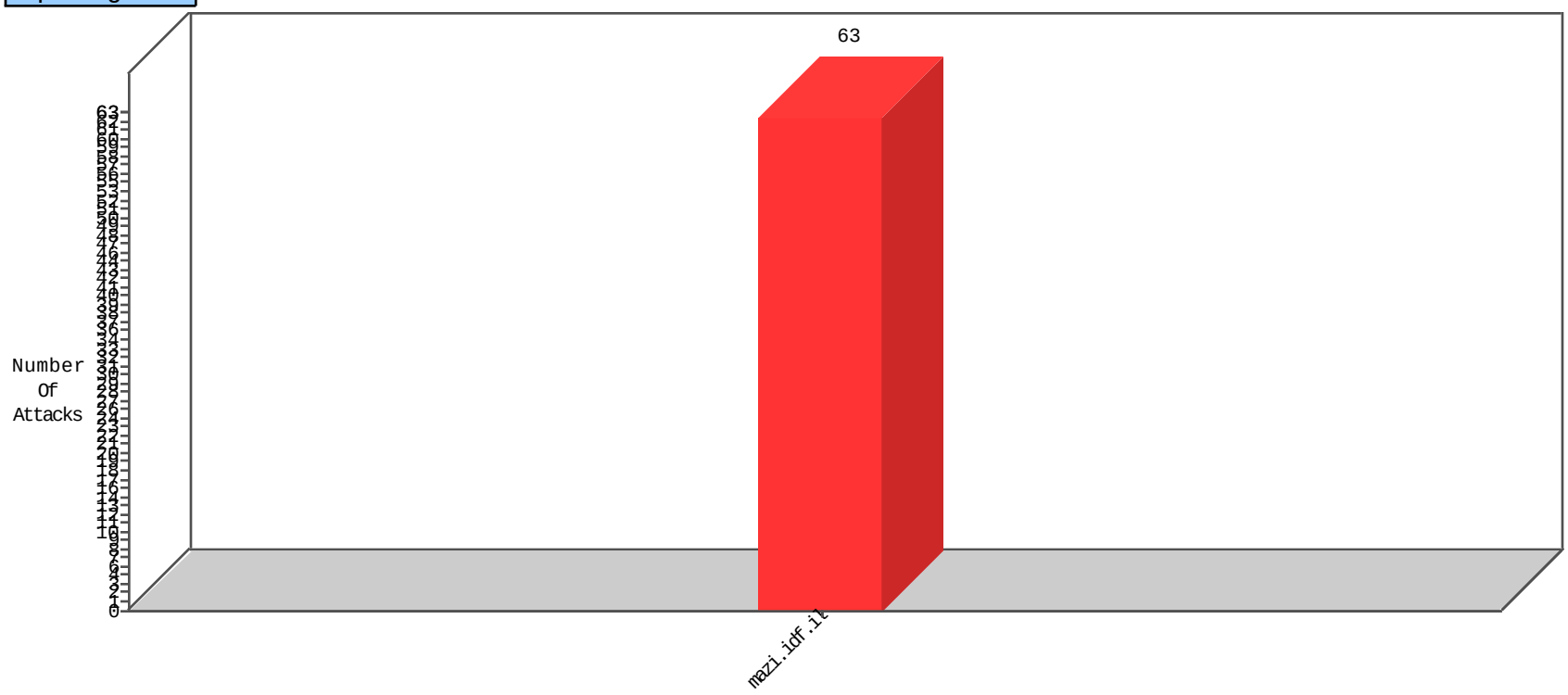
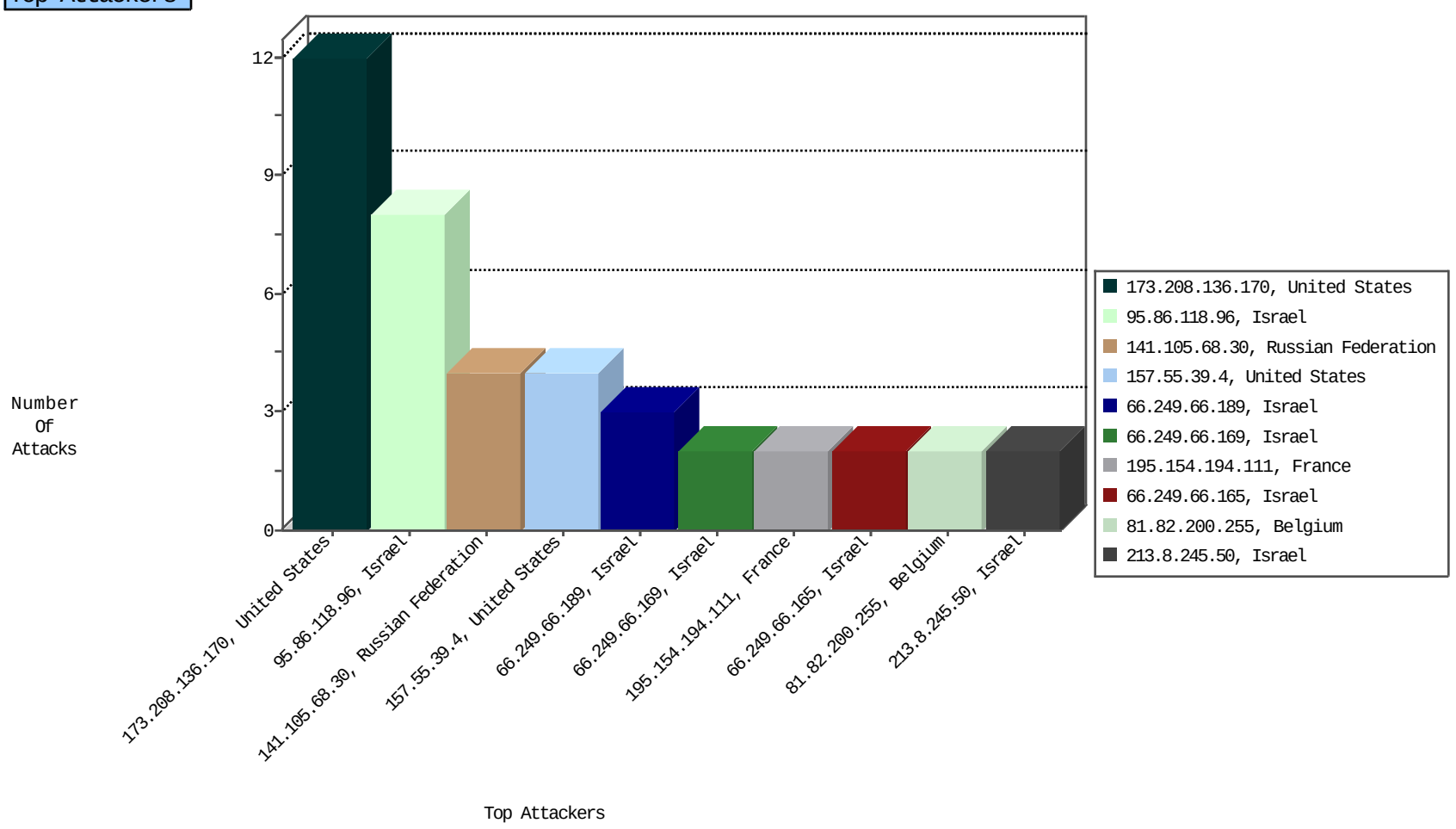
01-12-2016 to 01-13-2016

# Focused IP Under Attack Daily Report

## Top Targets




## Top Attackers



01-12-2016 to 01-13-2016

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | DP_location.Location | Count |
|---|---|---|---|---|---|---|---|

01-12-2016 to 01-13-2016

## Top Attackers In IPS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 157.55.39.4 | United States | 147.237.77.17 | mazi.idf.il | C072: HTTP: Access to - Ajax.aspx | Block | 1 |

01-12-2016 to 01-13-2016

## Top Attackers In IDS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Count |
|---|---|---|---|---|---|
| 61.166.33.184 | China | 147.237.77.17 | mazi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 81.82.200.255 | Belgium | 147.237.77.17 | mazi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 117.31.224.80 | China | 147.237.77.17 | mazi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 212.48.74.51 | United Kingdom | 147.237.77.17 | mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 81.82.200.255 | Belgium | 147.237.77.17 | mazi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 89.248.167.162 | Netherlands | 147.237.77.17 | mazi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.106.92.109 | | 147.237.77.17 | mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

01-12-2016 to 01-13-2016

## Top Attackers In FW

| Attacker Address | Attacker Geo | Target Address | Site | Name | Signature | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 84.111.84.98 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1369 |
| 40.77.167.43 | United States | 147.237.77.17 | mazi.idf.i | drop | SAM rule | drop | 760 |
| 212.76.127.219 | Israel | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 333 |
| 132.74.244.137 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN retransmit with different window scale | monitor | 129 |
| 173.208.136.170 | United States | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 117 |
| 212.76.127.10 | Israel | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 45 |
| 141.105.68.30 | Russian Federation | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 40 |
| 2.52.140.96 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 14 |
| 46.19.86.253 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 85.250.255.225 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 37.46.39.235 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 195.239.16.40 | Russian Federation | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 46.19.86.183 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 9 |
| 195.239.16.53 | Russian Federation | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 9 |
| 31.210.187.226 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 94.159.166.221 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 217.132.72.224 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 46.19.86.183 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 37.26.147.186 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 94.159.166.221 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 24.114.43.96 | Canada | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 2.54.35.106 | Israel | 147.237.77.17 | mazi.idf.i | Web Server Enforcement Violation | Web Servers Slow HTTP Denial of Service | reject | 2 |
| 207.46.13.18 | United States | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 213.8.71.26 | Israel | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 2 |
| 2.54.160.56 | Israel | 147.237.77.17 | mazi.idf.i | Web Server Enforcement Violation | Web Servers Slow HTTP Denial of Service | reject | 2 |
| 85.64.28.23 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 46.19.85.44 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 149.78.58.253 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 37.26.148.143 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 5.22.131.40 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 77.127.179.106 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 46.146.224.35 | Russian Federation | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 194.90.198.147 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid sequence number | monitor | 1 |
| 46.19.86.71 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 169.229.3.91 | United States | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 68.144.48.134 | Canada | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 46.121.44.147 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 185.3.147.33 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 46.19.85.144 | Israel | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 149.78.58.253 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 94.159.180.66 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 5.102.253.45 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 2.52.57.123 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 61.242.114.58 | China | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 195.154.146.225 | France | 147.237.77.17 | mazi.idf.i | drop | SAM rule | drop | 1 |
| 46.19.85.9 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 31.210.187.226 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 89.138.177.226 | Israel | 147.237.77.17 | mazi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 2.54.152.192 | Israel | 147.237.77.17 | mazi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 1 |
| 71.6.165.200 | United States | 147.237.77.17 | mazi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |

01-12-2016 to 01-13-2016

## Top Attackers In WAF

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 95.86.118.96 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif | Block | 8 |
| 173.208.136.170 | United States | 147.237.77.17 | mazi.idf.i | Multiple Admin Blocking from 173.208.136.170 | Block | 5 |
| 173.208.136.170 | United States | 147.237.77.17 | mazi.idf.i | Multiple Unauthorized URL Access from 173.208.136.170 | Block | 5 |
| 141.105.68.30 | Russian Federation | 147.237.77.17 | mazi.idf.i | Multiple Unauthorized URL Access from 141.105.68.30 | Block | 4 |
| 66.249.66.173 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/5484-7277-he/igf.aspx | Block | 1 |
| 66.249.66.49 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/vodchannel/ | Block | 1 |
| 213.8.245.50 | Israel | 147.237.77.17 | mazi.idf.i | Multiple Unauthorized URL Access from 213.8.245.50 | Block | 1 |
| 173.208.136.170 | United States | 147.237.77.17 | mazi.idf.i | Admin Blocking | Block | 1 |
| 84.109.116.45 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx | Block | 1 |
| 66.249.66.165 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/robots.txt | Block | 1 |
| 5.28.131.167 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx | Block | 1 |
| 195.154.194.111 | France | 147.237.77.17 | mazi.idf.i | PHP Attempt | Block | 1 |
| 157.55.39.4 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/scripts/sites/coremetrics/cmdatatagutils.inc | Block | 1 |
| 66.249.66.189 | Israel | 147.237.77.17 | mazi.idf.i | Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined | Block | 1 |
| 66.249.66.134 | Israel | 147.237.77.17 | mazi.idf.i | Multiple Unauthorized URL Access from 66.249.66.134 | Block | 1 |
| 213.8.245.50 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to www.mazi.idf.il/sip_storage/files/4/11464.jpg | Block | 1 |
| 149.78.80.199 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx | Block | 1 |
| 93.173.23.127 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined | Block | 1 |
| 66.249.66.169 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/6222-9239-he/igf.aspx | Block | 1 |
| 65.55.212.76 | United States | 147.237.77.17 | mazi.idf.i | Distributed Unauthorized URL Access on igf.idf.il/templates/newslist/undefined | Block | 1 |
| 195.154.194.111 | France | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/wp-login.php | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.17 | mazi.idf.i | Multiple Illegal Byte Code Character in Method from 169.229.3.91 | Block | 1 |
| 131.253.24.135 | United States | 147.237.77.17 | mazi.idf.i | Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined | Block | 1 |
| 66.249.66.189 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/5551-11516-he/×ž×©×œ×‘×™×? ×§×”×™×œ×”.aspx | Block | 1 |
| 66.249.66.134 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined | Block | 1 |
| 157.55.39.4 | United States | 147.237.77.17 | mazi.idf.i | Multiple Unauthorized URL Access from 157.55.39.4 | Block | 1 |
| 95.86.101.229 | Israel | 147.237.77.17 | mazi.idf.i | Multiple Unauthorized URL Access from 95.86.101.229 | Block | 1 |
| 66.249.66.169 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx | Block | 1 |
| 65.55.218.38 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to igf.idf.il/templates/newslist/undefined | Block | 1 |
| 212.179.185.157 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.17 | mazi.idf.i | NULL Character in Method | Block | 1 |
| 132.74.244.137 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx | Block | 1 |
| 66.249.66.189 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/ | Block | 1 |
| 66.249.66.165 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx | Block | 1 |
| 173.208.136.170 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to igf.idf.il/admin/ftb.imagegallery.aspx | Block | 1 |
| 157.55.39.4 | United States | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/5551-11516-he/Ã–Å¾Ã–Â©Ã–Å“Ã–â€˜Ã–â„¢Ã–Â? Ã–Â§Ã–â€?Ã–â„¢Ã–Å“Ã–â€?.aspx | Block | 1 |
| 95.86.101.229 | Israel | 147.237.77.17 | mazi.idf.i | Unauthorized URL Access to mazi.idf.il/4170-he/igf.aspx&sa=u&ved=0ahukewjf9t2r3ktkahwhpxqkhznnafuqfgglmae&sig2=s56ciu_6fy_ezjwyxxx7-q&usg=afqjcnfgyo7tnqu-ek37cirnv5lwhyrmzg | Block | 1 |

01-12-2016 to 01-13-2016