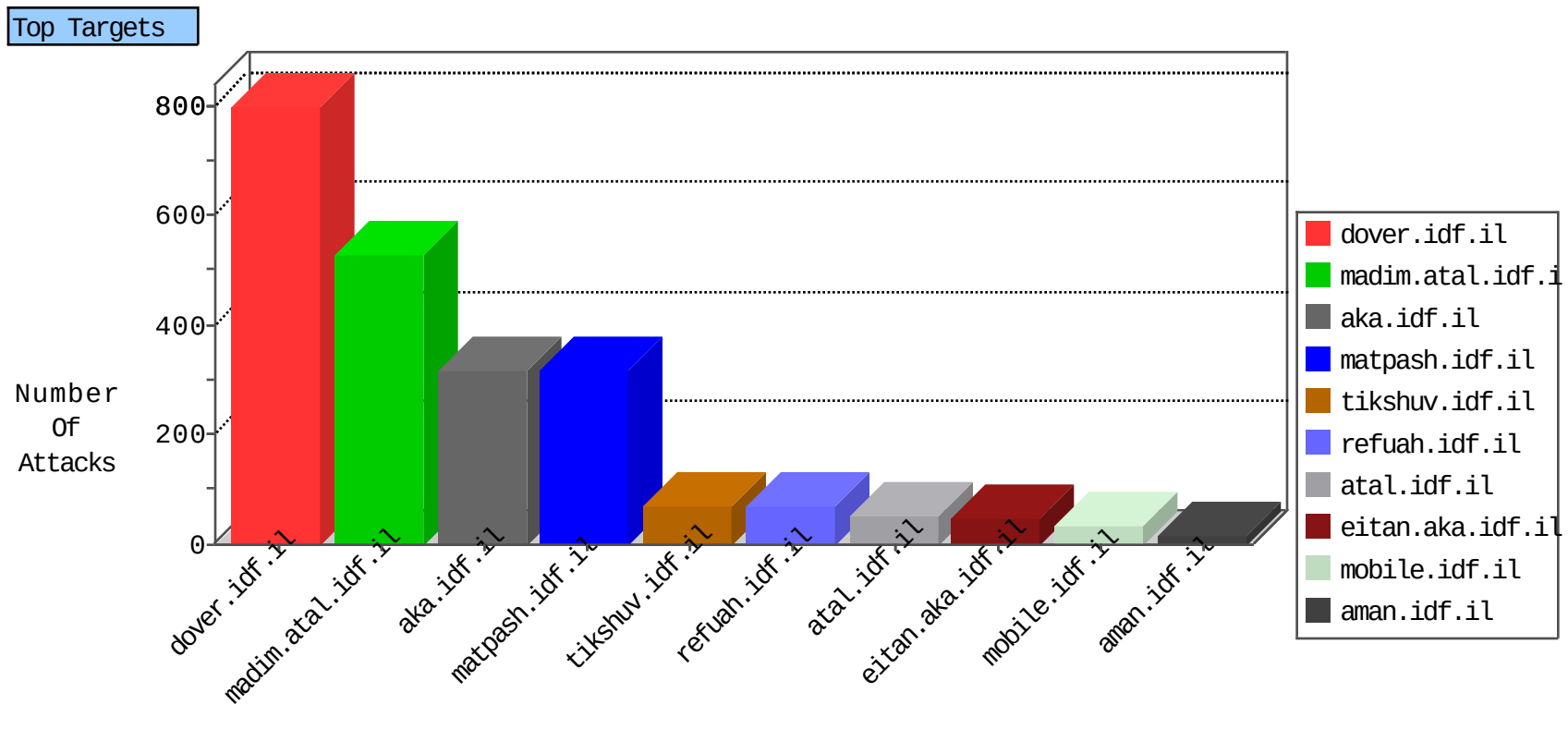
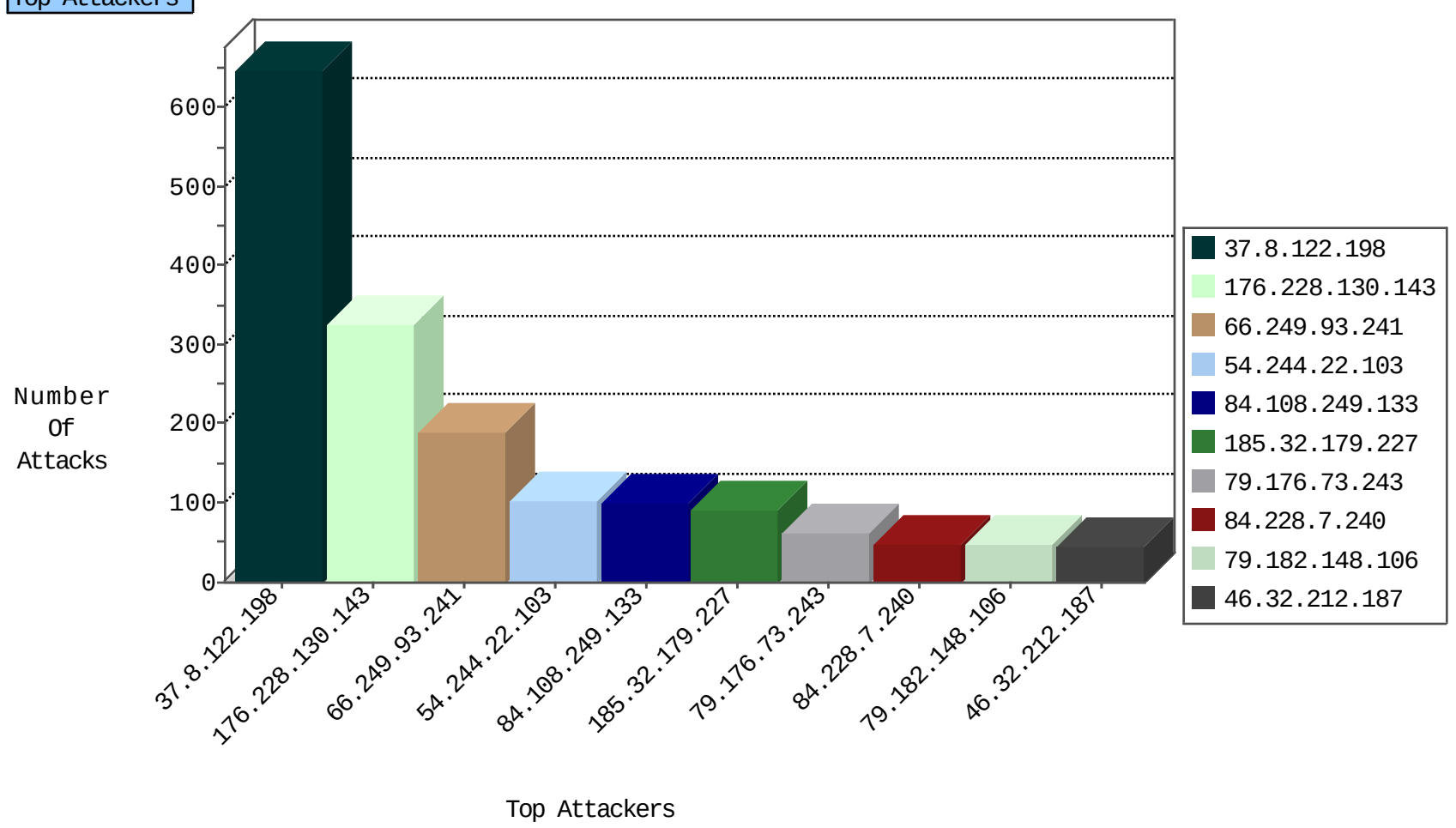
02-06-2016-22:04:05 to 02-06-2016-23:04:05

# IDF Under Attack Daily Report

Top Targets




Top Attackers



02-06-2016-22:04:05 to 02-06-2016-23:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 37.8.122.198 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | HTTP-MISC-Acunetix-Url | dest-reset | 4 |
| 85.64.158.221 | Israel | 147.237.72.156 | aman.idf.il | ID-OpenSSL-Heartbeat-ex1 | dest-reset | 3 |
| 109.66.216.80 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 142.54.185.230 | United States | 147.237.76.34 | yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 175.25.170.77 | China | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 49.65.154.180 | China | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 66.249.93.180 | Israel | 147.237.72.166 | aka.idf.il | HTTP-Misc-BadBlue-Dir-Trave-2 | dest-reset | 1 |
| 142.54.160.211 | United States | 147.237.72.156 | aman.idf.il | block-sp-traf1 | drop | 1 |
| 74.91.28.58 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | block-sp-traf1 | forward | 1 |

02-06-2016-22:04:05 to 02-06-2016-23:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 37.8.122.198 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | C091: HTTP: Access to - admin.asp | Block | 45 |
| 37.8.122.198 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | C003: HTTP: phpMyAdmin access | Block | 2 |
| 37.8.122.198 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | C023: HTTP: administrator in URI | Permit | 2 |
| 83.130.109.130 | Israel | 147.237.77.216 | dover.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |
| 188.165.15.191 | France | 147.237.77.226 | www.chamatz.aka.idf.il | C228: HTTP:  AhrefBot crawler | Block | 1 |

02-06-2016-22:04:05 to 02-06-2016-23:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.249.93.241 | 147.237.77.176 | United States | matpash.idf.il | ET SCAN NMAP -sA (2) | 190 |
| 37.8.122.198 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | SERVER-WEBAPP adminlogin access | 7 |
| 37.8.122.198 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | SERVER-WEBAPP admin.php access | 7 |
| 37.8.122.198 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | SERVER-WEBAPP login.htm access | 4 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 125.140.41.3 | 147.237.0.34 | Korea, Republic of | tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 109.64.81.163 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 50.204.188.142 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 209.126.116.147 | 147.237.72.167 | United States | ishurim.aka.idf.i | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 188.126.77.138 | 147.237.77.243 | Sweden | mobile.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 188.126.77.138 | 147.237.0.200 | Sweden | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.61.143.147 | 147.237.76.42 | China | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 123.204.186.155 | 147.237.76.30 | Taiwan | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 85.75.195.212 | 147.237.0.19 | Greece | madim.atal.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 50.204.188.142 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 188.126.77.138 | 147.237.76.177 | Sweden | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.61.143.147 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |

02-06-2016-22:04:05 to 02-06-2016-23:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 54.244.22.103 | United States | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 68 |
| 84.228.7.240 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 49 |
| 79.182.148.106 | Israel | 147.237.77.176 | matpash.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 48 |
| 46.32.212.187 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 42 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 32 |
| 54.244.22.103 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 29 |
| 207.241.229.100 | United States | 147.237.72.166 | aka.idf.il | Web Server Enforcement Violation | Web Servers Slow HTTP Denial of Service | reject | 26 |
| 72.9.148.10 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 23 |
| 79.176.73.243 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 17 |
| 46.19.85.33 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 79.176.73.243 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 13 |
| 109.64.81.163 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 77.127.209.155 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 79.176.73.243 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 79.176.73.243 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 79.176.73.243 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 11 |
| 79.176.73.243 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 141.8.132.112 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 79.182.137.140 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 2.54.59.217 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 85.64.122.228 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 109.67.101.102 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.13.15.232 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 70.64.70.73 | Canada | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 6 |
| 54.244.22.103 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.160.134.26 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.122 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.52.7.227 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 213.8.204.41 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | alert | 5 |
| 213.8.204.41 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 31.210.187.179 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 91.200.12.106 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |
| 91.200.12.136 | Ukraine | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 4 |
| 84.228.107.162 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 31.154.40.50 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 217.132.58.238 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 46.117.107.241 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 91.200.12.136 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 4 |
| 5.102.219.23 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 213.8.204.56 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 85.65.61.158 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 77.125.138.46 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 79.183.98.63 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.179.104.98 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 212.150.252.59 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.135.48 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 5.102.232.48 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

02-06-2016-22:04:05 to 02-06-2016-23:04:05

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 79.182.103.116 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

02-06-2016-22:04:05 to 02-06-2016-23:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 37.8.122.198 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 37.8.122.198 | Block | 372 |
| 176.228.130.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 179 |
| 176.228.130.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 107 |
| 37.8.122.198 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Multiple Admin Blocking from 37.8.122.198 | Block | 105 |
| 37.8.122.198 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 98 |
| 84.108.249.133 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 97 |
| 185.32.179.227 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 51 |
| 185.32.179.227 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 40 |
| 176.228.130.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (403) in Session from 176.228.130.143 | Block | 39 |
| 192.243.55.132 | Dominica | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.132 | Block | 6 |
| 37.75.204.241 | Russian Federation | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 6 |
| 192.243.55.135 | Dominica | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.135 | Block | 5 |
| 176.13.15.153 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 37.75.204.241 | Russian Federation | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 37.75.204.241 | Block | 5 |
| 192.243.55.131 | Dominica | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.131 | Block | 4 |
| 109.253.158.193 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 192.243.55.137 | Dominica | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.137 | Block | 3 |
| 192.243.55.134 | Dominica | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.134 | Block | 3 |
| 192.243.55.129 | Dominica | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.243.55.129 | Block | 2 |
| 2.110.142.157 | Denmark | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 2 |
| 46.19.85.74 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 84.108.249.133 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 2 |
| 190.45.66.156 | Chile | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 2 |
| 46.120.220.76 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 198.58.103.36 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1294-he/www.idf.il | Block | 1 |
| 149.78.170.246 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 192.243.55.131 | Dominica | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/tizmoret/gallery | Block | 1 |
| 87.242.64.205 | Russian Federation | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/ | Block | 1 |
| 66.249.93.35 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/favicon.ico | Block | 1 |
| 188.138.9.49 | Germany | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - sigalgs DoS Attack | None | 1 |
| 66.249.66.115 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx | None | 1 |
| 109.253.150.51 | Israel | 147.237.77.233 | atal.idf.il | Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx | Block | 1 |
| 37.75.204.241 | Russian Federation | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php | Block | 1 |
| 192.243.55.134 | Dominica | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/giyus/kadatz | Block | 1 |
| 84.94.185.197 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.78.148 | Israel | 147.237.76.30 | himush.idf.il | Unauthorized URL Access to www.chimush.atal.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 46.121.18.32 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 1 |
| 164.138.125.206 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/haredim/&sa=u&ved=0ahukewiy-t3_getkahxcwz4khqfycrcqfgghmaa&sig2=cpniclggjnkt6fc-lhqcba&usg=afqjcnfd5s02zieedmbmfxvss2_oefusww | Block | 1 |
| 87.246.192.21 | Poland | 147.237.76.200 | eitan.aka.idf.il | Distributed PHP Attempt | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx | Block | 1 |
| 190.45.66.156 | Chile | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 176.228.130.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many 403: Response Code per Session | Block | 1 |
| 66.249.69.26 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp | Block | 1 |
| 40.77.167.105 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 5.28.129.43 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc | Block | 1 |
| 192.243.55.129 | Dominica | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/giyus/general | Block | 1 |
| 185.120.125.6 |  | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 66.249.64.190 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/giyus/[[#11]]general.aspx | Block | 1 |
| 37.8.122.198 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/ar/wp-admin | Block | 1 |

02-06-2016-22:04:05 to 02-06-2016-23:04:05