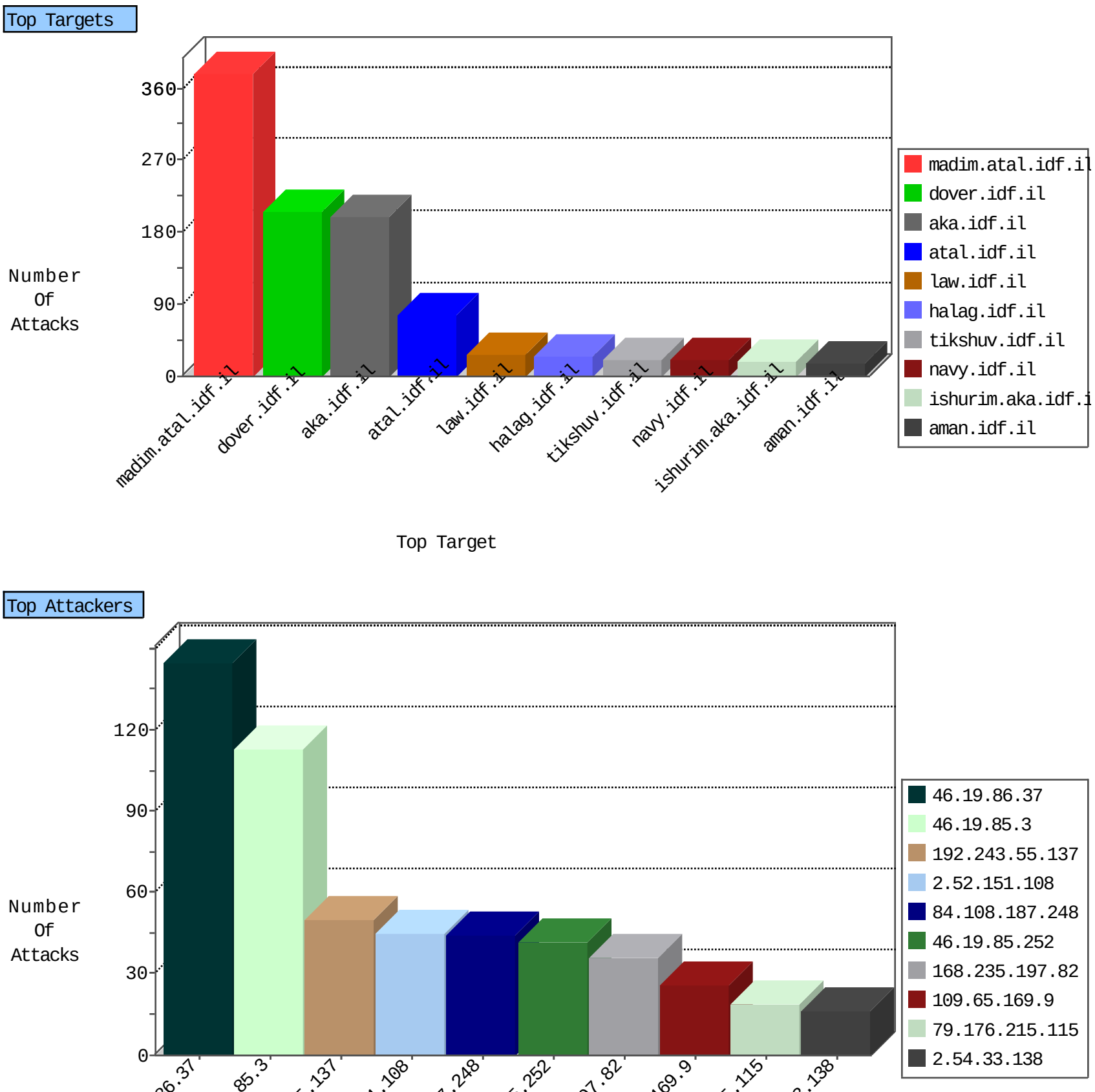
03-04-2016-12:04:07 to 03-04-2016-13:04:07

# IDF Under Attack Daily Report



03-04-2016-12:04:07 to 03-04-2016-13:04:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 4 |
| 168.235.197.82 | United States | 147.237.77.216 | dover.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 81.218.65.210 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 204.42.253.2 | United States | 147.237.77.216 | dover.idf.il | Block_Ntp_All_Net | drop | 2 |
| 168.235.197.82 | United States | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 2 |
| 204.42.253.2 | United States | 147.237.72.217 | e.idf.il | Block_Ntp_All_Net | drop | 2 |
| 204.42.253.2 | United States | 147.237.77.212 | e.dover.idf.il | Block_Ntp_All_Net | drop | 2 |
| 185.94.111.1 | | 147.237.0.35 | akaws.idf.il | Block_Udp_All_Nets | drop | 1 |
| 208.85.244.2 | United States | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 179.43.144.33 | Switzerland | 147.237.72.217 | e.idf.il | Block_Ntp_All_Net | drop | 1 |
| 124.111.175.185 | Korea, Republic of | 147.237.0.200 | m4u.idf.il | Block_Udp_All_Nets | drop | 1 |
| 184.105.247.231 | United States | 147.237.77.121 | e.navy.idf.il | Block_Udp_All_Nets | drop | 1 |

03-04-2016-12:04:07 to 03-04-2016-13:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 89.138.94.248 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 109.64.252.190 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 79.181.149.106 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 163.172.13.244 | United Kingdom | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 1 |
| 86.34.138.111 | Romania | 147.237.77.216 | dover.idf.il | C1000008: HTTP: Xenu UserAgent | Block | 1 |
| 106.38.241.106 | China | 147.237.77.233 | atal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 109.66.15.155 | Israel | 147.237.77.216 | dover.idf.il | C1000008: HTTP: Xenu UserAgent | Block | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

03-04-2016-12:04:07 to 03-04-2016-13:04:07

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 |
| 112.33.3.69 | 147.237.72.156 | China | aman.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.215.89.20 | 147.237.76.196 | United States | e.sviva.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 40.117.92.242 | 147.237.72.217 | United States | e.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 40.117.92.242 | 147.237.72.217 | United States | e.idf.il | ET SCAN NMAP -f -sS | 1 |
| 180.97.215.33 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 112.33.3.69 | 147.237.72.217 | China | e.idf.il | ET SCAN Potential SSH Scan | 1 |
| 112.33.3.69 | 147.237.72.166 | China | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 112.33.3.69 | 147.237.72.14 | China | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 104.215.89.20 | 147.237.76.196 | United States | e.sviva.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 40.117.92.242 | 147.237.72.217 | United States | e.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 14.43.239.114 | 147.237.8.27 | Korea, Republic of | e.madim.atal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 180.97.215.33 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 171.250.13.235 | 147.237.76.30 | Vietnam | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 112.33.3.69 | 147.237.72.167 | China | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |

03-04-2016-12:04:07 to 03-04-2016-13:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 168.235.197.82 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 31 |
| 109.65.169.9 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 25 |
| 79.176.215.115 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 18 |
| 84.108.187.248 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 18 |
| 2.54.33.138 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 204.12.251.37 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 14 |
| 84.108.187.248 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 84.108.187.248 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 202.77.111.56 | Indonesia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 80.178.17.14 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 9 |
| 2.52.49.252 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.146.180 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 185.120.126.56 | | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.5 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 37.26.146.249 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.5 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.138 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.200 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 93.158.152.52 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.138 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 5.102.195.244 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 141.8.184.13 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.85.11 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 4 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 5.22.131.39 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.85.11 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 92.241.52.87 | Jordan | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 4 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 4 |
| 46.19.85.11 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 109.65.161.105 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.3 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.43.216 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.133.67 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.13.17.135 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 149.88.199.242 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 185.3.144.115 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 46.19.86.47 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.95.59.162 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 109.253.213.10 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.177.206.134 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 46.117.9.67 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 192.243.55.137 | Dominica | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.37 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 145 |
| 46.19.85.3 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 109 |
| 2.52.151.108 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 46.19.85.252 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 42 |
| 176.13.2.17 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 13 |
| 37.26.149.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 176.13.7.195 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 176.13.13.93 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 149.88.238.116 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 149.88.238.116 | Block | 3 |
| 89.139.136.159 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 3 |
| 2.52.138.60 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302 | Block | 2 |
| 155.94.195.17 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 2 |
| 77.126.151.206 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/valtam | Block | 2 |
| 2.52.181.4 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation Password in mobile.idf.il/sachar/login | Block | 2 |
| 213.8.204.2 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/registrationwizard/ | Block | 2 |
| 185.3.147.110 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized HTTP Method | Block | 2 |
| 2.52.138.60 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 2.52.138.60 | Block | 2 |
| 92.85.90.162 | Romania | 147.237.77.176 | matpash.idf.il | PHP Attempt | Block | 1 |
| 213.8.204.2 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/ | Block | 1 |
| 185.3.147.110 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/ | Block | 1 |
| 66.249.66.182 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/242.doc | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.200 | eitan.aka.idf.il | Illegal Byte Code Character in Method | Block | 1 |
| 109.66.15.155 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/ | Block | 1 |
| 207.46.13.98 | United States | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx | Block | 1 |
| 81.218.204.97 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp | Block | 1 |
| 37.26.146.172 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 92.85.90.162 | Romania | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php | Block | 1 |
| 213.57.155.171 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 192.243.55.137 | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.200 | eitan.aka.idf.il | NULL Character in Method | Block | 1 |
| 46.19.85.3 | Israel | 147.237.0.19 | madim.atal.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx | Block | 1 |
| 109.67.188.201 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 207.46.13.102 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 84.108.187.248 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 66.249.64.230 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/robots.txt | Block | 1 |
| 184.105.139.67 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 149.88.238.116 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx | Block | 1 |
| 95.86.110.3 | Israel | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 95.86.110.3 | Block | 1 |
| 213.57.200.23 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 213.57.200.23 | Block | 1 |
| 192.243.55.137 | Dominica | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1129-he/dover.aspx?searchtext=רמטכ"ל | Block | 1 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 68.180.229.239 | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | Illegal Byte Code Character in Method | Block | 1 |
| 46.19.85.219 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 2.52.152.248 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 130.185.155.74 | Sweden | 147.237.0.34 | tikshuv.idf.il | PHP Attempt | Block | 1 |
| 207.46.13.171 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 66.249.64.233 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp | Block | 1 |
| 185.3.147.110 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 185.3.147.110 | Block | 1 |
| 37.142.68.18 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |