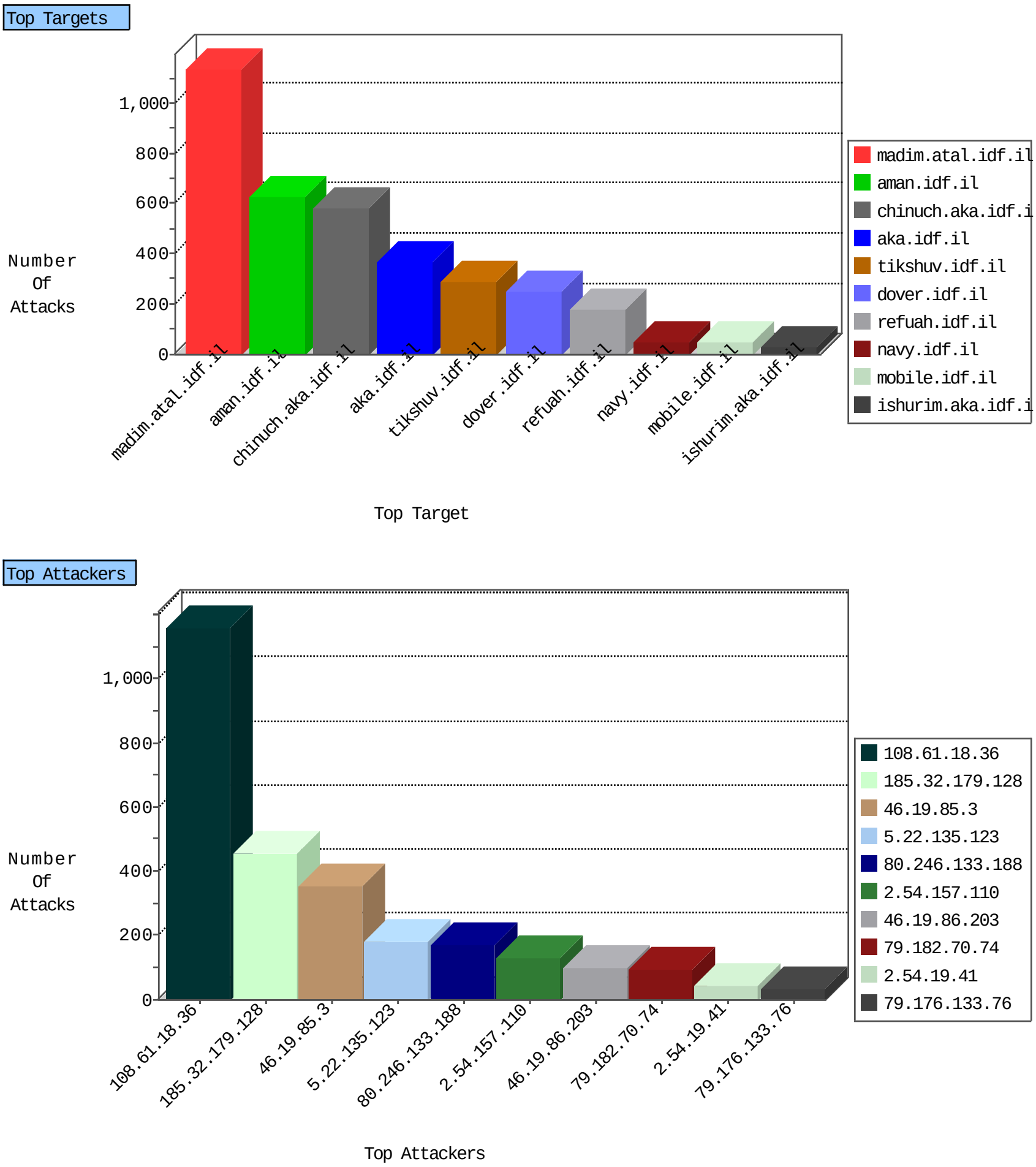
02-11-2016-17:04:04 to 02-11-2016-18:04:04

# IDF Under Attack Daily Report



02-11-2016-17:04:04 to 02-11-2016-18:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.176.133.76 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 35 |
| 109.67.50.138 | Israel | 147.237.72.156 | aman.idf.il | Block_Udp_All_Nets | drop | 6 |
| 79.177.221.84 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 115.239.228.10 | China | 147.237.76.147 | chinuch.aka.idf.il | JLM_Under_Attack_Con_Http | drop | 2 |
| 128.194.131.235 | United States | 147.237.72.166 | aka.idf.il | block-sp-traf1 | drop | 1 |
| 142.54.160.211 | United States | 147.237.77.233 | atal.idf.il | block-sp-traf1 | drop | 1 |
| 188.165.222.221 | France | 147.237.76.201 | e.atal.idf.il | Block_Udp_All_Nets | drop | 1 |

02-11-2016-17:04:04 to 02-11-2016-18:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 213.239.205.66 | Germany | 147.237.76.31 | nakchal.idf.il | 0543: HTTP: php.cgi Access | Block | 1 |

02-11-2016-17:04:04 to 02-11-2016-18:04:04

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 | 3 |
| 84.228.182.140 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.108.190.181 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.82.64.68 | 147.237.72.167 | Netherlands | ishurim.aka.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 75.112.30.10 | 147.237.8.50 | United States | e.tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 59.45.79.117 | 147.237.8.46 | China | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.246.0.97 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 59.45.79.117 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 119.196.222.180 | 147.237.76.44 | Korea, Republic of | e.refuah.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 51.254.23.230 | 147.237.77.176 | United Kingdom | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.226.18.233 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.151.52.161 | 147.237.77.178 | Ukraine | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 85.64.66.85 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.39.166 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.228.130.107 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 81.218.125.133 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.177.114.79 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 59.45.79.117 | 147.237.77.61 | China | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.186.34.177 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 59.45.79.117 | 147.237.0.200 | China | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 51.254.23.230 | 147.237.77.212 | United Kingdom | e.dover.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 109.226.26.30 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 51.254.23.230 | 147.237.0.19 | United Kingdom | madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.67.234.188 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 41.43.207.152 | 147.237.77.216 | Egypt | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

02-11-2016-17:04:04 to 02-11-2016-18:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 108.61.18.36 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 579 |
| 108.61.18.36 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 578 |
| 80.246.133.188 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 171 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 109.253.222.147 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 37.26.147.255 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 16 |
| 2.54.19.41 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 15 |
| 46.19.85.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 46.19.85.60 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 46.116.24.239 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 80.246.139.46 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 46.19.85.207 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 77.127.209.155 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 80.246.139.166 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 176.13.14.9 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 80.246.139.166 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 132.64.158.219 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.253.138.104 | Israel | 147.237.77.243 | mobile.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 31.210.187.4 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 80.246.139.166 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.86.28 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.253.138.104 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.188 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 95.91.214.24 | Germany | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.161 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 5.102.254.60 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.86.203 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.176.224.43 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 80.246.139.166 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 46.19.85.207 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.64.42.207 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 80.246.139.166 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.163 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 31.168.217.46 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 46.120.75.162 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 46.19.85.163 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.85.209 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 79.182.25.147 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 81.218.165.8 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 188.120.154.68 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 80.179.210.222 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 68.180.229.230 | United States | 147.237.0.15 | kosher-kravi.idf.i | drop | First packet isn't SYN | drop | 4 |
| 37.142.191.96 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 80.179.9.115 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 2.54.157.110 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 46.117.65.158 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 193.43.245.250 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 4 |

02-11-2016-17:04:04 to 02-11-2016-18:04:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 185.32.179.128 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 228 |
| 185.32.179.128 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 182 |
| 5.22.135.123 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 179 |
| 46.19.85.3 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 169 |
| 46.19.85.3 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 138 |
| 2.54.157.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 107 |
| 79.182.70.74 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 95 |
| 46.19.86.203 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 72 |
| 46.19.85.3 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (403) in Session from 46.19.85.3 | Block | 48 |
| 185.32.179.128 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 42 |
| 2.54.19.41 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 20 |
| 46.19.85.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 18 |
| 46.19.86.203 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 18 |
| 2.54.157.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 11 |
| 109.253.199.161 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 109.253.199.161 | Block | 9 |
| 36.224.242.141 | Taiwan | 147.237.76.86 | navy.idf.il | Distributed PHP Attempt | Block | 6 |
| 80.246.130.246 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 6 |
| 109.64.42.207 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Too Many of the Same Response Code (404) in Session from 109.64.42.207 | Block | 6 |
| 36.224.242.141 | Taiwan | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 36.224.242.141 | Block | 5 |
| 2.54.161.254 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 2.54.175.229 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 46.19.85.196 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.149.176 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.178.162.53 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 213.239.205.66 | Germany | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 213.239.205.66 | Block | 2 |
| 46.19.85.19 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.64.10.101 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/giyus/qanda/default.asp | Block | 2 |
| 79.180.168.122 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$58 in aka.idf.il/main/giyus/questionnaire.aspx | None | 2 |
| 2.54.19.41 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 2 |
| 5.22.131.60 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.180.168.122 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$82 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 208.80.194.30 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/www.youtube.com/embed/02xlfsfhjyk | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx | Block | 1 |
| 36.224.242.141 | Taiwan | 147.237.76.86 | navy.idf.il | Admin Blocking | Block | 1 |
| 109.67.202.42 | Israel | 147.237.72.166 | aka.idf.il | Distributed Malformed URL | Block | 1 |
| 93.172.10.216 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 62.114.167.92 | Egypt | 147.237.77.170 | maarachot.idf.il | Distributed PHP Attempt | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.200 | eitan.aka.idf.il | Multiple Unknown HTTP Request Method from 169.229.3.91 | Block | 1 |
| 157.55.39.104 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter tm in www.aka.idf.il/main/giyus/ | None | 1 |
| 84.108.186.33 | Israel | 147.237.77.233 | atal.idf.il | Distributed PHP Attempt | Block | 1 |
| 46.19.85.135 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp | Block | 1 |
| 37.142.68.19 | Israel | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 1 |
| 109.67.202.42 | Israel | 147.237.72.166 | aka.idf.il | Malformed HTTP Header Line 1 | Block | 1 |
| 79.177.204.44 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 1 |
| 197.53.27.35 | Egypt | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 66.249.69.11 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | Unknown HTTP Request Method J^ | Block | 1 |
| 109.67.202.42 | Israel | 147.237.72.166 | aka.idf.il | Abnormally Long Header Line request header name | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.200 | eitan.aka.idf.il | Illegal Byte Code Character in URL [[#22]]Ö½[[#29]]"Âž×‘ [[#20]][[#14]]ÃœÖ¶â€ž[[#1]]â€¢_ÃŸ×˜Â?74yÂ-jÂ³×š1â€˜ Â²[[#23]]Â?×´kg | Block | 1 |
| 85.65.202.64 | Israel | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |

02-11-2016-17:04:04 to 02-11-2016-18:04:04