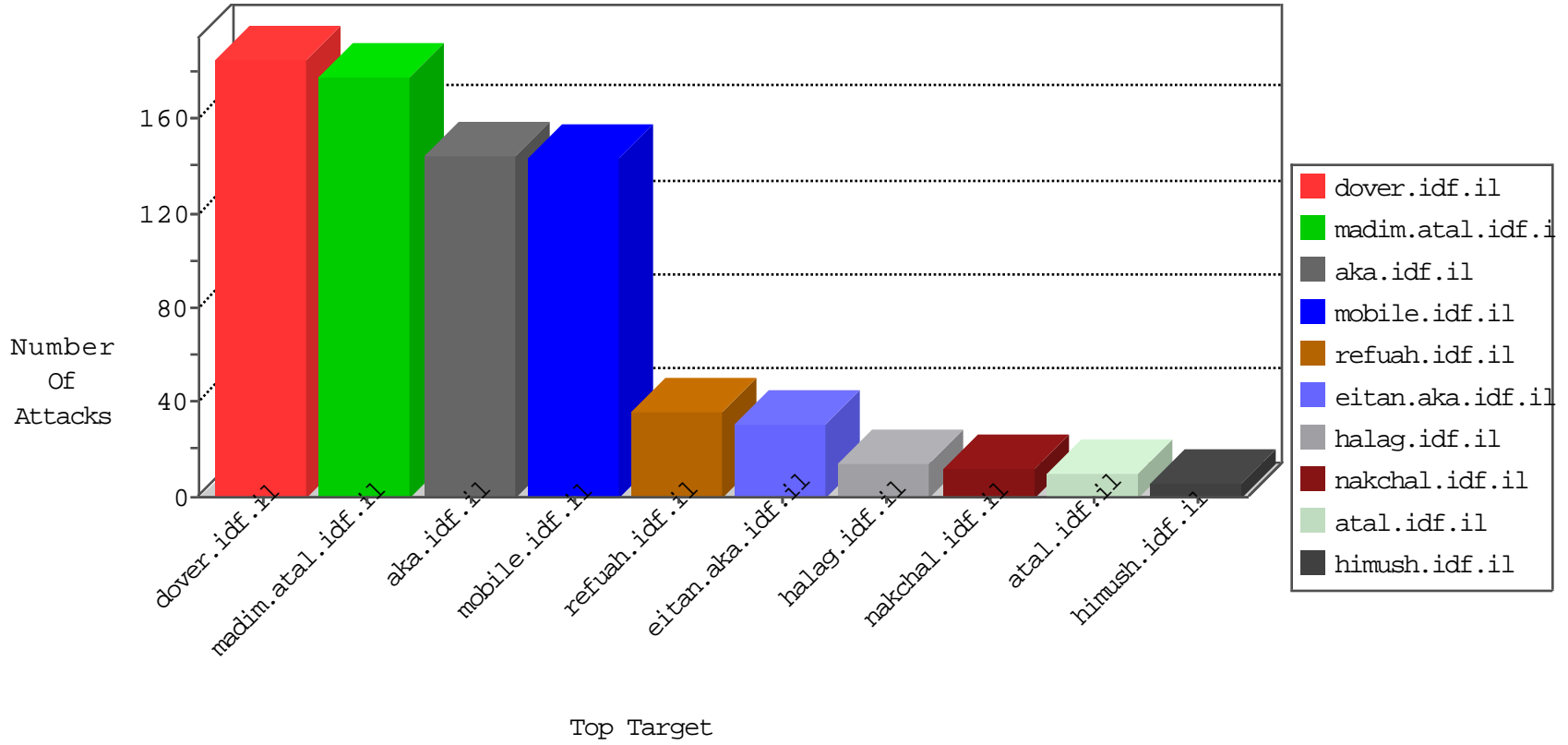


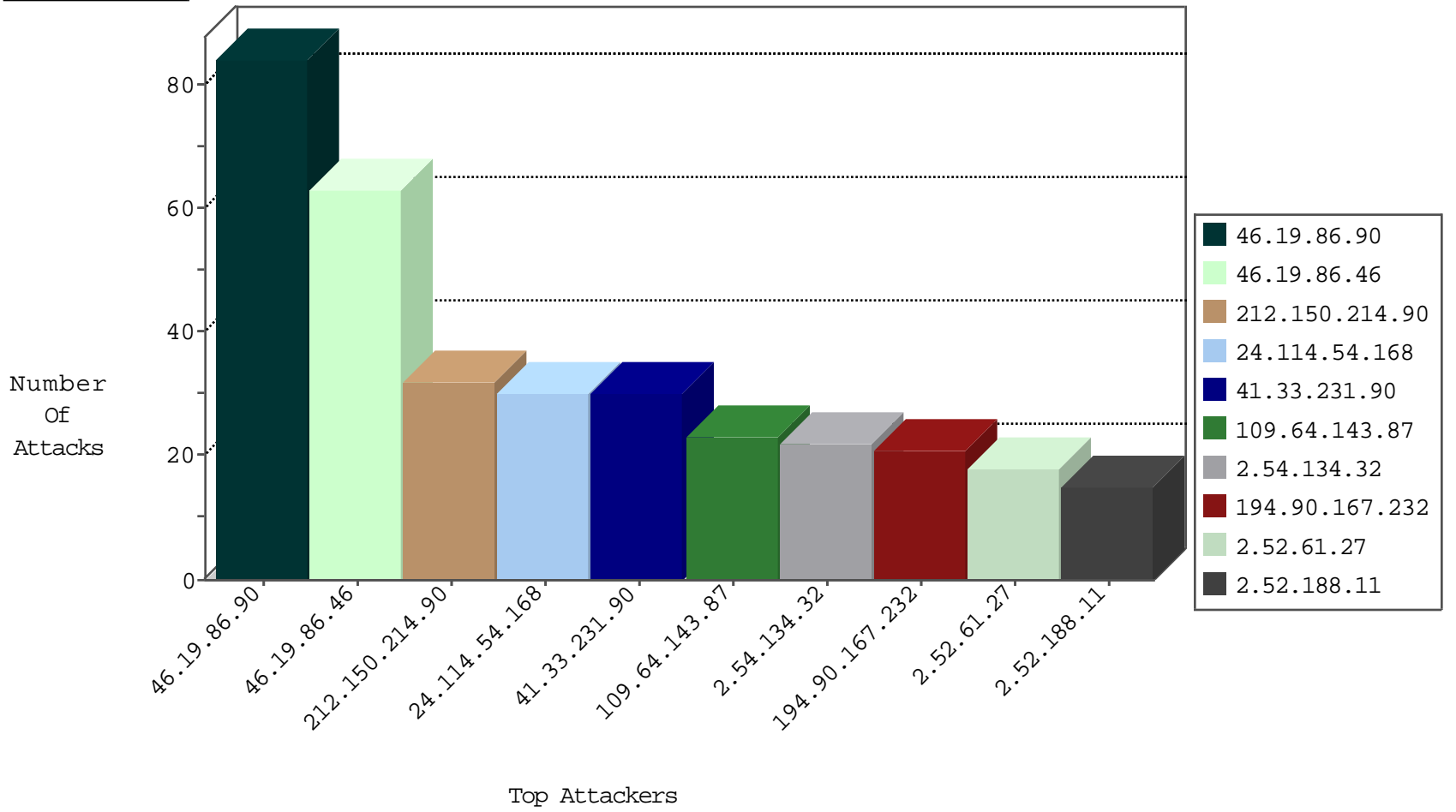
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|--------------------|----------------|------------------|----------------------------|---------------|-------|
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 211.58.138.167 | Korea, Republic of | 147.237.76.31 | nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 54.67.38.74 | United States | 147.237.76.42 | refuah.idf.il | DOS-httpdx-hreadrequest-FS | dest-reset | 1 |
| 211.58.138.167 | Korea, Republic of | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 54.67.38.74 | United States | 147.237.77.205 | prisha.idf.il | DOS-httpdx-hreadrequest-FS | dest-reset | 1 |
| 211.58.138.167 | Korea, Republic of | 147.237.76.201 | e.atal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 202.118.236.55 | China | 147.237.76.202 | e.halag.idf.il | Block_Udp_All_Nets | drop | 1 |
| 211.58.138.167 | Korea, Republic of | 147.237.76.202 | e.halag.idf.il | Block_Udp_All_Nets | drop | 1 |

Top Attackers In IPS

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

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|------------------|----------------|------------------|------------------------|---|-------|
| 212.199.57.207 | 147.237.76.30 | Israel | himush.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack | 4 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 183.60.48.25 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 137.117.105.139 | 147.237.0.200 | United States | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.76.23.7 | 147.237.0.19 | Bahrain | madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.82.64.190 | 147.237.0.16 | Netherlands | ny-kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 222.186.34.171 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 183.60.48.25 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 183.60.48.25 | 147.237.76.198 | China | e.yochalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.76.23.7 | 147.237.0.34 | Bahrain | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.76.14.46 | 147.237.0.16 | Bahrain | ny-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.151.53.217 | 147.237.0.200 | Ukraine | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.186.34.171 | 147.237.76.39 | China | mobile.meitav.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|--------------------------------|----------------|--------------------|---|--|---------------|-------|
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 24.114.54.168 | Canada | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 194.90.167.232 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 20 |
| 2.52.61.27 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 18 |
| 109.64.143.87 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 212.150.214.90 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 16 |
| 212.150.214.90 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 2.54.134.32 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 2.52.188.11 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 149.78.251.216 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.86.249 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 2.52.154.85 | Israel | 147.237.77.243 | mobile.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 37.26.146.206 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 79.181.229.121 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.189 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.120.15.31 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN 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 |
| 46.19.85.240 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.208 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.111 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.253.131.132 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.220 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.120.227.166 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.181.160.32 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.111 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.253.221.42 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.54.47.110 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.229 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 185.32.179.223 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.181.173.83 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.189 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.240 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 37.26.146.206 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | alert | 5 |
| 176.13.19.242 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 176.13.19.242 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 37.46.39.46 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.86.220 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 31.223.183.172 | Palestinian Territory Occupied | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 4 |
| 70.208.138.140 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 37.26.148.150 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.67.24.101 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 5.29.95.20 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 77.126.36.20 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 141.8.132.112 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.179.120.113 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 187.189.195.40 | Mexico | 147.237.8.24 | e.lifestyle.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 3 |
| 109.67.70.130 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 63.143.241.60 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 3 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|--------------------|----------------|------------------|---|---------------|-------|
| 46.19.86.90 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 82 |
| 46.19.86.46 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 63 |
| 5.29.90.95 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 5.29.90.95 | Block | 7 |
| 79.180.3.163 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword | Block | 6 |
| 37.26.148.150 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 37.26.148.150 | Block | 6 |
| 2.54.134.32 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 109.64.143.87 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 2.54.134.32 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 176.228.132.66 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 2.54.47.110 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 185.32.179.161 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 2.54.47.110 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 3 |
| 2.52.188.11 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.142.177.49 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 79.180.3.163 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 2.54.0.250 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 46.19.86.249 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.54.46.131 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 46.117.204.138 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 46.120.227.166 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.196 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 84.94.189.243 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 37.26.148.150 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1678 | Block | 2 |
| 79.179.150.9 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined | Block | 2 |
| 5.29.90.95 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1597 | Block | 2 |
| 176.13.7.72 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 1 |
| 194.90.167.232 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 109.253.221.42 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 5.167.133.137 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi'a=0 | Block | 1 |
| 85.65.99.36 | Israel | 147.237.72.166 | aka.idf.il | Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 85.65.99.36 | Block | 1 |
| 213.151.50.118 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx | None | 1 |
| 79.177.243.72 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/894-he/nakchal.aspx | Block | 1 |
| 46.120.129.152 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined | Block | 1 |
| 176.13.10.216 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 37.142.177.49 | Israel | 147.237.77.243 | mobile.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 204.13.201.138 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 66.249.78.240 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/70488.pdf | Block | 1 |
| 157.55.39.191 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewj-ienfrp_jahvdtbqkhd8_cw0qfggkmaq&sig2=lfjvi6ayozbqh88tgi4jzq&usg=afqjcnhcvyyg7w1cq-yhd5_amzoyodtwa | Block | 1 |
| 37.26.146.206 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 85.250.161.9 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 217.118.64.59 | Russian Federation | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 79.178.26.72 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.120.227.166 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 1 |
| 46.19.34.48 | Netherlands | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/ | Block | 1 |
| 79.181.229.121 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 5.29.42.229 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp | Block | 1 |
| 204.13.201.138 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 69.163.242.176 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/ | Block | 1 |