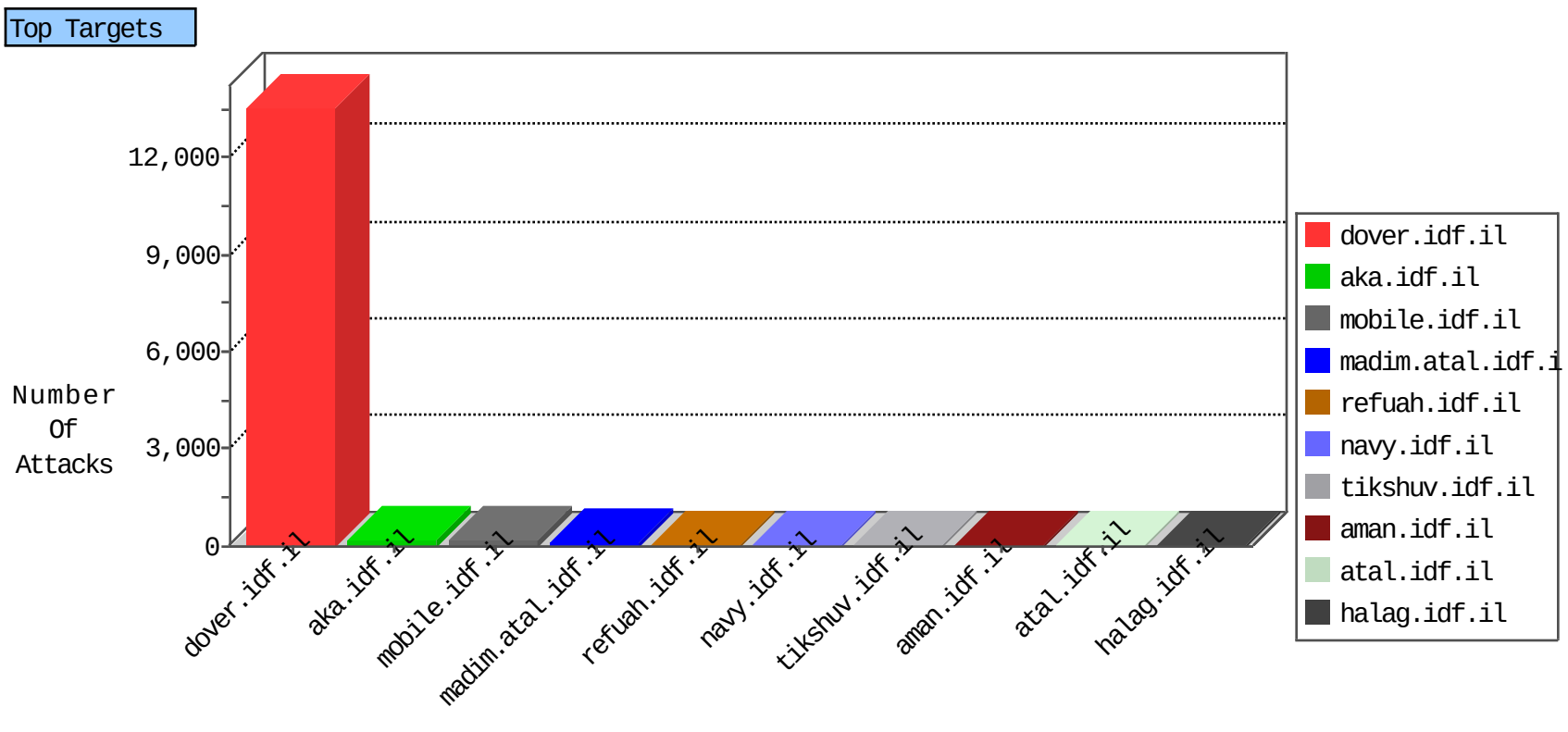
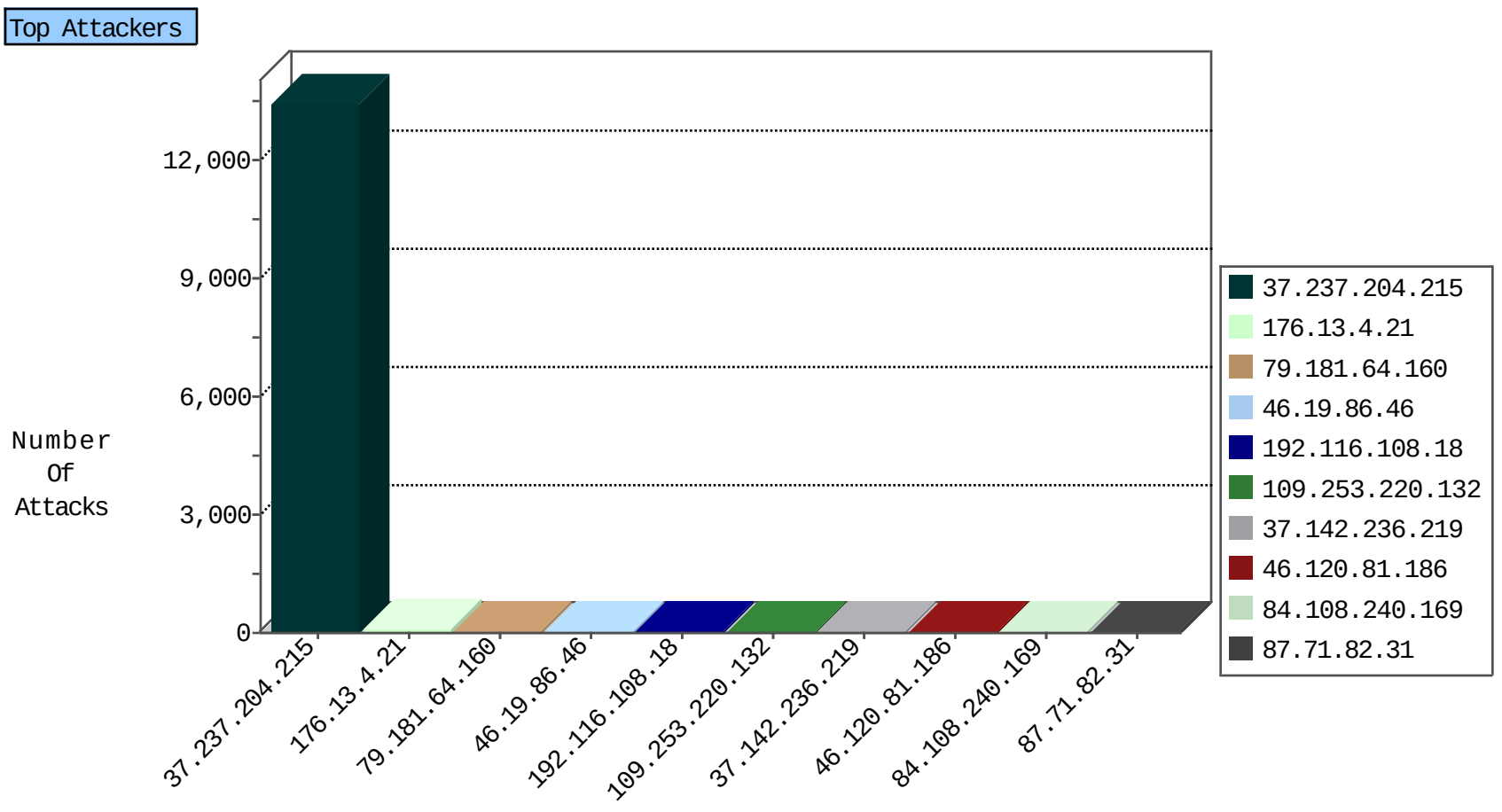
03-05-2016-19:04:09 to 03-05-2016-20:04:09

# IDF Under Attack Daily Report

Top Targets




Top Attackers



03-05-2016-19:04:09 to 03-05-2016-20:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 304 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | DOS-WEB-HOIC-HTTP-80-snc | dest-reset | 21 |
| 82.145.216.219 | Europe | 147.237.72.166 | aka.idf.il | Block_Ip_Web_In | drop | 10 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | JLM_Purple_Con_Limit_Http | drop | 3 |
| 212.179.54.237 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 81.218.65.210 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 3 |
| 149.78.148.181 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 3 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | JLM_Under_Attack_Con_Http | drop | 2 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | DOS-HOIC-TCP-80-gbo | dest-reset | 2 |
| 46.117.248.198 | Israel | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 2 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 80.246.130.47 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |
| 146.185.239.100 | Russian Federation | 147.237.77.74 | law.idf.il | block-sp-traf1 | drop | 1 |
| 199.217.118.49 | United States | 147.237.72.217 | e.idf.il | Block_Udp_All_Nets | drop | 1 |
| 66.240.192.138 | United States | 147.237.76.39 | mobile.meitav.idf.il | Block_Ntp_All_Net | drop | 1 |
| 84.109.155.166 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood out of context | drop | 1 |

03-05-2016-19:04:09 to 03-05-2016-20:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | 20034: HTTP: HOIC Denial-of-Service Tool Usage | Block | 81 |
| 37.142.236.219 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 20 |
| 95.86.117.109 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 109.66.2.249 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 5 |
| 162.210.196.98 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 66.249.66.187 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 106.38.241.106 | China | 147.237.77.233 | atal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 66.249.66.190 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

03-05-2016-19:04:09 to 03-05-2016-20:04:09

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 |
| 154.16.138.35 | 147.237.0.15 | Mauritius | kosher-kravi.idf.i | ET SCAN NMAP -f -sS | 1 |
| 104.197.227.249 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 218.246.0.97 | 147.237.77.235 | China | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.57.11.7 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.57.11.7 | 147.237.76.86 | China | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.57.11.7 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 213.136.91.26 | 147.237.76.38 | Germany | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 154.16.138.35 | 147.237.0.15 | Mauritius | kosher-kravi.idf.i | ET SCAN NMAP -sS window 2048 | 1 |
| 121.40.195.144 | 147.237.72.217 | China | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.237.204.215 | 147.237.77.216 | Iraq | dover.idf.il | ET CURRENT_EVENTS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA | 1 |
| 218.246.0.97 | 147.237.8.46 | China | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.57.11.7 | 147.237.76.148 | China | gqcenter.aka.idf.i | ET SCAN Potential SSH Scan | 1 |
| 218.57.11.7 | 147.237.76.44 | China | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 213.136.91.26 | 147.237.76.86 | Germany | navy.idf.il | ET SCAN Potential SSH Scan | 1 |

03-05-2016-19:04:09 to 03-05-2016-20:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12007 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | drop | | drop | 574 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 185 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN retransmit with different window scale | alert | 131 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | Bad TCP sequence | | monitor | 80 |
| 176.13.4.21 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 78 |
| 79.181.64.160 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 47 |
| 46.19.86.46 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 25 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 19 |
| 46.120.81.186 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 17 |
| 87.71.82.31 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 84.108.240.169 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 11 |
| 46.19.85.195 | Israel | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 10 |
| 79.182.122.65 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 10 |
| 109.64.145.112 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.86.46 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 84.111.2.82 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 93.172.236.188 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 7 |
| 66.249.69.46 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 87.68.71.201 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 85.64.118.41 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.181.64.160 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.180.129.161 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.179.3.32 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 5 |
| 37.142.166.177 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 37.142.236.219 | Israel | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 85.65.62.68 | Israel | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 109.67.197.173 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 84.108.192.145 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 80.246.130.47 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 89.204.138.78 | Germany | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 5.22.131.42 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 5.22.129.240 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.127.15.22 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 109.67.5.26 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.4.232 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.183.66.63 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.3.144.80 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 79.180.184.100 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 217.132.23.133 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.86.46 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.178.122.186 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.171.9 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.127.15.22 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 3 |
| 79.181.168.46 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

03-05-2016-19:04:09 to 03-05-2016-20:04:09

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 79.179.147.164 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |

03-05-2016-19:04:09 to 03-05-2016-20:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 192.116.108.18 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 34 |
| 109.253.220.132 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 34 |
| 176.13.4.21 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 9 |
| 176.13.8.144 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword | Block | 8 |
| 46.120.190.200 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 6 |
| 46.19.86.109 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 5 |
| 46.121.138.49 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 84.108.240.169 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 46.120.81.186 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 213.8.204.68 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 87.70.61.110 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.142.68.103 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 79.183.223.126 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 31.154.152.110 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx | Block | 2 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 37.237.204.215 | Block | 2 |
| 109.253.138.89 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 37.26.146.182 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 66.249.69.46 | United States | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 212.76.107.57 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 212.76.107.57 | Block | 1 |
| 198.20.69.74 | United States | 147.237.77.176 | matpash.idf.il | Distributed Unauthorized URL Access on 147.237.77.176/ | Block | 1 |
| 46.120.190.200 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 1 |
| 157.55.12.70 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 207.241.237.227 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/giyus/general | Block | 1 |
| 66.249.64.233 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.233 | Block | 1 |
| 46.116.243.125 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 93.172.236.188 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 66.249.75.218 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/yohalan/main/main.asp | Block | 1 |
| 212.76.107.57 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-19538-he/dover.aspx&sa=u&ved=0ahukewju95imhqrlahvdvrqkhb0rbs4qfggnmae&usg=afqjcnhcpmeomr0o3vofqvprlnnhxrmgxg | Block | 1 |
| 199.30.25.157 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 157.55.39.47 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to www.maarachot.idf.il/pdf/files/2/112922.pdf×ž× ×″×™×′×•×ª | Block | 1 |
| 80.179.225.42 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.64.233 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal | Block | 1 |
| 212.66.40.76 | Ukraine | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi'a=0 | Block | 1 |
| 46.117.248.198 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/style/shared/reset.css | Block | 1 |
| 37.26.146.139 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 79.181.64.160 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 202.69.11.247 | Pakistan | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 65.26.25.127 | United States | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 37.237.204.215 | Iraq | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/ar/' | Block | 1 |
| 173.247.228.10 | United States | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 66.249.66.182 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx | Block | 1 |
| 212.76.107.57 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 212.76.107.57 | Block | 1 |
| 37.26.146.154 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 79.182.122.65 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 203.133.171.95 | Korea, Republic of | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx | None | 1 |
| 65.55.210.31 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 40.77.167.72 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 173.247.228.10 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/wp-login.php | Block | 1 |
| 2.52.189.239 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.66.188 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt | Block | 1 |

03-05-2016-19:04:09 to 03-05-2016-20:04:09