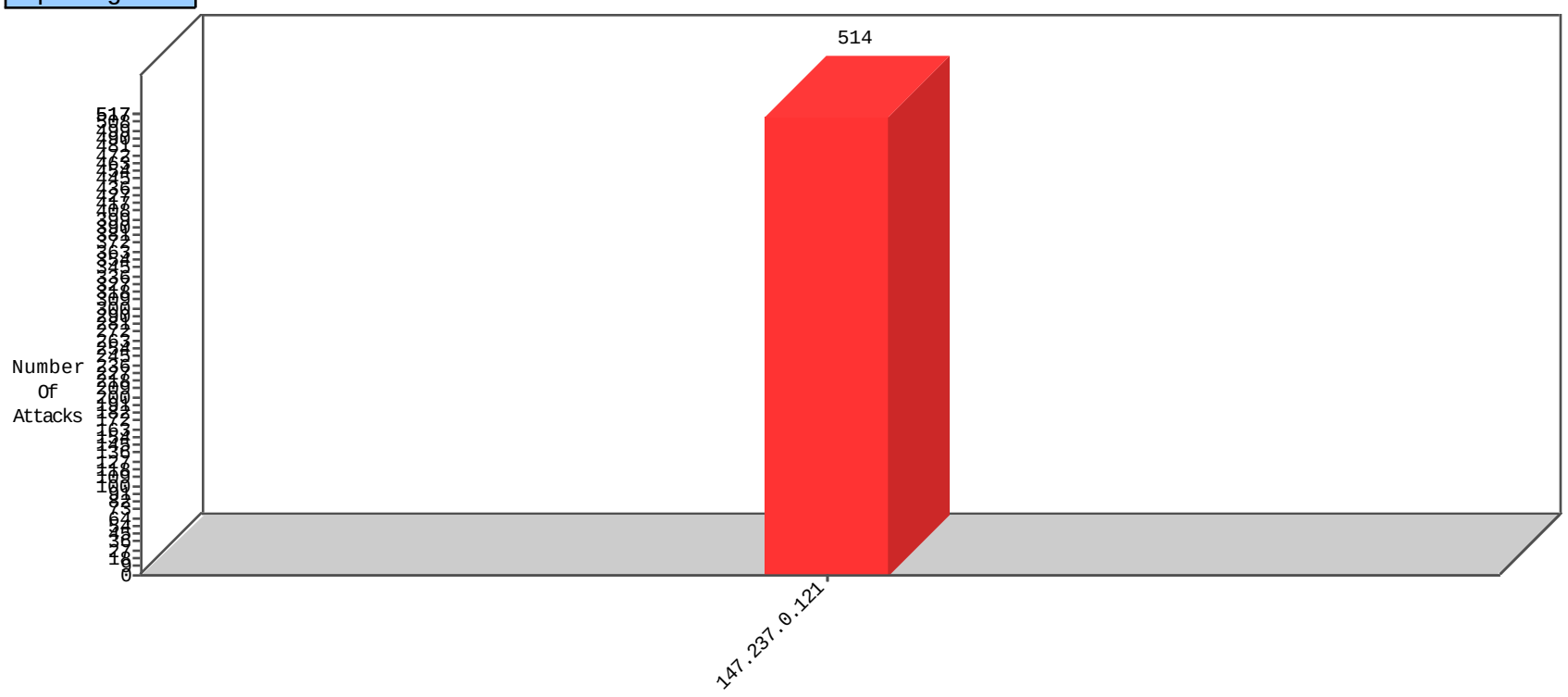
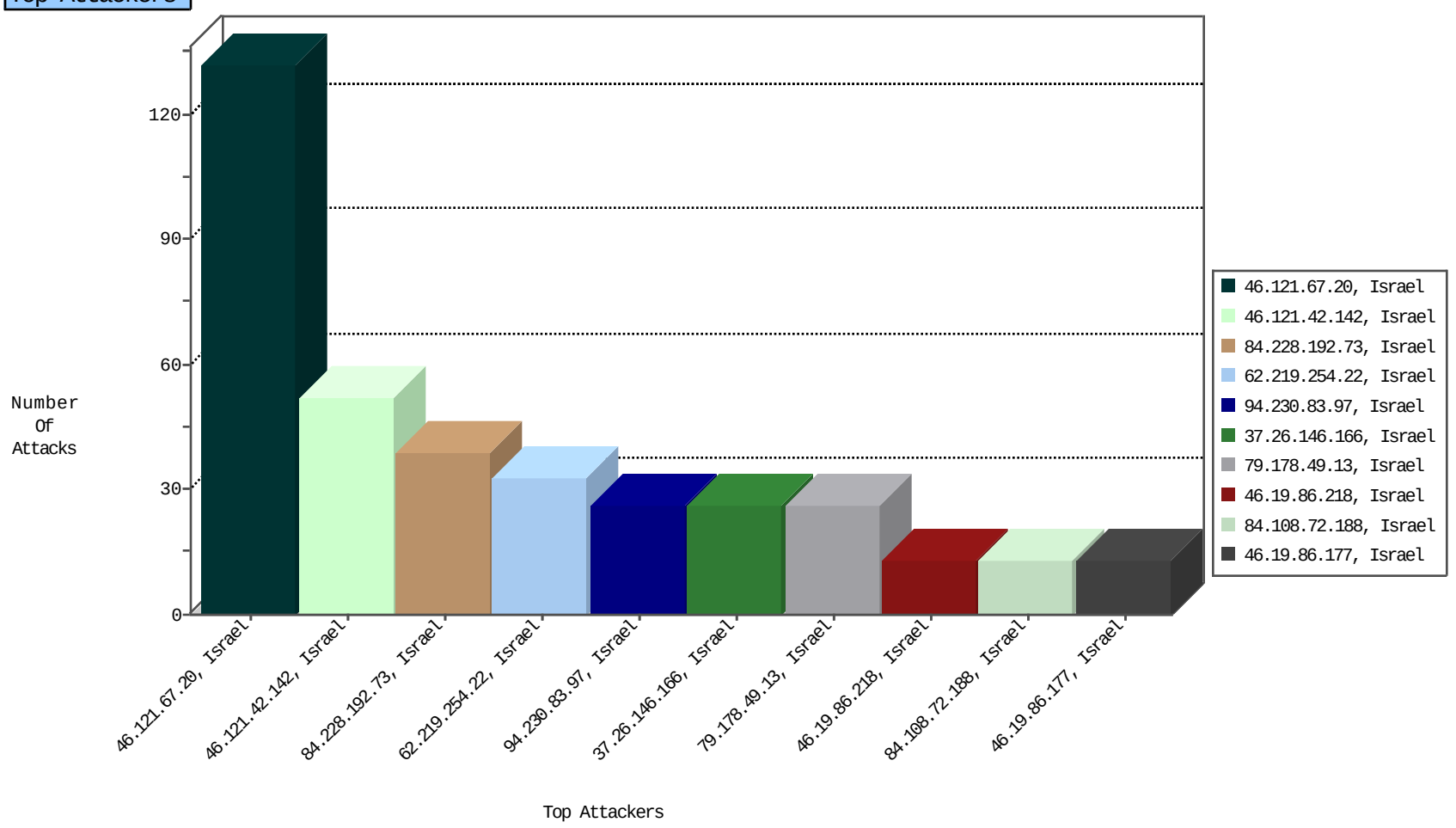
10-17-2015 to 10-18-2015

# Focused IP Under Attack Daily Report

## Top Targets




## Top Attackers



10-17-2015 to 10-18-2015

## 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 | 33 |

10-17-2015 to 10-18-2015

## Top Attackers In IPS

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

10-17-2015 to 10-18-2015

## Top Attackers In IDS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Count |
|---|---|---|---|---|---|
| 192.198.151.45 | Europe | 147.237.0.121 | | ET SCAN NMAP -sA (2) | 6 |
| 192.198.151.44 | Europe | 147.237.0.121 | | ET SCAN NMAP -sA (2) | 2 |
| 61.182.170.38 | China | 147.237.0.121 | | ET SCAN Potential SSH Scan | 1 |
| 41.74.9.153 | Benin | 147.237.0.121 | | ET SCAN Potential SSH Scan | 1 |
| 91.181.173.33 | Belgium | 147.237.0.121 | | ET SCAN Potential SSH Scan | 1 |

10-17-2015 to 10-18-2015

## Top Attackers In FW

| Attacker Address | Attacker Geo | Target Address | Site | Name | Signature | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.249.93.150 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 1950 |
| 66.249.93.154 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 1766 |
| 66.249.93.146 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 1543 |
| 149.78.231.47 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 648 |
| 149.78.225.110 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 450 |
| 149.78.237.24 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 437 |
| 149.88.177.91 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 250 |
| 200.126.195.111 | Argentina | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 225 |
| 149.78.160.59 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 213 |
| 149.78.19.178 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 204 |
| 216.67.15.19 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 190 |
| 149.78.209.64 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 176 |
| 93.48.250.101 | Italy | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 174 |
| 66.249.93.146 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 171 |
| 66.249.93.150 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 169 |
| 66.249.93.154 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 167 |
| 212.247.176.200 | Sweden | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 155 |
| 149.78.150.127 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 130 |
| 5.45.203.205 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 126 |
| 37.9.88.65 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 126 |
| 149.88.87.227 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 118 |
| 149.88.67.150 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 116 |
| 149.78.63.77 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 112 |
| 84.109.162.146 | Israel | 147.237.0.121 | | Bad TCP sequence | SYN retransmit with different window scale | monitor | 108 |
| 149.78.247.118 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 108 |
| 149.78.225.30 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 92 |
| 49.199.14.15 | Australia | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 92 |
| 149.78.14.139 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 90 |
| 149.78.154.118 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 90 |
| 149.88.217.33 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 86 |
| 149.88.239.57 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 81 |
| 149.78.157.134 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 78 |
| 217.69.133.249 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 78 |
| 66.249.81.254 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 73 |
| 66.249.81.130 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 71 |
| 66.249.75.44 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 69 |
| 149.78.175.124 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 68 |
| 66.249.93.241 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 61 |
| 149.78.46.41 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 56 |
| 66.249.75.28 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 51 |
| 149.78.248.54 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 46 |
| 149.78.151.245 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 45 |
| 149.78.62.3 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 42 |
| 66.249.81.251 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 42 |
| 149.78.225.174 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 40 |
| 66.249.93.247 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 38 |
| 149.78.235.113 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 38 |
| 217.69.133.21 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 35 |
| 66.249.81.254 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 34 |
| 79.183.171.4 | Israel | 147.237.0.121 | | Bad TCP sequence | SYN retransmit with different window scale | monitor | 33 |

## Top Attackers In WAF

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 84.228.192.73 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login | Block | 39 |
| 46.121.42.142 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting | Block | 39 |
| 94.230.83.97 | Israel | 147.237.0.121 | | Untraceable SSL Sessions: Open Mode | None | 26 |
| 37.26.146.166 | Israel | 147.237.0.121 | | Parameter Type Violation ReturnUrl in www.miluim-ishi.aka.idf.il/login | Block | 26 |
| 94.230.86.152 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest | Block | 13 |
| 79.178.49.13 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/changeunit | Block | 13 |
| 46.121.67.20 | Israel | 147.237.0.121 | | Multiple Untraceable SSL Sessions from 46.121.67.20 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)) | None | 13 |
| 46.19.85.210 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 13 |
| 84.228.22.38 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 13 |
| 46.19.86.218 | Israel | 147.237.0.121 | | Parameter Type Violation ReturnUrl in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 109.67.185.150 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition | Block | 13 |
| 79.178.49.13 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/medicalcommitteerequest | Block | 13 |
| 46.19.86.118 | Israel | 147.237.0.121 | | Untraceable SSL Sessions: Open Mode | None | 13 |
| 79.176.204.31 | Israel | 147.237.0.121 | | Cookie Tampering on cookie .ASPXAUTH: Expected E2DA17607D74422E26DCFF92454B109FD18CBACC416F7458BD61F7BD6F0F1ACBCD81E4EB83D2A53AE7080F7D48DD1DE5449443510CC83D1DA9ABA3EA816B05E17B6F62EC5F3572B421B87C216E79CFFBD5C1FECAED14C38106425A8E8C7728CCF1B8EAA615189702F1BCF261D015A43E4A63200961E21B7A8EE4A1BA59F6F62F, Observed 6692EF2A22E09420750A2A8D3AB92ABD06598FDD5F321A9B1FAB7D0116D8BB6790CD23E95F914DB3E035B3B1F7E96FBDCB5C35EFF45C95EB407E0BB71354EF46D0D6DC85EEB53DAA6A888C8908A4CA9D95486A678FD957E9CADD139A54AABCC1B67DCD | None | 13 |
| 46.121.42.142 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting | Block | 13 |
| 2.52.189.68 | Israel | 147.237.0.121 | | Parameter Type Violation ReturnUrl in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 79.183.171.123 | Israel | 147.237.0.121 | | Unknown Parameter returnUrl in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 46.19.86.145 | Israel | 147.237.0.121 | | Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 79.178.29.253 | Israel | 147.237.0.121 | | Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify | Block | 13 |
| 84.108.72.188 | Israel | 147.237.0.121 | | Unknown Parameter ctl00$ContentPlaceHolder1$fuAddDocsFiles in www.miluim-ishi.aka.idf.il/leaveinunit | Block | 13 |
| 46.121.67.20 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 13 |
| 46.19.86.177 | Israel | 147.237.0.121 | | Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login | Block | 13 |
| 46.121.67.20 | Israel | 147.237.0.121 | | Illegal Byte Code Character in Method Ã?Â¸Ã¢ÂªP8>Â»Ã¥Â–Â™HÃ’7Ã¤Â¹Ã‰Â¯Â”Âª[[#6]](DCaÃ‰ÂŽÂ©[[#24]]H[[#0]]Â¸Ã?C[[#7]]Ã?^Ã?UsÃ·Âª[[#15]]Â¸Â³Â¤Ã- | Block | 11 |
| 46.121.67.20 | Israel | 147.237.0.121 | | NULL Character in Header Name at Ã¼D7[[#16]]Ã•[[#21]]xÃŽ[[#0]]Ã˜Ã? [[#6]]Â†a>xÃ¤Ã¡YÂ”[[#20]]ÃšÃ‰ÃŸÃ³UÃ´`4=3Ãº-&Ã‰t[[#27]]Ã²Â‹D&AvÂ¿[[#1]]LÃ‰Æ’FÃ»Â¸7ÂŽÂ“xÃŸÂª[[#25]]Â³Â¼[[#4]]Â¥Â©Ã§ÃµÂ?AÃ§Â™Â±rÃ˜Â²}A[[#20]]Ã“ÃŸ1[[#16]]Kr[[#25]]Ã¶-ÂŒ=Ã“ÃŠÃƒÂ®8ÂšÂ–jÂ’o[[#29]][[#21]]1ÂžI[[#6]]Â†Ã”Ã®Âª[[#5]](ÂªÃŸÃˆÂ–dy[[#3]][[#31]]Â,+•Âž[[#21]]Â¾ÃŸÃ‹4m[[#26]]Ã· | Block | 11 |
| 46.121.67.20 | Israel | 147.237.0.121 | | Malformed HTTP Header Line 5 | Block | 11 |
| 46.121.67.20 | Israel | 147.237.0.121 | | Illegal Byte Code Character in Header Name Ã¼D7[[#16]]Ã•[[#21]]xÃŽ[[#0]]Ã˜Ã? [[#6]]Â† a>xÃ¤Ã¡YÂ”[[#20]]ÃšÃ‰ÃŸÃ³UÃ´`4=3Ãº-&Ã‰t[[#27]]Ã²Â‹D&AvÂ¿[[#1]]LÃ‰Æ’FÃ»Â¸7ÂŽÂ“ xÃŸÂª[[#25]]Â³Â¼[[#4]]Â¥Â©Ã§ÃµÂ?AÃ§Â™Â±rÃ˜Â²}A[[#20]]Ã“ÃŸ1[[#16]]Kr[[#25]]Ã¶-ÂŒ=Ã“ ÃŠÃƒÂ®8ÂšÂ–jÂ’o[[#29]][[#21]]1ÂžI[[#6]]Â†Ã”Ã®Âª[[#5]](ÂªÃŸÃˆÂ–dy[[#3]][[#31]]Â,+•Âž [[#21]]Â¾ÃŸÃ‹4m[[#26]]Ã· | Block | 11 |
| 46.121.67.20 | Israel | 147.237.0.121 | | Malformed URL | Block | 11 |
| 46.121.67.20 | Israel | 147.237.0.121 | | Illegal Byte Code Character in Header Value | Block | 11 |
| 46.121.67.20 | Israel | 147.237.0.121 | | Abnormally Long Header Line request header name | Block | 10 |
| 46.121.67.20 | Israel | 147.237.0.121 | | Unknown HTTP Request Method Ã?Â¸Ã¢ÂªP8>Â»Ã¥Â–Â™HÃ’7Ã¤Â¹Ã‰Â¯Â”Âª[[#6]](DCaÃ‰ÂŽÂ©[[#24]]H[[#0]]Â¸Ã?C[[#7]]Ã?^Ã?UsÃ·Âª[[#15]]Â¸Â³Â¤Ã- in URL | Block | 10 |
| 46.121.67.20 | Israel | 147.237.0.121 | | Abnormally Long Request method | Block | 10 |
| 46.121.67.20 | Israel | 147.237.0.121 | | NULL Character in Method Ã?Â¸Ã¢ÂªP8>Â»Ã¥Â–Â™HÃ’7Ã¤Â¹Ã‰Â¯Â”Âª[[#6]](DCaÃ‰ÂŽÂ©[[#24]]H[[#0]]Â¸Ã?C[[#7]]Ã?^Ã?UsÃ·Âª[[#15]]Â¸Â³Â¤Ã- | Block | 10 |