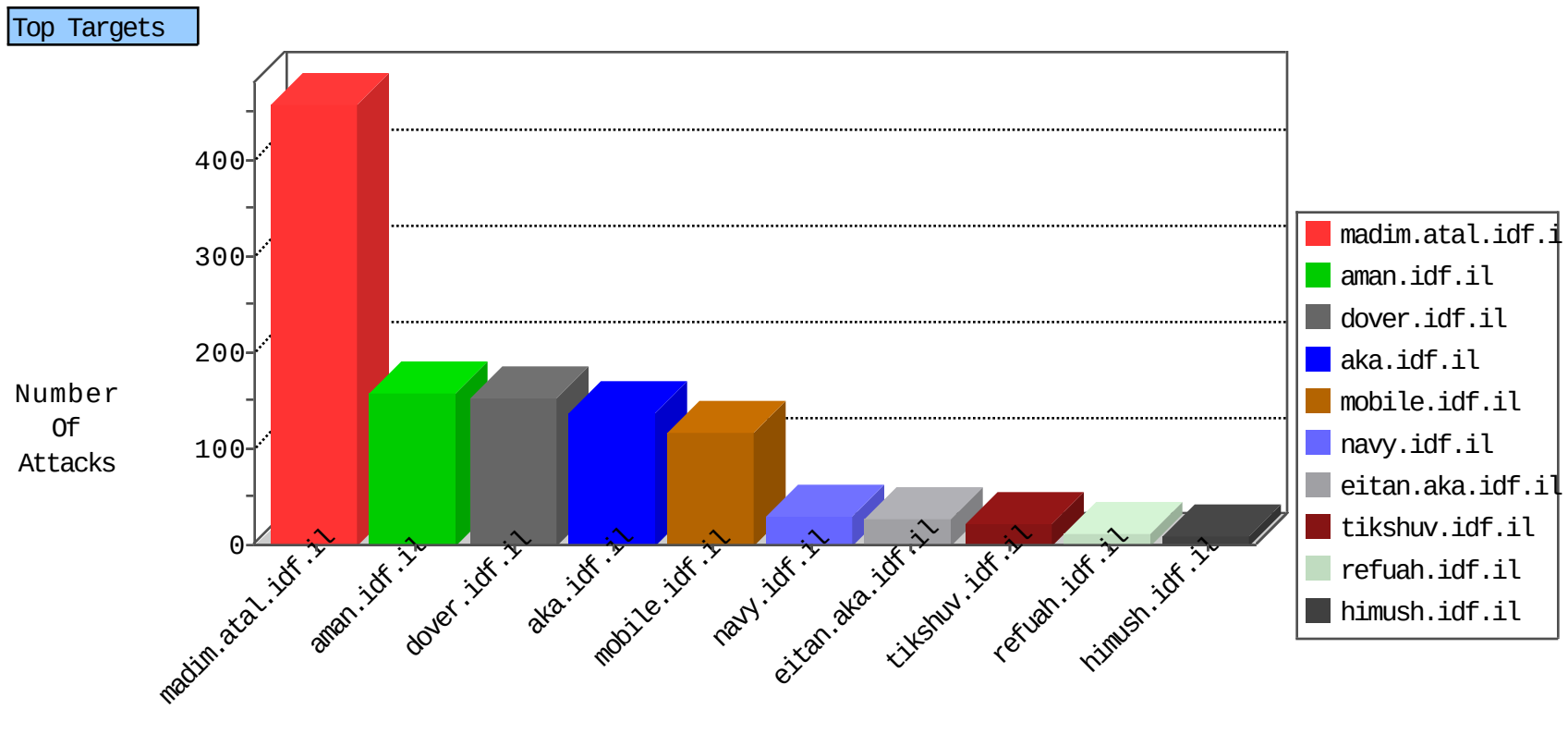
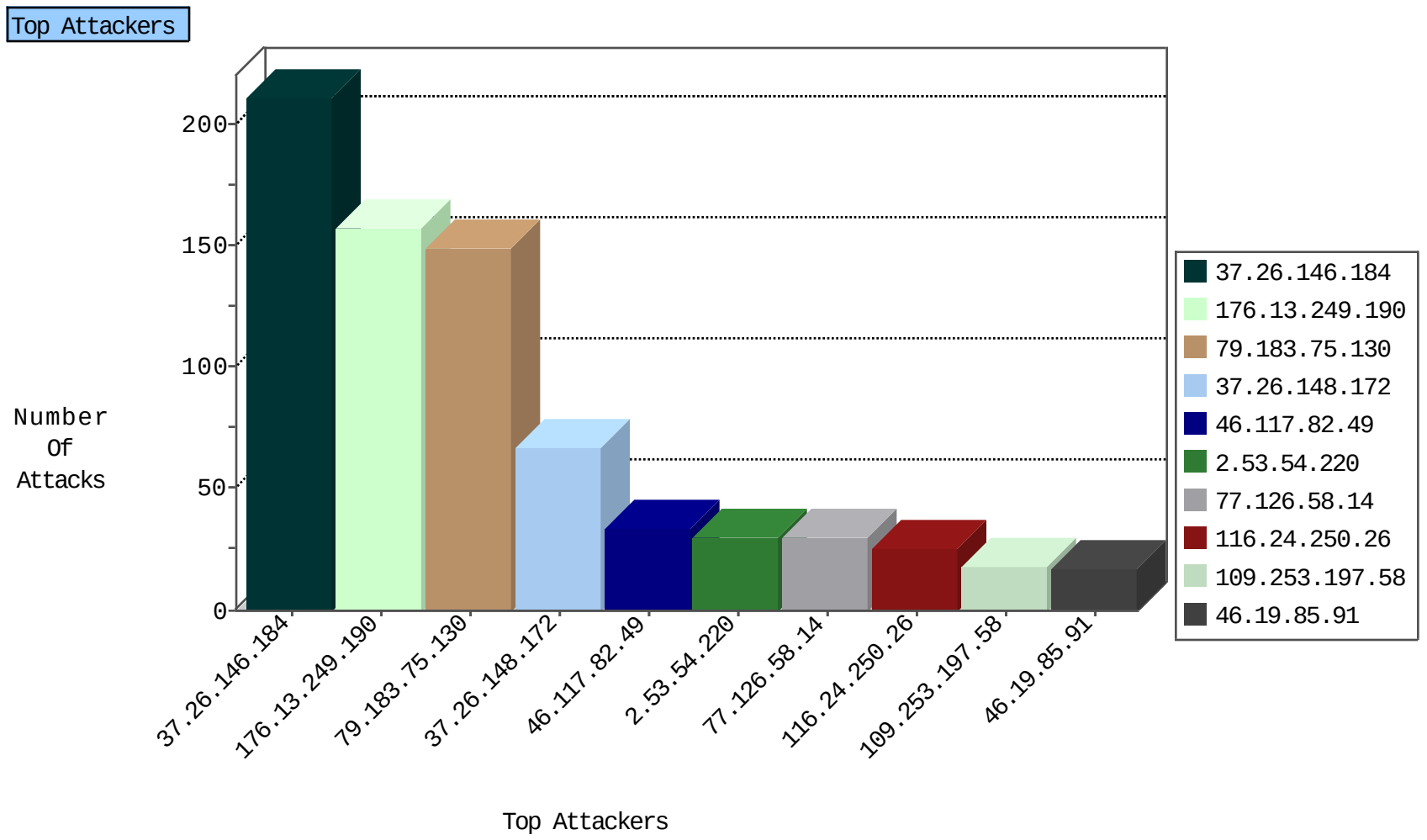
10-04-2016-21:04:09 to 10-04-2016-22:04:09

# IDF Under Attack Daily Report

Top Targets




Top Attackers



10-04-2016-21:04:09 to 10-04-2016-22:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 93.174.93.210 | Netherlands | 147.237.76.39 | mobile.meitav.idf.il | block-sp-traf1 | forward | 2 |
| 93.174.93.210 | Netherlands | 147.237.76.42 | refuah.idf.il | block-sp-traf1 | forward | 2 |
| 195.62.53.168 | Russian Federation | 147.237.77.170 | maarachot.idf.il | block-sp-traf1 | forward | 2 |
| 93.174.93.210 | Netherlands | 147.237.76.30 | himush.idf.il | block-sp-traf1 | forward | 2 |
| 209.126.136.2 | United States | 147.237.76.177 | ncore.idf.il | Black List | drop | 1 |
| 50.116.39.165 | United States | 147.237.76.38 | e.e.meitav.idf.il | Black List | drop | 1 |

10-04-2016-21:04:09 to 10-04-2016-22:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 162.210.196.97 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 162.210.196.97 | United States | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 123.126.68.119 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 1 |

10-04-2016-21:04:09 to 10-04-2016-22:04:09

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 195.154.39.188 | 147.237.76.44 | France | e.refuah.idf.il | ET SCAN Potential SSH Scan | 2 |
| 62.210.124.129 | 147.237.77.216 | France | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 146.200.148.0 | 147.237.77.74 | United Kingdom | law.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 117.102.89.209 | 147.237.77.212 | Indonesia | e.dover.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 202.65.138.2 | 147.237.77.178 | India | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 106.120.209.155 | 147.237.77.243 | China | mobile.idf.il | ET SCAN NMAP -f -sS | 1 |
| 195.154.39.188 | 147.237.77.205 | France | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 84.54.72.35 | 147.237.77.170 | Uzbekistan | maarachot.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 195.154.39.188 | 147.237.76.34 | France | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 62.150.255.205 | 147.237.77.212 | Kuwait | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 195.154.39.188 | 147.237.72.217 | France | e.idf.il | ET SCAN Potential SSH Scan | 1 |
| 54.147.7.228 | 147.237.72.166 | United States | aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 195.154.39.188 | 147.237.72.14 | France | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 46.229.223.8 | 147.237.77.226 | Russian Federation | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.205.151.198 | 147.237.77.243 | China | mobile.idf.il | ET SCAN NMAP -f -sS | 1 |
| 195.154.39.188 | 147.237.0.19 | France | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 211.149.222.5 | 147.237.77.226 | China | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 46.229.223.8 | 147.237.72.217 | Russian Federation | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 209.126.230.71 | 147.237.8.14 | United States | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 106.120.209.155 | 147.237.77.243 | China | mobile.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 198.20.69.74 | 147.237.76.147 | United States | chinuch.aka.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 91.138.208.87 | 147.237.72.167 | Greece | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.154.39.188 | 147.237.77.121 | France | e.navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 81.27.85.27 | 147.237.76.196 | United Kingdom | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.154.39.188 | 147.237.76.39 | France | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 62.150.255.205 | 147.237.77.212 | Kuwait | e.dover.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 195.154.39.188 | 147.237.76.30 | France | himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 62.150.255.205 | 147.237.77.212 | Kuwait | e.dover.idf.il | ET SCAN NMAP -f -sS | 1 |
| 195.154.39.188 | 147.237.72.167 | France | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 49.73.103.244 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 218.205.151.198 | 147.237.77.243 | China | mobile.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 195.154.39.188 | 147.237.0.200 | France | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.229.223.8 | 147.237.77.212 | Russian Federation | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 211.149.222.5 | 147.237.77.234 | China | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.169.150 | 147.237.76.39 | United Kingdom | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 211.149.222.5 | 147.237.77.216 | China | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

10-04-2016-21:04:09 to 10-04-2016-22:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 79.183.75.130 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 57 |
| 79.183.75.130 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 54 |
| 79.183.75.130 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 34 |
| 77.126.58.14 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 2.53.54.220 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 109.253.197.58 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 46.117.82.49 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 18 |
| 46.117.82.49 | Israel | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 16 |
| 5.22.134.111 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 176.58.71.162 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 46.19.85.200 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.42 | Israel | 147.237.0.34 | tikshuv.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.91 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.200 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 46.19.85.42 | Israel | 147.237.0.34 | tikshuv.idf.i | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 217.132.154.40 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 185.89.217.227 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.91 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 197.37.9.215 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.217 | Israel | 147.237.0.34 | tikshuv.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 2.55.152.145 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.253.137.201 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.116.2.110 | Israel | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 2.55.149.30 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 46.19.86.219 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 46.19.86.219 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 141.0.15.218 | Norway | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 185.3.147.196 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 109.66.58.1 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 4 |
| 197.37.9.215 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 2.55.131.223 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.93 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 185.89.217.232 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.86.216 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 212.29.252.81 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 4 |
| 46.19.85.133 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 185.32.179.193 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 79.176.29.241 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 197.37.9.215 | Egypt | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 109.253.134.117 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.85.217 | Israel | 147.237.0.34 | tikshuv.idf.i | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 46.19.85.133 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 46.19.86.102 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 80.246.139.109 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.55.11.176 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 185.89.217.231 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 87.69.122.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 2.53.14.197 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 185.89.217.226 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |

10-04-2016-21:04:09 to 10-04-2016-22:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 37.26.146.184 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 211 |
| 176.13.249.190 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 151 |
| 37.26.148.172 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 67 |
| 116.24.250.26 | China | 147.237.76.200 | eitan.aka.idf.il | Multiple Unauthorized URL Access from 116.24.250.26 | Block | 17 |
| 176.13.15.140 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 176.13.15.140 | Block | 7 |
| 116.24.250.26 | China | 147.237.76.200 | eitan.aka.idf.il | Distributed PHP Attempt | Block | 6 |
| 77.127.13.99 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 4 |
| 31.154.81.54 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 77.139.103.104 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx | Block | 3 |
| 37.26.148.215 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 37.26.149.147 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 109.253.145.117 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 212.179.227.221 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 87.68.46.85 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 80.246.139.109 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.239 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 46.117.70.132 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter SearchParam in www.aka.idf.il/main/sachar/ | None | 2 |
| 85.65.186.245 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 66.249.76.74 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/robots.txt | Block | 1 |
| 195.62.53.168 | Russian Federation | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to gmail.com/engine/log.txt | Block | 1 |
| 46.19.85.91 | Israel | 147.237.77.216 | dover.idf.il | Illegal HTTP Version | Block | 1 |
| 84.111.171.47 | Israel | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 77.138.193.58 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx | Block | 1 |
| 66.102.9.8 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx | Block | 1 |
| 85.65.202.69 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 79.176.51.236 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx | None | 1 |
| 66.249.76.75 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 46.19.85.91 | Israel | 147.237.77.216 | dover.idf.il | Malformed URL asp.net_sessionid=qtlh0345ydfj4c45h4bjn255 | Block | 1 |
| 84.111.171.47 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/wp-login.php | Block | 1 |
| 77.138.238.180 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.138.238.180 | Block | 1 |
| 66.249.64.33 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8769-he/refuah.aspx | Block | 1 |
| 79.177.212.248 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/giyus/kiosk/kiosk.aspx' | Block | 1 |
| 68.180.229.178 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx | Block | 1 |
| 217.132.53.67 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx | Block | 1 |
| 116.24.250.26 | China | 147.237.76.200 | eitan.aka.idf.il | Unauthorized Method HEAD for www.eitan.aka.idf.il/ | None | 1 |
| 46.19.85.91 | Israel | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method 1%7C32; in URL asp.net_sessionid=qtlh0345ydfj4c45h4bjn255 | Block | 1 |
| 84.111.171.47 | Israel | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 2.55.152.145 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 77.138.238.180 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/smalim/ | Block | 1 |
| 66.249.64.36 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-9238-he/refuah.aspx | Block | 1 |
| 192.118.78.57 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/rules.abe | Block | 1 |
| 93.78.230.27 | Ukraine | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/kapatz/contactus.aspx | Block | 1 |
| 217.132.154.40 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 116.24.250.26 | China | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/index.asp | Block | 1 |
| 31.154.81.2 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 84.111.171.47 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/wp-login.php | Block | 1 |
| 77.139.45.87 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx | Block | 1 |
| 66.249.66.197 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/robots.txt | Block | 1 |
| 193.43.246.250 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/giyus/manilot/miktzoot/ | Block | 1 |
| 84.95.112.107 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |

10-04-2016-21:04:09 to 10-04-2016-22:04:09