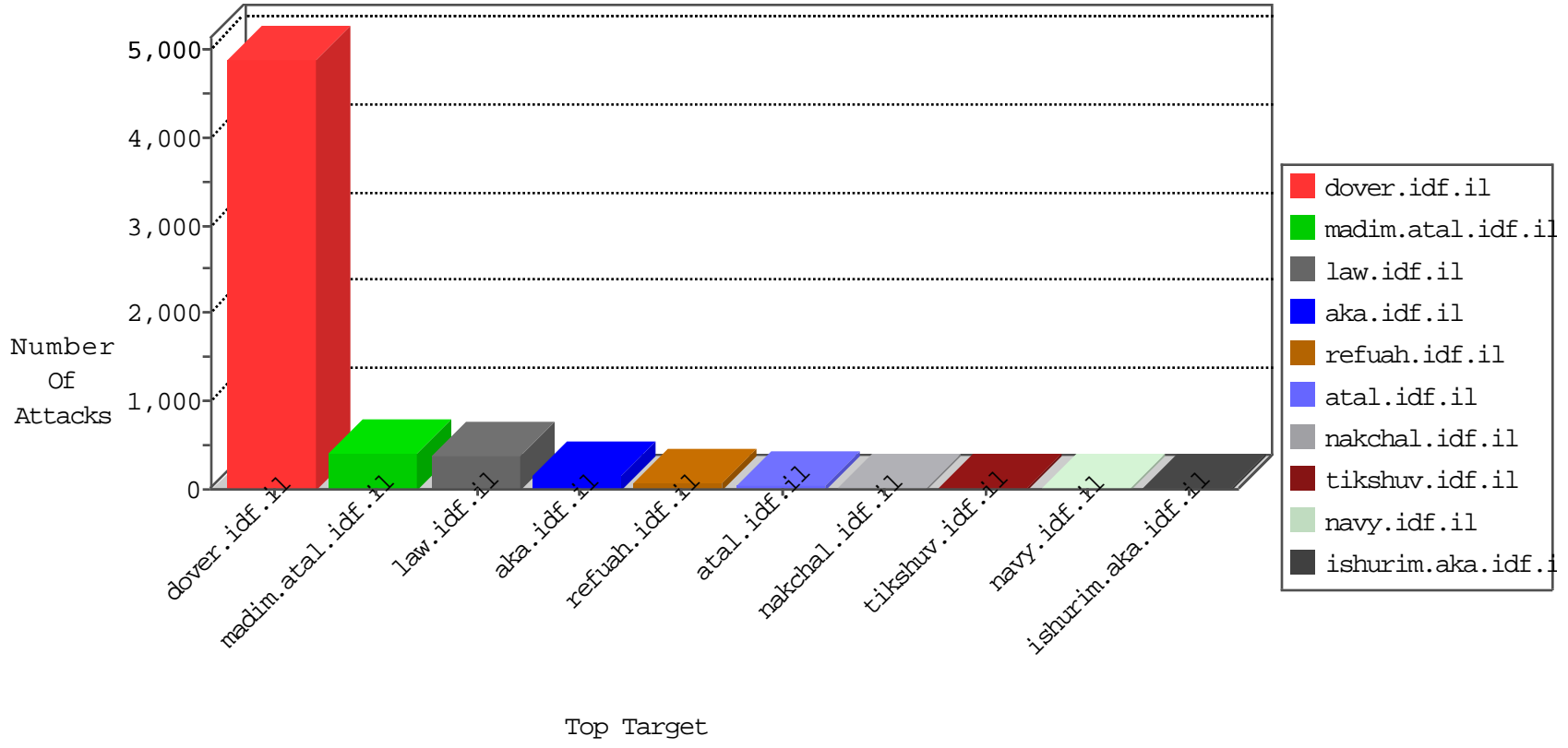


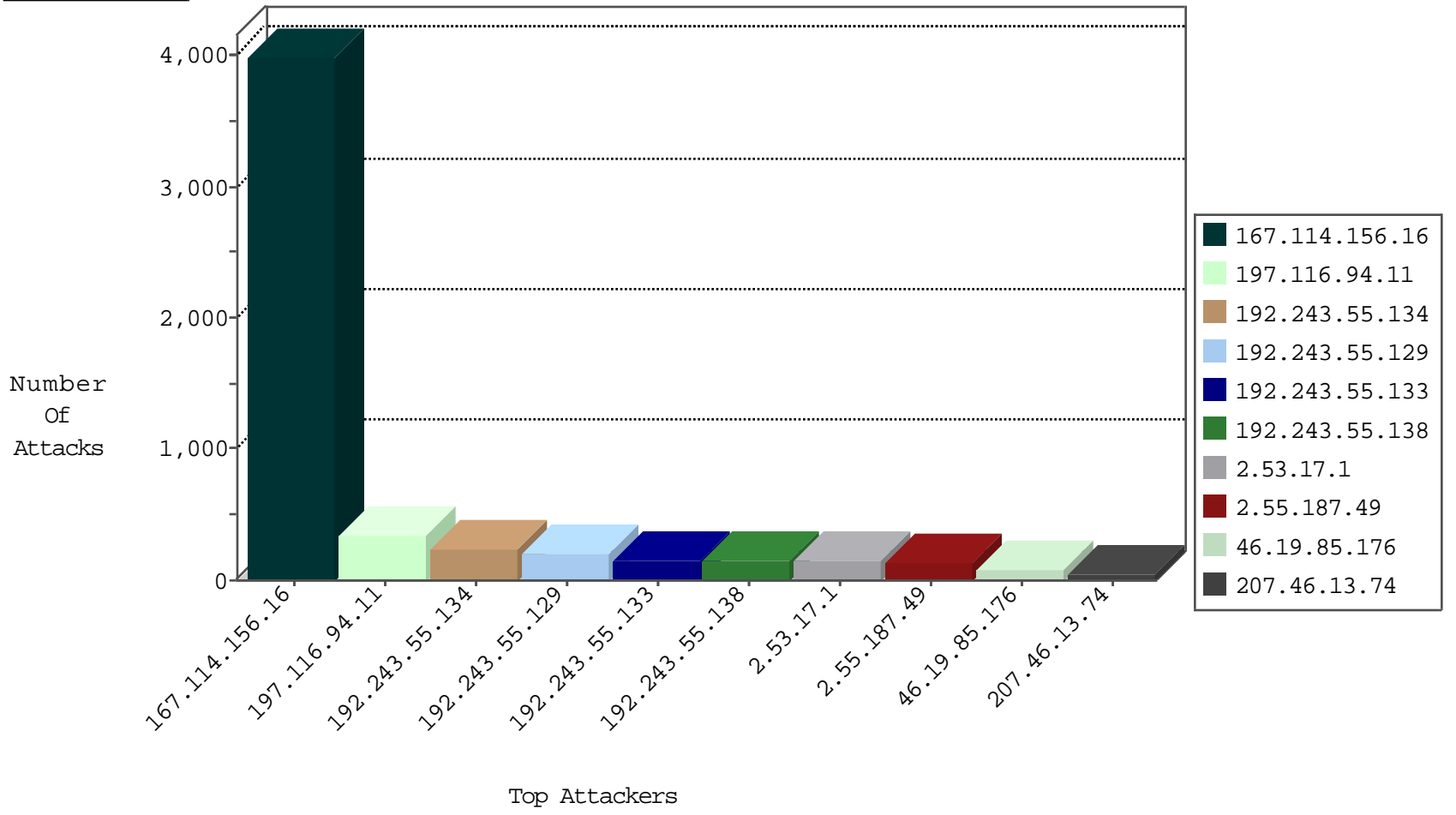
IDF Under Attack Daily Report



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 | Block_Tp_Web_In | drop | 3970 |
| 197.116.94.11 | Algeria | 147.237.77.216 | dover.idf.il | DOS-HTTP-flooding | dest-reset | 827 |
| 197.116.94.11 | Algeria | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 145 |
| 81.218.65.210 | Israel | 147.237.77.176 | matpash.idf.il | Block_Udp_All_Nets | drop | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 3 |
| 165.214.11.70 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 79.178.122.196 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 207.244.89.138 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 79.183.200.210 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 94.102.49.116 | Netherlands | 147.237.77.61 | e.cogat.idf.il | Block_Ntp_All_Net | drop | 1 |
| 71.6.135.131 | United States | 147.237.8.24 | e.lifestyle.idf.il | Block_Udp_All_Nets | drop | 1 |
| 207.244.89.138 | United States | 147.237.77.227 | e.hamaz.idf.il | Block_Udp_All_Nets | drop | 1 |
| 132.66.90.101 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 72.14.191.154 | United States | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 84.94.172.38 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 207.244.89.138 | United States | 147.237.76.86 | navy.idf.il | Block_Udp_All_Nets | drop | 1 |
| 151.51.6.191 | Italy | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 84.108.249.169 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|----------------|---|---------------|-------|
| 149.78.168.201 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 8 |
| 84.108.129.162 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 199.58.86.209 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 82.102.168.106 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 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 | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 61.135.189.122 | China | 147.237.76.31 | nakchal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.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 |
| 106.185.37.254 | Japan | 147.237.77.216 | dover.idf.il | C1000016: HTTP: administrator in URI | Block | 1 |
| 86.34.138.111 | Romania | 147.237.77.216 | dover.idf.il | C1000008: HTTP: Xenu UserAgent | 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 |
| 2.55.43.200 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 208.100.26.228 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 176.13.22.224 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 132.64.145.132 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 113.240.250.154 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.82.78.38 | 147.237.0.35 | Netherlands | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.19.86.55 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.139.35.239 | 147.237.0.15 | Russian Federation | kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 217.132.32.255 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 163.172.140.23 | 147.237.77.212 | United Kingdom | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 113.240.250.154 | 147.237.77.234 | China | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.173.149.42 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.183.200.210 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.26.147.179 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|------------------|------------------|----------------|----------------|--|---|---------------|-------|
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 35 |
| 192.243.55.134 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 32 |
| 192.243.55.134 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 30 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 28 |
| 192.243.55.134 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 28 |
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 27 |
| 192.243.55.134 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 25 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 24 |
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 23 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 22 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 22 |
| 192.243.55.134 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 22 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 22 |
| 192.243.55.134 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 19 |
| 207.46.13.74 | United States | 147.237.77.233 | atal.idf.il | drop | SAM rule | drop | 18 |
| 192.243.55.134 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 18 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 18 |
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 17 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 17 |
| 94.230.86.223 | Israel | 147.237.76.31 | nakchal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 16 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 15 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 15 |
| 192.243.55.134 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 15 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 13 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 13 |
| 197.116.94.11 | Algeria | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 12 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 12 |
| 46.19.85.105 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 192.243.55.134 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | | monitor | 12 |
| 207.46.13.74 | United States | 147.237.76.42 | refuah.idf.il | drop | SAM rule | drop | 12 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 207.46.13.74 | United States | 147.237.77.234 | halag.idf.il | drop | SAM rule | drop | 11 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 192.243.55.134 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 10 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 10 |
| 192.243.55.133 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 10 |
| 192.243.55.134 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 10 |
| 217.132.0.33 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 9 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 9 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 192.243.55.138 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 46.19.85.149 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 197.116.94.11 | Algeria | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 8 |

Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|------------------|------------------|----------------|------------------------|--|---------------|-------|
| 2.53.17.1 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 143 |
| 2.55.187.49 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 135 |
| 46.19.85.176 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 78 |
| 197.116.94.11 | Algeria | 147.237.77.216 | dover.idf.il | Post Request - Missing Content Type from 197.116.94.11 | Block | 18 |
| 46.19.86.202 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 18 |
| 5.189.190.212 | Germany | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 10 |
| 79.176.120.3 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 5 |
| 46.19.85.183 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 193.43.246.250 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 46.120.160.9 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 176.13.17.228 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.147.207 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.148.153 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 132.70.66.11 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 80.246.137.205 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 195.160.242.40 | Israel | 147.237.77.74 | law.idf.il | Unauthorized HTTP Method | Block | 2 |
| 46.19.85.251 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 78.180.83.242 | Turkey | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 78.180.83.242 | Block | 2 |
| 46.19.86.186 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 193.43.245.250 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 2 |
| 149.88.229.51 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https://www.idf.il/ | Block | 1 |
| 79.183.197.204 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp | Block | 1 |
| 66.249.66.190 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/robots.txt | Block | 1 |
| 207.46.13.72 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 130.185.155.10 | Sweden | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/wp-login.php | Block | 1 |
| 2.53.13.206 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 1 |
| 31.13.100.113 | Ireland | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 157.55.39.65 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 80.246.130.74 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.69.19 | Israel | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |
| 212.23.180.86 | France | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to 147.237.76.147/ | Block | 1 |
| 195.160.242.40 | Israel | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 195.160.242.40 | Block | 1 |
| 79.176.134.155 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 197.116.94.11 | Algeria | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 66.6.46.229 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/994-9223-he/atal.aspx#.vw0fzgcqpxs.tumblr | Block | 1 |
| 37.26.146.210 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 68.180.230.45 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 213.57.158.104 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/giyus/general | Block | 1 |
| 132.72.172.229 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 2.53.176.94 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 1 |
| 79.179.210.60 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 199.30.25.103 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.66.128 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/994-8736-he/atal.aspx | Block | 1 |
| 188.71.234.21 | Kuwait | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/arr/ | Block | 1 |
| 108.30.160.135 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 213.57.229.155 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp | Block | 1 |
| 195.244.23.42 | Israel | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/gen204 | Block | 1 |
| 149.88.90.36 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/atall/izkor/main.asp | Block | 1 |
| 79.181.25.134 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.66.186 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/oref/ | Block | 1 |