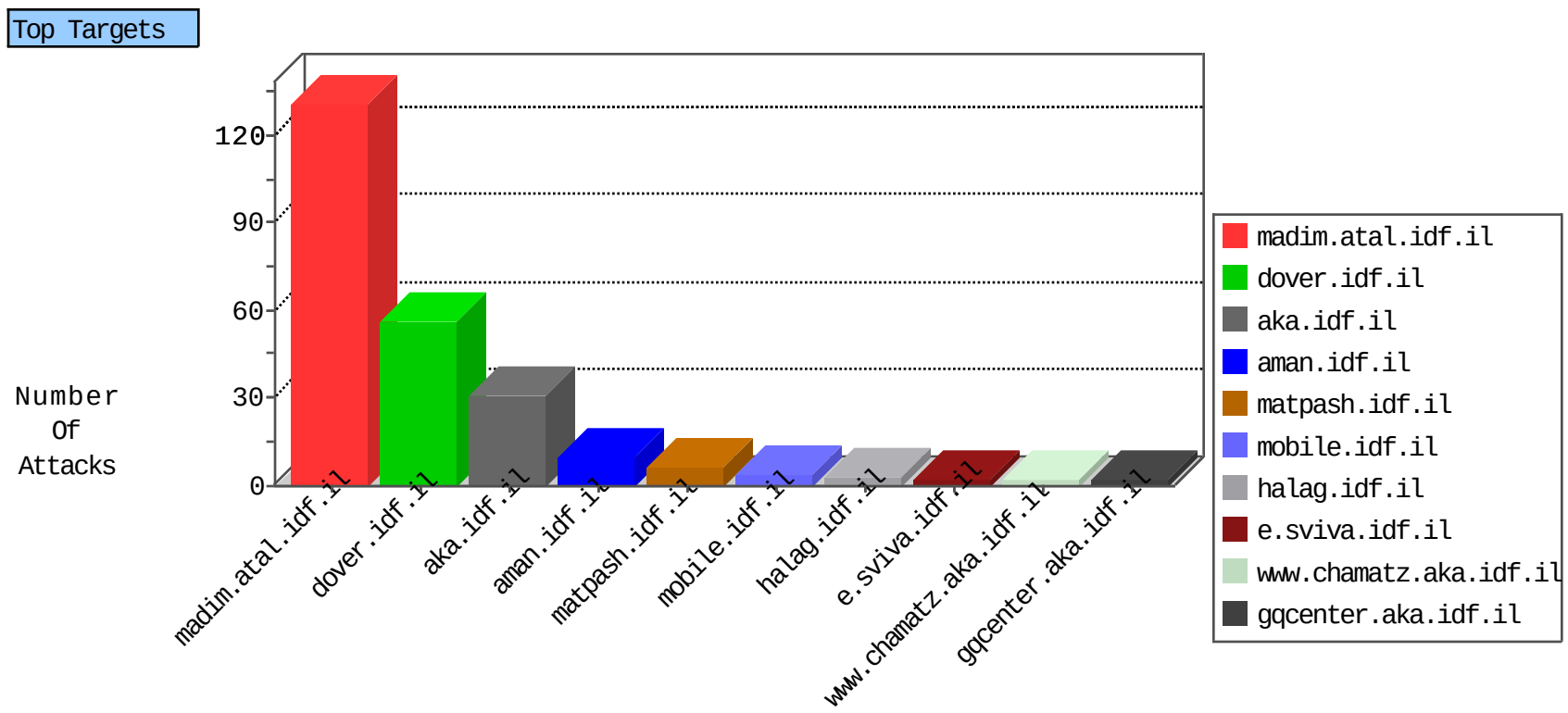
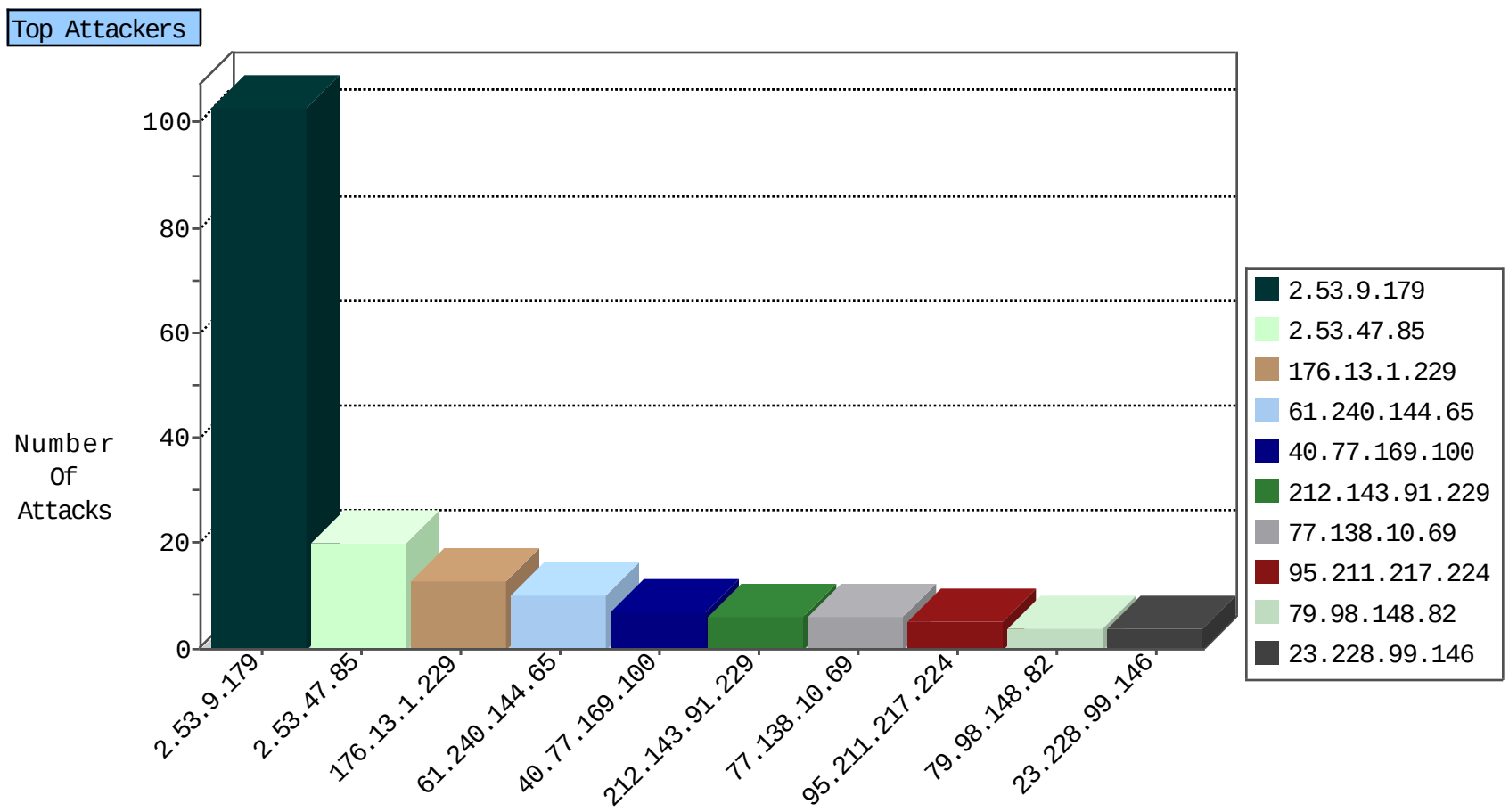
08-23-2016-22:04:04 to 08-23-2016-23:04:04

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



08-23-2016-22:04:04 to 08-23-2016-23:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.176.139.225 | Israel | 147.237.72.166 | aka.idf.il | Black List | drop | 2 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | forward | 2 |
| 89.248.168.21 | Netherlands | 147.237.76.42 | refuah.idf.il | Black List | drop | 1 |

08-23-2016-22:04:04 to 08-23-2016-23:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

08-23-2016-22:04:04 to 08-23-2016-23:04:04

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 88.249.106.23 | 147.237.8.50 | Turkey | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 66.240.213.93 | 147.237.76.39 | United States | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 216.81.230.167 | 147.237.76.31 | United States | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.77.205 | China | prisha.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 195.88.208.193 | 147.237.72.14 | Russian Federation | dover.idf.il(old) | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.77.176 | China | matpash.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 133.208.21.66 | 147.237.72.156 | Japan | aman.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 95.211.217.224 | 147.237.77.121 | Netherlands | e.navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.72.156 | China | aman.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 95.211.217.224 | 147.237.76.196 | Netherlands | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 95.211.217.224 | 147.237.76.147 | Netherlands | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 23.228.99.146 | 147.237.76.38 | United States | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.155 | 147.237.77.234 | Ukraine | halag.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 23.228.99.146 | 147.237.0.19 | United States | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 79.177.81.13 | 147.237.77.226 | Israel | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 65.156.199.242 | 147.237.76.34 | United States | yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 202.155.58.28 | 147.237.76.196 | Indonesia | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 190.219.88.249 | 147.237.76.30 | Panama | himush.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 61.240.144.65 | 147.237.76.202 | China | e.halag.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 107.191.53.122 | 147.237.77.235 | Japan | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 61.240.144.65 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 95.211.217.224 | 147.237.76.197 | Netherlands | e.himush.idf.il | ET SCAN Potential SSH Scan | 1 |
| 61.240.144.65 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 95.211.217.224 | 147.237.76.148 | Netherlands | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 23.228.99.146 | 147.237.76.176 | United States | test.ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.102.53.196 | 147.237.0.15 | Netherlands | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 23.228.99.146 | 147.237.76.30 | United States | himush.idf.il | ET SCAN Potential SSH Scan | 1 |

08-23-2016-22:04:04 to 08-23-2016-23:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 176.13.1.229 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 40.77.169.100 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 7 |
| 77.138.10.69 | France | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 212.143.91.229 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 62.128.62.1 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 128.242.249.12 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 79.98.148.82 | Poland | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 3 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 212.117.140.170 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 46.19.86.103 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 85.140.2.108 | Russian Federation | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 192.243.55.129 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 66.102.9.163 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.132.255 | Israel | 147.237.77.243 | mobile.idf.il | drop | First packet isn't SYN | drop | 1 |
| 157.55.39.34 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.253.145.113 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 61.240.144.65 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 109.253.156.69 | Israel | 147.237.77.243 | mobile.idf.il | drop | First packet isn't SYN | drop | 1 |
| 62.128.45.204 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 185.125.4.222 | Poland | 147.237.77.235 | sviva.idf.il | drop | SAM rule | drop | 1 |
| 31.217.176.21 | Greece | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 216.243.31.2 | United States | 147.237.0.33 | idf.il | drop |  | drop | 1 |
| 109.253.223.20 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 109.226.40.40 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 2.53.9.179 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 103 |
| 2.53.47.85 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 20 |
| 66.249.76.106 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/miluim/scriptresource.axd | Block | 3 |
| 46.116.99.58 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg | Block | 3 |
| 66.249.81.218 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 84.108.236.213 | Israel | 147.237.72.156 | aman.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 37.26.149.184 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.179.150.106 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.117.78.109 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.81.215 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.102.9.68 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 2.55.173.125 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 89.139.196.240 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 79.177.219.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/gius | Block | 1 |
| 180.76.15.28 | China | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-9236-he/refuah.aspx | Block | 1 |
| 80.230.231.16 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 66.249.66.75 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/yohalan/forums/forums.asp | Block | 1 |
| 5.29.124.47 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx | Block | 1 |
| 89.237.69.83 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 79.178.157.172 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 66.249.79.37 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.79.37 | Block | 1 |
| 207.46.13.126 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter pagenum in aka.idf.il/chinuch/gallery/ | None | 1 |
| 46.116.195.114 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/ | Block | 1 |
| 84.52.185.106 | Slovenia | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png | Block | 1 |
| 77.138.144.199 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp | Block | 1 |
| 66.249.66.78 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 1 |
| 37.19.116.11 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar | Block | 1 |
| 109.66.30.31 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 66.249.79.108 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/02112010.aspx | Block | 1 |
| 77.139.190.82 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp | Block | 1 |
| 66.249.66.142 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/.well-known/assetlinks.json | Block | 1 |
| 157.55.39.231 | United States | 147.237.77.176 | matpash.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 37.19.116.11 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/main/sacha | Block | 1 |
| 80.99.178.60 | Hungary | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.81.212 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |
| 46.117.197.2 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/עיטוד | Block | 1 |
| 85.250.58.114 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx | Block | 1 |
| 79.98.148.82 | Poland | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.76.30 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1751 | Block | 1 |
| 176.13.233.75 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/nekudot/index | Block | 1 |
| 80.230.231.12 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 1 |

08-23-2016-22:04:04 to 08-23-2016-23:04:04