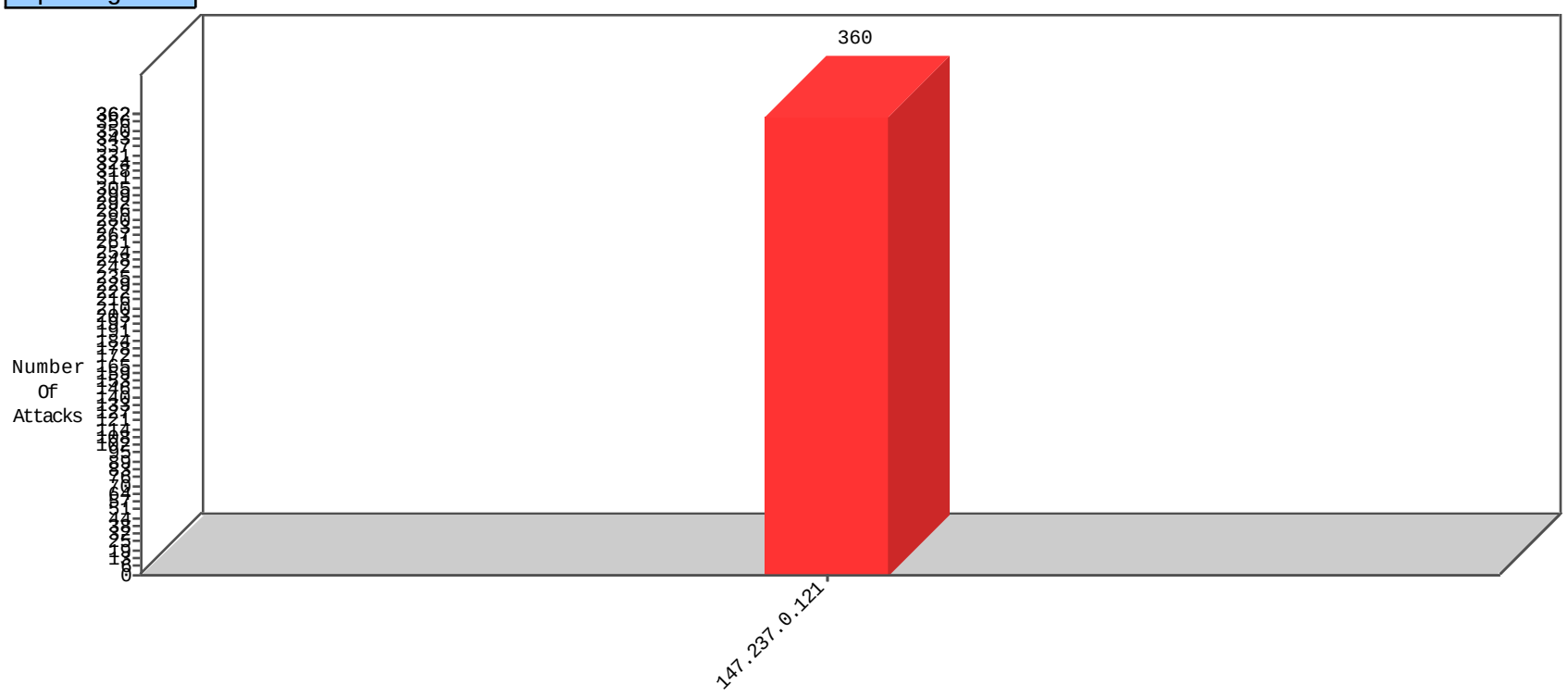
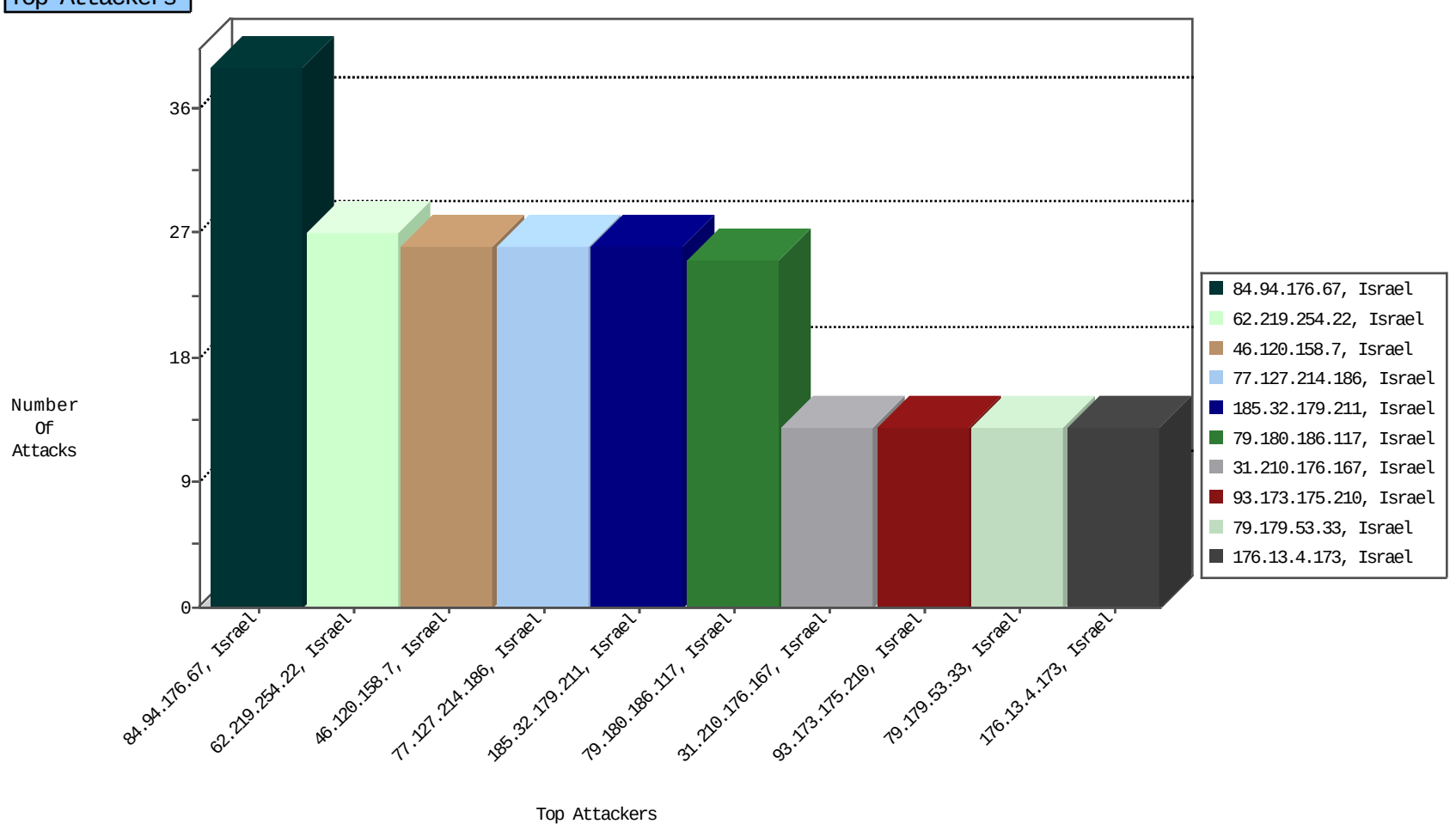
10-16-2015 to 10-17-2015

# Focused IP Under Attack Daily Report

## Top Targets




## Top Attackers



10-16-2015 to 10-17-2015

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | DP_location.Location | Count |
|---|---|---|---|---|---|---|---|
| 62.219.254.22 | Israel | 147.237.0.121 | | Block_Udp_All_Nets | drop | BBL-Israel | 27 |
| 146.185.57.7 | Israel | 147.237.0.121 | | Block_Udp_All_Nets | drop | BBL-Israel | 3 |

10-16-2015 to 10-17-2015

## Top Attackers In IPS

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

10-16-2015 to 10-17-2015

## Top Attackers In IDS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Count |
|---|---|---|---|---|---|
| 61.240.144.67 | China | 147.237.0.121 | | ET SCAN NMAP -sS window 1024 | 1 |
| 181.177.245.75 | Peru | 147.237.0.121 | | ET SCAN NMAP -f -sS | 1 |
| 61.240.144.66 | China | 147.237.0.121 | | ET SCAN NMAP -sS window 1024 | 1 |
| 77.120.133.250 | Ukraine | 147.237.0.121 | | ET SCAN Potential SSH Scan | 1 |
| 181.177.245.75 | Peru | 147.237.0.121 | | ET SCAN NMAP -sS window 2048 | 1 |
| 60.185.177.23 | China | 147.237.0.121 | | ET SCAN Potential SSH Scan | 1 |

10-16-2015 to 10-17-2015

## Top Attackers In FW

| Attacker Address | Attacker Geo | Target Address | Site | Name | Signature | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 149.78.150.127 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 2434 |
| 66.249.93.150 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 1359 |
| 66.249.81.254 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 1264 |
| 66.249.81.251 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 1190 |
| 66.249.93.154 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 1061 |
| 66.249.93.146 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 1056 |
| 149.78.228.126 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 720 |
| 66.249.81.130 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 679 |
| 149.78.148.244 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 605 |
| 149.78.228.231 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 499 |
| 149.78.245.252 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 470 |
| 149.78.242.29 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 416 |
| 149.88.86.92 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 414 |
| 149.88.149.97 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 385 |
| 200.126.195.111 | Argentina | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 332 |
| 149.88.116.35 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 272 |
| 80.178.13.63 | Israel | 147.237.0.121 | | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 252 |
| 149.88.230.134 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 212 |
| 149.88.72.62 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 172 |
| 149.88.136.79 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 171 |
| 149.88.38.93 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 151 |
| 149.78.255.157 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 142 |
| 66.249.81.130 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 141 |
| 66.249.81.254 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 134 |
| 79.182.147.157 | Israel | 147.237.0.121 | | drop | SAM rule | drop | 133 |
| 149.78.26.200 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 129 |
| 84.228.64.80 | Israel | 147.237.0.121 | | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 117 |
| 66.249.93.146 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 112 |
| 98.254.60.1 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 108 |
| 149.78.45.28 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 108 |
| 190.16.164.165 | Argentina | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 99 |
| 66.249.81.251 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 94 |
| 66.249.93.150 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 94 |
| 149.88.101.131 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 90 |
| 66.249.93.154 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 87 |
| 66.249.93.247 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 81 |
| 190.104.214.7 | Argentina | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 80 |
| 149.78.164.41 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 74 |
| 149.88.82.194 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 65 |
| 204.145.74.25 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 64 |
| 153.160.114.186 | Japan | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 64 |
| 205.215.249.94 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 58 |
| 217.69.133.250 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 55 |
| 149.78.30.59 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 45 |
| 149.78.42.11 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 44 |
| 217.69.133.249 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 44 |
| 149.78.27.62 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 43 |
| 66.249.93.241 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 43 |
| 84.42.170.138 | Czech Republic | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 42 |
| 66.249.93.244 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 42 |

## Top Attackers In WAF

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.94.176.67 | Israel | 147.237.0.121 | | Parameter Type Violation ReturnUrl in www.miluim-ishi.aka.idf.il/login | Block | 39 |
| 79.180.186.117 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/medicalcommitteerequest | Block | 25 |
| 109.65.75.174 | Israel | 147.237.0.121 | | Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 79.179.53.33 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit | Block | 13 |
| 46.116.137.71 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddAddressAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 84.109.192.159 | Israel | 147.237.0.121 | | Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/ | Block | 13 |
| 46.121.113.242 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest | Block | 13 |
| 31.210.176.167 | Israel | 147.237.0.121 | | Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/ | Block | 13 |
| 176.13.4.173 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/firstlogin | Block | 13 |
| 46.120.158.7 | Israel | 147.237.0.121 | | Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 93.173.175.210 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 13 |
| 77.127.214.186 | Israel | 147.237.0.121 | | Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 46.19.85.20 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 13 |
| 185.32.179.211 | Israel | 147.237.0.121 | | Multiple Untraceable SSL Sessions from 185.32.179.211 (Open Mode) | None | 13 |
| 82.102.169.113 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 13 |
| 46.120.158.7 | Israel | 147.237.0.121 | | Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 109.65.35.65 | Israel | 147.237.0.121 | | Cookie Tampering on cookie .ASPXAUTH: Expected FF7FE77B29AC60750D8F98DDF40545708B47264416A4C26F73E70120469F863937480972773254 7571F7CA3004D9F155813AC82ED645F2879BED8793D306B80CC84F18ACE45FE67190775F03DD 19B82CE547F37BF42FDB2E2D2F41AF891017F625985EDF0271037AB95F4AF086251E9E887B01415 0E16F0C52E53514E8D15BDB, Observed AD5231CD405019BF02F0CEC804BC81FCD5B62A5A89247B4CDCAC5999D71C93486561530DC0 573C697B173E953E150A83BEC7446AC1BFDA90B51E7FB2B1E421B70053E49E4E02F2393AD563A 8A09FBFE2A7B6D32AE3D2CE0DD2936DA1B0D0EDE13C2D31 | None | 13 |
| 77.127.214.186 | Israel | 147.237.0.121 | | Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 46.19.85.90 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 13 |
| 185.32.179.211 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 13 |
| 46.121.26.97 | Israel | 147.237.0.121 | | Cookie Tampering on cookie .ASPXAUTH: Expected 849AC8EAB3159B769C62E8852AE76167A1E30598472E817C8864E43AD4689F32B6243EBF1E519E 095C330765646EAA7E56E47DAAD50FE2B294B6109C023FF55B94EFD8461F857182748382CD521 7CCA83D161EF23DFCC7B5CEF7914A746EC86DC402DED4C692505FF430F93B6A3E89D78C3904B 7338758DA719BB9D31D5C1559, Observed BD32C3BBACFA26F543C9685F7CC3012DADFD8BB1642D77A4EA92340471F51DCFEB7B6E9DDF0 CABC3BEBFA07DB243E2462140159AEF0472CA9083203A12D8DDD6550C9CB58E664462A1ED18 42E557EBA2CDCABDD7CA9D93EBB6A033B559F60BCDC378C8 | None | 13 |
| 2.54.176.24 | Israel | 147.237.0.121 | | Distributed Double URL Encoding | Block | 13 |