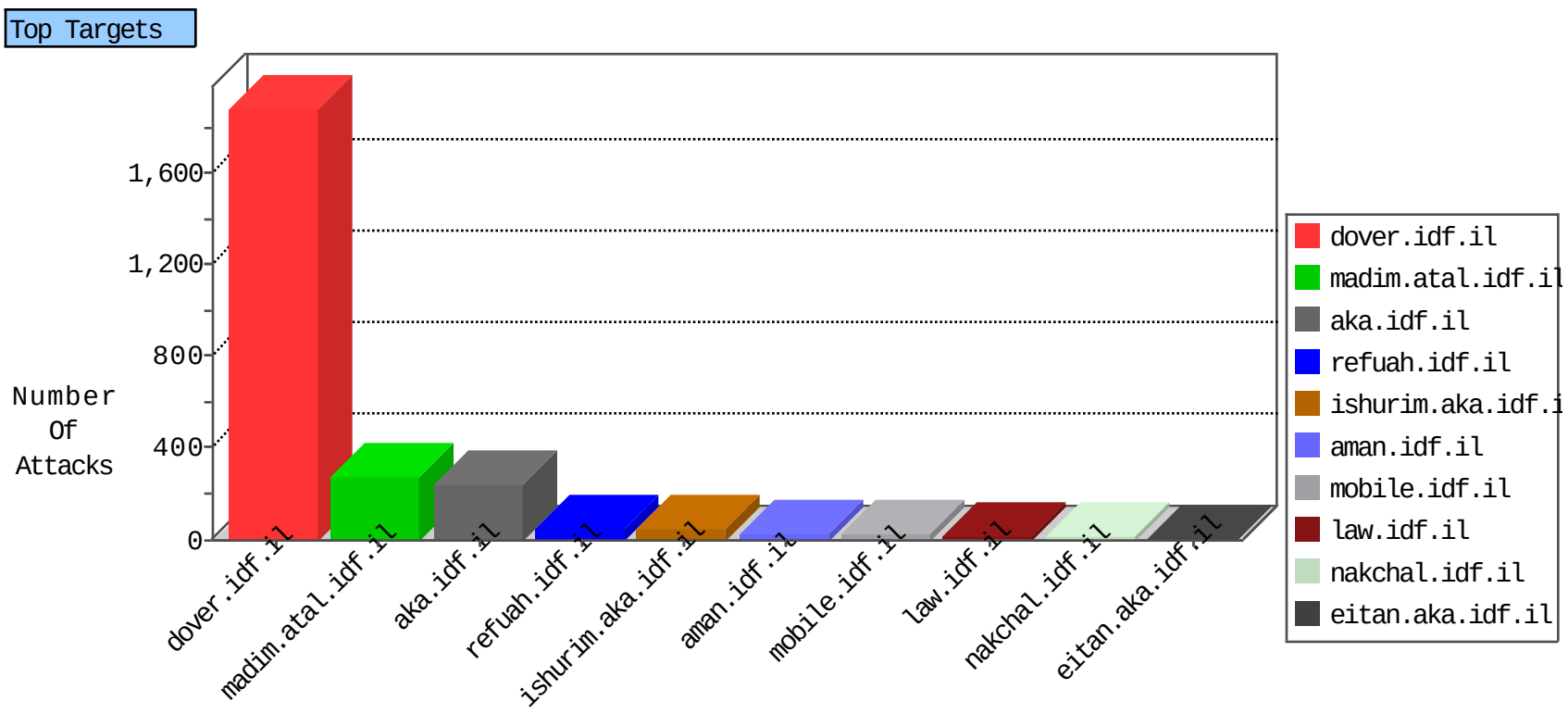
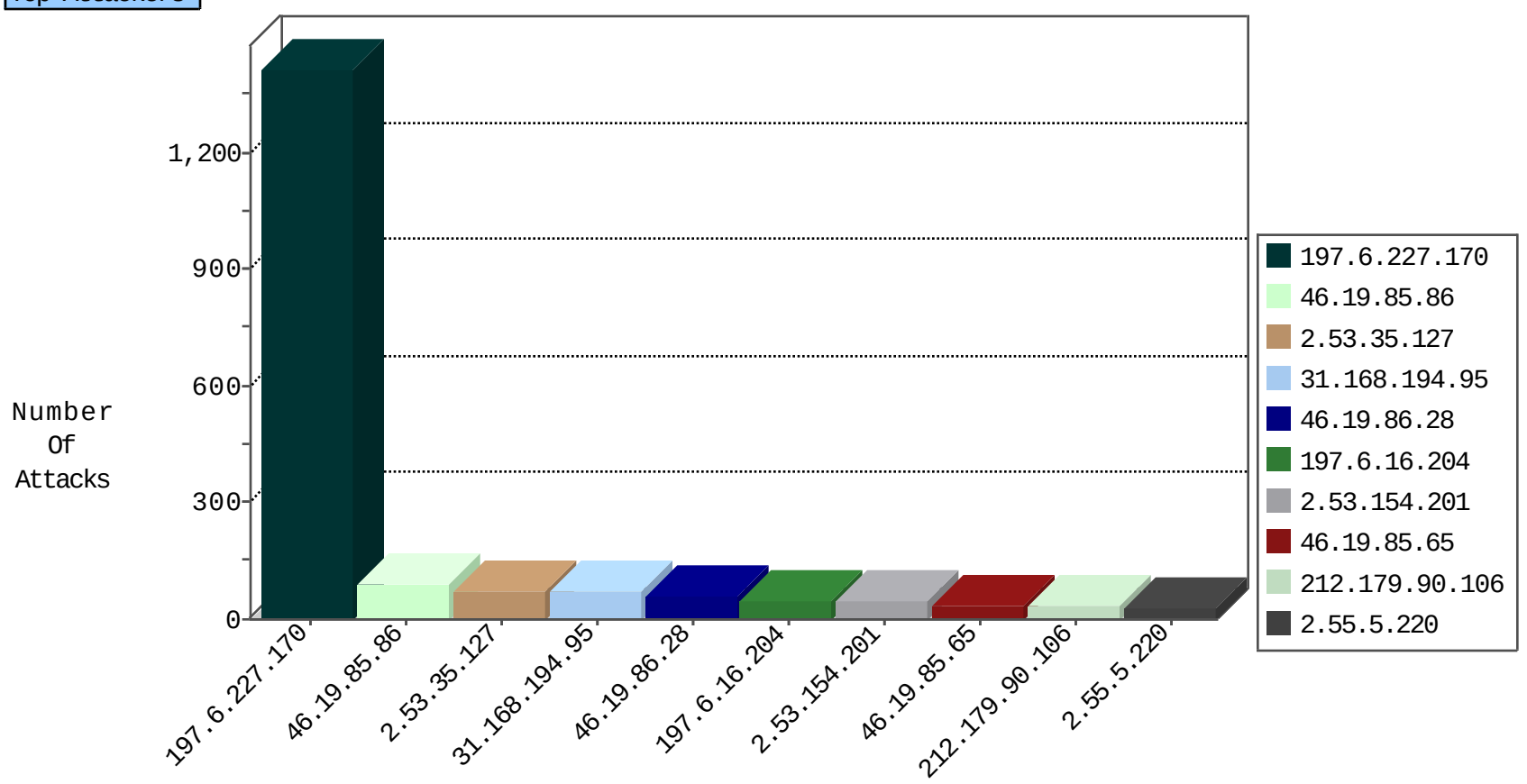
09-18-2016-09:04:08 to 09-18-2016-10:04:08

# IDF Under Attack Daily Report

Top Targets




Top Attackers



09-18-2016-09:04:08 to 09-18-2016-10:04:08

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 197.6.227.170 | Tunisia | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 1628 |
| 197.6.16.204 | Tunisia | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 95 |
| 31.168.194.95 | Israel | 147.237.72.166 | aka.idf.il | Black List | drop | 72 |
| 129.97.74.12 | Canada | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 5 |
| 130.195.4.69 | New Zealand | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 5 |
| 198.82.160.221 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 4 |
| 216.48.80.12 | Canada | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 129.10.120.193 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 164.107.127.12 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 129.93.229.139 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 46.19.86.141 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 3 |
| 134.117.226.180 | Canada | 147.237.72.217 | e.idf.il | network flood IPv4 ICMP | drop | 2 |
| 128.223.8.112 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 129.97.74.14 | Canada | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 77.124.32.66 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 204.85.191.10 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 165.242.90.128 | Japan | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 153.90.1.35 | United States | 147.237.72.14 | dover.idf.il(old) | network flood IPv4 ICMP | drop | 1 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 194.254.215.12 | France | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 139.78.141.243 | United States | 147.237.72.14 | dover.idf.il(old) | network flood IPv4 ICMP | drop | 1 |
| 128.223.8.114 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 156.56.250.227 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 195.113.161.84 | Czech Republic | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 147.83.29.234 | Spain | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 199.203.37.52 | Israel | 147.237.72.166 | aka.idf.il | Black List | drop | 1 |
| 128.10.18.52 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 153.90.1.34 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |

09-18-2016-09:04:08 to 09-18-2016-10:04:08

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 69.30.213.202 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 5.29.241.212 | Israel | 147.237.76.42 | refuah.idf.il | 15323: HTTP: User-Agent (MRSPUTNIK) | Block | 2 |
| 69.30.213.202 | United States | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |

09-18-2016-09:04:08 to 09-18-2016-10:04:08

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 73.14.6.116 | 147.237.77.74 | United States | law.idf.il | SQL Injection - Select From | 3 |
| 217.132.43.162 | 147.237.77.233 | Israel | atal.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 200.241.137.4 | 147.237.77.235 | Brazil | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.49.92 | 147.237.0.15 | Netherlands | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 77.126.49.223 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.69.103 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 31.168.65.25 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.53.138.248 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 216.72.40.185 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.102.49.92 | 147.237.0.34 | Netherlands | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.193.74.175 | 147.237.8.24 | Gibraltar | e.lifestyle.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.85.168 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.53.139.133 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

09-18-2016-09:04:08 to 09-18-2016-10:04:08

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 197.6.227.170 | Tunisia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 681 |
| 197.6.227.170 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 38 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 31 |
| 2.55.5.220 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 46.19.85.41 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 21 |
| 46.19.86.28 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 17 |
| 46.19.85.142 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 46.19.86.28 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 197.6.16.204 | Tunisia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 46.19.86.28 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 46.19.85.161 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 2.53.50.99 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.86.28 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 46.19.85.161 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 2.53.35.127 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 11 |
| 46.19.86.214 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 80.178.198.106 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 9 |
| 192.115.177.202 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 9 |
| 46.19.86.35 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 46.19.85.65 | Israel | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 8 |
| 79.182.51.233 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 62.0.236.1 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 176.13.12.241 | Israel | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 187.227.108.177 | Mexico | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.214 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 31.168.23.46 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 46.19.86.30 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 37.26.148.230 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.91 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 62.0.211.129 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 2.53.184.11 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.85.233 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 109.253.209.235 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 2.53.33.233 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.85.80 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 197.6.227.170 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 197.6.16.204 | Tunisia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 46.19.86.5 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 46.19.86.150 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 62.0.200.125 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.85.73 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 46.19.86.5 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.121.193.188 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 46.19.85.73 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 185.62.121.1 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 2.53.150.132 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 46.19.85.1 | Israel | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.86.35 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 193.43.246.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |

09-18-2016-09:04:08 to 09-18-2016-10:04:08

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.85.86 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 86 |
| 2.53.35.127 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 58 |
| 2.53.154.201 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 41 |
| 46.19.85.65 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 18 |
| 176.13.235.92 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 176.13.235.92 | Block | 13 |
| 109.253.241.3 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 10 |
| 46.19.85.24 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 10 |
| 77.127.87.30 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 109.253.196.100 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.136.112 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.53.164.231 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 195.160.242.40 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/ | Block | 3 |
| 80.246.137.191 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 37.26.146.193 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 185.32.179.196 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 46.19.85.65 | Israel | 147.237.0.19 | madim.atal.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 2.53.35.127 | Israel | 147.237.0.19 | madim.atal.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 2.53.56.205 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 194.90.15.61 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Unauthorized HTTP Method | Block | 2 |
| 176.13.234.73 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 37.26.146.154 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Untraceable SSL Sessions: Open Mode | None | 2 |
| 46.19.85.222 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 68.180.228.159 | United States | 147.237.77.176 | matpash.idf.il | Parameter Type Violation PageNum in www.cogat.idf.il/2063-he/cogat.aspx | Block | 1 |
| 2.55.44.230 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 157.55.39.238 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/main/misrot.aspx | Block | 1 |
| 95.86.84.121 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 62.219.137.5 | Israel | 147.237.72.156 | aman.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 194.90.15.61 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Unauthorized URL Access on www.nakhal.idf.il/sip_storage/files/2/ | Block | 1 |
| 79.180.156.201 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 2.53.176.122 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.64.183 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-ar | Block | 1 |
| 46.19.86.28 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx | None | 1 |
| 212.199.57.197 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 84.111.102.241 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew | Block | 1 |
| 80.246.130.175 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 37.26.148.239 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 71.235.28.21 | United States | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 1 |
| 2.55.164.108 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 157.55.39.238 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp | None | 1 |
| 2.53.157.254 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.253.133.10 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.102.9.26 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/main/home/default.aspx | Block | 1 |
| 80.246.138.67 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 194.90.15.61 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/ | Block | 1 |
| 37.26.146.248 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 176.13.245.17 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 79.180.174.181 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 2.53.180.162 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.79.139 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 66.249.79.139 | Block | 1 |
| 52.16.137.212 | Ireland | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to / | Block | 1 |

09-18-2016-09:04:08 to 09-18-2016-10:04:08