Focused IP Under Attack Daily Report

Top Targets

50

Number
Of
Attacks

miluim.aka.idf.il

Top Target

Top Attackers

Number
Of
Attacks

Top Attackers

Legend:

- 194.114.146.227, Israel
- 46.19.86.233, Israel
- 81.218.56.171, Israel
- 212.179.146.174, Israel
- 81.218.56.245, Israel
- 37.142.64.63, Israel
- 2.54.30.141, Israel
- 120.150.29.211, Australia
- 1.246.130.20, Korea, Republic of
- 176.13.14.119, Israel
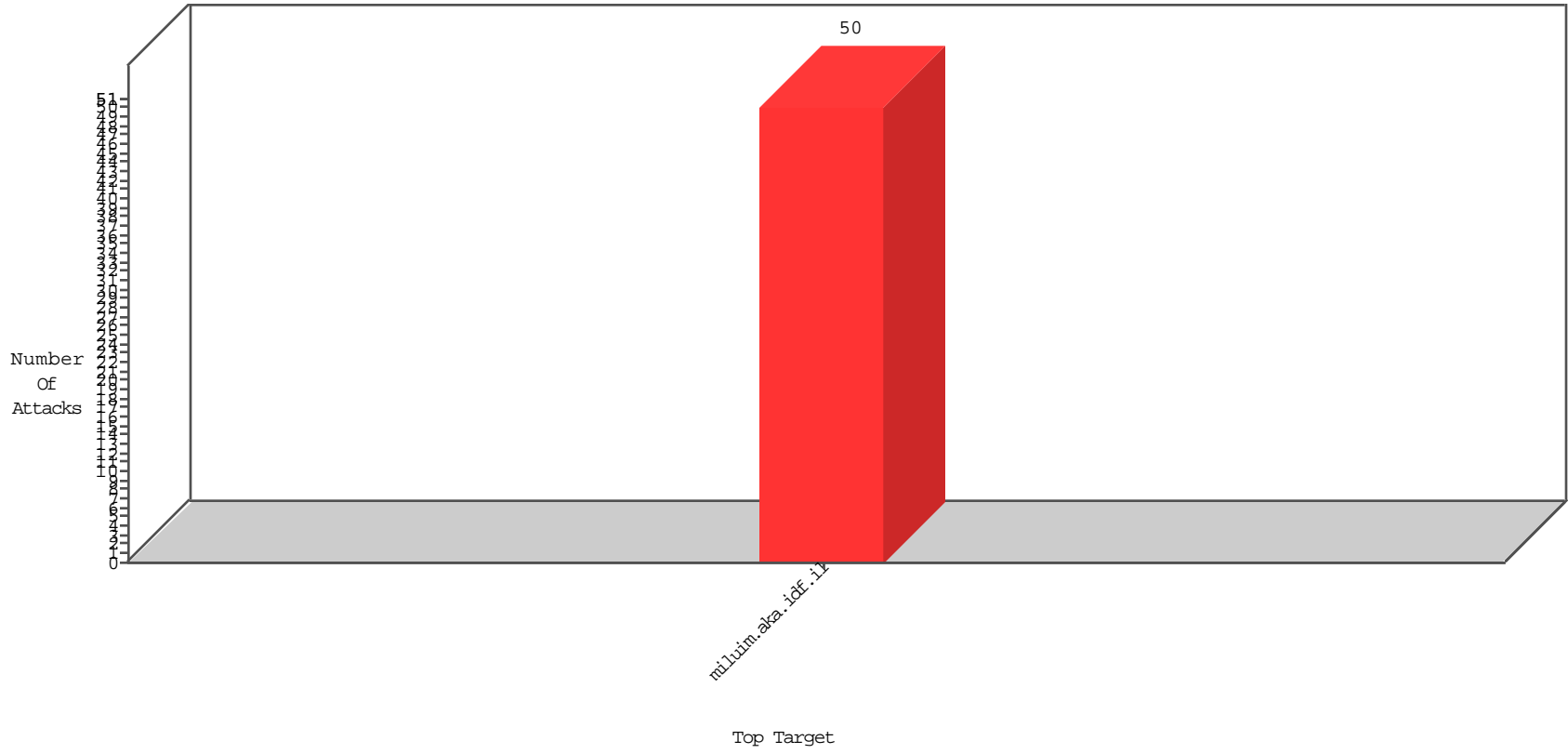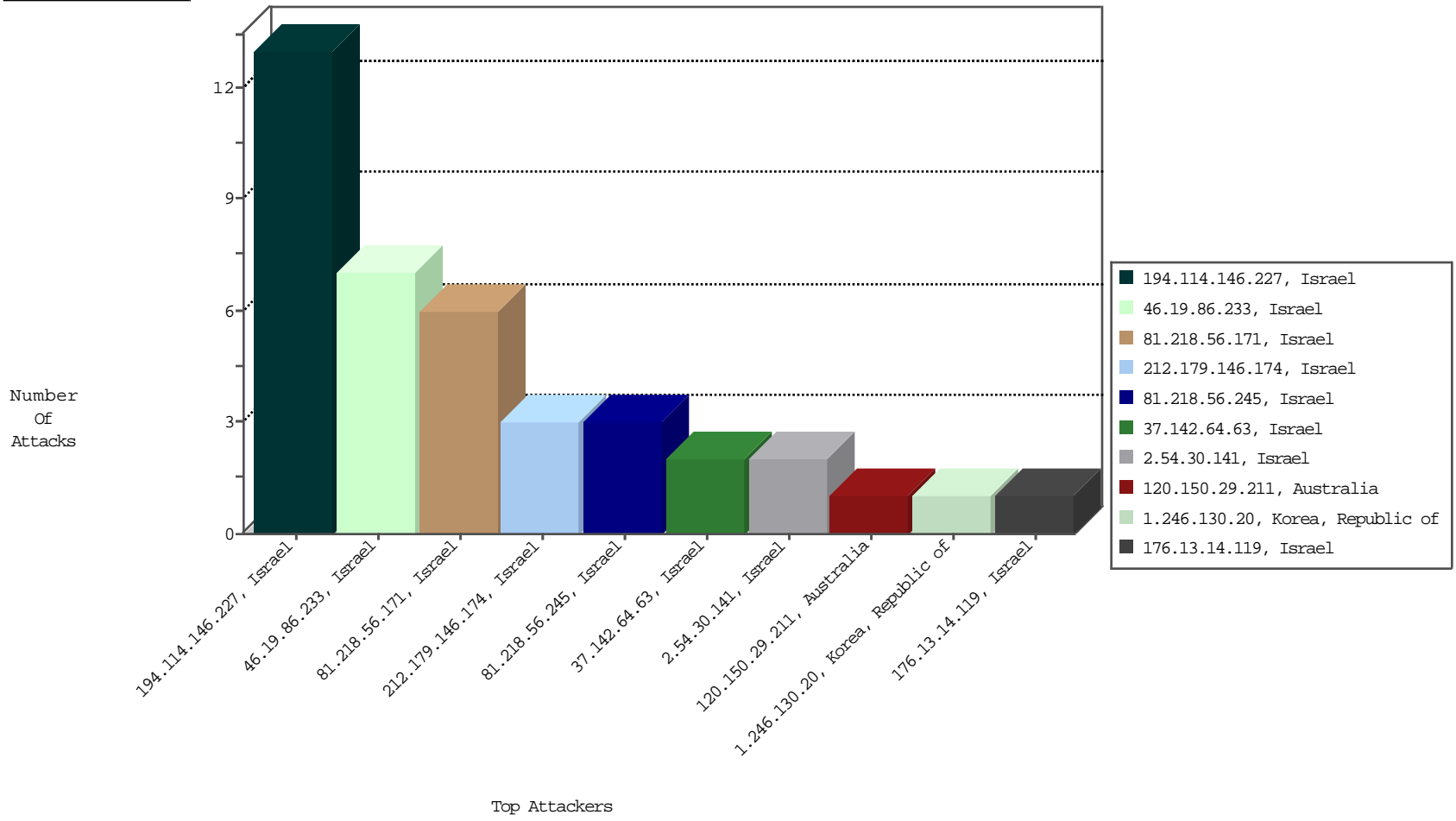
Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
81.218.56.245	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
212.179.146.174	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
108.161.253.41	United States	147.237.0.120	miluim.aka.idf.il	L4 Source or Dest Port Zero	drop	BBL-Israel	1

12-16-2015 to 12-17-2015

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
46.19.86.233	Israel	147.237.0.120	miluim.aka.idf.i	POLICY-OTHER TCP packet with urgent flag attempt	7
37.142.64.63	Israel	147.237.0.120	miluim.aka.idf.i	ET SCAN NMAP -sA (2)	2
1.246.130.20	Korea, Republic of	147.237.0.120	miluim.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.210.195.132	Qatar	147.237.0.120	miluim.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
108.184.162.6	United States	147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1
124.74.213.36	China	147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1
120.150.29.211	Australia	147.237.0.120	miluim.aka.idf.i	ET SCAN NMAP -sS window 3072	1
171.232.56.108	Vietnam	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
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	50383
141.0.15.36	Europe	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	35135
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	22168
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	17911
66.249.93.3	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	11838
149.78.237.23	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	6404
66.249.93.6	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4797
66.249.93.9	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	3263
66.44.32.210	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	626
157.55.39.142	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	505
199.207.253.96	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	450
17.138.55.234	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	314
149.78.229.205	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	287
207.59.14.130	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	285
2.52.130.221	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	274
149.88.54.170	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	272
68.180.229.121	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	271
149.88.80.46	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	263
64.236.4.1	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	235
72.37.140.47	Italy	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	203
134.191.232.68	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	177
207.46.13.40	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	165
207.46.13.169	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	158
66.249.66.52	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	151
205.167.7.247	France	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	145
82.166.91.164	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.64.152.81	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.182.128.45	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.183.33.236	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.33.79	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
51.175.93.165	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	138
149.88.225.136	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	135
157.55.39.61	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	134
46.19.86.51	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	130
186.107.85.34	Chile	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	125
95.108.132.183	Russian Federation	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	123
202.182.0.200	Thailand	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	122
207.46.13.30	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	115
149.88.216.167	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	112
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	110
149.78.235.251	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	102
66.102.9.100	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	92
66.249.66.49	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	88
134.191.232.70	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	82
66.249.93.212	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	82
79.183.96.141	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
207.46.13.126	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	79
85.115.52.201	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	78
108.196.31.101	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	73
66.249.66.52	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	70

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 194.114.146.227	Block	10
81.218.56.171	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 81.218.56.171	Block	5
2.54.30.141	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1388-he/miluim.aspxâ€?â€Ž	Block	2
194.114.146.227	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	2
2.54.3.197	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
194.114.146.227	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/7/1697.png	Block	1
79.180.63.130	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1381-he/miluim.aspxâ€?â€Ž	Block	1
176.13.7.5	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1388-he/miluim.aspxâ€?â€Ž	Block	1
176.13.14.119	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€¬	Block	1
31.168.74.208	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/homepage.aspx	Block	1
81.218.56.171	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/3/size220x0/1943.png	Block	1
46.19.85.103	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
109.253.158.109	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.253.158.109	Block	1

12-16-2015 to 12-17-2015

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count