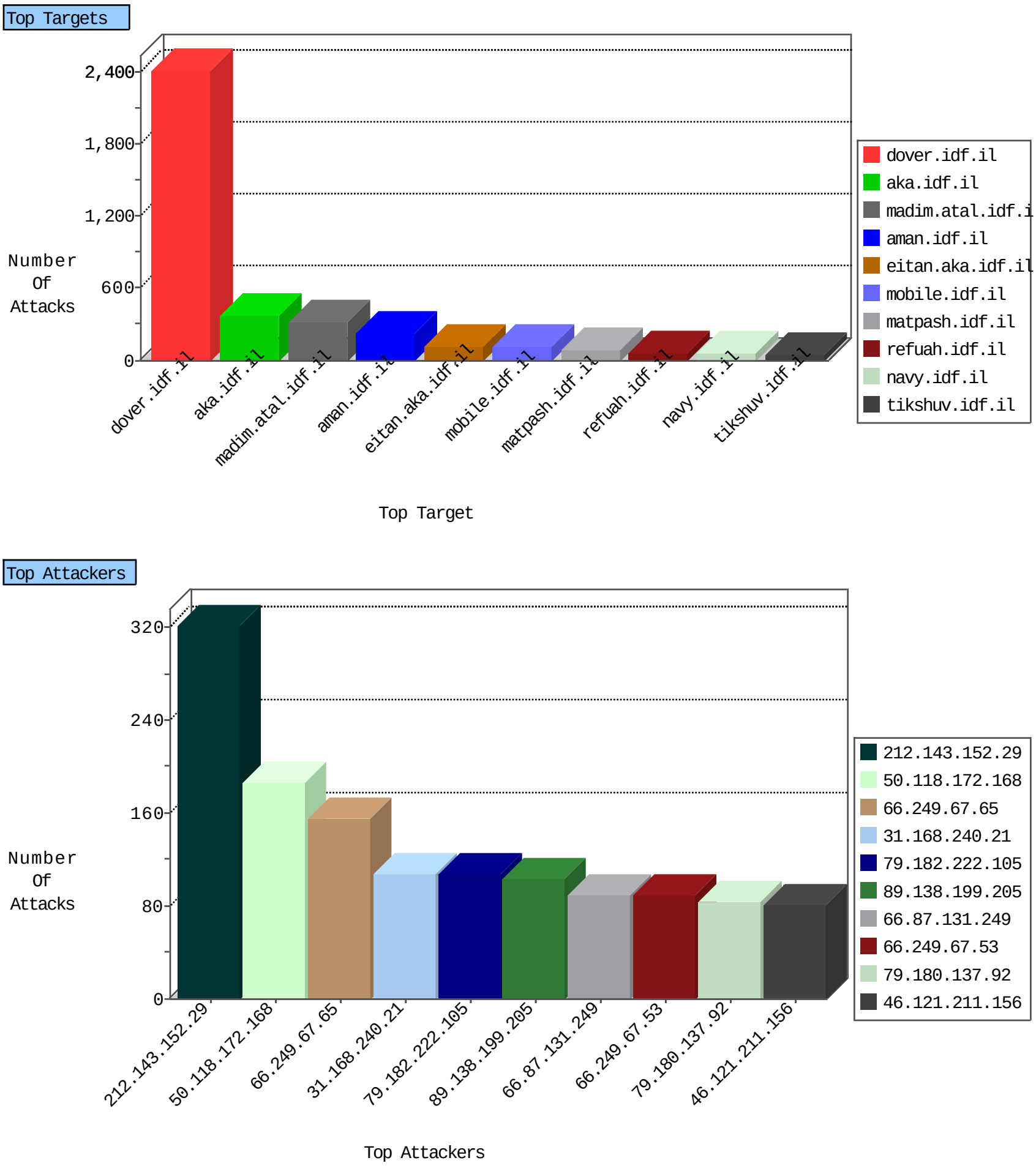
10-24-2015-20:04:04 to 10-24-2015-21:04:04

# IDF Under Attack
# Daily Report



10-24-2015-20:04:04 to 10-24-2015-21:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.67.73 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 15017 |
| 66.249.67.194 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 945 |
| 66.249.67.202 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 499 |
| 66.249.67.210 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 23 |
| 46.19.85.146 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 23 |
| 46.121.80.207 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 8 |
| 79.182.208.179 | Israel | 147.237.72.156 | aman.idf.il | Block_Udp_All_Nets | drop | 6 |
| 2.54.27.226 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 4 |
| 37.142.131.161 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood full table | drop | 3 |
| 185.61.136.94 | Ukraine | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 100.100.109.241 | | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 142.54.174.70 | United States | 147.237.76.42 | refuah.idf.il | block-sp-traf1 | drop | 1 |
| 203.133.170.9 | Korea, Republic of | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 103.13.96.170 | India | 147.237.0.33 | idf.il | L4 Source or Dest Port Zero | drop | 1 |
| 173.208.168.166 | United States | 147.237.0.34 | tikshuv.idf.il | block-sp-traf1 | drop | 1 |
| 79.176.96.65 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 103.13.96.170 | India | 147.237.8.24 | e.lifestyle.idf.il | L4 Source or Dest Port Zero | drop | 1 |
| 185.61.136.94 | Ukraine | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |
| 46.116.149.191 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood unverified cookie | drop | 1 |
| 142.54.172.101 | United States | 147.237.76.39 | mobile.meitav.idf.il | block-sp-traf1 | drop | 1 |

10-24-2015-20:04:04 to 10-24-2015-21:04:04

## Top Attackers In IPS

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

10-24-2015-20:04:04 to 10-24-2015-21:04:04

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 5 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 177.87.104.30 | 147.237.0.17 | Brazil | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 2 |
| 177.87.104.30 | 147.237.76.202 | Brazil | e.halag.idf.il | ET SCAN Potential SSH Scan | 2 |
| 66.249.67.235 | 147.237.77.176 | United States | matpash.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 177.87.104.30 | 147.237.77.205 | Brazil | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.0.15 | Brazil | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.77.61 | Brazil | e.cogat.idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.244.216.171 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 177.87.104.30 | 147.237.76.197 | Brazil | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 104.197.108.188 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 177.87.104.30 | 147.237.76.147 | Brazil | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 88.249.106.23 | 147.237.77.61 | Turkey | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.236.47.157 | 147.237.72.167 | Korea, Republic of | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.76.42 | Brazil | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.162.116.221 | 147.237.76.148 | Sweden | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 222.236.47.157 | 147.237.72.14 | Korea, Republic of | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.72.217 | Brazil | e.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.8.46 | Brazil | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.77.235 | Brazil | sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.0.34 | Brazil | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.77.216 | Brazil | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.77.74 | Brazil | law.idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.244.216.171 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 118.244.216.171 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -f -sS | 1 |
| 177.87.104.30 | 147.237.76.176 | Brazil | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.236.47.157 | 147.237.72.217 | Korea, Republic of | e.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.102.48.194 | 147.237.77.61 | Netherlands | e.cogat.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 177.87.104.30 | 147.237.76.44 | Brazil | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 222.236.47.157 | 147.237.72.156 | Korea, Republic of | aman.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.76.34 | Brazil | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.20.69.98 | 147.237.76.201 | United States | e.atal.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 177.87.104.30 | 147.237.72.156 | Brazil | aman.idf.il | ET SCAN Potential SSH Scan | 1 |
| 186.129.12.9 | 147.237.77.216 | Argentina | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 177.87.104.30 | 147.237.0.35 | Brazil | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.77.227 | Brazil | e.hamaz.idf.il | ET SCAN Potential SSH Scan | 1 |
| 177.87.104.30 | 147.237.0.33 | Brazil | idf.il | ET SCAN Potential SSH Scan | 1 |

10-24-2015-20:04:04 to 10-24-2015-21:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 50.118.172.168 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 186 |
| 79.182.222.105 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 108 |
| 89.138.199.205 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 104 |
| 66.87.131.249 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 90 |
| 46.121.211.156 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 68 |
| 93.173.247.146 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 57 |
| 207.228.78.161 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 56 |
| 79.183.195.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 36 |
| 2.105.134.180 | Denmark | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 34 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 34 |
| 212.179.42.241 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 66.249.67.65 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 26 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 68.180.230.29 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 24 |
| 151.80.31.115 | Italy | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 24 |
| 100.100.109.241 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 23 |
| 64.46.23.242 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 40.77.167.37 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 20 |
| 66.249.67.53 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 20 |
| 77.126.83.99 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 19 |
| 66.249.81.215 | Russian Federation | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 212.179.90.106 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 16 |
| 37.46.36.51 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 46.116.169.4 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 74.62.240.62 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 15 |
| 173.54.199.156 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 100.100.36.242 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 14 |
| 109.200.30.154 | United Kingdom | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 198.58.103.92 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 5.22.129.235 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 100.100.14.255 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 93.172.22.161 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 66.249.81.218 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 37.26.149.128 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 100.100.45.94 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 109.65.177.138 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 100.100.6.215 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 107.167.112.7 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 100.100.64.27 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 89.138.221.170 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 37.26.149.128 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 176.12.138.38 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 66.249.67.59 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 212.143.152.29 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 212.143.152.29 | Block | 308 |
| 66.249.67.65 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.67.65 | Block | 98 |
| 79.180.137.92 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp | Block | 84 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 56 |
| 66.249.67.53 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.67.53 | Block | 56 |
| 31.168.240.21 | Israel | 147.237.72.156 | aman.idf.il | Distributed Unauthorized HTTP Method | Block | 56 |
| 109.160.190.203 | Israel | 147.237.77.176 | matpash.idf.il | Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx | Block | 42 |
| 31.168.240.21 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/ | Block | 38 |
| 46.19.85.235 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432 | Block | 28 |
| 188.120.148.241 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/maim/sachar | Block | 28 |
| 46.120.74.200 | Israel | 147.237.72.156 | aman.idf.il | Distributed Unauthorized HTTP Method | Block | 28 |
| 46.19.85.235 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 46.19.85.235 | Block | 28 |
| 212.143.152.29 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many 404: Response Code per Session | Block | 14 |
| 5.29.95.197 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 14 |
| 176.12.143.37 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 14 |
| 84.228.67.49 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 14 |
| 66.249.67.79 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/general/×œ×§×©×¨ ×œ×—×§×§ ×©×ž×¡×¡×¡ ×¢×œ ×—×™×¨×” | Block | 14 |
| 198.1.101.123 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 109.186.190.120 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 77.126.24.250 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/ | Block | 14 |
| 95.86.116.75 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 14 |
| 66.249.67.194 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/ | Block | 14 |
| 199.16.156.125 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/17401.jpg | Block | 14 |
| 151.80.31.123 | Italy | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/ | Block | 14 |
| 77.126.24.250 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/ | Block | 14 |
| 66.249.67.59 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.67.59 | Block | 14 |
| 213.151.36.128 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 14 |
| 31.168.240.21 | Israel | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 31.168.240.21 | Block | 14 |
| 188.165.15.162 | France | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8688-he/refuah.aspx | Block | 14 |
| 109.65.205.66 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 199.16.156.126 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 199.16.156.126 | Block | 14 |
| 46.120.74.200 | Israel | 147.237.72.156 | aman.idf.il | Multiple Unauthorized URL Access from 46.120.74.200 | Block | 14 |
| 173.252.74.101 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/1740.png | Block | 14 |
| 66.249.67.65 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 190.234.11.118 | Peru | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 14 |
| 109.67.68.115 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/ | Block | 14 |
| 68.180.228.175 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 14 |
| 199.16.156.126 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17418.jpg | Block | 14 |
| 46.120.74.200 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/ | Block | 14 |
| 176.12.141.229 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 14 |
| 84.109.190.15 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx | None | 14 |
| 192.99.39.235 | Canada | 147.237.0.34 | tikshuv.idf.il | Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx | Block | 14 |
| 46.121.211.156 | Israel | 147.237.76.42 | refuah.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$ucFaqControl$txtSearch in www.refua.atal.idf.il/1540-he/refuah.aspx | Block | 13 |
| 66.249.81.130 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 10 |

10-24-2015-20:04:04 to 10-24-2015-21:04:04