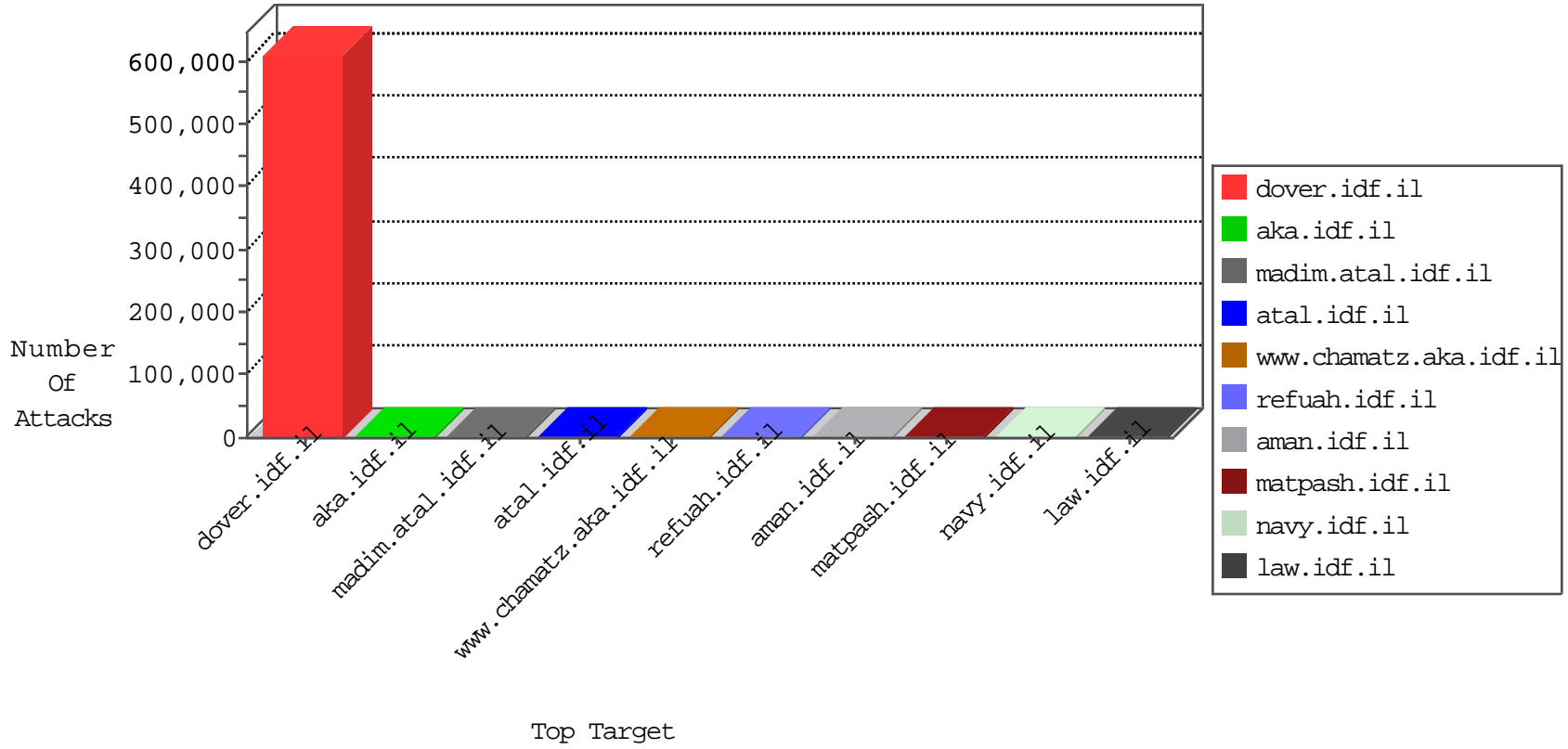


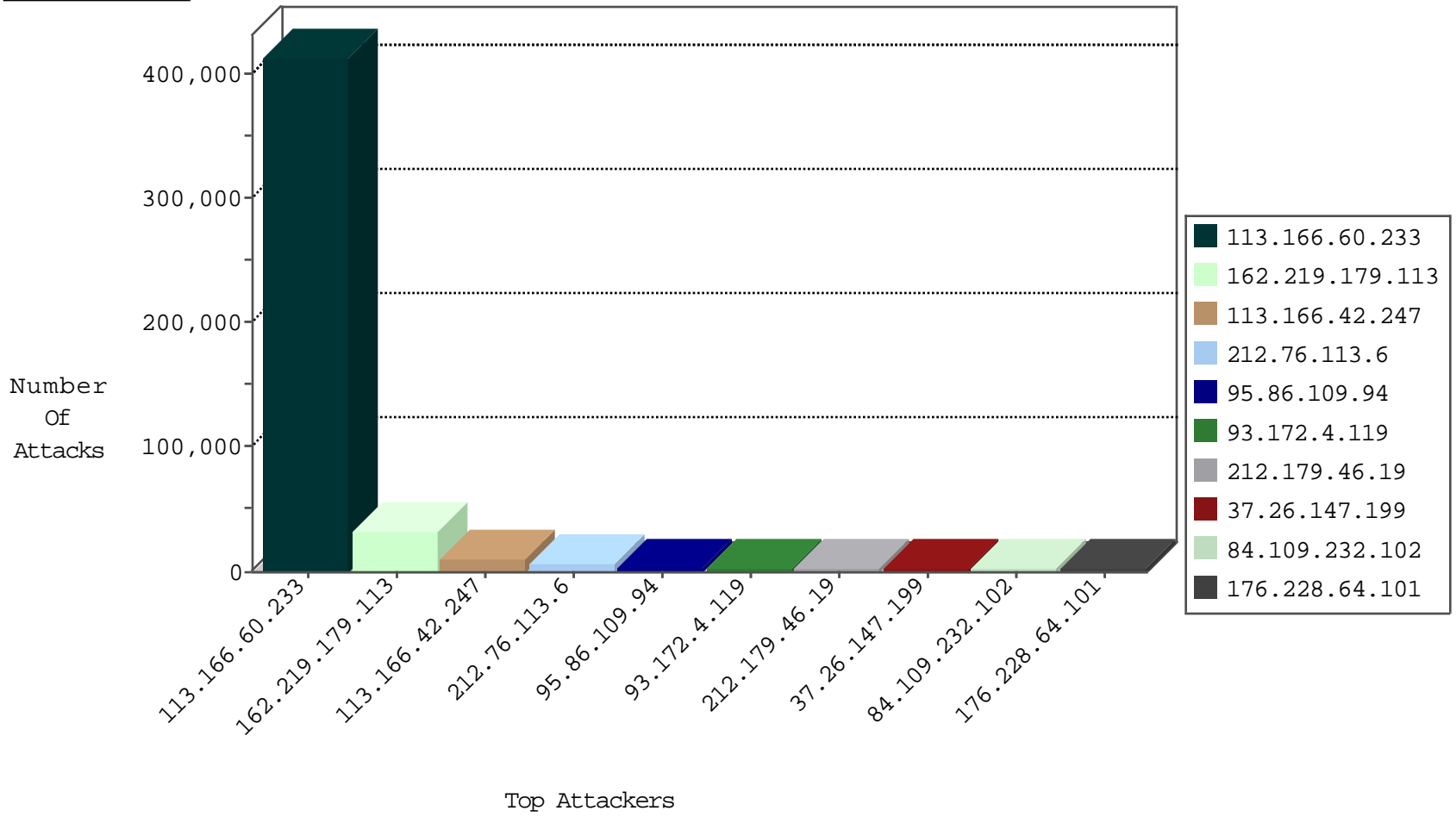
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | IP_Map.site | Name | Device Action | Sum(Packet_Count) |
|------------------|---------------------------------|----------------|--------------------|---|---------------|-------------------|
| 66.249.67.39 | Israel | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 5405 |
| 66.249.67.40 | Israel | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 4511 |
| 94.230.85.13 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 4057 |
| 220.181.108.105 | China | 147.237.76.42 | refuah.idf.il | TCP handshake violation, first packet not syn | drop | 3979 |
| 220.181.108.161 | China | 147.237.76.42 | refuah.idf.il | TCP handshake violation, first packet not syn | drop | 3577 |
| 81.218.251.252 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3087 |
| 109.186.25.244 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3002 |
| 109.67.133.211 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2737 |
| 46.120.228.7 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2547 |
| 185.32.178.104 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2525 |
| 46.19.86.247 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2437 |
| 10.0.0.4 | | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1958 |
| 66.249.67.24 | Israel | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 1783 |
| 46.19.86.85 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1687 |
| 185.26.180.145 | Europe | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1315 |
| 66.249.79.74 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1305 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1298 |
| 109.24.219.145 | France | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1271 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 1267 |
| 46.19.85.2 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1236 |
| 188.225.183.2 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1227 |
| 79.183.211.40 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1061 |
| 109.66.0.231 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 979 |
| 93.173.167.191 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 889 |
| 66.249.78.197 | Israel | 147.237.77.176 | matpash.idf.il | TCP handshake violation, first packet not syn | drop | 886 |
| 77.125.215.186 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 847 |
| 37.54.210.227 | Ukraine | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 803 |
| 79.180.124.132 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 768 |
| 105.237.250.130 | South Africa | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 735 |
| 176.12.141.87 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 688 |
| 79.181.11.64 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 687 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 664 |
| 66.249.67.32 | Israel | 147.237.77.170 | maarachot.idf.il | TCP handshake violation, first packet not syn | drop | 658 |
| 147.236.238.10 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 652 |
| 188.120.153.148 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 652 |
| 37.142.209.187 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 652 |
| 5.29.151.206 | Israel | 147.237.72.156 | aman.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 638 |
| 77.127.213.29 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 587 |
| 79.181.183.115 | Israel | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 567 |
| 62.219.46.141 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 563 |
| 109.66.107.68 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 523 |
| 37.26.148.252 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 520 |
| 109.253.140.248 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 519 |
| 149.78.15.101 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 498 |
| 62.219.162.219 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 480 |
| 109.65.205.131 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 462 |
| 176.228.140.94 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 459 |
| 46.19.86.237 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 457 |
| 193.239.152.249 | Ukraine | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 453 |
| 46.19.85.148 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 450 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|------------------|---------------------------------|----------------|-------------------|---|---------------|-------|
| 84.109.232.102 | Israel | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 2208 |
| 192.92.94.23 | Europe | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 2000 |
| 184.173.183.172 | United States | 147.237.77.233 | atal.idf.il | DVRep_P-N_40-59 | Permit | 577 |
| 184.173.183.172 | United States | 147.237.76.42 | refuah.idf.il | DVRep_P-N_40-59 | Permit | 317 |
| 184.173.183.172 | United States | 147.237.77.74 | law.idf.il | DVRep_P-N_40-59 | Permit | 193 |
| 184.173.183.172 | United States | 147.237.77.176 | matpash.idf.il | DVRep_P-N_40-59 | Permit | 186 |
| 184.173.183.172 | United States | 147.237.76.86 | navy.idf.il | DVRep_P-N_40-59 | Permit | 142 |
| 174.121.21.2 | United States | 147.237.72.166 | aka.idf.il | DVRep_P-N_40-59 | Permit | 73 |
| 193.105.134.192 | Sweden | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 65 |
| 128.242.249.12 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 57 |
| 125.227.255.30 | Taiwan | 147.237.77.176 | matpash.idf.il | C1000108: HTTP: Trying to locate existing FCKeditor | Block | 36 |
| 180.76.5.193 | China | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 22 |
| 46.137.134.188 | Ireland | 147.237.72.156 | aman.idf.il | DVRep_P-N_40-59 | Permit | 20 |
| 46.137.134.188 | Ireland | 147.237.72.166 | aka.idf.il | DVRep_P-N_40-59 | Permit | 20 |
| 184.173.183.172 | United States | 147.237.77.216 | dover.idf.il | DVRep_P-N_40-59 | Permit | 15 |
| 212.199.224.24 | Israel | 147.237.72.166 | aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 12 |
| 46.116.211.238 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 10 |
| 212.117.143.250 | Israel | 147.237.76.31 | nakchal.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 9 |
| 188.138.9.50 | Germany | 147.237.76.201 | e.atal.idf.il | DVRep_B-N_60_100 | Block | 7 |
| 79.179.198.101 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 7 |
| 149.88.66.6 | United States | 147.237.76.86 | navy.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 7 |
| 192.117.2.162 | Israel | 147.237.72.166 | aka.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 6 |
| 109.67.172.202 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 212.34.12.189 | Jordan | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 79.177.113.15 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 46.19.85.144 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 79.181.183.115 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 6 |
| 176.106.46.74 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 188.138.9.50 | Germany | 147.237.8.46 | e.chimuch.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 71.6.167.142 | United States | 147.237.72.156 | aman.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 71.6.167.142 | United States | 147.237.76.176 | test.ncore.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 46.19.85.197 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 188.138.9.50 | Germany | 147.237.0.33 | idf.il | DVRep_B-N_60_100 | Block | 5 |
| 46.19.85.253 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 46.19.85.98 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 188.138.9.50 | Germany | 147.237.77.235 | sviva.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 77.125.132.29 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 71.6.165.200 | United States | 147.237.77.234 | halag.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 37.26.147.221 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 188.138.9.50 | Germany | 147.237.77.243 | mobile.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 109.65.210.236 | Israel | 147.237.72.166 | aka.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 71.6.165.200 | United States | 147.237.76.196 | e.sviva.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 188.138.9.50 | Germany | 147.237.76.34 | yohalan.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 62.90.221.180 | Israel | 147.237.77.234 | halag.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 109.66.197.59 | Israel | 147.237.76.42 | refuah.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 5 |
| 198.20.70.114 | United States | 147.237.76.42 | refuah.idf.il | DVRep_B-N_60_100 | Block | 5 |
| 71.6.167.142 | United States | 147.237.76.202 | e.halag.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 46.19.85.76 | Israel | 147.237.77.216 | dover.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |
| 71.6.165.200 | United States | 147.237.0.34 | tikshuv.idf.il | DVRep_B-N_60_100 | Block | 4 |
| 46.19.85.30 | Israel | 147.237.76.86 | navy.idf.il | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute | Block | 4 |

Top Attackers In IDS

| Attacker Address | Attacker Country | Target Address | Site | Name | Count |
|------------------|--------------------|----------------|------------------------|--|-------|
| 66.249.65.12 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 536 |
| 82.80.25.221 | Israel | 147.237.77.216 | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 101 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 96 |
| 79.177.118.55 | Israel | 147.237.77.176 | matpash.idf.il | POLICY-OTHER TCP packet with urgent flag attempt | 42 |
| 66.249.67.32 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 30 |
| 66.249.67.40 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 16 |
| 162.219.179.113 | Canada | 147.237.77.216 | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 13 |
| 66.249.67.24 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 12 |
| 66.249.73.203 | United States | 147.237.77.74 | law.idf.il | ET SCAN NMAP -sA (2) | 10 |
| 66.249.73.219 | United States | 147.237.77.74 | law.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 66.249.73.211 | United States | 147.237.77.74 | law.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 66.249.67.31 | United States | 147.237.77.170 | maarachot.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 66.249.65.44 | United States | 147.237.76.86 | navy.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 66.249.65.26 | United States | 147.237.77.74 | law.idf.il | ET SCAN NMAP -sA (2) | 4 |
| 109.67.24.178 | Israel | 147.237.0.34 | tikshuv.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack | 3 |
| 43.255.191.161 | Japan | 147.237.0.15 | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 3 |
| 59.106.108.116 | Japan | 147.237.77.216 | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 93.173.251.128 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 66.249.64.65 | United States | 147.237.76.42 | refuah.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.79.66 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 46.116.95.85 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 87.139.236.153 | Germany | 147.237.72.167 | ishurim.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 2 |
| 81.218.77.162 | Israel | 147.237.77.216 | dover.idf.il | GPL SCAN nmap TCP | 2 |
| 31.184.242.17 | Russian Federation | 147.237.77.216 | dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 2 |
| 2.52.2.221 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 84.228.204.20 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 5.29.12.142 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 66.249.78.190 | United States | 147.237.77.176 | matpash.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 61.240.144.66 | China | 147.237.76.39 | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 85.65.213.40 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 162.219.179.113 | Canada | 147.237.77.216 | dover.idf.il | ET CURRENT_EVENTS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA | 2 |
| 62.90.202.62 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 61.240.144.64 | China | 147.237.0.33 | idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 93.172.152.10 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 43.255.191.161 | Japan | 147.237.76.200 | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 2 |
| 212.150.82.221 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 2.54.130.131 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 46.117.126.250 | Israel | 147.237.72.166 | aka.idf.il | portscan: TCP Distributed Portscan | 2 |
| 43.255.191.163 | Japan | 147.237.8.27 | e.madim.atal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 61.240.144.64 | China | 147.237.77.227 | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 84.108.166.64 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.178.65.123 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 82.80.196.44 | Israel | 147.237.77.216 | dover.idf.il | portscan: TCP Distributed Portscan | 2 |
| 61.240.144.66 | China | 147.237.0.35 | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 2 |
| 85.64.94.95 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 79.183.49.186 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 66.249.65.30 | United States | 147.237.77.74 | law.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 66.249.93.164 | United States | 147.237.77.216 | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 79.176.23.155 | Israel | 147.237.0.34 | tikshuv.idf.il | LOCAL_RULES DOS attack 01/2012 | 2 |
| 66.249.81.167 | United States | 147.237.76.30 | himush.idf.il | ET SCAN NMAP -sA (2) | 2 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Message | Name | Device Action | Count |
|------------------|------------------|----------------|--------------|------------------------|------|---------------|--------|
| 113.166.60.233 | Vietnam | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 412647 |
| 162.219.179.113 | Canada | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 31760 |
| 113.166.42.247 | Vietnam | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 10875 |
| 212.76.113.6 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 5981 |
| 95.86.109.94 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 3651 |
| 93.172.4.119 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 3594 |
| 212.179.46.19 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2511 |
| 37.26.147.199 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2390 |
| 176.228.64.101 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2069 |
| 212.179.140.132 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 2015 |
| 81.218.251.250 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1962 |
| 95.86.68.225 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1878 |
| 81.218.71.132 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1846 |
| 95.86.104.73 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1843 |
| 80.179.15.154 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1685 |
| 212.76.118.37 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1650 |
| 2.54.187.12 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1532 |
| 149.88.100.211 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1532 |
| 85.64.123.186 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1528 |
| 5.29.88.18 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1438 |
| 212.179.61.125 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1357 |
| 71.239.223.59 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1350 |
| 91.135.102.169 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1347 |
| 212.76.102.182 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1334 |
| 46.19.86.247 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1312 |
| 46.19.85.254 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1277 |
| 82.145.220.14 | Europe | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1204 |
| 2.54.163.32 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1192 |
| 212.179.42.225 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1166 |
| 46.19.86.239 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1136 |
| 46.19.85.103 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 1101 |
| 2.54.23.186 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 975 |
| 84.228.85.49 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 883 |
| 185.26.180.145 | Europe | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 853 |
| 147.236.238.10 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 821 |
| 84.109.235.23 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 806 |
| 2.54.33.146 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 800 |
| 84.228.120.243 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 788 |
| 95.86.123.136 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 750 |
| 46.210.102.84 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 748 |
| 212.179.61.122 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 739 |
| 212.179.21.198 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 699 |
| 107.170.144.19 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 679 |
| 212.76.114.70 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 673 |
| 162.243.61.230 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 647 |
| 46.19.86.91 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 635 |
| 162.243.225.144 | United States | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 630 |
| 82.145.222.117 | Europe | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 626 |
| 84.229.36.169 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 614 |
| 79.180.135.192 | Israel | 147.237.77.216 | dover.idf.il | First packet isn't SYN | drop | drop | 598 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Name | Device Action | Count |
|------------------|------------------|----------------|------------------|--|---------------|-------|
| 78.46.174.55 | Germany | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 78.46.174.55 | Block | 436 |
| 2.54.152.248 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 2.54.152.248 | Block | 259 |
| 2.54.41.59 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 248 |
| 2.54.11.137 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 2.54.11.137 | Block | 157 |
| 78.46.174.55 | Germany | 147.237.72.166 | aka.idf.il | Multiple Illegal HTTP Version from 78.46.174.55 | Block | 155 |
| 78.46.174.55 | Germany | 147.237.72.166 | aka.idf.il | Multiple Abnormally Long Request from 78.46.174.55 | Block | 155 |
| 46.19.86.173 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 46.19.86.173 | Block | 129 |
| 176.12.139.46 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 65 |
| 109.64.61.118 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 48 |
| 93.173.169.92 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd | Block | 42 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 38 |
| 79.180.12.16 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp | Block | 34 |
| 31.154.9.62 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 31.154.9.62 | Block | 26 |
| 66.249.79.74 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.79.74 | Block | 26 |
| 66.249.79.66 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.79.66 | Block | 19 |
| 213.151.45.157 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd | Block | 18 |
| 46.19.86.145 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd | Block | 16 |
| 82.80.141.94 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd | Block | 14 |
| 194.116.233.62 | Ukraine | 147.237.77.216 | dover.idf.il | Distributed Extremely Long HTTP Request | Block | 13 |
| 194.116.233.62 | Ukraine | 147.237.77.216 | dover.idf.il | Distributed Illegal Byte Code Character in Method | Block | 13 |
| 46.19.85.252 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 46.19.85.252 | Block | 12 |
| 37.26.148.189 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd | Block | 11 |
| 109.67.114.84 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd | Block | 10 |
| 212.179.155.129 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd | Block | 9 |
| 82.80.196.44 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized HTTP Method | Block | 9 |
| 79.179.102.178 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd | Block | 9 |
| 85.65.25.86 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd | Block | 9 |
| 79.178.103.138 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd | Block | 9 |
| 212.199.133.77 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd | Block | 9 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 8 |
| 66.249.67.55 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/m/ | Block | 8 |
| 5.29.47.68 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd | Block | 8 |
| 66.249.64.59 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 7 |
| 79.183.152.179 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd | Block | 7 |
| 93.172.169.104 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined | Block | 7 |
| 109.186.172.25 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 7 |
| 176.12.142.222 | Israel | 147.237.77.243 | mobile.idf.il | Suspicious Response Code | Block | 7 |
| 109.67.119.113 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd | Block | 7 |
| 79.179.131.118 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 7 |
| 157.55.39.81 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 157.55.39.81 | Block | 6 |
| 84.108.145.2 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 6 |
| 157.55.39.251 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 6 |
| 157.55.39.6 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 6 |
| 46.119.113.155 | Ukraine | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/getfile/ | Block | 6 |
| 212.76.115.99 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd | Block | 6 |
| 157.55.39.3 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 6 |
| 85.65.213.217 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 6 |
| 157.55.39.252 | United States | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 5 |
| 81.218.33.77 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd | Block | 5 |
| 65.208.151.117 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+ | Block | 5 |