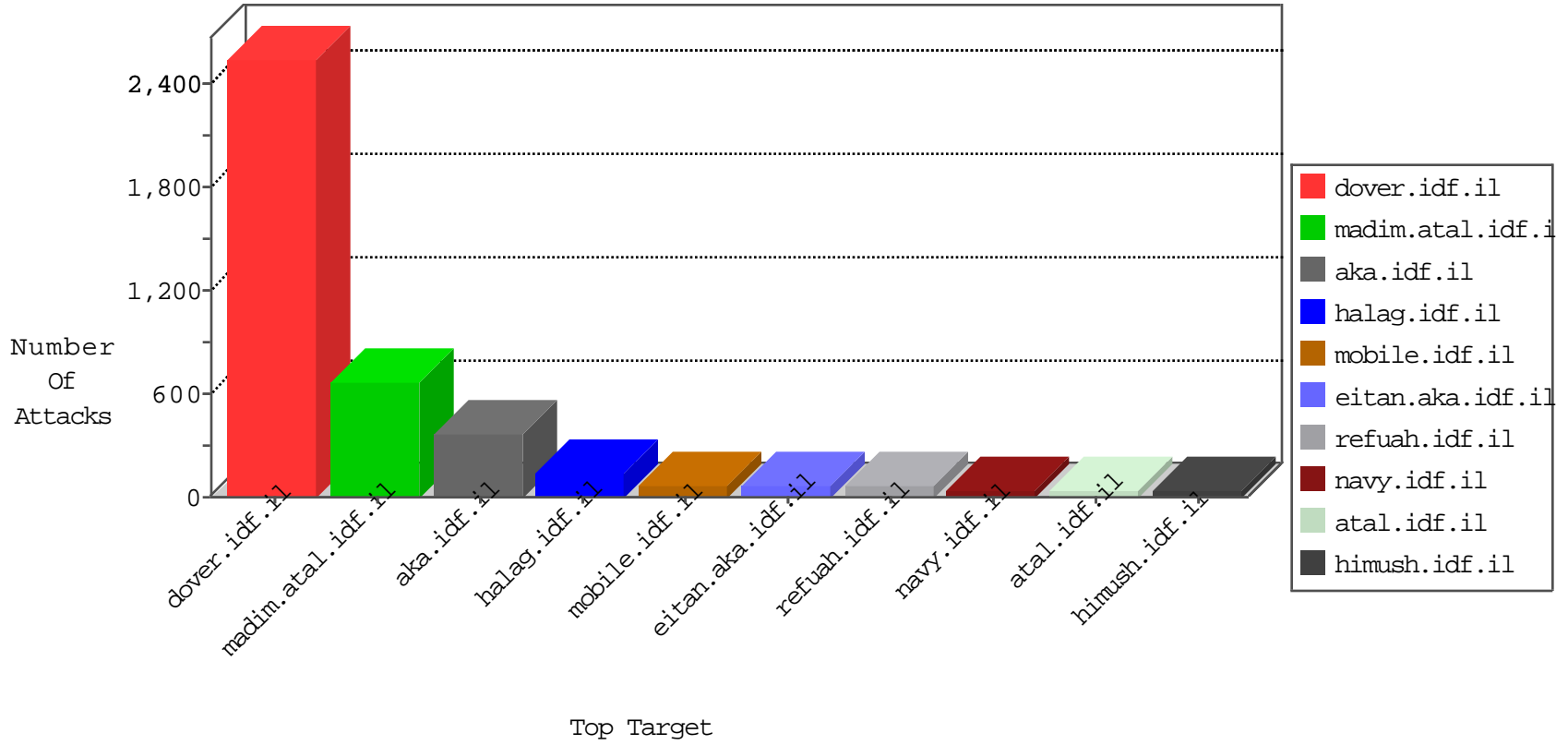


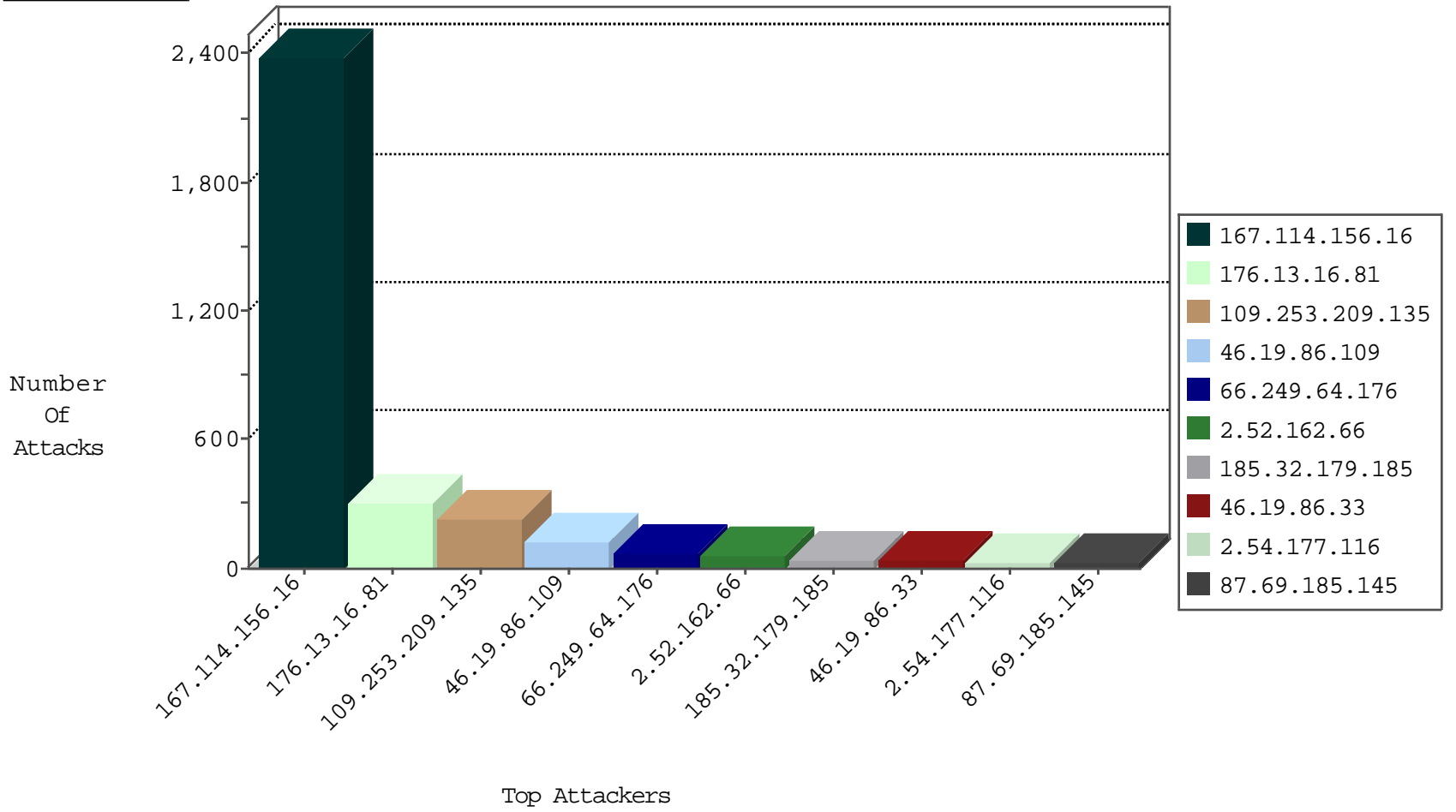
IDF Under Attack Daily Report



Top Targets



Top Attackers



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 | 3101 |
| 82.81.12.176 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 12 |
| 81.218.56.245 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 74.91.28.60 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | block-sp-trafl | drop | 1 |
| 81.100.56.209 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|--------------|--------------------------|---------------|-------|
| 108.59.8.80 | United States | 147.237.77.216 | dover.idf.il | C106: HTTP: majestic bot | Block | 1 |

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 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 218.246.0.97 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.253.133.117 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.64.26.32 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.182.201.73 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.120.123.114 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.160.168 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 198.20.69.76 | 147.237.76.177 | United States | ncore.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 163.172.13.173 | 147.237.76.38 | United Kingdom | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.64.128.73 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.246.137.196 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.177.163.154 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------|----------------|--------------------|--|---|---------------|-------|
| 46.19.86.109 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 120 |
| 66.249.64.176 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 54 |
| 2.52.162.66 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 53 |
| 85.130.190.75 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 37.26.149.133 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 20 |
| 2.54.130.60 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 79.179.168.123 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 46.19.86.222 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 46.19.85.32 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 10 |
| 109.253.137.110 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | alert | 10 |
| 109.253.137.110 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 37.26.149.205 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | alert | 9 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 79.182.194.57 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 87.69.185.145 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | | monitor | 8 |
| 109.66.53.57 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.86.69 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 172.85.9.66 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 6 |
| 62.219.190.76 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 176.13.13.49 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.71 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 51.36.0.209 | United Kingdom | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 46.19.85.215 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.33 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 80.246.137.133 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.19.85.192 | Israel | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 6 |
| 62.128.35.253 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.118 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 31.210.187.197 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 37.26.149.231 | Israel | 147.237.72.166 | aka.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 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 37.142.68.83 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 188.120.148.144 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.85.138 | Israel | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 80.246.137.133 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 149.78.15.182 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 37.26.149.205 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 87.69.185.145 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 91.200.12.141 | Ukraine | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 4 |
| 87.69.185.145 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 176.13.1.120 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 91.200.12.141 | Ukraine | 147.237.77.233 | atal.idf.il | drop | SAM rule | drop | 4 |
| 5.22.131.1 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 87.69.185.145 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 5.29.16.53 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.85.138 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|---------------------------------|----------------|------------------|--|---------------|-------|
| 176.13.16.81 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 155 |
| 176.13.16.81 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 139 |
| 109.253.209.135 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 127 |
| 109.253.209.135 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (404) | Block | 85 |
| 185.32.179.185 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 32 |
| 2.54.177.116 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 26 |
| 46.19.86.33 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 25 |
| 176.13.22.124 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 20 |
| 109.253.209.135 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (403) | Block | 18 |
| 75.167.70.34 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 75.167.70.34 | Block | 11 |
| 176.13.16.81 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Too Many of the Same Response Code (403) | Block | 9 |
| 66.249.64.176 | Israel | 147.237.76.200 | eitan.aka.idf.il | Multiple Unauthorized URL Access from 66.249.64.176 | Block | 3 |
| 176.13.2.75 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.185 | Israel | 147.237.0.19 | madim.atal.idf.i | Suspicious Response Code | Block | 3 |
| 2.54.50.230 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 176.13.7.42 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 109.253.159.66 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.195 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.215 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.86.209 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 46.19.86.108 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 37.142.68.83 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 81.218.56.171 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 81.218.56.171 | Block | 2 |
| 176.13.13.49 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 80.178.17.110 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.19.86.151 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 169.139.224.201 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 75.167.70.34 | United States | 147.237.76.86 | navy.idf.il | Unauthorized HTTP Method | Block | 1 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 37.142.168.150 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage | Block | 1 |
| 120.151.113.188 | Australia | 147.237.77.74 | law.idf.il | Illegal Byte Code Character in Method Â.. [[#0]][[#0]][[#0]]m[[#17]]ÃŠÃ„=xÃ~Ã> | Block | 1 |
| 2.54.158.78 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.64.176 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter searchText in eitan.aka.idf.il/1149-en/eitan.aspx | None | 1 |
| 185.32.179.195 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/sachar/index | Block | 1 |
| 84.111.248.7 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 149.78.136.147 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 77.247.181.162 | Netherlands | 147.237.77.216 | dover.idf.il | URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js | Block | 1 |
| 213.151.43.223 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 204.13.201.137 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 37.46.39.133 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.254 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx | None | 1 |
| 66.249.64.176 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter searchText in eitan.aka.idf.il/1028-en/eitan.aspx | None | 1 |
| 176.65.7.156 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/894-ar | Block | 1 |
| 95.35.85.8 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https://www.idf.il/ | Block | 1 |
| 80.179.141.237 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 176.13.2.64 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 75.167.70.34 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/apskbzqo.cgi | Block | 1 |
| 212.143.120.5 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 37.142.190.206 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |