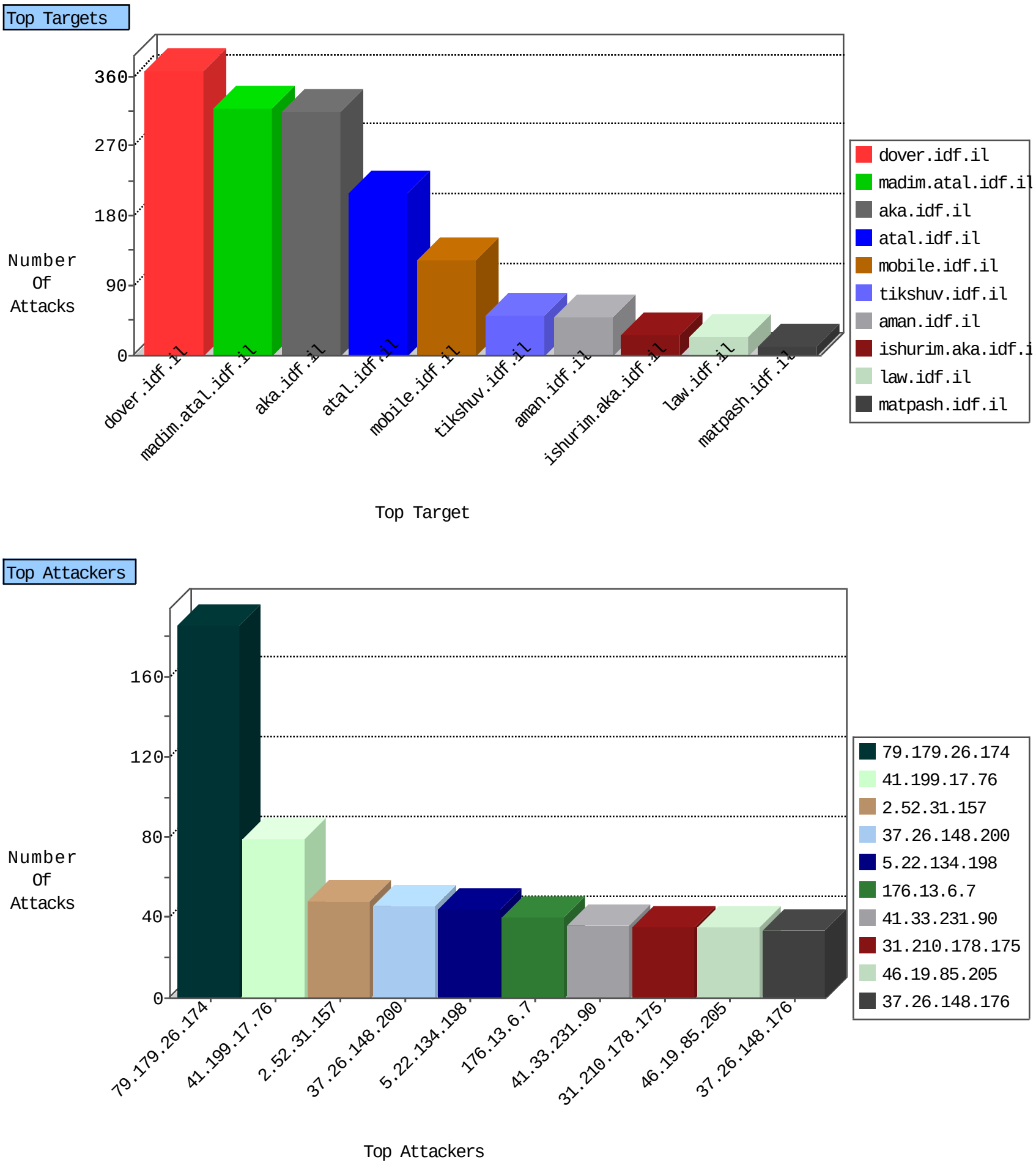
02-04-2016-19:04:02 to 02-04-2016-20:04:02

# IDF Under Attack
# Daily Report



02-04-2016-19:04:02 to 02-04-2016-20:04:02

## 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 | drop | 6 |

02-04-2016-19:04:02 to 02-04-2016-20:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 121.100.143.153 | China | 147.237.76.42 | refuah.idf.il | 22280: HTTP: Joomla Object Injection Vulnerability | Block | 1 |
| 188.165.15.13 | France | 147.237.76.42 | refuah.idf.il | C228: HTTP:  AhrefBot crawler | Block | 1 |

02-04-2016-19:04:02 to 02-04-2016-20:04:02

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 | 4 |
| 80.246.133.217 | 147.237.77.216 | Israel | dover.idf.il | ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack | 3 |
| 66.249.81.253 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 61.90.3.152 | 147.237.76.34 | Thailand | yohalan.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 115.236.75.201 | 147.237.77.216 | China | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.90.3.152 | 147.237.76.34 | Thailand | yohalan.idf.il | ET SCAN NMAP -f -sS | 1 |
| 218.246.0.97 | 147.237.72.166 | China | aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 115.236.75.201 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 37.142.223.171 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.160.238.207 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.54.138.161 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.112.81.67 | 147.237.76.202 | | e.halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.112.81.67 | 147.237.76.30 | | himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 71.6.165.200 | 147.237.76.199 | United States | e.nakchal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 185.112.81.67 | 147.237.0.19 | | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.37 | 147.237.77.19 | China | law-forum.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.182.170.38 | 147.237.76.198 | China | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.37 | 147.237.72.166 | China | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.182.170.38 | 147.237.76.147 | China | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 149.88.140.109 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 61.90.3.152 | 147.237.76.34 | Thailand | yohalan.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 115.236.75.201 | 147.237.76.199 | China | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.116.50.241 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.57.165.243 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.186.28.130 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 37.142.134.102 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.112.81.67 | 147.237.77.234 | | halag.idf.il | ET SCAN Potential SSH Scan | 1 |
| 87.69.207.137 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.112.81.67 | 147.237.76.199 | | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 77.125.118.165 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.112.81.67 | 147.237.72.14 | | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 71.6.165.200 | 147.237.76.199 | United States | e.nakchal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 185.106.92.137 | 147.237.76.42 | | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 66.249.81.129 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 180.97.106.37 | 147.237.72.167 | China | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.182.170.38 | 147.237.76.176 | China | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 176.13.18.15 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

02-04-2016-19:04:02 to 02-04-2016-20:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 79.179.26.174 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 186 |
| 41.199.17.76 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 71 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 77.126.85.80 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 31.210.182.173 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 46.19.85.205 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 17 |
| 109.253.132.177 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 217.132.126.250 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 2.54.48.191 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 2.52.37.172 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 11 |
| 37.140.189.200 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 11 |
| 2.54.53.52 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 95.108.133.213 | Russian Federation | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 192.117.150.233 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 192.116.111.11 | Israel | 147.237.72.167 | ishurim.aka.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 213.57.235.229 | Israel | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 130.203.136.75 | United States | 147.237.77.74 | law.idf.il | Web Server Enforcement Violation | Web Servers Slow HTTP Denial of Service | reject | 8 |
| 46.19.85.94 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.104 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 66.249.78.230 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.182.22.72 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.7 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 82.166.112.179 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.182.34.183 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.85.176 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 80.246.139.190 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 46.121.102.214 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 37.26.147.207 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 46.19.85.205 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 185.24.207.44 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 31.168.186.184 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 46.19.85.104 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 37.26.147.207 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 5 |
| 79.176.54.208 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 37.26.147.207 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 79.176.54.208 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 37.26.147.207 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.85.56 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 176.13.1.168 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 41.199.17.76 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 76.164.237.123 | United States | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 5 |
| 37.26.147.207 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 5 |
| 176.13.1.168 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.85.6 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 31.210.187.237 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 185.120.126.73 | | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 87.69.33.189 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 31.210.187.58 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |

02-04-2016-19:04:02 to 02-04-2016-20:04:02

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.52.31.157 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 37.26.148.200 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 45 |
| 5.22.134.198 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 44 |
| 176.13.6.7 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 40 |
| 31.210.178.175 | Israel | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 35 |
| 37.26.148.176 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 33 |
| 176.13.16.137 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 29 |
| 213.57.235.229 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 20 |
| 176.13.19.65 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 15 |
| 176.13.19.65 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 46.117.26.238 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 109.65.122.137 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 8 |
| 46.19.86.202 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 76.164.237.123 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 91.90.100.121 | France | 147.237.0.34 | tikshuv.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 4 |
| 109.253.132.177 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 176.13.1.122 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 31.210.182.173 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 87.68.35.236 | Israel | 147.237.72.166 | aka.idf.il | Multiple Redundant HTTP Headers in header Referer | Block | 3 |
| 82.102.169.113 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 192.241.201.65 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 192.241.201.65 | Block | 3 |
| 46.118.155.216 | Ukraine | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 46.118.155.216 | Block | 3 |
| 87.69.33.189 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.178.233.199 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 77.126.85.80 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.179.171.171 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown SSL Session | None | 2 |
| 109.64.135.92 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown SSL Session | None | 2 |
| 213.8.204.7 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx | None | 2 |
| 77.209.201.205 | Spain | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 66.249.78.87 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 85.250.203.219 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage | Block | 2 |
| 66.249.78.159 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.78.159 | Block | 2 |
| 213.151.42.167 | Israel | 147.237.77.170 | maarachot.idf.il | Multiple Unauthorized URL Access from 213.151.42.167 | Block | 2 |
| 2.52.37.172 | Israel | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 37.26.146.128 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 217.132.126.250 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 2.54.53.52 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.118.155.216 | Ukraine | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 192.243.55.135 | Dominica | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59268&docid=77987 | Block | 1 |
| 87.69.33.189 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 37.60.47.13 | Israel | 147.237.72.166 | aka.idf.il | Multiple Untraceable SSL Sessions from 37.60.47.13 (Unknown SSL Session) | None | 1 |
| 66.249.78.242 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2726.jpg | Block | 1 |
| 31.154.166.47 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 137.116.240.150 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/ | Block | 1 |
| 66.249.65.2 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/templates/news/{"key":" | Block | 1 |
| 192.243.55.130 | Dominica | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz | Block | 1 |
| 84.228.98.148 | 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 |
| 37.26.148.176 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Parameter Type Violation on madim.atal.idf.il/mobile/1088-he/meretz.aspx parameter ctl00$ContentPlaceHolder1$txtStreet | Block | 1 |
| 5.22.134.193 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 109.67.184.47 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/sachar/ | Block | 1 |

02-04-2016-19:04:02 to 02-04-2016-20:04:02