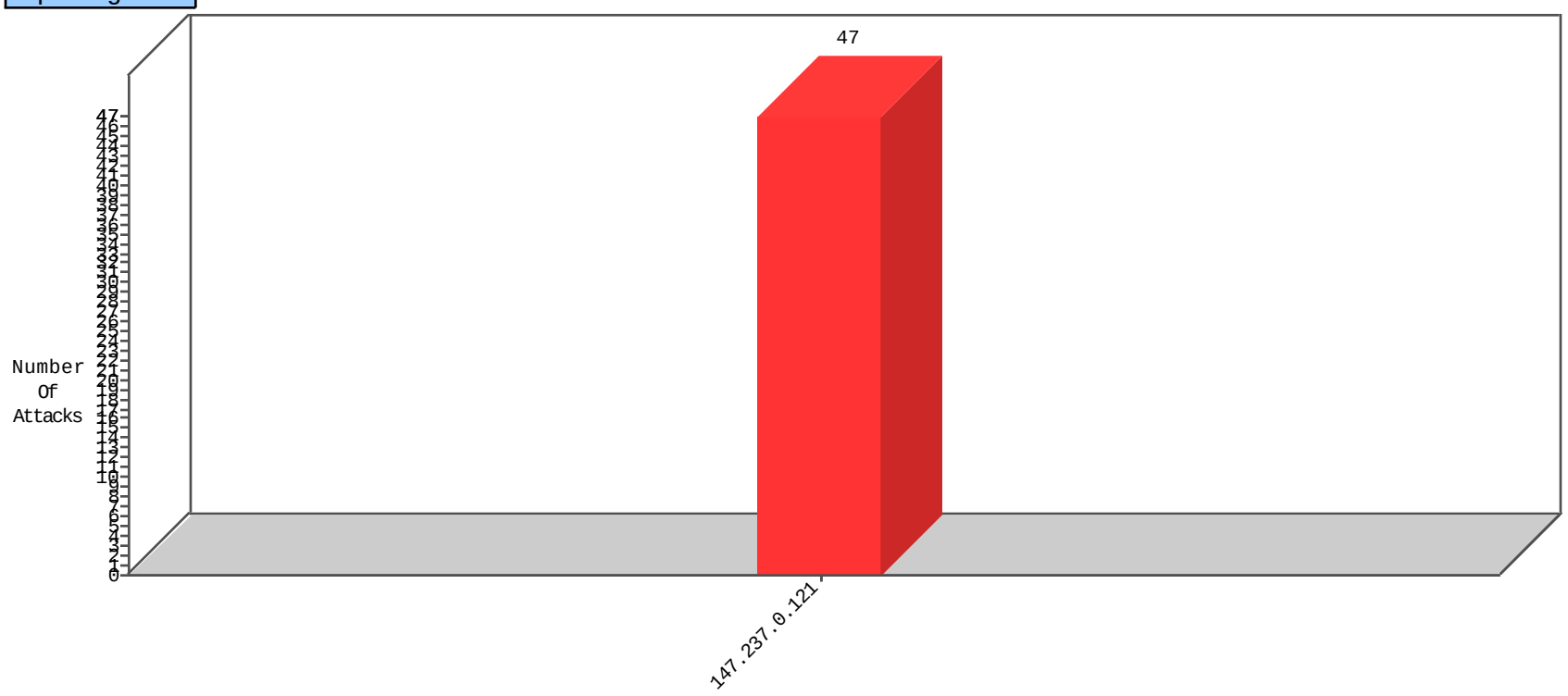
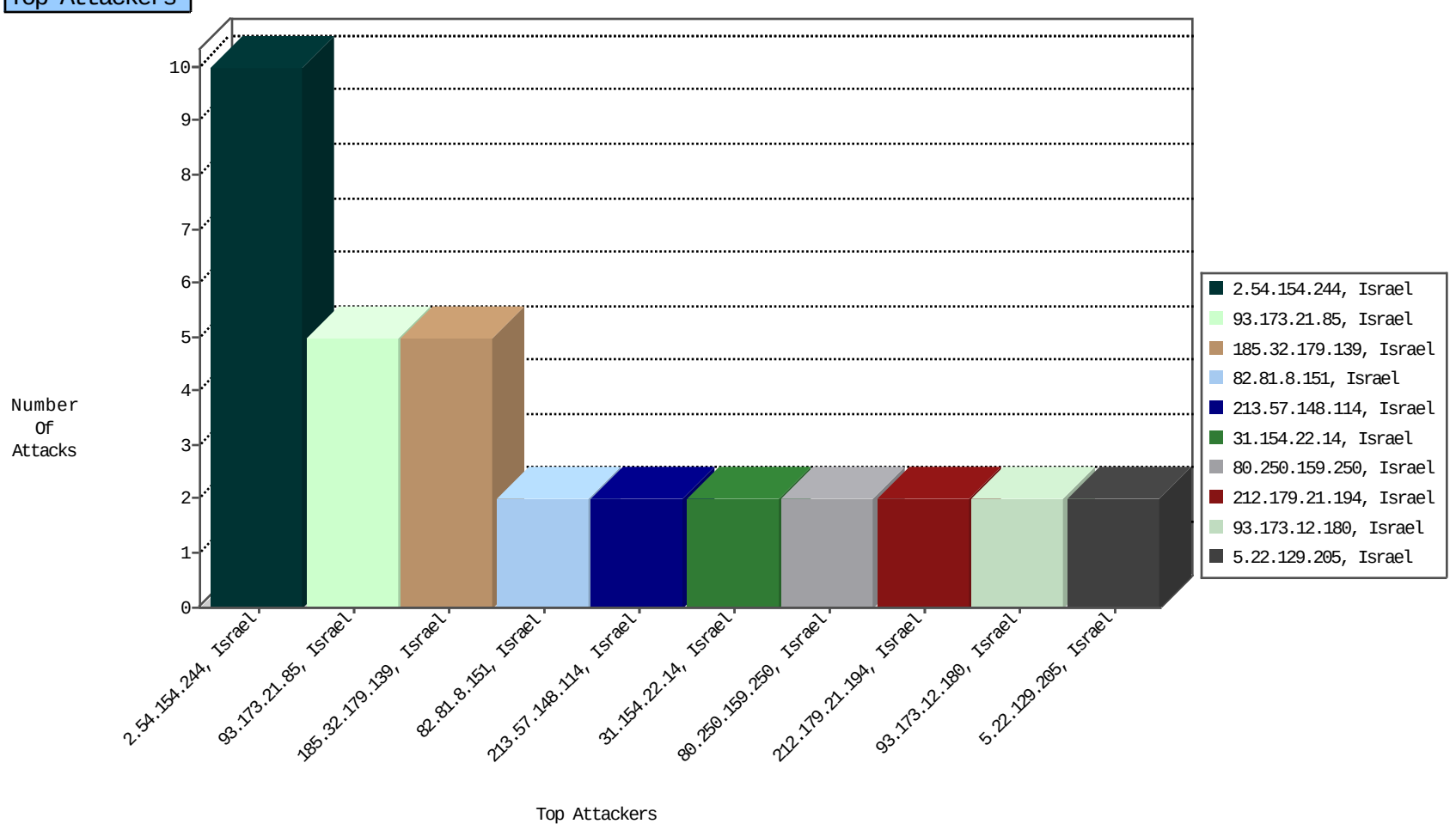
11-24-2015 to 11-25-2015

# Focused IP Under Attack Daily Report

## Top Targets




## Top Attackers



11-24-2015 to 11-25-2015

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | DP_location.Location | Count |
|---|---|---|---|---|---|---|---|
| 185.32.179.139 | Israel | 147.237.0.121 | | Anomaly-SSL-renegotiation-Cli | dest-reset | BBL-Israel | 5 |

11-24-2015 to 11-25-2015

## Top Attackers In IPS

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

11-24-2015 to 11-25-2015

## Top Attackers In IDS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Count |
|---|---|---|---|---|---|
| 169.54.233.119 | Netherlands | 147.237.0.121 | | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 74.208.43.251 | United States | 147.237.0.121 | | ET SCAN Potential SSH Scan | 1 |

11-24-2015 to 11-25-2015

## Top Attackers In FW

| Attacker Address | Attacker Geo | Target Address | Site | Name | Signature | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 149.78.47.62 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 6796 |
| 66.249.93.146 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 3263 |
| 66.249.93.150 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 3203 |
| 66.249.93.154 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 2803 |
| 149.78.22.6 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 1451 |
| 149.78.27.42 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 449 |
| 90.181.168.124 | Czech Republic | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 432 |
| 66.249.93.154 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 331 |
| 37.153.211.94 | Netherlands | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 330 |
| 66.249.93.146 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 298 |
| 66.249.93.150 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 263 |
| 2.52.16.26 | Israel | 147.237.0.121 | | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 144 |
| 149.88.38.203 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 144 |
| 185.32.179.241 | Israel | 147.237.0.121 | | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 144 |
| 149.78.253.156 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 139 |
| 149.78.125.159 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 117 |
| 149.78.63.20 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 115 |
| 66.249.81.251 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 115 |
| 66.249.81.254 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 112 |
| 66.249.81.130 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 94 |
| 217.69.133.169 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 63 |
| 66.249.66.109 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 58 |
| 66.249.66.105 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 56 |
| 31.168.23.60 | Israel | 147.237.0.121 | | SYN Attack | SYN -> SYN-ACK -> RST | reject | 50 |
| 66.249.81.130 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 50 |
| 217.69.133.252 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 50 |
| 66.249.81.251 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 48 |
| 66.249.81.254 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 46 |
| 217.69.133.249 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 44 |
| 149.88.81.41 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 40 |
| 78.192.73.64 | France | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 40 |
| 149.78.41.248 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 38 |
| 192.116.232.69 | Israel | 147.237.0.121 | | SYN Attack | SYN -> SYN-ACK -> RST | reject | 37 |
| 149.78.166.31 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 36 |
| 138.134.102.16 | Israel | 147.237.0.121 | | SYN Attack | SYN -> SYN-ACK -> RST | reject | 36 |
| 66.249.66.107 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 35 |
| 201.85.85.123 | Brazil | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 35 |
| 31.13.112.117 | Ireland | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 34 |
| 134.191.232.71 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 34 |
| 66.249.93.220 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 34 |
| 201.31.215.129 | Brazil | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 31 |
| 66.249.66.105 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 31 |
| 217.69.133.248 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 28 |
| 66.249.81.235 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 27 |
| 66.249.81.160 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 25 |
| 66.249.93.216 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 24 |
| 185.32.179.66 | Israel | 147.237.0.121 | | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 20 |
| 157.55.39.55 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 20 |
| 66.249.93.247 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 18 |
| 185.32.179.139 | Israel | 147.237.0.121 | | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |

11-24-2015 to 11-25-2015

## Top Attackers In WAF

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 93.173.21.85 | Israel | 147.237.0.121 | | Multiple Unauthorized URL Access from 93.173.21.85 | Block | 5 |
| 2.54.154.244 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd | Block | 5 |
| 2.54.154.244 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd | Block | 4 |
| 213.57.148.114 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest | Block | 2 |
| 31.154.22.14 | Israel | 147.237.0.121 | | Distributed Cookie Tampering on token: .ASPXAUTH | None | 2 |
| 80.250.159.250 | Israel | 147.237.0.121 | | Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 3834B564979ED2F4B96127C10E136D360184676170E92BB8257F62728492F5B04BA0E0B088D320030BEEF8B0977C8DDA8CE4B8926881CEDE1123762F9D30AD6557F12E3591A21AE343ABD80E094CC9F9F78AAED5AC2440D2FA365E8B704C0C760E7ED90123A48765CB12B949894C5E3A708F322A8B0412C4FF02BC0FA3FA7051058AF2A5FDBF91DD5EC6D73E5F21B9C32D6545B39C2ECEAC9F2435CE21E41B55 | None | 2 |
| 84.108.147.164 | Israel | 147.237.0.121 | | Cookie Tampering on cookie .ASPXAUTH: Expected 19991342F5FD604E82224A02A33D9546A9529CC560879881BC3E4BFCE13255034EE850BA48EB8A57406B1EA3ADCE739BDE76FF9735E39E0F5D77C1DD58F386575CE8C77DDF0913320DB4DEDB922B7BD19DED3FEF18C321D0EC132D7EB7A4FA6A52246C1088971F6A9490AB13C33371E7625D45114F269A2EB47535CE1B01DDCD, Observed F56A72A0B83C53EE304896E4EA5AC50E5463CA3162EF30CA3B4F182C10A9932625C207571827E62D167C256F319A3CC66F9F2A454DEB7E59E880FFBDCAB4846748BDDABAEF32F106A67BA21E8EF09664E441C9CBEC2E17C4C1243096B7392EC38A0BCB | None | 2 |
| 212.179.21.194 | Israel | 147.237.0.121 | | Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/ | Block | 2 |
| 84.95.211.33 | Israel | 147.237.0.121 | | Untraceable SSL Sessions: Open Mode | None | 1 |
| 2.52.61.203 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 1 |
| 5.22.129.205 | Israel | 147.237.0.121 | | Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login | Block | 1 |
| 213.57.162.165 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login | Block | 1 |
| 37.26.148.244 | Israel | 147.237.0.121 | | Multiple Untraceable SSL Sessions from 37.26.148.244 (Open Mode) | None | 1 |
| 2.54.154.244 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest | Block | 1 |
| 109.65.167.56 | Israel | 147.237.0.121 | | Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/ | Block | 1 |
| 82.81.8.151 | Israel | 147.237.0.121 | | Multiple Untraceable SSL Sessions from 82.81.8.151 (Unknown SSL Session) | None | 1 |
| 5.22.129.205 | Israel | 147.237.0.121 | | Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login | Block | 1 |
| 93.173.12.180 | Israel | 147.237.0.121 | | Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login | Block | 1 |
| 37.26.148.244 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 1 |
| 82.81.8.151 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Unknown SSL Session | None | 1 |
| 5.102.205.151 | Israel | 147.237.0.121 | | Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login | Block | 1 |
| 2.52.40.75 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 1 |
| 93.173.12.180 | Israel | 147.237.0.121 | | Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login | Block | 1 |
| 80.246.138.5 | Israel | 147.237.0.121 | | Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login | Block | 1 |

11-24-2015 to 11-25-2015