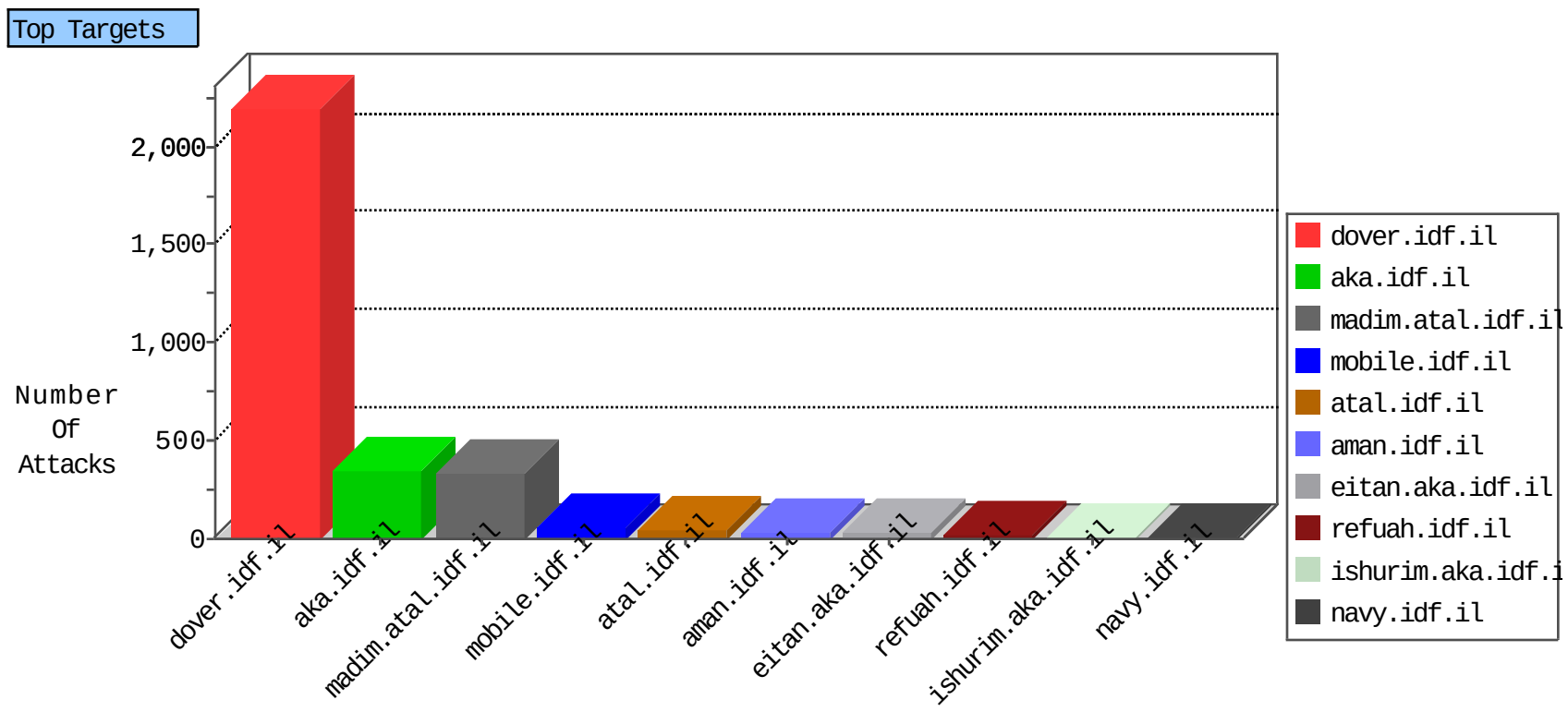
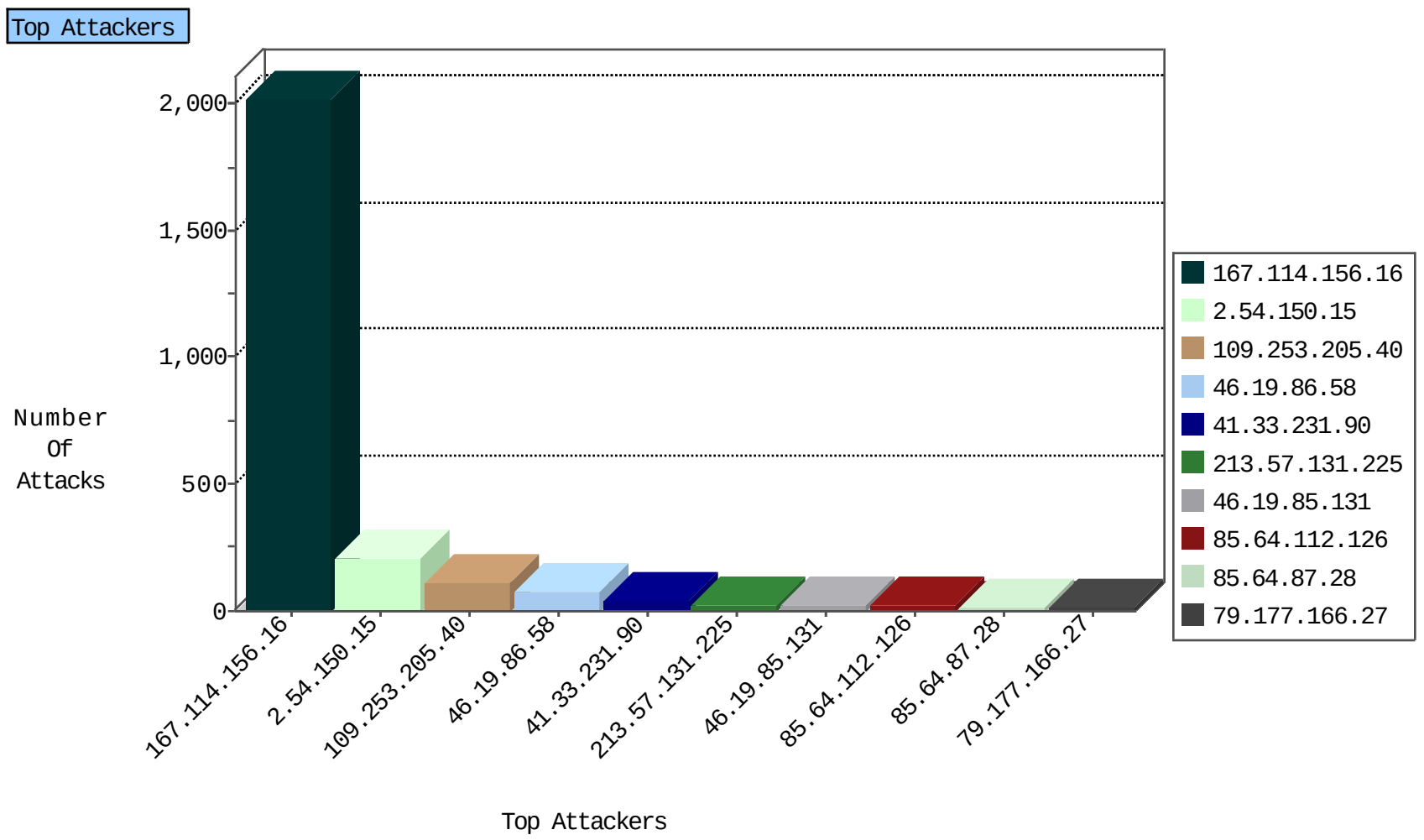
12-26-2015-21:04:05 to 12-26-2015-22:04:05

# IDF Under Attack Daily Report

Top Targets




Top Attackers



12-26-2015-21:04:05 to 12-26-2015-22:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3118 |
| 212.179.244.85 | Israel | 147.237.0.19 | madim.atal.idf.il | Block_Udp_All_Nets | drop | 1 |

12-26-2015-21:04:05 to 12-26-2015-22:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

12-26-2015-21:04:05 to 12-26-2015-22:04:05

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 |
| 175.3.70.6 | 147.237.76.177 | China | ncore.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 137.116.113.55 | 147.237.76.197 | United States | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 137.116.113.55 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 77.127.187.63 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 198.20.69.98 | 147.237.77.227 | United States | e.hamaz.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 177.239.209.102 | 147.237.76.34 | Mexico | yohalan.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 137.116.113.55 | 147.237.76.202 | United States | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 137.116.113.55 | 147.237.0.200 | United States | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 93.172.168.3 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

12-26-2015-21:04:05 to 12-26-2015-22:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 46.19.86.58 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 71 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 79.177.166.27 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 79.176.99.246 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 13 |
| 79.178.167.41 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 5.22.129.171 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 2.54.178.143 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 81.218.202.150 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 11 |
| 213.57.131.225 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 10 |
| 37.26.146.227 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.86.227 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 176.13.9.146 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 213.57.131.225 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 31.168.149.92 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 8 |
| 91.200.12.141 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 8 |
| 85.64.112.126 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 5.102.254.141 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 77.125.135.233 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.131 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 79.181.190.177 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.131 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 79.176.108.138 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.179.168.225 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.64.87.28 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 109.67.8.34 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.180.62.121 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.130.220.253 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 77.125.135.233 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.112 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 80.246.140.56 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.181.110.181 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.64.87.28 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 157.55.39.227 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.85.131 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 79.177.0.190 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 213.57.131.225 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 5 |
| 46.19.85.131 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 68.180.228.183 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.205 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 80.246.136.88 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 85.64.87.28 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | alert | 4 |
| 85.64.112.126 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 109.67.172.21 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 94.230.86.240 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 109.66.36.151 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.63.152 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.3.146.203 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 85.64.112.126 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | | monitor | 3 |

12-26-2015-21:04:05 to 12-26-2015-22:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.253.205.40 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 108 |
| 2.54.150.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 104 |
| 2.54.150.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 2.54.150.15 | Block | 85 |
| 2.54.150.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (403) in Session from 2.54.150.15 | Block | 21 |
| 46.117.24.3 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 5 |
| 79.177.122.43 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 4 |
| 77.125.75.187 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.147.207 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.9.146 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 84.109.71.160 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/giyus | Block | 3 |
| 23.254.243.147 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.146.227 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 31.168.119.31 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 31.168.119.31 | Block | 3 |
| 80.246.136.96 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.131 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation Email in mobile.idf.il/sachar/createaccount | Block | 3 |
| 85.64.86.85 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 31.168.182.99 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 2 |
| 176.13.8.14 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 2.54.178.143 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 185.110.111.180 |  | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â | Block | 2 |
| 5.29.104.57 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 2 |
| 46.117.143.79 | Israel | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx | Block | 2 |
| 37.26.147.130 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 197.221.14.187 | South Africa | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 5.29.118.194 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx | Block | 1 |
| 93.115.95.201 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.64.166 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/1098-he/nakhal.aspx | Block | 1 |
| 185.52.25.110 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 79.183.13.192 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |
| 46.19.86.153 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 142.4.213.25 | Canada | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 98.143.148.135 | United States | 147.237.76.31 | nakchal.idf.il | Unknown HTTP Request Method [[#1]]I20100 in URL | Block | 1 |
| 70.39.234.78 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 2.54.166.228 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 87.69.27.82 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 196.40.97.146 | South Africa | 147.237.77.170 | maarachot.idf.il | Distributed PHP Attempt | Block | 1 |
| 46.166.137.205 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 84.94.80.157 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 109.186.44.48 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 77.125.135.233 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 68.180.229.173 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 197.221.14.187 | South Africa | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 8.37.71.74 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/&usg=alkjrhhecjl0lmzjmq9jdxmsqwpmt_ga2g | Block | 1 |
| 93.115.116.100 | Romania | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 85.64.87.28 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |

12-26-2015-21:04:05 to 12-26-2015-22:04:05