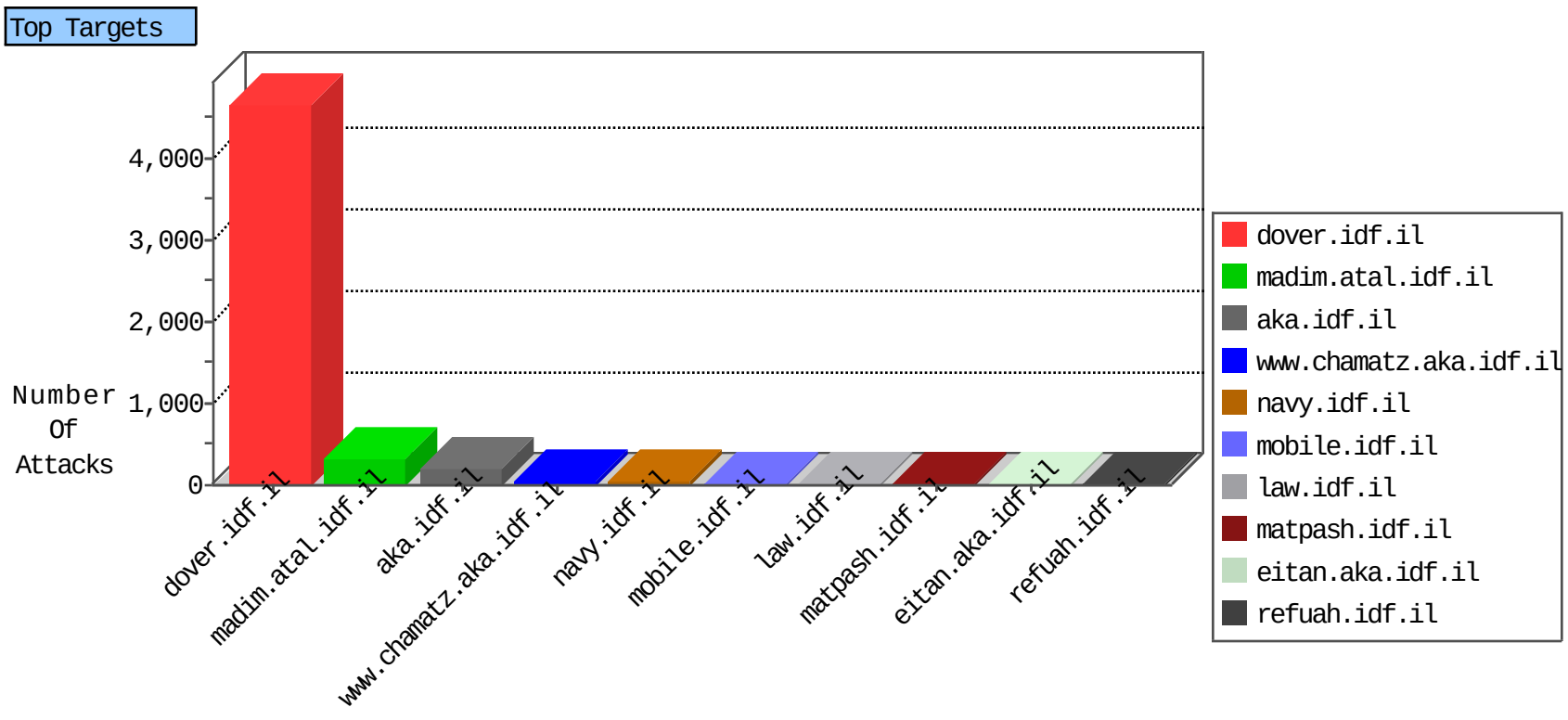
04-26-2016-17:04:01 to 04-26-2016-18:04:01

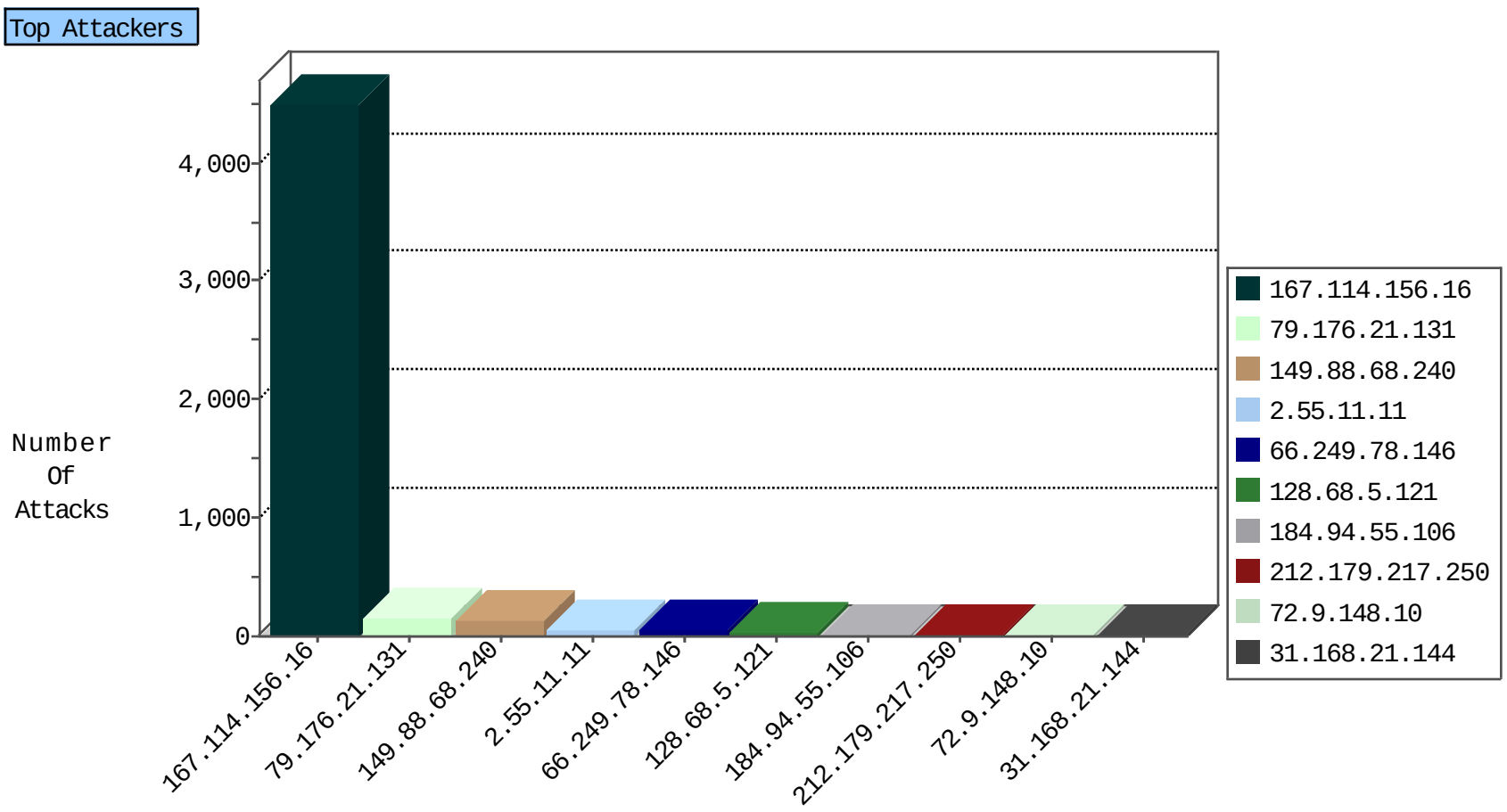
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

04-26-2016-17:04:01 to 04-26-2016-18:04:01

## 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 | HTTP-POST-Segmented-DoS | dest-reset | 10539 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 1935 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 1776 |
| 79.182.28.17 | Israel | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 204 |
| 213.8.7.207 | Israel | 147.237.77.216 | dover.idf.il | HTTP-POST-Segmented-DoS | dest-reset | 101 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 4 |
| 81.218.65.210 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 3 |
| 124.104.133.159 | Philippines | 147.237.0.200 | m4u.idf.il | Frk_Under_Attack_Con_Tcp | drop | 2 |
| 60.173.14.67 | China | 147.237.76.201 | e.atal.idf.il | JLM_Purple_Con_Limit_Http | drop | 1 |
| 94.102.49.116 | Netherlands | 147.237.76.31 | nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 94.102.49.116 | Netherlands | 147.237.76.177 | ncore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 198.20.69.74 | United States | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 31.148.219.11 | Netherlands | 147.237.76.198 | e.yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 89.46.102.242 | Romania | 147.237.76.177 | ncore.idf.il | Block_Udp_All_Nets | drop | 1 |

04-26-2016-17:04:01 to 04-26-2016-18:04:01

## Top Attackers In IPS

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

04-26-2016-17:04:01 to 04-26-2016-18:04:01

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 185.37.148.18 | 147.237.76.86 | Israel | navy.idf.il | ET SCAN NMAP -sA (2) | 6 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 191.181.202.252 | 147.237.8.27 | Brazil | e.madim.atal.idf.i | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 104.219.238.10 | 147.237.77.227 | United States | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.204.211 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 80.82.78.38 | 147.237.76.147 | Netherlands | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.116.214.240 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

04-26-2016-17:04:01 to 04-26-2016-18:04:01

## 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 | 3482 |
| 66.249.78.146 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 42 |
| 128.68.5.121 | Russian Federation | 147.237.77.226 | www.chamatz.aka.idf.il | drop | First packet isn't SYN | drop | 31 |
| 72.9.148.10 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 212.179.217.250 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 66.249.78.130 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 31.168.21.144 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 184.94.55.106 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 197.45.132.217 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 79.176.21.131 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 149.78.241.12 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.253.226.120 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 66.249.78.137 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.160.176.43 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 87.70.52.243 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.245 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.55.11.11 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.187 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 37.26.149.184 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 2.53.54.152 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 109.67.237.20 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 192.0.113.210 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 213.8.204.25 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 184.94.55.106 | Canada | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 87.70.11.222 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.235 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.180.4.231 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.149.208 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.126.203.13 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 149.78.41.243 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.180.38.206 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 130.193.51.91 | Russian Federation | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.126.213.230 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.201.181 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.148.202 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.71.23.120 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 149.78.41.252 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.27.105.76 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.93.182 | Europe | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.179.106.158 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.3.146.193 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 77.127.215.213 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

04-26-2016-17:04:01 to 04-26-2016-18:04:01

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.249.66.191 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.71.66.106 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.93.245 | Europe | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.64.70.203 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.52 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 52.16.5.197 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.176.21.131 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 144 |
| 149.88.68.240 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 125 |
| 2.55.11.11 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 40 |
| 79.180.15.139 | Israel | 147.237.77.74 | law.idf.il | Unauthorized HTTP Method | Block | 7 |
| 62.219.193.62 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 62.219.193.62 | Block | 5 |
| 85.236.157.21 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 85.236.157.21 | Block | 4 |
| 109.65.184.37 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/ | Block | 4 |
| 109.64.103.124 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile | Block | 4 |
| 80.178.2.8 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.14 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 79.180.15.139 | Israel | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 79.180.15.139 | Block | 2 |
| 79.180.15.139 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/ | Block | 1 |
| 62.219.193.62 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 1 |
| 213.8.204.25 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx | Block | 1 |
| 131.253.25.168 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 2.53.142.147 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 77.75.77.11 | Czech Republic | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/page/32/ | Block | 1 |
| 149.88.128.202 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.65.184.37 | Israel | 147.237.77.74 | law.idf.il | Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/647-2336-he/patzar.aspx | Block | 1 |
| 66.249.66.121 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2293.jpg | Block | 1 |
| 216.48.133.138 | United States | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 149.50.12.164 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile | Block | 1 |
| 85.236.157.21 | France | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/wp-admin/ | Block | 1 |
| 157.55.39.147 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 54.187.180.35 | United States | 147.237.77.176 | matpash.idf.il | Distributed PHP Attempt | Block | 1 |
| 82.110.109.208 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.78.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx | Block | 1 |
| 149.78.23.174 | United States | 147.237.76.86 | navy.idf.il | PHP Attempt | Block | 1 |
| 5.102.146.87 | Switzerland | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/tmp/php.class.php | Block | 1 |
| 93.172.189.145 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il | Block | 1 |
| 54.187.180.35 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/wp-login.php | Block | 1 |
| 184.94.55.106 | Canada | 147.237.77.176 | matpash.idf.il | Unauthorized HTTP Method | Block | 1 |
| 109.253.201.181 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 82.110.109.215 | United Kingdom | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 68.180.229.89 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method GET for www.aka.idf.il/iturim/asp/searchresults.asp | Block | 1 |
| 149.78.23.174 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/xmlrpc.php | Block | 1 |
| 14.215.165.4 | China | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 1 |
| 107.170.186.68 | United States | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 107.170.186.68 | Block | 1 |
| 213.8.204.25 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 109.253.226.120 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 84.111.129.22 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/ | Block | 1 |
| 68.180.229.241 | United States | 147.237.77.176 | matpash.idf.il | Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx | Block | 1 |
| 14.215.165.4 | China | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/diguo/changedb.php | Block | 1 |