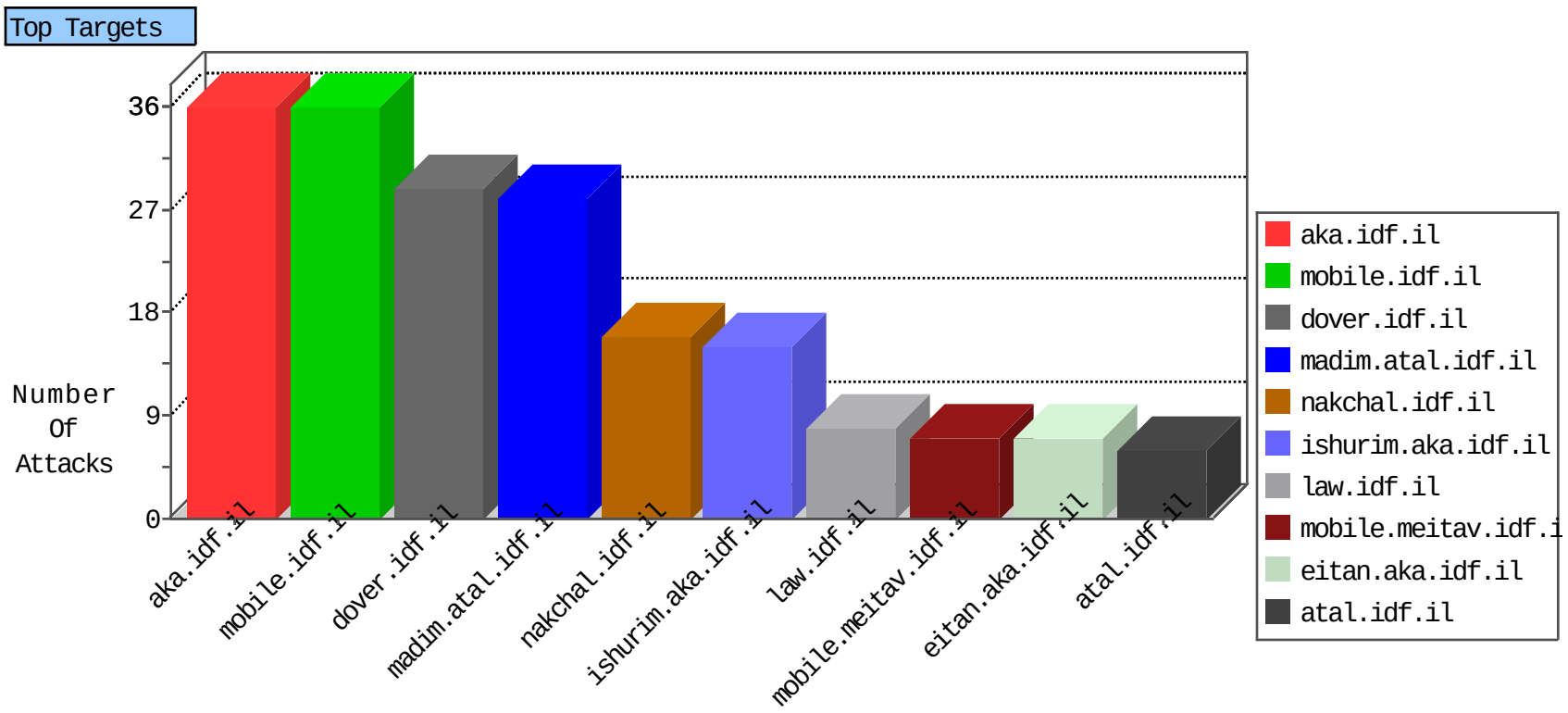
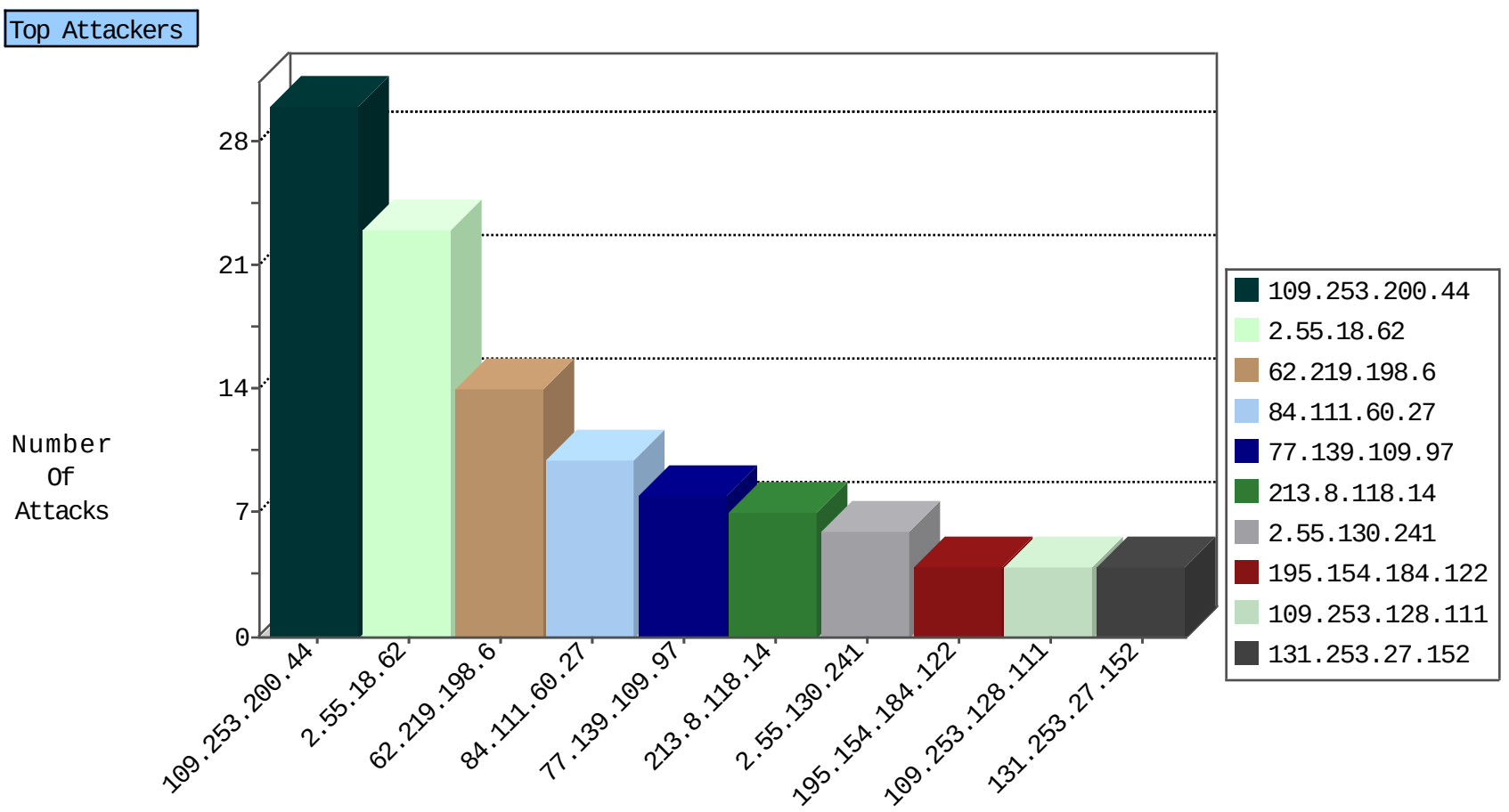
09-21-2016-06:04:07 to 09-21-2016-07:04:07

# IDF Under Attack Daily Report



09-21-2016-06:04:07 to 09-21-2016-07:04:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 123.59.59.52 | China | 147.237.76.39 | mobile.meitav.idf.il | block-sp-traf1 | forward | 4 |
| 183.60.48.25 | China | 147.237.0.16 | my-kosher-kravi.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 209.126.136.2 | United States | 147.237.76.201 | e.atal.idf.il | Black List | drop | 1 |
| 45.32.196.8 | United States | 147.237.76.148 | gqcenter.aka.idf.il | Black List | drop | 1 |

09-21-2016-06:04:07 to 09-21-2016-07:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.55.136.87 | Israel | 147.237.72.166 | aka.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

09-21-2016-06:04:07 to 09-21-2016-07:04:07

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 195.154.184.122 | 147.237.77.74 | France | law.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 4 |
| 109.236.86.32 | 147.237.76.201 | Netherlands | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.236.86.32 | 147.237.72.167 | Netherlands | ishurim.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 109.60.153.178 | 147.237.0.33 | Russian Federation | idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 78.139.97.121 | 147.237.8.28 | Russian Federation | e.mobile-ks.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 211.149.219.167 | 147.237.77.170 | China | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.116.121.53 | 147.237.72.14 | United States | dover.idf.il(old) | ET SCAN NMAP -sS window 3072 | 1 |
| 200.241.137.4 | 147.237.76.39 | Brazil | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 37.143.82.50 | 147.237.76.39 | Netherlands | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 24.173.213.138 | 147.237.77.227 | United States | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 128.232.110.28 | 147.237.72.14 | United Kingdom | dover.idf.il(old) | ET SCAN Potential SSH Scan | 1 |
| 109.236.86.32 | 147.237.77.233 | Netherlands | atal.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 109.236.86.32 | 147.237.76.34 | Netherlands | yohalan.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 109.197.167.218 | 147.237.76.31 | Ukraine | nakchal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 109.60.153.178 | 147.237.0.19 | Russian Federation | madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 211.149.240.243 | 147.237.76.202 | China | e.halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 50.116.121.53 | 147.237.72.14 | United States | dover.idf.il(old) | ET SCAN NMAP -sS window 4096 | 1 |
| 202.84.44.85 | 147.237.76.197 | Bangladesh | e.himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 46.183.223.228 | 147.237.0.17 | Latvia | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 200.241.137.4 | 147.237.76.31 | Brazil | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 31.24.228.20 | 147.237.76.201 | United Kingdom | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 179.43.141.198 | 147.237.76.148 | Switzerland | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 118.103.126.194 | 147.237.76.44 | Japan | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

09-21-2016-06:04:07 to 09-21-2016-07:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 109.253.200.44 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 30 |
| 213.8.118.14 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 7 |
| 2.55.130.241 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 84.111.60.27 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 77.139.109.97 | France | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 109.253.128.111 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 77.139.109.97 | France | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 131.253.27.152 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 176.13.16.30 | Israel | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 2.53.14.3 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 84.111.60.27 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 76.113.152.120 | United States | 147.237.77.121 | e.navy.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 46.19.86.73 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 2.53.182.137 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 84.109.160.251 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 141.226.217.65 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 5.102.227.140 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 2 |
| 2.53.185.1 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 84.108.238.67 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 199.30.24.116 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 84.111.65.145 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 84.108.238.67 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 87.69.87.163 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 141.212.122.140 | United States | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 5.22.134.194 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 109.65.164.202 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 84.111.60.27 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 84.108.134.84 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 184.105.247.247 | United States | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 139.162.37.147 | United States | 147.237.0.200 | m4u.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 104.33.203.77 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 84.111.64.173 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 84.108.134.84 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 185.3.147.107 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 46.19.86.140 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 141.212.122.131 | United States | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 104.255.67.115 | United States | 147.237.77.74 | law.idf.il | Header Rejection | header rejection pattern found in request | monitor | 1 |
| 84.111.38.242 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 216.218.206.90 | United States | 147.237.76.201 | e.atal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 5.102.242.136 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 84.111.65.145 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 66.249.66.177 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 141.212.122.132 | United States | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 2.53.185.1 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 104.255.67.115 | United States | 147.237.77.176 | matpash.idf.il | Header Rejection | header rejection pattern found in request | monitor | 1 |
| 79.180.242.8 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 184.105.247.235 | United States | 147.237.76.202 | e.halag.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 37.142.188.238 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 120.132.67.209 | China | 147.237.76.39 | mobile.meitav.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |

09-21-2016-06:04:07 to 09-21-2016-07:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.55.18.62 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 23 |
| 62.219.198.6 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized HTTP Method | Block | 7 |
| 62.219.198.6 | Israel | 147.237.76.31 | nakchal.idf.il | Multiple Unauthorized URL Access from 62.219.198.6 | Block | 5 |
| 62.219.198.6 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/ | Block | 2 |
| 79.181.105.113 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 46.19.85.211 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp | Block | 2 |
| 84.95.208.20 | Israel | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 66.249.65.160 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/robots.txt | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/news/piwik.php | Block | 1 |
| 66.249.66.188 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx | 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 |
| 66.249.76.112 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter SearchParam in www.aka.idf.il/main/giyus/ | None | 1 |
| 46.4.74.42 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp | Block | 1 |
| 194.114.146.227 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp | 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/booklets.aspx | Block | 1 |
| 66.249.65.156 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |

09-21-2016-06:04:07 to 09-21-2016-07:04:07