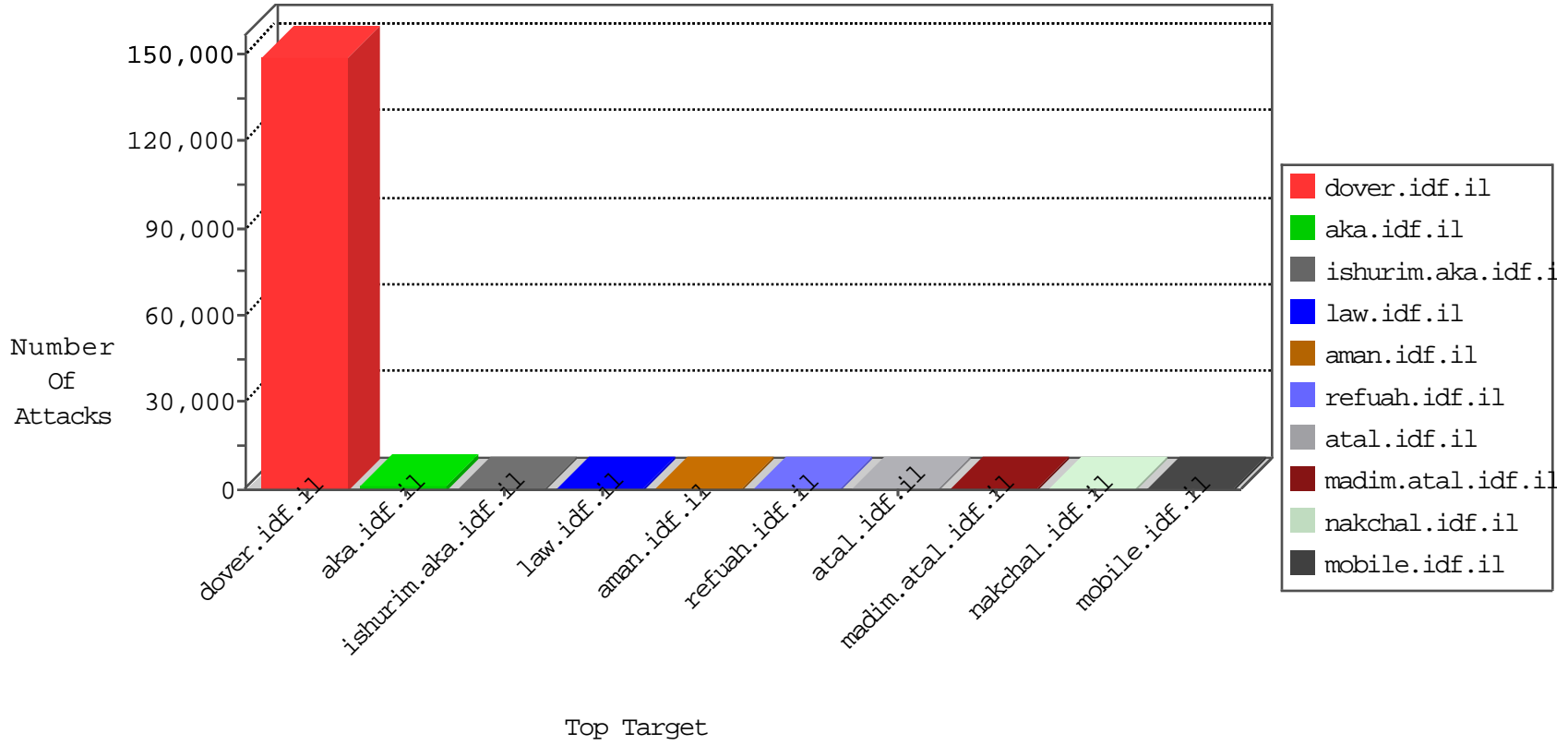


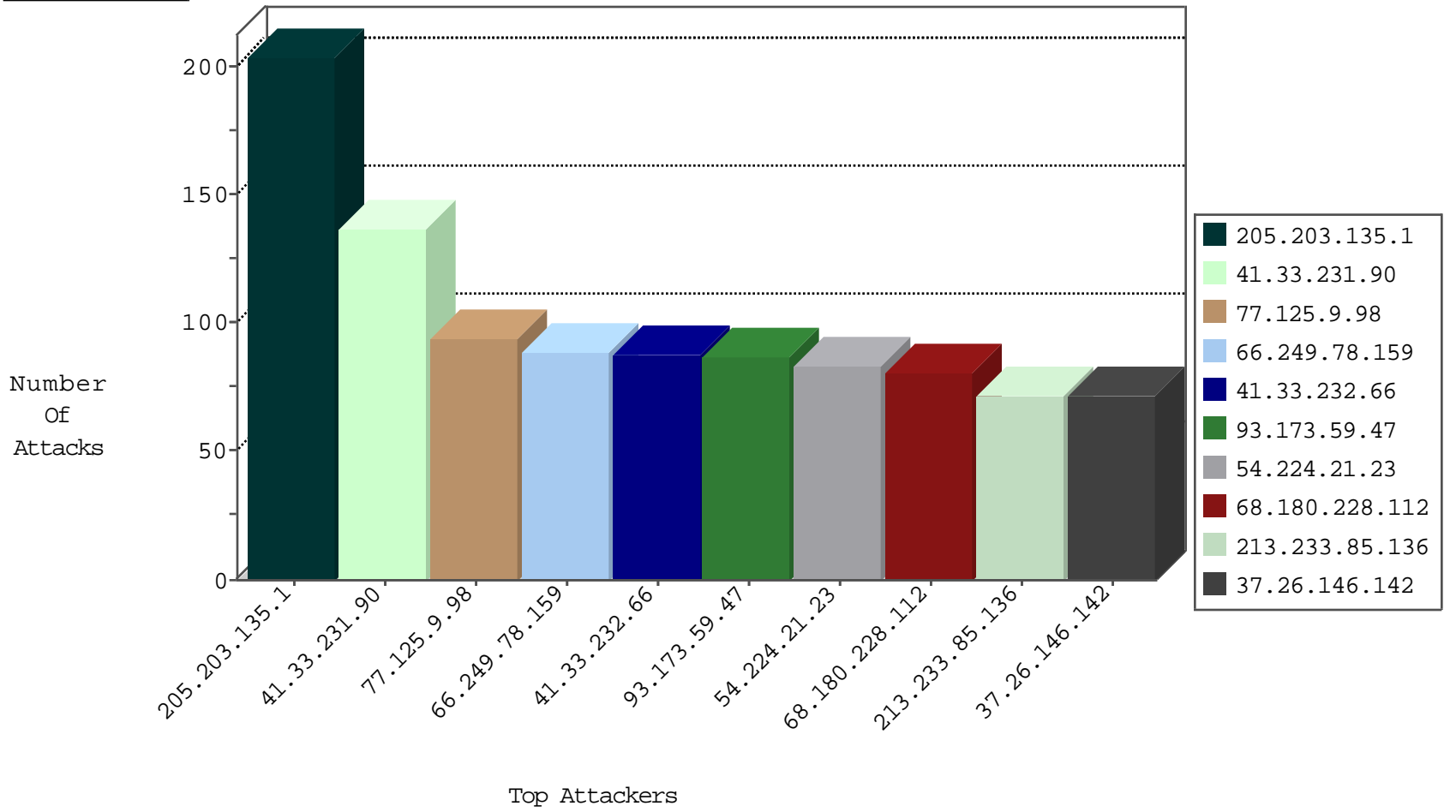
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country   | Target Address | Site               | Signature                                     | Device Action | Count |
|------------------|--------------------|----------------|--------------------|---|---------------|-------|
| 66.249.64.181    | United States      | 147.237.77.74  | law.idf.il         | TCP handshake violation, first packet not syn | drop          | 9831  |
| 186.8.127.114    | Uruguay            | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 3115  |
| 122.137.89.68    | China              | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 2947  |
| 45.218.117.20    | Uruguay            | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 2761  |
| 179.130.48.66    | Brazil             | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 2693  |
| 177.86.177.89    | Brazil             | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 2625  |
| 202.243.136.64   | Japan              | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 478   |
| 93.173.59.47     | Israel             | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 441   |
| 66.249.78.146    | United States      | 147.237.72.166 | aka.idf.il         | TCP handshake violation, first packet not syn | drop          | 419   |
| 194.95.76.31     | Germany            | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 338   |
| 115.14.118.92    | Korea, Republic of | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 279   |
| 46.10.127.41     | Bulgaria           | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 177   |
| 204.93.154.216   | United States      | 147.237.77.216 | dover.idf.il       | TCP Scan (vertical)                           | drop          | 169   |
| 126.23.239.46    | Japan              | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 156   |
| 121.62.212.57    | China              | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 115   |
| 119.216.235.82   | Korea, Republic of | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 90    |
| 110.13.51.22     | Korea, Republic of | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 81    |
| 183.98.141.65    | Korea, Republic of | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 75    |
| 58.230.132.26    | Korea, Republic of | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 51    |
| 81.199.122.29    | Israel             | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 26    |
| 167.114.156.16   | Canada             | 147.237.77.216 | dover.idf.il       | DOS-Tool-SwitchbladG                          | dest-reset    | 18    |
| 219.156.172.98   | China              | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 7     |
| 62.219.254.22    | Israel             | 147.237.72.167 | ishurim.aka.idf.il | Block_Udp_All_Nets                            | drop          | 3     |
| 130.209.170.14   | United Kingdom     | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 3     |
| 81.218.206.82    | Israel             | 147.237.77.170 | maarachot.idf.il   | Block_Udp_All_Nets                            | drop          | 3     |
| 66.35.85.27      | United States      | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 3     |
| 212.180.166.24   | Poland             | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 2     |
| 149.78.21.82     | Israel             | 147.237.77.216 | dover.idf.il       | SYN Flood unverified cookie                   | drop          | 2     |
| 213.159.42.77    | Lithuania          | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 2     |
| 46.9.249.120     | Norway             | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 2     |
| 84.20.64.54      | Albania            | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 2     |
| 134.147.203.115  | Germany            | 147.237.76.34  | yohalan.idf.il     | Block_Ntp_All_Net                             | drop          | 2     |
| 69.6.129.30      | United States      | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 196.47.132.24    | Cote D'Ivoire      | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 46.19.86.28      | Israel             | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 1     |
| 85.236.235.120   | Austria            | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 156.26.21.69     | United States      | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 39.80.22.41      | China              | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 1     |
| 83.168.94.66     | Poland             | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 141.32.222.110   | Germany            | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 219.215.206.118  | Japan              | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 1     |
| 66.76.251.19     | United States      | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 104.162.139.15   | United States      | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 1     |
| 191.153.173.114  | Colombia           | 147.237.77.216 | dover.idf.il       | TCP handshake violation, first packet not syn | drop          | 1     |
| 64.131.252.33    | United States      | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 96.30.239.117    | United States      | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 186.105.210.55   | Chile              | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 24.148.125.62    | United States      | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 78.136.77.39     | Spain              | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |
| 128.127.82.59    | Poland             | 147.237.77.216 | dover.idf.il       | Invalid TCP Flags                             | drop          | 1     |

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site                   | Signature                                  | Device Action | Count |
|------------------|------------------|----------------|------------------------|--|---------------|-------|
| 188.165.15.130   | France           | 147.237.77.74  | law.idf.il             | C228: HTTP: AhrefBot crawler               | Block         | 17    |
| 46.121.209.185   | Israel           | 147.237.76.31  | nakchal.idf.il         | C1000004: HTTP: options method (Microsoft) | Block         | 5     |
| 188.165.15.132   | France           | 147.237.77.176 | matpash.idf.il         | C228: HTTP: AhrefBot crawler               | Block         | 4     |
| 188.165.15.176   | France           | 147.237.76.86  | navy.idf.il            | C228: HTTP: AhrefBot crawler               | Block         | 3     |
| 188.165.15.201   | France           | 147.237.77.216 | dover.idf.il           | C228: HTTP: AhrefBot crawler               | Block         | 3     |
| 69.30.215.142    | United States    | 147.237.77.226 | www.chamatz.aka.idf.il | C1000106: HTTP: majestic bot               | Block         | 1     |
| 151.80.31.147    | Italy            | 147.237.0.34   | tikshuv.idf.il         | C228: HTTP: AhrefBot crawler               | Block         | 1     |
| 188.165.15.36    | France           | 147.237.77.170 | maarachot.idf.il       | C228: HTTP: AhrefBot crawler               | Block         | 1     |
| 188.165.15.127   | France           | 147.237.77.233 | atal.idf.il            | C228: HTTP: AhrefBot crawler               | Block         | 1     |
| 188.165.15.202   | France           | 147.237.76.30  | himush.idf.il          | C228: HTTP: AhrefBot crawler               | Block         | 1     |

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country   | Site             | Signature   | Count |
|------------------|----------------|--------------------|------------------|---|-------|
| 195.34.150.18    | 147.237.77.216 | Austria            | dover.idf.il     | Tehila - Perl LWP with fake user agent                                | 4     |
| 41.33.231.90     | 147.237.77.216 | Egypt              | dover.idf.il     | Tehila - Perl LWP with fake user agent                                | 3     |
| 176.13.0.96      | 147.237.77.233 | Israel             | atal.idf.il      | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack | 2     |
| 66.249.93.216    | 147.237.77.233 | United States      | atal.idf.il      | ET SCAN NMAP -sA (2)  | 2     |
| 79.176.152.75    | 147.237.77.216 | Israel             | dover.idf.il     | portscan: TCP Distributed Portscan                                    | 2     |
| 66.249.67.64     | 147.237.76.42  | United States      | refuah.idf.il    | ET SCAN NMAP -sA (2)  | 2     |
| 206.203.118.113  | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 148.248.148.12   | 147.237.77.216 | Mexico             | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 128.199.104.9    | 147.237.77.216 | Singapore          | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 139.167.175.96   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 89.114.9.113     | 147.237.77.216 | Portugal           | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 95.217.14.114    | 147.237.77.216 | Ukraine            | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 167.28.179.45    | 147.237.77.216 | Chile              | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 134.209.159.98   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 64.44.71.2       | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 198.48.19.85     | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 147.50.72.48     | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 148.178.222.53   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 128.168.157.98   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 170.113.245.51   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 139.167.34.56    | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 84.108.187.164   | 147.237.77.216 | Israel             | dover.idf.il     | portscan: TCP Distributed Portscan                                    | 1     |
| 204.236.11.44    | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 159.223.196.90   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 134.172.146.58   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 62.182.156.95    | 147.237.77.216 | Ukraine            | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 193.104.94.12    | 147.237.77.216 | Russian Federation | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 143.135.245.2    | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 95.216.135.11    | 147.237.77.216 | Ukraine            | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 128.168.82.43    | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 170.106.253.88   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 138.43.216.17    | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 79.110.182.111   | 147.237.77.216 | Russian Federation | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 204.106.222.76   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 148.178.57.81    | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 157.232.179.87   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 134.172.80.30    | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 40.115.58.160    | 147.237.8.50   | United States      | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024  | 1     |
| 192.219.202.122  | 147.237.77.216 | Canada             | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 143.135.202.93   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 94.131.138.114   | 147.237.77.216 | Russian Federation | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 170.106.98.15    | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 138.43.169.31    | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 204.93.154.216   | 147.237.77.216 | United States      | dover.idf.il     | portscan: TCP Distributed Portscan                                    | 1     |
| 148.105.232.24   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 128.168.19.118   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 134.172.48.1     | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 5.102.255.227    | 147.237.77.216 | Israel             | dover.idf.il     | portscan: TCP Distributed Portscan                                    | 1     |
| 192.112.120.120  | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |
| 143.135.141.34   | 147.237.77.216 | United States      | dover.idf.il     | ET DROP Spamhaus DROP Listed Traffic Inbound                          | 1     |

## Top Attackers In FW

| Attacker Address | Attacker Country   | Target Address | Site               | Signature                                    | Message   | Device Action | Count |
|------------------|--------------------|----------------|--------------------|--|---|---------------|-------|
| 205.203.135.1    | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 204   |
| 41.33.231.90     | Egypt              | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 99    |
| 41.33.232.66     | Egypt              | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 88    |
| 54.224.21.23     | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 83    |
| 68.180.228.112   | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 80    |
| 37.26.146.142    | Israel             | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 72    |
| 213.233.85.136   | Romania            | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 70    |
| 108.56.149.42    | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 68    |
| 66.249.78.159    | United States      | 147.237.77.216 | dover.idf.il       | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 63    |
| 77.125.9.98      | Israel             | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 61    |
| 109.200.30.154   | United Kingdom     | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 60    |
| 37.238.176.5     | Iraq               | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 60    |
| 52.16.5.197      | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 52    |
| 37.26.146.214    | Israel             | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 46    |
| 157.56.2.63      | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 45    |
| 54.72.0.55       | Ireland            | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 41    |
| 54.72.73.168     | Ireland            | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 41    |
| 46.19.85.122     | Israel             | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence                             | Invalid ACK number                              | monitor       | 37    |
| 37.26.146.166    | Israel             | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 36    |
| 149.78.154.69    | Israel             | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 35    |
| 60.225.38.100    | Australia          | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 34    |
| 62.44.135.129    | Denmark            | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 34    |
| 195.34.150.18    | Austria            | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 33    |
| 41.33.231.90     | Egypt              | 147.237.77.216 | dover.idf.il       | drop   |   | drop          | 32    |
| 85.250.22.48     | Israel             | 147.237.76.42  | refuah.idf.il      | Bad TCP sequence                             | SYN retransmit with different window scale      | monitor       | 32    |
| 188.165.15.130   | France             | 147.237.77.74  | law.idf.il         | drop   | SAM rule  | drop          | 31    |
| 77.125.9.98      | Israel             | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 30    |
| 66.249.78.166    | Israel             | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 29    |
| 50.87.144.145    | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 25    |
| 82.192.68.46     | Netherlands        | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 25    |
| 93.173.59.47     | Israel             | 147.237.76.31  | nakchal.idf.il     | Bad TCP sequence                             | SYN retransmit with different window scale      | monitor       | 25    |
| 93.173.59.47     | Israel             | 147.237.77.216 | dover.idf.il       | Bad TCP sequence                             | SYN retransmit with different window scale      | monitor       | 23    |
| 65.49.68.158     | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 23    |
| 100.100.99.41    |                    | 147.237.72.166 | aka.idf.il         | drop   | First packet isn't SYN                          | drop          | 22    |
| 157.55.39.19     | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 22    |
| 66.249.78.173    | Israel             | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 21    |
| 204.93.154.216   | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 21    |
| 95.147.171.58    | United Kingdom     | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 20    |
| 188.165.15.233   | France             | 147.237.72.166 | aka.idf.il         | drop   | SAM rule  | drop          | 18    |
| 66.249.78.159    | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 18    |
| 157.55.39.13     | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 17    |
| 100.100.123.66   |                    | 147.237.72.166 | aka.idf.il         | drop   | First packet isn't SYN                          | drop          | 17    |
| 70.39.185.40     | Satellite Provider | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 15    |
| 100.100.48.246   |                    | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 15    |
| 100.100.106.190  |                    | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 13    |
| 40.77.167.34     | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 13    |
| 128.242.249.10   | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 13    |
| 109.64.110.34    | Israel             | 147.237.72.166 | aka.idf.il         | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop          | 12    |
| 104.131.197.228  | United States      | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 12    |
| 93.173.59.47     | Israel             | 147.237.77.216 | dover.idf.il       | drop   | First packet isn't SYN                          | drop          | 12    |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site                | Signature   | Device Action | Count |
|------------------|------------------|----------------|---------------------|---|---------------|-------|
| 46.19.86.52      | Israel           | 147.237.0.19   | madim.atal.idf.il   | Distributed Suspicious Response Code  | Block         | 33    |
| 149.88.124.126   | Israel           | 147.237.0.19   | madim.atal.idf.il   | Distributed Suspicious Response Code  | Block         | 5     |
| 213.251.182.103  | France           | 147.237.77.176 | matpash.idf.il      | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src                        | Block         | 3     |
| 46.117.9.188     | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 2     |
| 2.54.158.237     | Israel           | 147.237.77.216 | dover.idf.il        | Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx  | Block         | 2     |
| 109.67.252.179   | Israel           | 147.237.72.166 | aka.idf.il          | Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp                                      | None          | 1     |
| 85.250.22.48     | Israel           | 147.237.76.42  | refuah.idf.il       | Unauthorized URL Access to 147.237.76.42/style/shared/960.css   | Block         | 1     |
| 79.176.36.144    | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 157.55.39.108    | United States    | 147.237.76.86  | navy.idf.il         | Multiple Unauthorized URL Access from 157.55.39.108   | Block         | 1     |
| 66.249.64.181    | Israel           | 147.237.77.74  | law.idf.il          | Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp                                    | Block         | 1     |
| 31.210.189.18    | Israel           | 147.237.0.19   | madim.atal.idf.il   | Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx                             | Block         | 1     |
| 94.159.247.150   | Israel           | 147.237.77.234 | halag.idf.il        | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif   | Block         | 1     |
| 79.183.104.38    | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 68.180.228.112   | United States    | 147.237.77.216 | dover.idf.il        | Distributed Suspicious Response Code  | Block         | 1     |
| 185.49.14.190    | Poland           | 147.237.77.235 | sviva.idf.il        | Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php   | Block         | 1     |
| 46.117.9.188     | Israel           | 147.237.77.234 | halag.idf.il        | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif                               | Block         | 1     |
| 85.250.22.48     | Israel           | 147.237.77.233 | atal.idf.il         | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx   | Block         | 1     |
| 216.218.206.66   | United States    | 147.237.72.167 | ishurim.aka.idf.il  | Unauthorized URL Access to 147.237.72.167/  | Block         | 1     |
| 79.176.180.100   | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 66.249.78.146    | Israel           | 147.237.72.166 | aka.idf.il          | Unknown Parameter pop in www.aka.idf.il/main/home/  | None          | 1     |
| 176.12.144.213   | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 46.19.85.94      | Israel           | 147.237.77.234 | halag.idf.il        | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif                               | Block         | 1     |
| 109.65.53.176    | Israel           | 147.237.72.166 | aka.idf.il          | Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/   | Block         | 1     |
| 80.246.136.198   | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 68.180.229.94    | United States    | 147.237.0.15   | kosher-kravi.idf.il | Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/                     | Block         | 1     |
| 199.203.240.37   | Israel           | 147.237.76.31  | nakchal.idf.il      | Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc                             | Block         | 1     |
| 149.88.139.154   | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 46.117.88.93     | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 93.172.176.164   | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 79.178.58.52     | Israel           | 147.237.72.166 | aka.idf.il          | Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx                  | None          | 1     |
| 66.249.78.234    | Israel           | 147.237.72.166 | aka.idf.il          | Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/general.aspx                                  | Block         | 1     |
| 185.49.14.190    | Poland           | 147.237.77.19  | law-forum.idf.il    | Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php  | Block         | 1     |
| 109.67.102.7     | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 80.246.139.80    | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 207.46.13.66     | United States    | 147.237.77.216 | dover.idf.il        | Unauthorized URL Access to www.idf.il/1589-en/dover.aspxthe   | Block         | 1     |
| 68.180.230.224   | United States    | 147.237.76.31  | nakchal.idf.il      | Parameter Type Violation PageNum in www.nakchal.idf.il/1073-he/nakchal.aspx                                   | Block         | 1     |
| 157.55.39.40     | United States    | 147.237.77.176 | matpash.idf.il      | Unauthorized URL Access to 147.237.77.176/  | Block         | 1     |
| 46.117.232.190   | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 93.173.59.47     | Israel           | 147.237.76.31  | nakchal.idf.il      | Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc   | Block         | 1     |
| 79.181.112.206   | Israel           | 147.237.72.156 | aman.idf.il         | Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/   | Block         | 1     |
| 66.249.93.139    | Israel           | 147.237.77.234 | halag.idf.il        | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif                               | Block         | 1     |
| 185.49.14.190    | Poland           | 147.237.77.216 | dover.idf.il        | Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php  | Block         | 1     |
| 46.19.86.193     | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 109.67.197.57    | Israel           | 147.237.72.166 | aka.idf.il          | Untraceable SSL Sessions: sigalgs DoS Attack  | None          | 1     |
| 84.108.7.140     | Israel           | 147.237.77.74  | law.idf.il          | Parameter Type Violation Master\$Header1\$ucHeaderSearch\$txtSearch in www.law.idf.il/421-2258-he/patzar.aspx | Block         | 1     |
| 207.46.13.105    | United States    | 147.237.76.42  | refuah.idf.il       | Unauthorized URL Access to 147.237.76.42/   | Block         | 1     |
| 77.125.11.108    | Israel           | 147.237.72.166 | aka.idf.il          | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/  | Block         | 1     |
| 157.55.39.48     | United States    | 147.237.72.166 | aka.idf.il          | Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx  | None          | 1     |
| 66.249.64.177    | Israel           | 147.237.76.147 | chinuch.aka.idf.il  | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm   | Block         | 1     |
| 2.54.158.237     | Israel           | 147.237.77.233 | atal.idf.il         | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx   | Block         | 1     |