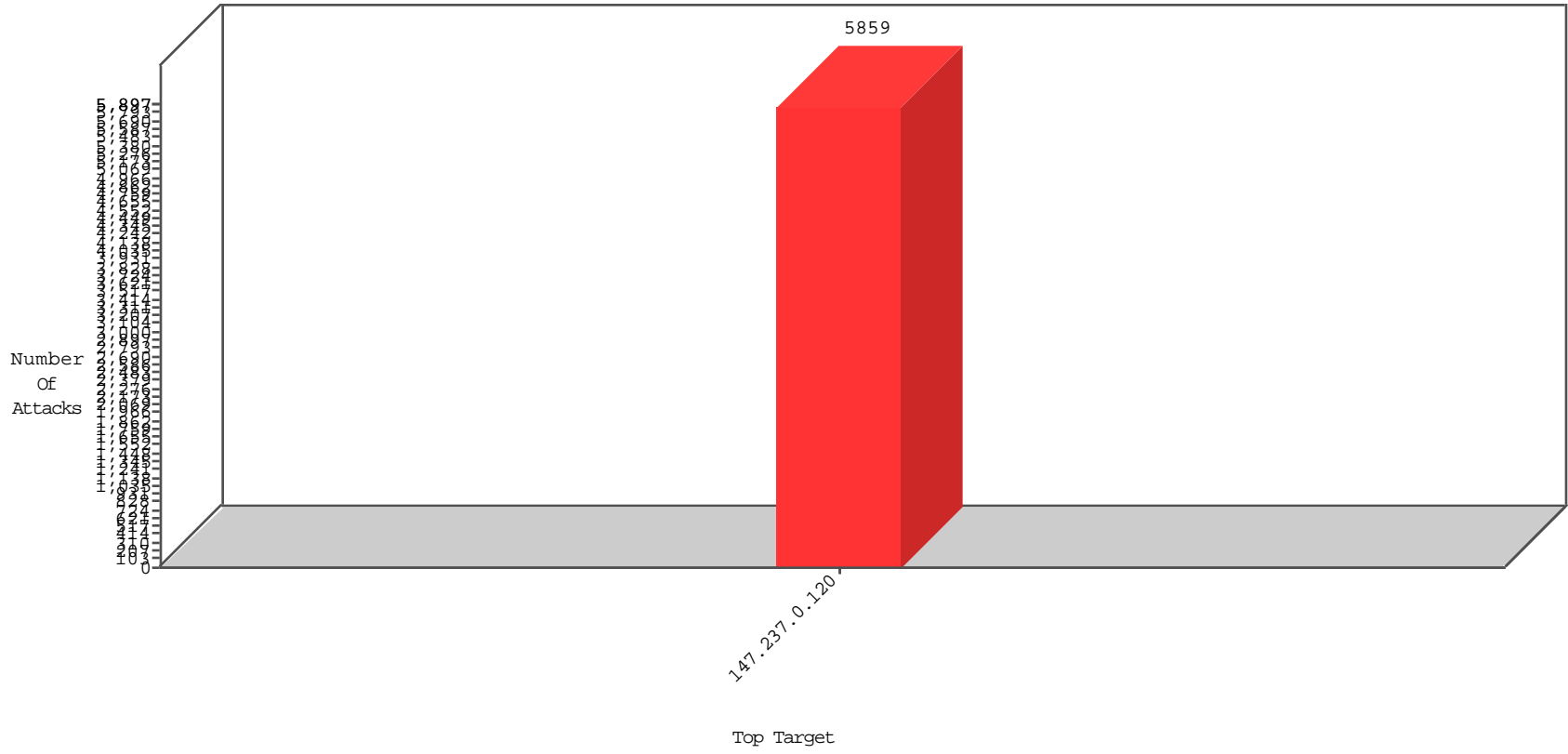


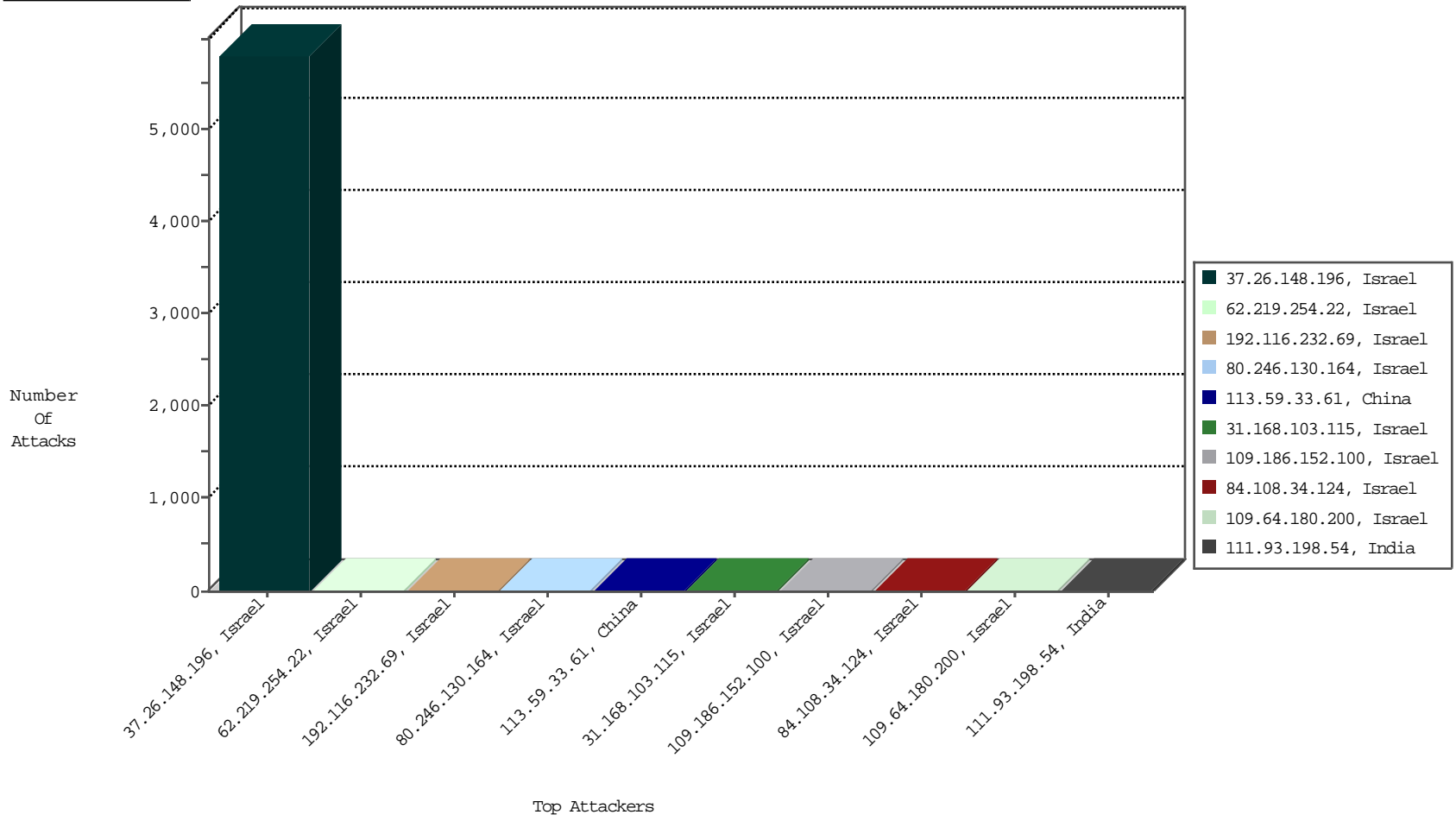
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
37.26.148.196	Israel	147.237.0.120		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	5813
62.219.254.22	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	12

11-12-2015 to 11-13-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.186.152.100	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	2
213.8.7.250	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
111.93.198.54	India	147.237.0.120		ET SCAN NMAP -sS window 1024	1
113.59.33.61	China	147.237.0.120		ET SCAN NMAP -f -sS	1
113.59.33.61	China	147.237.0.120		ET SCAN NMAP -sS window 4096	1
88.198.167.80	Germany	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
111.93.198.54	India	147.237.0.120		ET SCAN NMAP -sS window 4096	1
113.59.33.61	China	147.237.0.120		ET SCAN NMAP -sS window 2048	1
163.53.247.165	Macau	147.237.0.120		ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.120		ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	5026
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	4945
66.249.93.207	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	3649
168.63.137.102	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	3329
2.52.179.174	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3069
2.52.26.0	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2516
2.52.147.242	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
82.80.128.20	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
168.63.139.43	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2053
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1625
37.26.147.239	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1440
149.78.172.84	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1008
151.15.111.43	Italy	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	955
82.196.42.196	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	750
66.249.67.98	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	691
66.249.67.110	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	655
66.249.67.104	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	544
195.16.162.218	Germany	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	448
2.52.145.94	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
149.88.20.78	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	394
149.78.41.33	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	388
149.88.94.179	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	383
157.55.39.64	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	350
149.78.64.16	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	330
149.78.46.152	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	329
149.78.54.244	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	292
2.54.186.39	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
66.249.73.212	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	279
207.38.145.2	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	273
66.249.73.220	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	260
66.249.67.98	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	247
66.249.73.228	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	245
149.78.235.162	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	241
168.63.200.167	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	227
66.249.93.199	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	226
149.78.47.132	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	224
66.249.67.110	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	223
66.249.93.207	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	211
66.249.67.104	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	201
66.249.93.203	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	199
77.127.204.95	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.67.22.10	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
84.229.31.140	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.183.210.112	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.178.113.223	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.164.56	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.73.212	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	140
62.182.37.132	Russian Federation	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	129
149.88.190.86	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	123
149.88.110.13	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	121

11-12-2015 to 11-13-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
31.168.103.115	Israel	147.237.0.120		Multiple Unauthorized URL Access from 31.168.103.115	Block	2
192.116.232.69	Israel	147.237.0.120		Multiple Unauthorized URL Access from 192.116.232.69	Block	2
109.64.180.200	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	2
80.246.130.164	Israel	147.237.0.120		Redundant HTTP Headers from 80.246.130.164	Block	2
84.108.34.124	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	2
132.72.229.202	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he.miluim.aspx	Block	1
79.181.35.252	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	1
176.13.2.33	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
95.86.103.165	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
132.74.212.136	Israel	147.237.0.120		Unauthorized URL Access to miluim.aka.idf.il/1355-he/miluim	Block	1
80.246.130.164	Israel	147.237.0.120		Redundant HTTP Headers Referer	Block	1
31.168.103.115	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
168.235.198.195	United States	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/*?â€Ž	Block	1
192.116.232.69	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
109.67.111.237	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
79.178.4.177	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
176.12.148.190	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
2.54.143.99	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1

11-12-2015 to 11-13-2015