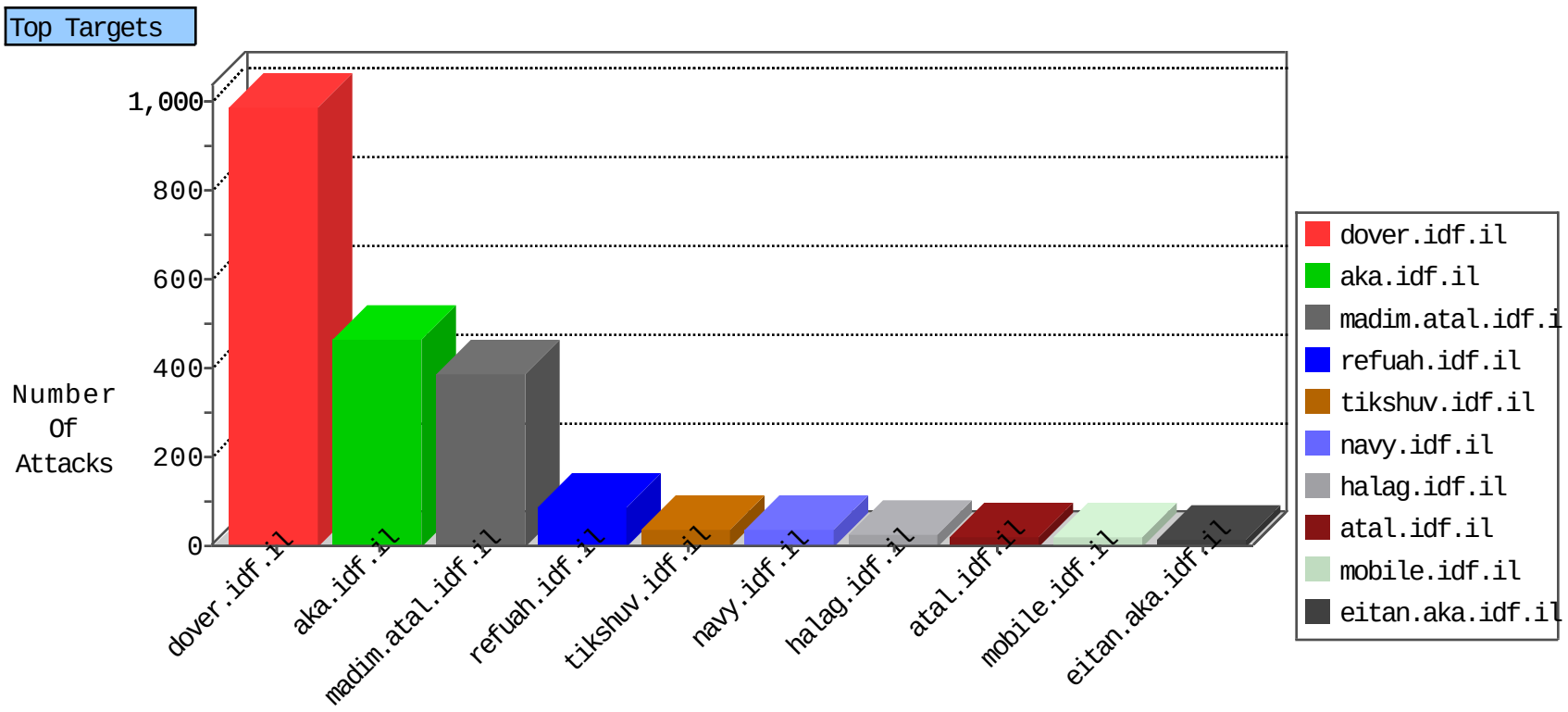
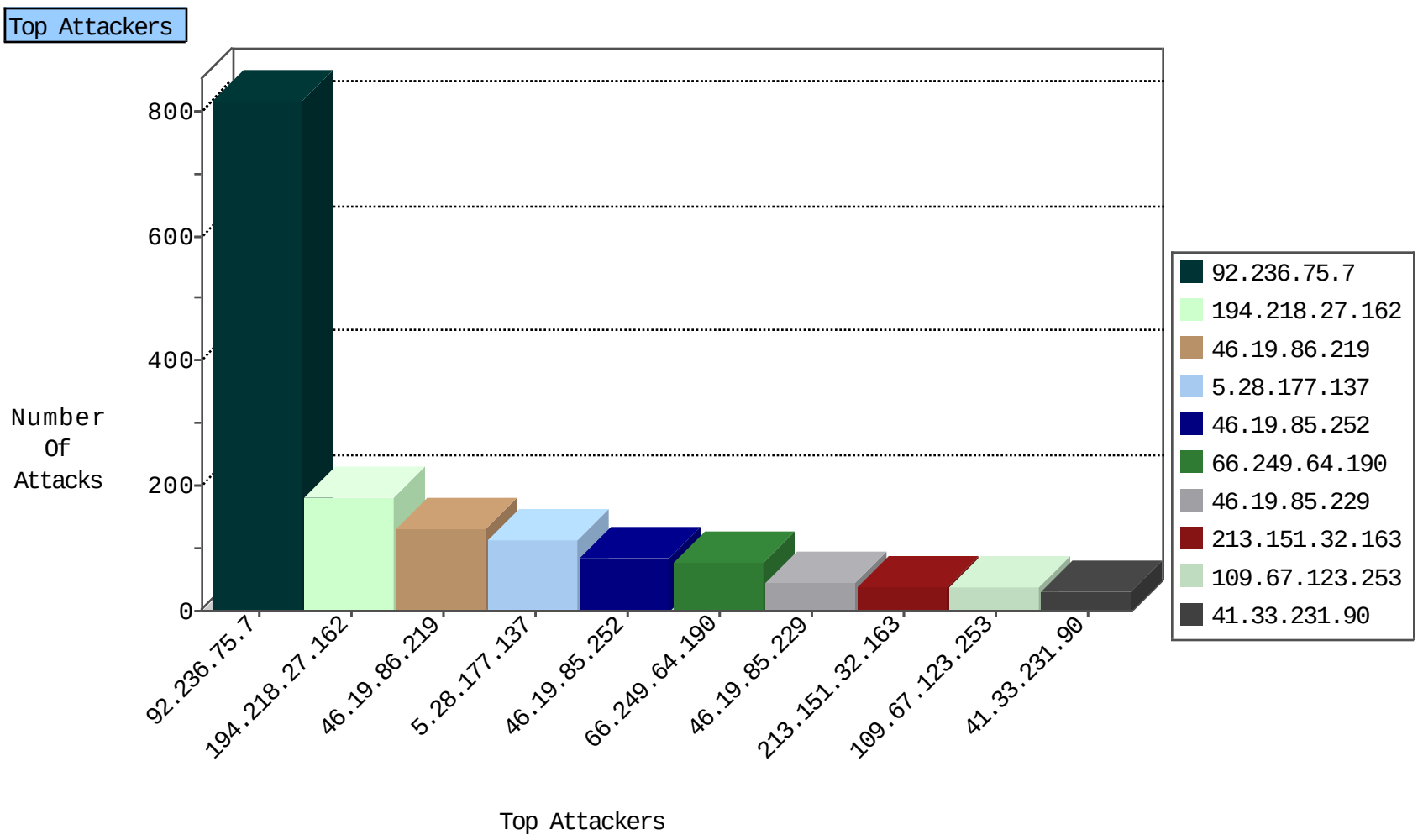
03-02-2016-22:04:04 to 03-02-2016-23:04:04

# IDF Under Attack Daily Report



03-02-2016-22:04:04 to 03-02-2016-23:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.65.181.46 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 6 |
| 81.218.65.210 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 146.185.239.100 | Russian Federation | 147.237.72.166 | aka.idf.il | block-sp-traf1 | drop | 1 |
| 164.132.54.194 | Italy | 147.237.72.166 | aka.idf.il | Block_Ntp_All_Net | drop | 1 |
| 1.245.176.64 | Korea, Republic of | 147.237.77.170 | maarachot.idf.il | Block_Udp_All_Nets | drop | 1 |
| 164.132.54.194 | Italy | 147.237.76.199 | e.nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 50.30.37.59 | United States | 147.237.8.14 | e.orchot.idf.il | Block_Udp_All_Nets | drop | 1 |
| 113.241.207.112 | China | 147.237.72.14 | dover.idf.il(old) | Block_Udp_All_Nets | drop | 1 |
| 54.72.182.187 | Ireland | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |

03-02-2016-22:04:04 to 03-02-2016-23:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 5.102.206.148 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 10 |
| 149.78.150.196 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 61.135.189.119 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 5 |
| 66.249.93.121 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 3 |
| 199.30.24.156 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 2.54.37.67 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 84.108.94.232 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 172.19.206.153 |  | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 185.24.207.50 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 109.253.220.133 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 66.249.93.117 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 123.126.113.80 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

03-02-2016-22:04:04 to 03-02-2016-23:04:04

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 92.236.75.7 | 147.237.77.216 | United Kingdom | dover.idf.il | WEB-MISC Chunked-Encoding transfer attempt | 8 |
| 80.246.133.89 | 147.237.77.170 | Israel | maarachot.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 62.210.69.71 | 147.237.76.147 | France | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 59.45.79.117 | 147.237.76.42 | China | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 59.45.79.117 | 147.237.8.45 | China | e.eitan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.211.77.35 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.216.176.244 | 147.237.76.42 | Latvia | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 120.71.117.5 | 147.237.77.74 | China | law.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 84.109.98.114 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.64.190 | 147.237.72.166 | United States | aka.idf.il | WEB-CGI redirect access | 1 |
| 60.217.72.16 | 147.237.76.44 | China | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 59.45.79.117 | 147.237.72.167 | China | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.246.0.97 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 137.226.113.7 | 147.237.76.30 | Germany | himush.idf.il | ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner | 1 |
| 94.102.48.193 | 147.237.77.178 | Netherlands | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 92.236.75.7 | 147.237.77.216 | United Kingdom | dover.idf.il | SERVER-WEBAPP DELETE attempt | 1 |

03-02-2016-22:04:04 to 03-02-2016-23:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 92.236.75.7 | United Kingdom | 147.237.77.216 | dover.idf.il | Command Injection | command injection detected in request: 'Sh' | monitor | 754 |
| 194.218.27.162 | Sweden | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 120 |
| 194.218.27.162 | Sweden | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 60 |
| 66.249.64.190 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 56 |
| 109.67.123.253 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 36 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 46.19.85.229 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 20 |
| 185.3.144.44 | Israel | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 20 |
| 79.177.181.177 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 2.124.229.205 | United Kingdom | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 46.19.85.229 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 12 |
| 92.236.75.7 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 10 |
| 107.150.24.158 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |
| 92.236.75.7 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 7 |
| 109.67.28.127 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 213.8.204.44 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 46.19.85.229 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 109.253.136.114 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.176.220.194 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.66.148.253 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.64.97.247 | Israel | 147.237.72.166 | aka.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 |
| 109.226.49.101 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.182.234.32 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.177.171.122 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 213.8.204.14 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 5.102.195.3 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 80.230.18.243 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 213.8.204.14 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | alert | 5 |
| 46.19.85.27 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 89.139.255.99 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 93.172.26.80 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 4 |
| 85.65.43.174 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 85.65.43.174 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.120.24.174 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 84.95.205.199 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 193.43.245.250 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.85.233 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 188.120.154.173 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 193.43.246.250 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 4 |
| 79.183.69.181 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.249.66.105 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.65.22.235 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 198.84.161.220 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 94.230.86.240 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 5.22.131.32 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.180.69.109 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.66.107.44 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.12 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.219 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 131 |
| 5.28.177.137 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 112 |
| 46.19.85.252 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 85 |
| 213.151.32.163 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 38 |
| 66.249.64.190 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 66.249.64.190 | Block | 18 |
| 92.236.75.7 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 14 |
| 92.236.75.7 | United Kingdom | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 92.236.75.7 | Block | 13 |
| 109.253.196.166 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 8 |
| 92.236.75.7 | United Kingdom | 147.237.77.216 | dover.idf.il | Multiple Unauthorized Request Content Type from 92.236.75.7 | Block | 7 |
| 87.69.26.102 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx | Block | 4 |
| 176.13.11.77 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 213.57.215.6 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.4.57 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 66.249.66.72 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 66.249.66.72 | Block | 3 |
| 66.249.66.75 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 66.249.66.75 | Block | 2 |
| 2.54.132.248 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx | Block | 2 |
| 66.249.66.78 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 66.249.66.78 | Block | 2 |
| 46.119.122.177 | Ukraine | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi/ | Block | 2 |
| 185.22.32.3 | Lebanon | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/arr/ | Block | 2 |
| 109.66.59.57 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 92.236.75.7 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized Request Content Type from 92.236.75.7 | Block | 2 |
| 84.108.27.14 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 37.142.168.95 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx | None | 1 |
| 207.46.13.89 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 1 |
| 168.9.214.221 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.93.14 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 94.159.159.232 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx | None | 1 |
| 46.117.205.24 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 87.251.222.124 | Sweden | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/arr/ | Block | 1 |
| 77.75.78.163 | Czech Republic | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/documents.asp | Block | 1 |
| 37.8.68.14 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Multiple Untraceable SSL Sessions from 37.8.68.14 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)) | None | 1 |
| 185.35.62.11 | Switzerland | 147.237.77.19 | law-forum.idf.il | Unauthorized URL Access to 147.237.77.19/ | Block | 1 |
| 66.249.74.100 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/coordinationofmed25022010.aspx | Block | 1 |
| 109.253.136.114 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 92.236.75.7 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized Request Content Type image/jpeg | Block | 1 |
| 66.249.64.190 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/valtam | Block | 1 |
| 85.65.43.174 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 40.77.167.0 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 213.8.204.14 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 68.180.228.95 | United States | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx | Block | 1 |
| 95.86.73.50 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx | None | 1 |
| 79.178.6.50 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/matash | Block | 1 |
| 37.8.68.14 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 185.35.62.11 | Switzerland | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to 147.237.77.226/ | Block | 1 |
| 66.249.79.195 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/list2.htm | Block | 1 |
| 92.236.75.7 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/3/1473.png | Block | 1 |
| 66.249.64.190 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter KEY in www.aka.idf.il/valtam/asp/default.asp | None | 1 |
| 213.8.204.18 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 46.19.85.170 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 2.54.134.202 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |