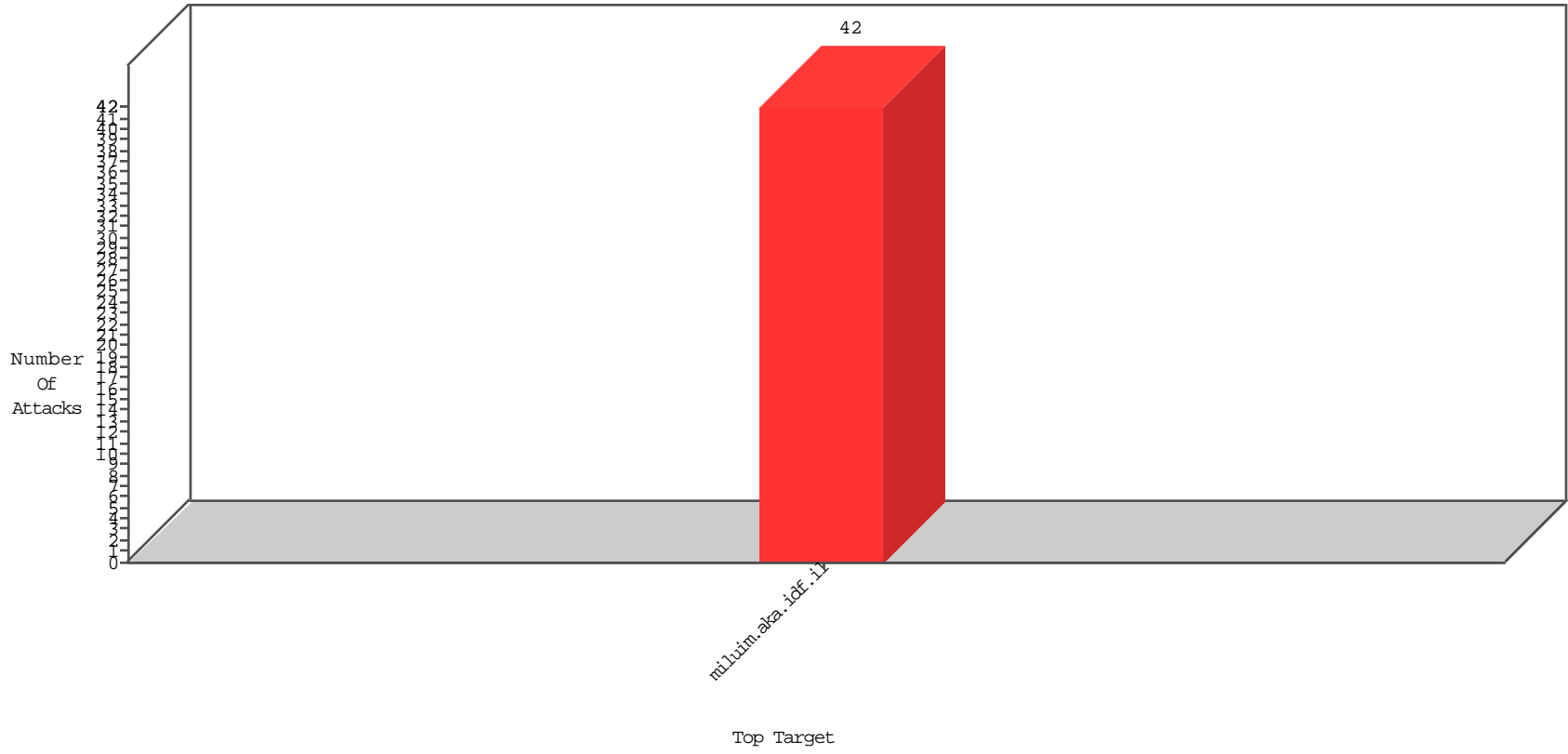


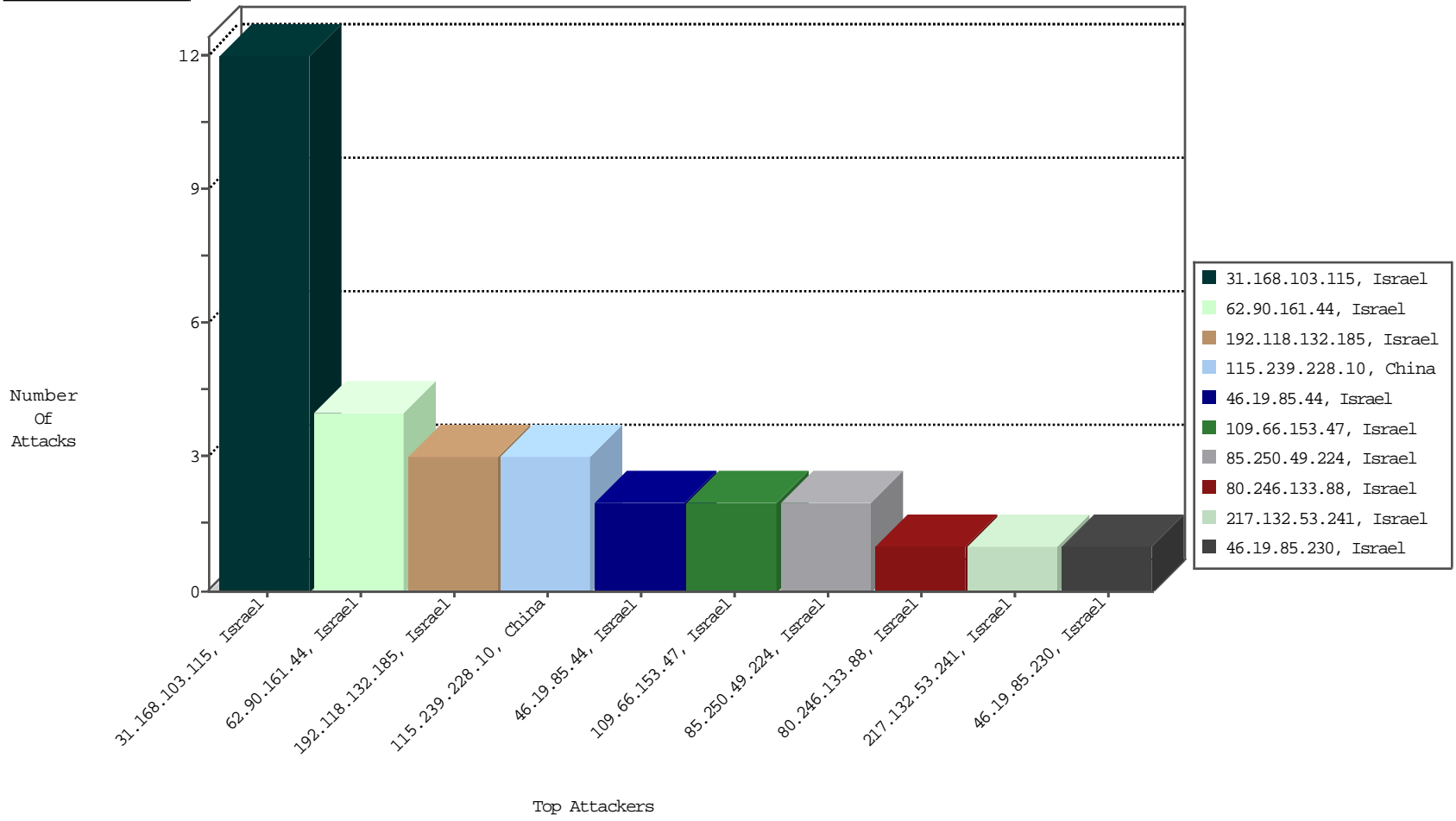
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
192.118.132.185	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	EEL-Israel	3
115.239.228.10	China	147.237.0.120	miluim.aka.idf.il	Frk_Under_Attack_Con_Http	drop	EEL-Frankfurt	2
115.239.228.10	China	147.237.0.120	miluim.aka.idf.il	Frk_Purple_Con_Limit_Http	drop	EEL-Frankfurt	1
52.91.59.24	United States	147.237.0.120	miluim.aka.idf.il	Invalid TCP Flags	drop	EEL-Israel	1

12-24-2015 to 12-25-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
62.90.161.44	Israel	147.237.0.120	miluim.aka.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	1

12-24-2015 to 12-25-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
87.158.99.108	Germany	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
190.208.55.250	Chile	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
137.116.113.55	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
223.4.144.212	China	147.237.0.120	miluim.aka.idf.il	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	206041
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	49949
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	42177
66.249.81.230	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	42146
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	30137
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	27730
79.176.119.191	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4608
216.185.58.15	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4413
141.0.14.218	Europe	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2739
109.65.230.228	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
207.232.27.5	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	2209
149.88.30.24	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1188
2.54.143.223	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1152
157.55.39.174	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1121
149.78.175.150	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	972
68.180.229.121	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	919
149.78.246.77	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	871
149.88.24.54	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	706
181.21.133.109	Argentina	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	579
66.249.93.212	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	456
66.249.93.215	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	384
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	383
168.63.137.102	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	310
40.77.167.37	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	262
165.225.72.81	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	229
143.176.244.40	Netherlands	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	157
149.78.14.206	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	155
157.55.39.136	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	151
181.21.146.219	Argentina	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	150
77.126.86.165	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.102.9.90	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	144
109.64.117.249	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.61.75.18	Hungary	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	144
149.78.11.39	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	141
149.88.127.48	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	141
93.12.45.39	France	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	140
149.78.10.81	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	138
66.102.9.80	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	134
66.249.81.227	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	121
157.55.39.54	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	119
88.176.38.40	France	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	112
51.175.93.165	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	112
157.55.39.137	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	106
213.57.129.164	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	93
66.249.81.224	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	92
66.249.81.230	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	92
149.78.21.26	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	90
149.88.153.5	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	88
40.77.167.20	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	84
85.115.52.201	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	81

12-24-2015 to 12-25-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
31.168.103.115	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 31.168.103.115	Block	12
85.250.49.224	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1405-he/miluim.aspx?â€Ž	Block	2
109.66.153.47	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1403-he/miluim.aspx?â€Ž	Block	2
2.54.48.174	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-	Block	1
62.219.237.196	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1393-	Block	1
46.19.85.44	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL	Block	1
109.67.147.171	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.67.147.171	Block	1
62.90.161.44	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 62.90.161.44	Block	1
80.246.133.88	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1405-he/miluim.aspx?â€Ž	Block	1
46.19.85.44	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method ;q=0.8,he;q=0.6 in URL	Block	1
217.132.53.241	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1400-he/miluim.aspx?â€Ž	Block	1
62.90.161.44	Israel	147.237.0.120	miluim.aka.idf.i	Multiple _vti_ from 62.90.161.44	Block	1
37.26.149.147	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1403-	Block	1
46.19.85.230	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1402-he/miluim.aspx?â€Ž	Block	1
62.90.161.44	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/_vti_bin/owssvr.dll	Block	1
37.26.149.243	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1403-	Block	1
46.19.86.68	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1399-he/miluim.aspx?â€Ž	Block	1

12-24-2015 to 12-25-2015