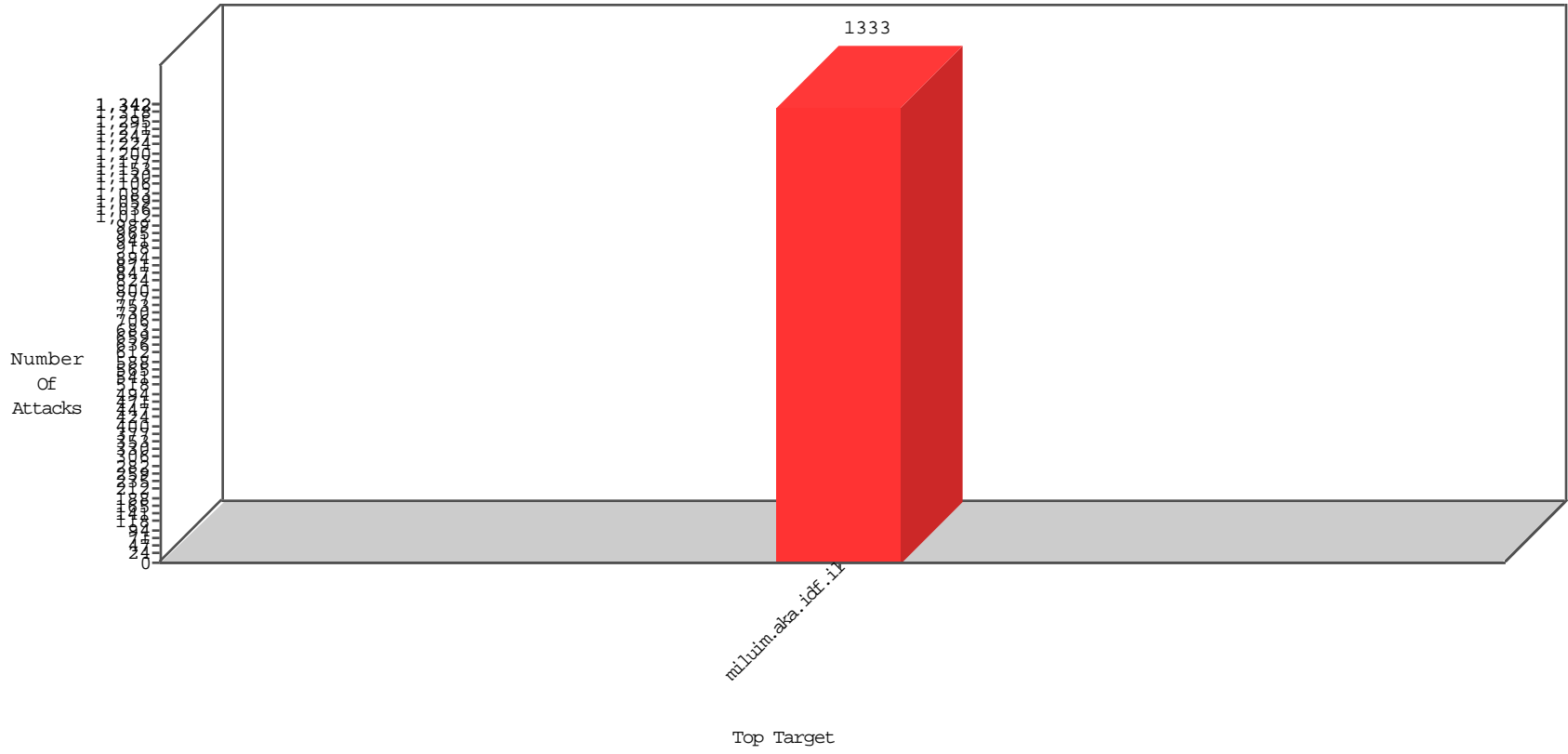


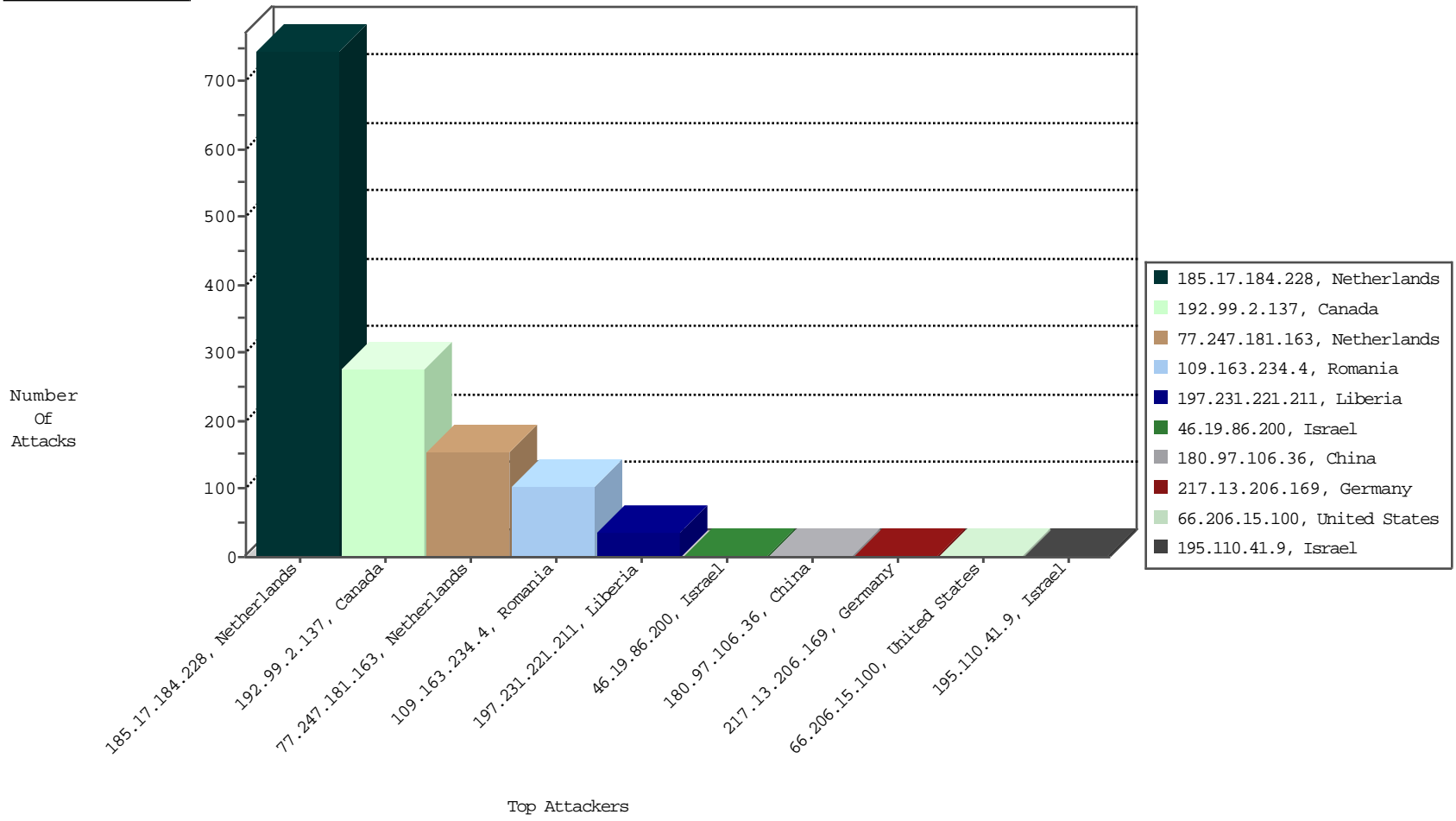
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



01-05-2016 to 01-06-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
217.13.206.169	Germany	147.237.0.120	miluim.aka.idf.il	I4 Source or Dest Port Zero	drop	DP-Tehila	1

01-05-2016 to 01-06-2016

Top Attackers In IPS

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

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
61.244.49.137	Hong Kong	147.237.0.120	miluim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
179.32.85.220	Colombia	147.237.0.120	miluim.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.110.41.9	Israel	147.237.0.120	miluim.aka.idf.i	ET SCAN NMAP -sA (2)	1
51.254.201.78	United Kingdom	147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1
66.206.15.100	United States	147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1
180.97.106.36	China	147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	166348
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	67501
66.249.81.230	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	45350
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	36290
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	31786
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	28712
149.88.238.102	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	3885
8.37.235.181	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2256
157.55.39.248	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1560
149.88.20.145	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1341
89.187.221.12	Lebanon	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1108
68.180.229.121	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1074
149.88.142.117	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1033
2.52.159.178	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	810
149.78.36.247	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	682
183.89.32.145	Thailand	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	472
149.78.25.41	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	424
134.191.232.70	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	380
17.78.98.154	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	269
66.102.9.100	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	269
40.77.167.47	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	257
176.56.230.162	Netherlands	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	243
91.213.8.43	Ukraine	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	196
108.49.242.57	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	167
73.253.173.22	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	163
149.50.89.142	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	162
40.77.167.95	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	150
109.67.125.206	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.66.103.79	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.183.98.214	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.75.227	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	142
149.88.101.143	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	140
149.78.46.99	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	135
212.95.7.122	Austria	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	135
149.78.190.132	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	129
79.173.127.7	Russian Federation	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	127
149.78.96.210	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	121
66.102.9.80	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	120
15.90.166.12	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	114
134.191.232.72	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	114
149.78.112.101	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	113
149.88.231.44	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	110
149.88.2.237	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	109
66.249.81.230	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	109
149.88.93.128	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	106
66.249.93.212	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	102
66.102.9.90	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	100
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	99
66.249.75.219	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	99
149.88.207.71	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	99

01-05-2016 to 01-06-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.17.184.228	Netherlands	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	746
192.99.2.137	Canada	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	277
77.247.181.163	Netherlands	147.237.0.120	miluim.aka.idf.i	Too Many of the Same Response Code (404) in IP from 77.247.181.163	Block	155
109.163.234.4	Romania	147.237.0.120	miluim.aka.idf.i	Too Many of the Same Response Code (404) in IP from 109.163.234.4	Block	101
197.231.221.211	Liberia	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
212.235.34.6	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/resource/userfollowresource/create/	Block	1
46.19.86.200	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 46.19.86.200	Block	1
46.19.86.200	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/8	Block	1
198.20.69.74	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
82.166.140.117	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1408-he/miluim.aspx?aež	Block	1
46.116.160.118	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	1
212.25.81.122	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1408-he/miluim.aspx?aež	Block	1
109.163.234.4	Romania	147.237.0.120	miluim.aka.idf.i	Too Many 404: Response Code per IP	Block	1
37.142.64.66	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/6_s3_	Block	1
193.43.246.250	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/994-8344-he/miluim.aspx	Block	1
77.247.181.163	Netherlands	147.237.0.120	miluim.aka.idf.i	Too Many 404: Response Code per IP	Block	1

01-05-2016 to 01-06-2016