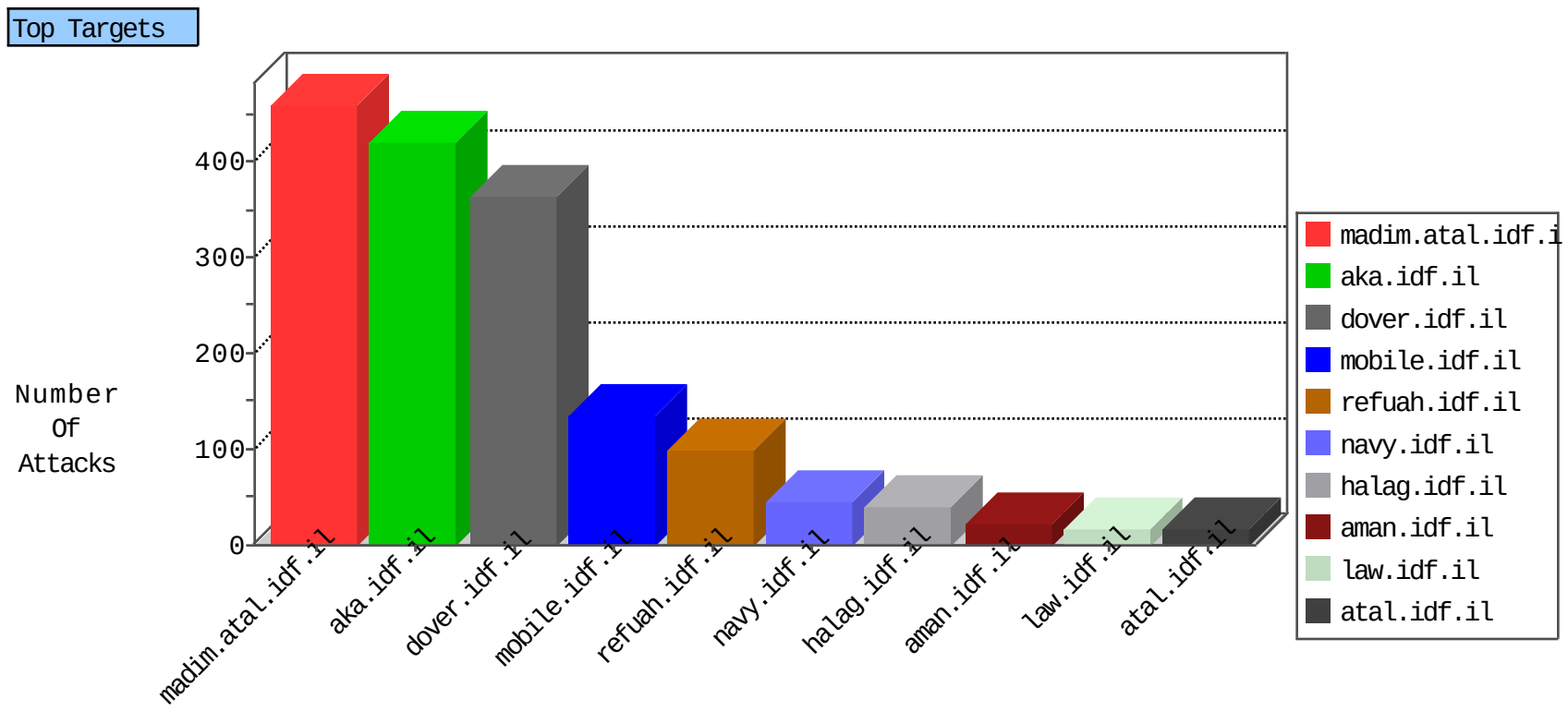
02-01-2016-20:04:04 to 02-01-2016-21:04:04

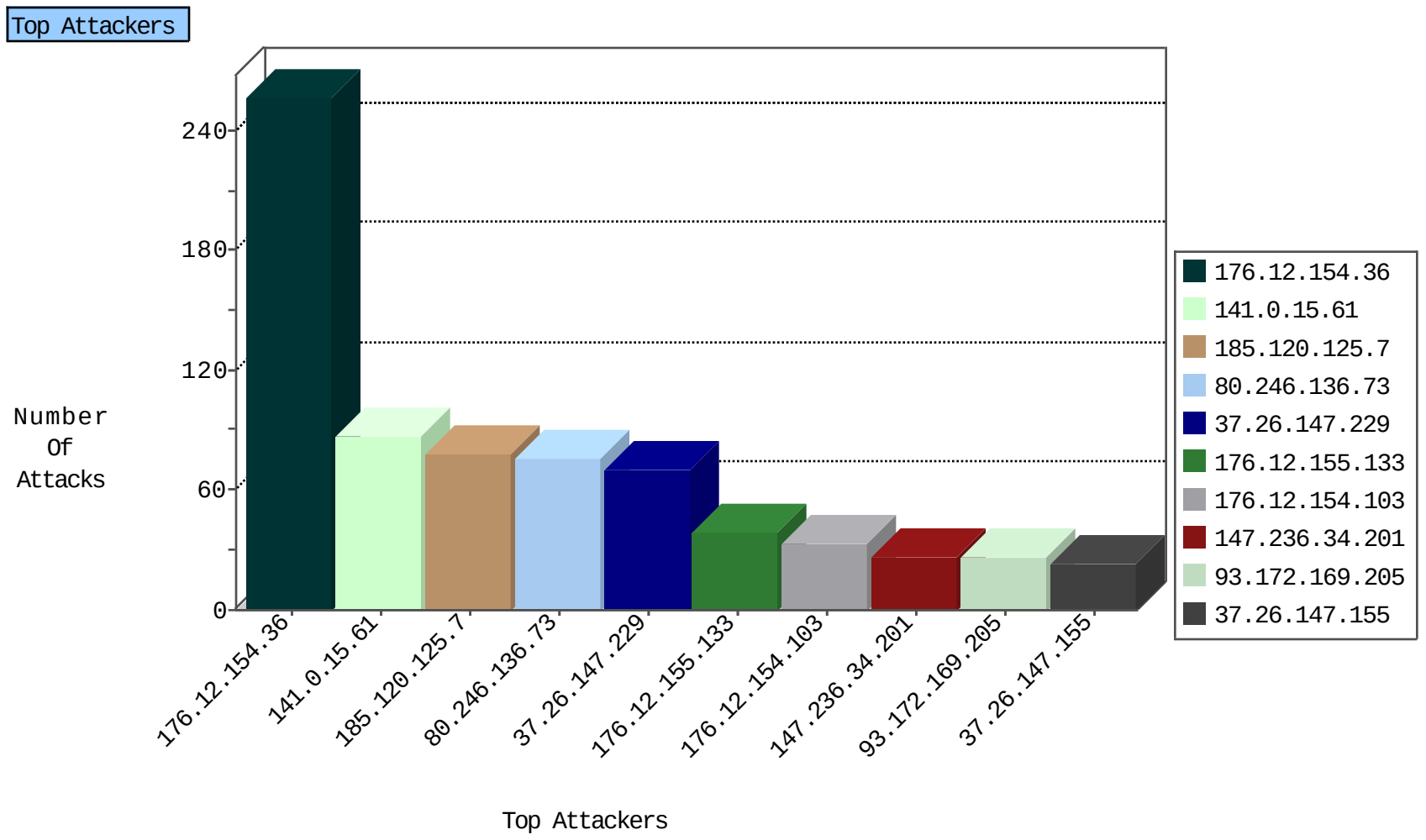
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

02-01-2016-20:04:04 to 02-01-2016-21:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 10 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 4 |
| 158.69.123.26 | United States | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 175.180.50.205 | Taiwan | 147.237.76.147 | chinuch.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 82.137.14.180 | Romania | 147.237.76.176 | test.ncore.idf.il | Block_Udp_All_Nets | drop | 1 |
| 175.180.50.205 | Taiwan | 147.237.76.148 | gqcenter.aka.idf.il | Block_Udp_All_Nets | drop | 1 |
| 142.54.169.163 | United States | 147.237.76.30 | himush.idf.il | block-sp-traf1 | drop | 1 |

02-01-2016-20:04:04 to 02-01-2016-21:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 151.80.31.151 | Italy | 147.237.72.166 | aka.idf.il | C228: HTTP: AhrefBot crawler | Block | 2 |
| 151.80.31.151 | Italy | 147.237.77.74 | law.idf.il | C228: HTTP: AhrefBot crawler | Block | 2 |
| 151.80.31.150 | Italy | 147.237.72.166 | aka.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |
| 151.80.31.153 | Italy | 147.237.76.42 | refuah.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |
| 151.80.31.150 | Italy | 147.237.77.74 | law.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |
| 151.80.31.154 | Italy | 147.237.72.166 | aka.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |
| 188.165.15.81 | France | 147.237.77.226 | www.chamatz.aka.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |
| 188.165.225.121 | France | 147.237.72.166 | aka.idf.il | 0543: HTTP: php.cgi Access | Block | 1 |
| 104.151.242.62 | United States | 147.237.77.216 | dover.idf.il | C008: HTTP: Xenu UserAgent | Block | 1 |
| 151.80.31.152 | Italy | 147.237.77.74 | law.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |

02-01-2016-20:04:04 to 02-01-2016-21:04:04

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 | 10 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 62.90.131.234 | 147.237.77.216 | Israel | dover.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 2 |
| 176.12.154.32 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 46.19.85.61 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 146.185.33.94 | 147.237.77.216 | Lebanon | dover.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 27.0.12.180 | 147.237.76.42 | Vietnam | refuah.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 87.69.190.212 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.65.140.243 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.109.149.24 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 218.246.0.97 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 80.83.135.131 | 147.237.77.170 | Georgia | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 209.126.116.147 | 147.237.8.27 | United States | e.madim.atal.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 79.178.63.56 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.247.74.186 | 147.237.77.216 | Jordan | dover.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 1 |
| 185.72.179.1 | 147.237.77.205 |  | prisha.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 46.19.86.70 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 149.78.154.69 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 128.39.168.79 | 147.237.8.46 | Norway | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 2.54.157.183 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 87.68.86.165 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.64.120.57 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 80.83.135.131 | 147.237.77.179 | Georgia | e.mazi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 209.126.116.147 | 147.237.72.14 | United States | dover.idf.il(old) | ET SCAN NMAP -sS window 1024 | 1 |
| 79.181.173.133 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.93.182 | 147.237.72.166 | United States | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 188.120.133.107 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 60.248.250.18 | 147.237.0.35 | Taiwan | akaws.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |

02-01-2016-20:04:04 to 02-01-2016-21:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 141.0.15.61 | Europe | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 87 |
| 185.120.125.7 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 52 |
| 185.120.125.7 | | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 26 |
| 37.26.147.229 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 26 |
| 37.26.147.229 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 93.172.169.205 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 25 |
| 107.167.116.69 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 22 |
| 176.12.155.217 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 37.26.147.229 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 16 |
| 147.236.34.201 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 46.19.86.121 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 176.12.155.142 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 84.108.173.95 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 2.54.0.37 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 10 |
| 147.236.34.201 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 80.246.130.194 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 9 |
| 185.32.179.144 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 185.120.125.3 | | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 37.26.149.228 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 185.3.147.203 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 109.65.254.46 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 213.151.32.163 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 46.19.86.14 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.86.209 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 37.26.147.155 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 7 |
| 37.26.147.155 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 46.19.86.122 | Israel | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 94.230.84.212 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 46.19.85.97 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.12.154.109 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 109.66.154.245 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.147.155 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 185.3.147.125 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.219 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 2.54.130.161 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.65.254.46 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 37.142.225.6 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.210.238.36 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 5.22.131.106 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 77.125.144.171 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 87.68.242.66 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 46.19.86.14 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 109.65.254.46 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 2.54.169.114 | Israel | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 188.120.148.251 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 2.54.169.114 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 5.102.254.29 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.86.104 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.12.154.36 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 130 |
| 176.12.154.36 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 97 |
| 80.246.136.73 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 75 |
| 176.12.155.133 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 39 |
| 176.12.154.103 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 33 |
| 176.12.154.36 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (403) | Block | 30 |
| 46.19.85.174 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 17 |
| 79.182.240.30 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 15 |
| 109.186.173.101 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 109.186.173.101 | Block | 8 |
| 46.19.85.157 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 2.54.14.148 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 176.12.155.217 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 82.81.250.122 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx | Block | 4 |
| 46.19.86.237 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 213.151.32.163 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 81.169.144.135 | Germany | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 81.169.144.135 | Block | 3 |
| 79.176.209.171 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.188 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.177.15.233 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.65.147.29 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.118 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 213.57.106.54 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/ | Block | 2 |
| 176.12.155.142 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 185.32.179.144 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.179.189.111 | Israel | 147.237.76.147 | chinuch.aka.idf.i | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 2 |
| 109.186.173.101 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/ | Block | 2 |
| 188.165.225.121 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 188.165.225.121 | Block | 2 |
| 157.55.39.93 | United States | 147.237.72.166 | aka.idf.il | Abnormally Long Request URL | Block | 1 |
| 68.180.230.29 | United States | 147.237.77.176 | matpash.idf.il | Parameter Type Violation PageNum in www.cogat.idf.il/1962-he/cogat.aspx | Block | 1 |
| 46.121.59.130 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 93.172.169.205 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 80.246.130.253 | Israel | 147.237.76.42 | refuah.idf.il | Suspicious Response Code | Block | 1 |
| 46.19.85.97 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 176.228.133.58 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.178.8.239 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 109.67.168.151 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.78.15 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx | Block | 1 |
| 82.166.20.192 | Israel | 147.237.72.166 | aka.idf.il | Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+) | None | 1 |
| 46.19.86.187 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif | None | 1 |
| 212.199.152.204 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 2.54.130.161 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.182.58.241 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main.gius | Block | 1 |
| 157.55.39.220 | United States | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/robots.txt | Block | 1 |
| 68.180.230.224 | United States | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation PageNum in www.nakhal.idf.il/994-he/nakhal.aspx | Block | 1 |
| 62.90.147.211 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 213.57.106.54 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/main/home/default.aspx | Block | 1 |
| 109.64.21.41 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 1 |
| 185.3.147.125 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.179.25.205 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown SSL Session | None | 1 |
| 66.249.78.147 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 66.249.78.147 | Block | 1 |