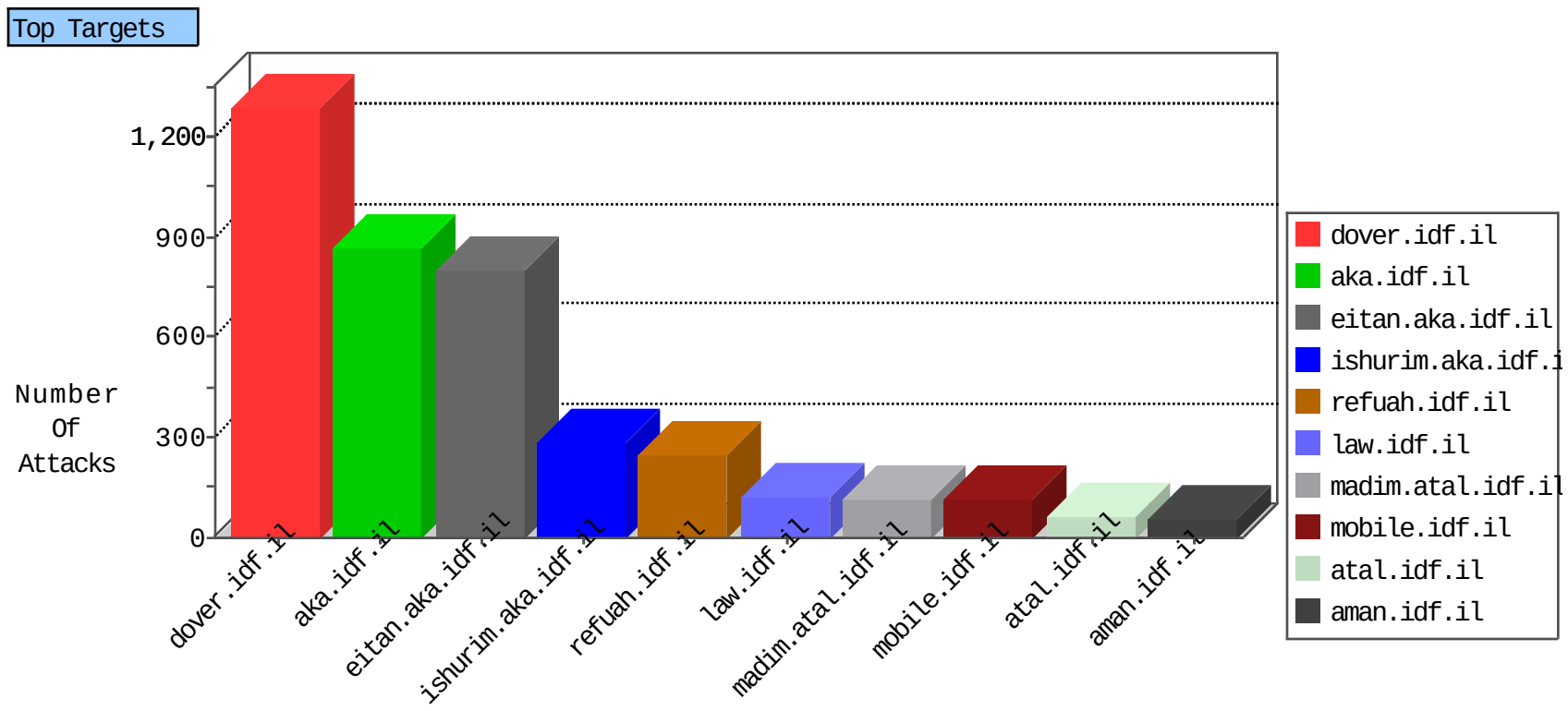
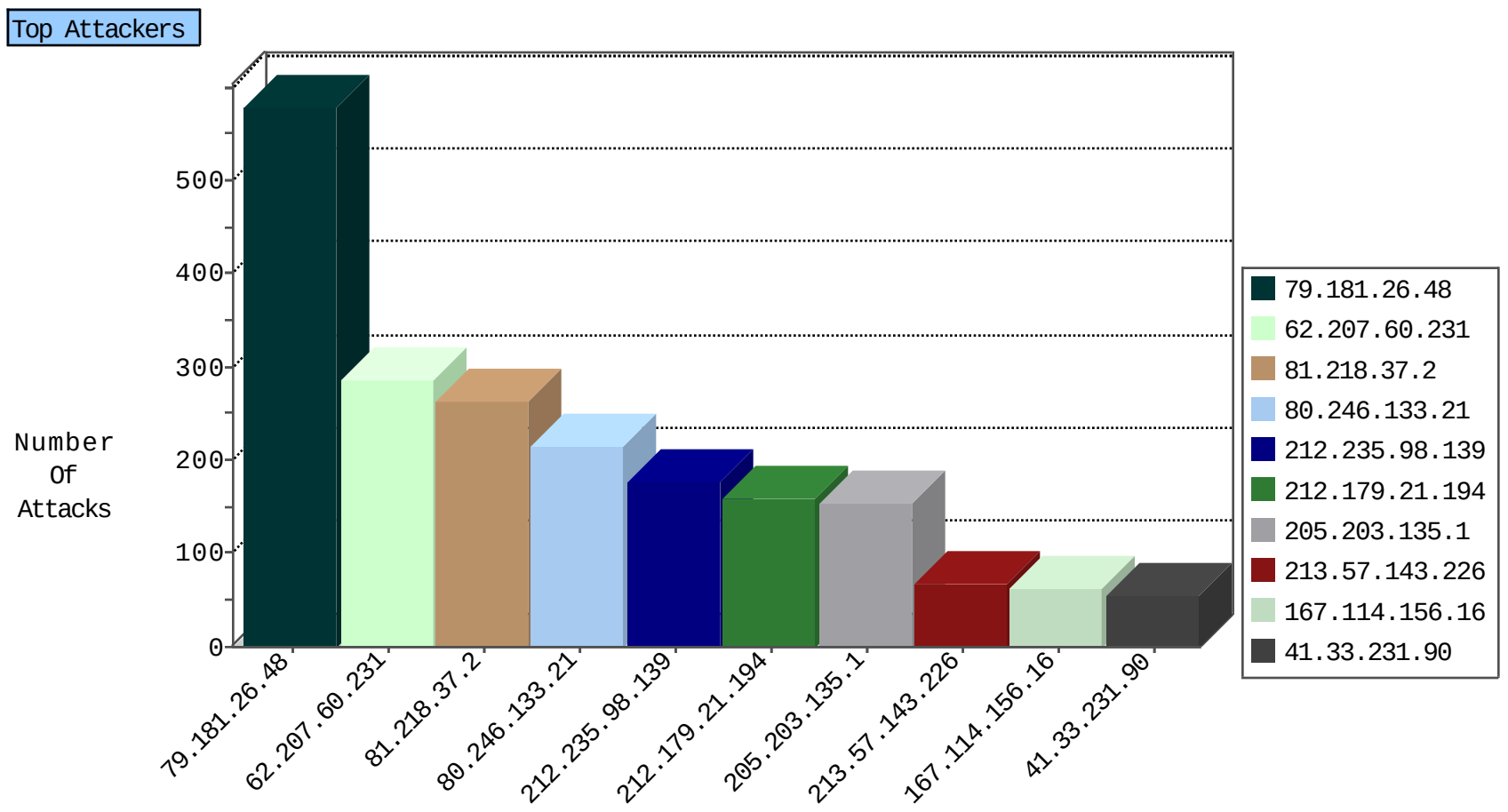
11-24-2015-14:04:05 to 11-24-2015-15:04:05

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



11-24-2015-14:04:05 to 11-24-2015-15:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.78.82 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 3453 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3114 |
| 81.218.37.2 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 1434 |
| 81.218.37.2 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | forward | 126 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 118 |
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 105 |
| 109.64.113.250 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 5 |
| 79.180.134.246 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 95.221.215.76 | Russian Federation | 147.237.76.200 | eitan.aka.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 95.221.215.76 | Russian Federation | 147.237.76.200 | eitan.aka.idf.il | JLM_Under_Attack_Con_Http | drop | 2 |
| 114.80.122.91 | China | 147.237.76.34 | yohalan.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.199 | e.nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.44 | e.refuah.idf.il | Block_Ntp_All_Net | drop | 1 |
| 178.130.36.10 | Russian Federation | 147.237.76.34 | yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 114.80.122.91 | China | 147.237.76.177 | ncore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.38 | e.e.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.202 | e.halag.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.86 | navy.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.196 | e.sviva.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.39 | mobile.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |
| 92.96.102.111 | United Arab Emirates | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 114.80.122.91 | China | 147.237.76.147 | chinuch.aka.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.31 | nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.197 | e.himush.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.42 | refuah.idf.il | Block_Ntp_All_Net | drop | 1 |
| 114.80.122.91 | China | 147.237.76.176 | test.ncore.idf.il | Block_Ntp_All_Net | drop | 1 |

11-24-2015-14:04:05 to 11-24-2015-15:04:05

## Top Attackers In IPS

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

11-24-2015-14:04:05 to 11-24-2015-15:04:05

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 79.176.114.119 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.57.50.233 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 74.117.209.135 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 198.20.69.98 | 147.237.77.216 | United States | dover.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 46.120.73.186 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 176.13.12.202 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.102.254.157 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 128.199.95.16 | 147.237.77.179 | Singapore | e.mazi.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 2.52.15.146 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.64.154.243 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 93.173.168.230 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.69.35.77 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.246.138.237 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 222.223.11.35 | 147.237.76.39 | China | mobile.meitav.idf.il | GPL SCAN nmap TCP | 1 |
| 74.117.209.135 | 147.237.77.243 | United States | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 208.80.155.223 | 147.237.77.216 | United States | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 66.249.78.96 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 46.116.113.187 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 176.12.142.19 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.28.172.160 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.253.87.163 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.102.60.175 | 147.237.0.16 | Netherlands | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 90.2.140.139 | 147.237.72.166 | France | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 84.94.119.108 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

11-24-2015-14:04:05 to 11-24-2015-15:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 79.181.26.48 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 513 |
| 80.246.133.21 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 214 |
| 62.207.60.231 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 200 |
| 212.235.98.139 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 177 |
| 205.203.135.1 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 153 |
| 81.218.37.2 | Israel | 147.237.72.167 | ishurim.aka.idf.i | drop | First packet isn't SYN | drop | 112 |
| 62.207.60.231 | Netherlands | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 86 |
| 212.179.21.194 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 80 |
| 213.57.143.226 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 65 |
| 66.249.81.212 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 54 |
| 100.100.41.196 |  | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 54 |
| 69.191.176.31 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 48 |
| 213.57.130.121 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 38 |
| 95.221.215.76 | Russian Federation | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 36 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 34 |
| 66.249.81.218 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 32 |
| 100.100.115.183 |  | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 29 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 27 |
| 2.54.132.180 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 27 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 24 |
| 52.34.154.234 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 79.178.177.75 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 22 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 66.249.81.215 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 208.115.111.68 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 21 |
| 82.233.248.204 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 136.243.5.203 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 37.26.148.174 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 100.100.83.113 |  | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 100.100.74.119 |  | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 16 |
| 157.55.39.67 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 2.52.57.96 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 2.52.15.26 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 100.100.77.33 |  | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 13 |
| 80.246.133.102 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 100.100.12.170 |  | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 81.218.241.25 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 107.170.61.36 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 139.162.216.112 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 79.182.109.238 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 80.246.133.102 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 212.179.42.66 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 11 |
| 207.46.13.17 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 213.57.130.121 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 10 |
| 66.249.79.75 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 87.203.98.130 | Greece | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |

11-24-2015-14:04:05 to 11-24-2015-15:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 212.179.21.194 | Israel | 147.237.76.200 | eitan.aka.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 78 |
| 79.181.26.48 | Israel | 147.237.76.200 | eitan.aka.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 66 |
| 176.12.145.144 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 29 |
| 46.19.86.67 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 25 |
| 176.13.3.232 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 22 |
| 212.199.53.161 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 9 |
| 2.54.132.180 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 7 |
| 46.19.86.153 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 84.229.55.183 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 2.52.15.26 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 84.108.97.237 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 5 |
| 185.32.179.79 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 2.54.46.245 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 2.54.148.235 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465 | Block | 3 |
| 54.244.22.103 | United States | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 3 |
| 46.19.86.60 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.8.47 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431 | Block | 3 |
| 185.32.179.149 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.49 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.64.219.41 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 2 |
| 185.32.179.215 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.121.92.46 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 46.19.85.175 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx | Block | 2 |
| 2.54.10.176 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 213.151.35.218 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 212.143.220.92 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/igf | Block | 2 |
| 185.27.105.96 | Israel | 147.237.77.74 | law.idf.il | Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/801-he/patzar.aspx | Block | 2 |
| 93.173.249.242 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 2 |
| 46.19.86.233 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 80.246.136.222 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 176.106.227.137 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 2 |
| 79.176.26.194 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 176.12.144.169 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.178.120.157 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser | Block | 2 |
| 212.150.214.90 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 2 |
| 46.121.46.192 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 109.67.213.1 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 82.80.230.199 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/smalim/undefined | Block | 1 |
| 208.184.112.75 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 79.178.177.75 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 178.215.213.206 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 93.172.64.195 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/ | Block | 1 |
| 221.231.6.246 | China | 147.237.76.30 | himush.idf.il | Unauthorized URL Access to 147.237.76.30/ | Block | 1 |
| 66.249.66.126 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/robots.txt | Block | 1 |
| 85.64.173.189 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/ | Block | 1 |
| 84.228.59.142 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/ | Block | 1 |
| 54.183.185.124 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to 147.237.76.86/ | Block | 1 |
| 152.62.109.206 | Europe | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/favicon.ico | Block | 1 |
| 46.19.86.99 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 80.230.19.43 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |

11-24-2015-14:04:05 to 11-24-2015-15:04:05