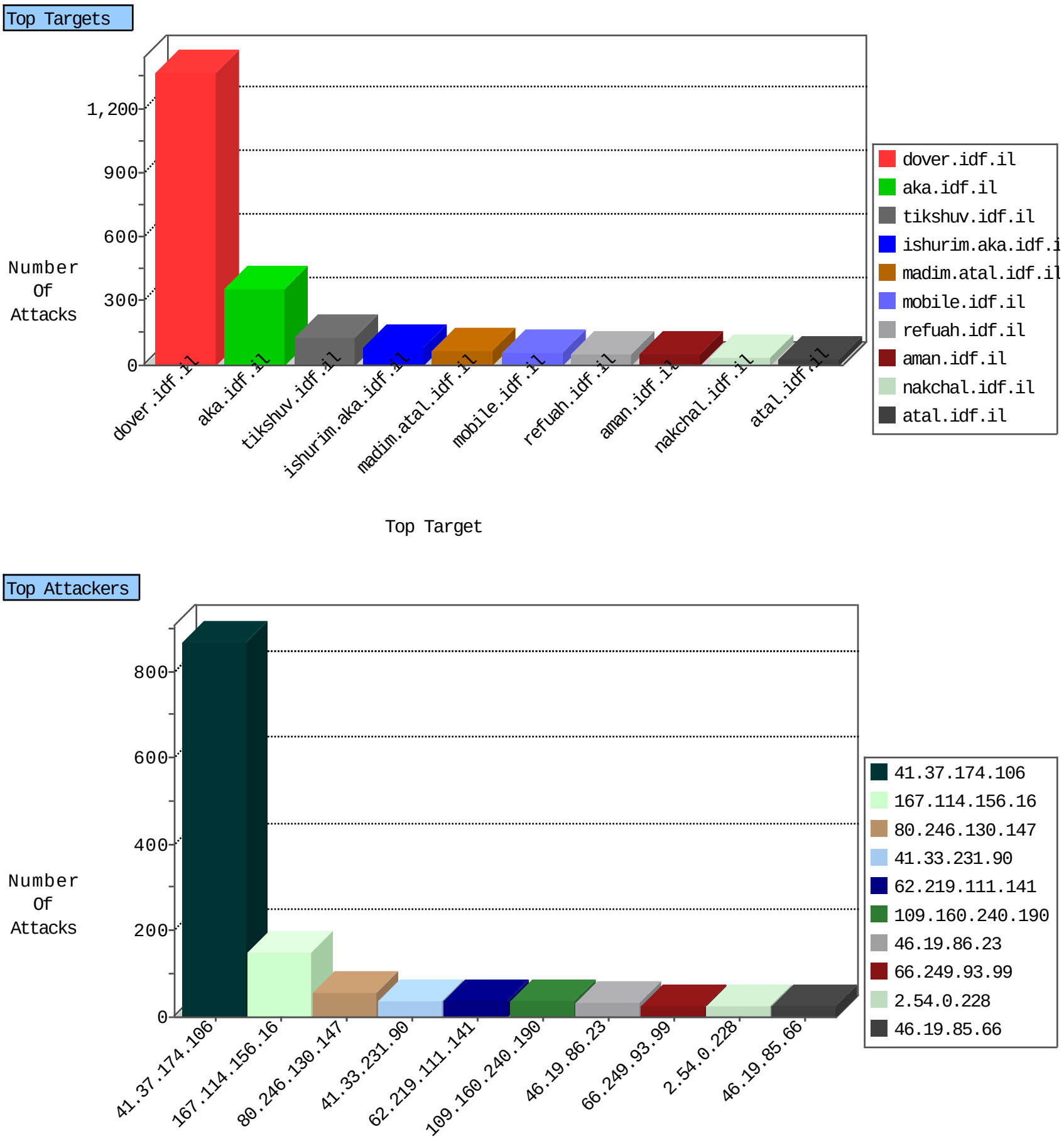
12-29-2015-10:04:07 to 12-29-2015-11:04:07

# IDF Under Attack Daily Report



12-29-2015-10:04:07 to 12-29-2015-11:04:07

## 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 | 3124 |
| 192.118.30.102 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 196 |
| 66.249.93.99 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 20 |
| 66.249.93.103 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 11 |
| 130.211.164.37 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 6 |
| 37.26.146.191 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 6 |
| 109.67.107.129 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 5 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | F_Dover_Under_Attack_Con_Http | drop | 5 |
| 207.46.13.122 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 37.26.149.217 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 31.168.133.226 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 40.77.167.77 | United States | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 3 |
| 37.26.149.210 | Israel | 147.237.72.156 | aman.idf.il | Invalid TCP Flags | drop | 2 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 2 |
| 107.150.98.131 | United States | 147.237.76.34 | yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 77.247.178.132 | Netherlands | 147.237.76.31 | nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 162.213.153.152 | United States | 147.237.76.38 | e.e.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |

12-29-2015-10:04:07 to 12-29-2015-11:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 41.37.174.106 | Egypt | 147.237.77.216 | dover.idf.il | C091: HTTP: Access to - admin.asp | Block | 43 |
| 41.37.174.106 | Egypt | 147.237.77.216 | dover.idf.il | C023: HTTP: administrator in URI | Permit | 4 |
| 41.37.174.106 | Egypt | 147.237.77.216 | dover.idf.il | C003: HTTP: phpMyAdmin access | Block | 2 |

12-29-2015-10:04:07 to 12-29-2015-11:04:07

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 37.26.149.210 | 147.237.72.156 | Israel | aman.idf.il | POLICY-OTHER TCP packet with urgent flag attempt | 6 |
| 41.37.174.106 | 147.237.77.216 | Egypt | dover.idf.il | SERVER-WEBAPP admin.php access | 5 |
| 41.37.174.106 | 147.237.77.216 | Egypt | dover.idf.il | SERVER-WEBAPP adminlogin access | 5 |
| 41.37.174.106 | 147.237.77.216 | Egypt | dover.idf.il | Admin login page scan - Havij | 4 |
| 41.37.174.106 | 147.237.77.216 | Egypt | dover.idf.il | SERVER-WEBAPP login.htm access | 3 |
| 82.166.65.18 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.199.185.108 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.142.163.10 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 37.26.147.238 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 176.106.42.131 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.0.228 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 151.217.178.88 | 147.237.72.166 |  | aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 131.109.15.15 | 147.237.76.200 | United States | eitan.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 84.94.23.53 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.93.249 | 147.237.72.166 | United States | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.57.181.80 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 195.95.183.254 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.161.246.102 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.29.6 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 176.13.2.210 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 151.217.178.55 | 147.237.0.15 |  | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 112.16.76.209 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

12-29-2015-10:04:07 to 12-29-2015-11:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 62.219.111.141 | Israel | 147.237.72.167 | ishurim.aka.idf.i | drop | First packet isn't SYN | drop | 34 |
| 46.19.85.66 | Israel | 147.237.76.31 | nakchal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 192.118.27.253 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 217.132.97.135 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 212.179.223.204 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 188.143.232.24 | Russian Federation | 147.237.72.156 | aman.idf.il | drop | SAM rule | drop | 11 |
| 212.150.255.134 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 10 |
| 109.160.240.190 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 10 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 217.194.206.108 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 109.160.240.190 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 46.19.85.90 | Israel | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 9 |
| 66.249.64.119 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 62.0.200.211 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 8 |
| 130.203.136.75 | United States | 147.237.77.74 | law.idf.il | Web Server Enforcement Violation | Web Servers Slow HTTP Denial of Service | reject | 8 |
| 218.213.70.136 | Hong Kong | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 212.235.43.9 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 8 |
| 176.13.20.132 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 37.26.146.191 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 79.177.132.122 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 7 |
| 141.0.15.13 | Europe | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.137 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 149.78.56.175 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.179 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 80.178.200.3 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.140 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.82 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.170 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 85.65.87.174 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.12.147.98 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.210.157.56 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 46.19.85.35 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 62.219.225.40 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.22.65 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.82 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.54.11.171 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.67 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.170 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.52.161.0 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 37.26.146.209 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.67 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.137 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.179 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.160.240.190 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 46.19.85.4 | Israel | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 31.210.187.34 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 109.160.240.190 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 46.19.85.131 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |

12-29-2015-10:04:07 to 12-29-2015-11:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 41.37.174.106 | Egypt | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 41.37.174.106 | Block | 496 |
| 41.37.174.106 | Egypt | 147.237.77.216 | dover.idf.il | Multiple Admin Blocking from 41.37.174.106 | Block | 157 |
| 41.37.174.106 | Egypt | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 149 |
| 80.246.130.147 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 57 |
| 46.19.86.23 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 31 |
| 37.26.146.212 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 20 |
| 46.19.86.195 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 13 |
| 109.253.203.123 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 80.246.139.154 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 4 |
| 79.180.37.252 | Israel | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx | Block | 4 |
| 176.13.20.105 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.35 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.210.152 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.12.26 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.64.168.145 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 3 |
| 66.249.66.28 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Suspicious Response Code_Custom_Temporary | Block | 3 |
| 176.13.5.21 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.8.243 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 3 |
| 176.13.22.181 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 37.26.147.218 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.182.2.162 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 176.13.20.132 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 85.65.32.174 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 79.182.101.219 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 79.182.101.219 | Block | 2 |
| 109.253.212.79 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 2 |
| 176.13.20.132 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 2 |
| 109.65.203.87 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 2.54.164.244 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/sachar/index | Block | 2 |
| 37.26.147.146 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 80.246.137.59 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 217.132.97.135 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/11â€‹33-19857-hâ€‹e/dover.asâ€‹px | Block | 1 |
| 46.19.85.117 | Israel | 147.237.0.34 | tikshuv.idf.il | Too Many of the Same Response Code (404) in Session from 46.19.85.117 | Block | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 40.77.167.54 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 1 |
| 62.219.99.154 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 62.219.99.154 | Block | 1 |
| 176.13.1.15 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation Password in mobile.idf.il/sachar/login | Block | 1 |
| 128.127.107.80 | Netherlands | 147.237.76.147 | chinuch.aka.idf.i | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 31.168.10.92 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/×™×?×¦×©×“ | Block | 1 |
| 80.179.223.31 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg | Block | 1 |
| 212.143.186.38 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 212.143.186.38 | Block | 1 |
| 46.19.85.179 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 109.253.129.160 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password | Block | 1 |
| 2.54.46.203 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 79.176.48.184 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.66.183 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx | Block | 1 |
| 176.13.11.192 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 41.37.174.106 | Egypt | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/ar/admin.php | Block | 1 |
| 84.228.171.15 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 46.19.86.229 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |

12-29-2015-10:04:07 to 12-29-2015-11:04:07