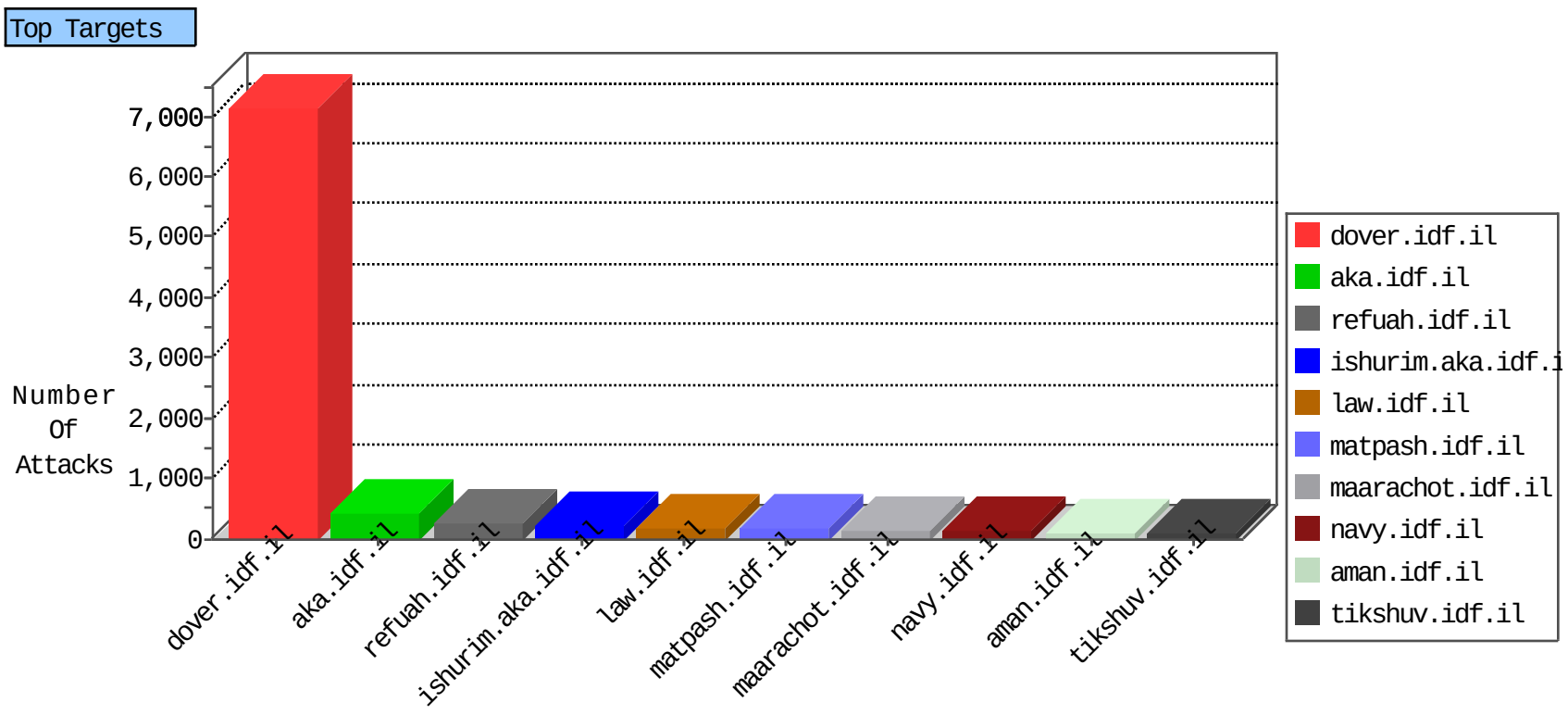
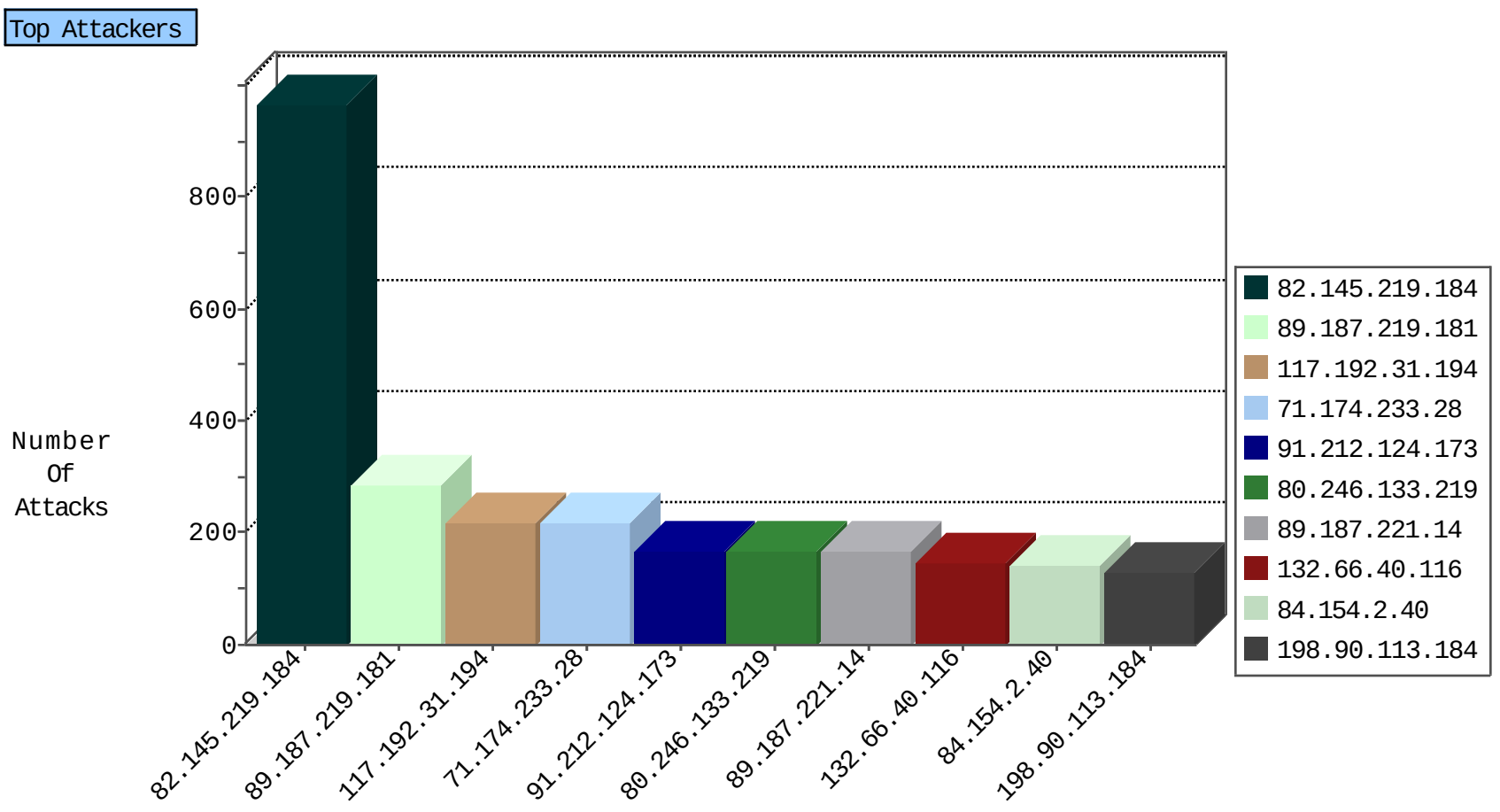
10-22-2015-13:04:02 to 10-22-2015-14:04:02

# IDF Under Attack Daily Report

Top Targets




Top Attackers



10-22-2015-13:04:02 to 10-22-2015-14:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1401 |
| 85.158.138.21 | Germany | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1259 |
| 66.249.67.227 | United States | 147.237.77.176 | matpash.idf.il | TCP handshake violation, first packet not syn | drop | 824 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 201 |
| 80.246.136.181 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 123 |
| 93.172.178.130 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 15 |
| 88.191.108.74 | France | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 14 |
| 84.94.26.182 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 9 |
| 46.19.85.189 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 46.19.86.28 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 176.106.226.115 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-SSL-renegotiation-Cli | dest-reset | 8 |
| 212.199.9.109 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 176.13.12.242 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 8 |
| 66.249.67.219 | United States | 147.237.77.176 | matpash.idf.il | TCP handshake violation, first packet not syn | drop | 6 |
| 31.210.187.240 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 6 |
| 79.180.179.204 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 176.12.136.150 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 46.19.86.110 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 5 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 4 |
| 85.250.84.54 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 185.32.179.169 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 176.13.15.171 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 80.246.136.17 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 37.26.146.233 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 212.199.224.24 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 87.68.80.171 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 188.247.65.118 | Jordan | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 2.126.39.144 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 85.65.32.165 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 176.12.136.207 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 46.19.85.162 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 2 |
| 71.174.233.28 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 2 |
| 2.52.171.24 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 119.25.44.205 | Japan | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 37.26.149.147 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 14.202.136.39 | Australia | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 194.56.215.66 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 176.228.134.243 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 2.52.144.241 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 1 |
| 66.249.67.59 | United States | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |

10-22-2015-13:04:02 to 10-22-2015-14:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 81.218.198.54 | Israel | 147.237.77.216 | dover.idf.il | C1000004: HTTP: options method (Microsoft) | Block | 1 |

10-22-2015-13:04:02 to 10-22-2015-14:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 82.80.196.44 | 147.237.72.166 | Israel | aka.idf.il | POLICY-OTHER TCP packet with urgent flag attempt | 6 |
| 93.173.165.180 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.250.72.49 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.78.159 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 223.71.180.106 | 147.237.8.24 | China | e.lifestyle.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.19.86.123 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 193.105.134.220 | 147.237.76.86 | Sweden | navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.26.146.195 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 176.13.17.210 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 5.29.93.6 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 133.36.145.13 | 147.237.77.216 | Japan | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.102.48.194 | 147.237.76.201 | Netherlands | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 89.139.160.61 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.109.226.29 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.180.174.26 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 223.71.180.106 | 147.237.8.45 | China | e.eitan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.120.35.92 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.199.175.138 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.26.148.163 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.198.151.44 | 147.237.72.167 | Europe | ishurim.aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 5.43.204.36 | 147.237.77.216 | Palestinian Territory, Occupied | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.78.90.27 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.19.165 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 115.236.75.201 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |

10-22-2015-13:04:02 to 10-22-2015-14:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 82.145.219.184 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 967 |
| 89.187.219.181 | Lebanon | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 284 |
| 117.192.31.194 | India | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 219 |
| 71.174.233.28 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 216 |
| 80.246.133.219 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 166 |
| 89.187.221.14 | Lebanon | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 152 |
| 132.66.40.116 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 144 |
| 84.154.2.40 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 142 |
| 198.90.113.184 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 130 |
| 84.154.7.85 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 116 |
| 86.108.12.231 | Jordan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 105 |
| 194.56.215.66 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 87 |
| 14.202.136.39 | Australia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 82 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 81 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 81 |
| 185.58.201.28 | Lebanon | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 76 |
| 85.158.138.21 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 74 |
| 194.90.83.233 | Israel | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 63 |
| 108.59.253.71 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 62 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 60 |
| 176.12.142.192 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 59 |
| 84.228.49.197 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 58 |
| 116.66.133.28 | India | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 57 |
| 31.210.187.207 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 53 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 52 |
| 80.246.133.104 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 51 |
| 185.27.105.134 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 50 |
| 81.218.251.252 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 50 |
| 5.35.55.193 | Russian Federation | 147.237.0.34 | tikshuv.idf.il | drop | First packet isn't SYN | drop | 50 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 44 |
| 41.218.182.44 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 41 |
| 212.117.138.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 39 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 39 |
| 188.247.65.118 | Jordan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 39 |
| 93.172.184.58 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 193.191.208.195 | Belgium | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 37 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 46.19.86.72 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 35 |
| 91.228.167.109 | Slovakia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 35 |
| 212.179.146.134 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 34 |
| 100.100.101.141 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 33 |
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 31 |
| 46.19.86.25 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 31 |
| 137.95.1.11 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 212.179.21.194 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 46.19.86.61 | Israel | 147.237.72.156 | aman.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 66.249.78.159 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 89.138.198.148 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 30 |
| 37.142.115.206 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 29 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 91.212.124.173 | Ukraine | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 84 |
| 68.180.230.29 | United States | 147.237.77.176 | matpash.idf.il | Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx | Block | 84 |
| 91.212.124.173 | Ukraine | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 91.212.124.173 | Block | 70 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 56 |
| 46.19.85.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx | Block | 42 |
| 212.143.212.222 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp | Block | 42 |
| 46.19.86.116 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 28 |
| 84.55.42.31 | Lithuania | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to /tmunblock.cgi | Block | 14 |
| 66.249.67.53 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp | Block | 14 |
| 207.46.13.39 | United States | 147.237.0.34 | tikshuv.idf.il | Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx | Block | 14 |
| 151.80.31.115 | Italy | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/iraq/english/info07.asp | Block | 14 |
| 37.8.45.111 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-22777-ar/dover.aspx) | Block | 14 |
| 89.247.29.4 | Germany | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx | Block | 14 |
| 46.19.85.103 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 188.143.232.10 | Russian Federation | 147.237.77.176 | matpash.idf.il | Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx | Block | 14 |
| 109.65.39.217 | Israel | 147.237.72.166 | aka.idf.il | Multiple Untraceable SSL Sessions from 109.65.39.217 (Protocol violation (SSL_CONN_CLIENT_HELLO)) | None | 14 |
| 84.111.100.184 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx | Block | 14 |
| 66.249.67.65 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/robots.txt | Block | 14 |
| 207.46.13.119 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 207.46.13.119 | Block | 14 |
| 157.55.39.26 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 37.187.56.47 | France | 147.237.76.86 | navy.idf.il | Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 14 |
| 91.55.189.253 | Germany | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx | Block | 14 |
| 79.180.191.176 | Israel | 147.237.72.166 | aka.idf.il | Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter | None | 14 |
| 194.114.146.227 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1777.jpg | Block | 14 |
| 109.65.39.217 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 14 |
| 85.65.191.119 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/aman | Block | 14 |
| 66.249.78.104 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 14 |
| 162.243.188.75 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to / | Block | 14 |
| 37.187.56.47 | France | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 37.187.56.47 | Block | 14 |
| 80.246.133.130 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2009.jpg | Block | 14 |
| 46.19.86.9 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 14 |
| 199.203.215.1 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 14 |
| 109.67.153.95 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx | None | 14 |
| 87.68.165.148 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 14 |
| 66.249.78.173 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp | Block | 14 |
| 176.12.136.239 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 14 |
| 37.187.56.47 | France | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper | Block | 14 |
| 81.218.65.98 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 14 |
| 203.133.169.32 | Korea, Republic of | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx | Block | 14 |
| 141.212.122.96 | United States | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to /x | Block | 14 |
| 88.75.177.215 | Germany | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx | Block | 14 |
| 185.27.105.134 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif | Block | 14 |
| 46.19.85.14 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 14 |
| 91.212.124.173 | Ukraine | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/592-4071-en/index.php | Block | 14 |