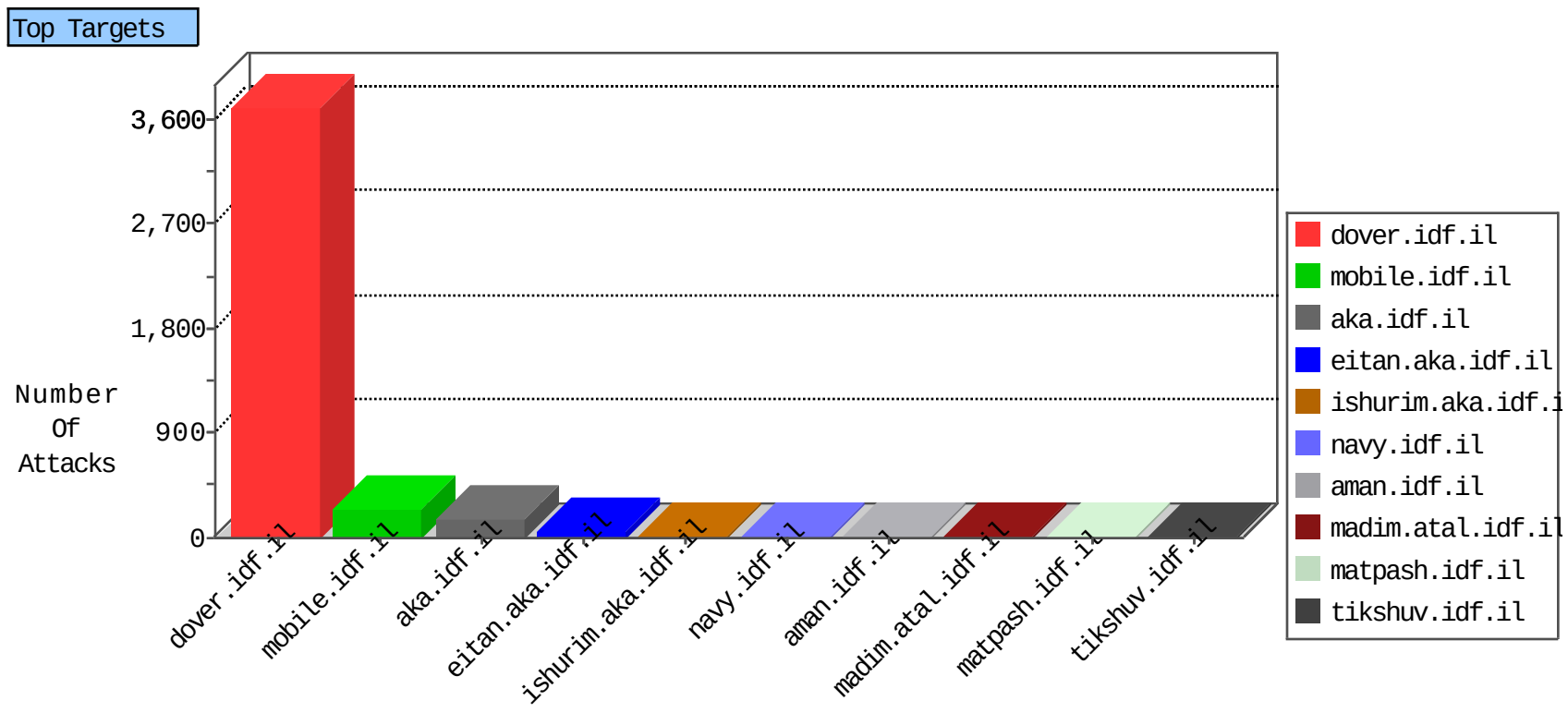
04-28-2016-19:04:06 to 04-28-2016-20:04:06

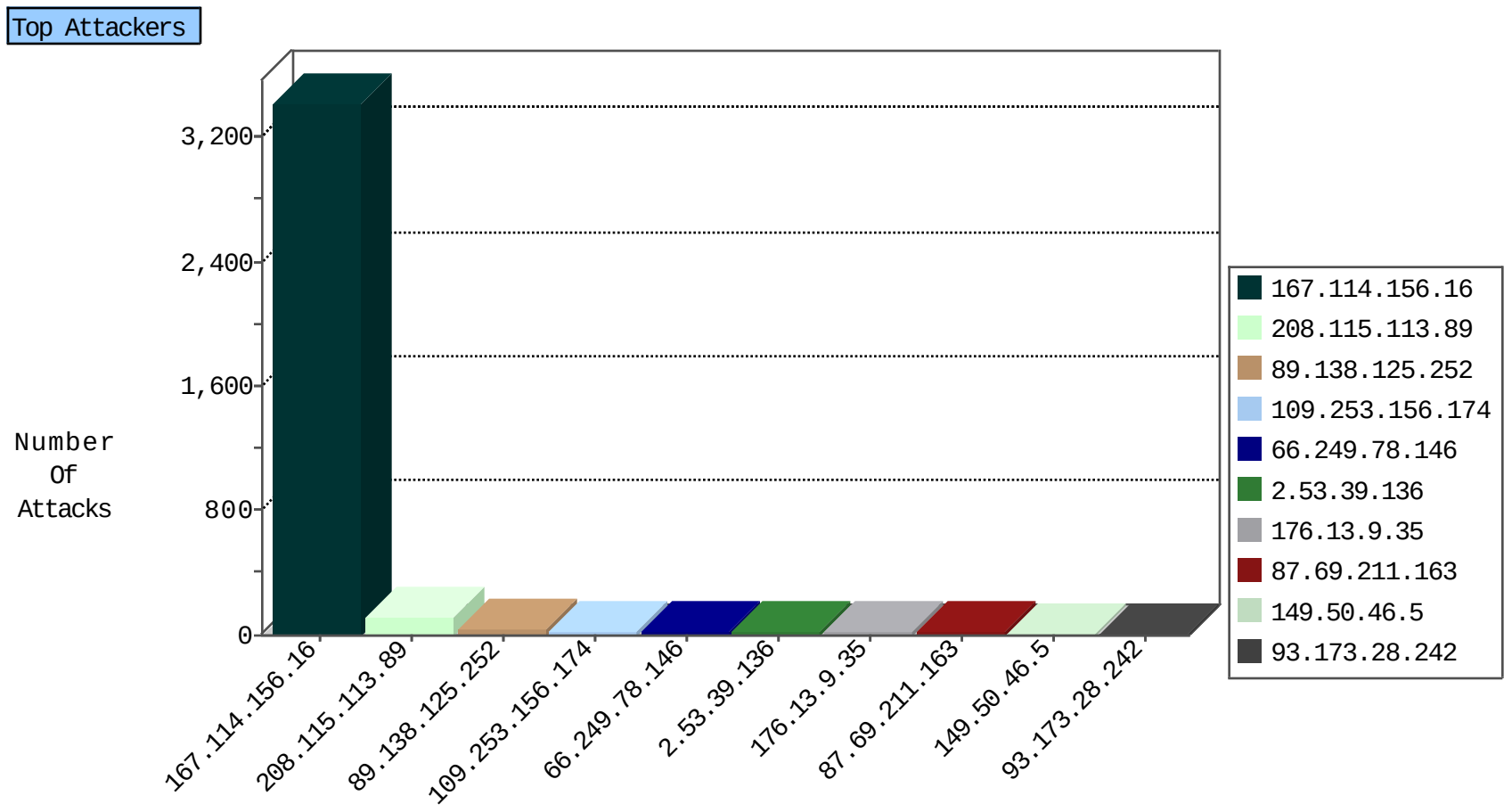
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

04-28-2016-19:04:06 to 04-28-2016-20:04:06

## 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 | 2149 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 1108 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 471 |
| 81.218.65.210 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 6 |
| 14.111.147.186 | China | 147.237.76.198 | e.yohalan.idf.il | Block_Udp_All_Nets | drop | 2 |
| 71.6.135.131 | United States | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 94.102.49.116 | Netherlands | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |

04-28-2016-19:04:06 to 04-28-2016-20:04:06

## Top Attackers In IPS

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

04-28-2016-19:04:06 to 04-28-2016-20:04:06

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 | 4 |
| 180.97.106.162 | 147.237.76.44 | China | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.36 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 171.106.48.63 | 147.237.8.46 | China | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.82.78.38 | 147.237.72.217 | Netherlands | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 13.92.178.142 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 13.92.100.128 | 147.237.0.16 | United States | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 193.201.227.63 | 147.237.0.35 | Ukraine | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.37 | 147.237.77.205 | China | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 171.106.48.63 | 147.237.8.46 | China | e.chinuch.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 109.253.227.33 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 13.92.178.142 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 13.92.178.142 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN NMAP -f -sS | 1 |

04-28-2016-19:04:06 to 04-28-2016-20:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2455 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 118 |
| 89.138.125.252 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 27 |
| 66.249.78.146 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 109.253.156.174 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 2.53.39.136 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 176.13.9.35 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 79.177.94.171 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 86.59.234.142 | Hungary | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 149.50.46.5 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 93.173.28.242 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 87.69.211.163 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 45.35.64.142 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 37.142.64.47 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 149.50.90.232 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 10 |
| 46.19.85.194 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 213.8.204.72 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 185.89.217.234 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 2.53.13.203 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 37.60.145.49 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 9 |
| 109.65.146.183 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 82.81.212.213 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 8 |
| 69.30.213.202 | United States | 147.237.76.200 | eitan.aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 8 |
| 5.39.180.210 | United Kingdom | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 8 |
| 85.130.250.133 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 128.62.16.154 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 37.26.149.178 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 66.249.93.182 | Europe | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 198.58.103.92 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.53.55.105 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.236 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 80.230.223.183 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 66.249.64.190 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.94 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 80.230.222.136 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.53.58.186 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.179.205.134 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 88.171.13.112 | France | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 93.172.139.233 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 73.245.43.179 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 81.67.116.178 | France | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 79.181.221.49 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 37.26.149.130 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

04-28-2016-19:04:06 to 04-28-2016-20:04:06

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 185.120.125.119 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.70.48.238 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.65.188.252 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 89.138.125.252 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 2.53.39.136 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 87.69.211.163 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 109.253.156.174 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 149.50.90.232 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 109.65.146.183 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.142.64.47 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.9.35 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 149.50.46.5 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.178.151.149 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 176.13.9.251 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 2.53.144.92 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 93.173.28.242 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.130.83 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 8.37.230.190 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 80.246.130.254 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 185.89.217.233 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 2.53.13.203 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 199.30.25.0 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 213.8.204.72 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 185.89.217.225 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 85.65.183.235 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 85.65.183.235 | Block | 2 |
| 46.19.85.194 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 85.65.183.235 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/ | Block | 2 |
| 46.19.85.236 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 157.55.39.133 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx | None | 1 |
| 68.64.168.226 | United States | 147.237.72.166 | aka.idf.il | Admin Blocking | Block | 1 |
| 141.8.132.78 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1283-13885-en/dover.aspx. | Block | 1 |
| 2.53.58.186 | Israel | 147.237.77.243 | mobile.idf.il | Suspicious Response Code | Block | 1 |
| 207.98.171.35 | United States | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 1 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx | Block | 1 |
| 62.90.235.98 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/templates/links/mobile | Block | 1 |
| 17.142.155.123 | United States | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 17.142.155.123 | Block | 1 |
| 109.67.198.9 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif | Block | 1 |
| 84.108.62.107 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx | None | 1 |
| 185.89.217.235 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 68.64.168.226 | United States | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 37.147.107.80 | Russian Federation | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 37.147.107.80 | Block | 1 |
| 2.53.62.162 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/authentication/index | Block | 1 |
| 87.70.105.97 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 207.98.171.35 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1086-14000-en/ | Block | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69851.pdf | Block | 1 |
| 17.142.155.123 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/apple-app-site-association | Block | 1 |
| 85.64.20.66 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/article/mobile | Block | 1 |
| 68.64.168.226 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/administrator/index.php | Block | 1 |
| 37.147.107.80 | Russian Federation | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 80.95.38.249 | Russian Federation | 147.237.0.19 | madim.atal.idf.i | Parameter Type Violation ReturnUrl in madim.atal.idf.il/login.aspx | Block | 1 |
| 66.249.78.240 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 130.185.155.82 | Sweden | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 1 |
| 27.7.237.81 | India | 147.237.77.170 | maarachot.idf.il | PHP Attempt | Block | 1 |