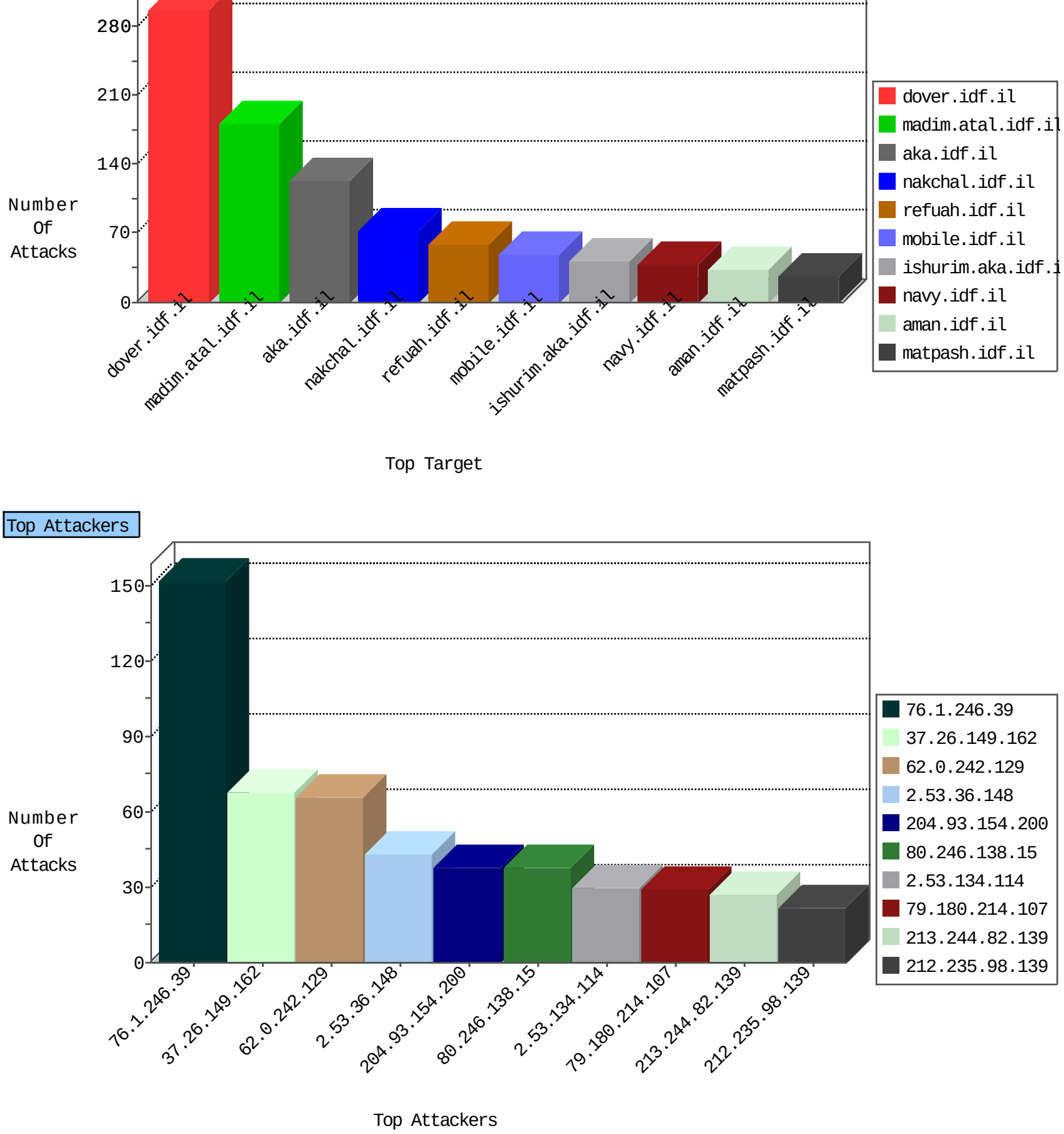
09-06-2016-11:04:06 to 09-06-2016-12:04:06

# IDF Under Attack Daily Report



09-06-2016-11:04:06 to 09-06-2016-12:04:06

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 204.93.154.200 | United States | 147.237.77.216 | dover.idf.il | TCP Scan (vertical) | drop | 155 |
| 31.168.177.230 | Israel | 147.237.77.216 | dover.idf.il | Black List | drop | 8 |
| 43.225.204.2 | Bangladesh | 147.237.77.61 | e.cogat.idf.il | Invalid TCP Flags | drop | 1 |
| 94.102.49.193 | Netherlands | 147.237.76.202 | e.halag.idf.il | Black List | drop | 1 |
| 43.225.205.2 | Bangladesh | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 1 |
| 43.225.206.2 | Bangladesh | 147.237.77.19 | law-forum.idf.il | Invalid TCP Flags | drop | 1 |
| 43.225.204.2 | Bangladesh | 147.237.77.19 | law-forum.idf.il | Invalid TCP Flags | drop | 1 |
| 43.225.206.2 | Bangladesh | 147.237.77.61 | e.cogat.idf.il | Invalid TCP Flags | drop | 1 |

09-06-2016-11:04:06 to 09-06-2016-12:04:06

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.4.32.75 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 195.154.185.20 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 195.154.185.20 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |

09-06-2016-11:04:06 to 09-06-2016-12:04:06

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 45.79.71.122 | 147.237.77.176 | United States | matpash.idf.il | WEB-MISC Chunked-Encoding transfer attempt | 2 |
| 91.121.136.34 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 77.125.64.251 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 177.200.192.50 | 147.237.77.170 | Brazil | maarachot.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 46.19.85.44 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 141.226.243.83 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.127.46.15 | 147.237.8.28 | United Kingdom | e.mobile-ks.idf.il | ET SCAN Potential SSH Scan | 1 |
| 109.123.101.31 | 147.237.0.33 | United Kingdom | idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 2.53.175.124 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.201.236.158 | 147.237.77.176 | Ukraine | matpash.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 2.53.9.29 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.57.42.121 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.201.236.158 | 147.237.77.176 | Ukraine | matpash.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 208.100.26.228 | 147.237.76.44 | United States | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 84.109.228.151 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 195.110.40.7 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.177.118.55 | 147.237.72.167 | Israel | ishurim.aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 192.115.163.105 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.176.103.245 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.93.185.10 | 147.237.0.16 | Ukraine | my-kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 46.227.67.172 | 147.237.76.42 | Sweden | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 176.13.16.78 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 132.69.196.11 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.55.172.148 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.102.48.195 | 147.237.0.200 | Netherlands | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 213.57.82.2 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 2.53.39.17 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.201.236.158 | 147.237.77.176 | Ukraine | matpash.idf.il | ET SCAN NMAP -f -sS | 1 |
| 212.143.217.21 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 208.100.26.228 | 147.237.0.33 | United States | idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 82.81.86.234 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.116.60.185 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.177.37.204 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 185.93.185.10 | 147.237.77.243 | Ukraine | mobile.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |

09-06-2016-11:04:06 to 09-06-2016-12:04:06

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 62.0.242.129 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 34 |
| 62.0.242.129 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 32 |
| 213.244.82.139 | Palestinian Territory Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 26 |
| 212.235.98.139 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 76.1.246.39 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 21 |
| 76.1.246.39 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 21 |
| 76.1.246.39 | United States | 147.237.76.39 | mobile.meitav.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 20 |
| 76.1.246.39 | United States | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 19 |
| 76.1.246.39 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 19 |
| 76.1.246.39 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 18 |
| 76.1.246.39 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 76.1.246.39 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 17 |
| 193.43.246.250 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 46.19.86.75 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 207.46.13.68 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.85.88 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 46.19.85.110 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 46.19.85.248 | Israel | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 2.53.134.114 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 46.19.85.248 | Israel | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.53.134.114 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 37.26.148.150 | Israel | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 2.53.134.114 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 46.19.85.88 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.53.134.114 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 2.53.36.188 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.19.86.99 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 77.218.229.89 | Sweden | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 2.53.134.114 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 6 |
| 81.218.118.126 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 46.19.86.121 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 31.168.114.2 | Israel | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.86.121 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 81.218.118.126 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 5 |
| 2.55.180.192 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 46.19.85.110 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 46.19.86.109 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 4 |
| 85.65.23.44 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 46.19.85.35 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 81.218.116.129 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 37.26.148.209 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence |  | monitor | 4 |
| 82.81.5.202 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 46.19.85.35 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 109.253.130.103 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 46.19.85.67 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 46.19.86.105 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 100.92.230.29 |  | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 81.218.118.126 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 176.13.13.43 | Israel | 147.237.76.42 | refuah.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 3 |
| 46.19.86.130 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

09-06-2016-11:04:06 to 09-06-2016-12:04:06

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 37.26.149.162 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 68 |
| 2.53.36.148 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 43 |
| 80.246.138.15 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 38 |
| 79.180.214.107 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Unauthorized HTTP Method | Block | 21 |
| 66.249.76.106 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx | Block | 9 |
| 79.180.214.107 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/ | Block | 7 |
| 46.19.86.75 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 46.19.86.42 | Israel | 147.237.0.19 | madim.atal.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx | Block | 5 |
| 95.35.135.175 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 194.114.146.227 | Israel | 147.237.72.156 | aman.idf.il | Distributed Unauthorized HTTP Method | Block | 4 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 4 |
| 89.139.222.0 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 3 |
| 46.19.86.99 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.28 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.136.32 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 81.218.208.242 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431 | Block | 3 |
| 46.19.86.37 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.86.42 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 84.95.208.20 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | PHP Attempt | Block | 2 |
| 46.19.86.129 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Unknown HTTP Request Method | Block | 2 |
| 81.218.208.242 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1362 | Block | 2 |
| 84.95.208.20 | Israel | 147.237.77.234 | halag.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 84.95.208.20 | Israel | 147.237.0.34 | tikshuv.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 80.178.89.129 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 81.218.208.242 | Israel | 147.237.77.243 | mobile.idf.il | Multiple Unauthorized URL Access from 81.218.208.242 | Block | 2 |
| 2.53.179.40 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.19.86.129 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed Malformed URL | Block | 2 |
| 84.95.208.20 | Israel | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 2 |
| 77.139.194.39 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/lomdim/tochen/ | Block | 1 |
| 46.19.85.250 | Israel | 147.237.76.42 | refuah.idf.il | Malformed URL 9_3_1 | Block | 1 |
| 176.13.229.111 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.69.10 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/724-5764-he/patzar.aspx | Block | 1 |
| 84.95.208.20 | Israel | 147.237.0.15 | kosher-kravi.idf.il | Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/piwik.php | Block | 1 |
| 79.182.112.92 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/undefined | Block | 1 |
| 212.235.62.200 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized HTTP Method | Block | 1 |
| 45.79.71.122 | United States | 147.237.77.176 | matpash.idf.il | Multiple Unknown HTTP Request Method from 45.79.71.122 | Block | 1 |
| 75.82.117.252 | United States | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico | Block | 1 |
| 52.30.171.229 | Ireland | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to / | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 84.95.208.20 | Block | 1 |
| 217.132.124.110 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 79.178.131.108 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/894-ar | Block | 1 |
| 46.19.85.250 | Israel | 147.237.76.42 | refuah.idf.il | Unknown HTTP Request Method S in URL 9_3_1 | Block | 1 |
| 185.32.179.166 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.69.232 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json | Block | 1 |
| 45.79.71.122 | United States | 147.237.77.176 | matpash.idf.il | Malformed HTTP Header Line 3 | Block | 1 |
| 46.19.86.129 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Abnormally Long Request from 46.19.86.129 | Block | 1 |
| 212.235.62.200 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal | Block | 1 |
| 46.19.86.42 | Israel | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx | Block | 1 |
| 45.79.71.122 | United States | 147.237.77.176 | matpash.idf.il | Unknown HTTP Request Method 1 in URL | Block | 1 |
| 77.138.6.132 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx | Block | 1 |

09-06-2016-11:04:06 to 09-06-2016-12:04:06