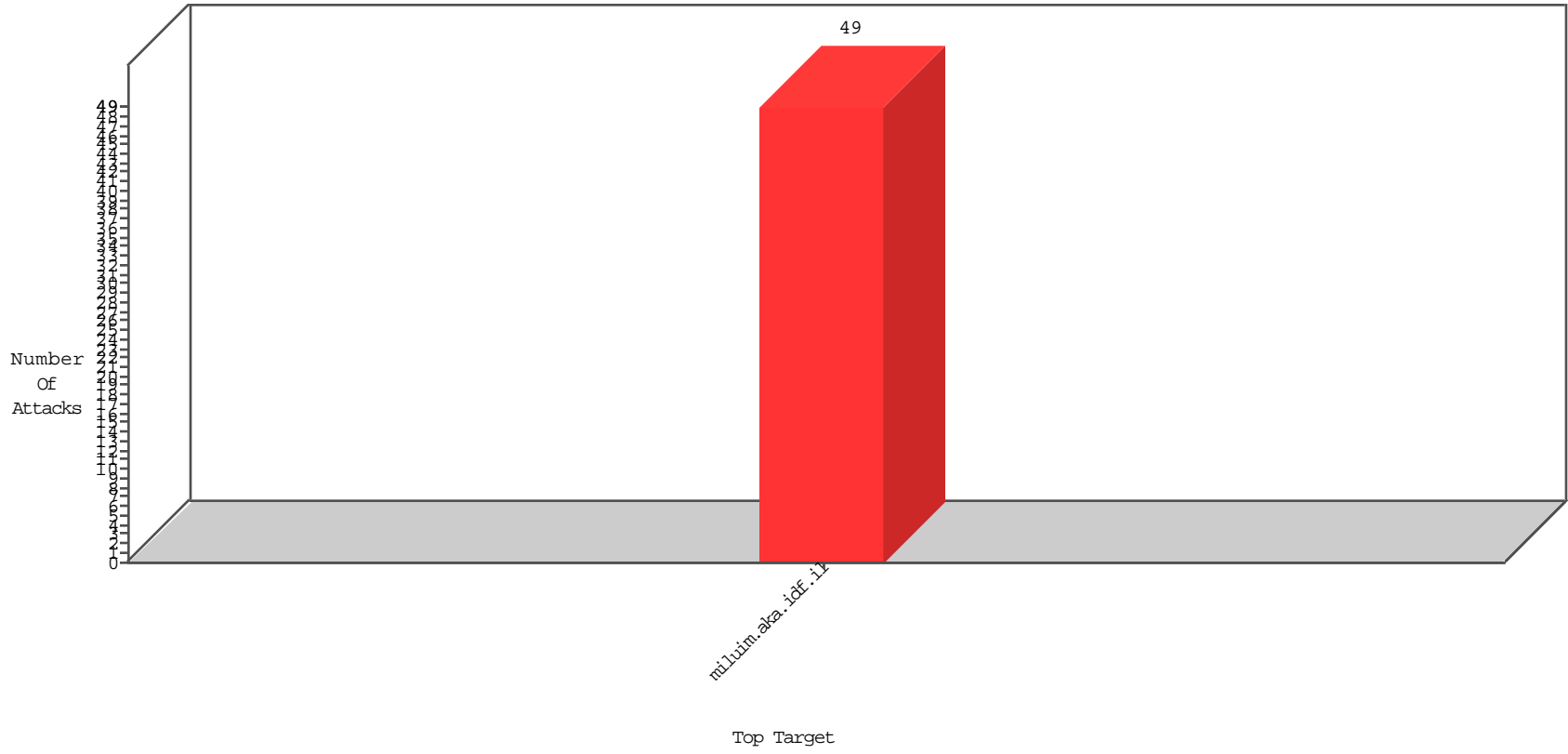


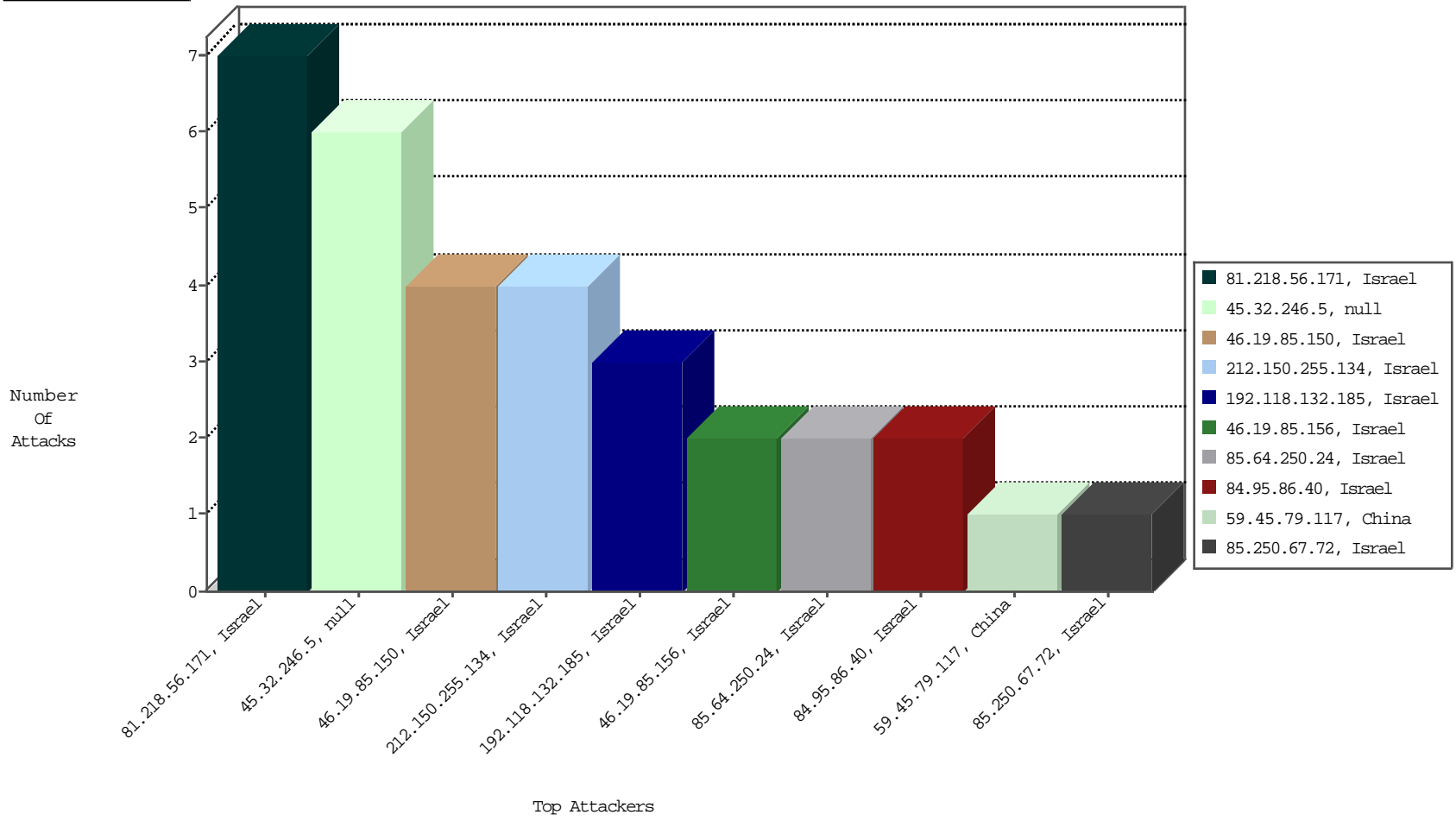
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



12-09-2015 to 12-10-2015

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	BEL-Israel	3
45.32.246.5		147.237.0.120	miluim.aka.idf.il	Invalid TCP Flags	drop	BEL-Frankfurt	2
109.67.139.29	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	1

12-09-2015 to 12-10-2015

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
45.32.246.5		147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
82.166.184.187	Israel	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
111.207.163.88	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
223.4.174.30	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.246.5		147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -f -sS	1
45.32.246.5		147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.21	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
114.215.111.222	China	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.229.53.89	Japan	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5		147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.198	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	295585
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	268142
66.249.93.202	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	116613
66.249.93.206	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	107471
66.249.81.230	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	61729
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	57644
2.52.130.59	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4349
207.46.13.59	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	3534
2.54.180.84	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
84.229.131.219	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
109.65.62.102	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.182.30.208	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.179.191.10	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
84.228.166.170	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
149.78.134.165	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2124
68.180.229.121	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	982
207.46.13.17	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	884
149.88.7.210	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	796
40.77.167.98	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	788
2.54.178.55	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	765
2.54.56.14	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	729
149.88.145.157	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	664
40.77.167.65	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	593
149.78.76.61	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	568
149.78.167.132	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	550
149.78.174.62	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	452
149.88.193.52	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	400
149.78.49.182	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	329
192.88.162.1	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	324
66.102.9.100	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	314
66.249.93.198	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	288
63.232.147.98	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	272
2.52.152.161	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	256
199.207.253.101	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	255
66.249.93.206	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	246
40.77.167.8	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	226
85.130.199.157	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	226
85.130.199.157	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	226
149.88.198.173	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	223
168.63.139.43	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	219
66.249.93.202	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	217
66.102.9.80	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	194
15.90.166.11	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	192
167.220.196.29	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	186
66.102.9.90	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	178
66.249.81.227	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	178
141.0.14.217	Europe	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	176
66.249.81.224	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	170
149.88.127.48	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	168
149.88.5.166	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	161

12-09-2015 to 12-10-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.218.56.171	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 81.218.56.171	Block	6
212.150.255.134	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	2
46.19.85.150	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method pk_id.104.b624=406albecal9c4c65.1449680414.1.1449680414.1449680414. ; in URL _pk_ses.104.b624=*	Block	1
192.114.87.5	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1381-he	Block	1
85.64.250.24	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 85.64.250.24	Block	1
79.176.18.233	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to ww.miluim.aka.idf.il/1359	Block	1
46.19.85.150	Israel	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
109.226.14.172	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 109.226.14.172	Block	1
84.95.86.40	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 84.95.86.40	Block	1
46.19.85.156	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL	Block	1
212.150.255.134	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.150.255.134	Block	1
85.64.250.24	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
46.19.85.150	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version	Block	1
109.226.21.155	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/valtam	Block	1
84.95.86.40	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1384-he/miluim.aspx?â€Ž	Block	1
46.19.85.156	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method q=0.4 in URL	Block	1
85.250.58.191	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1378	Block	1
81.218.56.171	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
46.19.85.150	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL _pk_ses.104.b624=*	Block	1
185.35.62.11	Switzerland	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
85.64.137.254	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1359-he/milu	Block	1
46.19.85.236	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1	Block	1
46.19.85.44	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1381-he/miluim.aspx?â€Ž	Block	1
212.150.255.134	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1
85.250.67.72	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter _ in www.miluim.aka.idf.il/1203-he/miluim.aspx	Block	1
81.218.241.26	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/	Block	1

12-09-2015 to 12-10-2015