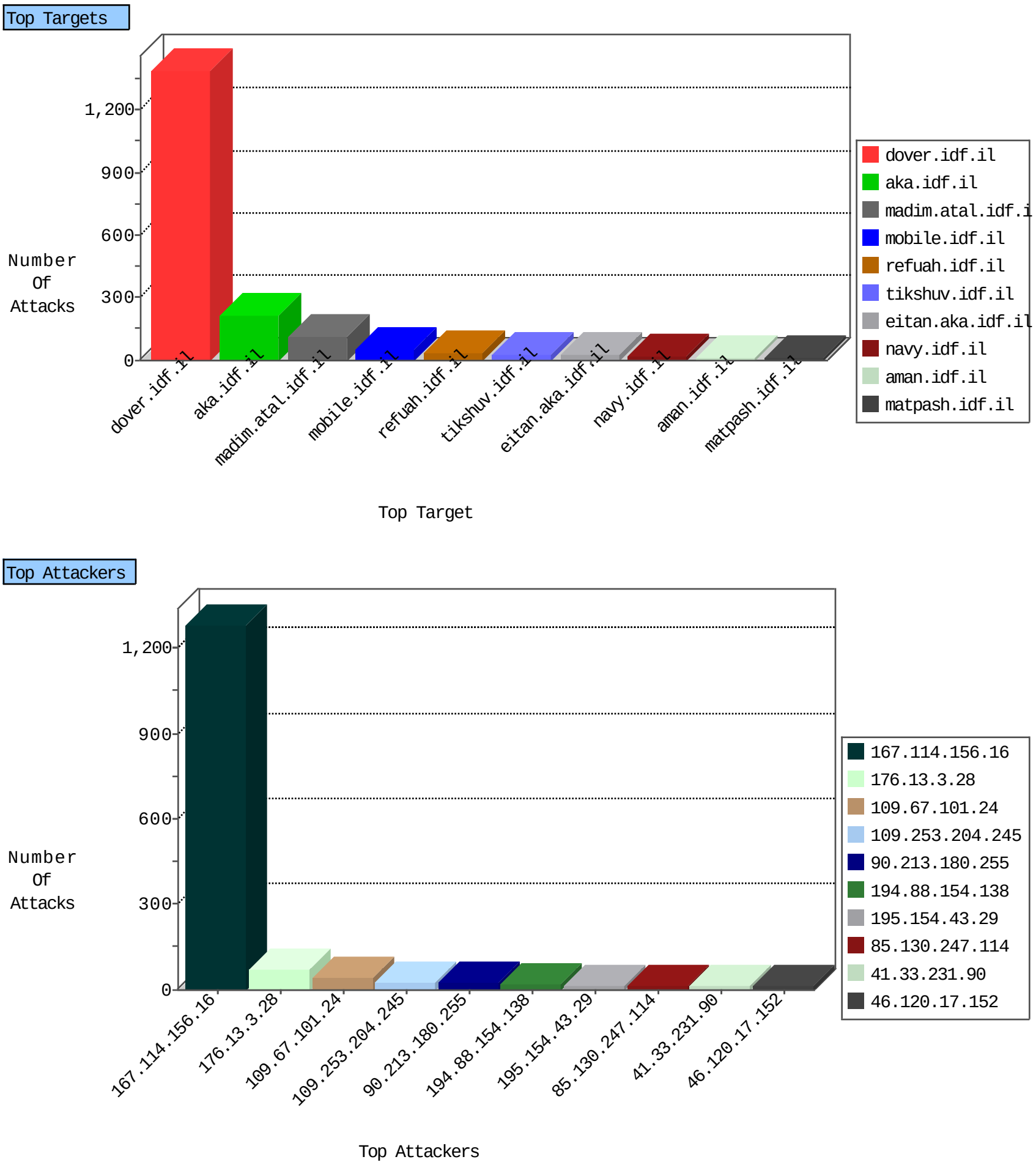
04-14-2016-20:04:03 to 04-14-2016-21:04:03

# IDF Under Attack Daily Report



04-14-2016-20:04:03 to 04-14-2016-21:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | Block_Ip_Web_In | drop | 1283 |
| 123.59.59.52 | China | 147.237.77.170 | maarachot.idf.il | block-sp-traf1 | forward | 2 |
| 185.94.111.1 | Russian Federation | 147.237.72.166 | aka.idf.il | Block_Ntp_All_Net | drop | 1 |
| 202.88.1.3 | Hong Kong | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 1 |
| 81.218.56.125 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.44 | e.refuah.idf.il | Block_Ntp_All_Net | drop | 1 |
| 202.88.1.4 | Hong Kong | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.202 | e.halag.idf.il | Block_Ntp_All_Net | drop | 1 |
| 202.88.1.10 | Hong Kong | 147.237.77.216 | dover.idf.il | Invalid TCP Flags | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.77.176 | matpash.idf.il | Block_Ntp_All_Net | drop | 1 |
| 66.249.64.190 | Israel | 147.237.72.166 | aka.idf.il | HTTP-Misc-BadBlue-Dir-Trave-2 | dest-reset | 1 |

04-14-2016-20:04:03 to 04-14-2016-21:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.178.52.195 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 6 |
| 194.88.154.138 | Poland | 147.237.76.42 | refuah.idf.il | 6134: HTTP: SQL Injection Variable Declaration Evasion | Block | 4 |
| 207.241.237.222 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 4 |
| 149.88.195.86 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 199.30.24.158 | United States | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 2 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 66.249.66.158 | Israel | 147.237.0.34 | tikshuv.idf.il | C1000138: HTTP: prefix 1.01 in the URL | Block | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

04-14-2016-20:04:03 to 04-14-2016-21:04:03

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 194.88.154.138 | 147.237.76.42 | Poland | refuah.idf.il | SQL Injection - Select From | 14 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 8 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 195.154.43.29 | 147.237.8.46 | France | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.154.43.29 | 147.237.0.33 | France | idf.il | ET SCAN Potential SSH Scan | 1 |
| 23.96.109.87 | 147.237.0.15 | United States | kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 195.154.43.29 | 147.237.77.243 | France | mobile.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.154.43.29 | 147.237.77.178 | France | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.103.252.98 | 147.237.76.42 | Russian Federation | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 195.154.43.29 | 147.237.77.121 | France | e.navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.37 | 147.237.77.227 | China | e.hamaz.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.154.43.29 | 147.237.76.196 | France | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.158 | 147.237.8.46 | Ukraine | e.chinuch.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 195.154.43.29 | 147.237.76.86 | France | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 85.64.123.3 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 195.154.43.29 | 147.237.76.34 | France | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 84.200.15.174 | 147.237.77.243 | Germany | mobile.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 195.154.43.29 | 147.237.72.156 | France | aman.idf.il | ET SCAN Potential SSH Scan | 1 |
| 66.249.78.158 | 147.237.72.166 | United States | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 195.154.43.29 | 147.237.8.14 | France | e.orchot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 23.96.109.87 | 147.237.0.15 | United States | kosher-kravi.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 195.154.43.29 | 147.237.0.17 | France | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 23.96.109.87 | 147.237.0.15 | United States | kosher-kravi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 195.154.43.29 | 147.237.77.235 | France | sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.154.43.29 | 147.237.77.176 | France | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.162 | 147.237.76.197 | China | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.154.43.29 | 147.237.76.199 | France | e.nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.97.106.37 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 195.154.43.29 | 147.237.76.147 | France | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.158 | 147.237.8.46 | Ukraine | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 195.154.43.29 | 147.237.76.38 | France | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 84.200.15.174 | 147.237.77.243 | Germany | mobile.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 195.154.43.29 | 147.237.72.167 | France | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 80.82.78.38 | 147.237.72.166 | Netherlands | aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

04-14-2016-20:04:03 to 04-14-2016-21:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 109.67.101.24 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 42 |
| 90.213.180.255 | United Kingdom | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 2.53.160.119 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 82.81.2.115 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 10 |
| 85.130.247.114 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 109.66.3.254 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 46.19.85.175 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 87.70.21.164 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 213.57.69.125 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 2.53.49.249 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 6 |
| 79.183.176.113 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 149.78.210.60 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.130.247.114 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 82.81.40.83 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.66.70.254 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 46.120.17.152 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 46.19.85.88 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 71.197.60.117 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 46.19.85.88 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 5.29.61.244 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 84.108.71.245 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 85.130.170.218 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 185.3.144.27 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 212.199.151.150 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 185.3.147.189 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 79.177.224.151 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 37.46.39.219 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 79.183.152.241 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 94.230.86.198 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 2.55.59.95 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.13.12.82 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.179.135.91 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.177.224.151 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 87.70.25.206 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.168.219.79 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 188.120.148.101 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 46.120.17.152 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 2.55.137.136 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 176.13.21.48 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.182.98.56 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.65.180.102 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 87.109.236.76 | Saudi Arabia | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 3 |
| 2.53.157.7 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

04-14-2016-20:04:03 to 04-14-2016-21:04:03

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 80.178.197.104 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.183.2.155 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.177.6.185 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 5.22.130.100 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |

04-14-2016-20:04:03 to 04-14-2016-21:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 176.13.3.28 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 71 |
| 109.253.204.245 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 27 |
| 185.32.179.35 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 9 |
| 161.113.11.16 | United States | 147.237.76.86 | navy.idf.il | Unauthorized HTTP Method | Block | 4 |
| 176.13.20.140 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 161.113.11.16 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 161.113.11.16 | Block | 3 |
| 2.55.59.95 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 84.94.171.171 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/ | Block | 2 |
| 149.78.30.34 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 149.78.30.34 | Block | 2 |
| 77.50.183.19 | Russian Federation | 147.237.77.216 | dover.idf.il | PHP Attempt | Block | 2 |
| 77.50.183.19 | Russian Federation | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 2 |
| 161.113.11.16 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/sip_storage/files/4/ | Block | 1 |
| 109.163.234.9 | Romania | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/main.asp | Block | 1 |
| 66.249.78.158 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 157.55.39.42 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx | None | 1 |
| 37.26.147.134 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/894-ar | Block | 1 |
| 66.249.93.78 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 197.189.206.93 | South Africa | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/ | Block | 1 |
| 157.55.39.199 | United States | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/ | Block | 1 |
| 84.108.91.107 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/https:/www.idf.il/ | Block | 1 |
| 38.111.147.83 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/templates/general/general.aspx | Block | 1 |
| 131.253.25.148 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 68.180.230.184 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/robots.txt | Block | 1 |
| 207.46.13.72 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/faq/faq.aspx | Block | 1 |
| 87.109.236.76 | Saudi Arabia | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 66.249.64.131 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/robots.txt | Block | 1 |
| 176.13.21.48 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423 | Block | 1 |
| 213.254.241.4 | France | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 89.31.140.30 | Germany | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/ | Block | 1 |
| 66.249.78.97 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 176.228.146.158 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/ | Block | 1 |
| 149.78.30.34 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx | Block | 1 |
| 23.29.125.155 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |

04-14-2016-20:04:03 to 04-14-2016-21:04:03